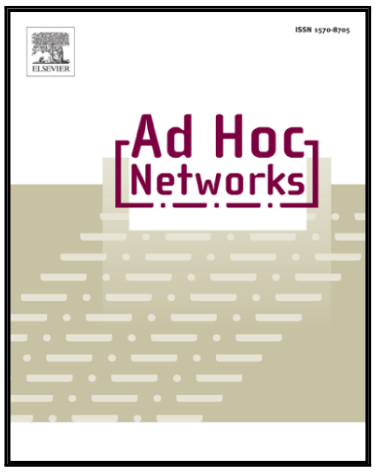
Journal Pre-proof



Intrusion Detection System using Deep Learning for In-vehicle Security

Zhang Jiayan , Li Fei , Zhang Haoxi , Li Ruxiang , Li Yalin

PII: S1570-8705(19)30435-4
DOI: https://doi.org/10.1016/j.adhoc.2019.101974
Reference: ADHOC 101974

To appear in: *Ad Hoc Networks*

Received date: 3 May 2019
Revised date: 31 July 2019
Accepted date: 31 July 2019

Please cite this article as: Zhang Jiayan , Li Fei , Zhang Haoxi , Li Ruxiang , Li Yalin , Intrusion Detection System using Deep Learning for In-vehicle Security, *Ad Hoc Networks* (2019), doi: https://doi.org/10.1016/j.adhoc.2019.101974

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2019 Published by Elsevier B.V.

Intrusion Detection System using Deep Learning for In-vehicle Security

Zhang Jiayan, Li Fei, Zhang Haoxi, Li Ruxiang, Li Yalin

Chengdu University of Information Technology, School of Cyberspace Security, Sichuan, China

***Abstract*—With the development of vehicle intelligence technology, the combination of network and vehicle becomes inevitable, which brings much convenience to people. At the same time, hackers can also use technical vulnerabilities to attack vehicles, leading to severe traffic accidents and even vehicle crash. Based on this situation, the vehicle information security protection techniques have drawn great attention from researchers. This paper studies the vehicle intrusion detection system (IDS) based on the neural network algorithm in deep learning, and uses gradient descent with momentum (GDM) and gradient descent with momentum and adaptive gain (GDM/AG) to improve the efficiency and accuracy of IDS. The accuracy and efficiency of the proposed model are validated and evaluated by using real vehicles at the end of the paper. Experiments show that the GDM/AG algorithm can achieve faster convergence in comparison with the GDM algorithm in vehicle anomaly detection, and can detect anomaly data at the level of milliseconds. At the same time, the proposed model can adapt itself to detect unknown attacks. The veracity rate ranges from 97% to 98% in directing the adaptation when facing unknown attack types.**

***Index Terms*—vehicle intelligence, intrusion detection system, deep learning, gradient descent with momentum, gradient descent with momentum and adaptive gain**

I. INTRODUCTION

Intelligent vehicles, as a product of the integration of computer technology and the Internet of Things technology, can achieve efficient operation of vehicles and the variety of comprehensive information services [3]. According to relevant reports, the number of users using automobiles worldwide has reached one billion and is expected to reach two billion until 2035 [24]. Therefore, whether the relevant business information on the Internet of Vehicles can meet the corresponding security requirements and reliability requirements is a crucial issue for the popularization and even development of the Internet of Vehicles [2, 4]. The core network of the Internet of Vehicles is still a traditional network but with a more complicated communication environment and an increasing number of connected nodes. In contrast, the Internet of Vehicles is more vulnerable to attacks than other traditional networks, and the impact is not limited to virtualized information, but also affects real-life casualties and economic losses, and may even involve the safety of a country.

In recent years, vehicle safety problems happen frequently, and the exposed automobile safety incidents can be divided into two categories: On the one hand, the problem is that the driver loses the control of the vehicle and the user's safety may threaten by external intrusion attack. In 2015, Chrysler's Jeep model was invaded by foreign security experts. It used Linux system vulnerabilities to control the vehicle's multimedia system remotely, then attacked the V850 controller, modified its firmware, and obtained the right to send instructions to the Control Area Network (CAN) bus remotely, to achieve the purpose of remotely controlling the power system and the brake system. The attacker can reduce the speed of the car, turn off the car engine, suddenly brake or disable the brakes without the user's informed consent [20]. In 2016, when the same Jeep model was physically contacted, the attacker could inject commands into the OBD (On-Board Unit) interface to control the vehicle's power system, manipulate the steering wheel or brake system, and to pose a severe threat to the driver's safety. In February, Nissan LEAF automobile API was leaked, so that hackers can control automobiles remotely. On July 28, 2017, Tencent Cohen Laboratory can control Tesla remotely in parking and driving state through remote contactless cracking. It implements the "remote no physical contact" mode of intrusion into Tesla Model X and gains the highest privileges. On the other hand, it suffers from internal system decision-making errors. Such incidents mainly occur in the automobile network. Because of the complexity of road traffic and the difficulty of predicting pedestrian behaviour, the automobile network cannot accurately judge traffic information, thus causing automobile safety accidents. For example, on January 20, 2016, Tesla Motors suffered the first "autopilot" death in China. On March 28, 2018, a pedestrian was knocked down and killed by Uber self-driving cars in Tempe, Arizona. Therefore, more and more people focus on the topic of automobile information security. At the same time, governments and their major automobile manufacturers are increasingly paying attention to the information security of the automobile network.

To ensure the safety of automobiles, Cars are deploying with a variety of Internet security technologies[22]. The first defensive line of the traditional Internet is usually a firewall, but because of its static protection mode, it cannot adapt to the complex and changeable environment of smart cars and various attack means. While the other network security technology, such as digital signature, digital certificate, and corresponding encryption of data, can achieve better security

JOURNAL PRE-PROOF

defence effect in some aspects of Internet security protection. However, we noticed that due to the unique characteristics of the CAN bus in the car, the traditional security technology for the Internet environment could not be immediately applied to the vehicle [8]. Intrusion detection technology is a critical technology in these information security technologies and faces the issues addressed in the appeal. In recent years, many of the researches are basing on rules or statistics for real-time intrusion detection. However, it is challenging to deploy these intrusion detection systems on automobiles. The reasons are as follows: (1) The limited computing resources and storage space of automobile devices: Many IDSs need to consume a lot of computing resources and storage space when detecting abnormal behaviours, For example, the host intrusion detection system (Host Intrusion Detection System) needs to call a large number of system resources when performing intrusion detection, which causes the system resources to be tight when HIDS is running [23]. (2) The versatility problem of the intrusion detection system: Many IDS implementations can only be implemented for specialized systems or in specific environments, so many IDS in existing research cannot be directly applied to automobiles. (3) IDS will produce a high false alarm rate: Because many intrusion detection systems in the current research are implemented by specific rules or statistics-based methods, these methods implementing anomaly detection by modelling the daily behaviour of users, this modelling method can easily lead the network to classify the corresponding behaviour as anomalous behaviour in the face of exceptional circumstances rather than anomalous situations. As a result, IDS has a high false alarm rate. When designing an intrusion detection system for automobiles, we should realize that the system can achieve a higher alarm rate in the face of known types of attacks, while in the face of unknown attacks and special situations, the system can achieve a lower false alarm rate through the corresponding adaptive update process. At the same time, aiming at the characteristics of automobile communication, such as stable dynamic topology and high real-time requirements, it is necessary to achieve lower communication load and smaller memory space.

To solve the technical defect of traditional IDS, that is, it can only detect specific threat models efficiently [32,33], and improve the efficient detection of unknown attacks on vehicular systems. The related technology of deep learning is applied to IDS. Utilizing heuristic search characteristics of deep learning and strong adaptive characteristics, the higher detection rate, and a lower false positive rate for abnormal conditions are achieved [34]. In this paper, the deep neural network (DNN) is applied to design in-vehicle IDS. With the help of the DNN, the intrusion characteristics can be extracted independently without human labeling, and the traditional problems faced by in-vehicle IDS can be solved. The traditional DNN model is trained to extract the relevant characteristics of the vehicle behavior data packet from the host, and the corresponding back propagation algorithm is combined with GDM algorithm and GDM/AG algorithm to implement the iterative updating process of the network. Experiments show that compared with the traditional rule-based or behavior-based intrusion detection system, this paper proposes a method that applies neural networks to the vehicle IDS system, and gradually improves the detection accuracy and detection speed through the corresponding adaptive update process. In the case of convergence speed, the corresponding optimal value can be obtained faster than the conventional back propagation neural network. The GDM/AG algorithm is superior to the GDM algorithm and the traditional back propagation neural network in terms of average sample iteration time and sample detection rate [7]. In terms of the accuracy of anomaly detection, compared with the traditional intrusion detection system, it can have higher detection accuracy and lower false alarm rate.

The rest of paper is organized as follows: The second part elaborates the relevant background knowledge of the Internet of Vehicles and the related work of deep learning in IDS. The third part describes the characteristics of the proposed IDS, and how the GDM-based back propagation neural network and the GDM/AG-based back propagation neural network are applied to the IDS of the vehicle system and how to detect the replay attacks in the vehicle network. In the fourth part, we use real cars to evaluate and compare the performance of our proposed models with traditional models. Finally, we summarize the problems raised and explains the future direction of work accordingly.

II. BACKGROUND KNOWLEDGE

For the sake of the integrity of the article, we will make bravely introduce in this chapter through the elemental composition of the Internet of Vehicles and the deep learning.

A. Internet of Vehicles

As shown in Fig. 1, on the Internet of Vehicles, it corresponds to a communication entity. Furthermore, each vehicle is equipped with a more significant number of devices for corresponding communication with other entities, such as GPS, Rader, T-Box and other equipment. GPS can accurately locate the geography information of the corresponding car via satellite signals. Rader is used to measuring the related signals between vehicles [25]; T-Box realizes the data exchange process between vehicles through the built-in communication module, special automobile SIM card, special short distance communication technology (DSRC, Dedicated Short Range Communications) and long Term Evolution-Vehicle (LTE-V).

Fig. 1. Vehicle network communication environment topology

JOURNAL PRE-PROOF

In the communication process, the internal data of the car is exchanged through the CAN bus. The maximum rate that the CAN bus can reach is 1 Mbps [26-28]; the data frame format is as shown in Fig. 2, it is made up of the data domain, the arbitration domain, the control domain, and the verification part [22].

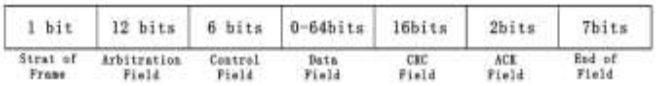


Fig. 2. Format of CAN data frame

B. Research Status of Deep Learning in Intrusion Detection

Vehicle intrusion detection system deploys the system on the vehicle in the form of corresponding software or hardware, collects data from ECU (Electronic Control Units) and CAN bus for corresponding analysis, and sends corresponding alarm information to the driver after discovering the relative abnormal behavior to ensure the safety of the real vehicle [21]. However, due to the limited computing resources and storage space of the car ECU, the traditional network-based IDS is challenging to apply to the vehicle directly. In order to solve the above problems, many IDS for automotive systems have been proposed in recent years. In the development of intrusion detection research, compared with the traditional cryptosystem [18,19], which aims at the security protection of automobile system, it can only target the penetration attacks from external attackers on the network; while the intrusion detection system can realize the efficient detection of internal attackers or external attackers [10-17]. The machine learning-based intrusion detection method proposed in [10, 11] can only be efficient for a specific threat model. [12, 13, 15] proposes to introduce the artificial neural network (ANN) and support vector machine (SVM) technology into the design of intrusion detection system, and use statistical methods to build relevant models for behavior data. In [14], the author proposes a method to detect intrusive nodes by using entropy value in information theory. By modeling normal behavior, any node deviating from normal behavior will be identified as anomaly node. After detecting the abnormal node, the network security will be protected by removing the anomaly node from the vehicle network. Through the corresponding experiments, we can find that this scheme has high detection efficiency and low false alarm rate. However, with the ever-increasing of numbers of automobile nodes in the network and the increasing of communication density, the overall performance of the system will decline. In [16], an automatic learning algorithm is proposed, which can achieve high accuracy in pattern recognition. This algorithm detects intrusion detection by collecting data packets from legitimate vehicle nodes and forwards false copies of them to attackers. Through experiments, the author points out that the accuracy of this algorithm in detecting abnormal data packets can reach nearly 95%. However, the application of this algorithm in the automotive network will bring huge computing overhead and transmission delay of network information, which is not suitable for automotive network topology nodes with high dynamic topology properties and real-time network requirements. In [17], an intrusion detection framework named IDFV is proposed. In this framework, the daily behavior of vehicles is modeled, and the anomalous behavior such as selective forwarding or worm vulnerability can be detected by using hybrid intrusion detection methods such as anomaly detection or rule-based detection. The proposed framework can achieve higher detection rate and lower false alarm rate when the number of abnormal vehicles is significant; however, the disadvantage of the model is that with the increasing of the number of vehicles, its communication overhead and load overhead are too much overhead.

At the same time, with the continuous development of deep learning technology in recent years, the application of deep learning technology in intrusion detection becomes more and more. The basic idea of using deep learning technology in intrusion detection is to design a corresponding classifier, which could extract features from data generated by entities to achieve efficient detection of abnormal behavior. Due to the limited ability of traditional vehicle's ECU in dealing with complex processes, many advanced algorithms in deep learning have hardly been applied to in-vehicle networks [29]. However, in the up-to-date vehicle system, the computing power of ECU has been significantly improved, and its ability to handle real-time tasks has been gradually enhanced [35]. As a sustainable development of deep learning, neural network mainly realizes the prediction and perception of unknown behavior by constructing corresponding multi-layer artificial neural network with learning ability. The neural network has made significant achievements in speech recognition, image processing, and feature extraction, which makes people pay more attention to improving the intelligence of the neural network [21]. The behavior data of entities are analyzed and processed by using related deep learning algorithm. By using corresponding data sets to build and train relevant models for user behavior, experiments show that the model trained by deep learning algorithm has higher accuracy and robustness compared with the traditional IDS [1,25,29-31].

III. Research on Vehicle Intrusion Detection Based on Deep Neural Network

A. The characteristics of IDS proposed

The attack scenario we need to consider is to attack the vehicle by injecting malicious data packets into the CAN bus in the vehicle. However, the in-vehicle network matches the mobile device of the corresponding driver by using a communication link like the 3g, 4g, 5g, Wi-Fi [36] or through a self-diagnostic tool such as an OBD port [37]. The proposed intrusion detection system CAN detect and classify the intrusion behavior by using the deep neural network model through the data packets broadcasted by CAN bus, as illustrating in Fig. 3. Its characteristics are as follows:

1. The proposed IDS is a HIDS, which can detect replay attacks.

2. It can monitor vehicle data packet parameters, such as vehicle speed, vehicle rpm (revolutions per minute) and more in real time.

JOURNAL PRE-PROOF

3. The proposed system is an IDS based on anomaly detection. In the simulation experiment environment, we set specific rules to implement the detection of vehicle replay attacks. The rules are as follows: We use the training data set to generate the corresponding intrusion detection model; then use the test data set as the input data of the network model, and perform the iterative operation in the same way to obtain the corresponding error value. By comparing the actual error value with the threshold we set, the threshold is the upper error limit between the estimated value and the actual value. If the corresponding error exceeds the corresponding threshold range, we would classify its behavior into the abnormal category and notify the administrator of the corresponding behavior. Otherwise, we consider that legitimately authorized users generate the behaviour, and classify it as the corresponding normal category.

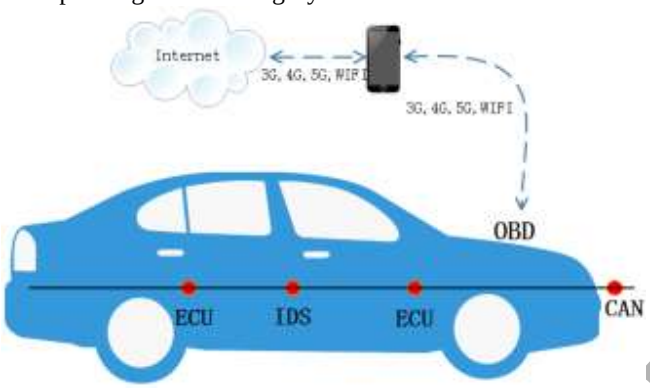


Fig. 3. Networked vehicle in real scene

B. Research on GDM algorithm in deep neural network

Compared with the traditional BP algorithm, GDM algorithm [6] is an enhanced gradient descent algorithm. GDM algorithm can improve the efficiency of the algorithm by iteratively adaptively changing the gain of each node connected to it to change the direction of finding the optimal global solution. In traditional neural networks, the mathematical problem corresponding to the objective function is to find a set of appropriate weight vectors, so that under the action of these weight vectors, the error between the experimental estimation and the real value can be minimized, so that under the action of these weight vectors, the error $E(w)$ between the experimental estimation and the real value can be minimized, which can be referred to (1):

$$\min_{w\in R^n} E(w) \tag{1}$$

In deep neural networks, we usually use formula (2) to define the error function:

$$\mathrm{E} = \frac{1}{2}\sum_0^K (\hat{y} - y)^2 \tag{2}$$

Among them, y is the real value, and $\hat{y}$ is the experimental estimate value. In traditional neural networks, we calculate the corresponding experimental predicted $\hat{y}$ by using the following equation:

$$\hat{y} = \sigma(\mathrm{z}) = \sigma(w^T \mathrm{X} + \mathrm{b}) \tag{3}$$

Then we update the weight parameter w and the corresponding gain term b by back propagation algorithm. Specifically, we use (4) and (5) to calculate the corresponding partial derivatives:

$$\frac{\partial E}{\partial w} = \frac{\partial E}{\partial \sigma}\cdot\frac{\partial \sigma}{\partial z}\cdot\frac{\partial z}{\partial w},\ w_{new} = w - \alpha\frac{\partial E}{\partial w} \tag{4}$$

$$\frac{\partial E}{\partial b} = \frac{\partial E}{\partial \sigma}\cdot\frac{\partial \sigma}{\partial z}\cdot\frac{\partial z}{\partial b},\ b_{new} = b - \alpha\frac{\partial E}{\partial b} \tag{5}$$

In the GDM algorithm, we calculate the gradient descent rule of weight by (6):

$$\frac{\partial E}{\partial w_{ij}^L} = \frac{\partial E}{\partial net^{L+1}}\cdot\frac{\partial net^{L+1}}{\partial o_j^L}\cdot\frac{\partial o_j^L}{\partial net_j^L}\cdot\frac{\partial net_j^L}{\partial w_{ij}^L}$$

$$= [-\delta_1^{L+1} \quad \cdots \quad -\delta_n^{L+1}]\begin{bmatrix} w_{1j}^{L+1} \\ \cdots \\ w_{nj}^{L+1}\end{bmatrix} f'\left(c_j^L net_j^L\right) c_j^L \cdot o_j^{L-1} \tag{6}$$

Then, the weight gain Δw_{ij}^L is calculated by using (7), and the corresponding weight values W_{new} are updated by (8):

$$\Delta w_{ij}^L = \eta\delta_j^L c_j^L o_j^{L-1} = \eta\frac{\partial E}{\partial w_{ij}^L} \tag{7}$$

$$W_{new} = W_{old} + \alpha\Delta w_{ij}^L \tag{8}$$

Correspondingly, we can use (9) and (10) to calculate the gradient descent rule of gain Δc_j^L and the updated expression of gain, respectively:

$$\Delta c_j^L = \eta\delta_j^L\frac{net_j^L}{c_j^L} \tag{9}$$

$$c_j^{new} = c_j^{old} + \Delta c_j^L \tag{10}$$

C. Research on GDP/AG algorithm in deep neural network

GDM/AG algorithm [7] is an enhanced BP algorithm, which can improve the performance by adaptively changing the gain of its activation function. The algorithm can modify the search direction of the optimal solution by adaptively changing the gain of the activation function corresponding to each node, so as to improve the performance of the algorithm. Similarly, the corresponding solution problem of the algorithm is to seek a set of optimal weight vectors and corresponding gains to realize that under the optimal parameters, its error can be less than a certain specified error term, and the following formula can calculate the corresponding network error evaluation:

$$\mathrm{E} = \frac{1}{2}\sum_0^K \left(y - o_k(o_j, c_k)\right)^2 \tag{11}$$

$$o_k(\mathrm{z}) = \frac{1}{1+e^{-z}} \tag{12}$$

Where y is the real value, $\mathrm{o_k}$ is the output value of the activation function corresponding to the network k-th node, and w_{ij} is the weight value connecting the corresponding nodes of the i-th and j-th layers.

After completing a forward propagation, we need to make a reverse propagation calculation for the generated network model. Firstly, the partial derivative $\frac{\partial \mathrm{E}}{\partial \mathrm{C_k}}$ of the node

JOURNAL PRE-PROOF

corresponding to the output layer k is calculated, and $\frac{\partial E}{\partial c_j}$ is needed to be calculated for corresponding hidden layer j. The expressions for calculating the gain and updating the result are described in (13) to (15), respectively:

$$\Delta c_k = \eta\left(-\frac{\partial E}{\partial c_k}\right) \tag{13}$$

$$\frac{\partial E}{\partial c_k} = -(t_k - o_k)o_k(1-o_k)\left(\sum w_{ij}o_i + \theta_j\right) \tag{14}$$

$$\Delta c_k(n+1) = \eta(t_k - o_k)o_k(1-o_k)\left(\sum w_{ij}o_i + \theta_j\right) \tag{15}$$

We can also calculate the gain of the node corresponding to the hidden layer j by the following equation. The specific formula is referred to (16) to (17):

$$\Delta c_j = \eta\left(-\frac{\partial E}{\partial c_j}\right) \tag{16}$$

$$\frac{\partial E}{\partial c_j} = -\sum c_j w_{jk} o_k(1-o_k)(t_k - o_k)o_j(1-o_j)\left(\sum w_{ij}o_i + \theta_j\right) \tag{17}$$

$$\Delta c_j(n+1) = \eta[-\sum c_j w_{jk} o_k(1-o_k)(t_k - o_k)o_j(1-o_j)(\sum w_{ij}o_i + \theta_j)] \tag{18}$$

The gain of the weights $\frac{\partial E}{\partial W_{jk}}$ calculated by the nodes corresponding to the output layer k-th and the updated expression of the weights Δw_{jk} are described as follows:

$$\frac{\partial E}{\partial W_{jk}} = -(t_k - o_k)o_k(1-o_k)c_k o_j \tag{19}$$

$$\Delta w_{jk} = \eta(t_k - o_k)o_k(1-o_k)c_k o_j \tag{20}$$

The gain of the calculated deviation of the node corresponding to the output layer k-th and the updated expression of the deviation are described as follows:

$$\frac{\partial E}{\partial \theta_k} = -(t_k - o_k)o_k(1-o_k)c_k \tag{21}$$

$$\Delta\theta_k = \eta(t_k - o_k)o_k(1-o_k)c_k \tag{22}$$

Correspondingly, we also need to calculate the corresponding gain values of the connection weights between the nodes of the hidden layer and update the nodes between the hidden layers with the obtained gain values. The specific calculation rule of the gain values and update expressions of the nodes between the hidden layers are as follows:

$$\frac{\partial E}{\partial w_{ij}} = -[\sum_k c_k w_{jk} o_k(1-o_k)(t_k - o_k)]c_j o_j(1-o_j)o_i \tag{23}$$

$$\Delta w_{ij} = \eta[\sum_k c_k w_{jk} o_k(1-o_k)(t_k - o_k)]c_j o_j(1-o_j)o_i \tag{24}$$

$$\frac{\partial E}{\partial \theta_k} = -[\sum_k c_k w_{jk} o_k(1-o_k)(t_k - o_k)]c_j o_j(1-o_j) \tag{25}$$

$$\Delta\theta_j = \eta[\sum_k c_k w_{jk} o_k(1-o_k)(t_k - o_k)]c_j o_j(1-o_j) \tag{26}$$

IV. SIMULATION RESULTS AND DISCUSSION

A. *Data Set Description*

To verify that the proposed algorithm can accelerate the convergence speed of back propagation network and achieve high intrusion detection efficiency, we collect data on the real intelligent vehicle CAN bus (Fig. 4). The way to collect data is to connect the CAN adapter directly to the CAN bus. The CAN bus data collection device is KvaserCAN Leaf Light V2. The computer simulates the attackers to launch spoofing command attacks on the vehicle, such as acceleration and emergency braking commands, and replay attacks. We collected nearly 300,000 vehicle-related traffic data. The relevant open source software BusMaster is used to generate corresponding data log files for the collected data. Part of the data is shown in Fig. 5. The data segment is composed of timestamp, message ID, description of relevant data, and description of relevant vehicle status information. Because the message ID and some of its corresponding parameters involve the confidential information of the cooperative enterprise, we fuzzify the ID. In this paper, the data we need are mainly vehicle-related status information, message ID, and the corresponding message format.

Fig. 4. The vehicle used for data acquisition in the experiment

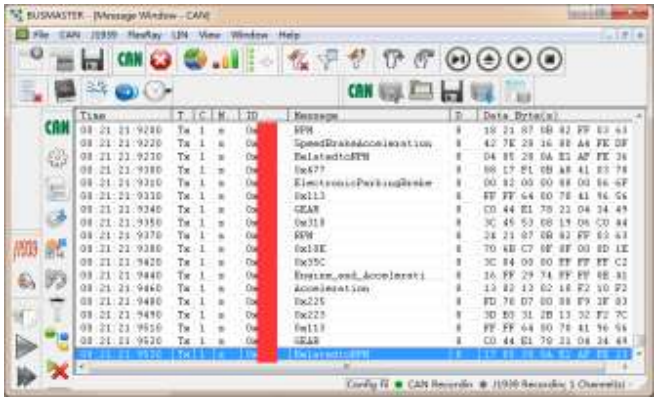


Fig. 5 Part of the sample data collected

From Fig. 5, we can see that most of the data transmitted on the CAN bus are the basic format of CAN data packets, that is, the data packets corresponding to different parameter IDs can transmit one or more parameters. For example, in eight bytes of a CAN data package, byte 1 and byte 2 correspond to the high 8-bit and low 8-bit of data information, while byte 3 and byte 4 represent the high 8-bit and low 8-bit of the corresponding vehicle speed, which can vary from 0x0000 to 0xffff. We use python's sklearn package to extract the relevant

JOURNAL PRE-PROOF

parameters from the CAN log file generated by BusMaster and convert it into the corresponding CSV file. The corresponding data file is shown in Fig. 6. The corresponding MAX-MIN method is used to normalize the data.

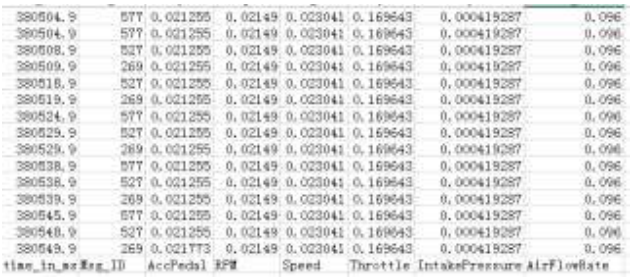


Fig. 6 Sample of some data after preprocessing

In order to avoid the problem of fitting in the neural network model, we use 70% of the data to train the data model according to the data partitioning proposal in [21]. We use the remaining 30% of the data to evaluate the performance of the trained model.

B. Data Set Analysis

We usually analyze the collected data by analyzing the corresponding characteristics of the data, such as the frequency and amplitude of the signal, or by combining the data correlation and the working principle of the car to analyze the parameters of the car, such as the relationship between the rpm of the vehicle and the speed of the vehicle. After analyzing the data related to vehicle operation, we summarize the data on the CAN bus of the automobile, which can be divided into two types according to whether there are clear rules or not. Some data merely has a distinctive feature, such as turning light signal, vehicle headlight signal, and so on. Data with distinctive pattern refers to data that has a direct relationship between engine speed and acceleration pedal or load. If an attacker forges one or several of the data, the corresponding relationship will be destroyed. Fig. 7 illustrates the relationship between the average change of speed, rpm, and gear from the data we collected.

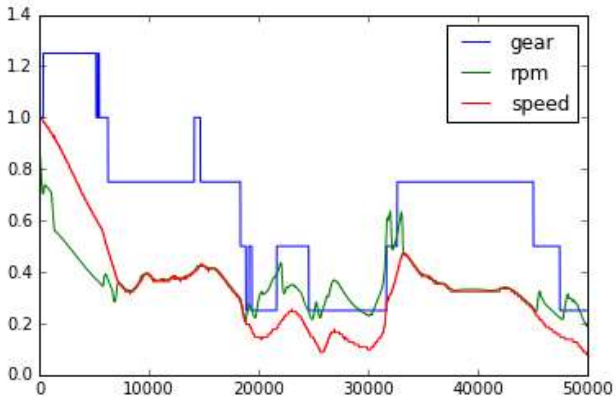


Fig. 7 Diagram of the relationship between vehicle speed, rpm, and gear

When we attempt to forge and replay these data, the change rate related to the data, as well as the correlation with other data, will change accordingly. These kinds of relationship are shown in Fig. 8.

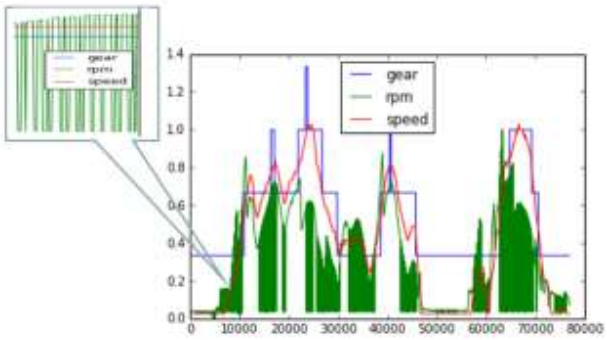


Fig. 8 Changes between three performance metrics when subjected to replay or data spoofing attacks

From Fig. 8, we can see that because of the replay attack on the vehicle, the replay data and the normal data are mixed, so the waveform of the rotational speed appears oscillation phenomenon, so we can believe that the location of the oscillation is abnormal. Although it can be seen from the figure that the replay attack on rpm does not affect other parameters, but it cannot be said that replay attack on one parameter of CAN bus will not have the corresponding impact on other parameters. Therefore, after correlation analysis, we use the strong correlation parameters, such as vehicle speed, rpm, intake pressure, throttle pedal position, and gear as the data vector of the learning model. Table 1 corresponds to the data that we preprocessed after 68 minutes of testing. Among them, MAF (Mess Air Flow Sensor) is the air flow sensor, and MAP (Mess Air Pressure Sensor) is the pressure sensor of the automobile intake system.

Time_ms	RPM	Speed	MAP	MAF	AccPedal	Throttle
138973	0.2879838	0.1342592	0.0590551	0.1675675	0.6971070	0.1377952
138974	0.2873125	0.1342592	0.0551181	0.1675675	0.6971070	0.1377952
138975	0.2873125	0.1342592	0.0511811	0.1675675	0.6971070	0.1377952
138976	0.285970	0.1342592	0.0472440	0.1675675	0.6971070	0.1377952
138977	0.285970	0.134259	0.0511811	0.1675675	0.6971070	0.1377952

TABLE 1 PREPROCESSED DATA SAMPLES

C. Experimental Evaluation

The purpose of this paper is to accelerate the convergence speed of the neural network through two methods and to achieve efficient intrusion detection efficiency through the proposed neural network model. So we use CPU time-consuming [10] and iteration times of training network as performance indicators of the corresponding network model and calculate TPR (True Positive Rate) and FPR (False Positive Rate) of samples by equation (27) and equation (28) respectively:

$$\mathrm{TPR} = \frac{TP}{TP+FN} * 100\% \tag{27}$$

$$\mathrm{FPR} = \frac{FP}{FP+TN} * 100\% \tag{28}$$

At the same time, we determine whether the training of the network model is finished by judging whether the error value of the training is less than the threshold value we specified to determine whether the model is generated or not. All simulations have been performed using ASUS laptop with inter® CoreTM i5 CPU 1.80 GHz processor, 8GB RAM, and

using MATLAB 9.1 (R 2016b). The architecture of the tested NNs is {6-12-2} fully connected networks. By using the data collected from CAN as input, we use the supervised learning method to compare the results obtained by neural network prediction with the actual corresponding categories and calculate the error between the actual value and prediction by using Equation 2 or Equation 11. When the corresponding error is greater than the threshold we specify, we can think that the corresponding vehicle behavior is abnormal, and can be judged as an intrusion.

In the experiment, we evaluate the whole network model by changing the learning rate and the momentum in the case of fixed momentum and evaluate the efficiency of the network model by calculating CPU time and the number of iterations of the corresponding samples. The experimental results are shown in following 4 tables from Table 2 to Table 5 respectively.

Momentum term α	the using algorithm GDM algorithm[6]		
	training data set		testing data set
	CPU compute time(s)	Convergence count	Detection time(ms)
0.2	303.573	5276	4.23
0.4	241.496	3573	3.64
0.6	129.326	1692	3.41
0.8	80.127	527	3.21
1.0	15.549	236	3.05

TABLE 2 THE EVALUATION RESULTS OF MOMENTUM TERM A ON THE EFFICIENCY OF GDM BASED BP FOR LEARNING IDS TO DETECT REPLAY ATTACK WITH FIXED LEARNING RATE EQUAL WITH 0.85

Momentum term α	the using algorithm GDM/AG algorithm[6]		
	training data set		testing data set
	CPU compute time(s)	Convergence count	Detection time(ms)
0.2	270.671	4467	3.63
0.4	164.721	2707	3.42
0.6	92.146	1342	3.21
0.8	30.635	624	3.14
1.0	10.279	140	2.98

TABLE 3 THE EVALUATION RESULTS OF MOMENTUM TERM ON THE EFFICIENCY OF GDM/AG BASED BP FOR LEARNING IDS TO DETECT REPLAY ATTACK WITH FIXED LEARNING RATE EQUAL WITH 0.85

Learning rate η	the using algorithm GDM algorithm[7]		
	training data set		testing data set
	CPU compute time(s)	Convergence count	Detection time(ms)
0.4	230.711	2437	3.37
0.8	120.659	1327	3.26
1.2	69.197	439	3.05
1.6	34.263	192	2.82

TABLE 4 THE EVALUATION RESULTS OF LEARNING RATE ON THE EFFICIENCY OF GDM BASED BP FOR LEARNING IDS TO DETECT REPLAY ATTACK WITH FIXED MOMENTUM TERM EQUAL WITH 0

Learning rate η	the using algorithm GDM/AG algorithm[7]		
	training data set		testing data set
	CPU compute time(s)	Convergence count	Detection time(ms)
0.4	182.647	1975	3.24
0.8	122.793	843	3.15
1.2	85.282	210	3.09
1.6	19.201	108	2.63

TABLE 5 THE EVALUATION RESULTS OF LEARNING RATE H ON THE EFFICIENCY OF GDM/AG BASED BP FOR LEARNING IDS TO DETECT REPLAY ATTACK WITH FIXED MOMENTUM TERM EQUAL WITH 0

According to the experimental results summarized in these four tables, we find that the training time of the corresponding neural network model is longer. When the learning rate is fixed at 0.85, and the momentum parameter is set to a small value, the training time complexity of the model is high, and the maximum time is obtained. The complexity is about 6 min, so according to the suggestion in [31], when training the corresponding neural network model, we should train the model offline. Furthermore, the experiment results illustrate that by using the network model trained with these two methods, our proposed model can achieve very efficient time cost (i.e. 2-4ms) in the detection of abnormal data packets, which demonstrates that our approach is not only theoretically sound, but also practical. The comparison between the actual value of the velocity value and the velocity predicted by the neural network is shown in Fig. 9. It can be seen that there is a small error between the actual value and the predicted value. In order to make the error result in Fig. 9 easier to observe, Figure 10 shows the variance sequence between the velocity observation and the predicted value, and the trained neural network has higher accuracy but lower error rate.

Fig. 9 The results of velocity prediction using the proposed network structure

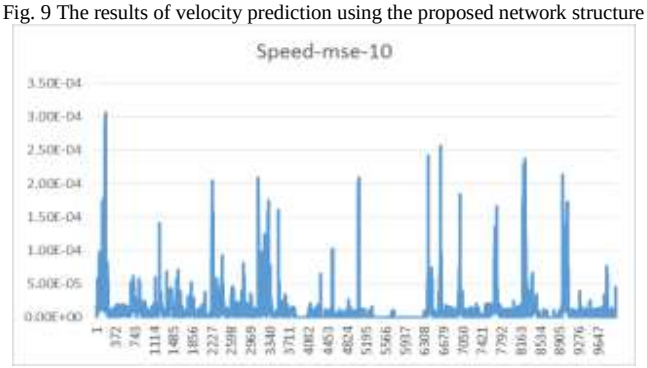


Fig. 10 The variance sequence between the actual value of velocity and the error value of network

Fig. 11 is a coordinate map of the vehicle engine rpm data obtained from the replay attack on the normal driving of the vehicle. After testing, we find that although only the abnormal rpm data are forged, the results of the abnormal rpm data calculated by the corresponding neural network model will also have the same impact on the prediction results of other parameters, that is, the abnormality will also appear in the prediction of other parameters. The results are shown in Fig. 11 illustrating that when the rpm is abnormal, the predicted results will also show the same abnormality, which means that no matter which parameter the attacker forges or replays, we

can classify the abnormality by the parameters themselves and their influence on the predicted and observed values of other arbitrary parameters. It allows our approach to detect replay attack and forgery attack very well. Fig. 13 shows an example of anomaly detection by comparing the predicted value with the classified value using speed as an indicator. Rpm in the input data set used here is anomalous; however, we can locate the anomaly by observing the variance between the predicted value and the observed value. The threshold in the figure is the maximum errors between real values and predict values. When the variance is larger than the threshold value, we can classify it as the corresponding anomaly. Moreover, we can also find that the variance calculated from the observed and predicted values of speed increases when the speed is abnormal. Because of the corresponding abnormalities can be detected, we can use emergency response measures such as firewalls to correspond communication links based on these abnormal detection results, and stop communication to protect the car from network attacks.

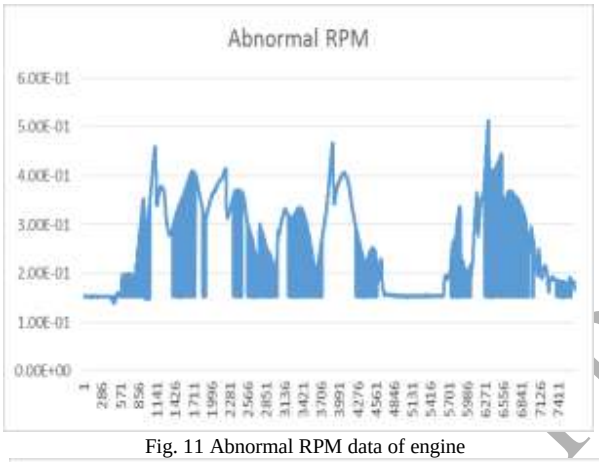


Fig. 11 Abnormal RPM data of engine

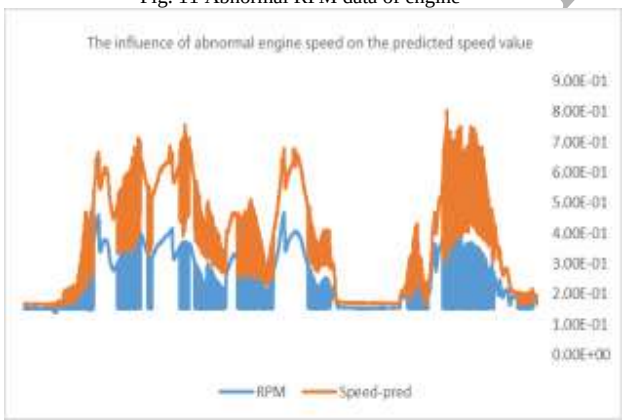


Fig. 12 Effect of abnormal engine RPM on speed prediction

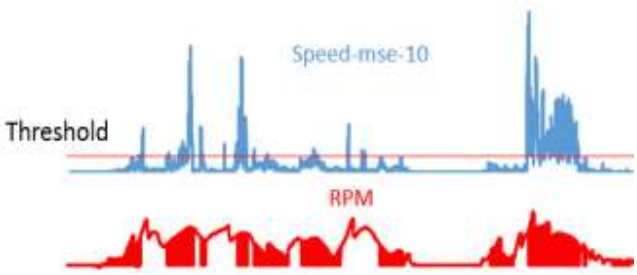


Fig. 13 Anomaly detection based on speed

In the confusion matrix of the test results shown in Fig. 14 we can calculate the corresponding TPR and FPR by using Equation 27 and 28. Experiments show that the proposed model can achieve approximately 98% accuracy and a low false alarm rate. Similarly, we compare the average processing time of our proposed IDS model with those of [38] and [39], respectively. The compare results are shown in Fig. 15. The results show that the average processing time of the proposed IDS model is less than that of the two models. Fig. 16 indicates that the TPR of the proposed scheme reaches nearly 98% by using the ROC curve, and the corresponding FPR is only about 1%-2%. The proposed scheme has higher detection efficiency than the former two. Similarly, the results show that by using the advantages of deep learning in feature extraction, our model achieves higher detection accuracy.

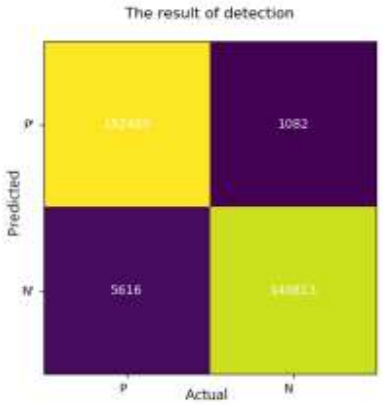


Fig. 14 Confusion matrix results

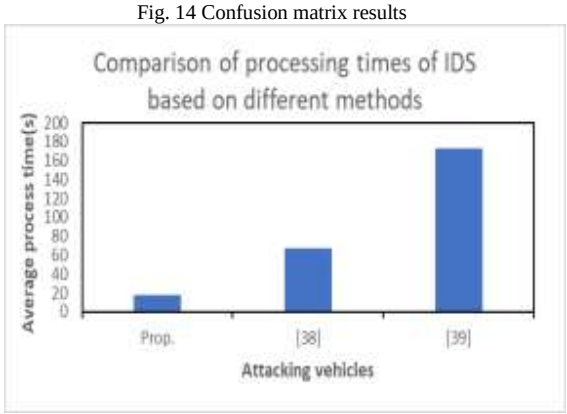


Fig. 15 Comparison of average processing time of IDS proposed by different schemes

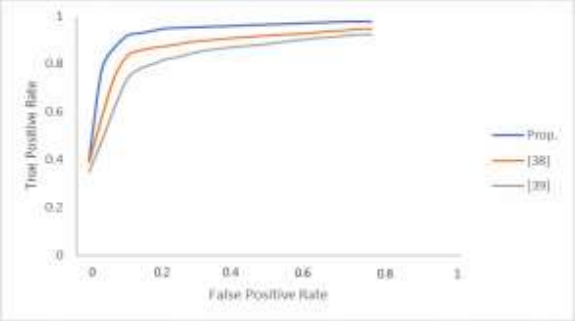


Fig. 16 ROC curves for in-vehicle intrusion detection performance

V. CONCLUSION

With the continuous combination of Internet technology and automobile industry technology, the application of Vehicle Networking in people's daily life is becoming more and more extensive. At the same time, due to its characteristics and the incompleteness of existing related research, people and researchers pay more attention to the development of vehicle networking security issues. Therefore, this paper analyses the current security problems faced by the Internet of Vehicles, mainly for the current vehicle IDS, and proposes the deep neural networks-based approach to achieve better intrusion detection of in-vehicle behavior and enhance the convergence of the model. By using the neural network and the corresponding accelerated convergence algorithm, the high recognition accuracy of abnormal behavior in the vehicle system can be achieved. Experiments show that the proposed approach learns and enables the legitimate detection of traffic-related attack types, and improve the internal security of the vehicle system to a great extent. In the future, we will work on the use of other deep learning methods to improve in-vehicle IDS detection performance and achieve higher security in the vehicle network security.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships
that could have appeared to influence the work reported in this paper

ACKNOWLEDGMENTS

This work was supported by Research on the Influences of Network Security Threat Intelligence on Sichuan Government and Enterprises and the Development Countermeasure (Project ID 2018ZR0220), Research on Key Technologies of Network Security Protection in Intelligent Vehicle Based on (Project ID 2018JY0510), the Research on Abnormal Behavior Detection Technology of Automotive CAN Bus Based on Information Entropy (Project ID 2018Z105), the Research on the Training Mechanism of Driverless Network Safety Talents for Sichuan Auto Industry Based on Industry-University Synergy (Project ID 18RKX0667).

REFERENCES

[1] H. Qiao, G. Li, and Y. Chen., "Research on Key Technologies of Vehicle Networking System Architecture," Electronic Production, vol. 352, no. 11, pp. 43-44+50, 2018.

[2] H. Sedjelmaci, S. M. Senouci, and M. A. Abu-Rgheff., "An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks," IEEE Internet of Things Journal, vol. 6, no. 1, pp. 570-577, 2014.

[3] V. Golovko and P. Kochurko, "Emotion recognition using neural networks" in Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Bulgaria, 2009.

[4] X. Li and B. Yang., "Analysis of Safety Protection in Vehicle Networking." Mobile Communication, vol. 39, no. 11, pp. 30-33, 2015.

[5] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and et al., "Intrusion detection by machine learning: A review." Expert Systems with Applications vol. 36,no. 10, pp. 11994-12000, 2009.

[6] N. M. Nawi, Nazri, M. R. Ransing, and R. S. Rajesh. "An Improved Learning Algorithm Based On the Conjugate Gradient Method for Back Propagation Neural Networks. " TRANSACTIONS ON ENGINEERING, COMPUTING AND TECHNOLOGY, vol. 4, pp. 211-215, 2009.

[7] N. M. Nawi, R. S. Ransing, M. N. M. Salleh, and et al., "An Improved Back Propagation Neural Network Algorithm on Classification Problems." in Database Theory and Application, Bio-Science and Bio-Technology - International Conferences, Korea, 2010.

[8] S. Woo, H. J. Jo, and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN." IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 1-14, 2014.

[9] H. I. Ahmed, N. A. Elfeshawy, S. F. Elzoghdy, and et al., "A Neural Network-Based Learning Algorithm for Intrusion Detection Systems." Wireless Personal Communications., vol. 97, no. 2, pp. 3097-3112, 2017.

[10] P. Tyagi and D. Dembla., "Investigating the Security Threats in Vehicular ad hoc Networks (VANETs): Towards Security Engineering for Safer on-road Transportation." in IEEE International Conference on Advances in Computing, Communications and Informatics, Indian, 2014.

[11] X. Sun, B. Yan, X. Zhang, and et al., "An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network." PLOS ONE., vol. 10, no. 10, pp. 1-16, 2015.

[12] V. Golovko and P. Kochurko, "Intrusion Recognition Using Neural Networks." In IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Bulgaria, 2005.

[13] Z. Zhang, J. Li, C. N. Manikopoulos, and et al., "HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification." In IEEE Workshop on Information Assurance and Security, United States, 2001.

[14] M. Raya, P. Papadimitratos, I. Aad, and et al., "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks." Selected Areas in Communications, IEEE Journal, vol. 25, no. 8, pp. 1557-1568, 2007.

[15] S. Ruj, M. A. Cavenaghi, Z. Huang, and et al., "Data-centric Misbehavior Detection in VANETs." in IEEE Vehicular Technology Conference 73th, United States, 2011.

[16] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs." Computers & Electrical Engineering, vol. 40, no. 6, pp. 1981-1996, 2014.

[17] H. Sedjelmaci and S. M. Senouci, "A new Intrusion Detection Framework for Vehicular Networks" in IEEE International Conference on Communications, Australia, 2014.

[18] K. Mershad and H. Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks" IEEE Trans. Veh. Tchnol., vol. 62, no. 2, pp. 536-551, 2013.

[19] H. Zhu, R. Lu and X. Shen, "Security in service-oriented vehicular networks." IEEE Wire. Comm., vol. 16, no. 4, pp. 16 – 22, 2009.

[20] Z. Feng, M. He, B. Li, and et al. "Research progress on Key Technologies of automobile information security attack and defense." Journal of Information Security, vol. 2, no. 2, pp.1-14, 2017.

[21] L. Gao, F. Li, X. Xu and et al., "Intrusion detection system using SOEKS and deep learning for in-vehicle security." Cluster Computing, to be published. DOI: 10.1007/s10586-018-2385-7, 2018.

[22] A. Samad, S. Alam, S. Mohammed and et al., "Internet of vehicles (IoV) requirements, attacks and countermeasures." In IEEE International Conference on "Computing for Sustainable Global Development, New Delhi, 2018.

[23] S. M. Othman, N. T. Alsohybe, F. M. Ba-Alwi, and et al., "Survey on Intrusion Detection System Types." Algorithms, security and soft computing tools,2018,[online].Available:https://www.researchgate.net/publication/329363322_Survey_on_Intrusion_Detection_System_Types

[24] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez "Internet of

JOURNAL PRE-PROOF

vehicles: architecture, protocols, and security." IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3701-3709, 2017
[25] J. Liang, "Application of Intrusion Detection System in Vehicle Networking," M.S. thesis, Dept. Computer. Soft., Shenzhen Univ., Shenzhen, China, 2017.
[26] R. I. Davis, A. Burns, R. J. Bril and et al., "Controller Area Network (CAN) schedulability analysis: Refuted, revisited and revised." Real-Time Systems, vol. 35, no. 3, pp. 239-272, 2007.
[27] S. Shreejith, S. A. Fahmy and M. Lukasiewycz "Reconfigurable Computing in Next-Generation Automotive Networks." IEEE Embedded Systems Letters, vol. 5, no. 1, pp. 12-15, 2013.
[28] M. Farsi, K. Ratcliff and M. Barbosa, "An overview of Controller Area Network." Computing and Control Engineering Journal, vol. 10, no. 3, pp.113-120, 1999
[29] M. J. Kang and J. W. Kang, "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security." PLOS ONE, vol. 11, no. 6, pp.1-17, 2016
[30] S. Mohammadi and A. Namadchian, "A New Deep Learning Approach for Anomaly Base IDS using Memetic Classifier." International Journal of Computers Communications and Control, vol. 12, no. 5, pp. 667, 2017.
[31] X. Zhang, C. Gu and J. Lin, "Support Vector Machines for Anomaly Detection" in IEEE World Congress on Intelligent Control and Automation., China, 2006.
[32] P. Tyagi and D. Dembla, "Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation" in Proc. IEEE Int. Conf. ACCI, 2014, pp. 2084-2090.
[33] X. Sun, B. Yan, X. Zhang and et al. "An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network" PLOS ONE, vol. 10, no. 10, pp. 1-16, 2015.
[34] A. J. Deepa and V. Kavitha, "A Comprehensive Survey on Approaches to Intrusion Detection System." Procedia Engineering, vol. 38, pp. 2063-2069, 2012.
[35] Handbook of networked and embedded control systems, Springer Basel Ag, Birkhäuser Boston, 2005, pp. 741-765.
[36] K. Koscher, A. Czeskis, F. Roesner and et al. "Experimental security analysis of a modern automobile." In IEEE Symposium on Security and Privacy, USA, 2010.
[37] S. Woo, H. J. Jo and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN." IEEE Trans. on Intel. Trans. Sys., vol. 16, no. 2, pp. 993-1006, 2015.
[38] Y. Bo, C. Xu and B. Xiao . "Detecting Sybil attacks in VANETs." Journal of Parallel and Distributed Computing, vol. 73, no. 6, pp. 746-756, 2013
[39] S. Yan, R. Malaney, I. Nevat, and et al. "Optimal Information-Theoretic Wireless Location Verification." IEEE Transactions on Vehicular Technology, vol.63, no. 7, pp. 3410-3422, 2014

Jiayan Zhang received the B.S. degree in Network Engineering from Nanchang Institute of Technology, Nanchang, Jiangxi, China, in 2018. He is currently working toward the M.S. degree in Chengdu University of Information Technology. His currently research interest is in vehicle security, such as identity authentication, intrusion detection and etc. Internet of vehicle and intelligent vehicle.

Fei Li received the B.E. degree in Internet of things from University of Science and Technology of Chengdu, Chengdu, Sichuan, China, in 1988 and M.E. degrees in computer science automatic control from the same university, in 1993. He is currently a Professor and the Dean of School of Cybersecurity, Chengdu University of Information Technology, Chengdu, Sichuan, China. His research interests are in the field of network and information system security, vehicle intelligence and security, Internet of things technology and applications and mobile Internet applications.

Haoxi Zhang is an Associate Professor from the Chengdu University of Information Technology, Chengdu, China. He received his Ph.D. degree in Knowledge Engineering from the University of Newcastle in 2013, and the master's degree in Software Engineering from the University of Electronic Science and Technology of China. His research interests focus on experience-oriented intelligent systems, knowledge engineering, Internet of Things, and Deep Learning. He has published more than 30 reputed journal and conference papers.

Ruxiang Li received the B.S. degree in Information Security from Chengdu University of Information Technology, Chengdu, Sichuan, China, in 2018. He is currently working toward the M.S. degree in Chengdu University of Information Technology. His currently research interest is in vehicle security, such as network situational awareness, intrusion detection and etc. Internet of vehicle and intelligent vehicle.

Yalin Li received the B.S. degree in Mechanical and Electronic Engineering from Chengdu University of Information Technology, Chengdu, Sichuan, China, in 2018. He is currently working toward the M.S. degree in Chengdu University of Information Technology. His currently research interest is in application of Artificial Intelligence in vehicle security, Internet of vehicle and intelligent vehicle.