proceedings

MDPI

Type of the Paper (Proceedings, Abstract, Extended Abstract, Editorial, etc.)

Intelligent Networked Vehicle CAN Bus Network Real-time monitoring and active defense system†

Jie Fang [1], Jin-Ze Li [2] , Yi-Nan XU [3] and Yu-Jing Wu [2,*]

[1] College of Engineering of Yanbian University; 645890656@qq.com
[2] College of Engineering of Yanbian University; 1255371992@qq.com
[3] College of Engineering of Yanbian University; ynxu@ybu.edu.cn
[4] College of Engineering of Yanbian University; yjwu@ybu.edu.cn
* Correspondence: yjwu@ybu.edu.cn; Tel.: +8615699580664
† Presented at the title, place, and date.

Abstract: With the maturity of automotive intelligent network technology, the number of ECUs loaded on vehicles by different car manufacturers is increasing year by year.For the real-time detection and defense mechanism of CAN bus, we propose the data-based anomaly detection algorithm to identify the anomaly information and attack types. A real-time intrusion detection model is established according to different attack types to propose a suitable error correction method for CAN bus to achieve the purpose of active defense. The network environment of real vehicle CAN bus is simulated in CANoe software. According to the attack model, data abnormalities are found in real time to eliminate unnecessary hidden dangers and meet the requirements of real-time defense while the vehicle is running. The experimental results show that the detection of the attack type achieves a 100% success rate among the 10,000 messages tested and can be effectively defended, and the time to perform one detection and defense is much less than the time to send and receive messages from the CAN bus (10ms). Therefore, it meets the requirements of CAN bus for real-time etc.

Keywords:In-vehicle Networks, Networked Vehicles, Controller Area Networks (CAN), Detection and real-time defense, Internal Penetration

Citation: Lastname, F.; Lastname, F.; Lastname, F. Title. *Proceedings* **2021**, *68*, x. https://doi.org/10.3390/xxxxx

Published: date

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

With the rapid development of intelligent network-connected vehicles and driverless technology, the vehicle control is becoming more and more intelligent and network-connected. Intelligent network-connected vehicles have become a strategic direction for the development of the automotive industry, and the in-vehicle bus network is a key assembly to determine the active safety performance of intelligent vehicles.For a long time, the in-vehicle bus network protocol has not considered the problem of network security [1]. 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 vehicles [2]. Therefore, the research on network security of in-vehicle bus has become the focus of many automobile manufacturers and research institutions [3].

The current stage of smart vehicle security is divided into two aspects, intrusion detection and active defense. The literature [4] proposed a method to analyze the intrusion detection of in-vehicle networks based on CAN message intervals. This method has high real-time performance, but it cannot detect tampering with the data content and does not have the ability to detect non-periodic signals. The literature [5] proposes a method for detecting anomalous data based on the application of an information entropy approach. This method requires interception of data for a period of time for judgment and has poor real time performance.S. Woo et al. proposed a 32-bit

MAC security protocol to verify the data. This method is easy to manage the keys but causes severe delays between nodes with similar keys due to periodic updating of session key patterns [6].

At present, the attack detection and defense technology is mainly established in the offline intrusion detection method and post-event defense system, which is difficult to meet the real-time and security in the vehicle driving. Therefore, we propose a combination of intrusion detection and defense for the requirements of real-time and reliability of in-vehicle bus. Appropriate and feasible detection and defense schemes are given for different attack types of intrusion. According to the detected abnormal information, the defense mechanism will be prompted, and in the error correction module, it will help users to find the data abnormalities in real time, recover the wrong data and eliminate unnecessary hidden dangers.

The structure of this paper is as follows. The second chapter of this paper introduces the types of CAN bus attacks and the detection and error correction methods. The third chapter designs the real-time monitoring and active defense system. Chapter 4 contains the experimental simulation and result analysis. Chapter 5 summarizes the whole paper.

2. Real-time monitoring and active defence system

Based on [7][8]][9] internal penetration methods, we have analyzed the full range of in-vehicle bus network intrusions. A range of intrusions are categorized from vulnerabilities in the on-board bus itself to a range of possible intrusion means triggered when external devices are connected. For the categorized attack types, we propose a data anomaly detection algorithm based on identifying anomalous information and attack types.

Currently, anyone can access the inside of the CAN bus through vehicle peripheral devices such as OBD-II, Bluetooth, and cloud-based networks to get ECU data or even falsify data for the purpose of hacking into the vehicle bus. In response to the problem of security attributes lacked by CAN bus, the following types of attacks are the main threats.

1. Inject: hackers can send malicious messages to achieve intrusion and lack data confidentiality.
2. Steal: an attacker can access the bus network at will, easily listen to the communication bus and obtain any messages transmitted between the various nodes, lacking data authenticity.
3. Flood: the CAN bus takes to sending high rate spoof messages to occupy the line causing paralysis and lack of data availability.
4. Modify: eavesdropping on a bus message and modifying part of the data content and sending it to the receiver, lacking data integrity.
5. Replay: The attacker listens to the CAN bus and captures some critical messages, later replaying them at the time the attacker needs them, lacking the ability to ensure message freshness.

The types of attacks, anomaly detection methods and defense mechanisms are described below. The overall module diagram is shown in Figure 1.

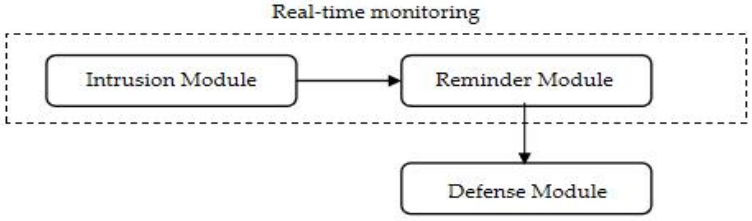

Figure 1. Overall Module Diagram

2.1. Intrusion identification and prompting module

Attacks against the CAN bus can be categorized into the following three main categories: Snooping Data, Inject Malicious Data, and Flood Data. intrusion detection is performed for the proposed types of attacks. Since the CAN bus data field is fixed, the maximum payload is 8 bytes. Firstly, we will use CAN bus data segment compression algorithm to compress the data [10]. Secondly, message authentication code is generated using HMAC authentication algorithm and after compression 2 bytes of message authentication code is loaded in the redundant data field. Since the TX at the sender side and RX at the receiver side authentication code authentication code is synchronized, the receiver side verifies the availability of this message based on the message authentication code. If the authentication is passed, this message is received and decompressed and restored to the original message to ensure normal communication of the bus; otherwise, the type of attack is judged according to the type of attack and the wrong data is corrected according to the error correction method.

The proposed authentication module uses HMAC algorithm. Each HMAC algorithm operation yields 16 bytes of authentication code and when all the authentication codes are used cumulatively to 16 bytes, then the HMAC algorithm is run again to get a new authentication code based on the next key and plaintext in the key matrix. The authentication code is obtained by running the key KEY and the plaintext PLAINTTEXT according to equation (1).

$$MAC = HMAC(KEY,PLAINTTEXT) \quad (1)$$

The rules for adding an identification code are as follows.

The compressed data CD (Compressed Data) is obtained by compression algorithm and 2 bytes of MAC is loaded in the redundant data field to get the send message according to equation (2).

$$\text{Send message} = CD \mid MAC, \quad (2)$$

The specific detection methods for different types of attacks are as follows.

1. Inject malicious data: The CAN bus transmission method is a broadcast mechanism, the hacker can send malicious messages to the CAN bus and the ECU of the corresponding ID can receive the messages sent by the hacker. Each ID will be assigned a message authentication code each time a message is sent, and the validity of the message can be detected by verifying the corresponding message authentication code. When the RX authentication at the receiver side is inconsistent, it is determined to be subject to Injection attacks.
2. Snooping data: According to ICANDR compression algorithm, the length of compressed data segment is between 1~5 bytes. Combined with AES 256 encryption algorithm, the compressed data field is encrypted to ensure the security of the message. When part of the RX authentication code disappears at the receiver, it is judged to be under Snooping attack.
3. Flood data: When a Flood attack is encountered, the availability of the message can be confirmed based on the message authentication code. When the RX authentication code is repeated N times at the receiving end, it is determined to be under Flood attack.

2.2. Error correction and fault tolerance module

For the vehicle driving can not do the combination of offense and defense in real time. When the intrusion detection is completed, a hint is given to the defense system and according to the hint the defense system corrects the wrong information. In this paper, the error correction method proposed in this paper is based entirely on the type of attack implemented for real time defense. The proposed defenses are listed below.

The CAN bus sends messages in 10ms, so the rate of change of the before and after data is almost zero. Therefore, we propose the first N messages correlation method for error correction, which combines the correlation between the horizontal and vertical variables of the data, determines the valid values of the predicted data, and controls the error correction tolerance for abnormal data according to the hints. For injection and snooping type attacks, we use the proposed method to segment according to the data frame signal cross-reference table, analyze the first N data values of each signal, determine the location of the anomaly, and perform error correction processing. In the case of flood type attacks, we first perform a deletion operation on N intrusion messages and then perform error correction processing.

The proposed flowchart for combining intrusion detection and error correction is as follows.

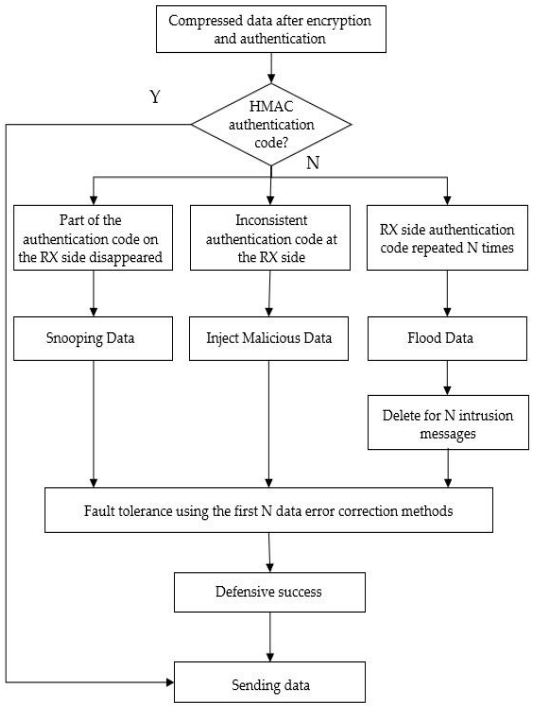

Figure 2. Intrusion detection and defense flow chart

3. Experimental simulation and analysis of results

Through the ReplayBlock module in the CANoe software, the measured vehicle driving data is transferred to the CAN bus network to simulate the internal CAN bus communication state of a real vehicle during normal driving.The overall CAN bus test environment consists of the MCU, CANcaseXL and CANoe software, as shown in Figure 3.

Through the test set, malicious messages are transmitted to do simulate the hacker's injection attack behavior. In which, Figure 4 shows the graph of the successful detection of anomalous information and the result of the attack type based on the data anomaly detection algorithm. In the output monitoring window, we can see the alert issued as an attack by injection type. Figure 5 shows the graph of the vehicle speed signal run obtained by the error correction module. From the graph we can see that the anomalous information in Fig. 4 is accurately eliminated, indicating that our proposed defense module has achieved successful defense. Regarding the detection and defense of the remaining attack types, we also experimented one by one and achieved successful results.

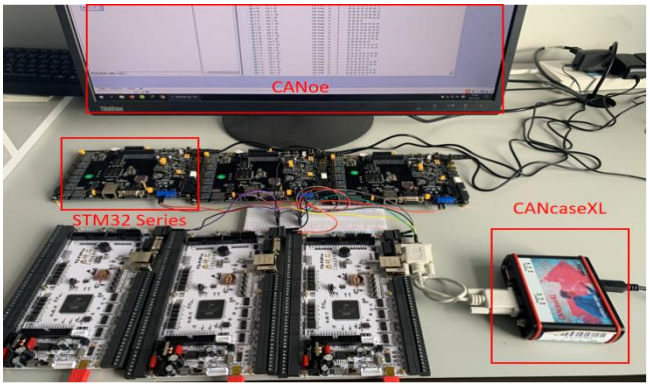

Figure 3. Real hardware test environment

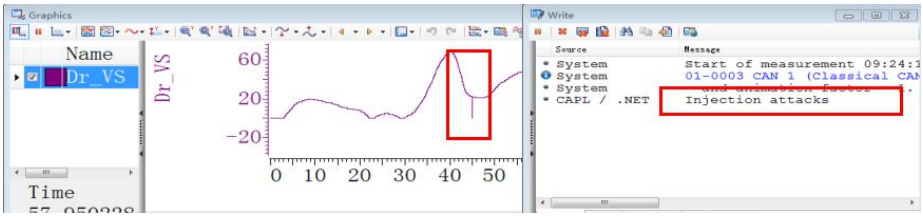

Figure 4. Injection attack and detection effect diagram

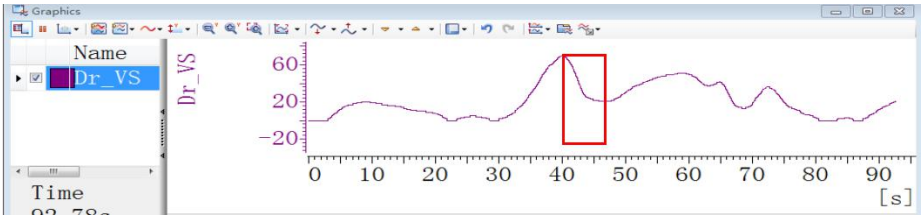

Figure 5. Run chart of speed signal after error correction

4. Conclusions

In this paper, we propose three types of attacks, Inject, Snooping and Flood, to address the issue of in-vehicle CAN bus security, and do the modules of intrusion detection, intrusion prompting and error correction and fault tolerance to achieve the effect of defense. According to the attack model, we propose the data anomaly detection algorithm to identify the anomaly information and attack type, and find the data anomaly in real time. According to the abnormal information detection result prompt, we propose the error correction method for abnormal information to eliminate unnecessary hidden dangers and meet the requirements of real-time defense in the vehicle driving.The joint experimental results of CANoe software and STM series show that the proposed algorithm tests 10,000 messages and can effectively detect different attack types and achieve a 100% detection rate; and can effectively defend against attacks. The time to perform one detection and defense is 1.15ms, which is much smaller than the time to send and receive messages from the CAN bus (10ms). Therefore, it meets the requirements of CAN bus for real time, etc., and greatly increases the effective protection of the vehicle.

References

1. S. Kang, J. Seong, M. Lee. Controller Area Network With Flexible Data Rate Transmitter Design With Low Electromagnetic Emission. IEEE Transactions on Vehicular Technology. 2018
2. S. Woo, H. J. Jo, D. H. Lee. A Practical Wireless Attack on the Connected car and Security Protocol for In-Vehicle CAN. IEEE Transactions on Intelligent Transportation Systems. 2014, 16(2): 1~14

3. Shi-Yi Jin,Shi-Nan Wang,Yu-Jing Wu,Yi-Nan Xu. Study of In-Vehicle CAN Bus Network Security Based on Tamper Attack Detection Method[J]. International Journal of Computer and Communication Engineering,2020,9(2).
4. Hyun Min Song, Ha Rang Kim, Huy Kang Kim. Intrusion Detection System Based on The Analysis of Time Intervals of CAN Messages for In-vehicle Network. International Conference on Information Networking. 2016: 63-68.
5. Muter M, Asaj N. Entropy-based anomaly detection for in-vehicle networks[J]. Intelligent Vehicles Symposium IEEE, 2011:1110-1115.
6. Woo S,Jo H J,Lee D H,A practical wireless attack on the connected car and security protocol for in-vechicle CAN[J].IEEE Transactions on Interlligent Transportation Systems,2015,16(2): 993-10006.
7. Siti-Farhana Lokman,Abu Talib Othman,Muhammad-Husaini Abu-Bakar. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review[J]. EURASIP Journal on Wireless Communications and Networking,2019,2019(1).
8. Narayanan S N, Mittal S, Joshi A. Using data analytics to detect anomalous states in vehicles[J]. arXiv preprint ar Xiv:1512.08048, 2015.
9. Z. Lu, G. Qu, Z. Liu. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Transactions on Intelligent Transportation Systems. 2019, 20(2):760~776
10. Yujing WU,Jin-Gyun CHUNG. An Improved Controller Area Network Data-Reduction Algorithm for In-Vehicle Networks[J]. The Institute of Electronics, Information and Communication Engineers,2017,E100.A(2):
11. J. Turjak, R. Grbić, D. Spasojević and M. Kovačević. Recovery from Error States During Communication based on CAN and FlexRay. 2018 Zooming Innovation in Consumer Technologies Conference (ZINC). 2018: 114-117.