International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

In-Vehicle Data Communication with CAN &Security Monitoring: A Review

Karuppusamy S, Satheeshkumar S*, Jagannadhanaidu K, Karthikeyan B, Sundar S, Venugopal P
School of electronics engineering,
Vellore Institute of technology, Vellore
Tamilnadu, India
Email: satheeshkumar.s@vit.ac.in
Ankamma Rao J
Electrical & Computer Engineering
Assosa University,
Ethiopia
Email: jaraoeee04@asu.edu.et

Abstract— Automobiles are now being created with more electronic components for efficient functioning such as Anti Lock Braking system, Adaptive Cruise Control, Traction control system, Airbag, Power Steering etc. managed by networked controllers that include hundreds of ECUs (electronic control units) that can coordinate, control, and monitor loads of internal vehicle components. Each component, such as ABS, TCS (Traction control system), tire pressure monitoring system and telematics system, may communicate with nearby components over the CAN (Controller Area Network) bus, establishing an in-vehicle communication network. These modern automobile system networks intended for safety with minimal consideration for security have drawn the attention of researchers for providing security in CAN. The Paper reviews the behavior and vulnerabilities of CAN within an in-vehicle network including various attacks possible in CAN along with the proposed solutions in the literature with extensive survey on a security promising approach named as IDS (Intrusion detection system).
Keywords- Data Communication, Security, CAN, In-Vehicle, Air bag.

I. INTRODUCTION

In the automotive industry, there has been a growing interest in replacing hydraulic or purely mechanical components with embedded electrical system alternatives since the 1970s. As technology advances, more and more functions are introduced to vehicles, resulting in a rise in the amount of wires. With further advancement, the wiring between the units grows more complex, making real-time data analysis a time-consuming procedure. Because of the complicated wiring arrangement, the bit rate drops and communication between nodes becomes inefficient. To reduce wiring complexity, a communication protocol with a simple two wire system and an increase in data throughput of up to 1Mbps was developed. As the goal was to provide more assistance and safety to the driver, the number of sensor nodes in the vehicle increased, as did the number of ECUs, with the introduction of features such as ABS, TCS, Tire pressure monitoring, Collision avoidance system, Fuel monitoring system, Air bags, electric power steering, adaptive cruise control, and so on. The CAN network connects all of the sensor nodes, forming an in-vehicle network. The rising amount of information exchanges within the CAN bus system with buses that connect with the outside world creates a slew of security concerns vying for entry into the system. These flaws in the CAN bus could jeopardize not just the driver's safety, but also the safety of other vehicles. Before learning about CAN's flaws and attacks. Section 1.1 begins with an overview of the CAN architecture and its standard and extended frame formats. Whereas sections 1.2 and 1.3 help to understand CAN bus vulnerabilities and attacks.

1.1 Controller Area Network (CAN)

A standard Controller Area Network (CAN bus) bus enables a communication between different devices consisting of various applications and its controller, without any computer host. It is a message-based system that was designed to save copper by multiplexing electrical cabling in automobiles, but it may also be used for a variety of other purposes. The CAN protocol (bus) is used for data transfer due to its unique properties. CAN bus is serial, 2-wire i.e CANH (CAN high) and CANL (CAN low) differential bus technology having numerous appliances which are ranging in various speeds with different complexity of wiring. The 2-wires are complementary to each other.. The CAN transceiver can handle two kinds of signals: single-ended signals (TXD and RXD) and differential signals (CANH and CANL). The CAN transceiver converts the single-ended logic-level output signal (TXD) of the CAN controller to a differential signal during normal operation.

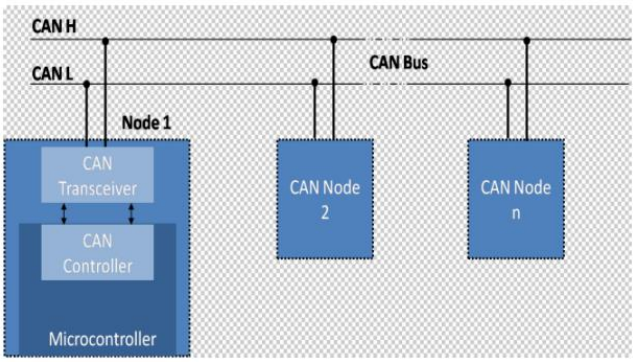

Fig.1 Architecture of CAN bus

It also converts the differential signal from the bus to single-ended logic signal (RXD) for use by the CAN controller lines. The transceiver effectively provide differential driving and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

receiving capabilities to and from the CAN bus, up to 1mbps speed data speed it can maintain while transmitting data over channel. A car is often equipped with an analogue driver vehicle interface for signaling various elements of vehicle condition such as temperature, obstacle, and fuel level indicator digitally and speed to improve the driver vehicle interface interactive digital system. We'll need a number of components to put this digital circuitry together. The main component will be processor that will be used to control and test all parameters. A temperature sensor, a speed sensor, a fuel level sensor, an obstruction detection sensor, and a power supply will bused for sensing.

The CAN Working Principle: Data messages exchanged over a CAN bus do not include the sender or receiving node's addresses. The CAN message is broadcasted to all nodes of the network with a unique network-wide identification number. Hence, it is difficult for the receiver to identify whether the message is irrelevant or relevant to it. If the message is relevant, it will be handled; otherwise, it will be disregarded. The unique identity also determines the message's priority. The most prevalent type of two-wire bus is the CAN Physical Bus with a Twisted Pair (shielded or unshielded). Flat pair (telephone) cable also performs well, however it generates more noise and is more susceptible to external noise sources. The robustness of CAN will work in harsh situations, with advanced error checking algorithms ensuring that transmission defects are recognized.

Types of CAN:
There are 2 types of CAN implementations, based on the identifier field of the CAN message

- STANDARD: Identifier field with an 11-bit width.
- EXTENDED: Identifier field is now 29 bits wide.

The standard CAN protocol, which is known as BASE FRAME, consists of 11-bit as identifier and also it is known as version 2.0A. Similarly, version2.0B i.e. is Extended CAN protocol has a 29-bit field identifier. If a standard 11-bit identifier node receives an extended frame identifier, it will discard it. But whereas extended frame format can receive both types of CAN frame messages.

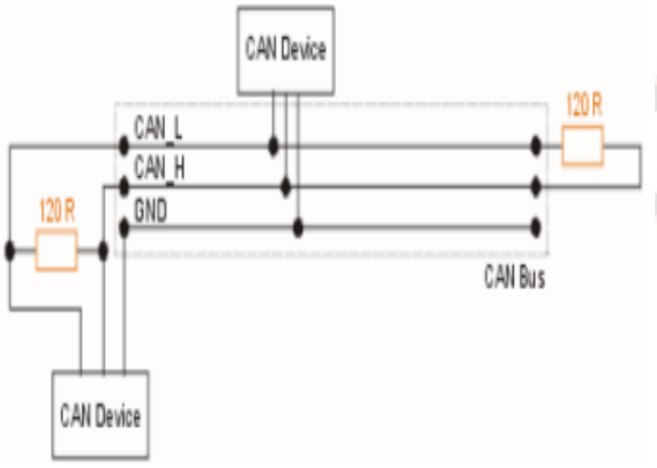

Fig.2 Implementation of CAN bus

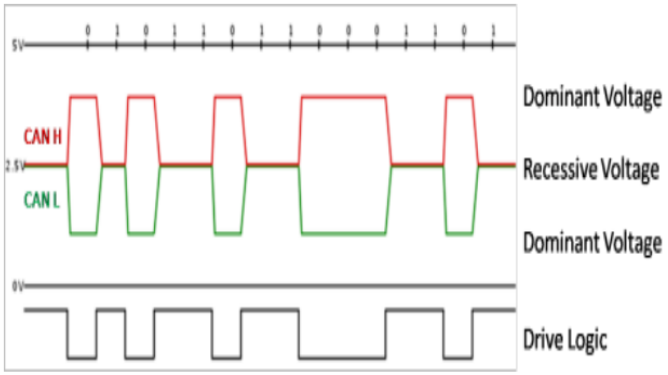

Fig.3 CAN Bus – Voltage Levels

STANDARD: Identifier field with an 11-bit width(Version 2.0 A)

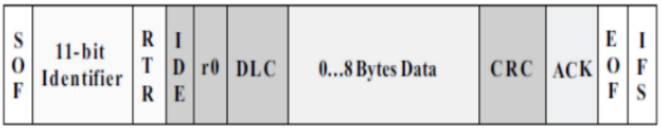

Fig.4 CAN Standard Frame Format

The following bit fields are shown in the diagram:

- SOF–The single dominant start of frame (SOF) bit is used to synchronize idle nodes on a bus.
- Identifier—A communication's priority is determined by its Standard CAN 11-bit identifier. The lower the priority of a binary value, the lower it is.
- RTR–The single remote transmission request (RTR) bit takes precedence when data from another node is requested. The request is received by all nodes, but the identification identifies the individual node. All nodes get the response data, which may be utilized by any interested node. As a consequence, a system's data is all consistent.
- IDE–A dominant single identification extension (IDE) bit denotes the transmission of a standard CAN identify with no enhancements.
- r0 - is a portion that has been set aside (for possible use by future standard amendment).
- DLC–The 4-bit data length code (DLC) specifies the number of bytes being delivered.
- Data–Up to 64 bits of application data can be sent.
- CRC–For error detection, the preceding application data's checksum (number of bits transmitted) is saved in a 16-bit (15 bits + delimiter) cyclic redundancy check (CRC).
- ACK–Every node that receives a valid message replaces this recessive bit with a dominant bit, indicating that the message was properly sent. The transmission is refused if a receiving node detects a mistake and leaves this bit recessive, and the message is re-bit rated by the sender node. Each node acknowledges (ACK) the integrity of its data in this way. The length of the ACK bit is two bits. The acknowledgement bit is one, while the delimiter is the other.
- EOF–When dominant, this 7-bit end-of-frame (EOF) field signifies a stuffing mistake by detecting the end of a CAN frame (message) and prohibiting bit stuffing. During

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

normal operation, if 5 bits of the same logic level occur in a sequence, a bit of the opposing logic level is pushed into the data.

- IFS–The controller uses this 7-bit inter frame space to store the time it takes to move a successfully received frame to its proper location in a message buffer area (IFS).

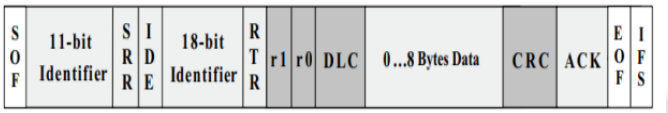

Fig.5 CAN Extended Frame Format

The Extended CAN message is the same as the Standard CAN message, except it includes the following information:

- SRR– In the enlarged format, the replacement remote request (SRR) bit works as a placeholder for the RTR bit in the usual message location.
- IDE–The presence of extra identifying bits is indicated by a recessive bit in the identifier extension (IDE). IDE is followed by the 18-bit extension.
- r1– Before the DLC bit, an extra reserve bit has been placed after the RTR and r0 bits.

1.2 CAN vulnerabilities

Carsten et al. [12] discussed a number of serious vulnerabilities in the CAN bus technology. According to the author, CAN packets do not carry any information about the transmitter or receiver address. As previously stated, all CAN packets are broadcast to all CAN nodes using the arbitration identifier field. But the receiving node doesn't know whether the received CAN packets are intended for it or not. Because of this, the recipient node was unable to determine if the packet received was valid or not. Furthermore, each ECU lacks a message authentication mechanism for safeguarding packets exchanged between nodes; hence, hacked ECUs could be utilized by attackers to spoof and deliver phony CAN messages.

1.3 Attacks on CAN bus

Koscher et al. launched a significant effort in detecting potential vulnerabilities in the automobile communication system, specifically for the CAN bus protocol, in 2010 [13]. Physical, non-physical, and short- and long-range access to a vehicle allowed the researchers to tweak a wide variety of safety-critical components. On-board diagnostics (OBD-II) was used in some of the physical access attack techniques, resulting in the manipulation of speedometer readings on the car's instrument panel, preventing door locks, stopping the engine, and so on. A large number of fake CAN packets flood the vehicle's CAN bus, causing these consequences. Furthermore, Boyes et al. (2015) voiced various worries about the security and privacy of the car network [14] due to the expanded attack surface. They revealed that a plethora of attack surfaces might be remotely exploited via USB, Bluetooth, and Wi-Fi due to the intrinsic properties of short and long wireless medium incorporated in the vehicle's infotainment system. Potential adversaries can exploit these weaknesses by simply reverse engineering the system. Miller and Valasek also displayed a few prepared messages in the form of CAN packets that were delivered remotely through the Jeep Cherokee's probable entry ports in 2015. (For example, TPMS and Cellular). Some of the vehicle's critical components, such as the braking system, were rendered useless as a result. Security specialists have determined that most current automotive systems were developed with safety in mind but no security in mind as a result of various attack surfaces in the vehicle system. As a result, presenting a holistic approach to security for these as well as being ill-equipped in determining which nodes have staged the attacks.

II. LITERATURE SURVEY

This section 2 reviews literature studies on various intra and inter vehicle data communication and security, with a focus on the CAN bus system. Recently, research on car security has evolved. Some ongoing studies and projects in offering prospective defense-in-depth procedures in safeguarding invehicle CAN bus systems have been published. Message authentication is a prominent security technique that makes use of cryptographic-based software [11–14]. In tackling CAN network security challenges, the researchers that presented this solution attempted to borrow from the internet security strategy. The recommended technique guarantees that the CAN information outline sent between the two end hubs is permitted. Despite this, the maximum length of a CAN data frame is just 8 bytes. As a result, the available area for implementing this procedure is extremely limited. In particular, paper [11] established and showed a real attack model in the connected automobile environment utilizing a malicious smartphone app through practical testing. They devised a security protocol that could be applied to the automotive environment after showing the attack model using a study of the vulnerability of in-vehicle CAN. Moreover, the creator assessed the security and execution of the proposed security convention utilizing Secure-ECU and CAN-oe. Subsequently, the accessible region for executing this strategy is incredibly limited. To settle the issue, numerous countermeasures have been carried out, including shortening a MAC across different CAN outlines [15], utilizing different CRC fields to add 8 bytes of CBC-MAC [16], and utilizing an out-of-band channel to verify the message [17]. However, relying solely on this strategy cannot guarantee perfect security in averting a high level of threat, particularly denial-of-service (DoS) attacks [18]. Furthermore, this strategy covers just a subset of vehicle components and demands a large redesign of all ECUs, which is unfeasible [19, 20].

The provided paper [21] examines the usage of honeypots to acquire attacker information such as preferences, methodologies, and weaknesses in current systems. This data was utilized to create security solutions for the invehicle network. They discussed collecting data from attackers, processing and analyzing the collected data, and highlighting key difficulties linked to employing honeypots in automobiles. The authors of paper [22] created, implemented, and tested a vehicular hardware security module that enables comprehensive protection of all relevant in-vehicle ECUs, and their communication feasibility was demonstrated practically with the first HSMequipped passenger. On a related issue, various organizations have been working hard to solve many areas of assaults within the in-vehicle network infrastructure. Arilou Cyber Security, for instance, conveys a leading edge

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

equal interruption counteraction framework (PIPS), a procedure that distinguishes the wellspring of each CAN parcel on the transport. It also employs an electronic signature to recognize the signals received from the various ECUs. In this approach, tainted CAN packets can be prevented from being transmitted. Argus Cyber Security, on the other hand, attempts to provide protection capabilities for a wide range of communication network protocols, including Flex Ray, CAN flexible data rate (CAN-FD), Ethernet, and others [23]. Furthermore, Berg et al. of Semcon Automotive Cyber Security [24] presented a protective layer at the infotainment unit via secure gateway implementation (SG).

The author of the paper [25] summarizes the current state of the research, including the challenges discovered and the solutions proposed. They organized the investigation by grouping the research into five categories: in-vehicle network difficulties, architectural security features, intrusion detection systems, honeypots, and threats and attacks.

III. INTRUSION DETECTION SYSTEM (IDS)

An interruption identification framework (IDS) specifically arouses individuals' interest, attributable to its usability and capacity to productively recognize dangers. As a general rule, IDS screens network action or straightforwardly on the host distinguishes and cautions on the off chance that any unforeseen events happen in the framework [34]. These odd occasions, known as interruptions, are battling their direction into the framework to acquire unapproved access. Inward interlopers might exist inside the designated framework parts and have legitimate organization access honors, while outer gatecrashers might dwell beyond the designated organization and try to procure unlawful admittance to the framework parts [35]. Depending on the way things are arranged, IDS can be latent or dynamic. Uninvolved IDS simply identifies the assault; though dynamic IDS forestalls the attack. Sensors, a recognition motor, and, at long last, a detailing module make up an ordinary IDS plan. The sensors are either networkincorporated (network-based IDS) or straightforwardly appended to the end hub (have based IDS). IDS approaches are named signature-, irregularity, or particular based. The accompanying part will go through the points of interest of IDS establishment for the car space. An investigation of the advantages and downsides will be advertised.

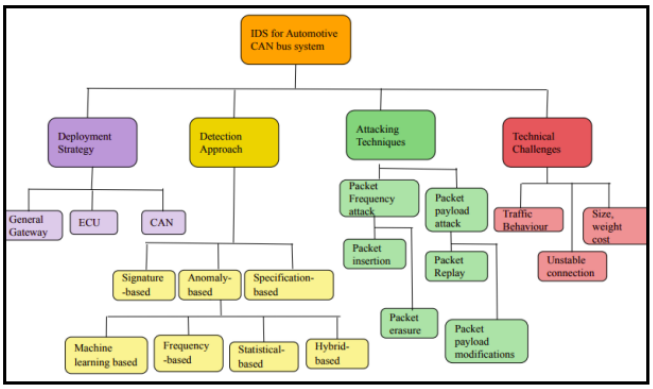

Fig 6. The IDS taxonomy for CAN bus network

3.1 IDS in the car area

In the vehicle business, there are. Hoppe et al. [36] werquick to apply IDS to the auto framework, zeroing in on thregular CAN transport organization. A synopsis of each anevery review distributed in the writing is given in segmen3.2, coordinated by discovery techniques: signature, oddity particular, and half breed. Nonetheless, before we proceedwe might want to give you a suggested scientific classification for the CAN transport network IDS in the car business (roused by [37]). IDS recognition procedure, sending methodology, attack strategies, and ultimately mechanical obstacles are immeasurably significant pieces of the CAN transport network IDS scientific categorization (see Fig. 3). The investigated research endeavors in building IDS for the auto climate are summed up in Table 1. on these four attributes

3.1.1 IDS deployment strategy

IDS should be sent to each observed framework to screen activities in the CAN arranged from different sources. In view of their discoveries in [36, 38, 39], they offered the accompanying spots for IDS sending in the auto climate (as demonstrated in Fig. 4): CAN networks (A), ECUs (B), and focal doors (C). A host-based IDS, like interruption location in work area IT, is joined straightforwardly to every vehicle ECU. It gives a far-reaching view of the framework's interior movement. Thus, vindictive code infused during runtime can be found. While network-based IDS alludes to the association of an IDS to the CAN arranged similarly to center point ports. It ceaselessly screens and actually takes a look at vehicle correspondences for dynamic assaults. Be that as it may, there are a few elements to consider while incorporating an IDS into an inserted framework. Kleberg et al. furthermore, Koscher et al. explored the effect of assaults on ECUs introduced in different pieces of shipboard correspondences [13, 40]. A compromised CAN organize and focal entryways give a greater risk than a compromised ECU [40]. This is on the grounds that a hacked organization and focal doors approach and command parcels that pass through network entryways on their course to the designated ECU spaces.

3.1.2 IDS attacking techniques

The different kinds of attacks framed in [1, 11, 13, 22, 23,41-45] are viewed as in this paper in light of late discoveries concerning assault surfaces dwelling inside the CAN arrangement detailed in Section 1.1.3. In a nutshell, two sorts of assaults influence CAN transport traffic: (1) assaults on CAN bundle recurrence and (2) assaults on CAN parcel payload. These going after techniques are the most regularly utilized in deciding the responsiveness and adequacy of proposed interruption recognition frameworks. In the accompanying part, we go over the CAN recurrence assault and the CAN bundle payload control assault more meticulously.

3.1.2.1 Attacks on CAN packet frequency

The CAN packet IDs are separated by a predetermined and periodic time interval. Thus, CAN packet frequency assaults are carried either by adding an extra packet or erasing genuine packets from CAN bus flow [22, 23, 41, 42, 45].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

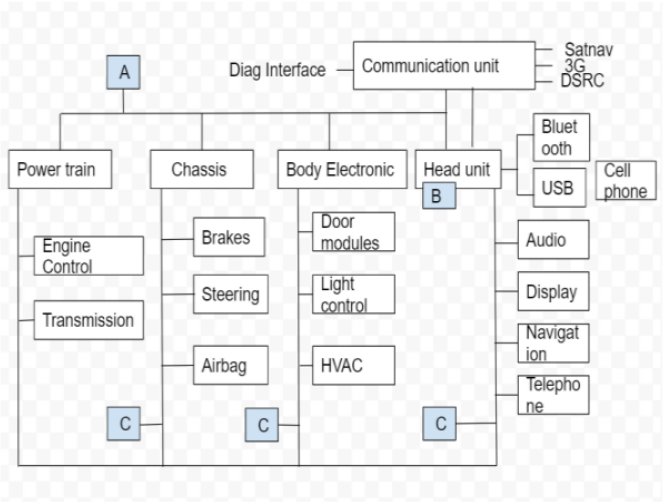

Fig 7. Possible locations for IDS deployment in the CAN bus system. A) CAN, B) ECU, C) gateways.

a. Packet insertion

Among attacks some of them go after that cause actual digital results on the vehicle incorporating extra CAN IDs or, simultaneously, the inclusion of changed CAN parcel payloads into traffic. In any case, for the vehicle to be impacted, the embedded parcel should be intended to be genuine and substantial. Notwithstanding the CAN recurrence assault, the bundle is overflowed with the CAN parcel's most elevated need ID and embedded inside a short cycle. By possessing the CAN transport with a need-based convention plot and in the event that the pace of inclusion is sufficiently fast, ECU could consistently communicate the CAN bundle with a prevailing state [11]. As an outcome, other lawful parcels with lesser need would be pushed back (e.g., DoS assault). b. Packet erasure The shortfall of a standard CAN bundle, which should come at a characterized stretch, may permit assaults to emerge in rush hour gridlock. For instance, the enemy could hold onto control of the objective ECUs and adjust them so all substantial CAN bundle transmission is stopped [22]. At the point when the casualty ECU quits giving the planned parcels, the mimicked ECU's bundles are totally deleted from the CAN transport stream. At long last, when the embedded bundle has completed the process of assuming control over the stream, the missing parcel stream will continue, with an unexpected stage compared to beforehand.

3.1.2.2 Attacks on CAN packet payload

The CAN packet's payload is gone after by changing or faking the information content of a CAN ID. The modified information might be sent as a component of the recently embedded bundle on the traffic or as a feature of the standard CAN parcel stream. The faked CAN bundle payload can be achieved by remotely compromising the ECU to send the altered parcels. This assault varies from the embedded bundle in that it centers around changing qualities inside parcel content as opposed to infusing new bundles. The changed parcel content must likewise be certified; in any case, it significantly affects the vehicle. This kind of assault includes parcel replay and bundle payload adjustment. a. Packet replay The packet replay attack is carried out by collecting realtime CAN packet traffic known to cause effects on the vehicle. The captured packet is then replayed, with the usual CAN packet in the flow substituted with the historical packet, resulting in the historical effects. This is the simplest attack to carry out because it does not necessitate any knowledge of how traffic works. The replacement packet is inconsistent with the earlier packet sequence, despite the fact that the replayed packet is a legitimate subsequence. As a result, it can cause more serious issues such as non-stop CAN packet transmission requests [46], deadline violations [47], and major CAN arbitration priority scheme inversion [48]. Furthermore, the sequence of the CAN packets would differ from the original, preventing the car from functioning properly because the packets are not transferred sequentially and thus violate the protocol requirement. Even if the frequency of CAN packets remains constant, the problems described above are critical, potentially jeopardizing vehicle safety.

b. Packet payload modifications
CAN packet modification is defined as modifying values within the packet payload to conduct unexpected behavior. In this instance, acceptable packet manipulation for this type of attack may be impossible to specify. Furthermore, the packet payload is controlled by changing the packet content to a constant value, i.e., minimum or maximum value, or to a random value. For example, a fuzzy attack works by changing the values of the CAN ID as well as the CAN packet content at random.

3.1.3 IDS technical challenges

Previous works [31, 40, 49] have identified certain issues that must be considered when building proposed solutions in the CAN bus network system: restricted resources, time requirements, traffic pattern behavior, unstable connection size, weight, and cost.
1. Limited resources: Every ECU in a car has numerous constraints in terms of memory capacity, computing power, and data transmission rate (bandwidth).
2. Real-time constraint: Because CAN packets are transmitted in real-time from ECUs to other nodes, delaying and queuing of packet buffers is too dangerous and unacceptable. The CAN packet received from the vehicle's sensors must be managed in real-time so that actuators can conduct vehicle functions without delay. When offering security solutions, the real-time constraint must be considered.
3. Traffic behavior: CAN traffic protocol patterns for automotive communication systems differ from those of traditional Internet Protocol (IP) networks. CAN packets, for example, are transmitted in nature. Furthermore, in order to perform firmware upgrades and wireless diagnostics on vehicles, a temporary link from in-vehicle to V2I must be created, which necessitates the use of different communication models and traffic protocols. As a result, implementing an IP network solution is not an option.
4. Unstable connections: Because vehicles are moving, regardless of speed, they may pass through areas without internet access. As a result, IDS solutions for the automobile industry should be aware that connecting to a third-party may not always be possible.
5. Size, weight, and cost: IDS solutions may vary in weight and size, and they may also require minor or substantial modifications, which will affect the cost. For example, replacing a CAN bus network with a line topology with an Ethernet bus network with a different topology needs a lot of extra wire and may be impossible.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

3.1.4 IDS detection approach

In the automotive area, the intrusion detection approach is determined by how the detection mechanism is used within the system. It is divided into four categories: anomaly-, signature-, specification-, and hybrid-based. In comparison to signature- and specification-based IDS, anomaly-based IDS is the most widely utilized and promising approach in automobile IDS. Section 4 goes into greater detail on the preference for anomaly-based IDS in the CAN bus system over alternative IDS technologies.

3.1.4.1 Anomaly-based approach

Basically, oddity based interruption location frameworks [50] screen continuous framework movement and contrast it with regular conduct put away in a profile. At the point when the disparity from standard profile conduct arrives at a predetermined edge, the caution will sound. After a preparation stage, this oddity based method can distinguish new dangers successfully. Regardless, it's anything but a simple interaction since this approach considers anything that strays from a commonplace way of behaving to be a side effect of interruptions [51]. Therefore, this strategy has an extreme blemish in that it makes bogus positive cautions on ordinary packets. The most well-known methodologies utilized by past specialists to foster a profile of a typical way of behaving are recurrence based, AI based, and measurable based procedures [52]. Meanwhile, a mixture based inconsistency identification technique is as yet being created [53, 54]. These arrangements, nonetheless, need a lot of handling assets [54], which ought to be considered prior to applying in low limit ECUs. Subsequently, the peculiarity based methodology ought to think about this issue, especially for the CAN transport framework in the auto field. Various review articles gave in the writing, for example, [22, 34, 36, 41, 55, 56], have utilized the timing timespan traffic and the recurrence of CAN parcel arrangements to recognize irregularities inside the CAN transport organization. This is on the grounds that CAN organize traffic continually communicates the fixed CAN bundle ID and payload to any listening ECUs at a foreordained time stretch and recurrence. Subsequently, any variety from regular traffic could be a mark of a framework assault. The accompanying scientific categorization of oddity based interruption recognition frameworks (IDS) in the car business makes sense of utilizing recurrence based, AI based, factual based, and crossover based procedures.

3.1.4.2 Frequency-based method

Miller and Valasek noted in [45] that detecting assaults on CAN bus is simple. This is because conventional CAN bus traffic, which broadcasts packets at regular intervals, is predictable. They hypothesized that using known CAN packet frequency between the packet sequence can detect abnormalities by analyzing the CAN behavior on which ECUs interact. However, due to the noisy environment in the CAN network, depending solely on the predictability of CAN frequency cannot detect abnormalities from irregular or unpredictable CAN packets in traffic [57]. Hoppe et al. were the first to introduce the IDS technique in the automotive arena, as described in Section 3.1.1.They offered an anomaly-based IDS system as an example of a short-term countermeasure in dealing with contemporary automotive hazards in [23, 36]. Four selected attack case studies targeting vehicle control systems were done to evaluate the strategy. Window lift, airbag control system, warning lights, and the central gateway ECU are among the targeted electric components. CERT taxonomy was used to organize a systematic procedural analysis of the attacks. According to the CERT analysis, three characteristics of identified patterns can be used in IDS to address previously demonstrated attacks: the increasing rate of cyclic CAN packet occurrences, the recognition of obvious forged packet IDs, and, finally, the examination of physical link layer features in low-level CAN bus communication. As a result, they were able to find patterns that are both simple to build and implement and very cost-effective. Song et al. used a very light-weight technique based on CAN packet frequency observance [57], which was inspired by [23, 45]. They simplified the detection technique so that it could respond to the incursion faster while using less processing power. The approach works by calculating the time delay between the most recent packets and their arrival time (usually lower than 0.2 ms). If the time interval is less than a certain threshold, the IDS will detect that intrusions are occurring. To test the algorithm's effectiveness, packet frequency assaults were performed on modified CAN packets obtained from a well-known vehicle manufacturer. The first sort of attack consisted of inserting packets with a single CAN ID. The second approach involved randomly injecting pre-ordered packets with numerous CAN IDs and, ultimately, injecting large volumes of CAN packets in a manner akin to a DoS attack. The overall experimental results demonstrated a detection accuracy of 100 percent with no false alarms. Despite its excellent detection accuracy, it was unable to detect abnormal incoming packets. Ling et al. used an algorithmic-based detection approach in [58] to cope with two primary vulnerabilities in CAN bus traffic: DoS attack and error flag misuse. Because it flooded the network with a huge number of high priority packets while dropping lower priority genuine packets, the DoS attack always wins priority-based arbitration ID. The error flag is used to disable the communication mechanism so that packets can be treated uniformly. Furthermore, the suggested system monitored legal and illegitimate CAN ID that transmitted consecutively outside the preset thresholds using threshold and resettable counters. Despite the model's architecture being predicated on the CAN system capacity constraint, it was able to detect malicious activities in the CAN network. Nonetheless, the author of [59] said that the proposed algorithm and the alarm response to the attack are unclear, undermining the findings. Gmiden et al. [60] suggested a method for detecting anomalies based on the time interval feature of successive CAN packets. The proposed IDS is conceptually similar to that of [58]. The only difference is that they calculated the packet arrival times and compared them to the previous packets. Though the solution did not necessitate large changes to the CAN protocol, it did not account for DoS attacks and could not detect irregular packets. Moore et al. [61] have made the nature of the fixed gap between CAN packets conspicuous in order to use time analysis in various vehicle models. The proposed method is based not only on the regularity of most parameter ID (PID), but also on the redundancy of PID signals emitted in CAN communication. They used a packet insertion attack to take advantage of the regular-frequency nature of a standard CAN packet. While this method made substantial progress in terms of high detection accuracy against the three forms of packet frequency assault, it is required to automate algorithm settings such as altering threshold and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

changing training duration when experimenting with larger and more diverse attacks.

3.1.4.3 Machine learning-based method

Techniques in light of AI are regularly portrayed as either managed or unaided, fully intent on gaining the element portrayal from input information. A managed classification requires totally marked information while preparing a model, though an unaided class doesn't, on the grounds that the characterizations between the given data sources are laid out in view of their likeness. The troubles in gauging and developing assault conduct while breaking down the CAN transport framework, as well as the prerequisite for speculation fitting with the CAN convention's particular climate, push specialists to offer administered or semimanaged peculiarity recognition procedures. Kang et al. were among the quick to utilize AI-based interruption location frameworks (IDS), explicitly a semi-managed profound brain organization (DNN) [62] technique for CAN transport networks [63]. The bundles traded between ECUs were recovered straightforwardly from a bit stream in the CAN transport lines prior to being decoded. Since CAN parcel properties are non-straight, the creator proposed preparing the recuperated boundaries with a restricted Boltzmann machine (RBM) [64]. To segregate between standard and vindictive parcels, the technique conveys the likelihood for each class as calculated values "1" and "0." To save time, disconnected preparation was performed during the preparation stage, while during the identification stage, the twofold choice in light of the prepared highlights was executed against showing up new CAN bundles. The creators assessed the model by using faked tire pressure checking framework (TPMS) parcels to show mistaken TPMS pointer values on the dashboard. Despite the close to 100% ID rate, as the number of layers expanded, so did the computational intricacy, preparing time, and testing time. To identify any deviations from standard CAN bundle frequencies, Taylor et al. utilized a directed one-class support vector machine (OCSVM) [41]. While inspecting CAN traffic, the creators raised stress over the high extent of phony problems. The model was tried by showing mistaken TPMS marker values on the dashboard utilizing fake tire pressure observing framework (TPMS) bundles. Regardless of the close to 100% location rate, as the number of layers expanded, the computational expense, preparing time, and testing time all increased. To identify deviations from ordinary CAN parcel frequencies, Taylor et al. used a managed one-class support vector machine (OCSVM) [41]. While exploring CAN interchanges, the creators communicated stress over the high opportunity of misleading problems. Assuming that traffic is actually taken a look at every 0.5 seconds, for instance, there will be 104 phony problems every hour. Thus, the driver will disregard it since he accepts it is inadequate. The creators gave a calculation in [65] that measurements of CAN transport traffic streams as far as frequencies and normal bundle changes, perceiving the technique's commonsense imperatives. To decide the deviant sign, the assembled insights are contrasted with past qualities. The OCSVM [66] is utilized to characterize the CAN correspondence streams in this case. The proposed strategy was scrutinized by reproducing a bundle addition assault utilizing changed precaught CAN parcels from a 5-minute drive vehicle at low speed. In the synopsis, they found few bundle infusions while having a low deception proportion. Since the items in crude CAN bundles are of the string information type, Taylor et al. fostered a regulated long transient memory (LSTM) [67] to expect the following incentive for a given information succession [43]. The proposed strategy is utilized to prepare the got CAN contribution to expect the information field values conveyed by every shipper associated with the CAN transport. Any mistakes in the information grouping are taken advantage of to recognize anomalies. The scientists utilized a changed CAN parcel to mimic assault traffic by utilizing three essential procedures: bundles have filled the transport, uncommon information bundles show up, and expected parcels don't show up. The exploratory discoveries showed that peculiarities might be related to the most un-number of phony problems. It did, be that as it may, just help a solitary CAN ID and didn't take into consideration internet learning. Wasicek and Weimerskirch concentrated on a semi-directed chip tuningbased strategy for recognizing attacks targeting changing settings or reflashing recollections inside ECUs, as well as adding extra equipment to cause CAN organize traffic to act strangely [68]. The creator gathered five components from each element to describe the motor's ECU conduct under particular CAN traffic situations: force, cycles each moment (RPM), and speed. To decrease commotion, they prescribed adding time-moving signs to the CAN transport framework. The preparation approach started with the CAN including information being taken care of into the bottleneck of the fake brain organization (ANN) model, which was then back spread prepared. At long last, they collected the outcomes and utilized root-mean-square mistakes to deliver a solitary oddity score. In spite of the great outcomes as far as a higher genuine positive location rate over a misleading positive rate, the examination's slanting ROC diagram is leaned toward the line of no segregation.

3.1.4.4 Statistical-based method

The measurable based IDS approach looks at the ongoing factual perception to the factual perception that is not entirely set in stone. For instance, to find surprising conduct inside the demonstrated framework, [69, 70] utilized factual properties like mean, fluctuation, and standard deviation. The measurable based strategy can be utilized in the CAN transport network IDS by integrating a folding window into the CAN transport traffic time series: univariate or multivariate time series. The univariate technique looks at each CAN ID field independently. Be that as it may, it could be liable to time spans incorporating CAN ID in multivariate methodology studies, however, it may not be successful for CAN parcel content. Because car boundaries are very interconnected [45], it doesn't break down the logic of strings in a CAN information grouping [49]. At the point when the vehicle speeds up, for instance, the substance of the CAN information field transforms the slightest bit at a time. Subsequently, the multivariate strategy might be reasonable for recognizing interruptions simply in the substance of CAN bundle information fields. Marchetti et al. proposed a data hypothetical procedure to recognize irregularities in CAN traffic [24], which was roused by the entropy application introduced in [55]. For preparing the model, the creators gathered approximately 48 million CAN parcels and fostered a gauge for ordinary bundle conduct in light of their measurable entropy level. Several sorts of manufactured CAN bundles were infused during the assessment stage, focusing on a vehicle's well-being and pertinent parts while the car was driven at a rapid. At long last, the consequences of the analyses showed that the entropy-based IDS methodology is equipped for recognizing a lot of

maverick CAN bundle. Nonetheless, the technique could distinguish enormous paces of parcel infusion and was less effective for an unassuming volume of bundle infusion since it required simultaneous execution of numerous entropy calculations doled out to every ID. Marchetti and Stabili contrived a model-building approach in view of the succession of parcel ID changes seen in the CAN transport framework [71]. The proposed model's cycle is partitioned into two sections: a preparation stage and a discovery stage. During the preparation stage, 20% of the members were shown how to foster a veritable model as a progress lattice utilizing pre-caught CAN bundles. The last model, which is valid or misleading, brought about an exceptionally brief time frame to arrive at the progress esteem. The model is tried by infusing CAN parcels into it to recreate veritable assaults. In general, the discoveries demonstrated the way that the recommended strategy could recognize both secrecy and high-likelihood assaults without creating any bogus positive cautions. It doesn't give off an impression of being viable, notwithstanding, in recognizing a replay assault, in which typical bundles are retransmitted. In their proposition [22], Cho and Shin took on a clock-based IDS (CIDS) in light of their examination of three normal attacks that occurred inside an in-vehicle CAN organize, in particular disguise, suspension, and manufacture assaults. As per their discoveries, the disguise attack couldn't be distinguished totally on the grounds that the source's location isn't shown in messages. In the wake of noticing the periodicity conduct of CAN parcel timing spans at the beneficiary's side, the creators conceived a technique to uniquely mark each ECU's timestamp. The fingerprinted ECUs' standard was made utilizing the recursive least squares (RLS) procedure, and the blunder was surveyed utilizing the combined aggregate (CUSUM) investigation. The model is tried by coordinating CIDS into a CAN transport network prototype. The proposed model was approved by the creators by reconstructing the CIDS on three different vehicle types. The whole trial result demonstrated the way that different types of assaults could be recognized with the most reduced 0.055 percent misleading positive blunder and the wellspring of the assault could be distinguished from the compromised ECUs. Müter et al. exhibited entropy-based discovery of abnormalities in the CAN transport framework [55]. The entropy approach utilized the data hypothetical idea of computing occurrences from a given dataset and utilized the subsequent outcome as an IDS definition conduct profile. Subsequently, as the quantity of assaults expanded, so did the quantity of entropies that demonstrated CAN transport invasions. The creators utilized bundle inclusion assaults to assess the technique's reasonability, as well as a DoS attack on the CAN transport organization to upset commonplace related events. The outcomes demonstrated the way that the strategy's low arbitrariness of traffic determination could distinguish any deviations from the CAN transport organizations' standard way of behaving. Then again, the entropy technique didn't have all the earmarks of being fit for giving point by point data on the perceived attack. In light of the timing stretch and offset proportion between the communicated solicitation and reaction CAN remote edges in the CAN transport organization, Lee et al. introduced an OTIDS (offset proportion and time span based interruption recognition framework) [11]. In request to identify fluffy, DoS, and pantomime attacks, they utilized the relationship coefficient of time stretches and counterbalances, the quick and lost answer proportion, and normal reaction terms. The discoveries uncovered that the proposed strategy could rapidly distinguish any state of assault models. The assailants were additionally unfit to dodge the framework because of the idiosyncrasies of the arranged distinguishing highlights. Notwithstanding, in view of the extra equipment coordination to further develop correspondence, the strategy possibly distinguished a little amount of information when contrasted with the general measure of information. To distinguish timing varieties inside CAN transport traffic, Tomlinson et al. utilized pre-decided normal time periods bundle communicates and utilized Z score and autoregressive incorporated moving normal (ARIMA) calculations [72]. The proposed strategies were contrasted with the regulated based mean time span technique. These techniques were scrutinized to check whether they could raise the need of dropped and infused bundles. While infusing lower need parcels unpredictably, the exhibition of both the unaided Z score and ARIMA calculations was diminished. They suggested, in any case, that utilizing a more practical assault bundle, changing the best limit, and improving model parts and boundaries ought to assist with expanding execution. To expect the time series of CAN transport traffic, Narayanan et al. [73] utilized a secret Markov model-based strategy. They began by changing over the information from the motor, like RPM, coolant temperature, speed, and O2 voltage, into a period series observation. They changed over perceptions into inclinations instead of providing the model with genuine esteemed perceptions. Progress probabilities (the ability to control the change starting with one state and then onto the next) and discharge probabilities have been incorporated into the model (i.e., create likelihood in light of the perception of a present status). Changes in a particular way of behaving in CAN correspondence, for example, RPM esteem decrease during fast driving, are kept in the CAN bundle logs utilized in the examination. The back likelihood of a given earlier information succession in a decided sliding window is utilized to distinguish these irregular CAN bundles. On the off chance that any perception probabilities fell under a specific level, the model set off an alert.The results demonstrated the way that the model could effectively identify irregularities in individual and blend states, too as perilous states in CAN transport traffic, while surveying the model utilizing practical CAN go after bundles could give an impressive improvement later on.

3.1.4.5 Hybrid-based approach

Hybrid based IDS is otherwise called a disseminated interruption identification framework in the present work area IT climate (DIDS). It joins numerous IDS procedures (e.g., network-based IDS and host-based IDS) on a huge organization of PCs that speak with each other and are checked by a focal server [74]. The organization facilitated IDS parts to gather and change data about the observed framework into a typical configuration prior to sending it to a focal framework. The focal framework unites and examines the information gathered from various IDS. In contrast to the CAN transport climate, half and half based abnormality discovery in CAN utilizes more than one way to deal with distinguishing assaults, considering the CAN ID field, CAN information payload, CAN particular, CAN timing stretch, and recurrence [53, 54]. Weber et al. utilized a blend of a detail based framework and an AI-based location component to recognize implanted ECUs in CAN transport traffic [53]. This strategy is straightforward and can be utilized on the web, like

[54]. The determination based half involved static really takes a look at in the primary stage to confirm payload properties statically portrayed as a correspondence lattice, while the AI based part involved learning actually looks at in the second stage to find transient conduct irregularities in the CAN time series. The static checks module directed chosen information to the learning checks module, which removed highlights utilizing RNN, OCSVM, and a lightweight online locator of oddities (LODA) [75]. Each program delivered a parallel worth to demonstrate an oddity. The methodology is tried against five CAN adjusted bundles with different types of assaults, and the outcomes show an amazing negligible irregularity score that is similar to the standard CAN specification. Wang et al. made a half and half peculiarity identification framework in view of various leveled fleeting memory (HTM), a memory-based framework that can at the same time prepare an enormous number of CAN time series inputs while learning CAN information field groupings [54]. The technique depended on the condition of earlier learning and worked on the web. At the point when another surge of CAN bundles is obtained, the memory will be refreshed and the growing experience will proceed. Moreover, the scoring system for computing the projected worth's mistake depends on the log misfortune work; the blunder of each anticipated CAN ID is determined and added to give a solitary judgement. They performed both parcel inclusion and bundle change assaults with various sliding windows for location to evaluate the technique's effect. When contrasted with existing CAN IDS that utilize the RNN and HMM approaches, the HTM calculation is exhibited to be more solid in recognizing known and new assaults. Notwithstanding, in the event that the model's preparation time is diminished and excess CAN fields are erased, the model's general execution can be altogether moved along.

3.1.4.6 Specification-based approach

In most cases, a specification is a set of thresholds and rules that characterize the well-known behavior of network components such as routing tables, protocols, and nodes. The specification-based technique [76] detects attacks anytime the network's expected behavior deviates from specified standards. As a result, the specification-based approach serves the same goal as the anomaly-based approach: anomalies are anything that deviates from the designated well-known behavior profile. Despite this, the only significant difference between the two systems is that each specification and rule must be manually defined by a human expert. This technique, on the other hand, does not require any training because it works right away once the specs are set up. Furthermore, manually providing specifications could be error-prone and time-consuming because the system may struggle to adapt to diverse domains [77]. Larson et al. investigated the applicability of specifications using data from the CAN version 2.0 and CAN open draught standard 3.01 protocols [30]. The goal was to create security specifications for the communication behavior and protocol of ECUs. The anomaly detector does not need to be installed on each ECU because the specification was developed from the behavior of the ECUs. Instead, the security specification may require ECUs to verify the legitimacy of all CAN packets sent and received. The authors tested the approach with six different forms of assaults based on [78]: spoofing, replaying, reading, modifying, flooding, and dropping. The examination revealed that the majority of the produced attack models were detectable. The detection, however, is strongly dependent on the role of the ECU; if an attacker has altered the ECU behavior specification, anomaly detection is impossible.

3.1.4.7 Signature-based approach

The signature-based technique distinguishes an assault by utilizing a data set module of IDS [78] to record a bunch of identified marks, unsafe occasions, or rules. This strategy analyzes the organization or framework's action to the assault designs put away in the IDS, and assuming that the conduct fits the malevolent examples, the caution is set off. The mark based method is promising since it is easy to carry out and can work on the exactness of recognizing known attacks. Notwithstanding, on the grounds that this approach is principally dependent on the assault signature data set, it neglects to distinguish new or obscure assaults [79]. Thus, an IDS should constantly refresh new assault signatures. Furthermore, not at all like laid out signature-based IDS in the PC network space, no car producers or logical specialists have yet freely unveiled assault marks in the auto region [36]. To act as assault marks for IDS, Müter et al. planned eight irregularity discovery sensors got from the CAN transport framework highlights [80]. The marks created in the sensors included CAN transport convention details, which characterized permitted bundles as for the expected correspondence transport framework, particulars of parcel payload that agreed with information range, supported bundles recurrence and span conduct, relationship of parcels on different transport frameworks that met the determinations, legitimate correspondence challengereaction conventions, practical information content of bundle payload, lastly non-redundant. To help in the assessment step, the creators provided the sensors' pertinence rules, which incorporate working conditions, necessities, and results for every model. The sensors had the option to identify oddities with no bogus positive alerts, as indicated by the general outcomes. The methodology, then again, couldn't identify infused attacks that followed the CAN particular's run of the mill conduct. Studnia et al. utilized limited state automata (FSA) in distinguishing an unusual succession of CAN parcels by means of the invehicle organization to extricate assault marks acquired from regular ECU determinations [38]. The proposed approach was tried by infusing pernicious parcels into adjusted CAN edges to mimic assault bundles. Albeit the methodologies were effective in distinguishing deviations from common CAN conduct, they were delivered inadequate when the underlying casings of the communicated assault bundles were delivered.

IV. IDPS IN CAN NETWORK

IDS is known as a latent checking framework in the work area IT region. As the name infers, the location is expected to create no reaction to the interruption. An IDPS, otherwise called a preventive IDS, then again, answers odd ways of behaving inside the framework. For instance, firewall rules or details are reinvented to obstruct any parcels in network traffic that begin from the suspect source [81]. Tobias et al. recommended a preventive IDS idea using the vehicle's sight and sound framework in supporting the innovation of car IDPS sooner rather than later in a CAN transport car space [36, 56]. The proposed idea depends on conceivable human-PC interface (HCI) approaches that can be incorporated into IDPS to help

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

drivers once a caution has been raised. The interruption identification framework that fills in as HCI ought to be appropriately developed in light of the fact that its responses could endanger the drivers' wellbeing. Be that as it may, in [6, 12], the principal center was not around a client upheld or robotized interruption discovery framework. All things being equal, the essayists investigated the potential outcomes of a cutting edge mixed media framework that could be utilized to accumulate and assess the driver's response. Thus, this paper momentarily examined the three unique techniques for an IDPS to speak with the driver by means of an assortment of haptic (e.g., force reaction capacity parts, for example, ABS stopping mechanism), acoustic (e.g., sound subsystems part like media player, telephone, sound), and visual (e.g., on-board video screen part like TV framework) actuators gave in present day vehicles. The most ideal cooperation between the vehicle and its driver can be distinguished by involving a variety of ebb and flow vehicle sensors as info. At the point when an interruption is distinguished, the versatile powerful procedure can be engaged. However, Hoppe et al. likewise investigated the issue of interruption reaction frameworks, where it may not be imaginable to make dynamic decisions in the vehicle because of lawful imperatives for wellbeing basic frameworks [36]. Mill operator and Valasek fostered another interruption location and anticipation approach in [1]. They made a smaller irregularity identifying contraption that can be embedded straightforwardly into the vehicle's OBD-II port. From that point forward, the gadget took in the correspondence transport traffic design and perceived any anomalies. At the point when irregularities are found, the CAN transport is short circuited, and all parcels that cross the transport are disabled. This, nonetheless, got new difficulties guaranteeing the expected and carried out implanted frameworks: various security and respectability highlights, constant observing affirmation, and costadequacy [81].

Table 1 Summary of the IDS for CAN bus system literature in the automotive domain. IDS detection strategy methods are proposed based on how the attack manifest into CAN bus network: Manipulation on CAN frequency and CAN packet payload.

References	Detection strategy	Method	Placement strategy	Packet frequency	Packet payload modification
Hoppe et al. [56]	Anomaly-based	Frequency-based	CAN	✓	-
ho et al. [41]	Anomaly-based	Statistical-based (RLS and CUSUM)	CAN	✓	✓
Larson et al. [31]	Specificationbased	CAN 2.0 and CANopen 3.01 specification	ECU	✓	✓
Song et al. [57]	Signature-based	Frequency-based	CAN	✓	✓
Studnia et al. [33]	Signature-based	Finite-state automata	CAN	✓	✓
Müter et al. [55]	Anomaly-based	Statistical-based (entropybased)	CAN	✓	✓
Ling et al. [58]	Anomaly-based	Frequency-based	CAN	✓	✓
Miller and Valasek et al. [1]	Anomaly-based	Frequency-based	CAN	✓	-
Miller and Valasek et al. [45]	Anomaly-based	Frequency-based	ECU	✓	-
Deng et al. [62]	Anomaly-based	Machine learning-based	CAN	-	✓
Wasicek et al.[68]	Anomaly-based	Machine learning-based (ANN)	Central gateway	-	✓
Taylor et al. [43]	Anomaly-based	Machine learning-based	CAN	✓	-
Narayanan et al. [73]	Anomaly-based	Statistical-based (hidden Markov)	CAN	-	✓
Müter et al. [55]	Signature-based	Sensor-based	ECU	-	-
Hoppe et al. [23]	IDPS	Adaptive dynamic-based	CAN	-	-
Hoppe et al. [36]	Anomaly-based	Frequency-based	CAN	-	-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

V. DISCUSSION AND SUMMARY

In the preceding part, we described a study of a wide range of intrusion detection in the CAN bus system, which resulted in various concerns that need to be highlighted in order to support and shape future research for CAN bus IDS in the automotive domain. We studied whether the preference of CAN packet IDS for the anomaly-based technique over other methods (shown in Fig. 5) is attributable to limits and limitations. The private nature of the CAN protocol makes it impossible to employ a signature- or specification-based method, as these approaches necessitate semantic knowledge of the CAN packet, and the protocol may change often. Anomaly detection that is learning-based may be a viable detection method since it can learn from examples and intelligently adapt to the CAN environment independent of the protocol, model, or year of the car. Furthermore, because the characteristics of outliers are often unknown in advance, the anomaly-based technique may detect unique attacks, which is one of the important qualities in IDS [82, 83]. Aside from that, most of the techniques illustrated above, particularly those utilizing machine learning-based anomaly detection, are used in a supervised or semi-supervised fashion. Although the techniques used achieved great accuracy, they require completely labeled data. Obtaining completely labeled data from a real-time CAN, which generates a large volume of data in milliseconds, is problematic. It also requires the assistance of a human expert and takes a long time. As a result, it is preferable to use unlabeled CAN data in an unsupervised way for anomaly detection. In terms of pre-processing dataset methodologies for the CAN bus system, the training efficacy can be improved when a machine learning methodology emerges. The majority of the strategies used in the studies described focus on enhancing the core model and post-processing model while ignoring the study of pre-processing components. The amount of the data has a big impact on the IDS' overall performance, especially for CAN, which broadcasts a lot of packets per second. A comparative analysis of the computing efficiency of data pre-processing methods [84] would be worthwhile for future research. Furthermore, several of the above-mentioned frequency-based approaches can successfully identify a variety of attacks in CAN bus traffic. However, one of the issues we must address is that most approaches can only detect assaults from periodic malicious packets, not aperiodic incursions. Despite being able to detect the inserted aperiodic malicious packets, it is unable to pinpoint the source of the assault. Furthermore, it looks to be a new stumbling block, particularly when dealing with real-time response systems, because IDS monitors CAN bus networks and requires an exception. The response system's implementation may necessitate some further adjusting to the architecture of distinct IDS components. When the reaction mechanism senses something unexpected, it can immediately engage the security mode and allow the car to be parked safely [1, 54]. Because it requires coordination from multiple components, this type of response system may be more difficult to implement than improving detection performance. As a result, while creating a response system for IDS, the primary goal should be to incorporate intelligent human-vehicle interaction, as well as immediate action mechanisms. The majority of the research findings focused on a single IDS module, which may not provide a holistic strategy to fulfilling the vehicle communication system's security demands. It should be supplemented with a lighter cryptography-based approach, such as the message authentication method [72, 81]. Finally, despite the growing interest in developing IDS approaches for the CAN bus system depicted in Fig. 5, few studies have compared their proposed solutions to those developed under similar conditions. It is vital to examine and validate the suggested technique's significant distinctions from other ways in order for the concerned method to reach optimal performance.

VI. DISCUSSION AND SUMMARY

In this paper, we examined information correspondence through CAN transport and explored a few elements of conduct as well as weaknesses that exist basically in the CAN transport framework. The norm and upgraded CAN bundle structures utilized in the car correspondence framework were introduced. Also, we momentarily portray different kinds of plausible assault surfaces in the CAN transport in the accessible writing, going from direct actual admittance to long-go remote access. We likewise present a portion of the security arrangements created by specialists to battle this issue. As far as conventional organizations, perhaps the main security component in giving comprehensive assurance to the CAN correspondence framework in the auto business is the interruption identification system. As an outcome, we assess each potential exploration exertion done on IDS in a writing examine explicitly for in-vehicle CAN transport frameworks, to broaden the past work in giving different procedures of safety countermeasures. We picked 25 examination papers from the writing that introduced different IDS procedures and techniques for recognizing and moderating dangers. We utilize a scientific categorization to classify these exploration distributions in view of the accompanying elements: IDS location strategies, sending systems, going after procedures, and specialized obstacles. As indicated by our perceptions, IDS research for the auto region is building up momentum. In any case, we feel that the worries brought up in this work will furnish scholars with certain groundbreaking thoughts for further developing security around here.

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression, “One of us (R.B.G.) thanks . . .” Instead, try “R.B.G. thanks”. Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

REFERENCES

[1] Miller C, Valasek C. A survey of remote automotive attack surfaces. black hat USA. 2014 Aug;2014:94.
[2] Wolf M, Weimerskirch A, Wollinger T. State of the art: Embedding security in vehicles. EURASIP Journal on Embedded Systems. 2007 Dec;2007:1-6.
[3] Lokman, S.F., Othman, A.T. and Abu-Bakar, M.H., 2019. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP Journal on Wireless Communications and Networking, 2019(1), pp.1-17.

[4] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and Zedan, H., 2014. A comprehensive survey on vehicular ad hoc network. Journal of network and computer applications, 37, pp.380-392.
[5] Papadimitratos, P., De La Fortelle, A., Evenssen, K., Brignolo, R. and Cosenza, S., 2009. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE communications magazine, 47(11), pp.84-95. (2009)
[6] Humayed, Abdulmalik, Jingqiang Lin, Fengjun Li, and Bo Luo. "Cyber-physical systems security—A survey." IEEE Internet of Things Journal 4, no. 6 (2017): 1802-1831.
[7] Sakiz, F. and Sen, S., 2017. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks, 61, pp.33-50.
[8] Petit, Jonathan, and Steven E. Shladover. "Potential cyberattacks on automated vehicles." IEEE Transactions on Intelligent transportation systems 16, no. 2 (2014): 546-556.
[9] Lyamin, N., Vinel, A., Jonsson, M. and Loo, J., 2013. Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks. IEEE Communications letters, 18(1), pp.110-113.
[10] Lee, H., Jeong, S.H. and Kim, H.K., 2017, August. OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame. In 2017 15th Annual Conference on Privacy, Security and Trust (PST) (pp. 57- 5709). IEEE.
[11] [Carsten, Paul, Todd R. Andel, Mark Yampolskiy, and Jeffrey T. McDonald. "In-vehicle networks: Attacks, vulnerabilities, and proposed solutions." In Proceedings of the 10th Annual Cyber and Information Security Research Conference, pp. 1-8. 2015..
[12] Koscher, Karl, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy et al. "Experimental security analysis of a modern automobile." In 2010 IEEE symposium on security and privacy, pp. 447-462. IEEE, 2010.
[13] Boyes, H. A., and A. E. A. Luck. "A security-minded approach to vehicle automation, road infrastructure technology, and connectivity." (2015): 6-6.
[14] Woo, Samuel, Hyo Jin Jo, and Dong Hoon Lee. "A practical wireless attack on the connected car and security protocol for in-vehicle CAN." IEEE Transactions on intelligent transportation systems 16, no. 2 (2014): 993- 1006.
[15] Han, Kyusuk, André Weimerskirch, and Kang G. Shin. "Automotive cybersecurity for in-vehicle communication." IQT QUARTERLY 6, no. 1 (2014): 22-25.
[16] Hartkopp, Oliver, and R. MaCAN SCHILLING. "Message authenticated can." In Escar Conference, Berlin, Germany. 2012.
[17] Groza B, Murvay S, Herrewege AV, Verbauwhede I. LiBrA-CAN: A lightweight broadcast authentication protocol for controller area networks. InInternational Conference on Cryptology and Network Security 2012 Dec 12 (pp. 185-200). Springer, Berlin, Heidelberg.
[18] Szilagyi, Christopher Johnathan. "Low cost multicast network authentication for embedded control systems." PhD diss., Carnegie Mellon University, 2012.
[19] Nilsson, Dennis K., Ulf E. Larson, and Erland Jonsson. "Efficient in-vehicle delayed data authentication based on compound message authentication codes." In 2008 IEEE 68th Vehicular Technology Conference, pp. 1-5. IEEE, 2008.
[20] Van Herrewege, A., Singelee, D. and Verbauwhede, I., 2011, November. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus. In ECRYPT workshop on Lightweight Cryptography (Vol. 2011, p. 20). ECRYPT.
[21] Cho, Kyong-Tak, and Kang G. Shin. "Fingerprinting electronic control units for vehicle intrusion detection." In 25th USENIX Security Symposium (USENIX Security 16), pp. 911-927. 2016.
[22] Hoppe, T., Kiltz, S. and Dittmann, J., 2008, September. Security threats to automotive CAN networks–practical examples and selected short-term countermeasures. In International Conference on Computer Safety, Reliability, and Security (pp. 235-248). Springer, Berlin, Heidelberg.
[23] Marchetti, Mirco, Dario Stabili, Alessandro Guido, and Michele Colajanni. "Evaluation of anomaly detection for invehicle networks through information-theoretic algorithms." In 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), pp. 1-6. IEEE, 2016.
[24] Verendel, Vilhelm, Dennis K. Nilsson, Ulf E. Larson, and Erland Jonsson. "An approach to using honeypots in invehicle networks." In 2008 IEEE 68th Vehicular Technology Conference, pp. 1-5. IEEE, 2008.
[25] Wolf, Marko, and Timo Gendrullis. "Design, implementation, and evaluation of a vehicular hardware security module." In International Conference on Information Security and Cryptology, pp. 302-318. Springer, Berlin, Heidelberg, 2011.
[26] Arilou Cyber Security. (2016). [Online] https://www.nng.com/arilou-cybersecurity/
[27] [28] Argus Cyber Security. (2013). [Online] https://argussec.com/ [29]Berg, Jonas, Jens Pommer, Chuan Jin, Fredrik Malmin, Johan Kristensson, and A. B. Semcon Sweden. "Secure gateway-a concept for an in-vehicle IP network bridging the infotainment and the safety critical domains." 13th Embedded Security in Cars (ESCAR'15) (2015): 1-12.
[28] Larson, U. E., Nilsson, D. K., & Jonsson, E. (2008, June). An approach to specification-based attack detection for in-vehicle networks. In 2008 IEEE Intelligent Vehicles Symposium (pp. 220-225). IEEE.
[29] Nilsson, D. K., & Larson, U. (2009). A Defense-inDepth Approach to Securing the Wireless Vehicle Infrastructure. J. Networks, 4(7), 552-564.

[30] Kleberger, P., Olovsson, T., & Jonsson, E. (2011, June). Security aspects of the in-vehicle network in the connected car. In 2011 IEEE Intelligent Vehicles Symposium (IV) (pp. 528-533). IEEE.

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

[32] Kemmerer, R. A., & Vigna, G. (2002). Intrusion detection: a brief history and overview. Computer,

[33] CHECKOWAY, S., MCCOY, D., KANTOR, B., ANDERSON, D., SHACHAM, H., SAVAGE, S., KOSCHER, K., CZESKIS, A., ROESNER, F., AND KOHNO, T. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In USENIX Security (2011).

[34] Hoppe, T., Kiltz, S., & Dittmann, J. (2009). Applying intrusion detection to automotive it-early insights and remaining challenges. Journal of Information Assurance and Security (JIAS), 4(6), 226-235.

[35] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[36] I. Studnia, E. Alata, V. Nicomette, M. Kaâniche, Y. Laarouchi, A languagebased intrusion detection approach for automotive embedded networks. Int. J. Embed. Syst. 10(1) (2018) United Kingdom

[37] Studnia, I., Alata, E., Nicomette, V., Kaâniche, M., & Laarouchi, Y. (2018). A language-based intrusion detection approach for automotive embedded networks. International Journal of Embedded Systems, 10(1), 1-12.

[38] Bécsi, T., Aradi, S., & Gáspár, P. (2015, June). Security issues and vulnerabilities in connected car systems. In 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS) (pp. 477-482). IEEE.

[39] Taylor, A., Japkowicz, N., & Leblanc, S. (2015, December). Frequency-based anomaly detection for the automotive CAN bus. In 2015 World Congress on Industrial Control Systems Security (WCICSS) (pp. 45-49). IEEE.

[40] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In 20th USENIX Security Symposium (USENIX Security 11).

[41] Taylor, A., Leblanc, S., & Japkowicz, N. (2016, October). Anomaly detection in automobile control network data with long short-term memory networks. In 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA) (pp. 130-139). IEEE.

[42] Lee, H., Choi, K., Chung, K., Kim, J., & Yim, K. (2015, March). Fuzzing can packets into automobiles. In 2015 IEEE 29th International Conference on Advanced Information Networking and Applications (pp. 817-821). IEEE.

[43] C. Miller, C. Valasek, Adventures in automotive networks and control units. Def. Con. 21, 260–264 (2013)

[44] Davis, R. I., Burns, A., Bril, R. J., & Lukkien, J. J. (2007). Controller Area Network (CAN) schedulability analysis: Refuted, revisited and revised. Real-Time Systems, 35(3), 239-272.

[45] D.A. Khan, R.J. Bril, N. Navet, in 2010 IEEE International Workshop on Factory Communication Systems Proceedings. Integrating hardware limitations in CAN schedulability analysis (Nancy, 2010), pp. 207–210

[46] M. Di Natale, H. Zeng, P. Giusto, A. Ghosal, Understanding and using the controller area network communication protocol: theory and practice (Springer Science & Business Media, NY, 2012)

[47] Pike, L., Sharp, J., Tullsen, M., Hickey, P. C., & Bielman, J. (2015, May). Securing the automobile: A comprehensive approach. In InProc. International Conference Embedded Security Cars.

[48] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 28(1-2), 18-28.

[49] Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys (CSUR), 46(4), 1-29.

[50] Butun, I., Morgera, S. D., & Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1), 266-282.

[51] Weber, M., Klug, S., Sax, E., & Zimmer, B. (2018, January). Embedded hybrid anomaly detection for automotive CAN communication. In 9th European Congress on Embedded Real Time Software and Systems (ERTS 2018).

[52] Wang, C., Zhao, Z., Gong, L., Zhu, L., Liu, Z., & Cheng, X. (2018). A distributed anomaly detection system for in-vehicle network using HTM. IEEE Access, 6, 9091- 9098.

[53] M. Müter, N. Asaj, in 2011 IEEE Intelligent Vehicles Symposium (IV). Entropy-based anomaly detection for invehicle networks (Baden-Baden, 2011), pp. 1110–1115

[54] Hoppe, T., Kiltz, S., & Dittmann, J. (2008, September). Adaptive dynamic reaction to automotive it security incidents using multimedia car environment. In 2008 The Fourth International Conference on Information Assurance and Security (pp. 295-298). IEEE.

[55] Song, H. M., Kim, H. R., & Kim, H. K. (2016, January). Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In 2016 international conference on information networking (ICOIN) (pp. 63-68). IEEE.

[56] C. Ling, D. Feng, in 2012 National Conference on Information Technology and Computer Science. An algorithm for detection of malicious messages on CAN buses (Atlantis Press, Paris, 2012) Lokman et al. EURASIP Journal on Wireless Communications and Networking (2019) 2019:184 Page 16 of 17

[57] Carsten, P., Andel, T. R., Yampolskiy, M., & McDonald, J. T. (2015, April). In-vehicle networks: Attacks, vulnerabilities, and proposed solutions. In Proceedings of the 10th Annual Cyber and Information Security Research Conference (pp. 1-8).

[58] M. Gmiden, M.H. Gmiden, H. Trabelsi, in 2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA). An intrusion detection method for securing in-vehicle CAN bus (Sousse, 2016), pp. 176–180

[59] Moore, M. R., Bridges, R. A., Combs, F. L., Starr, M. S., & Prowell, S. J. (2017, April). Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research (pp. 1-4).

[60] Deng, L., & Yu, D. (2014). Deep learning: methods and applications. Foundations and trends in signal processing, 7(3–4), 197-387.

[61] Kang, M. J., & Kang, J. W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. PloS one, 11(6), e0155781.

[62] D. Erhan, Y. Bengio, A. Courville, P.A. Manzagol, P. Vincent, S. Bengio, Why does unsupervised pre-training help deep learning? J. Mach. Learn. Res. 11(Feb), 625–660 (2010)

[63] Valdes, A., & Cheung, S. (2009, May). Communication pattern anomaly detection in process control systems. In 2009 IEEE Conference on Technologies for Homeland Security (pp. 22-29). IEEE.

[64] Zhou, X., Zhang, X., & Wang, B. (2016). Online support vector machine: A survey. In Harmony Search Algorithm (pp. 269-278). Springer, Berlin, Heidelberg.

[65] Hochreiter, S., & Schmidhuber, J. (1997). Long shortterm memory. Neural computation, 9(8), 1735-1780. [69]Avalappampatty Sivasamy, A., & Sundan, B. (2015). A dynamic intrusion detection system based on multivariate Hotelling's T2 statistics approach for network environments. The Scientific World Journal, 2015.

[66] Islam, M. R., Oh, I., Batzorig, M., Kim, S., & Yim, K. (2021, October). A Concept of IDS for CAN Protocol Based on Statics Theory. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 294-302). Springer, Cham.

[67] Marchetti, Mirco, and Dario Stabili. "Anomaly detection of CAN bus messages through analysis of ID sequences." In 2017 IEEE Intelligent Vehicles Symposium (IV), pp. 1577-1583. IEEE, 2017.

[68] Kalutarage, Harsha Kumara, M. Omar Al-Kadri, Madeline Cheah, and Garikayi Madzudzo. "Context-aware anomaly detector for monitoring cyber attacks on automotive CAN bus." In ACM Computer Science in Cars Symposium, pp. 1-8. 2019.

[69] Narayanan, S.N., Mittal, S. and Joshi, A., 2016, May. OBD_SecureAlert: An anomaly detection system for vehicles. In 2016 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 1-6). IEEE.

[70] Krishnan, Deepa, and Madhumita Chatterjee. "An adaptive distributed intrusion detection system for cloud computing framework." In International Conference on Security in Computer Networks and Distributed Systems, pp. 466-473. Springer, Berlin, Heidelberg, 2012.

[71] Pevný, Tomáš. "Loda: Lightweight on-line detector of anomalies." Machine Learning 102, no. 2 (2016): 275-304.

[72] Tseng, Chin-Yang, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, and Karl Levitt. "A specification-based intrusion detection system for AODV." In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 125-134. 2003.

[73] Amaral, João P., Luís M. Oliveira, Joel JPC Rodrigues, Guangjie Han, and Lei Shu. "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks." In 2014 IEEE international conference on communications (ICC), pp. 1796-1801. IEEE, 2014.

[74] Kruegel, Christopher, and Thomas Toth. "Using decision trees to improve signature-based intrusion detection." In International workshop on recent advances in intrusion detection, pp. 173-191. Springer, Berlin, Heidelberg, 2003.

[75] Howard, John D., and Thomas A. Longstaff. A common language for computer security incidents. No. SAND 98- 8667. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Sandia National Lab.(SNL-CA), Livermore, CA (United States), 1998.

[76] Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36, no. 1 (2013): 16-24.

[77] Müter, Michael, André Groll, and Felix C. Freiling. "A structured approach to anomaly detection for in-vehicle networks." In 2010 Sixth International Conference on Information Assurance and Security, pp. 92-98. IEEE, 2010.

[78] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S.A. Fahmy, S. Chakraborty, in Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition. Lightweight authentication for secure automotive networks (Grenoble, 2015), pp. 285–288

[79] Omar, S., and A. Ngadi. "H. jebur, h.(2013)." Machine Learning Techniques for Anomaly Detection: An Overview. International Journal of Computer Applications 79, no. 2: 33-41.

[80] Nawi, Nazri Mohd, Ameer Saleh Hussein, Noor Azah Samsudin, Nur Hamizah Abdul Hamid, Mohd Amin Mohd Yunus, and Mohd Firdaus Ab Aziz. "The effect of preprocessing techniques and optimal parameters selection on back propagation neural networks." International Journal on Advanced Science, Engineering and Information Technology 7, no. 3 (2017): 770-777.

[81] Alasadi, Suad A., and Wesam S. Bhaya. "Review of data preprocessing techniques in data mining." Journal of Engineering and Applied Sciences 12, no. 16 (2017): 4102- 4107.

[82] Malhotra, Pankaj, Anusha Ramakrishnan, Gaurangi Anand, Lovekesh Vig, Puneet Agarwal, and Gautam Shroff. "LSTM-based encoder-decoder for multi-sensor anomaly detection." arXiv preprint arXiv:1607.00148 (2016).

[83] Ji, Haojie, Yunpeng Wang, Hongmao Qin, Yongjian Wang, and Honggang Li. "Comparative performance evaluation of intrusion detection methods for in-vehicle networks." IEEE Access 6 (2018): 37523-37532.

[84] Li, J., 2016. Cansee-an automobile intrusion detection system. In Presentation slides on Hack In The Box Security Conference (HITBSecConf).