Intrusion Detection of Vehicle Based on Generative Adversarial Networks

YingJiangLiu, JuanWang*, YangZhao

College of Cyberspace Security, Chengdu University of Information Technology, Chengdu, Sichuan, 610225, China

*wangjuan@cuit.edu.cn

Abstract. In the process of applying deep learning to intrusion detection, in order to ensure the recognition accuracy of the model, a large number of data sets need to be classified manually, and then the model training is carried out after labeling. In practice, the efficiency of manual label designation for enough data sets is extremely low. This paper aims to solve the intrusion detection problem of intelligent network vehicles. The problem of classification difficulty is proposed, and a method of vehicle intrusion detection based on Generative Adversarial Networks is proposed. Firstly, the vehicle driving data is collected, the collected data are put into the Generative Adversarial Networks for data classification, and the data set after training classification is used for model training. The experimental results show that the data classification can effectively improve work efficiency and reduce the resource overhead, which is practical in the application field.

Keywords: GANs; Intelligent network vehicle; Intrusion detection; Data classification

1. Introduction

In recent two years, the development of vehicle networking technology is particularly rapid. The Internet of vehicles has been widely used in the automobile manufacturing industry on a large scale, which not only makes intelligent transportation become a reality but also makes intelligent vehicles possible[1]. At the same time, the related security risks and loopholes are constantly found, resulting in the user may lose control of the vehicle in the process of driving, seriously endangering the safety of the driver's life and property. For example, in June 2015, two white hat hackers passed tests and found that Fiat Chrysler's Jeep free light could be controlled by a remote attack. As a result, Fiat had to recall 1.4 million vehicles urgently, the first time that the industry has recalled vehicles due to potential hacker attacks. However, intrusion detection can effectively avoid some attacks[2], just as it plays a role in the Internet of things[3] and industrial control system[4]. At present, when the real vehicle experimental data set is used for intrusion detection, the data is basically classified manually and the data label is specified manually, which is inefficient and inaccurate. It has seriously affected the researchers' exploration of vehicle information security system, but also led to the lack of corresponding protection countermeasures.

Deep learning is an important branch of machine learning[5]. By learning the inherent laws and relationships contained in sample data, the computer can analyze and learn text, sound, image, and other data[6]. As a deep learning model, Generative advanced networks are the most promising...
unsupervised learning method[7]. The model learns and generates the output through the game between the generative model and the discriminative model in the framework. In practical application, a deep neural network is used as a generative model and discriminative model. In the process of confrontation, G and D are promoted to each other until they reach Nash equilibrium, and an ideal output model is already produced.

In order to solve these above problems, this paper introduces Generative Adversarial Networks into the field of vehicle intrusion detection. By using the characteristics, GANs can learn features from the original data. GANs is used to learn the data features from the collected original vehicle data, and automatically label the data classification. After classification, a Softmax model will be trained with the labeled data. The experimental results show that the classification accuracy is not much different compared with manual marking, but the labor cost is greatly saved and the efficiency is greatly improved.

2. Principle and system design

2.1. Generative Adversarial Networks
The Generative Adversarial Networks is to make G learn the distribution of data through the continuous game between G (generator) and D (discriminator) and then adjust G and D according to optimization function[8]. After reaching Nash equilibrium, G can generate pseudo real data set from a random number. The implementation process is shown in fig.1.

![Fig.1 GANs network operation principle](image-url)

2.2. Implementation flow of the system
The implementation process of this method is roughly shown in Fig.2. Firstly, the vehicle data is collected through the OBD - II interface on the Automobile CAN-bus. The data to be collected includes CANID, Timestamp, DLC, and Data.
The data are stored in the database one by one after the completion of the collection. The collected data are preprocessed before the model training. Through the data preprocessing, the training time can be effectively reduced and the training efficiency and precision can be improved. Take the time window $T$ and put the data value in the time window into the matrix.

$$ f = \frac{f - \bar{f}}{\sigma} $$

(1)

Then we will standardize the original data according to the function before, which $\bar{f}$ represents the average value of $F$ and $\sigma$ represents the variance of $F$. After preprocessing, the data will put into the GANs network.

$$ \min_{G} \max_{D} (D, G) = E_{x \sim p_{data}(x)}[\log D(x)] + E_{z \sim p_{z}}[\log(1 - D(G(z)))] $$

(2)

After the adjustment, the existing data will be classified by the model we trained. After that, the classified data of GANs network is stored as a Classified Set, and CS is divided into a training set, test set and development set according to the ratio of 7:2:1. At the end of data classification, a softmax classifier model is trained by using a training set and test set, and the classification effect of the model is verified by verification set after training. The classification recognition rate of the model should be higher than that of the model trained only by manual data classification data set.

3. Experimental results and analysis
The experimental environment is NVIDIA 2060s, 16G ram, windows 10 operating system. Data classification and processing are based on Python and Tensorflow platform.

OTID$sdata set is used as an original dataset, and the data format is shown below.

In the collected raw data, we include four fields, they are:

- Timestamp: recorded the time we catch the data.
CAN ID: identifier of CAN message in hexadecimal.
DLC: Length of collected data bytes, from 0 to 8
DATA[0~7]: data value (byte).

\[
\begin{array}{|c|c|c|c|c|}
\hline
\text{Timestamp} & \text{ID} & \text{DLC} & \text{DATA} & \text{Detection} \\
\hline
1481193194.692547 & 01f1 & 000 & 00 00 00 00 00 00 00 00 & \\
1481193194.692785 & 0220 & 000 & 03 03 ff 03 0c 00 37 10 & \\
1481193194.696629 & 0316 & 000 & 05 18 18 09 19 11 00 7f & \\
1481193194.696860 & 018f & 000 & 00 22 19 00 00 3f 00 00 & \\
1481193194.697095 & 0000 & 000 & 00 17 f8 09 18 11 19 6d & \\
1481193194.697335 & 0081 & 000 & 4d 84 60 00 00 00 00 00 & \\
1481193194.697570 & 0260 & 000 & 05 19 00 30 ff 8f 5d 16 & \\
\hline
\end{array}
\]

Fig.3 Original data format

And After preprocessing, the data is putting into GANs network for data classification. We can finally get a data set with a detection tag just like this one below. In the previous implementation process, we need to add tags manually, which consumes a lot of time and resources. After the training of GANs model, we can quickly classify data and add tags through the model.

\[
\begin{array}{|c|c|c|c|c|}
\hline
\text{Time} & \text{CANID} & \text{DLC} & \text{Data} & \text{Detection} \\
\hline
1480116144.611851 & 05a2 & 000 & 25 00 a5 01 & 1 \\
1480116144.612099 & 051a & 000 & c8 11 00 8a 3c 00 40 00 & 0 \\
1480116144.610140 & 00a0 & 000 & 5a 7f 5e 0a 00 26 00 02 & 0 \\
1480116144.610350 & 00e1 & 000 & 7f 34 80 80 2e 00 00 00 & 0 \\
1480116144.613268 & 04b0 & 000 & 00 00 00 00 00 00 00 00 & 1 \\
1480116144.617012 & 018f & 000 & fe 42 26 00 00 43 00 10 & 0 \\
1480116144.617245 & 006a & 000 & 00 17 8a 00 26 1e 26 94 & 0 \\
\hline
\end{array}
\]

Fig.4 Data Set after classification

The classified data set is then used for Softmax model training. The implementation of Softmax classifier is to compress a k-dimensional vector $Z$ containing any real number into another k-dimensional real vector by learning and analyzing the samples so that the range of each element is between $(0,1)$, and the sum of all elements is 1, then the classification result can be obtained by the probability[10]. The classifier model is finally obtained through multiple feature extraction.
In the end, we can get the recognition rate of the model trained by the data set trained by the GANs network, and compare it with the artificial classification model. In this experiment, we also compare the recognition rate of the model after the classification of the GANs network under different data sizes. The results are shown in this figure.

The experimental results show that when using GANs network for data classification and post improvement work efficiency, the recognition rate is also slightly improved. The improvement of the
recognition rate is not positively related to the number of data generated for anti network classification. When there is too much classified data, the recognition rate will decline, but it still has a better recognition rate than manual data marking.

4. Conclusion and existing problems
This paper proposes a vehicle intrusion detection method based on GANs generation countermeasure network, which can effectively improve the efficiency of the deep learning model in vehicle intrusion detection and reduce resource consumption. The feasibility of this method is proved by experiments.

However, some problems still need to be optimized: even if the data are classified by GANs network, the recognition rate of the model is not ideal; it takes a long time to process the data directly using one-dimensional data, and the resource consumption is relatively large. These problems can be used as the direction of future research.

Acknowledgments
The work is supported by Sichuan Science and Technology Program, No.2019YFG0425, No.2019YFG0186, No.2019YFG0408 and the open Project of Network and Data security Key Laboratory of Sichuan Province (No. NDS2018-1).

References
[1] Sampo Kuutti,Saber Fallah,Richard Bowden,Phil Barber and Amir Khajepour 2019 Deep Learning for Autonomous Vehicle Control (Morgan & Claypool Publishers)
[2] Ibrahim Al-Shourbaji and Samaher Al-Janabi 2017 Intrusion Detection and Prevention Systems in Wireless Networks Kurdistan Journal of Applied Research 2(3)
[3] Elrawy Mohamed Faisal, Awad Ali Ismail and Hamed Hesham F. A. 2018 Intrusion detection systems for IoT-based smart environments: a survey J. Journal of Cloud Computing 7(1)
[4] YingXu L, ZengHui L, XiaoTian C 2017 Research on intrusion detection of industrial control system J. Journal of Communications 38(02) pp 143-156
[5] Bhattacharyya Siddhartha, Snasel Vaclav, Ella Hassanien Aboul, Saha Satadal and Tripathy B.K. 2020 Deep Learning: Research and Applications (De Gruyter)
[6] Qinghai W. 2019 Image retrieval method based on deep learning semantic feature extraction and regularization softmax Multimedia Tools and Applications (prepublish)
[7] ShaoQian W, XiMing L 2020 Survey on Research Progress of Generating Adversarial Networks J. Computer science and exploration 14(03) pp 377-388
[8] Hamed Alqahtani, Manolya Kavakli-Thorne and Gulshan Kumar 2019 Applications of Generative Adversarial Networks (GANs): An Updated Review Archives of Computational Methods in Engineering (prepublish)
[9] Peng R, Ling W, Xin L and Pengwei L 2018 Improved softmax classifier for deep convolution neural networks and its application in face recognition J. Journal of Shanghai University (Natural science edition) 24(03) pp 352-366