Analysis of current attacks on the CAN bus and development of a new solution to detect these types of malicious threats

Mohammed KARROUCHI[1,2] , *Mohammed* RHIAT[1], *Ismail* NASRI[1], *Ilias* ATMANE[1,3], Kamal HIRECH [1,3], *Abdelhafid* MESSAOUDI [4], *Mustapha* MELHAOUI [5], *Kamal* KASSMI[1]

[1]Electrical Engineering and Maintenance laboratory, High School of Technology BP. 473, Mohammed first University, Oujda, Morocco
[2]Research Center, High Studies of Engineering School, EHEI, Oujda, Morocco
[3]Higher School of Education and Training, Mohammed First University, Oujda, Morocco
[4]Energy, Embedded Systems and Information Processing laboratory, National School of Applied Sciences, Mohammed First University, Oujda, Morocco
[5]Faculty of Sciences and Technologies, Cadi Ayyad University, Marrakech, Morocco

Abstract. The majority of modern vehicles have electronic control units (ECUs) in charge of controlling their functions. These ECUs communicate with one another using the CAN (Controller Area Network) communication protocol. This practical bus offers great transfer of data quality by enabling wide propagation that quickly reaches all sections of a vehicle. Unfortunately, this specific protocol places little focus on security, making the CAN bus control system susceptible. This is owing to its ease of physical or remote access and lack of confidentiality. This vulnerability makes it feasible to take control of the vehicle and endanger the safety of the passengers. The main objective of this work is to present the current existing vulnerabilities of the CAN Bus, to discuss a practical demonstration of hacking as well as to propose a technique to fight against these malicious actions, and all this by practical demonstrations on a DACIA Lodgy and Sandero 2014 vehicles.

1 INTRODUCTION

Modern automobiles contain a variety of electrical components, that use various installed sensors to perform relevant tasks in order to process the data measured [1]. The electronic components interconnect through the Controller Area Network Bus (CAN Bus). These innovations illustrate the fact that the automotive sector is undergoing a series of developments and multiple functionalities aimed at reducing manufacturing costs, guaranteeing fast and fluid operation of on-board systems, and making driving tasks more comfortable on the road [2]. This discovery opens the door to many benefits, but also to weaknesses that hackers can exploit specifically on the CAN bus, and on all fieldbuses in general [3]. A network vulnerability assessment is essential to highlight security problems.

Therefore, the CAN protocol vulnerability assessment can be carried out on the basis of confidentiality, integrity and availability. Other external connections, such as Wi-Fi, 3G/4G, Bluetooth, GPS, and the wireless communications provided by the vehicle's system, are also integrated [4, 5]. These exposed interfaces allow attackers and pirates to enter the in-vehicle network (IVN). Researchers in the security field have previously shown a number of prototypes attacks against contemporary unmodified and licensed vehicles [6]. These findings have spurred new industry and academic efforts to develop state-of-the-art methods for protecting modern automobiles in the face of computer attacks. A particularly interesting and as yet unexplored area of research is the development of techniques and algorithms for evaluating CAN bus messages in order to identify potential indicators of illegal activity. Indeed, all known attacks that pose significant security risks involve the injection of malicious messages into the CAN bus of attacked vehicles [7].

Based on an experimental study carried out on authentic CAN network data from a licensed vehicle, we present a detailed experience of an attack targeting a vehicle ECU, and propose an algorithm to protect the CAN system from this kind of risk.

This paper is structured as follows: Part II covers the fundamentals of the CAN bus and the concepts of the CAN frames, forming the basis of the present work. Part III covers existing methods of hacking the vehicle, as well as solutions to counter them. Our study demonstrating the attack is described in Part IV. The last part explains the proposed algorithm that detects intrusions on the vehicle's CAN network to protect it against malicious attacks. Part VI concludes the paper.

2 ESSENTIAL BACKGROUND

2.1 CAN Bus (Controller Area Network Bus)

A local Area Network called the CAN bus was initially created to control industrial and automotive equipment. A serial broadcast bus standard, CAN is used to connect peripherals for electronic control units (ECUs), or microcontrollers, known as multiplexing [8]. A failure in any one component has no impact on the rest. All units are capable of sending and receiving frames signals [9]. A schematic diagram of the CAN topology is shown in Fig. 1.

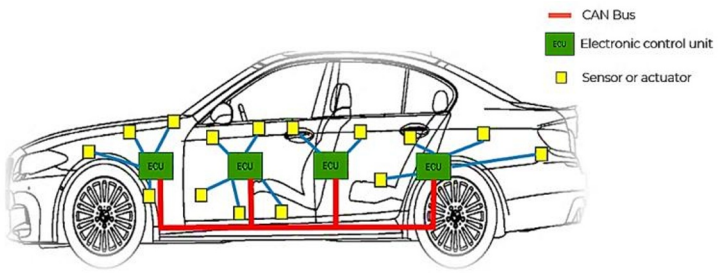

Fig.1. Vehicle CAN network design.

2.2 CAN frame

The CAN frame is made up of several fields, A start bit, followed by an 11-bit identification zone where all devices communicate their addresses to determine who can send their frame and which message has the highest priority. An RTR bit which defines whether the frame carries data or a data request. The identification zone and the RTR bit constitute the arbitration field. An IDE bit which indicates whether the frame is standard or extended. 4

DLC (Data Length Code) bits specifying the data length, followed directly by the data field, which can range from 1 byte to 8 bytes. Then the 16-bit CRC sequence, to check the integrity of the transmitted data. An ACK bit set to the dominant state by the receiver, followed by 7 bits identifying the end of the frame. Fig. 2 indicates the CAN message format.

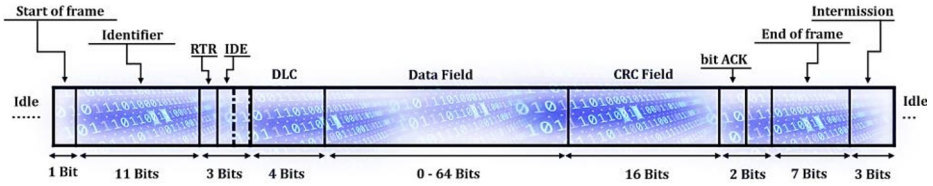

Fig.2. Structure of a standard CAN frame.

3 RELATED WORKS

Talking about attacks, many academic researchers have shown that it is possible to compromise a vehicle's control functions and gain physical access to its CAN bus [10, 11]. By attacking the JEEP Cherokee in 2015, Miller and Valasek demonstrated how easy it is for hackers to access the network and start harmful activity [12]. The attack known as CANDY CREAM was shown in practice by Gianpiero Costantino and Ilaria Matteucci [13], they identified and exploited the IVI Android OS flaws by linking to the actual CAN bus. As a result, they managed to take control of vehicles equipped with the Android. Sam Abbott-McCune and Lisa A. Shay [14] presented recent findings from their study on local car networks, and described methods for gathering data from the CAN bus through a simulation model. To be clear about this idea, the modern car security system is vulnerable according to research by Koscher et al [15], who also assessed its security frameworks through experimentation. They have demonstrated how an intruder has the ability of accessing practically any ECU as well as bypassing a variety of vital safety measures in order to take control of different vehicle operations, such as stopping the car's engine and deactivating the brakes, among others. To combat this malicious activity and to enhance the CAN's security aspects, researchers [6] have described a technique for integrating a mechanism for message authentication into a prototype in-vehicle network (IVN) based on the CAN network and equipped with an anti-lock braking system (ABS) created in MATLAB and MATLAB Simulink. The approach incorporates additional data on the frame's own security characteristics into each transmitted CAN frame in order to detect any third-party intrusion. Others [16, 17, 18] provide a method for detecting malicious signals introduced into the CAN by intruders. Based on a dynamic identifier, the suggested algorithm detects irregularities in the flow of data on the CAN bus. Also, Miller and Valasek [19] have established the idea of message rate analysis for intrusion detection based on injection frequency in integrated networks.

4 ATTACK PROCECESS

4.1 Operational attack points

The development of electronic technology has enabled drivers to improve their level of comfort, safety and functionality, but it has also given rise to real sources of aggression, as shown in Fig. 3. Such attacks can be classified as physical access attacks, requiring the

attacker to gain physical access to the vehicle, and remote access attacks, implemented via wireless communication interface.

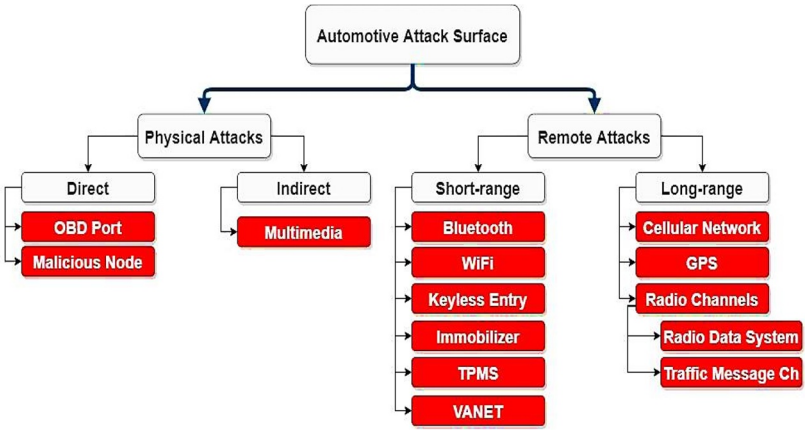

Fig.3. Automotive intrusion surface [20]

4.2 Physical attack demonstration

Fig. 4 shows a schematic diagram of the material handling structure. The CAN bus control circuit consists of a computer, a management and control system (SGC) to manage and supervise communications between peripherals, a CAN adaptation system (SA-CAN) consisting of a CAN controller for managing sending and receiving operations, and a CAN interface for adjusting voltage settings on the network at speeds of up to 500kbit/s. Through the OBD2 connector, the CAN circuit harvests the data that is being circulated in the car, then broadcasts these frames to the computer for decryption and analysis. The computer's function is to program the CAN board, read sequential data, and display it. It is also used to configure the CAN circuit to transmit unauthorized frames on the physical bus and intrude into the car. Our circuit is used to control and drive the dashboard ECU.

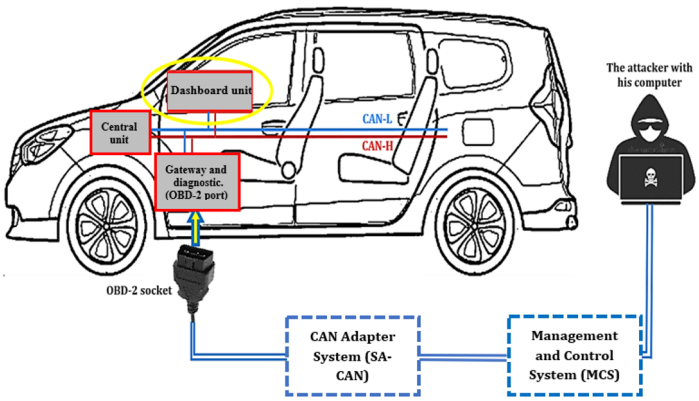

Fig.4. System Block Diagram

4.2.1 The steps involved

To carry out a physical attack, the software implemented is divided into 3 phases.

The first program charged by the task with collecting and reading all frames traveling on the CAN bus in real time and displaying them based on their identifiers. Table 1 shows the frames and their identifiers retrieved from the CAN bus. The Frames are threaded based on their identifiers using the masks and filters registers. Masks and filters must therefore be configured appropriately and set to zero in order to obtain the entire contents of frames travelling on the serial bus.

Table 1. Collected frames with their identifiers.

Identifiant	Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7	Octet 8
0x65C	86	26	-	-	-	-	-	-
0x1F6	1E	0	40	2E	40	13	0	FE
0x3B7	FF	FF	7F	CF	FE	0	-	-
0x666	0	0	0	-	-	-	-	-
0x18A	2E	0	0	6C	0	0	-	-
0x564	F5	A0	-	-	-	-	-	-
0x55D	0	DD	50	0	82	80	0	0
0x186	0	0	32	3	20	0	21	-
0x29C	0	0	0	0	FF	FF	FF	FF
0x5DE	0	A	40	0	0	0	0	42
0x62B	0	0	-	-	-	-	-	-
0x354	0	0	0	0	0	0	0	0
0x6FB	7F	3	FF	E	0	FF	0	35

During this stage, we noticed that some frames contain lighter data fields than others, such as frame identifiers 0x65C and 0x564, while others are initialized to zero and remain unchanged during testing, such as 0x62B and 0x354. Note that during the testing of this contribution, the vehicle remained stationary.

A second step is to select only one frame with a specific identifier. The masks must be set to 1 with filters having the value of the ID selected for this filtering. It must repeat specific activities (turning the steering wheel, activating the indicators, pressing the accelerator pedal, etc.) for each frame and note the byte values changing in the data associated to each identifier. In this manner, the identity and executive accountable for each action in the vehicle can be identified.

Following the identification of the frames and their IDs for the different activities, the final objective is to enter the car outside and inject frames with a specific identifier, manipulating the frame content (changing bytes) to get an overview of actions conducted by the ECU affected in the assault.

4.2.2 Results obtained

As shown in Fig 5, and after the tests carried out, identification of the frames responsible for the RPM display data was made, as well as determination of the frames that react with changes in the dashboard light indicators. After repeated efforts, it was discovered that only the 1st byte of the frame with ID_0x5DE affects the changing display of signals on the dashboard. Since engine speed varies from 0 rpm to 7000 rpm, it takes 2 bytes to encode these values, so we found that the RPM engine speed variation values change using the first two bytes of the frame with ID_0x186. Fig. 5 shows the processes and demonstrations discovered.

Fig. 5. (a). Test vehicle. (b) Monitor revolutions per minute. (c) Hardware used. (d) Monitor the indicator lights.

5 INTRUSION DETECTION

During normal vehicle activity, each ECU generated message ID has a uniform frequency. Our proposed method is based on detecting the frequency of message injection on the CAN bus. For more details, take the example of the 0x186 identifier frame dedicated to engine speed RPM shown in Fig 6. The real ECU present at node 2 has sent frames on the vehicle's CAN network, and at the same time our system injects frames with the same identifier but different data content. In this case, the ECU presented at node 1, which is already programmed to receive frames with identifier 0x186, will accept and receive data from this real ECU as well as from the intrusive system manufactured by the attacker.

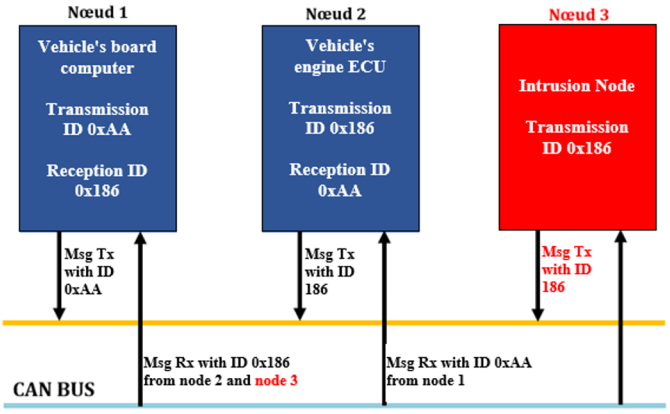

Fig. 6. Summary of intrusion in our study.

As shown in this Fig. 7, both frames are inserted and circulate in the vehicle's CAN bus, but in order to make the real ECU frames unreadable, it is necessary to increase the sampling

frequency or inject intrusive messages to minimize the inter-frame time and mask the exact frames.

The fundamentals of detection are as follows:

Firstly, IDS checks the ID and calculates the time interval from the arrival time of the last message transmitted on the CAN bus. After that, and if the new message's time interval is less than the typical model, the IDS flags the message as an abnormal message because it arrived earlier than expected.

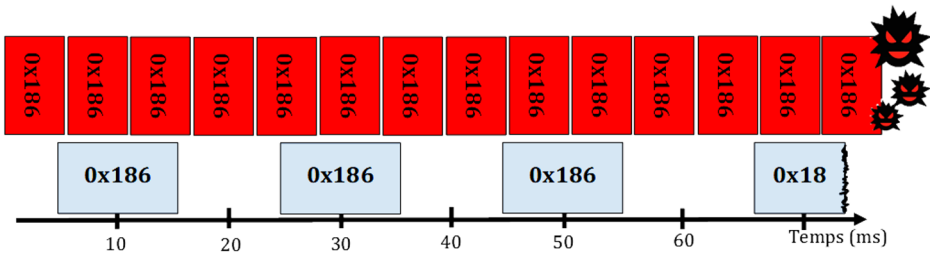

Fig. 7. Representative of the scenario

6 CONCLUSION

Vehicle safety has become one of the biggest challenges in the face of new security violations. Many studies show that it is possible to hack into the vehicle's electronic system, while others propose several security mechanisms to defend against attacks from the vehicle. To detail and discuss the problem and its solution, we presented our physical attack on the vehicle's CAN network, with a higher frequency of intrusive message injection than that of the real ECU, and based on this type of attack, we proposed a solution to distinguish this type of malware. As a result, it has the potential to vastly increase vehicle safety and security. As a result, vehicle safety and security can be considerably enhanced.

REFERENCES

1. Karrouchi, M., Nasri, I., Snoussi, H., Messaoudi, A., Kassmi, K. (2021). Implementation of the Vehicle Speed and Location Monitoring System to Minimize the Risk of Accident. In: Motahhir, S., Bossoufi, B. (eds) Digital Technologies and Applications. ICDTA 2021. Lecture Notes in Networks and Systems, vol 211. Springer, Cham. https://doi.org/10.1007/978-3-030-73882-2_140
2. M. Karrouchi, I. Nasri, H. Snoussi, I. Atmane, A. Messaoudi and K. Kassmi, "Black box system for car/driver monitoring to decrease the reasons of road crashes," 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Alkhobar, Saudi Arabia, 2021, pp. 01-06, doi: 10.1109/ISAECT53699.2021.9668545.
3. Li, X., Yu, Y., Sun, G., & Chen, K. (2018). Connected vehicles' security from the perspective of the in-vehicle network. IEEE Network, 32(3), 58-63. **DOI:** 10.1109/MNET.2018.1700319
4. KARROUCHI, Mohammed, et al. "Practical investigation and evaluation of the Start/Stop system's impact on the engine's fuel use, noise output, and pollutant emissions." e-Prime-Advances in Electrical Engineering, Electronics and Energy (2023): 100310. https://doi.org/10.1016/j.prime.2023.100310

5. Mohammed, K., Abdelhafid, M., Kamal, K., Ismail, N., & Ilias, A. (2023). Intelligent driver monitoring system: An Internet of Things-based system for tracking and identifying the driving behavior. Computer Standards & Interfaces, 84, 103704. https://doi.org/10.1016/j.csi.2022.103704
6. Ishak, M. K., & Khan, F. K. (2019). Unique message authentication security approach based controller area network (CAN) for anti-lock braking system (ABS) in vehicle network. Procedia Computer Science, 160, 93-100. https://doi.org/10.1016/j.procs.2019.09.448
7. Karrouchi, M., Messaoudi, A., Kassmi, K., Nasri, I., Atmane, I., Blaacha, J. (2023). Design and Demonstrate an Attack Strategy to Control a Vehicle's Computer by Targeting Its Electrical Network. In: Bekkay, H., Mellit, A., Gagliano, A., Rabhi, A., Amine Koulali, M. (eds) Proceedings of the 3rd International Conference on Electronic Engineering and Renewable Energy Systems. ICEERE 2022. Lecture Notes in Electrical Engineering, vol 954. Springer, Singapore. https://doi.org/10.1007/978-981-19-6223-3_58
8. Minu A Pillai, Sridevi Veerasingam and Yaswanth Sai D, "Implementation of Sensor Network for Indoor Air Quality Monitoring using CAN interface," IEEE international conference on Advances in Computer Engineering ,2010. DOI: 10.1109/ACE.2010.85
9. Karrouchi, M., Nasri, I., Kassmi, K., Messaoudi, A., Zerouali, S. (2023). Analysis of the Driver's Overspeed on the Road Based on Changes in Essential Driving Data. In: Motahhir, S., Bossoufi, B. (eds) Digital Technologies and Applications. ICDTA 2023. Lecture Notes in Networks and Systems, vol 668. Springer, Cham. https://doi.org/10.1007/978-3-031-29857-8_80
10. Ashraf, J., Bakhshi, A. D., Moustafa, N., Khurshid, H., Javed, A., & Beheshti, A. (2020). Novel deep learning-enabled lstm autoencoder architecture for discovering anomalous events from intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems. **DOI:** 10.1109/TITS.2020.3017882
11. Avatefipour, O., Al-Sumaiti, A. S., El-Sherbeeny, A. M., Awwad, E. M., Elmeligy, M. A., Mohamed, M. A., & Malik, H. (2019). An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning. IEEE Access, 7, 127580-127592. **DOI**: 10.1109/ACCESS.2019.2937576
12. Miller, C. (2019). Lessons learned from hacking a car. IEEE Design & Test, 36(6), 7-9. **DOI:** 10.1109/MDAT.2018.2863106
13. Abbott-McCune S, Shay LA (2016) Techniques in hacking and simulating a modem automotive controller area network. In: 2016 IEEE international Carnahan conference on security technology (ICCST). IEEE. https://doi.org/10.1109/CCST.2016.7815712
14. Gianpiero Costantino and Ilaria Matteucci, CANDY CREAM hacking infotainment android systems to command instrument cluster via can data frame, 2019 IEEE International Conference on Computational Science and Engineering (CSE). **DOI:** 10.1109/CSE/EUC.2019.00094
15. Koscher, Karl, et al. "Experimental security analysis of a modern automobile." The Ethics of Information Technologies. Routledge, 2020. 119-134. **DOI**:10.1109/SP.2010.34
16. Marchetti, M., & Stabili, D. (2017, June). Anomaly detection of CAN bus messages through analysis of ID sequences. In 2017 IEEE Intelligent Vehicles Symposium (IV) (pp. 1577-1583). IEEE.
17. Islam, R., & Refat, R. U. D. (2020). Improving CAN bus security by assigning dynamic arbitration IDs. Journal of Transportation Security, 13(1-2), 19-31.

18. Desta, A. K., Ohira, S., Arai, I., & Fujikawa, K. (2020, March). ID sequence analysis for intrusion detection in the CAN bus using long short term memory networks. In 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 1-6). IEEE.
19. Miller, C., & Valasek, C. (2014). A survey of remote automotive attack surfaces. black hat USA, 2014, 94.
20. Bozdal, M., Samie, M., Aslam, S., & Jennions, I. (2020). Evaluation of can bus security challenges. Sensors, 20(8), 2364.