Research of Security and Reliability for In-Vehicle FlexRay Bus Network Based on Message Perception Method

Yujing Wu, Yihu Xu, Shinan Wang, Jingyi Jia, and Yinan Xu*

***Abstract*—The in-vehicle bus network is the main tool for transferring data between automotive electronic control systems. This study focuses on the network security of the in-vehicle FlexRay bus network. The objective is to improve the fault information detection and fault tolerant control technology of FlexRay bus network information by using advanced technologies such as big data management and optimal guaranteed performance. For the problem of fault information detection in the data layer, an anomaly detection system of information and a message perception module based on the message perception method are proposed. We are keen to capture the horizontal and vertical correlation of FlexRay bus network information. Automatic correction of fault information through up and down message perception methods achieve the goal of fault-tolerant control. We have built the Hardware-in-the-Loop Simulation (HILS) experimental architecture using bus information from real vehicles and an automotive-specific bus network design platform. The security and operability of the proposed anomaly detection system of information and fault tolerance control scheme are verified. The experimental simulation results show that the detection accuracy of anomaly information in the vehicle FlexRay bus network reaches 99%.**

***Index Terms*—In-vehicle network security, FlexRay, anomaly detection of information, message perception, fault-tolerant control**

I. Introduction

FlexRay is an attentative network communication protocol developed by the FlexRay consorting to govern on-board automative computing. With the continuous development of automotive electronics technology, the intelligent technology of automobiles has been mature. In the field of automotive network security, the security and reliability of in-vehicle bus networks are receiving more and more attention. After the launch of Advanced Driver Assistance (ADAS) and autonomous driving, vehicle power and brake control need to be partially or fully authorized to the intelligent driving system, and the vehicle is easily exposed to the Internet. If the intelligent driving system is hacked, the consequences will be unimaginable. [1]

How to guarantee the security and reliability of in-vehicle network is one of the difficulties that need to be solved in the automotive industry, and it brings us a new research direction. However, the development of in-vehicle network is facing many challenges. The network security, data management and network topology architecture technology of in-vehicle bus network traditionally lack theoretical guidance and have strong arbitrariness and hardware dependency.

In 2014, at the Internet Security Conference, the door locks of a Mercedes-Benz car were remotely cracked by 360 technicians. In 2015, two technicians remotely hacked into a Jeep Cherokee and managed to control the car's entertainment system and engine, steering, and other control systems, and the driver lost control of the vehicle [1]. The development of connected cars has been followed by malicious attacks, illegal control, private theft and so on. However, relevant security specifications for automobiles have been stopped in their tracks, and international standardization organizations such as ISO, IEEE, and SAE have stagnated in the framework stage without specific detailed specifications for the security of connected cars [2, 3].

360 has developed a system for Controller Area Network (CAN) bus intrusion detection, which implements anomaly detection of information by means of machine learning [4]. M. Kang and J. Kang [5] applies deep neural networks for supervised anomaly detection and compares the detection effects of networks with different depths. In Song *et al.*'s research [6], an in-vehicle network intrusion detection method based on CAN message time interval analysis is proposed. Time interval is an important factor for detecting abnormal CAN bus data in real-time, but this method cannot detect tampering with the data content and does not possess the ability to detect non-periodic signals.

Wu *et al.* [7] presents a method for detecting anomalous data based on the application of an information entropy approach. This method requires intercepting data for a period of time for judgment and has modest real-time performance. Liu *et al.* [8] analyzes the bus network security defects and possible network attack methods for FlexRay vehicle bus network system, and it proposes an encryption authentication protocol based on AES-128 and SHA-1 algorithms.

In Wang and Xu's research [9], a network optimization scheme with a composite deadline algorithm is proposed for FlexRay dynamic segments. The priority of message transmission is affected by the size of the ratio of cutoff period to message length, which effectively shortens the transmission time and thus improves the network utilization. In Jin *et al.*'s research [10], a signal creating method is proposed based on the message transmission characteristics of static segments and performance evaluation indexes, with bandwidth utilization as the constraint, and using a adaptation algorithm. On the basis of message packing, message scheduling strategy with static time slots multiplexed by multiple FIDs is constructed, which minimizes the required FIDs for the system.

Most recently, to stengthen the security level and robutness, Piao *et al.* [11] recommended using ECC (Elliptic Curves Cryptography) encryption algorithm and dual channel model

Manuscript received June 19, 2022; revised October 17, 2022; accepted November 3, 2022.

Yujing Wu and Yihu Xu are the first authors, and Yinan Xu is the corresponding author. The authors are with the College of Engineering of Yanbian University, Yanji 133002, China.

*Correspondence: ynxu@ybu.edu.cn

DOI: 10.7763/IJCTE.2023.V15.1328

for the security framework, which can reduce bandwidth by 25% so as to decrease the computational time.

This paper is structured as follows: Section II proposes an anomaly detection method for information based on message perception method. We establishes the FlexRay message set based on SAE standards and information from actual automotive buses. Section III analyzes the simulation experimental results by building an in-vehicle bus network architecture and experimental platform based on the combination of software and hardware. Section IV summarizes the whole paper.

II. Proposed Method

The data of all things are closely correlated, and the relationship between transactions can be described by association rules, which have been widely used in many aspects, especially in data mining. The anomaly detection architecture based on message perception proposed in this paper is shown in Fig. 1, which explores the correlation between messages through the perception of them, so as to achieve the purpose of anomaly detection.

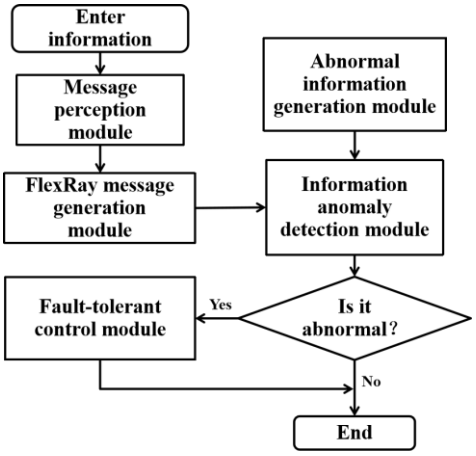


Fig. 1. Anomaly detection architecture.

First, the information message set is input to the message perception module, which enables the study of the message correlation and outputs the horizontal and vertical correlation rules of the on-board bus messages. The correlation rules generated by the message sensing module are combined with SAE standards in the message generation module, and the FlexRay bus message generation work is realized by program writing. Based on the breaking message correlation, an exception message generation model is designed to insert a message into the message data set. The abnormal messages in the message data set are accurately detected by the abnormality detection module. Through the former N message detection method, the abnormal messages are fault-tolerantly controlled, and the purpose of securing the on-board bus is finally realized.

A. Analysis of Bus Message Data from Actual Vehicles

FlexRay networks cannot read the bus information directly with the OBD-II interface due to the protection of the gateway, which requires a corresponding password or cracked password. This is one of the reasons why there has been less research on anomaly detection for FlexRay networks. There are many kinds of anomaly detection studies for CAN bus, while the communication method and data frame format of FlexRay network are slightly different from CAN, so it is difficult to apply these methods directly to the FlexRay network. Therefore, we designed a module to simulate the generation of FlexRay bus information.

Combining SAE protocol and automotive bus information planning table (as shown in Table I) with the extracted real driving information (to which Fig. 2 belongs), the module analyzes the combination and sending law of bus information the concept of longitudinal-horizontal information correlation. It is found that there is a certain regularity of load content in the data frame. The information semantics under the same ID are correlated, since the parameters related to power and speed, such as vehicle speed, engine speed, torque, etc., are under the same ID. Thus, it is understood that the in-vehicle bus information can be divided into power system data, control system data, multimedia data, etc. Suitable and correlated signals need to be selected to create tables for effective planning of data frames.

TABLE I: Automotive Bus Information Planning Table

Signal label	Signal designation	Bit add.	Bit ind.	Init. value
TCS_REQ	Request TCS	0	1	00H
MR_ REQ	Request for drag control functions	1	1	00H
TCS_PAS	TCS “passive” indication	2	1	00H
TCS_GSC	TCS gear shift characteristic	3	1	00H
ABS_DEF	ABS “defective” indication	7	1	00H
TCS_DEF	TCS “defective” indication	8	1	00H
TCS_CTL	TCS “control” indication	9	1	00H
ABS_ACT	ABS (or TCS) active signal	10	1	00H
EBD_DEF	EBD “defective” indication	11	1	00H
ESP_PAS	ESP disabled by user	12	1	00H
ESP_DEF	ESP “defected”	13	1	00H
ESP_CTL	ESP active	14	1	00H
WHEEL	Mean front wheel velocity	16	8	00H
TQI_TCS	Torque intervention for TCS	24	8	FFH
TQI_MSR	Torque intervention for drag controls	32	8	00H
TQI_TCS	Slow torque intervention for TCS	40	8	FFH

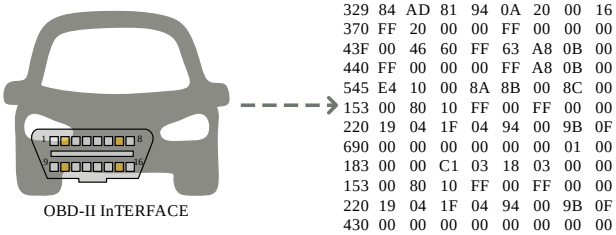


Fig. 2. Real-time information of vehicle bus.

The meaning of each piece of information in the corresponding data frame can be interpreted, including the signal name, signal semantics, and the position of the signal in the data frame. Based on the vehicle bus information

planning table, the actual vehicle bus big data information is used to generate a reliable and characteristic information set for the FlexRay bus information.

Based on the contents of the planning table, the message generation scheme is implemented through in the Spyder compilation environment. By understanding the basics of on-board bus messages, the ID value is set for each message, and the ID value in the figure is set arbitrarily. According to the data frame planning table, different types of signals are planned, and the generated data load length varies from 1 byte to 8 bytes, fully reflecting the characteristics of FlexRay messages and how they differ from other buses. The generated FlexRay information set is shown in Fig. 3 after a practical operation in Python.

```
[ '010' , '29' , '22' , '07' , '7E' ]
[ '020' , '41' , '29' , '58' , '0C' ]
[ '050' , '00' , '00' ]
[ '030' , '02' ]
[ '040' , '40' , 'BA' , '84' , '0C' , '00' , '20' , 'FF' ]
[ '329' , '40' , 'BA' , '84' , '0C' , '00' , '20' , 'FF' , '14' ]
[ '545' , 'FA' , '82' , '01' , '8B' , '00' , '00' , '00' , '00' ]
[ '440' , '00' , '00' , '07' , '04' , 'FF' , 'B2' , '0A' , '00' ]
[ '010' , '82' , 'A4' , '0A' , '00' ]
[ '020' , '41' , '29'  , '58' , '0C' ]
[ '050' , '00' , '00' ]
[ '030' , '7E' ]
[ '040' , '40' , 'BA' , '84' , '0C' , '00' , '20' , 'FF' ]
[ '260' , '00' , '00'  , '29' , '00'  , '00' , '00' , '00' , '00' ]
[ '2A0' , '00' , '00' , '6D' , '1F' , '7B' , '08' , 'FB' , '02' ]
[ '010' , '00' , '20' , 'FF' , '14' ]
[ '020' , '41' , '2C' , '60' , '0C' ]
[ '050' , '00' , '00' ]
[ '030' , '00' ]
[ '040' , '40' , 'BA' , '84' , '0C' , '00' , '20' , 'FF' ]
[ '43F' , '01' , '45' , '40' , 'FF' , '82' , 'A4' , '0A' , '00' ]
```

Fig. 3. FlexRay information set.

B. Message Perception Module

Based on in-vehicle FlexRay network bus information, this paper proposes the design scheme of message perception module in Fig. 4.

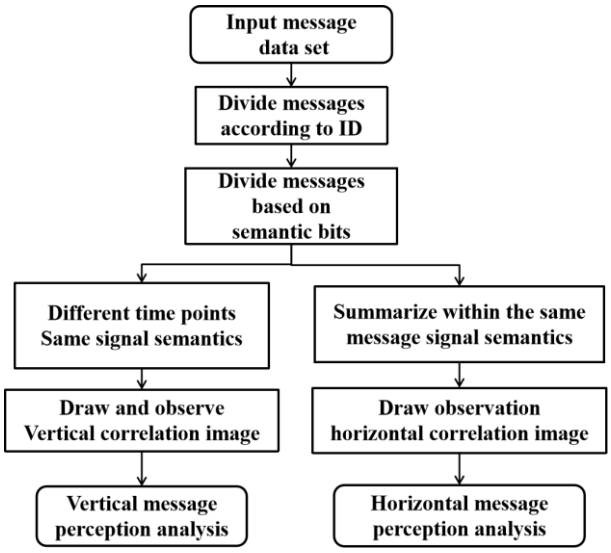


Fig. 4. Flow chart of message perception module.

The bus information is input to the message perception module, the information correlation of the upper and lower messages is analyzed, and the horizontal and vertical correlation rules of the bus information are output. In the FlexRay message generation module, the correlation rules generated by the message perception module are combined with the SAE standard to generate the FlexRay data frame structure. With the information anomaly detection module, the anomalous information in the information dataset is detected accurately. By using a multi-point information fusion method, the abnormal information is fault-tolerantly controlled. Thus, the safety and reliability purpose of the on-board FlexRay bus network is further improved.

First of all, vehicle bus information is divided by searching the ID types contained in the dataset row by row, and creating datasets for different ID types for loading each message in a separate set. ID bits of each message are read and matched with the ID kinds and loaded into their corresponding independent sets. Secondly, the divided information datasets with different IDs are divided into signals. The division is built on semantics according to Table I. X bits of y bits of each message corresponding to ID*i* in the network are read by it. The values of *x* and *y* are determined by "Bitadd." and "Bitind." at the planning table. Name the signal content at ID*i*_Name*j*, which means this signal is the signal with the name Name*j* under the information of ID*i*. Finally, the trend of the signal is output in the form of an image, and the horizontal correlation results are plotted for each combination of signals within the ID*i* information. Individual signals within the ID*i* information are plotted for longitudinal correlation results.

The details of each part of the flowchart are shown below and are implemented in four steps:

step 1: *f*=open(Datasheet)
Frame=*f*.readlines()
step 2: for(*i*=0, *i*<max(*f*), *i*++)
if Frame_ID*i*==ID*i*
ID*i*.append(Frame_ID*i*)
step 3: for(*j*=0, *j*<max(ID*i*), *j*++)
ID*i*_Name*j*.append(ID*j*[*x*,*y*])
step 4: print(Name*j*)
print(ID*i*_Name1, ID*i*_Name2.....ID*i*_Name*j*)

C. Horizontal Information Correlation Analysis Module

In order to explore the correlation between different signals in the same data frame, a lateral correlation analysis method is proposed in this paper. Based on the message characteristics of the FlexRay bus, it is known that the subsequent subsequent signals follow a data load of variable length. The bus transmission message format expressed bytes and hexadecimal numbers is shown in Fig. 5.

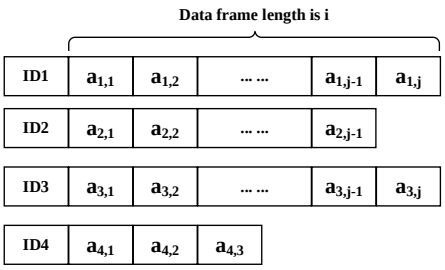


Fig. 5. Bus transmission information format.

In each horizontal message, multiple signals are included. The signals are classified according to the name, the meaning,

the frame offset and the length of each signal included in the vehicle bus information planning table. The trend of signals in the same data frame is analyzed for lateral correlation of the message perception module, as shown in Fig. 6. In Fig. 6, it can be seen that there is a clear correlation between the signals.

It can be divided into three types: positive correlation, inverse correlation and mutation correlation. When the data of one signal is suddenly changed abruptly, the corresponding values of other signals will also happen to decrease abruptly or increase steeply. In the smooth driving state, although there are small fluctuation, in the overall trend, several signals show a proportional increase or decrease. According to the above law, this study calls the phenomenon of different signals in the same message which presents certain correlation as lateral correlation and describes the characteristics of each message in detail. The concept of correlation of information plays an important role in the detection of abnormal in-vehicle bus information.

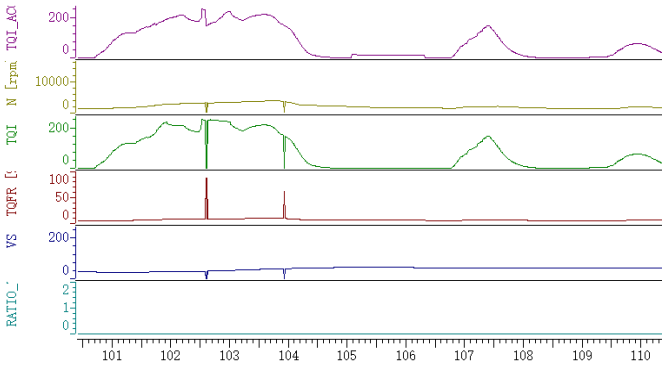


Fig. 6. Schematic diagram of signal lateral correlation.

D. Longitudinal Information Correlation Analysis Module

In order to explore the correlation between similar signals for different data frames, a longitudinal information correlation analysis method is proposed in this paper. After dividing the bus information set according to IDs, the information set is designed as shown in Fig. 7. The information load is sent when the same ID can represent the information set of multiple signals. Data frame lengths of different IDs are different and set to *i*. The longitudinal correlation requires a collection of n messages, which can analyze the change trend of the same signal in consecutive data frames.

The movement of a vehicle is a coherent action. Therefore, the information in the in-vehicle bus network, the values represented by the signals at the same location, is correlated at different moments. In this study, 1000 messages under the same ID are randomly intercepted, and a signal in the data frame is selected to plot the change trend, as shown in Fig. 8. In Fig. 8, the signal values show a step climb or a steady decline. If the range of values is expanded and the plot is more intensive, the plotted image will show a coherent curve characteristic. The vertical correlation plays a crucial role in the fault-tolerant control scheme based on the multi-point information fusion method.

E. FlexRay Bus Information Generation Module

Due to the encryption settings of the gateway in the FlexRay bus network and lacking the corresponding key of the car brand to read the information, the university researchers cannot read it directly through the OBD interface. Therefore, the FlexRay information generation module is designed by combining the results of the message sensing module with the SAE standard related content in the previous subsection. The flowchart of the message generation module design is shown in Fig. 9.

The specific steps to achieve this are shown below：

step 1: L_{frame}=length of frame
step 2: Horizontal correlation
for (j=0; j<L_{frame})
IDi.append =_IDi_Namej
step 3: Longitudinal correlations
H=min(H)~max(H)
V=min(V)~max(V)
step 4: if Hx<H
IDi_Namej=IDi_Namej
else IDi_Namej=IDi_Namej+V
step 5: Frame=Framei+1

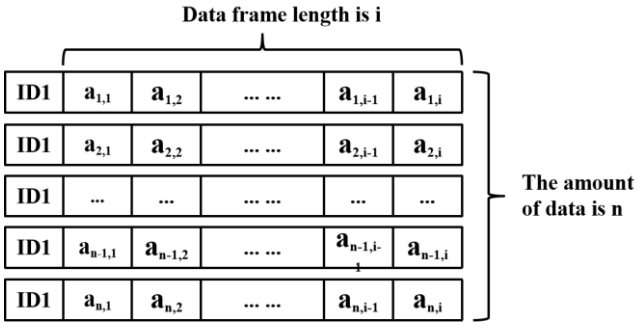


Fig. 7. Vertical format of information divided by ID.

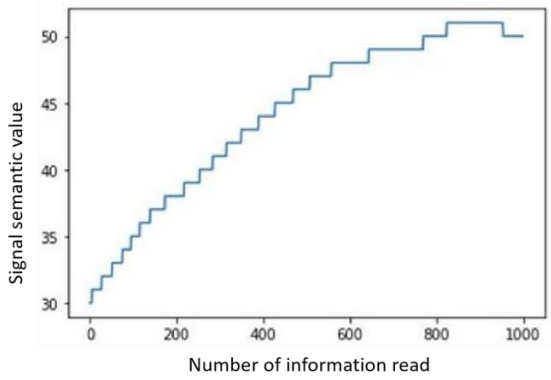


Fig. 8. Schematic diagram of longitudinal information correlation.

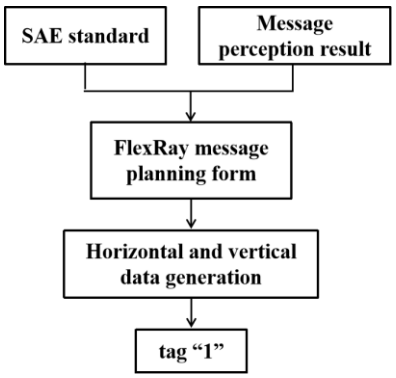


Fig. 9. Flow chart of FlexRay bus information generation module.

Firstly, the bus network information length L_{frame} and repetition rate C specified in SAE standard are introduced and then stored. Next, the information is created in terms of

both horizontal and vertical correlation. By means of the horizontal correlation, the already known relevant information is combined to generate the FlexRay bus information planning table, which is described in detail in the next section. According to the content of the information planning table, the horizontal information is generated, and the length of the information cannot exceed L_{frame}.

Subsequently, the vertical information is generated, and according to the known longitudinal correlation of the on-board bus information, the signals that are not monotonically linear are treated with a plateau period defined as H after each change. Ensuring that H is within the reasonable space min(*H*) to max(*H*), and the plateau height of the signal is recorded as V. Hx represents the length of the current plateau period, if it is less than H, ID*i*_Name*j*=ID*i*_Name*j*, the value remains unchanged. If it is equal to or greater than H, ID*i*_Name*j*=ID*i*_Name*j*+V, the value will be added to V.

Finally, since the generated information is used for anomaly detection, supervised anomaly detection requires tagging for the information set. The final generated on-board FlexRay bus travel information is passed to the anomaly message generation module.

III. Experimental Simulation and Result Analysis

A. Simulation Experiments of Python-Based Convolutional Neural Networks

Using TensorFlow, and programmed in Python language, a convolutional neural network model is built, the processed information is put into the built anomaly detection module, and the network parameters are set to achieve the desired detection rate. After the network parameters are set, the model is trained according to the divided number of iterations. When the number of iterations is less than the specified value, the current batch is processed. When the number of iterations reaches the maximum value, this training ends and the results such as the detection rate are output. If the desired effect is achieved, the model building is completed and the next test is performed. If the detection results are not satisfactory, the parameters of the training model are adjusted and the training is performed again.

TABLE II: Convolutional Neural Network Parameters Configuration

Parameter	value	Parameter name	value
Filter_number	512	Filer_length	2
Dropout	0.4	Dense_num	2
Dense 1	2048	Dense 2	1024
Learn rate	0.01	Nesterov	True
Momentum	0.9	Decay	e-6
Batch_size	16	Epoch	10

The number of iterations of the model is mainly determined by the number of epochs and batches, and there are many parameters related to the network performance in the network, as shown in Table II, which contains many important parameters in the convolutional neural network. In the table, Filter_number is the number of convolutional kernels, which represents the number of extracted data features. The number of parameters and the risk of overfitting increase with the number of convolutional kernels, so it is important to choose the right number of convolutional kernels.

Filter_length is the size of each convolutional kernel. If a convolutional kernel is too large, it may lead to long training time. Some researchers tested the convolutional kernel size and found that small order of magnitude differences have little effect on the detection results. Dropout is used to avoid overfitting by controlling the probability of neuron retention. When the probability is 1, all are hidden.

Hiding a part of neurons at each cycle can achieve the purpose of saving training data, so that the network has fewer parameters during training and more parameters and stronger performance during testing. In general, the dropout value is set between 0.3 and 0.5.

Dense in the table is the fully connected layer, which is used to integrate the extracted features. One neuron represents one way of combining the features, so the neurons in the fully connected layer are related to the data characteristics and the number of extracted features. The experimental model in this paper has two fully connected layers, the first fully connected layer is set with 2048 neurons, and the second fully connected layer is set with 1024 neurons.

Learn rate is the initial learning rate, which plays an important role in parameter convergence. When the learning rate is too large, it may produce the situation that the parameters to be optimized fluctuate around the minimum value but do not converge, and when the learning rate is too small, it will make the parameters optimized. Nesterov represents whether to use Newtonian momentum, which is an optimization method; Decay is the regularization coefficient, which is used to slow down the overfitting phenomenon of the model. The neural network is input by batch, and Batch_size is the amount of data contained in each batch when input.

B. Analysis of Information Anomaly Detection Results

The parameters are adjusted so that the trained network can effectively identify anomalous information, and the experimental results are plotted in Fig. 10. The yellow line in the figure is the detection result of the test set, the blue line is the detection result of the training set, and the horizontal coordinates are in epoch. From the result, it can be observed that the detection accuracy is basically stable at a high level, both during training and testing.

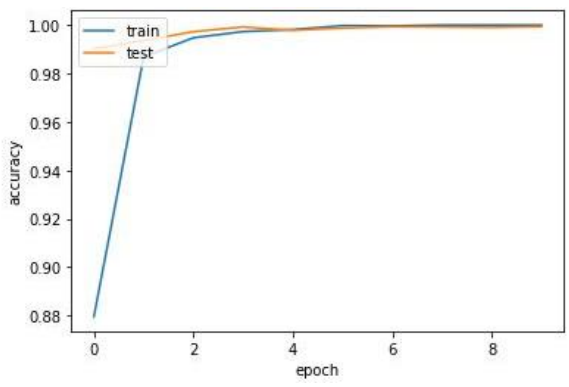


Fig. 10. Anomaly detection accuracy.

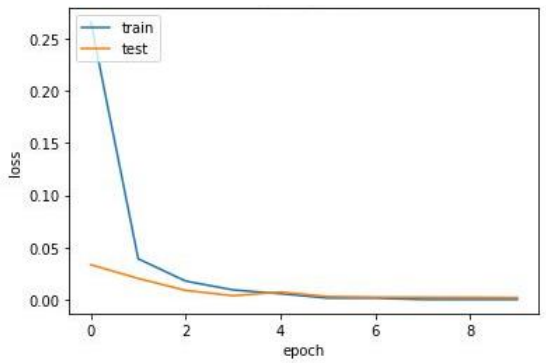


Fig. 11. Neural network loss function curve.

During training, the detection rate is initially around 88%, then it gradually increases, and finally the detection rate stabilizes at 99%. After the detection rate reached the target value, the trained network was tested; the network detection rate was only 98.5% at the beginning the test set, and the detection rate was all stable at 99% at the later stage.

Fig. 11 shows the loss function curve, recording the average gap in an epoch. The smaller the value of the loss function is and the faster it decreases, the better the detection effect of the is. The blue curve on the way represents the training set, where the function drops rapidly and then does not fluctuate significantly and stays smoothly below 0.05. The loss function stays below 0.05 in the test set experiment. The loss function eventually approaches zero for both testing and training.

C. Joint Experiment

The overall software and hardware joint experiment flow chart is shown in Fig. 12.

In order to verify the reliability of the scheme proposed in this paper, an experimental simulation platform was built using a dedicated CANoe vehicle bus network platform and a FlexRay hardware development version, and the architecture of the experimental environment is shown in Fig. 13. Network Designer is used to set up the network parameters and establish the bus information data set. We set up the network topology in CANoe and schedule the information to be sent.

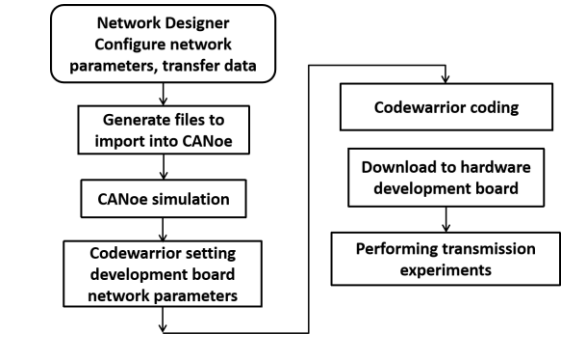


Fig. 12. Flow chart of overall software and hardware joint experiment.

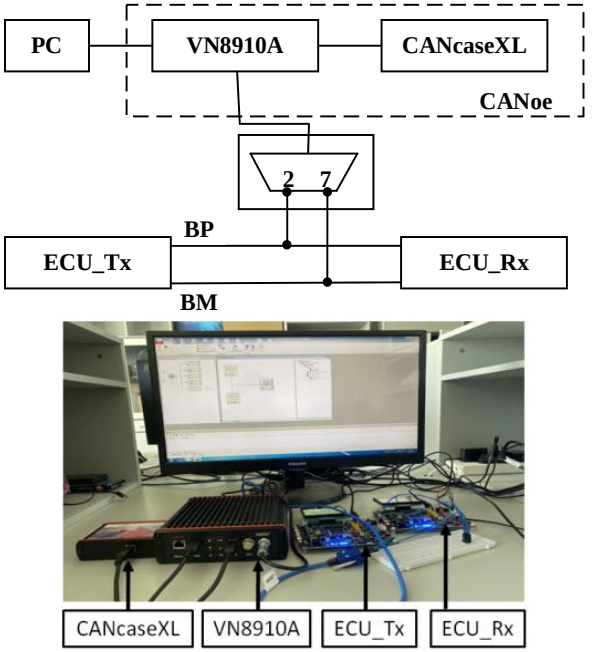


Fig. 13. Experimental environment architecture.

The data load and corresponding network parameters are written in the ECU_Tx transmitter node, and the ECU_Rx receiver node is used to receive the information. The hardware ECU processor model used in this study for the transmitter and receiver side is MC9S12XF512MLM. Fig. 13 shows the actual experimental simulation environment.

Time	Channel	Name	Identif...	Type	Cy...	Dir	DLC	Data								Frame S...	Frame Sta...	Schedule	Syne FL...	Startup F...	PP Flag	Spy Flag
5....	F....	New_Frame_1	25	D...	41	Tx	4	41	34	7	126					0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_2	26	D...	41	Tx	4	65	41	88	12					0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_3	27	D...	41	Tx	2	0	0							0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_4	28	D...	41	Tx	2	2	0							0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_5	29	D...	41	Tx	8	64	186	132	12	0	32	255	0	0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_6	30	D...	41	Tx	8	64	186	132	12	0	32	255	20	0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_7	31	D...	41	Tx	8	244	130	1	139	0	0	0	0	0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_8	32	D...	41	Tx	8	0	0	7	4	255	178	10	0	0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_9	33	D...	41	Tx	4	130	164	10	0					0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_10	34	D...	41	Tx	4	65	41	88	12					0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_11	35	D...	41	Tx	2	0	0							0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_12	36	D...	41	Tx	2	126	0							0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_13	37	D...	41	Tx	8	64	186	132	12	0	32	255	0	0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_14	38	D...	41	Tx	8	0	0	41	0	0	0	0	0	0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_15	39	D...	41	Tx	8	0	0	109	31	123	8	251	2	0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_16	40	D...	41	Tx	4	0	32	95	20					0x20	VAL	d...	0	0	0	0
5....	F....	New_Frame_17	41	D...	41	Tx	4	65	44	96	12					0x20	VAL	d...	0	0	0	0

Fig. 14. Bus transmission information before anomaly detection.

Time	Channel	Name	Identif...	Type	Cy...	Dir	DLC	Data								Frame S...	Frame Sta...	Schedule	Syne FL...	Startup F...	PP Flag	Spy Flag
31...	F....	New_Frame_1	25	D...	11	Tx	4	41	34	7	126					0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_2	26	D...	11	Tx	4	65	41	88	12					0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_3	27	D...	11	Tx	2	0	0							0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_4	28	D...	11	Tx	2	2	0							0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_5	29	D...	11	Tx	8	64	186	132	12	0	32	255	0	0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_6	30	D...	11	Tx	8	64	186	132	12	0	32	255	20	0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_7	31	D...	11	Tx	8	244	130	1	139	0	0	0	0	0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_8	32	D...	11	Tx	8	0	0	7	4	255	178	10	0	0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_9	33	D...	11	Tx	4	130	164	10	0					0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_10	34	D...	11	Tx	4	65	41	88	12					0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_11	35	D...	11	Tx	2	0	0							0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_12	36	D...	11	Tx	2	126	0							0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_13	37	D...	11	Tx	8	64	186	132	12	0	32	255	0	0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_14	38	D...	11	Tx	8	0	0	41	0	0	0	0	0	0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_15	39	D...	11	Tx	8	0	0	109	31	123	8	251	2	0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_16	40	D...	11	Tx	4	0	32	95	20					0x20	VAL	d...	0	0	0	0
31...	F....	New_Frame_17	41	D...	11	Tx	4	65	44	96	12					0x20	VAL	d...	0	0	0	0

Fig. 15. Bus transmission information after fault-tolerant control.

In order to test the reliability of the anomaly detection system of information. Random fault messages are set in the bus information data set. Fig. 14 shows the bus transmission information before the anomaly detection. Among them, the black box marks the accurate detection of abnormal information.

After anomaly detection, the fault information is automatically corrected according to the context-aware method, as shown in Fig. 15. The semantics of the corrected information is more in line with the relevant rules of the information, thus ensuring safe driving.

IV. Conclusions

The technologies of network protection, data management and network topology architecture of in-vehicle bus network traditionally lack theoretical guidance and have strong arbitrariness and hardware dependency. This study addresses the information security of in-vehicle FlexRay bus and builds the information database of the FlexRay bus according to SAE standard, FlexRay communication protocol and bus information of actual vehicles. Innovative anomaly detection system of information and message perception module based on message perception method is proposed. Based on the interrelationship between the upper and lower messages in the actual vehicle bus information, the horizontal information correlation analysis method and the vertical information correlation analysis method are innovatively proposed.

The experimental simulation platform is built by using CANoe in-vehicle bus network dedicated platform and FlexRay hardware development version to simulate and verify the scheme proposed in this study. The accuracy of information anomaly detection in the in-vehicle FlexRay bus network reaches 99% by the experimental simulation results. And the fault information is automatically corrected according to the up and down the message perception method. Thus, active safety of the in-vehicle FlexRay bus network is further improved.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Yujing Wu and Yihu Xu: Methodology and writing of original draft; Shinan Wang and Jingyi Jia: Software and formal analysis; Yinan Xu: Conceptualization and supervision.

Funding

This research was supported by National Natural Science Foundation of China (grant number 62161049 and 62201492) and Jilin Province Science & Technology Development Project (grant number 20220101141JC).

References

[1] M. Markovitz *et al*., "Field classification, modeling and anomaly detection in unknown CAN bus networks," *Vehicular Communications*, vol. 9, pp. 43-52, 2017.

[2] SAE Vehicle Electrical System Security Committee, *SAEJ3061-Cybersecurity Guidebook for Cyber-Physical Automotive Engineers*, 2016.

[3] H. Ji, Y. Wang, and H. Qin, "Comparative performance evaluation of intrusion detection methods for in-vehicle networks," *IEEE Access*, vol. 6, pp. 37523-37532, 2018.

[4] Z. Zijian, Z. Yue, and W. Jian, "An anomaly detection system applied to CAN bus," *Information Security and Communications Privacy*, 2015.

[5] M. Kang and J. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *Proc. IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016, pp. 1-5.

[6] 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 (ICOIN)*, 2016, pp. 63-68.

[7] W. Wu *et al*., "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 919-933, 2020.

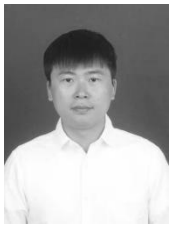
[8] M. Z. Liu, Y. H. Xu, Y. J. Wu, and Y. N. Xu, "Research of authenticated encryption security protocol for FlexRay in-vehicle network," *International Journal of Computer Theory and Engineering*, vol. 10, pp. 175-179, 2018.

[9] S. N. Wang and Y. N. Xu, "Research of FlexRay dynamic segment network optimization based on composite deadline message scheduling algorithm," *International Journal of Computer and Electrical Engineering*, vol. 12, pp. 14-21, 2020.

[10] S. Jin, M. Liu, Y. Wu, Y. Xu, J. Zhang, and Y. Xu, "Research of message scheduling for in-vehicle FlexRay network static segment based on Next Fit Decreasing (NFD) Algorithm," *Applied Science Computer Science and Electrical Engineering*, vol. 8, pp. 1-13, 2018.

[11] J. Piao, Y. Wu, and Y. Xu, "A security framework for in-vehicle FlexRay bus network," *International Journal of Modeling and Optimization*, vol. 12, no. 3, pp. 92-98, 2022.

Yujing Wu received her M.S. and Ph.D. in electronic and information engineering from Chonbuk National University, South Korea in 2013 and 2016. She is currently working in Department of Electronics & Communication Engineering with the Yanbian University, China. Her research interests are in the area of VLSI implementation for digital signal processing and communication systems which include the design of CAN data reduction and DisplayPort, implementation of security protocol for in-vehicle networks.



Yihu Xu received his Ph.D. in electronic and information engineering from Chonbuk National University, South Korea in 2015. Since 2016, he has been with the Department of Electronics & Communication Engineering, Yanbian University. His research interests include next-generation mobile communications, cognitive radio, and in-vehicle networks.

Shinan Wang was born at Jilin Province of China. She received the bachelor degree in communication engineering from YanBian University, China, in 2019. She received her M.S. in Department of Electronics & Communication Engineering with the Yanbian University, China. Her research interests include the design of security architecture of FlexRay of security protocol for in-vehicle network.

Jingyi Jia is currently studying communication engineering with the Yanbian University, China. She won the 32nd China adolescents science & technology innovation contest, and the third prize in the 13th Mathematics Competition in Jilin Province.

Yinan Xu received his Ph.D. in electronic and information engineering from Chonbuk National University, South Korea in 2009. He is with the Department of Electronics & Communication Engineering, Yanbian University. His research interests are in the area of in-vehicle networks and automotive electronic control.