An Intrusion Detection Method for Securing In-Vehicle CAN bus

Mabrouka Gmiden, Mohamed Hedi Gmiden, Hafedh Trabelsi
Computer and Embedded System Lab (CES), ENIS
Sfax,Tunis
Email: mabroukagmiden@hotmail.fr mohamedhedi.gmiden@enis.rnu.tn hafedh.trabelsi@enis.rnu.tn

***Abstract*: Controller area network (CAN) bus has become the most used protocol in automotive network since its robustness and efficiency. However, CAN bus does not have enough security prosperities to protect the whole automotive system even to protect its network. So, security mechanism to protect CAN bus became an emergency need. One of the efficient methods for securing CAN bus, is Intrusion Detection System (IDS). In this work, a simple intrusion detection method for CAN bus is proposed. Our algorithm does not require any modification in standard procedure of CAN bus nor to be implemented in each calculators of network.**

***Keywords*: CAN bus; intrusion detection system; attacks; in-vehicle security;**

I. INTRODUCTION

For decades, automotive domain know serial of developments .Numerous functionality insured by computer components, called Electronic Control Units (ECUs) [17] and modern cars can contain from 70-100 of these devices [4]. By the growing of complexity and of modern cars, ECUs need to exchange data between them. By the development of automotive networks such as Controller Area Network (CAN), FlexRay, MOST, and LIN [13], communication between nodes has became more efficient. Although, recent studies have shown that in-vehicle protocols are not protected against malicious attacks [1] because they have not any type of authentication [12].

CAN bus is the based protocol of in-vehicle networks. But the fact that CAN message is broadcasted to all nodes [6] as that it does not contain any authenticator fields [1], makes it easy for an attacker to full control the network message transmission, as mentioned in previous study like [14][11]. Until recent years, security has not been a concern in spite this clear issue.

On the other hand, vehicles have not no more been a closed machine. In fact modern, cars can connect to wired devices like: USB and CD or wireless one like 4G, smart phone and WiFi, even communicate with their similar.

Therefore, vehicle becomes an open system which increases the probabilities of attacks [8].
Consequently, CAN bus security becomes a big concern and it takes over a place between recent topics of research. In fact, it threats the security of passengers as well as the safety of networks like showed koscher et al. in [6]. To overcome security problems, two main strategies of defense have been made: message authentication and intrusion detection. Previous study such as [19] provided that limitations of message authentication mechanism make intrusion detection one of the most efficient ways of defending against attacks. In litterateur, there are several mechanisms based on this latter. But, few of them investigated CAN attacks.

In this paper, we treat the security problem in CAN bus by suggesting a simple intrusion detection method for CAN bus IDS. Our mechanism based on the analysis of time intervals of CAN message.

The remainder of this paper is organized as follows. We introduce the related work in Section II. The following section gives the necessary background of CAN bus attacks. Section IV depicts the system and the attack model. Section V details our intrusion detection method. In section VI, We give a summary and a discussion of the proposed method and conclude in Section VII.

II. RELATED WORK

A. Actual researches

As mentioned previously, possible attacks threat driver life or safety of automotive so security has been a motivation for many researchers. They are two major types of security mechanism: message authentication and intrusion detection.

In [2], Larson et al. an in-vehicle delayed data authentication based on compound MAC is presented. The proposed solution is based on calculation of MAC message to detect attacks in the in-vehicle network. Similarly, authors of [10] proposed a message authentication protocol: CANAuth. The solution is based on sending authentication data through an out-of-band channel.

On the other hand, Müter et al. proposed in [9] the calculation of an entropy of CAN bus while the observing of traffic during a "normal" activity refers to a CAN bus. If

a deviations in entropy (compared to reference values) is found an alert is then lifted. Hoppe et al. proposed IDS and demonstrated anomaly detection method by looking at frequency of message transmitted on the bus on simulation [5].Meanwhile, in [3] an approach where each ECU has a sensor that observes the interaction of the latter with the network (sent messages but also consumed messages) is proposed. Intrusion detection is based on a set of security rules based on network protocol specifications and host ECU. Intrusion detection is done independently in each ECU. ECUs gateways which have a sensor bus to which they are attached, may correlate information obtained via these and thereby detecting more attacks. Similarly [16], [11] proposed the saturation of the bus as a reaction to attacks. In [16], Miller and Valzak, built a small device that plugs into the OBD-II port of a car, learns traffic patterns, and then detects anomalies. When the device does detect something, it short circuits the CAN bus, thus disabling all CAN message. In [11], the solution presented is based on the monitoring of network traffic by each of the present ECU. When a calculator observes a message circulating on the bus which is supposed to be its transmitter (based on the ID of the message), the ECU immediately sends an alert on to crush the transmitted message. However, previous mechanisms require to be implemented in each ECU. So they are considered as expensive solutions. By against, in [18] a lightweight intrusion detection algorithm for in-vehicle network based on the analysis of time intervals of CAN messages is proposed. This algorithm does not require any hardware modification but it could not detect irregular message incoming.

III. CONTROLLER AREA NETWORK

In network based on Controller Area Network (CAN) bus, ECUs communicate with each other by broadcasting CAN messages. A message or frame consists mainly of the ID (identifier), which represents the priority of the message, Data Length Code (DLC), Data, and CRC as shown in Figure 1. The identifier of the CAN frame is unique. For example, the frame with ID=0x20 may present the wheel speed values and the frame with ID=0x30 may present the temperature values. Normally, in CAN bus, each node has the right to make a message on bus or to receive it. But if two nodes or more need to transmit message simultaneously, arbitration is the solution of contention in transmission of CAN frame. So the CAN message with the highest priority wins the arbitration and transmitted the first.

Moreover, in CAN bus, message sent by a node will be received by all nodes connected to the bus. So, an attacker can connect to the network traffic and reads data frame easily. Moreover, ECUs in CAN network communicate via messages which do not have any authenticator fields. Thus, an attacker can prevent a frame to reach its receiver. This attack is related to Denial of Services (DoS) attack. In addition, the fact that transmitted messages in CAN bus have not any information about their sender allows an attacker to modify the continent of legitimate message and force the target ECU to receive the modified message. Therefore, after these scenarios, we could find four categories of malicious frame.

- Frames including unknown ID, an incorrect CRC….We talk about frames which do not respond to network protocol specification
- Malicious frames (or frame sequences) generated periodically while the transmission of normal traffic.
- Malicious frames generated periodically and replaced normal frame.
- Malicious frames related to a specific event

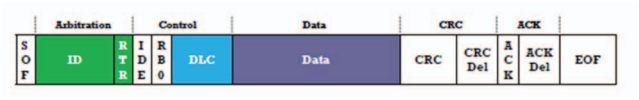

Figure 1. CAN frame format

IV. SYSTEM AND ATTACK MODEL

A. System model

We adapt the automotive network architecture consists of five nodes which are connected to CAN bus in the vehicle via a serial data communication bus. Each ECU controls a particular function of the vehicular system. As shown in Figure 2. In fact, ECU1 is the Instrument Panel Cluster, ECU2 presents the engine control unit, ECU3 is the Cruise control unit, ECU4 is the Wheel-speed sensor and the ECU5 is the Brake pedal position unit.

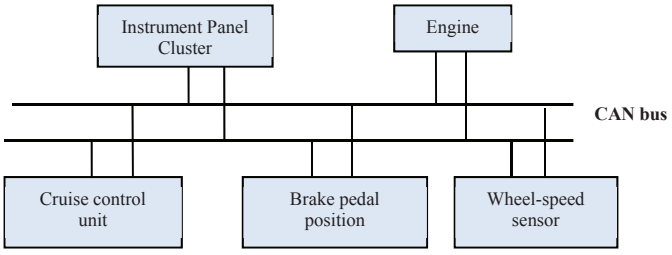

Figure 2. Architecture of the system model

B. Attack Model

We adopt the same threat model as previous works, such as [15] and [20]. If we consider the way over it the attacker could accede to the network as presented in Figure 3, we could assume two attack models:

Model1: The first adversary method is when the attacker relies on additional external device to access to the bus. The attacker could insert the additional device into the On-Board Diagnostics (OBD)-II port. Moreover, the adversary could access to network via an external device like laptop and a smart phone. With an additional device, an attacker could inject malicious messages.

Model2: the adversary could access to the CAN network by compromising an existing ECU. The attacker compromise one ECU to send frames with correct ID but from different ECU compared to its legitimate one so authorized ECUs believe that is a legitimate message and it is sent by an authorized one. An example of an ECU could be compromised were telematic ECUs because they provide

several access points through external networks such as Bluetooth, Wi-Fi, and 3G communication.
The goal of our work is the detection of intrusions regardless to their origins.

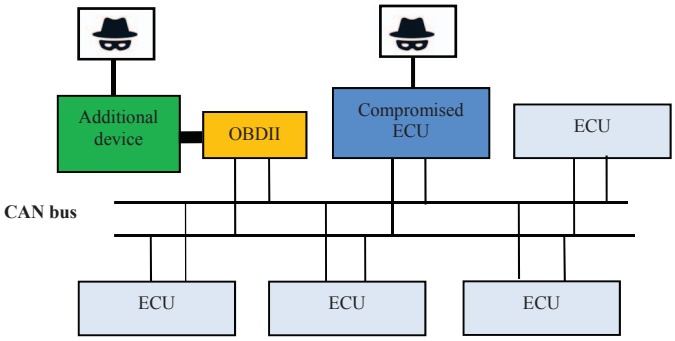

Figure 3. Possible attacker connectivities

As mentioned later, CAN bus has not any type of authentication. Therefore, if an attacker succeeds to access to the bus, he could get code running on an ECU (via an attack over Bluetooth, telemetric, tire sensor, physical access…). Also, he could full control the vehicle by injecting spoofed messages. CAN injection messages could be normal or diagnostic. As the attacker tries to send a malicious message to an ECU, as well as authorized ECUs still send their normal messages periodically. So the target ECU will receive messages from the authorized ECU and from the attacker. Thus, the attacker reaches his goal to transmit injected message, unless he sends it faster than the original ECU. Previous research [16],[18] mentioned that an attacker should send messages from 20-100 times faster than the original ECU to make the target ECU listens to the injected messages. Finally, the rate of messages on the network will be increased more than two times (20 – 100) times higher than the normal).

Focusing in message rate feature, easy detection and prevention of attacks can be possible. In [18], propose a lightweight intrusion detection algorithm for in-vehicle network based on the analysis of time intervals of CAN messages. As a result, they found the time interval is a meaningful feature to detect attacks in the CAN traffic.
To satisfy better compatibility constraints, we do not want to change the ECU existing. In this case, the source of the data is exclusively network traffic
In this paper, we supposed that the attacker can send but we do not consider Denial-of-Service (DoS) attack

V. PROPOSED INTRUSION DETECTION METHOD

Automotive security has become a priority for manufacturers requiring the implementation of security policies into the automotive embedded system while considering automotive networks as a whole. Thus, in addition to preventative mechanism which dedicated to prevent the access of an attacker into the network, it is necessary to think to interior mechanisms could able to detect attacks, such as intrusion detection systems IDS.

A. The Fundamental Idea:

We adapt the Intrusion detection system with this aspect:

- Data source: the proposed IDS is a network intrusion detection systems (i.e.it analyzes incoming network traffic).
- Method of detection: as its ability to detect new attack as well as its easy implementation than the Signature-based IDS, we adapt Anomaly-based IDS.
- frequency of analysis: the detection is in real time
- Concerning its behavior after detection our IDS assumed to alert the user if suspicious frame is detected.
- In our works, We focused on the tow first type of malicious frame, so the proposed IDS dedicated to detect Frames including incorrect ID and Malicious frames generated periodically while the transmission of normal traffic.
- As each authorized ECUs sends their normal messages periodically, the time interval of each CAN ID is unique. So, in this work we adopted this fact. Therefore, our IDS detects message which its ID de not respect its own interval time, as the procedure in the next section.

After introducing the main aspects of our IDS, we continue with presenting the procedure according to it our system detects messages: each ECU connected to CAN bus sends its message regularly, so each message ID (0x1, 0x2, …) generated by ECUs has its own regular frequency or interval. The IDS checks the arrival time of CAN ID. It calculate the time interval of the arrival message compared to last message .If the interval message is less than the normal one, the alert will be lifted . The entire process of the IDS is summarized in Figure 4.

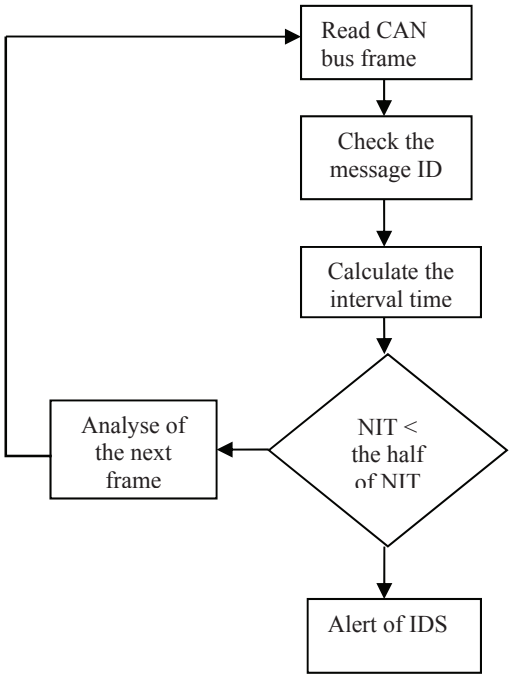

Figure 4. Diagrame of the propsed IDS

B. Attack scenario:

To more explain the functionality of our IDS we choose the study of the cruise control system which works as following: at the beginning the cruise control is in “off mode”, and it could switch to “off mode” unless it overshoots a specific value. When the operator turn on the

cruise control function, via the Instrument Panel Cluster (ECU1), a command frame is sent to the cruise control unit (ECU3) also this frame contains the speed which it should make the vehicle run on it. The cruise control system asks regularly, the vehicle speed from the Wheel-speed sensor (ECU5), if the new value is lower than the target one, the CCU send a message of to the engine (ECU2) unit to accelerate. Else if value sent by the sensor is upper than the demanded speed, a frame demand deceleration is sent. Finally, the operation of the cruise control system turns off, if the operator stops it by pressing the Brake pedal (ECU4) or if the speed value becomes lower than the threshold value.

If we adapt the attack model discussed later, we assume the following scenarios: an attacker sends message to the engine asking acceleration, as shown in Figure 5. This message normally sent by the cruise control unit. While the injection of unauthorized message, the Wheel-speed sensor remains sending regularly frame.

First of all, it is important to mention that all frame transmitted in this system are periodic. The time interval of 0x01 and 0x03 are respectively 10ms and 30ms. The attacker injects, at a high frequency, the message with ID=0x03 after 10 milliseconds from the last one. So, the time interval of 0x03 decreases from 20ms to 5ms. Therefore, ECU2 receives message injected by the attacker. When the attacker sends the message, the IDS calculated the time interval of the arrival message and compared it to last one. The IDS found that the arrival message is less than the half of the normal, so the alert is lifted.

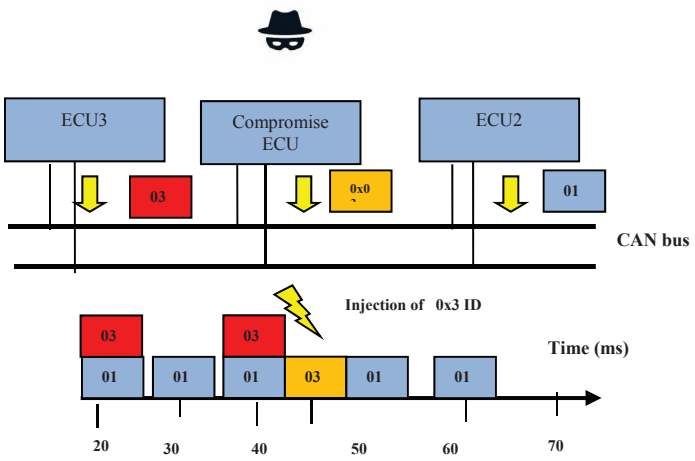

Figure 5. representative of scenario

VI. DISCUSSION AND SUMMARY

In this last section, we give a brief evaluation of the proposed method by comparison with some works and according to criteria for a detection method of intrusions which purpose CAN bus.

Compatibility: The advantage of our proposed method that does not require any modification in CAN protocol unlike methods proposed in [12] and [2]. In fact, the proposed method in [12] is required the implementation in physical layer. Similarly in [2] the CAN standard protocol is should be modified by replacing the CRC field with MAC

Cost of Implementation: Whereas, one additional ECU to the bus is sufficient for implementing our method, cryptography based methods such as [3] as well as [12] and [16] need to be implemented in each ECU which increases cost of implementation in the industrial scale.

Compatibility with other protection mechanisms: our proposed method could work even other security methods are implemented as long as they are suitable with our assumption

VII. CONCLUSION

To defends against vehicle attacks, a recent security approaches have been proposed in the literature. However, the greater part they require hardware modification or implementation in each ECU. In this work, we proposed a simple intrusion detection method for CAN bus IDS. Our mechanism based on the analysis of time intervals of CAN message. The main idea is to implement an IDS which checks the CAN ID of the transmitted message then calculates the time intervals from the latest one. Also, in this paper, we provided a general overview about attacks, their classification and some mechanisms to defend against them. The advantage of our method is that does not require a modification in hardware layer and implementation in each ECU. As perspective of this work, we intend to perform the proposed method to detect Dos attacks and the other type of attacks.

REFERENCES

[1] M. Wolf, A. Weimerskirch, and C. Paar, “Security in automotive bus systems,” Workshop on Embedded Security in Cars, 2004.

[2] 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.

[3] U. E. Larson, D. K. Nilsson, and E. Jonsson,” An Approach to Specification-based Attack Detection for In-Vehicle Networks”, 2008.

[4] R. N. Charette, “This car runs on code,” IEEE Spectr.,vol. 46, no. 3, p. 3, 2009.

[5] 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.

[6] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S.Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, “Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy”, 2010.

[7] I. Rouf, R. Miller, H. Mustafa, et al., "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in Proc. of the 19th USENIX Security Symposium, Aug. 2010.

[8] S. Checkoway, D. McCoy, et al., ”Comprehensive experimental analyses of automotive attack surfaces”, Proc.20th USENIX Security, San Francisco, CA, 2011 .

[9] M. Müter, N. Asaj, “Entropy-based anomaly detection for in-vehicle networks”, Intelligent Vehicles Symposium (IV), Baden Baden, Germany, 2011. IEEE.

[10] A. Van Herrewege, D. Singelee, I. Verbauwhede, “Canauth - a simple, backward compatible broadcast authentication protocol for can bus”, ECRYPT workshop on Lightweight Cryptography, 2011.

[11] T. Matsumoto, M. Hata, et al., “A method of preventing unauthorized data transmission in controller area network”, Vehicular Technology Conference (VTC Spring), pages 1–5, Yokohama, Japan, 2012. IEEE

[12] C-W. Lin, A. Sangiovanni-Vincentelli, “Cyber Security for the Controller Area Network (CAN) Communication Protocol”, 2012

[13] I. Studnia, V. Nicomette, et al., “Survey on security threats and protection mechanisms in embedded automotive networks”, 2nd

Workshop on Open Resilient Human-aware Cyber- Physical Systems, Budapest, Hungary, 2013.
[14] C. Miller, C. Valasek, “Adventures in automotive networks and control units”, 2013.
[15] Q. Wang, S. Sawhney, “VeCure: A Practical Security Framework to Protect the CAN Bus of Vehicles”, 2014.
[16] C. Miller, C. Valasek, “A survey of remote automotive attack surfaces”, 2014
[17] C. Miller, C. Valasek, “Remote exploitation of an unaltered passenger vehicle”, BlackHat USA, 2015.
[18] H. M. Song, H. R. Kim and H. K. Kim, “Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In-Vehicle Network”, 2016.
[19] K-T. Cho, K.G. Shin,” Fingerprinting Electronic Control Units for Vehicle Intrusion Detection”, 2016.
[20] W. Choi, H.J. Jo, et al., “ECUs Using Inimitable Characteristics of Signals in Controller Area Networks”, 2016