CAN-Bus and its Impact on Autonomous Vehicles : Challenges & Complexities.

Omar Najjar
Department of Electrical and Electronic Engineering
Süleyman Demirel University
Isparta , Turkey
ORCID: 0000-0001-7493-9318

***Abstract*—The controller area network (CAN-Bus) is the nervous system that enables communication among vehicles. It contains 'nodes' or 'electronic control units' (ECUs) which are like the parts of the body, interconnected via the CAN bus and help in receiving information about a certain vehicle. Information sensed by one part can be shared with another. The Can-bus is simple, with low cost. Also, it is fully centralized, extremely robust and efficient. In this research paper, the ability of CAN-bus to achieve its characteristics within the scope of Autonomous vehicles will be discussed. Also, The challenges and complexities to use Can-bus and its protocol will be mentioned. The power of Can-bus in the future of IOT systems and cars must be qualified enough to work in such autonomous systems.**

Keywords— CAN-Bus, Internet of Things, ECUs, Autonomous systems, Protocols.

I. Introduction

Automotive vehicles are equipped with electronic control units that are responsible for preparing and broadcasting information like data from a certain sensor. These nodes are able to communicate with each other by Can-bus. Can-bus is simple where ECUs can communicate via only one single Can interface,not via analog lines which might produce errors and has weights and costs[1]. In addition, Can-bus is fully centralized which allows for central error diagnosis and configuration across all electronic control units. The Can-bus system is extremely robust towards failure of other subsystems which makes it ideal for automotive vehicles. These mentioned advantages have made the Can-bus system and protocols one of the most efficient and used in-vehicle communication protocols. Additionally, The protocols that Can-bus support like Can-open, OBD-II, and SAE that are further defined to how data is communicated over a network have made the power of can-bus in automotive vehicles widely used.

The Can-bus protocols will stay relevant, though it will be impacted by major trends such as the rise of cloud computing and the growth of Internet of things and connected vehicles. Actually, the rise in connected vehicles and cloud might lead to a rapid growth in vehicle telematics and Iot Can loggers. In turn, bringing the Can-bus network online will expose vehicles to some security risks that will be discussed later. The difficulties and complexities should be considered especially when sharing information and data online. The lack of encryption and authentication causes serious security issues which might result in attacks that make autonomous vehicles a risk to people[2]. In this research paper, attacks, challenges and potential solutions will be discussed in order to bring can bus protocols to the right place to deal correctly and efficiently with autonomous vehicles.

The autonomous vehicles are equipped with more than 75 ECUs which are responsible for different tasks such as safety critical engine control and anti-lock braking system to maintain and improve the safety of driving [3][4] . Although Can-bus is resilient to noise and has some security features, it is vulnerable to attacks. Most of these attacks are implemented via physical access to the bus, wireless attacks are increasing especially when dealing with cloud computing, internet of things and autonomous systems in general. Vehicle-to-vehicle or vehicle-to-infrastructure are improving which in turn the increasing wireless attacks will become the main challenge for Can-bus for connected vehicles.

Furthermore, for every autonomous system and for every protocol, there should be a cyber security involvement to maintain confidentiality, Integrity, and availability. Explaining all of them together will bring the Can-bus system and protocol to a level that could work when dealing with the internet of things and with autonomous systems.

In the research paper, section II will discuss some security shortcomings for CAN protocols. Then, a security analysis of CAN network by using the CIA triad to build a security model for Can bus in general. In section III some possible solutions will be mentioned in order to deal with these security risks in an organized matter. Finally, other complexities and challenges will be explored in order to generalize the idea of can buses in autonomous systems.

II. SECURITY OVERVIEW

A. Security Shortcomings of CAN Protocol

The improvement of Can protocols over the years and with the rapid change in the automobile industry, the security now matters especially while dealing with a lot of Ecus over a wireless network to be reached to end users[3]. One of the

main problems of security is authentication. Unallowed nodes could simply join the network and share or send information that could have a bad impact on the real data. Can bus is a broadcast network so any node can listen to information and even steal it. The main reason for this issue is that the Can bus data is not encrypted which results in many security risks. For instance, an attack could be made to steal a user's location, address with details which results in breaking the privacy of the cars and their owners.

Denial of service (DoS) is one of the attacks that could be made for Can-bus data. Since Can protocols allow higher priority nodes to take place first, any unauthorized noder with the highest priority could take place and attack the networks. In the internet of things (IoT) and cloud computing everything is shared online which makes the data that is received a risk.

Moreover, the encryption methods couldn't be used in Can-bus data because it makes overhead for real-time communication especially for autonomous vehicles[5]. If so, Can-bus protocols will lose their main features; lightweight and speed. Therefore, this problem made the Can system not safe and could receive many attacks by simple methods like sniffing. So, a security level is required for Can-bus to be able to handle data wirelessly.

Security shortcomings could be even more than that since the system loses the main structure of security including encryption and authentication. Existing works are available to deal with such risks and to bring Can-bus to another place with good security levels. These proposed solutions will be discussed in the following section.

B. Security analysis of CAN Network

As mentioned above, the features that Can-bus have starting from the simplicity to the robust systems reaching to lightweight and fast have made these systems used widely. In addition, it could be applied in real-time and suitable for autonomous vehciles[6]. But in ture these protocols are vulnerable to some security risks. To explain these furthermore, a security analysis is required to evaluate the security level of Can-bus by using CIA triad .CIA triad is a security model that is widely used in cyber security to assess the system vulnerability. CIA triad analyses three essential principles including Confidentiality, Integrity, and Availability.

Starting from confidentiality where is the communication between authorized nodes that should be protected against unauthorized nodes. Then, data integrity where the information which is received by the end users should be exactly the same as the source (ECUs) has been sent over the network without any alteration. Finally, availability is the security solution that should ensure that the system's availability throughout different circumstances are guaranteed[7].

For the Can-bus system, there are no security levels for confidentiality. There are some car manufacturers that use cryptographic methods for local functionalities like keyless entry[3]. But our main goal is to standardize this idea so all vehicle manufacturers use it to maintain a security level and the level of confidentiality goes well.

The way that Can-bus do verification is as follows; Can uses CRC checksum for verification so if any bit is corrupted during the sending level, it could be detected by the end users. On the other hand, CRC checksum cannot detect the altered data that is coming from malicious nodes because of the lack of authentication. As a result, Can-bus systems fail to achieve data integrity .

Accessing the Can-bus network or data by all authorized end users at all time is not possible by Can protolcs because of the physical implementation of the protocol. Since the protocol allows only the higher priority ECU to access the data or the network in general. This issue made availability weak and couldn't be achieved. At the same time, if it allows for highest priority to access all the time, no other ECUs could access the network.

There is a clear lack of the security level of the Can-bus network and its protocol since it fails at some point to achieve the CIA triad. These complexities and challenges are research opportunities to find solutions to handle the, especially the whole automobile industries are going into connected cars and the use of cloud computing and internet of things.

There have been some attacks that were implemented to measure how further Can-bus systems maintain security. One of the attacks was implemented on the electric window lift on the simulation environment by Hoppe and Dittman in 2007[8]. Other attacks have been implemented in real applications to measure security level which are summarized in the following table.

TABLE 1. Summarization of different attacks implemented.

Name of Atack	Cause	Reason
Eavesdropping [9]	Allows any node to understand the bus traffic so an adversary can sniff CAN frames and gather the information.	Lack of encryption techniques in Can-bus systems and protocols .
data insertion [10]	Malicious nodes can attach the network and insert data and allow for data manipulation.	CAN protocol does not have an authorisation mechanism

denial of service (DoS): [11][12]	Preventing any particular node/s or the whole network to provide service.	CAN error confinement is not effective enough to prevent DoS attacks.

III. PROPOSED SOLUTIONS

There are some solutions that have already applied in some places such as the secure network topology in commercial cars. Critical ECUs and no-critical ECUs are separated so end users will not be able to access the critical ECU network easily. Also, the connection between other networks will be via a gateway ECUS. This is a simple solution for some situations but still the gateway ECU and critical network could be attacked and accessed. Kammerer et al. [13] implemented star coupling router topology as the paper called it.. The router not only separates a single-bus based CAN system to multiple CAN segments but also brings new security features like unidirectional channels, traffic shaping, traffic partitioning, message integrity, and intrusion detection.

In order to discover solutions to solve the authentication issue, Wang et al [14]. proposed a practical security framework for vehicular systems (VeCure). In the proposed method each node which sends a CAN packet needs to send the message authentication code packet (8 bytes) as well. They divided the ECUs into two categories namely Low-trust group and High-trust group. ECUs which have external interfaces e.g. OBD-II or telematics are put in the low-trust group. Hightrust groups share a secret symmetric key to authenticate each coming and outgoing messages in a way that an ECU from a Low-trust group that does not know the key cannot send messages to critical ECUs in a high-trust group.

In addition, Siddiqu et al. [15] proposed a physical unclonable function (PUF) based encryption and authentication and provide secure communication over CAN bus. They used an elliptic curve Diffie-Hellman based asymmetric encryption method also called public-private key cryptography. Asymmetric key encryption is safer than symmetric key encryption but it requires high computational power for current ECU controllers. According to their data, AES-128 encryption generates 366.66 ns and 110 ns latency at 60 MHz and 200MHz clock frequency respectively. This proposed solution has some disadvantages including the limitation that ECUs have in the computational power. In reality, latency will increase significantly. The other negative side of this proposal is it requires hardware change in the CAN controller and a server to authenticate the nodes. This will increase the system cost and having a server can create other potential attacks. Although the solution provides some security level, some of Can-bus systems and protocols advantages will be lost. Additionally, while dealing with autonomous vehicles and real-time application will not be work, latency and speed are two important features of Can-bus that shouldn't be affected while improving the security level of the protocols and systems. These solutions need more work in order to find solutions that are suitable for autonomous vehicles.

IV. FUTURE OF CAN-BUS IN AUTONOMOUS VEHICLES

Autonomous vehicles still are not on our roads and that's because of many reasons that some are fundamental and other reasons come with each technology such as CAN-BUs. There are many works that are maintained in order to overcome these obstacles.

In terms of fundamental reasons, there are five main obstacles that have not yet been overcome. These obstacles are shortly mentioned as following:

- **Sensors:** Autonomous vehicles use a broad set of sensors that are able to see the environment around and help in detecting objects such as pedestrians. The data that comes from the sensor feeds data back to the car's control which in turn a decision is made. The main challenge is that sensors have a big accurate detectability of objects, distances, speeds and the whole environment.
- **Machine Learning:** The data that comes from the sensor will be trained, tested, classified and predicted by artificial intelligence. These models should be effective in making decisions in order to not make a risk to human lives. But at the moment there is no widely accepted and agreed basis for ensuring that the machine learning algorithms used in the cars are safe.
- **Open Roads & Intersections:** The new and continuous learning are required by these autonomous vehicles because once these vehicles are on roads, new shapes of roads, intersections and objects will be around. Is the car able to recognize these new roads and objects in a safe manner with real time? This is the main obstacle that needs a clear answer.
- **Regulation:** Actually, one of the important things to be maintained is having sufficient and international standards and regulations for autonomous systems and vehicles. Unfortunately, these regulations still do not exist in any industry.
- **Social Acceptability:** The last reason is obviously clear which mentions the way people should be involved in this subject and how to make decisions about these types of vehicles especially while some challenges and difficulties still exist.

These are several fundamental obstacles of the autonomous vechiles, Although these are not our subjects but CAN-Bus

still is one of the other obstacle for the future of autonomous vechiles since it is used widely now in our vehicles.

As mentioned in this article, one of the main challenges of the CAN-Bus network and protocols is the security. Many securtiy actions must be taken in order to minimize the effect of attacks on these networks and to make Can-bus able to be involved Online and in autonomous vehicles in general.

Other obstacles are exists that make CAN-Bus network and protocol still not yet ready to be me implemented in CAN-Bus[16] which summarized as following:

- ➔ Autonomous vechiles use big sets of sensors and cameras to be able to detect objects and see the whole environment. Increasing the amount of sensors leads to a very complex cabling effort and to more weight and material consumption. This means higher assembly and material costs as well as additional fuel consumption for the vehicle. With a growing amount of cabling, the complexity of shielding the wires will increase. This is considered one of the difficulties of CAN-bus especially its advantage is low cost and less wiring.

- ➔ As knowon, Can-Bus protocols use the method of priorities in order to receive data from ECUs. For autonomous vechiles, there is also the problem when assigning priorities to the messages, which are transported over the bus[17]. In most cases, no issue will occur for those messages with a low identifier. Messages with a low identifier will most certainly be transmitted. Messages with a high identifier however might be delayed or suppressed completely. This delay might end up with many risks that could affect human lives and the environment.

- ➔ As known, the Can-bus network uses a copper-wire based bus system. With autonomous vechiles, the number using a copper-wire based bus system will increase with every single addition. Although the price dropped somewhat over the past few years, the cost will be a factor in the future [18]. The electronics within a vehicle are increasing and so is the effort to protect the systems from these interfering signals, which can lead to a system failure in the worst case. Malfunctions in a vehicle often originate in the electronics of a vehicle. External interferences and especially electromagnetic impulses can pose a serious threat to the electronics [19]. So this is also considered to be a big challenge for Can-bus networks that should be taken into consideration. Some works are excited that suggested using optic data bus communication for Can-bus [16].

These are several challenges and difficulties for Can-bus, with the security risks that were first mentioned in the article. In order to reach a good use of CAN-bus network and protocols many edits need to be made. These edits include security edits, wiring edits , network topology changes and also modifying on Can- protocols. These remain as challenges form more research opportunities in order to solve the mentioned obstacles.

V. CONCLUSION

Although some existing possible solutions are available to secure Can-Bus systems and their protocols. Achieving the CIA triad is the first step for achieving security level and then the ability for Can-bus to be used wirelessly in autonomous vehicles could be achieved. This research paper discussed some of the challenges and complexities of CAN systems and protocols especially while dealing with connected vehicles, internet of things and cloud computing.

REFERENCES

[1] CAN Bus Explained,(2021). Css Electronics. CAN Bus Explained - A Simple Intro (2021) (csselectronics.com)

[2] Figueroa-Lorenzo, S., Añorga, J., & Arrizabalaga, S. (2020). A survey of IIoT protocols: A measure of vulnerability risk analysis based on cvss. *ACM Computing Surveys (CSUR)*, *53*(2), 1-53.

[3] R. Buttigieg, M. Farrugia, and C. Meli, "Security Issues in Controller Area Networks in Automobiles," in 18th international conference on Sciences and Techniques of Automatic Control & Computer Engineering, 2017, pp. 21–23.

[4] T. Hoppe, S. Kiltz, and J. Dittmann, "Security Threats to Automotive CAN Networks -- Practical Examples and Selected Short-Term Countermeasures," in SAFECOMP 2008 : 27th International Conference on Computer Safety, Reliability, and Security, 2008, pp. 235–248

[5] Avatefipour, O., & Malik, H. (2018). State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vulnerabilities. *arXiv preprint arXiv:1802.01725*.

[6] Tindell, K., & Burns, A. (1994, September). Guaranteeing message latencies on control area network (CAN). In Proceedings of the 1st International CAN Conference. Citeseer.

[7] Stallings, W., & Tahiliani, M. P. (2014). Cryptography and network security: principles and practice (Vol. 6). London: Pearson

[8] B. Groza and S. Murvay, "Security solutions for the Controller Area Network: Bringing Authentication to In-Vehicle Networks," IEEE Vehicular Technology Magazine, 2018

[9] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno, "Automobile Driver Fingerprinting," in Proceedings on Privacy Enhancing Technologies, vol. 2016, no. 1, pp. 34–51.

[10] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proceedings - IEEE Symposium on Security and Privacy, 2010, pp. 447–462.

[11]]S. Mukherjee, H. Shirazi, I. Ray, J. Daily, and R. Gamble, "Practical DoS Attacks on Embedded Networks in Commercial Vehicles," 2016, vol. 10063

[12] Nilsson, D. K., Larson, U. E., Picasso, F., & Jonsson, E. (2009). A first simulation of attacks in the automotive network communications protocol flexray. In Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08 (pp. 84-91). Springer, Berlin, Heidelberg.

[13] R. Kammerer, B. Frömel, and A. Wasicek, "Enhancing security in CAN systems using a star coupling router," in 7th IEEE International Symposium on Industrial Embedded Systems, SIES 2012 - Conference Proceedings, 2012, pp. 237–246

[14] Q. Wang and S. Sawhney, "VeCure: A practical security framework to protect the CAN bus of vehicles," 2014 International Conference on the

Internet of Things (IOT), Cambridge, MA, 2014, pp.13-18.doi: 10.1109/IOT.2014.7030108

[15] A. S. Siddiqui, Y. G. J. Plusquellic, and F. Saqib, “Secure communication over CANBus,” in Midwest Symposium on Circuits and Systems, 2017, vol. 2017–Augus, pp. 1264–1267.

[16] Kraus, D., Leitgeb, E., Plank, T., & Löschnigg, M. (2016, July). Replacement of the Controller Area Network (CAN) protocol for future automotive bus system solutions by substitution via optical networks. In 2016 18th International Conference on Transparent Optical Networks (ICTON) (pp. 1-8). IEEE.

[17] E. Mayer: Serielle Bussysteme im Automobil, Sicherer Datenaustausch mit CAN, Elektronik Automotive 4, 2012, pp. 5-8, http://vector.com/portal/medien/cmc/press/PressReport-SerielleBussysteme-DE.pdf, last accessed date 12/04/16.

[18] Copper Prices Forecast: Long Term to 2025 – knoema.com http://knoema.de/prujshc/copper-prices-forecast-long-term-to-2025, last accessed date 14/04/16.

[19] Robert Bosch GmbH: Bosch Automotive Electrics and Automotive Electronics: Systems and Components, Networking and Hybrid Drive (Bosch Professional Automotive Information), 5th Edition, Springer Vieweg, Nov. 2013.