Research on CAN Bus Anomaly Detection Based on LSTM AndResNet

Jiaqi Song, Fei Li*, Ruxiang Li, Yalin Li, Qiyang Zhou, Jiayan Zhang

School of Cyberspace Security, Chengdu University of Information Technology, Chengdu 610225, China

*lifei@cuit.edu.cn

Abstract. With the rapid development of intelligent network vehicles, the safety of the vehicle network is taken seriously increasingly, the CAN as the most widely used car on-board network, its security problem has become one of the most important problems in intelligent made car development, the communication of CAN bus network characteristic and the existing safety problems and analyzes the common means of attack, on the basis of this puts forward the anomaly detection model based on LSTM And ResNet, through the experimental results show that this method CAN effectively detect deception attack.

Keywords: intelligent network vehicles; CAN, LSTM; ResNet; Anomaly detection

1. Introduction

With the rapid development of communication networks and industrial intelligence, the automobile industry has begun to change into an intelligent and networked one. With the increase of various intelligent devices in automobiles, the interaction with the external network is increasingly frequent. While bringing convenience to people, it also faces various security risks such as privacy leakage and vehicle attack[1]. In recent years, car networking security accidents have been constantly emerging: In 2016, China Qihoo 360 announced that it cracked BYD cloud service, remote driving, and other functions as well as Tesla remote control function[2]. In 2017, Tencent Cohen’s Lab successfully launched a remote attack on Tesla, realized the remote coordinated Control of multiple ECU (Electronic Control Unit) of Tesla, and finally invaded tesla's interior network to achieve any remote Control. In 2018, a thief in the UK managed to steal a Tesla Model S car by using the frequency of the owner's key intercepted by tablets and phones to unlock the door. To make matters worse, the thieves appear to have found a way to disable remote login, making it impossible for the...
owner or Tesla to track the whereabouts of the stolen vehicle. In 2018, security researchers Daan Keuper and Thijs Alkemade from Computest in the Netherlands tested Volkswagen Golf GTE and Audi A3 Sportback E-tron models and found that the flaw in their in-car infotainment (IVI) system could be exploited remotely via the Internet.

As the underlying communication system, CAN bus safety is directly related to the safety of the vehicle, so the protection for CAN bus has become many scholars of the research direction, CAN bus protection is mainly divided into based on encryption and authentication, based on the anomaly detection, and based on the security framework, because the CAN bus load ability is limited and bound by real-time communication, the method based on encryption and authentication and security framework based by certain restrictions, so the method based on anomaly detection is more widely applied to the safety protection of CAN bus[3].

Long Short-Term Memory (LSTM) is suitable for processing and predicting time series. Since CAN bus is a single channel, all messages on the bus are serialized, and LSTM is more suitable for predicting and processing such messages[4]. The residuals network (ResNet) is characterized by being easy to optimize and being able to increase accuracy by adding considerable depth[5]. The internal residual block use jump connection to alleviate the problem of gradient disappearance caused by increasing depth in the deep neural network. Therefore, this paper proposes an anomaly detection model based on LSTM AndResNet and proves that this model can detect replay attacks and spoofing attacks in a limited way through implementation.

2. Introduction to CAN Bus

Communication between ECUs mainly relies on CAN bus for transmission. ECU broadcasts data packets with a specified ID to the network, and ECU on the network CAN receive or respond to messages selectively according to the message ID. Using data frames for messaging between ECUs, CAN bus data message consists of the following parts: 1 bit frame start (SOF), 11 bit standard frame ID or 29 bit extension frame ID, 1 bit identifier extension IDE indicating whether its use extension format, 6 bit control field instructions with the length of the data bytes, following a CAN data frames can carry 0 to 8 bytes of data, data domain with 16 bit CRC check code after, 2 bit ACK response field and 7 bit "stealth" end of the frame (EOF)[6].

![Fig.1 Can bus data frame format](image-url)
2.1. Can bus communication characteristics
Broadcast transmission: According to the design of the physical layer and logical link layer of CAN bus, once CAN message is sent, it is broadcast to all nodes on the bus, and malicious components on the network CAN easily spy on all communications or data packets sent to any node on the network.

No authentication domain: CAN bus in the data message does not contain the authentication domain, or even any source identifier field, which means that any nodes in a network of CAN indiscriminately to send datagrams to any other node, which means the node is unable to determine the data came from a normal nodes or malicious nodes.

No encryption mechanism: The data on CAN bus provides no encryption mechanism and is almost transmitted in plaintext, so it is easy to be cracked by attackers.

Arbitration mechanism: CAN bus is CSMA/CA communication protocol, the physical and electrical characteristics of CAN bus to guarantee its bus arbitration logic link layer, with the identifier as arbitration domain, has the high priority the dominant position of "0" priority to send, so CAN bus message sent completely determined by the priority of identifier ID[7]. If a node keeps sending messages with high ID priority, other messages cannot be sent normally, affecting the normal operation of CAN bus.

2.2. Common attack mode of CAN bus
In view of various defects existing in CAN bus, attackers CAN gain access to the bus through various means, and the main attack means are as follows:

DoS attack: Since the message mediation mechanism of CAN bus determines its priority according to the size of the ID number when the attacker controls the malicious node to send messages with a smaller ID number or a higher priority, CAN bus cannot operate normally.

Discard attack: The attacker controls the gateway to delete or not forward some ECU data, resulting in the failure of the ECU.

Spoofing attack: Due to the lack of authentication mechanism on CAN bus, the source of data message cannot be determined. The attacker CAN send error messages to the ECU on the bus to respond and consume the ECU processor resources.

Replay attack: When an attacker exploits the broadcast characteristics of CAN bus to eavesdrop on messages, it is easy to implement a replay attack, because a replay attack does not require too much prior knowledge and only needs to ensure that there is no data transmission on CAN bus during replay attack.

Among them, the detection of Dos attack, discard attack, and replay attack has been studied in depth by researchers, so this paper focuses on the study of deceptive attack behavior.

3. LSTM
LSTM network is a branch of RNN. Due to its unique design structure, it is suitable for the prediction and processing of serialized data, while all messages on CAN bus are serialized, which actually shows time series data[8]. Better results CAN be obtained by using LSTM for processing.

3.1. The working principle of LSTM
The unit structure at time $t$ in LSTM is shown in the figure below. Where, the input at time $t$ is $x_t$, and $h_{t-1}$ is the hidden layer output at time $t-1$, $c_{t-1}$ is the output of historical information at time $t-1$, $f_t$, $i_t$, and $o_t$ are respectively the forgetting gate, input gate and output gate at time $t$, $\tilde{c}_t$ is the new information after the tanh transformation at time $t$, $c_t$ is the historical information updated at time $t$, $h_t$ is the output of the hidden layer at time $t$.

![Fig. 2 Internal structure of LSTM unit](image)

The calculation formula of each parameter in Figure 2 is as follows:

$$f_t = \sigma(W_f [h_{t-1}, x_t] + b_f)$$

$$i_t = \sigma(W_i [h_{t-1}, x_t] + b_i)$$

$$o_t = \sigma(W_o [h_{t-1}, x_t] + b_o)$$

$$\tilde{c}_t = \tanh(W_c [h_{t-1}, x_t] + b_c)$$

$$c_t = f_t * c_{t-1} + i_t * \tilde{c}_t$$

$$h_t = o_t * \tanh(c_t)$$
Among them: $\sigma$ stands for the sigmoid function, $W_i, W_f, W_c, W_o$ respectively represent the weight matrix of input gate, forgetting gate, tanH function and output gate, $X_t$ is the input vector at time $t$, $b_i, b_f, b_c, b_o$ Represents the bias values for the input gate, forgetting gate, tanH function, and output gate.

4. ResNet

ResNet is a deep convolutional network proposed by He Mingkai et al. for image recognition and classification in 2015[9]. The biggest difference of ResNet is the introduction of residual mechanism, that is, every 2-3 layers is regarded as a unit, and the output of the unit is the sum of the forward output of the internal convolutional layer and the output of the unit:

$$y = f(x, W_l) + x$$ (7)

Where $x$ and $y$ are input and output, $W_l$ is the parameter of layer $l$. The residual learning module of ResNet is shown in Figure 3. The specific method is as follows: $x$ is input data, the expected output is $H(x)$, if you pass the input $x$ directly to the output as the initial result, Now, the target that we need to learn is $F(x) = H(x) - x$. In the traditional convolutional layer or full connection layer, there are more or less problems such as information loss and loss in information transmission. ResNet solves this problem to a certain extent. It protects the integrity of the information by directly passing the input information to the output. The whole network only needs to learn the part of the difference between the output and the input, which simplifies the learning goal and difficulty.

![ResNet Diagram](image)

**Fig.3** The residual learning module of ResNet

5. CAN bus anomaly detection model based on LSTM And ResNet

LSTM and ResNet's handling of the data is slightly different: the convolution ResNet network can be seen as an application on time sequence and sliding filter, filter the results or a time series, the dimension and the dimension of the filter used is the same, but after this process will produce more has the characteristics of distinctiveness, it is crucial to the accuracy of experimental results. LSTM can learn and remember the input data sequence, and it can judge whether the current information is
normal or not based on the historical information. Such a correlation between data is very effective for the classification of time series data. Therefore, this paper integrates LSTM and ResNet to build a new data processing model. First, the data is entered into ResNet, then into the LSTM, and then the data is normalized and processed through PRelu and a Dropout layer. This is followed by a Softmax layer for classification, with the complete model structure shown in Fig.4.

![Fig. 4 LSTM and ResNet combination model](image)

6. Simulation experiment and result analysis

6.1. Data set introduction
This paper uses the Seo.EunbiA CAN bus data set disclosed by et al. In 2018 includes spoofing transmission devices and cheating tachometer[10]. Data set records can bus data from the real vehicle through OBD port during message injection. The data set contains every 300 messages injected intrusions, and each intrusion is executed for 3-5 seconds. Each data set has 30-40 minutes of can traffic. The specific data are shown in Tab.1.

| Attack Type               | # of messages | # of normal messages | # of injected messages |
|---------------------------|---------------|----------------------|------------------------|
| Spoofing the drive gear   | 4,443,142     | 3,845,890            | 597,252                |
| Spoofing the RPM gauze    | 4,621,702     | 3,966,805            | 654,897                |

Tab.1 Architecture of CNN model

6.2. The simulation results
In this paper, the TensorFlow open source framework is adopted to divide the data set into a training set and test set, and the validity of the CAN bus anomaly detection model fused by LSTM and ResNet is constructed and verified. In order to better evaluate the performance of the model, indicators such as accuracy rate, recall rate, precision rate, and F1-score were introduced for evaluation[11]. The results were compared with CNN, LSTM, and ResNet50.

\[
ACC = \frac{TP + TN}{TP + TN + FN + FP}
\]

(8)

\[
P = \frac{TP}{TP + FP}
\]

(9)
\[ R = \frac{TP}{TP + FN} \]  
\[ F_1 = \frac{2TP}{2TP + FN + FP} \]

\( TP \) means that the correct sample is predicted to be the correct number, \( TN \) stands for the number of false samples predicted to be false, \( FP \) is predicting the wrong sample to the right number, \( FN \) is the number of correct samples predicted to be wrong. The specific experimental results are shown in Fig.5 and Tab.2.

![Accurate figure](image)

**Fig.5** Accuracy of each model

| Detection model    | F1-Score | Recall rate | Accurate rate |
|--------------------|----------|-------------|---------------|
| LSTM-ResNet        | 0.9135   | 0.9032      | 0.9105        |
| ResNet50           | 0.9021   | 0.8921      | 0.8798        |
| LSTM               | 0.8219   | 0.8136      | 0.8205        |
| CNN                | 0.8894   | 0.8657      | 0.8742        |

**Tab. 2** Evaluation parameters of each model

From the experimental results, the performance of the CAN bus anomaly detection model proposed in this paper has been significantly improved after 30 rounds of iteration, and the high F1-Score also indicates that the fused model is more effective than other models.

7. Conclusion
This paper proposes a CAN bus anomaly detection model based on deep learning. This model uses LSTM and ResNet, neural network models to fuse, so as to learn the characteristics of CAN bus data more comprehensively and efficiently and judge whether the data is abnormal more accurately and effectively. Experiments show that this model has a good detection effect on spoofing attacks on CAN bus.

There are still some shortcomings in this paper. The detection results still have room for further improvement, and the detection efficiency still needs to be improved. It should also be considered whether multiple attacks can be detected simultaneously and whether the detection of various attacks is efficient and accurate.

Acknowledgments

This work was supported by Natural Science Foundation of Sichuan Province under grant No.2019YFG0201, No.2018GZDZX0011, and Chengdu Science and Technology Project No.2018-YF05-00707-SN.

References

[1] Ming S, Lingshan C 2019 A CAN bus anomaly detection method based on time series J. Journal of Shanghai university of engineering and technology 33(03) pp237-242
[2] He Y Research on information security of Networked Automobiles and CAN Bus Anomaly Detection Technology (2016 the academic degree's dissertation of Jilin University)
[3] An Tong Le, Wang Chundong and Yang Cheng 2020 Study on abnormal detection of vehicle-mounted CAN bus based on LSTM network J. Journal of tianjin university of technology 36(03) pp6-10
[4] Hongsong C, Jingjiu C 2020 Research on construction and Optimization of Intrusion detection Classification Model of Internet of Things based on ResNet and Two-way LSTM fusion J. Journal of human university (natural science edition) 47(08) pp1-8
[5] Yue T, Futai Z 2019 Botnet detection method based on ResNet and BiLSTM J. Communications technology 52(12) pp2975-2981
[6] Chen D Research and Implementation of Vehicle CAN Bus Intrusion Detection System (2019 the academic degree's dissertation of Beijing Jiaotong University)
[7] Jing P Research on information security and detection technology of networked automobile CAN bus (2019 the academic degree's dissertation of Tianjin University of Technology)
[8] Yadong G Research on in-car CAN Bus Intrusion Detection Algorithm (2019 the academic degree's dissertation of Harbin Institute of Technology)
[9] Bo X Research on intrusion Detection Model based on ResNet (2019 the academic degree's dissertation of Lanzhou University)
[10] Seo E, Song H M and Kim H K GIDS: GAN based Intrusion Detection System for In-Vehicle Network 2018 16th Annual Conference on Privacy, Security and Trust (PST) IEEE Computer Society
[11] Feifan Z 2020 Anomaly detection model based on ResNet Deep Neural network J. Internet new media technology 9(02) pp16-22