DESIGN AND DEVELOPMENT OF ANTI-LOCK BRAKING SYSTEM FOR ELECTRIC VEHICLE

Ch. Shyamala, D.V.S.Ram Krishna, P.Supriya, G.Sahith

Abstract:

Modern automobiles are more than just mechanical gadgets. Because of the connectivity which is increased between the vehicular networks and the present outside world, hackers now have more security flaws via which they can cause exploitations of a vehicular network. The CAN network that is controlled area network is a common communication bus protocol that helps ECU that is electronic control units in a vehicular network to communicate with one another. The safety systems which connect to network, on the other hand, are particularly vulnerable to malicious internal or external assaults due to their varied security flaws. This study presents a new way for introducing a Message Authentication System to enhance CAN security. The electric vehicle is basically driven by the lithium-ion battery coupled to hub motor. The motor needs a power supply to run which can be from an array of source. Electric vehicles do not emit any carbon dioxide because they are fuelled by electricity rather than any other fuel. Carbon dioxide contributes to the greenhouse effect. The design of the electric vehicle includes Hub motor which is brushless dc motor the outer part which rotates is called rotor and permanent magnets is used above the rotor inner part is called as stator and windings are used above it. Hence hub motors are dc motors as they work on dc voltage. Lithium-ion battery is made up of anode, cathode, electrolyte and two current collectors (positive and negative). Li-ion batteries can be recharged 100 times and are more stable. Henceforth, high efficiency with less noise and environment friendly electric vehicle is designed. The method that is proposed and implemented in a MATLAB and Simulink of CAN-based in the networks of the vehicle design along with ABS. By introducing additional security characteristic information unique to each transmitted CAN packets, model that applies Authentication of messages with a safety mechanism for any unknown detection that is intruded. The suggested method's result analysis revealed the fact that the feature which is security that has been proven to be very effective method that detects and blocks any third-party that has been intruded into the anti-lock braking system through the controlled area network bus protocol, The stability is maintained between all coupled Electronic control units. Hence method that is implemented with the design of electric vehicle gives the best results of the output.

1. INTRODUCTION:

To meet the growing demand for increased vehicle comfort, safety, security, and intelligence, vehicles are being revolutionised by the integration ECUs (electronic control unit) which enhances different features such as the net connectivity, the controlling of voice, automated navigation system and so on. In order to establish a sustainable energy system, the amount of renewable energy must be increased. By using controlled or smart charging, electric vehicles can become a valuable asset to the power system, serving as flexible consumption for a variety of grid services. Integration of electric vehicles into the power system may help to prevent the self-inflicted negative impacts of EVs in terms of increased grid load, and make the EV an active component in maintaining a stable, cost-effective power system based on renewable energy sources. so the electric vehicle design is implemented with this method by using CAN protocol. The CAN Protocol includes five error-checking methods: three at the message level and two at the bit level. The fundamental benefit of the CAN Protocol is broadcasting messaging, which means that any node on the network can send and receive messages and assess whether or not they are relevant. The primary concept is that automobiles may communicate with the outside world using smart gadgets. As vehicles link to the internet, this causes a slew of security risks. The primary purpose of the is to send crucial information (such as accident reports) to cars with guaranteed latency and accuracy. However, as explained in, this is a difficult process. The CAN protocol is widely used for controlling and supplying numerous functions to a vehicular system through in-vehicle communication. Broadcast communications underpin CAN. Messages do not have an authentication mechanism, and encryption is not used. A single node that can cause the entire IN VEHICLE NETWORK at risk because there are no security measures in place. If we consider the three different protocols like attacks if they pose threat on non-critical bus protocol then the networks that are present are like LIN that may cause software navigation and other threats. if the attacks were on the networks such as the critical networks, then the flex ray networks that may fail to function the important parts of the system and consider the application that are based on ABS that it may not provide the driving safety. Blockchain is a secure system that is impervious to data manipulation. It has decentralisation, transparency, open-source autonomous, immutable and anonymous. Now the blockchain if it is considered to be the hybrid block chain then the meaning g the hybrid block chain is that both the public and private is combined as now data is authenticated within the vehicles that are autonomous when they travel in a decentralised manner. A secure framework that is resistant to data modification is block chain. We'll look at a hierarchical (or hybrid) block chain, which is a mix of public and private chains. A secure framework that is resistant to data modification is block chain. We consider a hierarchical (or hybrid) block chain, in which public and private blockchains are combined, so that data can be securely processed within autonomous vehicles while they move decentralised. To improve the security features of the electric vehicle, the security based approach of messages has been implemented using CAN bus protocol for ABS.

2. WORKING OF AN ELECTRIC VEHICLE

The electric vehicle which is driven with the help of the battery coupled to electric motor. The motor needs a power supply to run which can be from an array of source. Electric Vehicles are powered by electricity rather than any fuel which means that they do not produce any carbon dioxide emission Carbon dioxide contributes to the greenhouse effect and is known as the "Most important long lived forcing of climate change. As the cost for maintaining the electric vehicle is comparatively cheap when compared to maintaining an internal combustion engine vehicle.

Main principle: It works on the principle that the electromotive force of an A.C. motor which receives electrical energy stored in D.C. battery is converted with the help of D.C. to A.C. converter.

The wheel is driven by the rear wheel. Thus, the electric bike is mobilized by using electric power. Where and how to magnetize the windings is decided by Hall Effect sensor. Hall Effect sensor is mounted on stator as the main principle of the Hall Effect sensor is to sense the permanent magnets and they generate a feedback signal. This feedback signal is given as input to controller and controller in turn generates a response signal which is a DC signal. The response signal is a DC signal through windings of stator and magnetizes the windings or slots. Now the hub motor starts rotating. Controller is a circuit board through sensor and firm away manages the voltage and current input and output and controls all the critical functions of the Electric vehicle. Controller main principle is to transform the battery's direct current into alternating current. The lithium-ion battery which is used for the designing of the electric vehicle as it can withstand higher voltages and currents and it can be recharged to 100 more tines and more stable. Hence this is the operation of the electric vehicle.

2.1 Block diagram of an electric vehicle

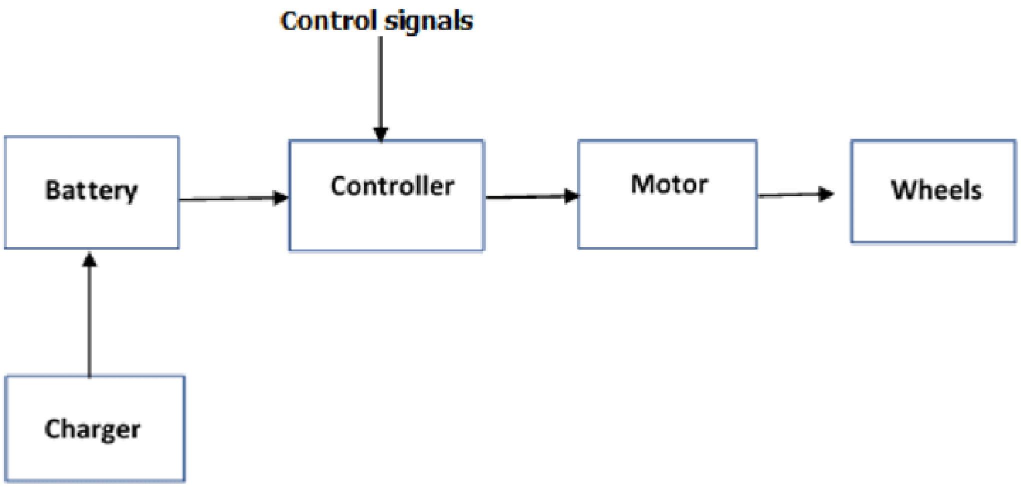


Fig 1: represents the block diagram of the electric vehicle

The block diagram of the electric vehicle consists of the parts

- Battery
- Controller
- Motor
- Wheels
- Charger

3. In Vehicular Networks

The internal communications networks are in vehicle networks that basically interconnects the different components that are present inside the vehicle. There are different components that are present inside the vehicle for example the sensors, actuators, gateways and the electronic control units. These components that is electronic components use data through a variety of Sensors to perform calculations. The sensors are in built in vehicle to assist in identifying and resolving potential issues, such as those that require repair or maintenance. Sensors are essential in automobiles. Different Sensors provide all of these features to help drivers detect problems early and avoid accidents. There will be the process of exchanging the data during the vehicle operation by the electronic control unit.

TABLE 3: Various protocols used in in-vehicle network communications are compared.

Protocols Types	Bandwidth range	Domain in application	Advantages	Disadvantages
Controlled area network	130 kbps–2 Mbps	It is commonly employed in the motor and core stability areas.	No need for a central coordinator at a low cost	Bandwidth is less
Lin	18 kbps	It's commonly utilized in non-time-critical operations.	Low-cost and simple to implement	Speed is low
Flex Ray	9 Mbps	Advanced chassis control is widely used	Faster and more fault-tolerant than CAN and Lin	Cost is very high
MOST	22 mbps	Frequently utilised in the area multimedia sectors	Extremely fast	Cost is very high
Ethernet	98 Mbps	In the future, it will be widely used in for acquiring high bandwidths	Extremely fast when compared to Controlled area network	Cost per each node is very high

3.1 CAN BUS PROTOCOL: For in-car networks, CAN is a well-known vehicle bus standard. Because of its inexpensive cost and process of developing new, which decreases the wiring harness, it is useful in applications especially in vehicle networks. The Controlled area network protocol which is mainly used for communication bus technology that uses differential signal characteristics to deliver messages. It's been effectively widely used in a variety of applications since its inception in the late 1970s, however it is most recognized for its use in automobiles in in vehicle networks. It's a multi-enhanced single-bus protocol in which only one way communication(serial) that delivers simultaneously the information the nodes that are connected on a bus, handles bus contention with a non-destructive bitwise arbitration procedure, uses a primary considered messages are identified with priority scheme, and can transmit the information at the speed which ranges from 45 Kbits/sec to 2. Gbits/sec.

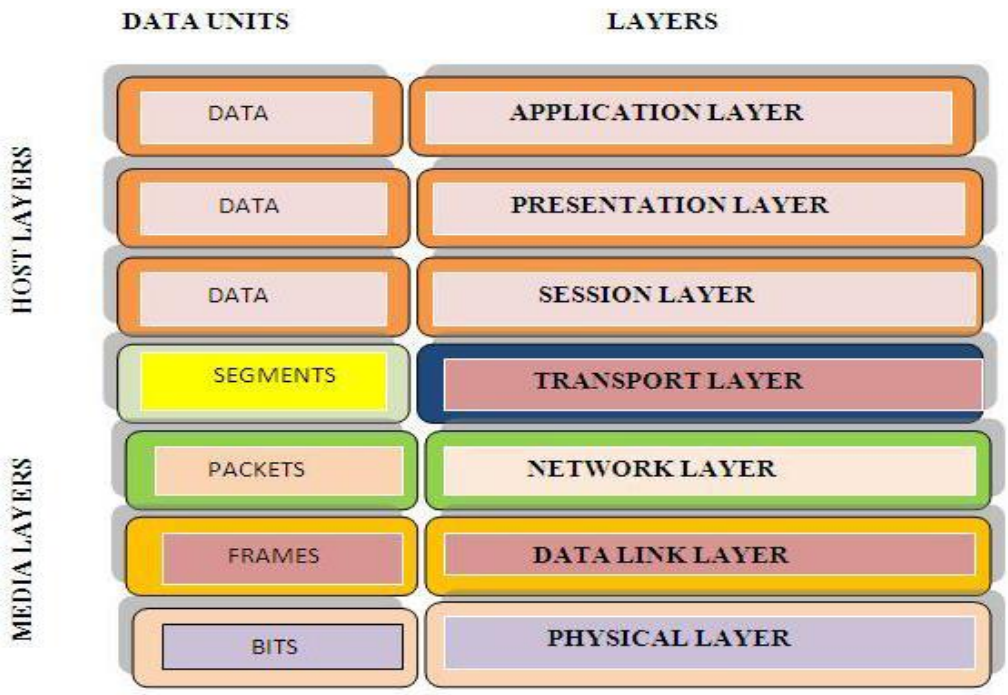


Fig 2: Representation of Layers of CAN Protocol

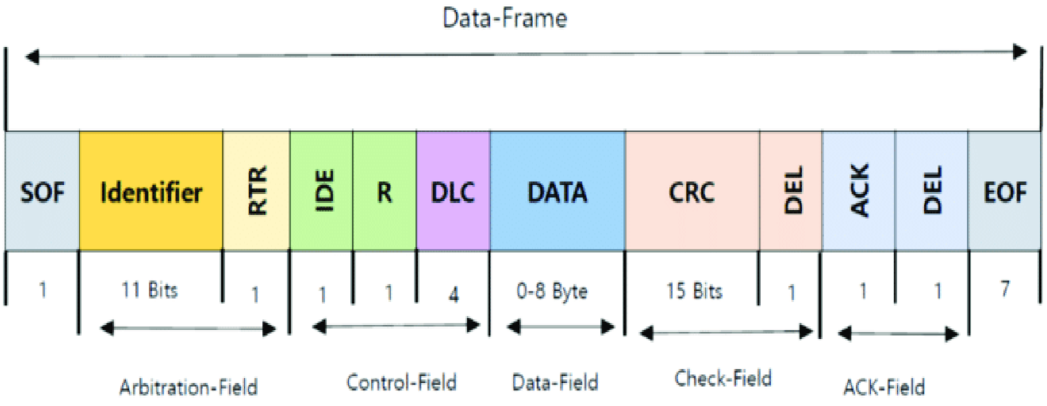


Fig 3: CAN Protocol Frame Format

- **SOF** – Start of Frame
- **Identifier –** The Data Frame's Priority is determined by a Message Identifier.
- **RTR – Remote** Transmission Request, specifies the type of frame (data frame or remote frame). For data frames, it must be dominant (0), while for remote request frames, it must be recessive (1).
- **IDE –** For the base frame format with an 11-bit identifier, it must be dominant (0)
- **R –** The bit which is reserved must be dominant (0)
- **DATA –**User defined data
- CRC – cyclic redundancy checks for error (data corruption) detection
- **ACK** – receivers acknowledgement
- **DEC-** data length code
- **EOF - end** of the frame

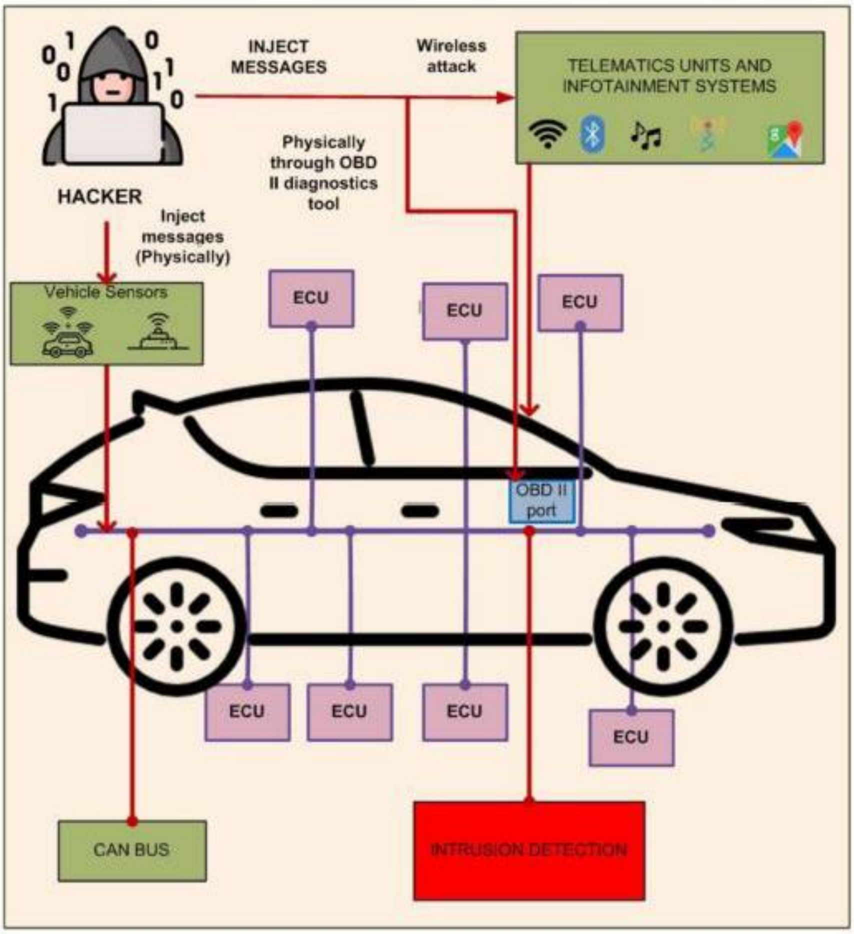


Fig 4: controlled area network bus attack interfacing

3.2 Automotive ethernet protocol:

In response to more requirement of BW (bandwidth) for present technology-based vehicles, hence this protocol named automotive ethernet was introduced as integral part of car networks. This protocol is an important protocol for next-generation in the networks of in vehicular networks and it can handle the demands based on bandwidth of several applications, automatic cars, and on critical situations based on like improved driver assistance systems (ADAS). Whenever there is new launching of the vehicle in market then once the vehicle is launched there is no scope of changing the protocols. As a result, procedures and requirements should be used with caution during the architectural process. Because the protocols which are basically the bus protocols are insecure, there is room in this nascent technology for improved security measures.

3.3 FLEX RAY PROTOCOL

Flex Ray is a dependable, time-triggered protocol that provides up to 10 Mbps of bandwidth versus 1 Mbps for CAN networks. The electronic control units that are connected using the flex ray protocol are synchronised to world - wide time, and data packets that are transmitted and acquired within a certain mentioned time periods. Flex ray protocol has a greater impact level of failure tolerance. This protocol is not designed to protect against external threats. These characteristics help with network security, but they don't guarantee security against attacks.

4. ABS (Anti-lock braking system)

ABS has now achieved one of the common standards and important application in the path of vehicles and automobiles industry. These devices are designed to keep the wheel from slipping during hard braking or low friction situations. Because their goal is to keep the wheel from locking, the systems are sometimes referred to as ABS System. To illustrate wheel’s skidding behaviour in relation to the surface of the road, the distance which is named as the braking distance and coefficient of friction are commonly used. When brakes are applied, it's an empirical model that shows how vehicles Wheel Friction changes with respect to slip which is in terms of relativeness. The following is a schematic diagram.

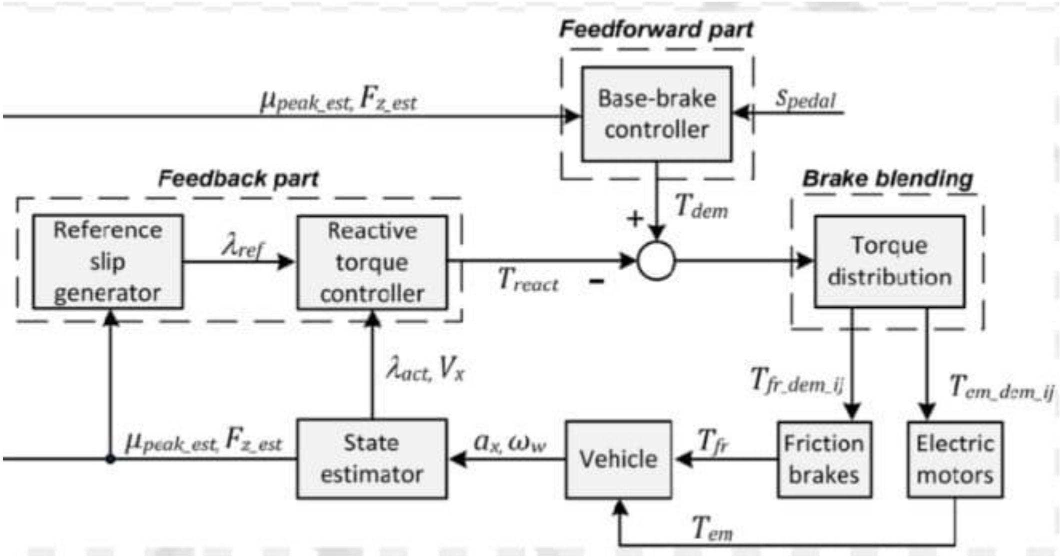


Fig 4.1: Anti – Lock Braking system

4.1. Security Peculiarities of CAN Protocol

The lack of a secure way to protect all the coupled electronic control units from dangerous attacks over the in vehicular networks, according to several experts, is the most serious security flaw in the CAN protocol. Message spoofing is also considered a significant insecurity to in vehicular networks because it leads a way to hackers to transmit false messages for a system such as a commandeer the vehicle's security and important functions of control systems. This is possible because of commonly exploited flaws in the CAN protocol, some of which are listed below.

- **Identity Authentication:** The CAN protocol lacks any method of message identification that secures the vehicle and that has the ability to identify the message sender, that has been prone to threat to the Controlled area network bus likely to recap attacks and the messages that are faked by any unauthorised device that is connected.
- **Encryption of the data**: The protocol that is controlled area network which does not provide an encryption feature to ensure all the electronic controlled units messages secure and private. As a result, any unauthorised device can listen in on IVN transmissions.
- **Insufficient network integration**: the main advantage of controlled area network is that it supports the multi- master bus which is line by line(serial) communication that is coupled to all the electronic control units. the data or the messages that are transmitted over a network this network is basically a single network and any number of electronic control units that are coupled on the network that can transmit messages to any other ECUS that are coupled on the same network. As it is analysed that the network which is open to other devices allowing the other devices that are connected to inter communicate with safety units. hereby the attacker is likely to use Controlled area network wires to get access for the all over network.

5. PROPOSED METHOD

5.1 Modelling of an anti-lock braking system Using the controlled area network

The modelling of the system is performed in Matlab and Simulink TM libraries so that to mimic for in vehicular networks environment for the anti-lock braking system using the controlled area network. Simulink blocks that were utilised to build the model are listed below. Fig. The source blocks include:

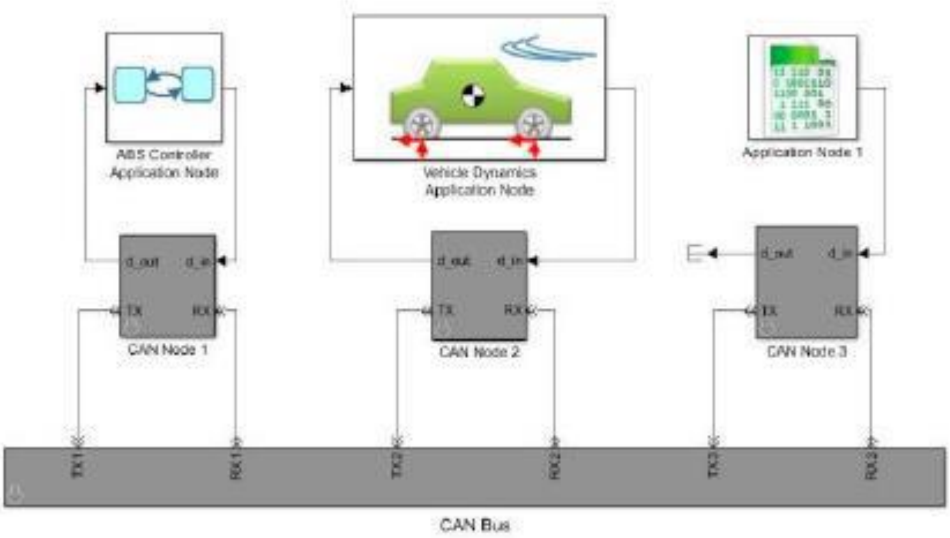


Fig 4.2: Controlled area network designed with ABS

- It basically consists of three nodes

1. The ABS controller node
2. Vehicle dynamic node
3. Application node

- The vehicle dynamic node the name itself indicated that the node simulates the dynamic behaviour of the vehicle. this node is particularly relays on the critical function or the control signals that are acquired from the anti-lock braking system controller.

- The controller node that is anti -lock braking system controller block is in the charge of sending the proper controlled signals or the messages to the dynamic block of the vehicle so that the braking action will work properly. The ABS is built by coupling of the node which is anti -lock braking system controller and dynamic node of the vehicle.

In sending and receiving the messages via the controlled area network bus protocol in the real time the remaining node that is the application node basically mimics the nature or the action of the electronic control units that are present.

5.2 Implementation of the Security Feature based on Unique Message Authentication method

One of the main security concerns with the CAN protocol is the inability to identify the messages and provide security feature. The model can be used to simulate this security flaw. The diagram below depicts the problem has paved a way to hostile threat to controlled area network bus protocol traffic.

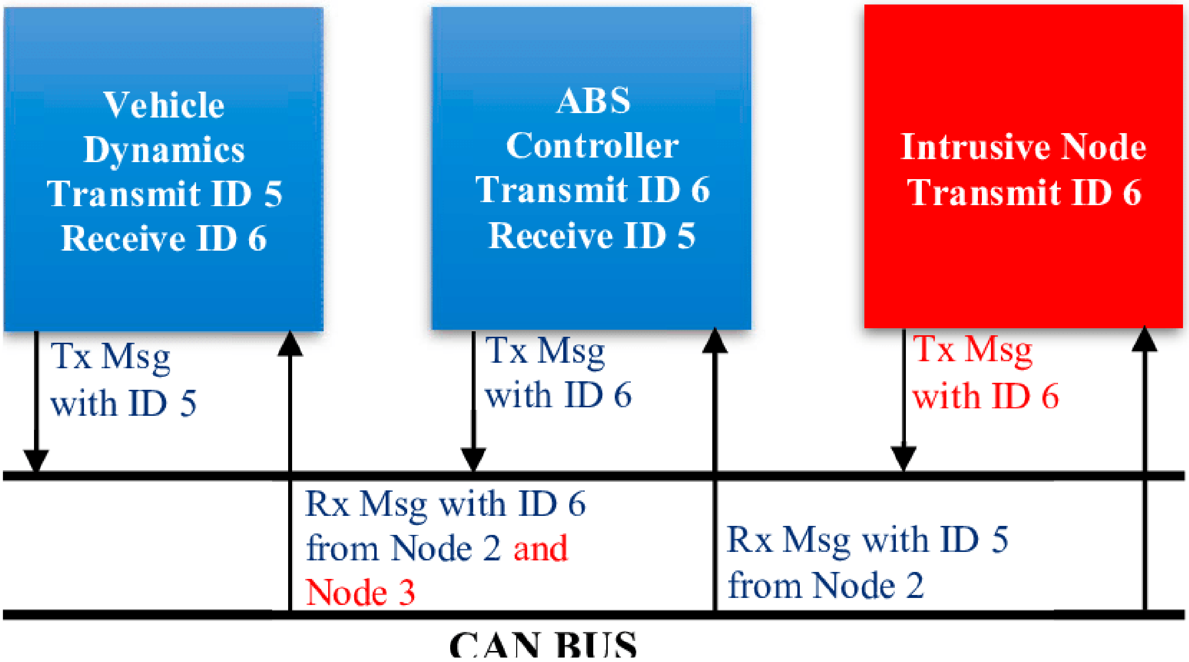

Vehicle Dynamics Transmit ID 5 Receive ID 6
ABS Controller Transmit ID 6 Receive ID 5
Intrusive Node Transmit ID 6
Tx Msg with ID 5
Tx Msg with ID 6
Tx Msg with ID 6
Rx Msg with ID 6 from Node 2 and Node 3
Rx Msg with ID 5 from Node 2
CAN BUS

Fig 4.3: CAN bus security breach

In-vehicle networks use CAN as a broadcast bus. CAN controllers broadcast their messages to all connected nodes, and each receiving node uses an acceptance filter to determine whether the message is acceptable. To ensure that the highest priority messages are transmitted first, CAN uses a priority-based CSMA/CA media access method. To detect bus errors caused by electromagnetic fields, CAN provides an error broadcast mechanism that uses an error frame to detect transmission errors. The CAN controller also includes mechanisms for automatic backoff, such as disconnecting a faulty status. In terms of security, our focus is on guaranteeing message authenticity and integrity toward a spoofing attack. We do not address eavesdropping. In the following, we give two examples of our expected use case of spoofing attacks. The present design contains 2 primary nodes, the Anti-lock braking system controller and the (VDA) nodes, which Interacts with one and other in real time, and each node's behaviour and input is influenced by the output of the others. The method devised is shown in the diagram below. The method that is proposed in which every transceiver is also provided with an ID which is hard-coded and unique that provides a number that is random, which has ability to create a unique 2^8-bit hash code. moreover, if we consider the CAN frame the number of bits is limited, including the 2^8-bit information is difficult. The complete 2^8-bit hash code is broken down into 2^5 single-byte tiny pieces to solve this problem, one of which is chosen at random, along with its location. This information is stored in CAN frames and sent over the CAN bus. For the purpose of encoding, it requires 2 bytes from the CAN. One of the following schemes can be used to accomplish this:

- Scheme 1: Use the 8-byte data field's last two bytes.
- Scheme 2: Add two more bytes just before the data field to the controlled area network frame

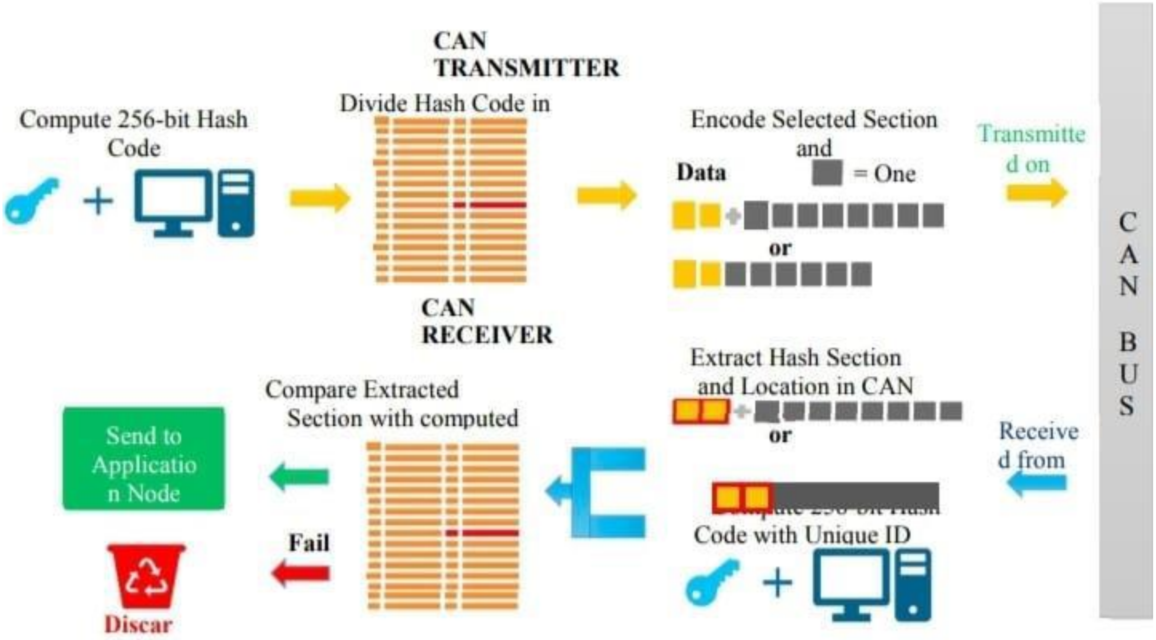


Fig 4.4: Represents the Unique Authentication Security Feature Concept

The CAN trans receiver that is present on the receiving side will perform the decoding of the data which compares to the its hash code that is generated by it first and then it then extracts data from the frames and send it to the appropriate application based on the matching data. If the information does not match, now the Frames of the CAN will be discarded.

The safety application attributes that are introduced in the transceiver node block of the CAN. The transmitter and reception parts are separated. Each transmitted CAN frame is encoded with hash information by the transmitter portion. After successfully acquiring the a Controlled area network packet, the information that is encoded are retrieved and are provided to the freshly established 'hash Verification' Simulink and matlab code block in the receiver section.

6. Simulation Results and Discussion

6.1. Case study scenario 1: Anti-lock braking system without the implemented Security Feature and without the Intruded node.

The design of the ABS is done in Matlab and Simulink based on CAN bus protocol. the simulation is first performed without and safety measures or security method implemented and there is no intruded node introduced. The results are shown in the below graphs in which the speed of the wheels of the vehicle is fluctuating and the vehicle speed decreased. During hard braking or whenever sudden brake is applied to the vehicle the vehicle speed is reduced suddenly as shown in the graph but the wheel speed is gradually decreasing so that the wheels of the vehicle is locked there will be no skidding of the vehicle. If we consider the figure 5(b) in which the graph represents the number of messages that are received and the number of intrusion messages as we know that in the case study 1

there is no security feature implemented and there is no intrusive node that is introduced hence the number of intrusion messages are equal to zero and the received messages are increasing linearly with respect to time

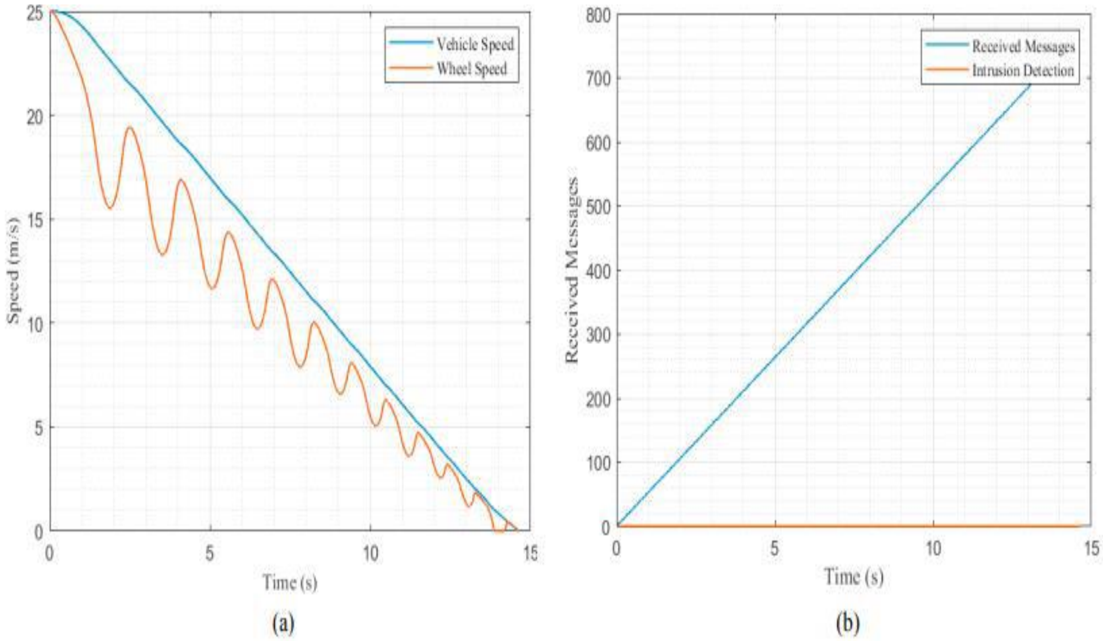


Fig. 5. Results of Test Case Scenario 1 (a) Vehicle and Wheel Speed during braking; (b) Messages received by the Vehicle Dynamics Node

6.2. Case study scenario 2: ABS with intruded node and without security

The intrusive node signals are depicted by the vehicle dynamic node and as soon as it detects it starts sending them at the simulated time of six seconds. the messages are now accepted and the dynamic node of the vehicle analyses and depicts the data from there. Here is the solution to the problem that the intruded nod containing of random garbage data in such a case the data is known as ramp data. From the figure below it is clear that when the intrusion of the node takes places due to which there is an injecting of the data into the design.as its clear from the graph that from the anti-lock braking system controller node and the intrusive nodes the vehicle dynamic node receives the messages. This problem arises because of not the correct process that is undergoing in the model for detecting and identifying whether the messages that are received are from the right node or not.

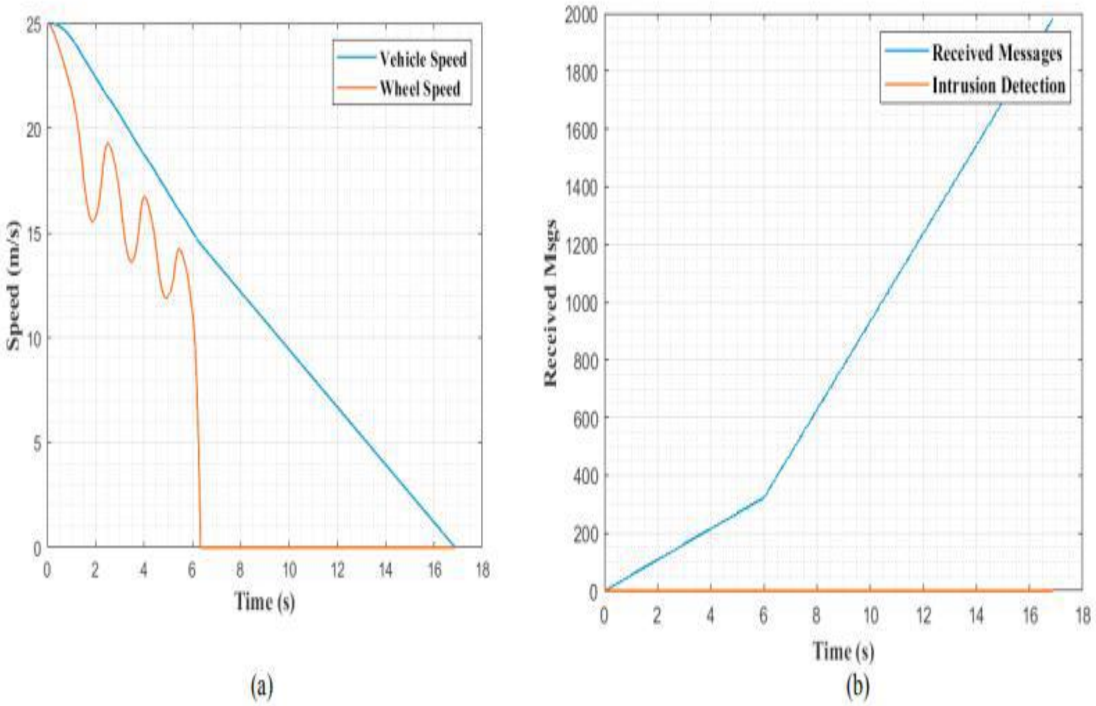


Fig. 6. Results of Test Case Scenario 2 (a) Vehicle and Wheel Speed during braking; (b) Messages received by the Vehicle Dynamics Node

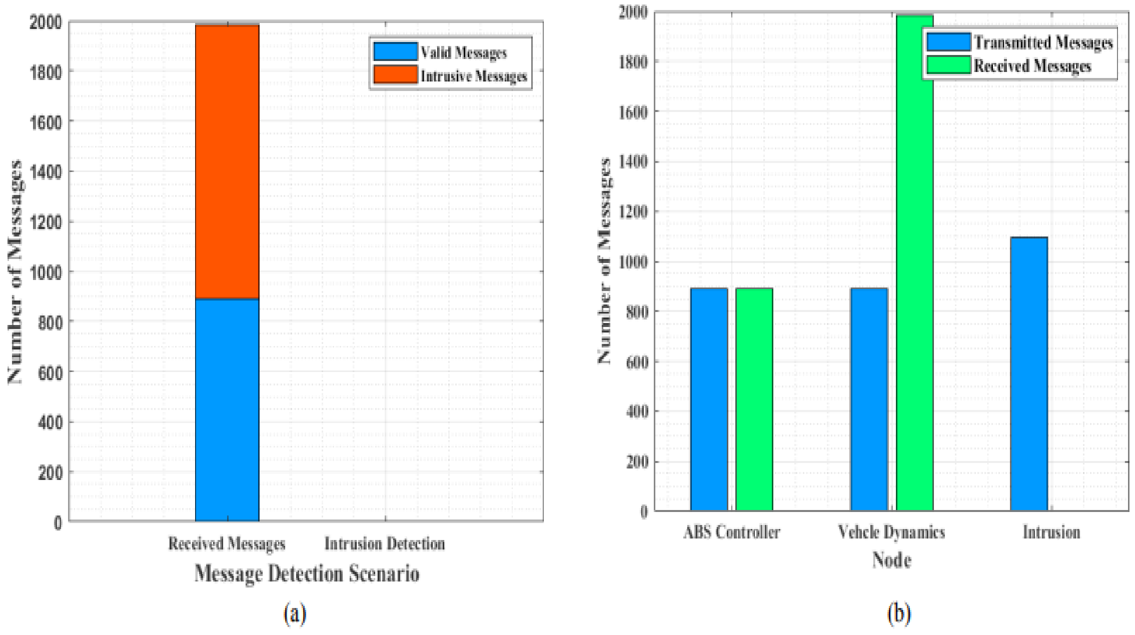
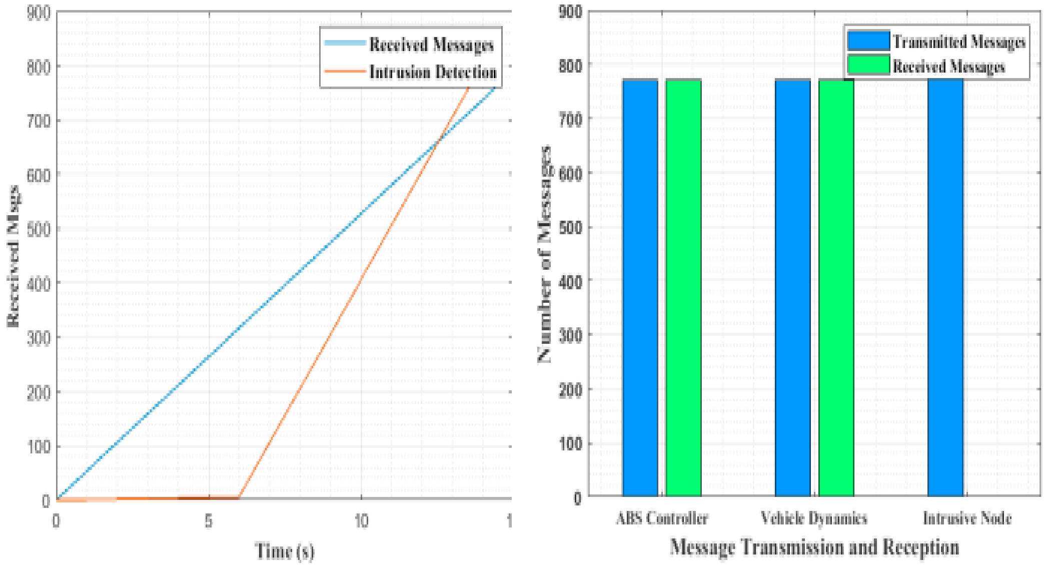


Fig. 7. (a) Vehicle Dynamics Node Message Detection Scenario; (b) Messages Transmitted and Received by each node

6.3. Case Study 3: ABS with Intrusion Detection and Security Feature

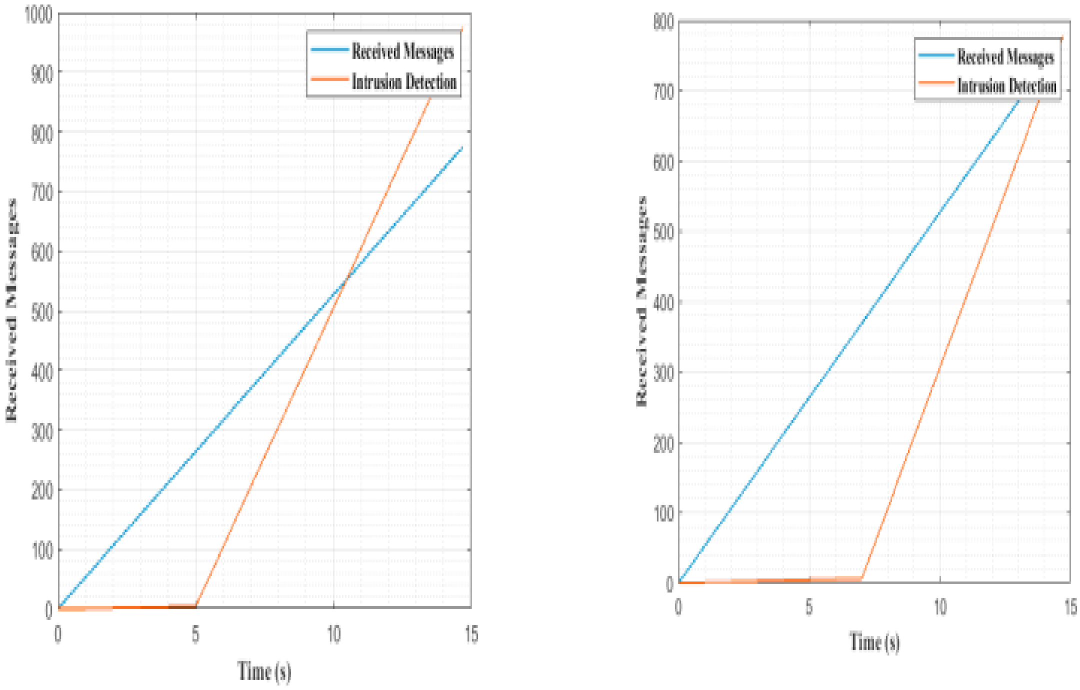
The safety feature is added and one intruded node consider as intruded node 1 that transmits of a time considered after the six seconds, the model is simulated. Figure 8 depicts the results. The Vehicle Dynamics Node, as previously stated, can not only detect but also remove unnecessary messages from the model. This ensures the ABS's integrity by preventing the Vehicle Dynamics node from processing potentially harmful input. The model is put to the test again by adding a new intrusive node with the same settings.

The new node which is intruded node 2 is designed to perform intrusions in the Vehicle Dynamics and Anti- lock braking system Controller node at the same time, as previously stated. Thanks to the Safety improvement characteristics applied to Anti-lock braking System Nodes, the intruded communications that are properly recognised and then deleted, and any problem effects on ABS is not necessary to be included. below shown in Fig the ABS controller node and the dynamics node of the vehicle has now the ability to identify the dynamics intruded data as quick as possibly it is received. (Rate of five sec for the ABS controller a seven sec for vehicle).



(a) (b)

Fig. 8. Results of Test Case Scenario 3 (a) Messages received by Vehicle Dynamics node; (b); Messages Transmitted and Received by nodes



(a) (b)

Fig. 9. Results for two intrusive nodes (a) Messages received by ABS Controller node; (b) Messages received by Vehicle Dynamics node

7. Conclusion

The proposed system uses the brushless hub motor due to which the power consumption is reduced. And the cost of the vehicle is reduced as parts which are taken from the scrap of the best material and lithium-ion battery is used as it has higher voltage capacity and the battery charging time is reduced. Hence the speed of the vehicle is 35kmph and the mileage of the proposed system is 40km/charge by using the above specified controller, motor, battery the low-cost electric vehicle is designed. For the proposed system anti-lock braking system will be implemented so that the vehicle will avoid skidding during hard braking. At the time of sudden brake applied the ABS implemented electric vehicle will have pumping and releasing operation of the wheels of the vehicle so that the vehicle wheels will not get locked. As we can observe that when the vehicle speed decreases the wheels speed decreases gradually. For a NON-ABS vehicle at the time of hard braking the vehicle speed when decreases the wheels speed reduces suddenly and the vehicle starts skidding after 6 seconds. Hence designing of Anti - lock braking system to the proposed system is done in MATLAB and Simulink. As a result, this study has given a MATLAB and Simulink-based CAN model of a car with ABS. The designed model employs the unique message authentication security feature, which provides additional security features to each transmitted message. With the implementation of this approach, all the messages were sent by any intruded node are correctly recognised and they erased, preventing the ABS from being influenced. As a result, the proposed method in the model is used to mimic an effective intrusion detection and prevention system.

REFERENCES

1. L. L. Bello, R. Mariani, S. Mubeen, and S. Saponara, "Recent Advances and Trends in On-board Embedded and Networked Automotive Systems," IEEE Transactions on Industrial Informatics, vol. 15, pp. 1038-1051, 2019

2. M. a. Simulink, "Effects of Communication Delays on an ABS Control System," 2018.

3. R. Currie, "Hacking the CAN bus: Basic manipulation of a modern automobile through CAN bus reverse engineering," SANS Institute, 2017.

4. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, et al., "Experimental security analysis of a modern aut omobile," in 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447-462.

5. F. Li, L. Wang, and Y. Wu, "Research on CAN network security aspects and intrusion detection design," SAE Technical Paper 014 8-7191, 2017.

6. R. Rudd, "Estimating the Mu slip curve via extended Kalman filtering," The Mathematica Journal, vol. 11, p. 91, 2008. [6] O. Avatefipour and H. Malik, "State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vulnerabilities," arXiv preprint arXiv:1802.01725, 2018.

7. I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN -W), 2013, pp. 1-12.

8. H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue, and S. Horihata, "Security authentication system for in-vehicle network," SEI technical review, vol. 81, pp. 5-9, 2015.

9. R. Buttigieg, M. Farrugia, and C. Meli, "Security issues in controller area networks in automobiles," in 2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2017, pp. 93-98.

10. M. a. Simulink, "Effects of Communication Delays on an ABS Control System," 2018.