Study of In-Vehicle CAN Bus Network Security Based on Tamper Attack Detection Method

Shi-Yi Jin, Shi-Nan Wang, Yu-Jing Wu, Yi-Nan Xu*
Division of Electronic and Communication Engineering, College of Engineering, Yanbian University, Yanji 133002, China.

* Corresponding author. Tel.: +86-433-273-3955; email: ynxu@ybu.edu.cn
Manuscript submitted September 28, 2019; accepted December 11, 2019.
doi: 10.17706/ijcce.2020.9.2.97-104

Abstract: With the maturity of intelligent and networking technology of automobiles, automobiles enhance driving pleasure by connecting to the Internet, Bluetooth and mobile phones. At the same time, it brings security problems such as security vulnerabilities and attacks from hacker, which can seriously affect the driving safety and public safety. The in-vehicle network system is no longer an independent and a secure network system. Therefore, how to ensure the safety and reliability of the in-vehicle network is one of the most serious problems to be solved in the current intelligent automobile industry. This paper uses statistical analysis method to analyze the change range of CAN bus data. And proposes a CAN bus intrusion detection method to detect tampering attacks. Based on the actual vehicle bus information and the experimental verification of the CANoe simulation platform, an intrusion detection method which can effectively detect the tampering attack of the CAN bus is proposed.

Key words: CAN, network security, intrusion detection, statistical analysis, change range.

1. Introduction

ECUs in the vehicle need to transmit message through LIN, CAN, FlexRay and other buses. The in-vehicle CAN bus has been used in almost all automobiles on the market, because of its high reliability, fast transmission speed and low cost [1]. In 2015, Miller C and others showed the world the process of remote intrusion into in-vehicle bus network and seize the right of vehicle control [2]. Since then, the research on network security of in-vehicle bus has become the focus of many automobile manufacturers and research institutions.

For a long time, the in-vehicle bus network protocol has not considered the problem of network security. When the automobile electronic control systems are connected to the smartphone, OBD II network tester and wireless network system used in the automobile repair shop, it is easy for hackers to find a way to intrude in-vehicle bus to control cars [3]. Therefore, how to actively defend the attacks in the data layer and physical layer of the communication protocol is the serious problem that must be solved in the development of Intelligent Vehicle.

At present, the authenticity of in-vehicle CAN bus message is mainly improved by encryption and authentication technology, and the reliability of in-vehichle CAN bus is mainly improved by intrusion detection system and security framework [4], [5]. Literature [6] proposed a lightweight intrusion detection system for automotive ECUs based on Bloom Filter. The algorithm is efficient in detecting threats, but because of its own characteristics, it cannot avoid the problem of false alarm. Literature [7] proposed an

intrusion detection system based on information entropy. However, this method has a long detection period and low real-time performance. It is not suitable for some automotive electronic control systems, which are related to safety. Literature [8] proposed an anomaly detection system based on the periodicity of message. The system can detect blocking and discarding behavior of periodic messages, but it cannot detect tampering attacks. Artificial intelligence algorithm based on learning model is also widely used in intrusion detection of in-vehicle CAN bus. Learning model can accurately identify abnormal messages, but most of the attack data used by hackers are normal data, which is stolen from the bus. Simply detecting the abnormal data of a single message cannot completely guarantee the security of the bus [9].

Hackers must send real and meaningful CAN bus messages to control vehicles. Therefore, messages injected into the in-vehicle CAN bus must compliance with the requirements of CAN bus communication protocol. If the relationship between message contexts cannot be established correctly, intrusion behavior is still difficult to detect. Therefore, we propose an intrusion detection method for CAN bus based on analyze the change range of the CAN message, which considering the relationship between message contexts.

The structure of this paper is as follows. Chapter 2 of this paper analyses the threat of CAN bus. Chapter 3 designs the method of information intrusion detection based on CAN bus. Chapter 4 includes the simulation and result analysis. Chapter 5 summarizes the whole paper.

2. The Threat Analysis of CAN Bus

2.1. Potential Threats

At present, hackers can penetrate the in-vehicle CAN bus through OBD-II, car entertainment systems, Bluetooth, WiFi, keyless access, RFID and tire pressure management system and other auxiliary systems. Hackers attack ECUs mainly through the following ways after intruding into in-vehicle network:

(1) Spoofing: In the in-vehicle CAN bus, hackers maliciously disguise themselves as legitimate ECUs to gain the right to transmit messages on the CAN bus.

(2) Tampering: Hackers shield messages sent by real nodes and send malicious messages to buses to achieve their goals.

(3) Information leakage: CAN bus messages are sent by broadcasting mechanism in the CAN bus. Hackers can easily obtain useful information from unencrypted CAN messages after obtaining the bus monitoring rights.

(4) Denial of service: CAN bus uses arbitration mechanism to send messages. When two or more messages request to send at the same time, messages with high priority will be sent first.

The algorithm and decision model of vehicle network security need to embed in the vehicle ECUs. Considering the limitation of computing resources in automobile ECUs, it is difficult to apply complex algorithms in automobile. For spoofing attacks, document [10] proposed detection methods based on software and hardware levels. For information leakage, document [11] proposes the encryption and authentication method to ensure that information cannot be easily decoded by hackers, which ensures the authenticity of the messages. For denial of service attacks, traffic detection and frame ID detection can be performed. However, there is no research on tampering attacks. This paper proposed a low complexity, low cost and high efficiency coping strategy, which cannot only ensure the real-time detection, but also further enhance the security of the existing intrusion detection system.

2.2. Attack Model

Attack process of in-vehicle CAN bus:

(1) Hackers can eavesdrop on messages in in-vehicle CAN bus by utilizing the broadcast characteristics of

CAN bus.

(2) Then use the reverse analysis method to get useful information from the eavesdropping messages, such as they can know which message represents the engine speed.

(3) Hackers can obtain the right to transmit messages in in-vehicle CAN bus by disguising it as a legitimate ECUs by some means.

(4) As shown in the Fig. 1, hackers can block or disconnect ECU_B, and use ECU_Hacker to transmit attack messages to ECU_A to implement the attack on ECU_A.

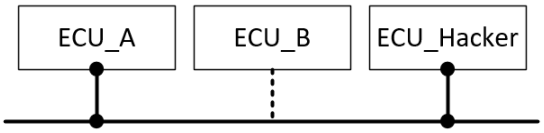

Fig. 1. Attack process of CAN bus.

3. Intrusion Detection Method for CAN Bus

3.1. Statistical Analysis

The data field of in-vehicle CAN bus message can store 8 bytes and allocate memory space according to the amount of information carried by the signal. As shown in Fig. 2, sometimes one byte in the data field of CAN message can contain a variety of vehicle control signals, but sometimes one or even two bytes in the data field of in-vehicle CAN messages represent only one signal.

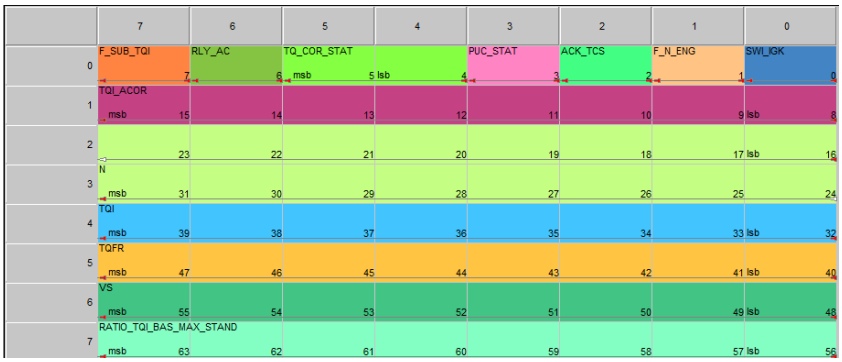

Fig. 2. Layout of data field.

In this paper, aiming at the message tampering problem of in-vehicle CAN bus, a new fault detection method of in-vehicle CAN bus is proposed. Through statistical analysis, we set the threshold of numerical change range according to the normal change range of numerical value. In the process of determining the change range of threshold, we exclude some extreme cases, which can greatly reduce the false alarm rate of system. Finally, we proposed an anomaly detection method for message tampering attack. The scheme uses the simplest subtraction operation to detect message anomalies caused by tampering attacks. The proposed scheme not only does not greatly increase computational burden of ECUs, but also improves the deficiencies of existing intrusion detection systems against tampering attacks.

The CAN bus data are collected by OBD-II during the normal driving process of the vehicle on the road. The maximum speed during driving is 70 km/h. In the data field with ID of 0x316, it is found that the threshold of byte_6 is the easiest to set. The change range of byte_6 in data field with ID of 0x316 is shown in Table 1.

Table 1. Change Range of Byte_6 with ID of 0x316

Change range	Frequency	Change range	Frequency
0	11866	37	1
1	408	66	2
17	2	67	1
36	3	68	1

As shown in Table 1, the change range of numerical value is basically stable between 0 and 1. However, there have been several abrupt changes, which are much larger than 1. Therefore, it is unreliable to set threshold only by the change range of numerical value. Further analysis was conducted to locate all the abrupt changes of numerica value, we can find that some extreme changes occur regularly. As shown in Fig. 3, when the byte_6 abrupt change, it always abrupt to the value of 01, and returns to its pre-abruption value after a maximum of 2 message cycles. After the above rules are obtained, the threshold of anomaly detection is set to 1. When the change range exceeds the threshold, it is further determined whether it is similar to the normal behavior.

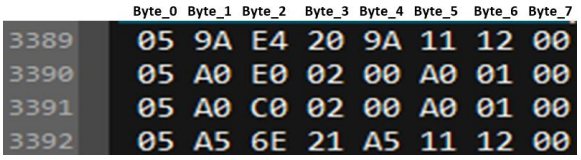

Fig. 3. Abrupt message on the CAN bus.

3.2. Intrusion Detection Process

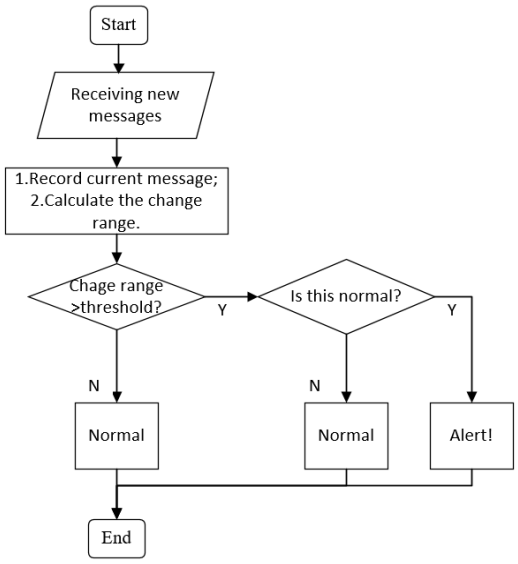

Fig. 4. Flow chart of intrusion detection system.

Fig. 4 is a flow chart of the proposed anomaly detection scheme, which consists of five steps:

Step1: Record the normal numerical values and set the threshold of the change range under normal conditions.

Step2: When the receiving node receives the message with the corresponding ID, it records the numerical value of the message and calculates the change range between the message and the previous received message.

Step3: Judging whether the change range of numerical value exceeds the threshold.

Step4: If the abrupt change of numerical value is found, make further judgment and exclude some normal abruption.

Step5: If a abnormal condition is found, issue a warning.

4. Experimental Simulation

For the proposed intrusion detection scheme in this paper, the CANoe experimental platform developed by Vector Company is used to simulate and verify it. As shown in Fig. 5, TxEMS1 and RxEMS1 are the sending and receiving nodes of messages, respectively. ReplayBlock is a module of replaying bus messages recorded in the CANoe software. In this experiment, ReplayBlock is responsible for sending messages received from the real vehicle ECU to the bus. We can simulate hacker intrusion bus by rewriting the .ASC file. The intrusion detection method proposed in this paper is programmed by CAPL language, which is similar to C and C++. It can program for CAN bus events, which can greatly improves the efficiency of programming.

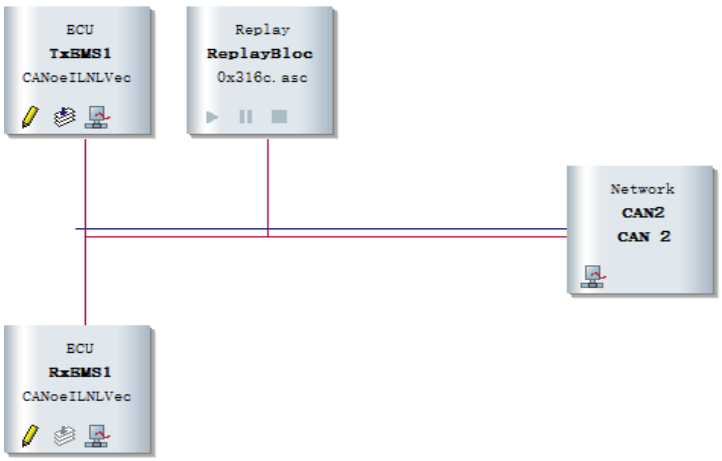

Fig. 5. Network topology in CANoe.

Simulate the specific implementation process of hacker's tampering attack on CAN bus by using ReplayBlock module:

Fig. 6 is the normal 500th~504th message. We can inserting the normal 500th~504th message into the 1000th~1004th message, simulating hacker stealing message and tampering messages. Fig. 7 shows the normal 1000th~1004th message. As shown in Fig. 8, the 1000th~1004th message are changed after hacker implement tampering attack. Repeat this process to insert 5 attack messages at 2000th, 3000th, 5678th and 7000th messages respectively.

```
500  4.99901 1 316 Rx  d 8 05  5F  1E  1D  5F  10  0C  00
501  5.00901 1 316 Rx  d 8 05  5F  26  1D  5F  10  0C  00
502  5.01901 1 316 Rx  d 8 05  5F  34  1D  5F  10  0C  00
503  5.02901 1 316 Rx  d 8 05  5F  42  1D  5F  10  0C  00
504  5.03901 1 316 Rx  d 8 05  5E  60  1D  5E  10  0C  00
```

Fig. 6. The normal 500th~504th message.

```
1000  9.99901  1 316 Rx  d 8 05  08  64  11  08  0E  13  00
1001 10.00901  1 316 Rx  d 8 05  08  5E  11  08  0E  13  00
1002 10.01901  1 316 Rx  d 8 05  08  5E  11  08  0E  13  00
1003 10.02901  1 316 Rx  d 8 05  08  62  11  08  0E  13  00
1004 10.03901  1 316 Rx  d 8 05  08  6E  11  08  0E  13  00
```

Fig. 7. The normal 1000th~1004th message.

```
 999   9.98901  1 316 Rx  d 8 05  08  6A  11  08  0E  13  00
1000   9.99901  1 316 Rx  d 8 05  5F  1E  1D  5F  10  0C  00
1001  10.00901  1 316 Rx  d 8 05  5F  26  1D  5F  10  0C  00
1002  10.01901  1 316 Rx  d 8 05  5F  34  1D  5F  10  0C  00
1003  10.02901  1 316 Rx  d 8 05  5F  42  1D  5F  10  0C  00
1004  10.03901  1 316 Rx  d 8 05  5E  60  1D  5E  10  0C  00
1005  10.04901  1 316 Rx  d 8 05  08  64  11  08  0E  13  00
```

Fig. 8. The 1000th~1004th message after hacker implement tampering attack.

Fig. 9 is a real-time record of CAN bus messages in the Trace window of CANoe. The titles from left to right are: time, CAN channel of data transmission, frame ID, message name, event type, transmission flag, data length and content of data segment. Write window shows the feedback information from CAPL language. In this experiment, the feedback information is the alarm of ECU to bus abnormal behavior. The simulation results show that the intrusion detection scheme can accurately detect the bus data anomalies, and there are no missing or false alarms.

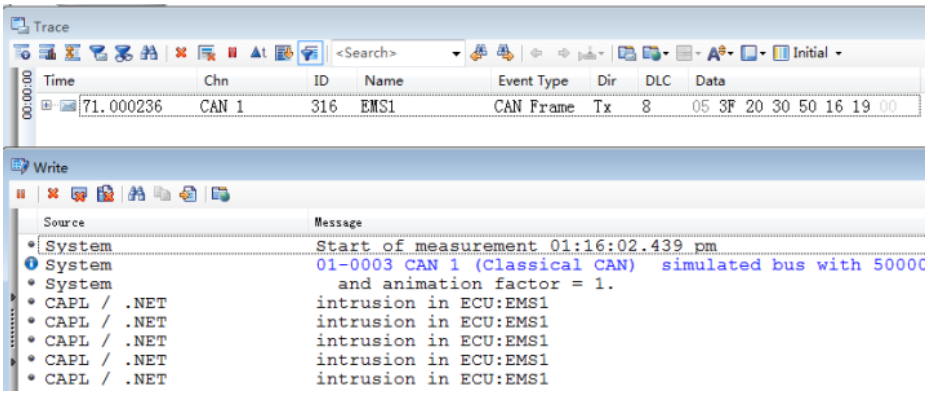

Fig. 9. Simulation result in CANoe platform.

5. Conclusion

In this paper, aiming at the network security problem of in-vehicle CAN bus, we propose an innovative in-vehicle network intrusion detection scheme. By analyzing the normal range of data change and setting the threshold of the change range to judge whether the in-vehicle CAN message is abnormal, the simulation results show that the scheme can effectively detect tampering attacks. The intrusion detection scheme has low complexity, fast response, and does not need any additional hardware support, which can be used together with other intrusion detection scheme. Therefore, this scheme can solve the shortcomings of the proposed intrusion detection system for in-vehicle CAN bus against tampering attacks.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Shi-Yi Jin: Methodology and writing of original draft; Shi-Nan Wang: Software and formal analysis; Yu-Jing Wu: Validation and review & editing of original draft: Yi-Nan Xu: Conceptualization and supervision.

Acknowledgment

This research was supported by National Natural Science Foundation of China Grant Number 61763047.

References

[1] Kang, S., Seong, J., & Lee, M. (2018). Controller area network with flexible data rate transmitter design with low electromagnetic emission. *IEEE Transactions on Vehicular Technology*.

[2] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat*, 84-86.

[3] Woo, S., Jo, H. J., & Lee, D. H. (2014). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems, 16(2)*, 1-14.

[4] Wang, J., Li, J. Q., Wang, H. H., Zhang, L. Y., Lee, C. M., & Lin, Q. Z. (2018). Dynamic scalable elliptic curve cryptographic scheme and its application to in-vehicle security. *IEEE Internet of Things Journal*.

[5] Jarrah, O. A., Maple, C., & Dianati, M. (2019). Intrusion detection systems for intra-vehicle networks: A review. *IEEE Access*.

[6] Groza, B., & Murvay, P. (2018). Efficient intrusion detection with bloom filtering in controller area networks (CAN). *IEEE Transactions on Information Forensics and Security*, 1037-1051.

[7] Wu, W. F., Li, R. F., Xie, G. Q., An, J. Y., Bai, Y., Zhou, J., & Li, K. Q. (2019). A survey of intrusion detection for in-vehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, 1-15.

[8] Song, H. M., Kim, H. R., & Kim, H. K. (2016). Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. *Proceedings of the 2016 International Conference on Information Networking*. Kota Kinabalu, Malaysia.

[9] Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *IEEE Access, 6(1)*, 3491-3508.

[10] Choi, W., Jo, H. J., Woo, S., Chun, J. Y., Park, J. Y., & Lee, D. H. (2018). Identifying ECUs using inimitable characteristics of signals in controller area networks. *IEEE Transactions on Vehicular Technology*, 4757-4770.

[11] Halabi, J., & Artail, H. (2018). A lightweight synchronous cryptographic hash chain solution to securing the vehicle CAN bus. *Proceedings of the 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET*). Beirut, Lebanon.

Shi-Yi Jin was born at Jilin Province of China. He received the bachelor degree in electronic information engineering from Yanbian University, China, in 2018.

He is a currently working toward a master degree in the area of in-vehicle network, which include the design of security architecture of FlexRay.

Shi-Nan Wang was born at Jilin Province of China. She received the bachelor degree in communication engineering from Yanbian University, China, in 2019.

She is a currently working toward a master degree in the area of in-vehicle network, which include the design of security architecture of FlexRay.

Yu-Jing Wu was born at Jilin Province of China. She received her M.S. and Ph.D in electronic and information engineering from Chonbuk National University, South Korea, in 2013 and 2016, respectively.

She is a lecturer of the Division of Electronic and Communication Engineering of Yanbian University, China. Her research interests are in the area of VLSI implementation for digital signal processing and communication system, which include the design and in implementation of security protocol for in-vehicle networks.

Yi-Nan Xu was born at Jilin Province of China. He received the Ph.D. degree in electronics engineering from the Chonbuk National University, Korea, in 2009.

He is a professor of the Division of Electronics and Communication Engineering of Yanbian University, Yanji, China. His research interests include the In-vehicle network and automobile electronic control.