An Intrusion Detection Method for In-Vehicle CAN Bus Network

Anyu Cheng [1, a], Yongwei Cao [2, b], Ling Wang [3,c]

[1] Chongqing University of Posts and Telecommunications, Chongqing 40065, China;

[2] Chongqing University of Posts and Telecommunications, Chongqing 40065, China.

[3] Chongqing University of Posts and Telecommunications, Chongqing 40065, China.

[a]591263202@qq.com, [b]Caoyongwei_mail@163.com, [c]335952995@qq.com

Abstract

The problem of data safety in vehicle are serious because the In-Vehicle network are easily invaded. An intrusion detection method based on BP (Back Propagation, BP) neural network was proposed in this paper. The relations between each data in In-Vehicle CAN network are checked to judge whether the network was invaded. The simulation experiment environment is built to verify the method. The experiment proves that the method proposed in this paper can effectively detect the intrusion data and has a high detection rate.

Keywords

In-vehicle network security, CAN Bus, Intrusion Detection.

1. Introduction

CAN bus is widely used in vehicle electronic control system to transmit control information between controllers. However, the CAN bus has security defects. Once the vehicle is invaded, CAN bus becomes an intruder's media. In addition, due to the increasing demand for the interaction between the inside information and the outside information, a variety of interfaces for communication with the outside are added. This undoubtedly increases the number of intrusion interfaces available to the intruder, the interface can be used by intruder are illustrated in figure 1.

（1）Physical interfaces such as OBD and USB are the most basic intrusion interfaces, In 2013, Miller and Valasek, invaded a Toyota Prius through the OBD port, they can commend the car execute some abnormal actions such as brake failure or braking suddenly at high speed.[1].

（2）Wireless interfaces such as WIFI and Bluetooth are often attacked by intruders. In 2015, white hat hackers Miller and Valasek gained remote access to key functions of a Jeep Cherokee car, such as acceleration, braking and steering, by attacking the entertainment system vulnerability of the car[2]. Network security experts use the loopholes in tesla Model S to open the door and drive away the car, or command the car to suddenly shut down the system engine when the car is normal driving[3].

（3）Remote services can make driving easier, but they are also a way for hackers to gain access, Samy Kamal developed a tool called Ownstar to attack OnStar service, and successfully obtained the control right of OnStar, which can remotely control car startup, door lock, etc. [4]. In addition, Audi, Porsche, Bentley, Lamborghini and other brands have also been affected by network security which seriously affecting the safety of vehicle driving, so the In-Vehicle network intrusion detection research is urgent.

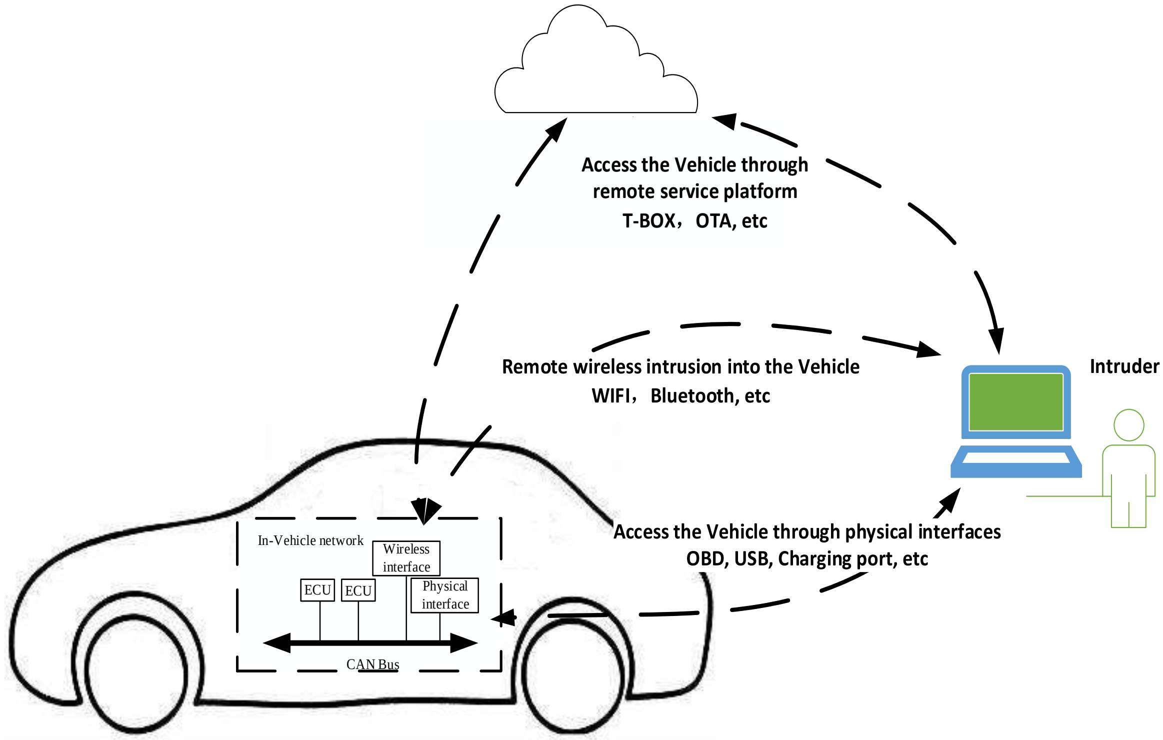
Access the Vehicle through
remote service platform
T-BOX，OTA, etc
Remote wireless intrusion into the Vehicle
WIFI，Bluetooth, etc
Intruder
Access the Vehicle through physical interfaces
OBD, USB, Charging port, etc
In-Vehicle network
Wireless interface
ECU
ECU
Physical interface
CAN Bus

Fig. 1 The interfaces can be invaded by intruder

After the intrusion of vehicles, hackers can take a variety of attack methods, As for data leakage problem caused by the plaintext broadcast of CAN messages, Wan Ailan proposed an encryption and authentication mechanism to ensure the confidentiality of data, but the delay of key distribution and data encryption and decryption affected the real-time performance of the network. For the bus blocking problem caused by DoS and packet replay attacks, Yu He proposed a packet anomaly detection method based on entropy of CAN bus packet periodic, but this method could not detect the intrusion of packet data tampering, and there were detection defects in this method[5]. For the attack of data tampering, M. Muter proposed an intrusion detection algorithm of CAN bus based on anomaly detection sensor, but this method needs to add sensors and modify the network architecture which resulting in increased costs and not applicable to the production vehicles[6]. Min-Ju Kang proposed an intrusion detection method based on deep neural network, but this method did not consider the data meaning in the message data field[7]. Therefore, this paper proposes an intrusion detection method of vehicle-mounted CAN bus based on BP network. the tampered intrusion data can be detected effectively.

2. Proposed Method

2.1 Overview of Proposed Intrusion Detection System

An intrusion detection method based on message signal detection was proposed in this paper which mainly includes four steps: message acquisition, signal extraction, intrusion detection and analysis of detection result. Message collection: collect vehicle messages from real vehicles, mainly collect messages related to vehicle power and vehicle status; Signal extraction: extract the signal which can best reflect the driving state of the vehicle from the collected message; Intrusion detection: the extracted signal as the intrusion detection algorithm input to obtain the detection results; Analysis of detection results: according to the detection results, measures are taken and the detection results are collected, the accuracy of the detection algorithm need to be counted. The core of intrusion detection system is the algorithm of detection, because the number of signals in vehicle is huge and there are relationships between multiple signals, such as the speed signals and the accelerator pedal, engine speed signal and vehicle speed signal, etc., but it is difficult to use simple function to map the relationship between the signal because these relationship between signals are complex. MLP(Multi-layer Perceptron) neural network was trained with BP algorithm can match complex function, the function of normal signals in vehicle can be matched , the function can be used to check signals in vehicle. If the signals match the function, they are normal data, otherwise they are intrusion data.

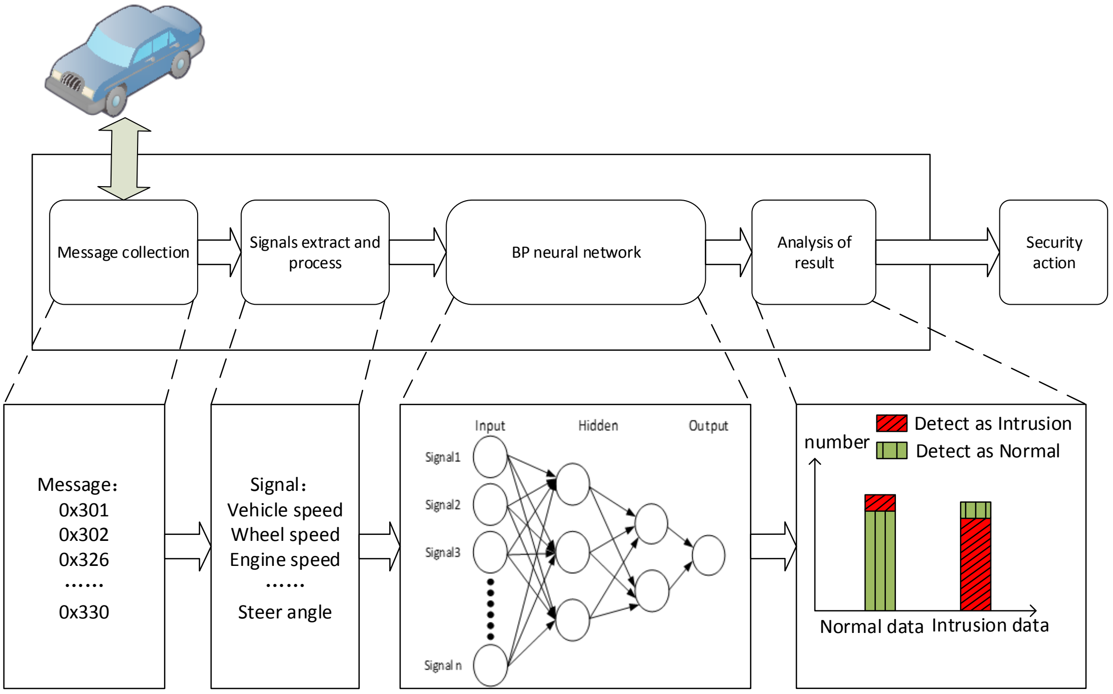

Fig. 2 Intrusion detection system

2.2 Data Processing

Messages in the In-Vehicle CAN bus include real-time running status signals and vehicle control signals, so detect such signals CAN effectively detect whether there is intrusion in the network. Since the period of packets in the network is inconsistent, the signal values collected are not at the same time. Therefore, it is necessary to unify the time of signals when extracting signals from packets, it is necessary to extract each signal value at each time point. Therefore, the latest value of each signal is taken as the signal value at this moment. See Table1:

Table 1 Signals extract

Time (ms)	Signal					
	Engine speed (rpm)	FL Wheel speed (km/h)	Steer angle (deg)	FR Wheel speed (km/h)	Accelerator pedal (%)	Steer speed (deg/s)
t1	793	29	3	30	3	1
t2	799	31	3	30.5	4	1
t3	805	31	3	30.5	5	1
t4	807	31	3	30.5	6	1
t5	807	30	3	30	6	1
t6	809	30	3	30	4	1
t7	804	30	3	30	5	1
t8	804	30	2	30	5	1.5

Due to the different meanings represented by each signal, the dimensionality and numerical range of each signal value are greatly different, which affects the data analysis results. Therefore, this paper normalizes each signal to eliminate the dimensionality of the signal, so as to improve the comparability between data. After data processing is completed, each signal at each moment seen as a set of input of the network.

The normalization method of deviation standardization is used in this paper, and its calculation formula is as follows:

$$x^* = \frac{x - \min(\mathrm{x})}{\max(x) - \min(x)} \tag{1}$$

The x is the signal value, min(x) is the minimum value for the selected signal data, the Max (x) is the maximum value for the selected signal data, x * is the data after the normalization, the data after normalization are listed in Table 2.

Table 2 Signals after Normalization

Time (ms)	Signal					
	Engine speed(rpm)	FL Wheel speed (km/h)	Steer angle(deg)	FR Wheel speed(km/h)	Accelerator pedal (%)	Steer speed (deg/s)
t_1	0	0	1	0	0	0
t_2	0.375	1	1	1	0.333	0
t_3	0.75	1	1	1	0.667	0
t_4	0.875	1	1	1	1	0
t_5	0.875	0.5	1	0	1	0
t_6	1	0.5	1	0	0.333	0
t_7	0.6875	0.5	1	0	0.667	0
t_8	0.6875	0.5	0	0	0.667	1

2.3 Intrusion Detection Method Based on BP Neural Network for CAN Bus

The In-vehicle network transmits a large number of information data that can reflect the running condition of the vehicle, such as speed, steering wheel Angle, throttle pedal status and so on. There is a certain nonlinear relation between these information data, the relation can fit by BP network training. Then the fitted function is used as the intrusion detection function to detect the signals in the network and determine whether there is intrusion behavior.

the input layer input vector $X_i = \{ x_1, x_2, x_3, \ldots x_n \}$, which represents signals at a certain time in the networks , Hidden layer input vectors $H_i = \{h_1, h_2, h_3, \ldots h_p\}$,they comes from the result of calculate by X_i with W_{ip} which are weight vectors for input layer to hidden layer. hidden layer output vector H_O = $\{ h_{o1}, h_{o2}, h_{o3}, \ldots h_{op} \}$, W_{pq} are weight vectors for hidden layer to output layer, Y_i = $\{y_{i1}, y_{i2}, y_{i3}, \ldots y_{iq}\}$ are input vector for output layer, Y_o = $\{y_{o1}, y_{o2}, y_{o3}, \ldots y_{oq}\}$ are output vector for output layer, D = $\{d_1, d_2, d_3, \ldots d_q\}$ are expected output vectors. the threshold value for each cell in hidden layers is b_h, b_o is the threshold value for each cell in output layers, $f(\cdot)$ is the activation function.

The H_i calculation formula is below:

$$h_p = \sum_{i=1}^{n} w_{ip} x_i + b_h \tag{2}$$

The H_O calculation formula is below:

$$H_o = f(H_i) \tag{3}$$

The Y_i calculation formula is below:

$$y_{iq} = \sum_{j=1}^{p} w_{jq} h_{oj} + b_h \tag{4}$$

The output in output layer is below:

$$Y_o = f(Y_i) \tag{5}$$

The error of the q th neuron in the output layer is:

$$e(n) = d_q(n) - y_q(n) \tag{6}$$

The sum of the error of all neurons in the output layer is:

$$E(n) = \frac{1}{2}\sum_{k=0}^{q} e_k^2(n) \tag{7}$$

In order to reduce the sum of error, it is necessary to adjust each weight through the back-propagation algorithm. When the error reaches the acceptable range, the network training is completed. the network output can be obtained by inputting collected signals into the network, According to the output, intrusion behavior can be judged.

The processing of getting intrusion detection is below:

Real vehicle data of different road conditions were collected and intrusion data were randomly .

Feature extraction of data, according to the analysis of signal security level to extract important signals.

The BP network structure and initialization parameters were determined, and the gradient descent method was used for network training to obtain the network meeting the error requirements.

The samples are detected based on the trained network, and security measures are adopted when the intrusion is detected.

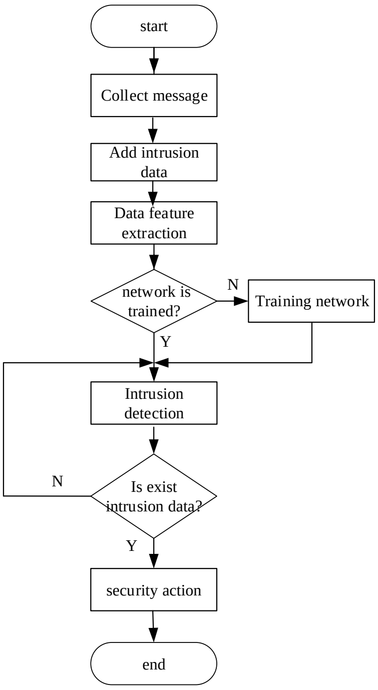

Fig. 3. model training and detection

3. Experiments and Analysis

3.1 Data Set

The data set were collected from a real vehicle which was driving on the road under condition of intrusion-free and without false. The simulation environment of intrusion is built in CANOE 9.0,see Fig. 4 the final data will be consisted of data collected from vehicle and intrusion data. Intrusion data were made according to intrusion scenes which were listed in table 2.

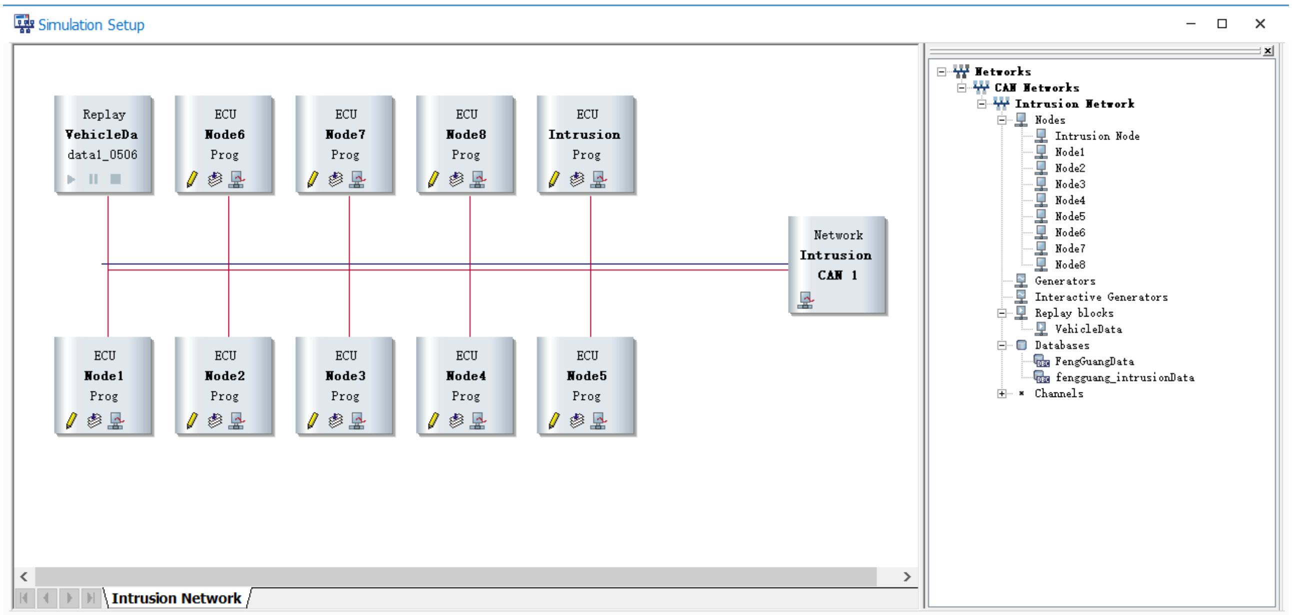

Fig. 4 Simulation intrusion environment

Table 2 shows the intrusion scenarios simulated in this experiment, including the intrusion scenarios on the vehicle power system. Such attacks have a huge impact on the safety of vehicles.

Table 2 Intrusion scene simulation

Intrusion Scenarios	Node	Describe
Anomaly engine torque	Node1	The actual engine torque signal value is inconsistent with the driver's request torque signal value
Abnormal engine speed	Node2	Make the engine speed signal in an unreasonable range
Abnormal Speed	Node3	Put the speed signal in an unreasonable range
Abnormal brake pedal	Node4	Make brake and acceleration pedal pressed at the same time
Abnormal throttle	Node5	Make the throttle signal in an unreasonable range
Abnormal wheel speed	Node6	Make the four wheels speed signal values inconsistent
Abnormal steer angle	Node7	The speed of the steering wheel speed is unreasonable
Abnormal accelerator pedal	Node8	Make accelerator pedal and engine speed unreasonable
Abnormal engine state	Node9	Turn off the engine while the car is running

Table 3 shows part of the data set; label 0 represents normal signal; label 1 represents intrusion signals.

Table 3 Part of data set

Engine speed	Engine torque	Accelerator pedal	Vehicle speed	……	Steer angle	Label
736	-4	0	0	……	0	0
499.5	-4	0	0	……	0	1
736	-4	0	0	……	203	0
669	39	0	5	……	132	1
210	31	0	4	……	148	1

……	……	……	……	……	……	……
1632	3	3	49	……	126	1
1376	109	21	53	……	0	0
1600	20	6.8	62	……	0	0

3.2 Result Analysis

First set up BP network and message signal extraction and data processing, In order to avoid the data set's influence on the algorithm, the method of cross validation is used in experiments, the data set divided into training set and test set in a ratio of 7:3 randomly, the network was training with training set and was test with test set. The results are recorded, the steps above should be repeated 10 times, 10 groups of test results were got. In this experiment, TP (true positive), FP(false positive), TN(true negative) and FN(false negative) were recorded. TP means normal data are detected as normal data, FP means intrusion data are detected as normal data, TN means intrusion data are detected as invasion data, FN means normal data are detected as invasion data.

The formula for calculating the accuracy of intrusion detection is as follows：

$$R_T: = \frac{T_p+F_p}{T_N+F_P+T_p+F_N} \tag{8}$$

The figure below shows the comparison between the intrusion detection algorithm proposed in this paper and the detection method of packet data field bit as network input. It can be seen from the figure that the method proposed in this paper has improved the accuracy by 2.85% on average.

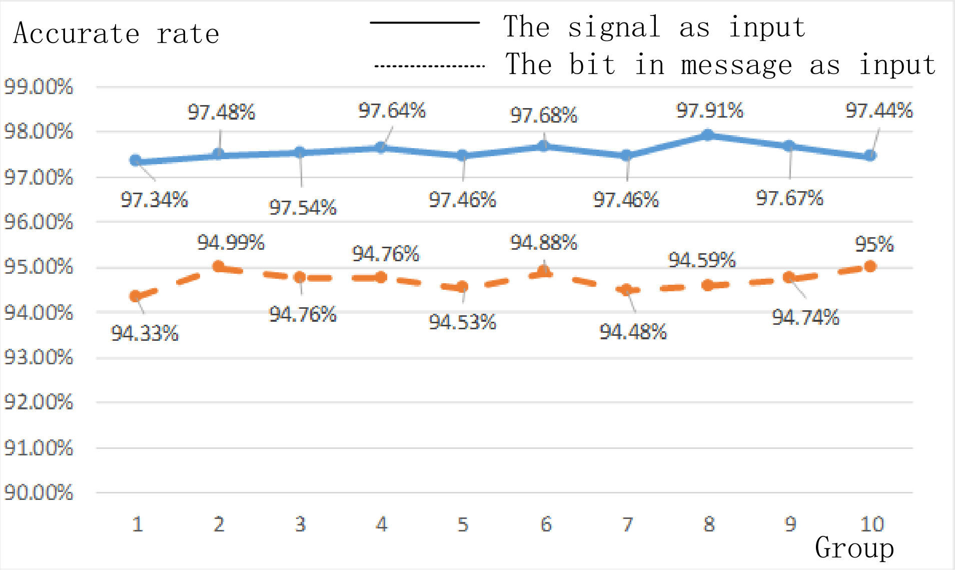

Fig. 6 Verification result

In order to further analyze the characteristics of the intrusion detection algorithm, the confusing matrix was used to analyze the results of the eighth group of experiments. The results of the confusing matrix are shown in figure 7. In order to ensure the security of vehicle network and prevent intrusion, intrusion detection algorithm is required to have a high degree of identification of intrusion data, it should detect all intrusion data as much as possible and ensure a low false positive rate.

The calculation formula of true negative rate R_N is:

$$R_N: = \frac{T_N}{T_N+F_P} \tag{9}$$

The calculation formula of false positive rate R_W is:

$$R_W: = \frac{F_N}{T_P+F_N} \tag{10}$$

	Predicted lable	
True lable	TP 8118 (94.7%)	FN 452 (5.3%)
	FP 53 (0.3%)	TN 14207 (99.7%)

Fig. 7. Test result

The experimental results show that the true negative rate of the intrusion detection method is 99.7%, the false positive rate is 0.3%, It is proved that the intrusion detection algorithm has a high degree of identification for intrusion data and can guarantee the CAN network in In-vehicle safe. However, this algorithm has false negative rate which reaches 5.3%.

4. Conclusion

An intrusion detection method based on BP network for CAN network is proposed in this paper, The relationship between signals in CAN network can be fitted by using the characteristic that BP network can fit complex functional relationship, and the intrusion behavior in the network can be detected by using this function relationship. Experimental results show that this method has a high true negative rate, but there is a certain false positive rate. the algorithm will be optimized to reduce the false positive rate in next research.

References

[1] Miller C, Valasek C. Adventures in Automotive Networks and Control Units[C]. // DEFCON 21 Hacking. Conference, Las Vegas, 2013.

[2] Miller C, Valasek C. Remote Exploitation of an Unaltered Passenger Vehicle[C]. Black Hat USA, 2015.

[3] Koscher K, Czeskis A, Roesner F, et al. Experimental Security Analysis of a Modern Automobile ［C］// 2010 IEEE Symposium on Security and Privacy (SP). IEEE, 2010: 447－462.

[4] S. Kamal, OwnStar: Locates, Unlocks, Remote Starts GM/OnStar Cars, 2015.

[5] Yu He. Research on information security and CAN bus anomaly detection technology of network - connected vehicle [D]. Jilin University，2016.

[6] M. Muter, A. Groll, and F. C. Freiling, "A Structured Approach to Anomaly Detection for In-Vehicle Networks, " in 6th Int, Conf.Information Assurance and Security (lAS). Atlanta, GA: IEEE, 2010: 92-98.

[7] Min-Ju Kang, Je-Won Kang. A Novel Intrusion Detection Method Using Deep Neural Network for In-Vehicle Network Security[C] // Vehicular Technology Conference. IEEE, 2016: 1-5.

[8] Larson U E, Nilsson D K, Jonsson E. An Approach to Specification-Based Attack Detection for In-Vehicle Networks[C]. Intelligent Vehicle Symposium，2008 IEEE，2008: 220-225.

[9] Woo S, Jo H J, Lee D H. A practical wireless attack on the connected car and security protocol for in-vehicle CAN[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 993-1006.

[10] Parkinson S, Ward P, Wilson K, et al. Cyber threats facing autonomous and connected vehicles: future challenges[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(11):

2898-2915.

[11] Groza B, Murvay S. Efficient protocols for secure broadcast in controller area networks[J]. IEEE Transactions on Industrial Informatics, 2013, 9(4): 2034-2042.

[12] Woo S, Jo H J, Kim I S, et al. A practical security architecture for in-vehicle can-fd[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2248-2261.

[13] Berg J, Pommer J, Jin C, et al. Secure gateway—A concept for an in-vehicle IP network bridging the infotainment and the safety-critical domains[J]. 13th Embedded Security in Cars (ESCAR'15), 2015.

[14] Rizvi S, Willet J, Perino D, et al. A Threat to Vehicular Cyber Security and the Urgency for Correction[J]. Procedia Computer Science, 2017, 114: 100-105.

[15] Chung S M, Jin H W. Isolating system faults on vehicular network gateways using virtualization[C]//Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on. IEEE, 2010: 791-796.