Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 4, 269-277

A REVIEW ON CONTROLLER AREA NETWORK AND ELECTRONIC CONTROL UNIT IN AUTOMOTIVE ENVIRONMENT

Beniel Dennyson W[1*] Dr. C. Jothikumar[2]
Department of Computing Technologies
bw3332@srmist.edu.in, jothikuc@srmist.edu.in

Abstract:
Security issues are the major part in the Connected Autonomous Vehicles. They are way more intelligent than the cars that runs in the market. Connected Autonomous Vehicles use a technology to steer, accelerate and brake with no human involvement where as people aren't aware or may not know that a car can be attacked. In such cases people might face major issues while driving such as delayed braking or braking failure or ABS failure, failure of the Traction Control System, engine failure or engine may not start. The Electronic Control Unit is a part of all cars and also known as the brain of vehicles. Also, Electronic Control Unit is a communication device which performs operations om the vehicles. Controller Area Network is a bus network which enables each Electronic Control Unit to communicate with all the other Electronic Control Unit without any complex wiring. By connecting these devices to the vehicles, we can find out the vulnerabilities and attacks in the system. I'll be detecting and preventing numerous threats in the Controller Area Network bus network in my research project.

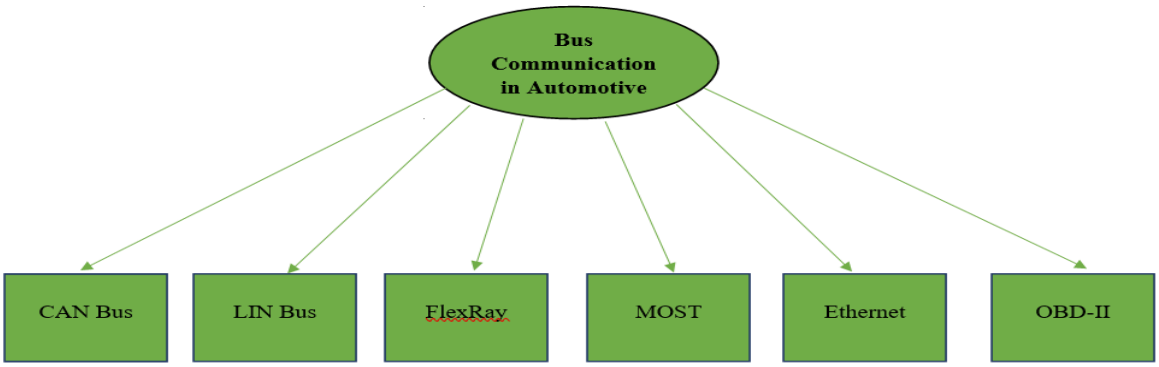
Keywords: Anti-lock Braking System, Wheel Speed Sensors, Controller Area Network bus communication, In-Vehicle attack generation, Electric Control Units.

1. Introduction:

The sophisticated automobile might feature up to 70 electronic control units for various sub-frameworks. The engine control unit is usually the most powerful Central Processing Unit. Transmissions, airbags, antilock braking systems, cruise control, electric power steering, sound systems, power windows, doors, auto-retractable mirrors, battery and re-energizing frameworks for electric cars, and so on are all examples of others. Auto Start/Stop, Electric Park Brakes, Park Assist, and Auto Lane Assist/Collision Control are among the models available.

The CAN transport standard is generally acknowledged and is utilized for all intents and purposes all vehicles and many machines. This is for the most part due to beneath key advantages: Simple and Low Cost: Electronic Control Unit impart by means of a solitary Controller Area Network framework rather than through direct complex simple sign lines - diminishing mistakes, weight, wiring, and expenses. Controller Area Network chipsets are promptly accessible and reasonable. Fully Centralized: the Controller Area Network transport gives one place of passage to speak with all organization Electronic Control Units - empowering focal diagnostics, information logging, and setup. Extremely Robust: the framework is powerful towards electric unsettling influences and electromagnetic impedance - ideal for security basic applications (for example vehicles) Efficient: Controller Area Network outlines are focused on by identity numbers. The first concern information gets quick transport access, without causing interference of different edges. Reduced Vehicle Weight: by the disposal of kilometers of vigorously protected electrical wires and their weight from the vehicle. Easy Deployment: a demonstrated norm with a rich help biological system. Resistant to EMI: this makes Controller Area Netw ideal for basic applications in vehicles.

2. Bus Communication Systems:



2.1. CAN bus:

Can a bus be considered a sequential mode of transportation, since it was invented in 1986 by Robert Bosch GmbH for a part of automobiles which is in-vehicle networks. Twisted wire sets are used by CAN bus, which works to be robust in electro magnetic turbulent situations. Seat operations (low speed) and window operations, management of engine (high speed), brake controlling system (high velocity), the variety of other frameworks employ CAN buses in automobiles. Other embedded control applications that use the CAN bus include processing plant automation, building automation, and aeronautical systems.

2.2. OBD-II:

2.3. OBD-II is the second era of the OBD determination. Since on-board vehicle PCs were presented in the mid 1980's, OBD frameworks have made it conceivable to give the vehicle owner or a specialist admittance to data on the condition of vehicle subsystems. Early executions of OBD observed a couple of outflow related parts and essentially enlightened a breakdown marker light. OBD II characterizes a correspondences convention to give a normalized series of symptomatic difficulty codes (DTCs) through a normalized quick advanced interchanges port. These codes permit a client to recognize and cure glitches inside the vehicle. These are the various sorts of Bus interchanges in the car business. Furthermore, every transport correspondence is identified with various bunches of a vehicle. **LIN bus:**

Since it was established in 1986 by Robert Bosch GmbH for a part of automobiles which is in-vehicle networks, can a bus be called a sequential mode of transportation? The twisted wire sets used in the CAN bus were intended to withstand electromagnetically turbulent conditions. In vehicles, CAN buses are used for seat operations (low speed) and window operations,management of engine (high speed), brake controlling system (high velocity), and a number of other systems. Processing plant automation, building automation, and aviation systems are some of the other embedded control applications that employ the CAN standard.

2.4. FlexRay:

FlexRay is an in-vehicle network's high-speed sequential communication bus. It's a long-winded convention version of byte flight. The drawn-out FlexRay features the performance highlights required for dynamic security, such as repeating transmission channels and a synchronization component that is issue-tolerant. FlexRay can be used in by-wire and brake-by-wire systems.

2.5. MOST:

MOST was created with the collaboration of BMW, Daimler Chrysler and Becker Radio by Oasis Silicon Systems AG (now SMSC) for applications of multimedia in automobiles. A bus system's cycle times are far quicker than earlier automotive bus systems since it was intended to run on optical fiber. This

accomplishment has been made possible by seventeen worldwide automakers and more than fifty important component vendors, including vehicle electrical and audio-video manufacturers, since 1997. MOST buses, among other auto accessories, provide optical solutions for vehicle radios, Compact disc and DVD player's, and Global PositioningSystems.

2.6. Ethernet:

Regardless of the fact that Ethernet isn't widely used in modern vehicles, it has a number of appealing benefits. Ethernet data speeds vary from 10 megabits per second to 100 gigabits per second (a lot quicker than existing car organizations). Likewise, Ethernet is generally utilized outside the automotive industry, so parts and experienced designers are promptly accessible.

3. CAN based attacks and implementations in automotive environment:

3.1 Convolutional Neural Network-Based Adaptive Source Node Identifier for CAN:

For networks of in-vehicle, the CAN works as the de-facto standard. A CAN bus is used to connect electronic control units in a variety of automobiles. The CAN, on the other hand, is subject to security threats because it has an intrinsic secured identifying system. In this paper, we propose a message source identification based on convolutional neural networks (CNNs) [1]. The technique suggested can also be implemented without modifying the CAN protocols since it makes use of the physical properties of the CAN bus channel.They have assessed to the genuine CAN channel qualities utilizing the channel-model through the exhibition of proposed CNN-based msg source identifier, the arbitrary and genuine CAN information design. We affirmed that the proposed plot performs above and beyond different transport conditions without physically predefined include extraction strategies, higher-layer verification conventions or whole CAN signal [14]. The programmed highlight extraction, it can anticipate that proposed plan can give dependable execution in different conditions too. misfortune because of the CNN-based source distinguishing proof mistake can be likewise limited with appropriate settings of identifier. For the work in future, we will stretch out a proposed plan for recognizing different sorts of assaults, for example, transport of and information adjustment assaults.

3.2 Long Short Term Memory - Based Intrusion Detection System for In-Vehicle Can Bus Communication :

An advanced car is complicated innovation piece which utilizes the CAN bus framework as focal framework to deal with correspondence between an Electronic Control Unit. In spite of it's focal significance, the Controller Area Network transport framework doesn't uphold verification also, approval components, i.e., Controller Area Network messages are communicated without fundamental security highlights [2]. Thus, it is simple for assailants to dispatch assaults at the Controller Area Network bus network framework. Assailants can think twice about the Controller Area Network bus framework in more than one way including Denial of Service, spoofing assaults, Fuzzing. It's basic to devise procedures to ensure current vehicles are against the previously mentioned assaults.

3.3 MAuth-CAN: Masquerade-Attack-Proof Authentication for In-Vehicle Networks:

Various hacking endeavors on current vehicles have as of late showed that a foe can distantly vehicle control utilizing powerless telematics administrations. With the endeavors, disguise assault mimicking some wellbeing basic ECU is typically performing to control vehicles. Somewhat recently, a few message verification conventions for regulator region organization have been proposed to shield vehicles from disguise assaults. In any case, a few message confirmation conventions are adequately not to secure a vehicle from disguise assaults by compromising Electronic Control Units [3]. Some other conventions which are secured against disguise assaults fill in the network limit of Controller Area Network up to 100% or requires equipment adjustments of the Controller Area Network-regulator, committed equipment utilized for Controller Area Network interchanges. In the paper, we proposed a new validation convention, MAuth-CAN, that it is secured against disguise assaults. MAuth-CAN either tops off to 100% of the organization limit or requires equipment adjustments of a Controller Area Network-regulator. What's more, we proposed a strategy which ensures Electronic Control Units from transport off assaults, and applies

the method to MAuth-CAN for taking care of transport off assaults.

3.4 A Combination of Design Optimization and Secure Communication: Ensuring Safety and Security in CAN-based Automotive Embedded Systems:

As car-installed frameworks included ECU's associated through a CAN has kept on creating, volumes of data these frameworks are needed to deal with have additionally quickly expanded. Digital assaults focusing on weak marks of auto inserted frameworks specifically are on the ascent to impede the typical activity of a vehicle. Be that as it may, adding security components to protect against assaults can't disregard timing necessities in terms of vehicle wellbeing. This is on the grounds that it might prompt an infringement of car wellbeing. To put it plainly, sides of the issue should have been tended from a start of a framework configuration stage, to give ideal security and wellbeing [4]. As reaction to the major problem, they proposed a novel and productive plan. A planned improvement during a framework configuration stage not just guarantees all of these real-time applications have executed inside the cutoff time yet additionally lessens the quantity of sent msg over the CAN bus. We add a HMAC to explicit messages after streamlining, ensuring safe communications between ECU and protecting against digital attacks [8]. The suggested conspiracy can counter attacks on the CAN transport while achieving time requirements, according to security analysis and test findings. In this manner, our proposed plot is successful in fulfilling the improvement of both wellbeing and security.

3.5 An Intrusion Detection Method for Securing In-Vehicle CAN bus:

CAN bus has became the most utilized convention in-car networks since it's heartiness as well as effectiveness. In any case, CAN transport doesn't have enough security successes to ensure the entire car framework even to secure its organization. Thus, security instruments to secure CAN bus turned into a crisis need. One of the productive strategies for getting the Controller Area Network bus is an IDS Framework. In the following work, a straightforward interruption recognition strategy for a CAN bus is proposed [5]. As the calculation doesn't requires any change in the standard method of Controller Area Network bus neither to be carried out in every adding machines to organization. To protect against vehicle assaults, new security approaches has been implemented in the writing. In any case, the larger part requires equipment adjustment or execution in each ECU. In the following work, they propose a basic interruption location strategy for CAN bus IDS [11]. Our system depends on the investigation of periods messages. The fundamental thought is to carry out an IDS which actually takes a look at the CAN ID of the sent message then, at that point, works out the time stretches from the most recent one. Likewise, in this paper, they gave a general outline about assaults, their characterization, and a few instruments to shield against them. The benefit of their strategy is that doesn't need a change in equipment layer and execution in each ECU. As the viewpoint of the work, they mean to play out the propose technique to distinguish Do's assaults and to the other kind of assaults.

3.6 Intrusion Prevention System of Automotive network CAN bus:

Car networks dependent on the CAN transport (ISO-11898) group of conventions has been demonstrated to be helpless against taking advantage of by programmers who has been outside the vehicle. The organizations could be compromised in the way that can imperil vehicle inhabitants. The acclaimed exploit drove to an exorbitant auto review that impacted in excess of 1,000,000 vehicles. Different endeavors can permit lawbreakers to take vehicles without truly breaking them [12]. Where no fatalities has yet happened, programmers can trigger an occasion which prompted mishaps including genuine injury or even demise. The CAN transport interfaces ECUs, some of which are needed for security and outflows frameworks, for example, the antilock slowing down and fuel infusion frameworks. As well as controlling required capacities, other ECUs give purchasers arranged highlights, for example, infotainment and lighting. Regardless of whether the production line is introduced or secondary selling additional items, each ECU brings assault vectors into the by and large auto organization. This examination centers around getting these vehicle organizations, explicitly the CAN transport [15]. This paper will examine the current weaknesses and depict our plan for a continuous interruption counteraction framework (IPS) that kills

assaults by effectively observing the CAN transport and dispense with pernicious messages.

3.7 Techniques in hacking and simulating a modern automotive controller area network:

This evaluation will depict the planning and implementation of a benchtop test system, as well as hacking tactics on the modern vehicle network. The essential organization in currently delivered vehicles is based on the Controller Area Network (CAN) transport described in the ISO 11898 series of standards [13]. The CAN transport works effectively in the advanced vehicle's electronically raucous environment. While CAN transport was wonderful for data exchange in this context when the convention was organized, security was not a concern due to the organization's anticipated isolation. Later, publicly publicized attacks in which programmers were ready to remotely control a car disproved that theory, requiring an item review that affected over 1,000,000 automobiles [7]. The car features a significant number of electronic control units (ECUs) that are connected to the CAN transport to control many frameworks such as the infotainment, lighting, and motor systems. The CAN transport allows ECUs to share data in the same way that a standard transport does, which has resulted in improvements in fuel and discharge efficiency, but it has also introduced flaws by allowing access to digital actual frameworks on the same organization (CPS). These CPS frameworks include anti-lock brakes and, on late-model vehicles, the ability to turn the steering wheel and the gas pedal. Testing usefulness on a working vehicle can be dangerous and put people in peril, but recreating the vehicle organization and functionality of the ECUs on a seat top structure provides a safe way to test for flaws and possible security solutions to prevent CPS access over the CAN transport network. This paper will portray momentum research on the auto organization, give strategies in catching organization traffic for playback, and exhibit the plan and execution of a benchtop framework for proceeding with research on CAN transport.

4. Anti-lock Braking System:

4.1. ABS Mechanism:

The anti-lock braking system, often known as the ABS, which is vehicle safety device which can prevent the wheels from locking up and sliding uncontrollably during braking. In an emergency stop, modern anti-lock brake systems allow the driver to steer while applying brake, gives them most control over the vehicles. The primary applications of an Anti-skid Breaking System in the car are that it can improve vehicles control and reduces the stopping distance on wet and slick road areas. When braking, an ABS-equipped automobile gives improved steering control since there is less chance of sliding. Without the usage of an ABS system, even the experienced driver's may not be able to keep the car from sliding on the dry and slick roads during quick braking. The ABS system, on the other hand, allows a regular driver to simply keep the car from sliding and acquire greater steering control when braking.

Cadence braking principles and the threshold are used for its operations. Cadence braking can be called as threshold braking, occurs when the driver tries to applies and releases the brakes before locking the wheel, and then again applies and releases the brakes before locking the wheel. To avoid wheel locking and sliding, this operation of applying and releasing the brakes on the wheel is done in pulses. This strategy is used by the driver to gain more control of the car during quick braking and avoid skidding. The ABS system performs cadence braking when the brake pedal is applied to prevent wheel locking and vehicle skidding.

4.2. ECU Mechanism:

The motor ECU, in general, regulates the fuel injection and, in hydrocarbon motors, the situation of the spark igniting. It uses a Crankshaft Position Sensor to determine the state of the motor's internals, allowing the injectors and ignition to fire at precisely the proper time. While this sounds like something that should be possible precisely (and was before), there's something else to it besides that.

An internal combustion engine is basically a major vacuum apparatus that powers itself by utilizing fuel. As the air is sucked in, enough fuel must be given to make the ability to support the engine's activity while having a valuable sum left over to move the vehicle when required. This blend of air and fuel is known as a 'combination'. An excessive

amount of combination and the motor will be maxing speed, too little and the motor can not control itself or the vehicle.

Not exclusively is the measure of combination significant, however, the proportion of that blend must be right. An excessive amount of fuel - too little oxygen, and the burning are filthy and inefficient. Too little fuel - a lot of oxygen makes the ignition slow and frail.

Engines used to have this combination amount and proportion constrained by a completely mechanical metering gadget called a carburetor, which was minimal in excess of an assortment of fixed breadth openings (jets) through which the motor 'sucked' the fuel. With the requests of current vehicles zeroing in on eco-friendliness and lower discharges, the combination should be all the more firmly controlled.

Surrendering control of the motor to an ECU, or Engine Control Unit, is the best approach to achieve these stringent requirements. Instead of using basic means, the ECU controls the fuel infusion, start, and ancillaries of the motor using precisely stored circumstances and numeric tables.

4.2.1. Control of air-fuel proportion:

The majority of modern motors use some form of fuel infusion to provide fuel to the chambers. Based on different sensor data, the ECU determines the amount of gasoline to inject. When compared to ideal conditions, oxygen sensors tell the ECU whether the motor is running rich (too much fuel or too little oxygen) or lean (too much oxygen or too little fuel) (known as stoichiometric). When the gas pedal (gas pedal) is forced down, the choke position sensor tells the ECU how far the choke plate is opened. The mass wind current sensor calculates the amount of air passing through the choke plate and into the motor. Whether the motor is hot or cold is determined by the temperature of the motor coolant. If the engine is still cool, more fuel will be injected. In the float bowl of the carburetor, a blend regulation solenoid or stepper engine is gathered, but air–fuel mixture management of carburetors with PCs is established with a relative guideline.

4.2.2. Control of idle speed:

Inactive speed control is built into most motor frames' ECUs. The driving rod position sensor measures the motor RPM and plays an important role in the motor's planning capabilities for fuel infusion, sparkle events, and valve timing. A programmable choke stop or a passive air side step regulation stepper engine limit inactive speed. Early carburetor-based frameworks used a bidirectional DC engine with a programmable choke stop. An inactive air control stepper engine was used in early choke body infusion (TBI) frameworks. In order to ensure successful passive speed control, the motor burden must be expected out of gear. A full-power choke control framework might be utilized to control inactive speed, give journey control capacities, and maximum velocity impediment. It additionally screens the ECU area for dependability.

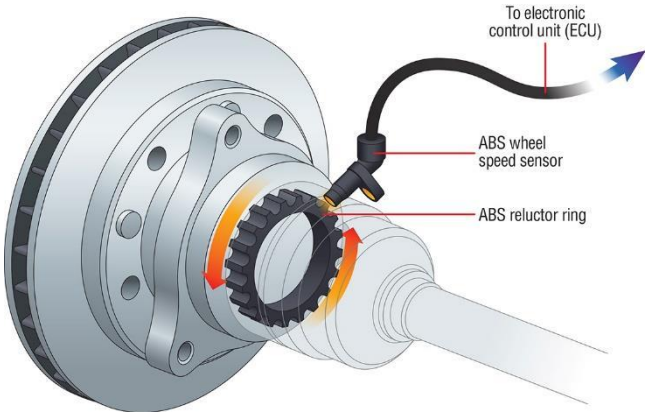
4.2.3. Control of variable valve timing:

Variable valve timing is available on a few motors. In such a motor, the ECU regulates when the valves open in the motorcycle. At a faster velocity, the valves are generally opened sooner than at a reduced speed. This can increase the rate at which air enters the chamber, increasing power and mileage.

4.2.4. Electronic valve control:

Trial motors without a camshaft but with full electronic control of the entrance and fumes valve opening, valve shutting, and valve opening space have been created and tested. Without the usage of a starter engine, certain multi-chamber motors equipped with precisely coordinated electronic start and fuel infusion can be started and run. This type of static-turnover motor would provide the efficiency and contamination-reduction benefits of a moderate half-breed electric drive without the cost and complexity of a large starter motor. The Alfa Romeo Mito was the first vehicle to employ this type of engine, which was developed by Italian company Fiat in 2002 and released in 2009. Electronic valve regulation is used in their Multiair motors, which boosts force and drive while lowering fuel consumption by 15% if you're lucky. The valves are effectively opened by ECU-controlled water-powered syphons. The valves may open a few times for each entering stroke depending on the motor load. The ECU then calculates how much gasoline should be pumped to accelerate ignition.

4.3. Diagrammatic Representation of ABS and ECU:



5. Conclusion:

Non-invasive assaults on cyber-physical frameworks present impressive dangers in circumstances that can be, on occasion, life-basic. Such assaults are more earnestly to identify at the sensor level furthermore, consequently require more elevated level discovery components. Utilizing vehicle anti-lock braking frameworks, we have shown both oversimplified and progressed techniques for non-invasive assaults on sensor subsystems. The high-level assault represents a truly skilled technique for disconnecting sensors from the general climate utilizing results from versatile criticism control hypothesis before injecting a spoofing signal in the system. The proposed procedure has been assessed for anti-lock braking sensors, where a little electronic module is planned and carried out to show the possibility of the thought. We investigated a few parts of planning such a module, and results got continuously from modern ABS equipment loan belief to the adequacy of the assault and the danger that comparable assaults present.

6. References:

1. Woojin Jeong,Sungmin Han,Eunmin Choi,Seonghun Lee,Ji-Woong Choi, et al, CNN-Based Adaptive Source Node Identifier for Controller Area Network(CAN), IEEE Transactions on Vehicular Technology(Volume:69, Issue: 11, Nov. 2020)
2. MD Delwar Hossain, Hiroyuki Inoue, HideyaOchiai, Dou Dou Fall and YoukiKadobayashi, et al, LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communications, IEEE Access (Volume: 8), 07 October 2020
3. Hyo Jin Jo, Jin Hyun Kim, Hyon-Young Choi, Wonsuk Choi, Dong Hoon Lee and Insup Lee, et al, MAuth-CAN: Masquerade-Attack-Proof Authentication for In-Vehicle Network, IEEE Transactions on Vehicular Technology (Volume: 69, Issue: 2, Feb. 2020)
4. Hyeran Mun, Kyusuk Han, Dong Hoon Lee, et al, Ensuring Safety and Security in CAN-based Automotive Embedded Systems: A Combination of Design Optimization and Secure Communication, IEEE Transactions on Vehicular Technology (Volume: 69, Issue: 7, July 2020)
5. MabroukaGmiden, Mohamed HediGmiden, HafedhTrabelsi , et al, An Intrusion Detection Method for Securing In-Vehicle CAN bus, 17th international conference on Sciences and Techniques of Automatic control & computer engineering - STA'2016, Sousse, Tunisia, December 19-21, 2016
6. ShahrozTariq, Sangyup Lee, Huy Kang Kim, Simon S.Woo , et al, CAN-ADF: The controller area network attack detection framework, Computers & Security, Volume 94, July 2020, 101857

7. Pascal Urien Telecom Paris Tech, Saclay University, LTCI 23 avenue d'Italie, 75013, Paris, Designing Attacks Against Automotive Control Area Network Bus and Electronic Control Units France 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)
8. Tobias Hoppe, Stefan Kiltz, and Jana Dittmann Research Group on Multimedia and Security Otto-von-Guericke University of Magdeburg Universitaetsplatz 2, 39106 Magdeburg, Automotive IT-Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats Germany SAFECOMP 2009: Computer safety, Reliability and Security pp 145-158
9. Gaurav Kalamkar M.E. Student Dept. of E&TC, Pimpri Chinchwad College of Engineering Akurdi, Maharashtra kalamkargaurav@gmail.com AjeyGotkhindikar Subject Matter Expert, Automotive Cybersecurity, KPIT Technologies Ltd. Pune, Maharashtra ajey.gotkhindikar@kpit.com A. R. Suryawanshi Associate Professor Dept of E&TC,Pimpri Chinchwad College of Engineering, Akurdi, Maharashtra, Low-level memory attacks on Automotive Embedded systems 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)
10. Kazuki Iehira , Hiroyuki Inoue, and Kenji Ishida Faculty of Information Sciences, Hiroshima City University, Hiroshima, Japan Graduate School of Information Sciences, Hiroshima City University, Hiroshima, Japan Connected Consumer Device Security Council (CCDS), Okinawa, Japan Spoofing Attack Using Bus-off Attacks against a Specific ECU of the CAN Bus 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)
11. Hyun Min Song, Ha Rang Kim and Huy Kang Kim Center for Information Security Technologies (CIST), Graduate School of Information Security Korea University Seoul, Republic of Korea, Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In-Vehicle Network 2016 International Conference on Information Networking (ICOIN)
12. Sam Abbott-McCune Virginia Tech Blacksburg, VA Lisa A. Shay Department of Electrical Engineering and Computer Science West Point, New York, Intrusion PreventionSystem of Automotive network CAN bus 2016 IEEE International Carnahan Conference on Security Technology (ICCST)
13. Sam Abbott-McCune Virginia Tech Blacksburg, Virginia Lisa A. Shay Department of Electrical Engineering and Computer Science West Point, New York, Techniques in hacking and simulating a modern automotive controller area network 2016 IEEE International Carnahan Conference on Security Technology (ICCST)
14. Shah Khalid Khan, Nirajan Shiwakoti, Peter Stasinopoulos, Yilun Chen School of Engineering, RMIT University, Carlton, Victoria 3053, Australia, Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions, Received 19 May 2020, Revised 12 August 2020, Accepted 3 October 2020, Available online 26 October 2020.
15. Hyeokchan Kwon, Sokjoon Lee, Jungyong Choi, Byung-ho Chung, Mitigation mechanism against in-vehicle network intrusion by reconfiguring ECU and disabling attack packet, 2018 International Conference on Information Technology (InCIT)
16. Chung-Wei Lin, Huafeng Yu, Cooperation or competition? Coexistence of safety and security in next-generation Ethernet-based automotive networks, 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)
17. Shuji Ohira, Araya Kibrom Desta, Ismail Arai, Hiroyuki Inoue,

Kazutoshi Fujikawa, Normal and Malicious Sliding Windows Similarity Analysis Method for Fast and Accurate IDS Against DoS Attacks on In-Vehicle Networks, IEEE Access (Volume: 8)

18. Aman Singh, Madhusudan Singh, An empirical study on automotive cyber attacks, 2018 IEEE 4th World Forum on Internet of Things (WF-IoT)