A Method of Preventing Unauthorized Data Transmission in Controller Area Network

Tsutomu Matsumoto, Masato Hata, Masato Tanabe, Katsunari Yoshioka, Kazuomi Oishi
Yokohama National University
Faculty of Environment and Information Sciences
79-7 Tokiwadai, Hodogaya, Yokohama, Kanagawa 240-8501, JAPAN
tsutomu@ynu.ac.jp, {hata, masato}@mlab.jks.ynu.ac.jp, {yoshioka, oishi}@ynu.ac.jp

***Abstract*— There is a strong demand for the security of Controller Area Network (CAN), a major in-vehicle network. A number of methods to detect unauthorized data transmission, such as anomaly detection and misuse detection, have already been proposed. However, all of them have no capability of preventing unauthorized data transmission itself. In this paper, we propose a novel method that realizes the prevention as well as detection. Our method can be effectively implemented with minimal changes in the current architecture of Electronic Control Unit. The method works even in a CAN with multiple buses interconnected by gateways.**

Keywords- CAN; Car; ECU; Embedded System; Error Frame; Real-time Response; Security

I. Introduction

Modern automobiles contain a number of Electronic Control Units (ECUs) interconnected by in-vehicle networks (Fig. 1). Controller Area Network (CAN) [1, 2] is a major in-vehicle network. Introduction of CAN bring merits on both safety and cost but may create new threats. For example, Koscher et al. showed that an attacker who has access to in-vehicle network can provoke a number of dangerous operations such as applying a break at speed by tampering the ECU firmware [3]. In paper [4], they even demonstrated that there are a number of existing attack vectors to in-vehicle networks, exploiting vulnerabilities of a media player in in-car audio system, hands-free phone using Bluetooth, and telematics providing various services using cellular phone network. Hoppe et al. proposed message injection attacks which can disable Power Window, Airbag Control System, etc. and demonstrated them by simulation and on their testing environment [5]. Many other works also indicate vulnerabilities in in-vehicle networks. Thus it is a pressing issue to develop effective countermeasures against such threats.

One of the most significant issues is the vulnerability of CAN. The CAN protocol is designed for bus networks. Each CAN message (CAN Frame) has no source and no destination addresses. Therefore every message is broadcast on a bus. Once an attacker infiltrates an ECU, he can impersonate any other ECUs on the same bus, because any ECU (node) connected to a bus can send arbitrary message. However the CAN protocol supports no sender authentication and no message authentication. To solve the problem, we propose a method of preventing unauthorized data transmission by leveraging the CAN's broadcasting nature. In the proposed method, the ECU to be impersonated monitors and detects the impersonated message and overrides it by sending Error Frame before the message transmission completes. The proposed method can prevent unauthorized data transmission itself. In addition, it achieves sufficient real-time response when processed on hardware. If the proposed method is implemented in a gateway, then it is possible to prevent transmission of unauthorized messages from being transmitted across the different buses.

The paper is structured as follows. In section II we introduce related works. In section III we review CAN briefly. In section IV we explain the problems and threats with respect to CAN, and in section V we propose a method of preventing unauthorized data transmission. In section VI the evaluation is discussed and a conclusion is given in section VII.

II. Related Works

Vulnerabilities of in-vehicle networks have been indicated by many authors. However, so far only several countermeasures to improve the security of in-vehicle network appeared in the literature.

The previous protection methods are classified into two

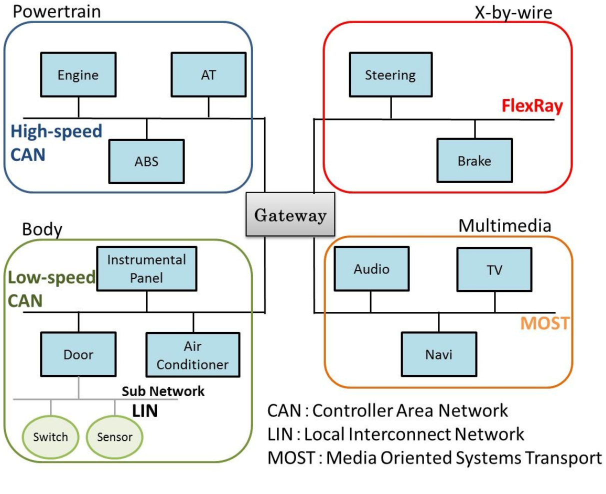

Figure 1. Example of in-vehicle network

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

types. One [6, 7] is the type using cryptographic techniques such as Encryption, Digital Signature, and Message Authentication Code (MAC). The other [5, 8, 9] is the type using Intrusion Detection System (IDS).

Wolf et al. proposed secure communication protocol [6] by using Symmetric Key Encryption and Public Key Encryption. Nilsson et al. proposed "Delayed Data Authentication" [7] to authenticate message by replacing CRC field with MAC field.

On the other hand, Hoppe et al. proposed three ideas for IDS [5]. Muter et al. defined nine anomaly detection sensors and discussed introducing sensors to in-vehicle network [8]. Hoppe et al. proposed IDS and demonstrated anomaly detection method by looking at frequency of message transmitted on the bus on simulation [9].

III. CAN (CONTROLLER AREA NETWORK)

The CAN, developed by BOSCH for vehicle, has standardized as ISO11898 and ISO11519. CAN uses voltage differences between two wires of a twisted pair cable. Because of its high noise immunity, CAN is utilized in vehicle, airplane, and industrial machinery as a serial communication protocol. Every ECU transmits data as a signal by setting the voltage difference and receives data by detecting a voltage difference at the same time. By the broadcasting nature of a bus, every transmitted data can be received by all ECUs on the bus.

Besides CAN, in-vehicle networks may adopt LIN, MOST, and FlexRay. These are the backbone of in-vehicle network (Fig.1). With respect to transfer rate, CAN has two versions: High-speed CAN and Low-speed CAN. The former controls driving related operations and the latter controls body related ones.

A. *The CAN Protocol*

Data is transmitted by binary model; dominant and recessive signals. These correspond to a logical 0 and a logical 1, respectively. Dominant is the state that the voltage difference between two wires is large. On the contrary, recessive is the state that the voltage difference between two wires is small. When two or more ECUs output recessive and dominant at the same time, the dominant state overwrites the recessive state.

B. *Data Frame and Arbitration*

CAN communication is performed in frame. In particular, data transmission between ECUs is performed in Data Frame which consists of ID Field, Data Field, CRC Field and more (see Fig.2). The data is put into Data Field, and 0-8bytes data can be transmitted by one Data Frame. The 11-bit ID Field represents the ID of each message, and ID priority of the message. CAN implements the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism. The message with smaller ID has higher priority. When two or more ECUs start transmitting messages at the same time, arbitration is done and the message with the highest priority ID survives. The detailed mechanism of arbitration is as follows. When an ECU starts transmitting of a Data Frame, SOF is transmitted, then first bit of ID field starts being transmitted. When two or more ECUs attempt to output different bit value at the same time, the dominant state ("0") overwrites the recessive state ("1") by physical implementation of CAN. Then the ECU which attempts to transmit the recessive state ("1") cancels its transmission, because it can recognize that other ECUs attempt to transmit messages with higher priority. In such a way arbitration is realized and only the message with the highest priority is transmitted on the bus.

C. *Error Frame*

Error Frame is a frame used for each ECU to notify other ECUs of an error occurrence when it detects any of five errors during sending and receiving a message (Fig.3). Error Frame consists of Error Flag, Error Delimiter and ITM (Intermission). The ECU which detects an error transmits 6-bit dominant ("0") so that it violates bit stuffing rule. Bit stuffing rule, which is defined by the CAN specification for synchronization among ECUs, is that opposite bit must be inserted immediately after five consecutive bits of the same polarity are transmitted. The ECU which receives first Error Flag (6 bits) detects a stuff error and transmits an Error Frame, therefore superposition of Error flags arises. Thus, all ECUs recognize the error, and the ECU during data transmission cancels its transmission. After that, an 8-bit Error delimiter and a 3-bit ITM are transmitted, and the bus state becomes Bus idle, in which any ECU can starts transmission.

The CAN protocol defines the following five errors; (a) Bit Error, (b) Staff Error, (c) CRC Error, (d) Form Error, and (e) ACK Error. When these errors are detected, Error Frames will be transmitted.

D. *Architecture of ECU*

Typical architecture of an ECU for CAN contains a CPU, a CAN Controller and a Transceiver (Fig.4). The CPU generates messages and processes commands. The CAN Controller sends and receives messages and does arbitration. The transceiver changes the voltage difference between two wires following the order from the CAN controller, and transfers digital signal ("0" or "1") to the CAN Controller by detecting the voltage difference. The CAN Controller and Transceiver are usually implemented as semiconductor chip(s).

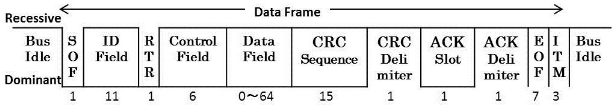

Figure 2. DataFrame

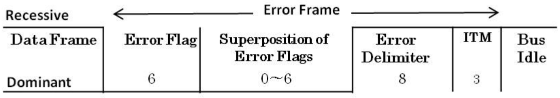

Figure 3. Error Frame

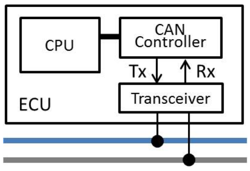

Figure 4. Architecture of ECU

IV. Problems and Threats in CAN

A. Security Problems in CAN

The following security vulnerabilities in CAN protocol are pointed out by previous studies.

- Lack of Security Mechanisms: Each CAN message can be easily spoofed because it contains no sender information and adopts no message authentication mechanism except for CRC.
- Broadcast Nature: The fact that every CAN message is delivered to all nodes connected to a single CAN bus allows an attacker to eavesdrop or analyze CAN messages easily.

We discuss potential attacks which exploit these vulnerabilities in the following.

B. Treats in CAN

- Eavesdrop: As CAN protocol does not support confidentiality and all CAN messages are broadcast, an attacker can eavesdrop on every CAN message. Some type of messages can be observed through OBD-II port.
- Unauthorized Data transmission: An attacker trying to impersonate an ECU can transmit arbitrary messages on CAN bus, by injecting them through OBD-II port, by connecting an additional unauthorized ECU, or by modifying an existing normal ECU. An attacker can conduct a replay attack easily as he can observe all messages transmitted on CAN bus.
- Denial of Service attacks: It is easy for an unauthorized ECU to prevent message transmission of normal ECU by keeping the bus in dominant state continuously or sending messages with higher-priority successively.

Among these threats, unauthorized data transmission leads to abnormal behavior of ECU and endangers the driver. Therefore study on countermeasure against the threat is very important. In this paper we discuss a countermeasure against unauthorized data transmission.

V. Proposed Method

We propose a method of preventing unauthorized data transmission in CAN. First, we describe evaluation criteria. Second, we make an assumption about the proposed method and explain the basic idea of the method. Finally, we illustrate implementation technique.

A. Evaluation Criteria

The following are evaluation criteria for a protection method against unauthorized data transmission in CAN.

- Cost of Implementation: Cost of implementing protection method in CAN is one of the most important features. It is desirable that necessary changes of ECUs to apply a protection method to CAN are small.
- Traffic in normal time & Traffic under attack: For the reliability of data transmission on CAN bus, the message occupancy on CAN bus needs to be low. It is desirable that data traffic is not increased by implementation of a protection method.
- Detection Accuracy: A protection method should achieve low rates in both false negative and false positive. A false negative means that the protection method recognizes unauthorized messages as authorized messages. A false positive means that the protection method regards authorized messages as unauthorized messages.
- Real-time Response: It is desirable that the system can achieve sufficient real-time response to prevent an unauthorized message.
- Compatibility: A protection method should be in accordance with CAN specifications in order to cover as many existing systems that used CAN as possible.
- Interconnected Buses: A vehicle is composed of multiple bus networks connected by a gateway. It is possible that a sender node and a receiver node are located in different CAN bus networks. A protection method should be applicable in such a situation.

B. Assumption

We assume that there is only one sender node corresponding to an ID of Data Frame in each bus network. The CAN specifications prohibit that two or more nodes transmit Data Frame with the same ID at the same time, thus this assumption is realistic.

C. The Fundamental Idea

In our prevention method, each to-be-protected ECU detects unauthorized transmission by monitoring all data on the bus: each ECU detects data transmission from other ECUs that delivers Data Frame indicating its own ID. Such data transmission is regarded as an unauthorized message. If an ECU detects an unauthorized message, then the ECU immediately transmits Error Frame to override the message before the message transmission is completed. Thus, our method has the capability of preventing the unauthorized Data Frame transmission itself. We can apply our prevention method to all ECUs or only to ECUs that send important messages.

D. Implementation

This prevention method requires implementation in physical layer in order to achieve sufficient real-time response. The ECU which detects unauthorized transmission is supposed to send Error Frame before the unauthorized transmission is completed. The followings are the techniques to implement this prevention method in CAN controller.

A flag, which indicates that a to-be-protected ECU is trying to transmit Data Frame, is implemented within the CAN controller of the to-be-protected ECU. The following is the timing of switching the flag when the ECU transmits Data Frame (Fig.5).

0) Bus Idle (the flag is OFF)

1) The ECU starts sending a Data Frame.

2) The ECU sets the flag if it has successfully transmitted ID field. (e.g. when the ECU transmits Control field.)

3) The ECU clears the flag when the CAN bus state is ITM.

4) Return to step0.

The ECU which detects an attempt of unauthorized transmission prevents it in the following way (Fig.6).

0) Bus Idle (the flag is OFF)

1) The ECU receives a target Data Frame.

2) By checking the flag, the ECU confirms whether or not it is in the process of its own data transmission. If the flag is OFF, then the ECU sends Error Frame immediately.

3) Return to step (0). These steps are repeated whenever the ECU receives a target Data Frame.

VI. Discussion

In this section, we evaluate our prevention method and compare it with other protection methods.

A. *Evaluation of Proposed Method*

- Cost of Implementation: The proposed method can be realized with a simple modification of CAN Controllers. Thus the implementation cost is low.

- Traffic in normal time & Traffic under attack: In normal time, there is no traffic increase by applying the proposed method. When the bus is under attack, it can reduce the traffic by preventing unauthorized messages. In fact, any unauthorized Data Frame of potentially 108 bits will be replaced by an Error Frame of 14 to 20 bits.

- Detection Accuracy: Our prevention method can detect all unauthorized messages in principle as far as every sender node is equipped with it. In addition, there is no false positive unless the detecting node itself is compromised.

- Real-time Response: The prevention method can be implemented in CAN Controller on hardware basis successfully achieving sufficient real-time response.

- Compatibility: Introducing the proposed method into existing systems hardly influences the compatibility of the system to a standard CAN. It indeed requires only an addition of a single error definition to CAN Controllers. Therefore, the method is expected to be well acceptable in many existing systems.

- Interconnected Buses: Modern automobiles utilize multiple buses connected to each other through gateways as depicted in Fig. 1. In such interconnected networks, data can be transmitted from one node in a bus to another node in another bus. Consider gateway g interconnecting bus x and bus y. Then, for detecting unauthorized data transmission in bus x, g can act as all sender nodes in bus y. Likewise, for detecting unauthorized transmission in y, g can act as all sender nodes in x. Therefore our method is still applicable to such interconnected networks. Moreover, in case that two different types of networks are interconnected (e.g. CAN-LIN, CAN-MOST, etc.), our method is still applicable as far as the receiver node is in CAN.

B. *Feasibility on Real-time Response*

In order to realize real-time response of our method, CAN Controller is required to check the ID field of all incoming data and immediately issue an Error Frame upon a detection of unauthorized data transmission. Recalling the fact that CAN Controller is required to handle a CRC error in similar manner, namely, checking the CRC field of all incoming data and immediately issuing an Error Frame right after the CRC delimiter, our method is expected to be reasonably implemented in an ECU with a standard CAN Controller.

C. *Comparison with Other Protection Methods*

We compare our method with other protection methods [6, 7, 8, 9] according to the evaluation criteria (Table. I).

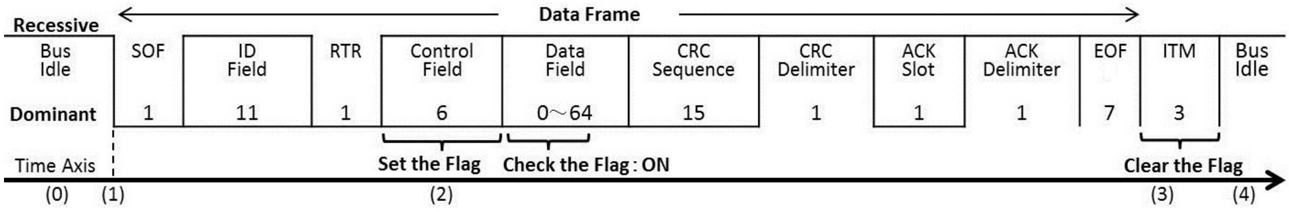

Figure 5. Switching the Flag while Transmission its own Data

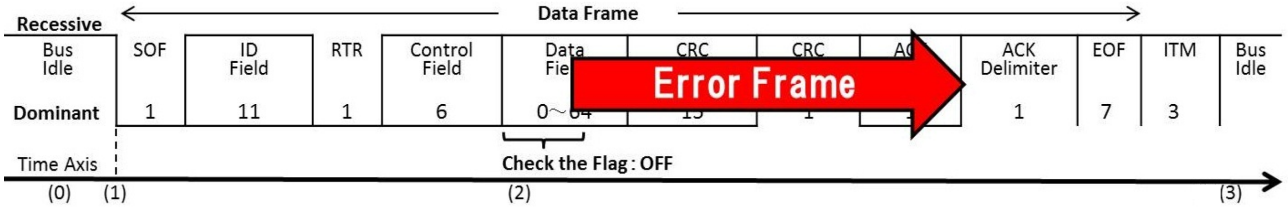

Figure 6. Detecting and Overriding of Unauthorized Transmission

- Cost of Implementation: The IDS based methods need at least one additional ECU as a detector node. The cryptography based methods need ECUs with cryptographic function. Although IDS needs to be developed for every car model, our method does not depend on car model, and development cost is small.
- Traffic in normal time & Traffic under attack: In normal time, the traffic of the CAN bus is not changed by any protection methods including ours, but our method can reduce the traffic when the bus is under attack. Our method surpasses the other methods in this point.
- Detection Accuracy: Our method and the encryption based method [6] can detect all unauthorized messages, and there is no possibility that these methods regard unauthorized messages as authorized messages. The MAC based method [7] cannot identify unauthorized message exactly. On the other hand, it is difficult to completely eliminate both false negative and false positive in IDS.
- Real-time Response: The encryption based method [6] can detect unauthorized messages and discard them. The MAC based method [7], can detect unauthorized message by verifying MAC after the receiver ECU received and handled the message. Similarly, the IDS based methods also allow receiver ECU to process unauthorized messages until they are detected.
- Compatibility: The IDS based methods do not deviate from CAN standard. Our method and the cryptography based methods require modifications to the standard procedures of CAN. Whereas our method requires only small changes within CAN Controller, the MAC based method [7] deviates heavily since it replaces the CRC field with MAC.
- Interconnected Buses: As cryptographic methods typically work on End-to-End, it can cope with interconnected networks. The IDS methods as well as our method work in interconnected networks if implemented in gateways.
- Others: The cryptographic methods typically suffer from key management issues including the case of leakage of secret keys while our method contains no secret information to be securely managed.

D. Coexistence with Other Protection Methods

The proposed method works even if other protection methods are employed since they do not damage our assumption.

VII. Conclusion

We have proposed a prevention method for unauthorized data transmission in CAN, which is characterized by the fact that anyone does not receive unauthorized Data Frames. The ECU implementing this method can detect any unauthorized Data Frame and overrides it by transmitting an Error Frame. Prevention of unauthorized data transmission has been supported by none of conventional security mechanisms so far studied. Our method is efficient in preventing unauthorized transmission itself and in achieving sufficient real-time response for greatly enhancing desirable CAN security.

References

[1] ISO 11898-1, “Road vehicles - Controller area network (CAN) - Part 1: Data link layer and physical signaling,” International Standards Organization (ISO), ISO Standard 11898-1, 2003.

[2] ISO 11898-2, “Road vehicles - Controller area network (CAN) - Part 2: High-speed medium access unit,” International Standards Organization (ISO), ISO Standard 11898-2, 2003.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental security analysis of a modern automobile,” IEEE Symposium on Security and Privacy 2010, pp. 447 – 462, 2010.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, “Comprehensive experimental analyses of automotive attack surfaces,” the 20th USENIX Security Symposium, 2011.

[5] T. Hoppe, S. Kiltz, and J. Dittmann, "Security Threats to Automotive CAN Networks - Practical Examples and Selected Short-Term Countermeasures" In Proceedings of the 27th international conference on Computer Safety, Reliability, and Security, SAFECOMP '08, pp. 235 – 248, 2009.

[6] M. Wolf, A. Weimerskirch, and C. Paar, "Secure In-Vehicle Communication," Embedded Security in Cars – Securing Current and Future Automotive IT Applications, 2006.

[7] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes," Vehicular Technology Conference VTC 2008, 2008.

[8] M. Müter, A. Groll, and F. Freiling, “Anomaly Detection for In-Vehicle Networks Using a Sensor-Based Approach,” Journal of Information Assurance and Security (JIAS), Volume 6, 2 (2011), 132-140, 2011.

[9] T. Hoppe, S. Kiltz, and J. Dittmann, "Applying Intrusion Detection to Automotive IT - Early Insights and Remaining Challenge," Journal of Information Assurance and Security (JIAS), pp. 226-235, 2009.

TABLE I. Comparison with Other Protection Methods

Protection Method		**The Proposed**	**Cryptography Based Methods**		**IDS Based Methods**	
Evaluation Criteria		**Method**	***Encryption[6]***	***MAC[7]***	***IDS[8]***	***IDS[9]***
Cost of Implementation	Number of ECU modified	Medium	Large	Large	Small	Small
	Amount of Modification per ECU	Small	Medium	Medium	Large	Large
Traffic	In Normal Time	Unchanged	Unchanged	Unchanged	Unchanged	Unchanged
	Under Attack	Decreased	Unchanged	Unchanged	Unchanged	Unchanged
Detection Accuracy		High	High	Moderate	Low	Low
Real-time Response		Fast	Slow	Medium	Medium	Medium
Compatibility		Yes	No	No	Yes	Yes
Interconnected Buses		Yes	Yes	Yes	Yes	Yes