Lokman *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:184
https://doi.org/10.1186/s13638-019-1484-3

EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review

Siti-Farhana Lokman*, Abu Talib Othman and Muhammad-Husaini Abu-Bakar

Abstract

The modern vehicles nowadays are managed by networked controllers. Most of the networks were designed with little concern about security which has recently motivated researchers to demonstrate various kinds of attacks against the system. In this paper, we discussed the vulnerabilities of the Controller Area Network (CAN) within in-vehicle communication protocol along with some potential attacks that could be exploited against it. Besides, we present some of the security solutions proposed in the current state of research in order to overcome the attacks. However, the main goal of this paper is to highlight a holistic approach known as intrusion detection system (IDS) which has been a significant tool in securing networks and information systems over the past decades. To the best of our knowledge, there is no recorded literature on a comprehensive overview of IDS implementation specifically in the CAN bus network system. Thus, we proposed an in-depth investigation of IDS found in the literature based on the following aspects: detection approaches, deployment strategies, attacking techniques, and finally technical challenges. In addition, we also categorized the anomaly-based IDS according to these methods, e.g., frequency-based, machine learning-based, statistical-based, and hybrid-based as part of our contributions. Correspondingly, this study will help to accelerate other researchers to pursue IDS research in the CAN bus system.

Keywords: Intrusion detection system, In-vehicle, Automotive communication system, Attack surface, CAN bus system

1 Introduction and motivation

Since the 1970s, there has been an escalating interest in replacing hydraulic or purely mechanical components with embedded electronic system alternatives in automotive industries. As information and communication technology continues to develop, today's vehicles are highly computerized and become rolling computer networks. Moreover, current modern cars which encompass of 20 to 100 ECUs (electronic control units) [1] can coordinate, control, and monitor loads of internal vehicle components. Each component, from the engine system to the braking system, and eventually to the telematics system, can exchange information between neighboring components [2]. As a result of the communication occurred between them finally forming an internal vehicle network. In a typical fuel-based vehicle, the Controller Area Network (CAN) is the most established automotive communication system protocol for the internal vehicle network. It allows safety-critical ECUs that attached to it to sufficiently broadcast information in the form of CAN packets between them and other connected busses (e.g., FlexRay, MOST, LIN) through several gateways (Fig. 1) [3]. Besides, embedded interfaces in modern cars currently could enable wireless (e.g., WiFi, Bluetooth, etc.) as well as wired (USB) to communicate with the outside world [4]. This trend will keep rising in the automotive industry with the future development of vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications [5, 6].

Nevertheless, due to the increasing number of the information exchange within CAN bus system with the busses that interact with the outside world, it introduces an array of security threats fighting their way to penetrate the system [7–10]. These vulnerabilities existing in

* Correspondence: farhana.lokman@s.unikl.edu.my
System Engineering and Energy Laboratory, Universiti Kuala Lumpur, Malaysian-Spanish Institute, Kulim Hi-Tech Park, 09000 Kulim, Kedah, Malaysia

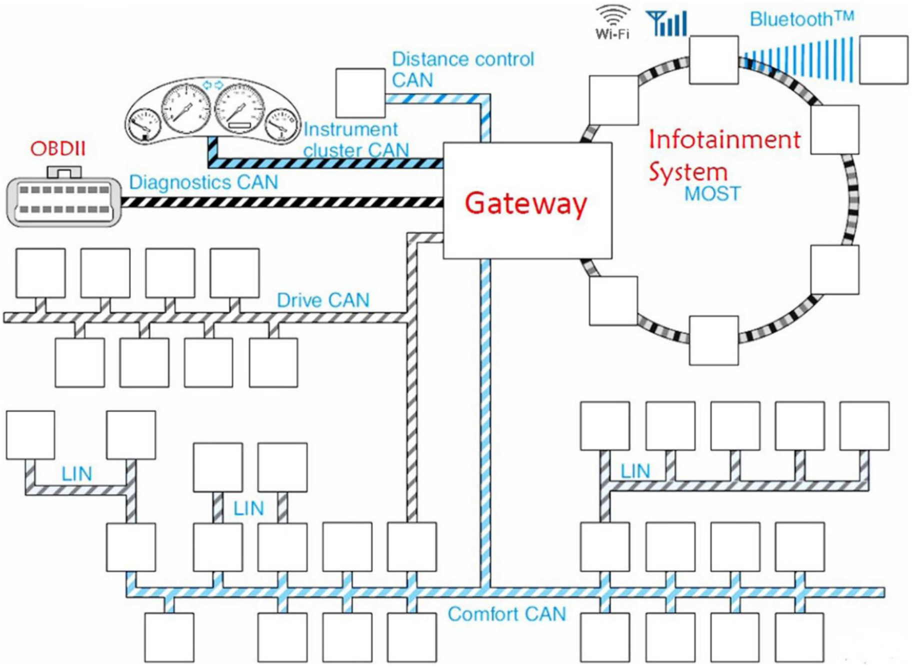

Fig. 1 In-vehicle communication system [88]

CAN bus could harm not only the safety of the driver, but also that of the other vehicles.

Thus, the objectives of this paper are to give an understanding of the behavior of CAN within in-vehicle network as well as its vulnerabilities, to present various potential attacks that could be deployed against CAN bus system, to describe some of the security solutions proposed in current literature, and finally to present an intensive survey of current work on intrusion detection system (IDS)—the most promising approach in securing CAN network. To the best of our knowledge, there is no recorded literature on a comprehensive overview of IDS implementation specifically in the CAN bus network system. Thus, we propose an in-depth investigation of IDS found in the literature based on the following aspects: detection approaches, deployment strategies, attacking techniques, and finally technical challenges. We also categorize the anomaly-based IDS according to these methods, e.g., frequency-based, machine learning-based, statistical-based, and hybrid-based as part of our contributions. The in-depth analysis of each IDS approaches is intended to give the readers a coherent point of view of the current research in this domain to determine a new direction in the future.

1.1 Controller Area Network (CAN)

The vulnerabilities of the system can be fully understood by knowing how the internal system works. Thus, this section describes the standard structure of a CAN protocol as well as some related works concerning attacks on the CAN bus.

1.1.1 CAN data frame structure

The Controller Area Network (CAN) which is also known as CAN bus is a message-based protocol. It was designed to enable numerous electric components, e.g., microcontrollers, electronic control units (ECUs), sensors, devices, and actuators, throughout the in-vehicle system to communicate with each other through a single/dual-wire bus. CAN works by broadcasting its packets in nature, which means all nodes that attached to the CAN bus can receive all packet transmissions. Further, a frame in CAN packet is defined as a structure; it carries a sequence of CAN data (bytes) in the network. The arbitration identifier (ID) field for each transmitted CAN frame indicates packets priority. The lower the ID bit value signifies the higher priority of the packet. This protocol is intended to avoid collisions within the CAN bus traffic.

CAN data frame is comprised of 4 types [11]: data frame, error frame, overload frame, and remote frame. The standard structure of each frame contains these fields: arbitration identifier, data, acknowledge, and a few others. In this paper, only CAN data frame with ID as well as data fields are considered. The bit value format for the CAN packet ID field is usually 11 bits or can be extended to 29 bits. While the CAN data field carries 0 to 64 bits of data. The details semantic of CAN ID and data field are proprietary and are kept highly confidential from vehicle manufacturers. Figure 2 exhibits the basic CAN data frame structure for standard and extended arbitration identifier versions.

Each field contained within the CAN data frame is described below:

a. *Start of frame* (*SOF*). It specifies the beginning of a CAN message with a dominant bit and notifies all nodes a start of CAN message transmission.
b. *Arbitration*. As stated earlier, it comprises of 11 bits and can be extended up to 29 bits' format.
c. *Control*. It is also known as *check field*; it provides information for the receiver to check whether all intended packets are received successfully.
d. *Data*. This data field contains actual information for CAN nodes to perform actions. It can be 0 to 8 bytes.
e. *CRC*. It is known as *cyclic redundancy code* or *safety field*, a 15-bit fault detection mechanism which checks for packets validity.
f. *Acknowledge* (*ACK*). Also known as *confirmation field***.** This field assures that the receiver nodes receive the CAN packets correctly. Whenever it detects an error during the transmission process, the transmitter will be notified immediately by the receiver to send the data packets again.
g. *End of frame* (*EOF*). This field indicates the end of the CAN frame by a recessive bit's flag.

The only frame that is used for transferring CAN packet information is the CAN data frame. Hence, the CAN bus communicates with other nodes by transmitting the packets through the data frames. Whenever the RTR (remote transmission request) bit flags as dominant, it turns into a CAN data frame.

1.1.2 CAN vulnerabilities

Carsten et al. [12] discussed several critical vulnerabilities that exist in the CAN bus system. The author has stated that CAN packets do not contain any information of the transmitter and the receiver address. As mentioned earlier, all CAN packets broadcast to all CAN nodes based on the arbitration identifier field. Thus, the receiver nodes could not tell whether the received packets are intended for them as the origin of the packets are not provided. Judging from this fact, the receiver node could not ascertain whether the packet received is legitimate or not. Moreover, each ECU does not have a message authentication mechanism in securing the packets transmitted between nodes; thus, compromised ECUs could be used by the attackers to spoof and send fake CAN packets. All of the above issues make a CAN bus system insecure as well as ill-equipped in identifying which nodes have mounted the attacks.

1.1.3 Attacks on CAN bus

Major work done in finding potential vulnerabilities in the automotive communication system, specifically for CAN bus protocol, was initiated by Koscher et al. in 2010 [13]. The researchers revealed that they could make changes to a wide range of vehicle's safety-critical components through a physical-access, non-physical access, and short- and long-range access to a vehicle. Some of the demonstrated attack models of physical access were through on-board diagnostics (OBD-II) which resulted in manipulating speedometer reading in the car's instrument panel, jamming the door locks, killing the engine, and etc. These impacts are resulted by flooding the vehicle's CAN bus with a large number of fake CAN packets.

Also, Boyes et al. (2015) raised several issues concerning the security and privacy of the vehicular network due to the expansion of the attack surface [14]. As a result of the inherent characteristics of short and long wireless medium embedded in the vehicle's infotainment system, they discovered that a multitude of attack surfaces could be remotely exploited through USB, Bluetooth, and WiFi. The potential adversaries can gain advantage from these vulnerabilities by just simply reverse engineering the system.

Further, in 2015, Miller and Valasek demonstrated a few crafted messages in the form of CAN packets that were sent remotely through the Jeep Cherokee's potential entry points (e.g., TPMS and Cellular). As a result, some of the car's critical component like the braking system was disabled. As well, the steering wheel turned 180° while the passenger was driving in traffic [4]. Thus, these attack surfaces that exist in the vehicle system eventually have brought to security researchers' attention that most modern automobile systems have been designed with safety, but no security in mind. For this reason, proposing a holistic approach for the security of the

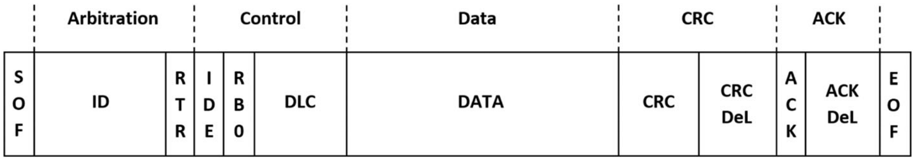

Fig. 2 The structure of the CAN data frame [22]

CAN bus is vital in ensuring long-term protection within an in-vehicle network.

2 Related works on automotive security

In this section, we review current literature studies on automotive security specifically on the CAN bus system. The research on automotive security has emerged recently. Some ongoing studies and projects have been published in providing possible defense-in-depth mechanisms in securing in-vehicle CAN bus system.

One of the popular security solutions which have been exploiting cryptographic-based software is message authentication [15–18]. Researchers that proposed this method attempted to borrow from the internet security approach in addressing CAN network security issues. This proposed method ensures that the exchanged CAN data frame between the two end nodes is authorized. Nevertheless, the maximum length of the CAN data frame is fixed to only 8 bytes. Thus, the available space allocated to adopt this method is very limited. Several countermeasures have been carried out to address the issue, e.g., truncating a MAC across several CAN frames [19], utilizing various of CRC fields to add 8 bytes of CBC-MAC [20], and using an out-of-band channel to authenticate the message [21]. However, relying on this approach alone cannot assure complete security in preventing a certain high level of threat especially denial-of-service (DoS) attack [22]. Additionally, this approach protects only a small scope of vehicle components and necessitates all ECUs to have a major modification which is unpractical [23, 24].

In another front, Verendel et al. [25] proposed a security mechanism known as honeypot which was placed at the wireless gateway and acted as a decoy in simulating the in-vehicle network. Any information regarding the attacks occurred was collected and analyzed in order to enhance the later version of the system. Nonetheless, one of the challenges in deploying honeypot is that it should be realistic as possible so that the attacker would not realize he is not infiltrating the “real” network.

Wolf et al. [26] proposed a firewall concept architecture in order to secure the vehicular communication gateways. The concept is based on the firewall signatures (a specific configurable rule) which filtered authorized controllers to exchange valid messages within the CAN bus network. However, he also claimed that the simple security mechanism like firewall could not fully shield the vehicle network, as most modern vehicles have embedded diagnostic interfaces that enable access to the entire car system.

On a side note, there are also numerous companies that have been putting their effort in addressing many aspects of attacks within the in-vehicle network system. For instance, Arilou Cyber Security offers a revolutionary parallel intrusion prevention system (PIPS), an approach that provides a detection of the source of each CAN packet on the bus. As well, it also utilizes an electronic signature to recognize the signals that came from the different ECUs. In this way, the transmission of infected CAN packet can be prevented. Being employed concurrently to the CAN bus, the PIPS gives a complete protection of the entire network [27]. On the other hand, Argus Cyber Security aims to provide protection capabilities on a wide array of communication network protocol such as FlexRay, CAN flexible datarate (CAN-FD), Ethernet, and more [28]. Besides, Berg et al. of Semcon Automotive Cyber Security [29] proposed a protection layer at the infotainment unit by implementing secure gateway (SG), a concept that gives secure access from installed applications in the infotainment system to the internal vehicle network. This concept is composed of three layers’ architecture: a network, messaging, and service layer.

In response to automotive security attacks, the authors in [30] proposed five layers of security defense approach in securing wireless vehicle framework: detection, prevention, recovery, countermeasure, and deflection. In [31], the authors extended the discussion on the five layers of potential security solutions by proposing detail approaches for each layer: message authentication in preventing unauthorized access, logging mechanisms for intrusion detection system (IDS), reacting towards the attacks via intrusion prevention system (IPS), and finally the need of traceability in conducting recovery. Moreover, [32, 33] reviewed the potential vulnerabilities within the in-vehicle network and some technical challenges in securing the in-vehicle bus system. As well, they presented some protection mechanisms through cryptography-based technique, IDS, honeypot, firewall, and IPS. Thus, we extend the discussion on the protection mechanism in this paper specifically on intrusion detection system (IDS).

Although many security solutions have been proposed, CAN bus communication system is still vulnerable to a multitude of attacks trying to violate the security of the network, especially for the vehicle long-term service life, the threat landscape that is constantly changing. Every new connectivity service introduces new attack vectors. Attackers are continuously perfecting their methods to undermine existing protection mechanisms and find loopholes. Judging from this fact, it is not enough to guarantee state-of-the-art security at the point where the vehicles roll off the production line. Another alternative layered security model is needed in providing a holistic approach, which is called an intrusion detection system (IDS). The details of work done by previous researchers on IDS in CAN bus system is explained further in Section 3.1.6.

3 Intrusion detection system (IDS)

An intrusion detection system (IDS), in particular, raises many interests largely due to its simplicity and the ability in detecting the attacks efficiently. Generally, IDS monitors activities in the network or directly on the host, detects, and raises the alarm if there are any unexpected events occurred in the system [34]. These unusual events, known as intrusions are fighting their way into the system so that unauthorized access can be obtained. The intrusions may come from internal, which resides inside the targeted system components having legal access privilege to the network, whereas external intruders may come from the outside of the targeted network, attempting to gain illegitimate access to the system components [35]. IDS can be passive or active depending on how it was set up. Passive IDS only detects the attack while active IDS takes preventive action on the attack. Essentially, a typical IDS architecture is encompassed of sensors, a detection engine, and finally a reporting module. The sensors are implemented either within the network (network-based IDS) or directly to the end node (host-based IDS). The IDS techniques can be categorized as signature-, anomaly- and specification-based. The details about IDS implementation for the automotive domain will be elucidated in the subsequent section. Analysis of advantages, as well as its disadvantages, will be presented.

3.1 IDS in automotive domain

The concept of IDS application to the automotive system was first introduced by Hoppe et al. [36] with the focus on the typical CAN bus network. A summary for every work done in the existing literature is explained based on the detection methods: signature, anomaly, specification, and hybrid based in section 3.2. However, before we begin to discuss further, we illustrated a proposed taxonomy (inspired from [37]) for the CAN bus network IDS in the automotive domain. The CAN bus network IDS taxonomy is discussed based on these core aspects (see Fig. 3): IDS detection approach, deployment strategy, attacking techniques, and finally technical challenges. The summary of investigated research efforts in designing IDS for the automotive environment based on these four attributes is illustrated in Table 1.

3.1.1 IDS deployment strategy

For IDS to monitor activities in the CAN network from different sources, it needs to be deployed to each monitored systems. Based on findings in [36, 38, 39], to achieve this in the automotive environment, they proposed these locations that are ideal for IDS deployment (as illustrated in Fig. 4): (A) CAN networks, (B) ECUs, and (C) central gateways. In analogy to intrusion detection of desktop IT, attaching an IDS directly to each vehicle ECUs is known as a host-based IDS. It provides a complete view of the internal activities occurred in the system. As a result, injected malicious code can be detected during runtime. Meanwhile, placing an IDS to the CAN network as well as central gateways are known as network-based IDS. It monitors and inspects the onboard vehicle communication system in identifying the active attacks.

However, there are a few aspects that need to be taken into account when designing an IDS into the in-vehicle system. A previous study done by Kleberger et al. and Koscher et al. examined the impact of attacks on the ECUs which were placed at a different location within the in-vehicle communication system [13, 40]. The risk of a compromised CAN network and central gateways

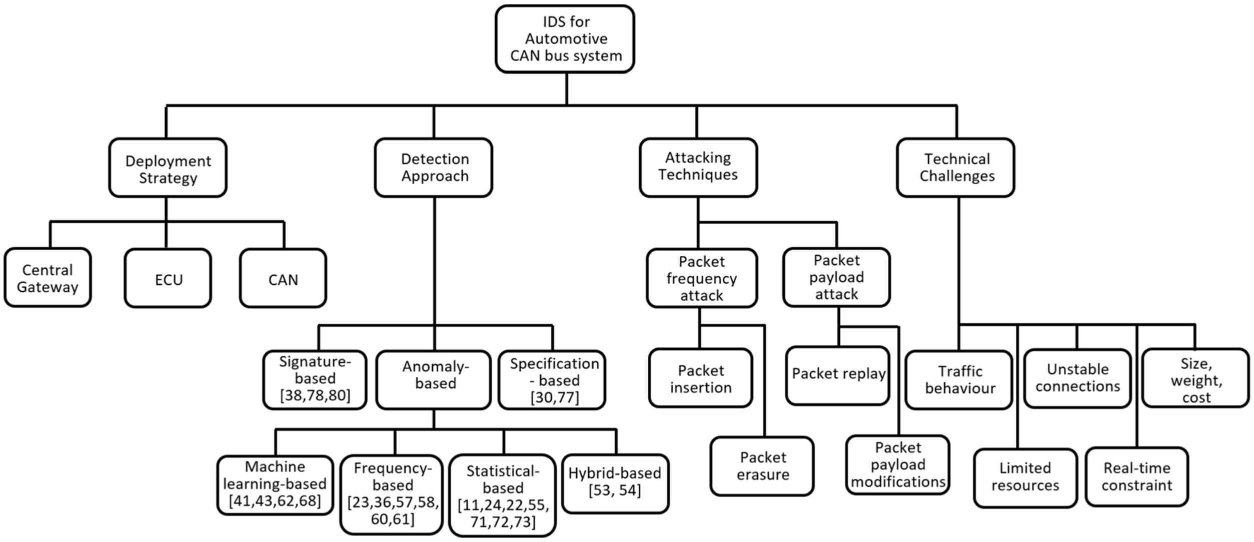

Fig. 3 The IDS taxonomy for CAN bus network in automotive domain is inspired by four core aspects covered in this review. The four core aspects are organized by their deployment strategies, attacking techniques, technical challenges, and finally detection approach

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

Key references	Detection strategy	Method	Placement strategy	Packet frequency	Packet payload modification
Hoppe et al. [36]	Anomaly-based	Frequency-based	CAN	✓	–
Hoppe et al. [56]	IDPS	Adaptive dynamic-based	CAN	–	–
Larson et al. [30]	Specification-based	CAN 2.0 and CANopen 3.01 specification	ECU	✓	✓
Hoppe et al. [36]	Anomaly-based	Frequency-based	CAN	✓	–
Müter et al. [81]	Signature-based	Sensor-based	ECU	–	–
Müter et al. [55]	Anomaly-based	Statistical-based (entropy-based)	CAN	✓	–
Ling et al. [58]	Anomaly-based	Frequency-based	CAN	✓	✓
Miller and Valasek [45]	Anomaly-based	Frequency-based	CAN	✓	–
Miller and Valasek [1]	Anomaly-based	Frequency-based	CAN	✓	–
Studnia et al. [38]	Signature-based	Finite-state automata	CAN	✓	✓
Wasicek et al. [68]	Anomaly-based	Machine learning-based (ANN)	Central gateway	–	✓
Taylor et al. [43]	Anomaly-based	Machine learning-based (deep neural network)	CAN	✓	–
Narayanan et al. [73]	Anomaly-based	Statistical-based (hidden Markov)	CAN	–	✓
Song et al. [57]	Signature-based	Frequency-based	CAN	✓	–
Kang et al. [62]	Anomaly-based	Machine learning-based (deep neural network)	CAN	–	✓
Cho et al. [22]	Anomaly-based	Statistical-based (RLS and CUSUM)	CAN	✓	✓
Taylor et al. [41]	Anomaly-based	Machine learning-based (OCSVM)	CAN	–	✓
Gmiden et al. [60]	Anomaly-based	Frequency-based	CAN	✓	✓
Marchetti et al. [24]	Anomaly-based	Statistical-based (information theoretic)	CAN	–	✓
Marchetti et al. [71]	Anomaly-based	Frequency-based (transition matrix)	CAN	✓	–
Lee et al. [11]	Anomaly-based	Time-based (offset ratio and time interval-based)	CAN	✓	✓
Moore et al. [61]	Anomaly-based	Frequency-based (Markov)	CAN	✓	–
Wang et al. [54]	Hybrid-based	Hierarchical temporal memory (HTM)	CAN	–	✓
Weber et al. [53]	Hybrid-based	Specification-based and machine learning-based	ECU	✓	✓
Tomlinson et al. [72]	Anomaly-based	Statistical-based (ARIMA and Z score)	CAN	✓	✓

are greater than a compromised ECU [40]. This is due to the reason that a compromised network and central gateways have access and control over packets that traverse through network gateways to the targeted ECU domains.

3.1.2 IDS attacking techniques

Based on the recent studies concerning attack surface exist within CAN network presented in Section 1.1.3, the different type of attacks described in [1, 11, 13, 22, 23, 41–45] are considered in this paper. Briefly, the CAN bus traffic is affected by these two types of attacking techniques: (1) attack on CAN packet frequency and (2) attack on CAN packet payload. These attacking techniques are the most commonly used in evaluating the sensitivity and the effectiveness of the proposed IDS. We explained on the CAN frequency attack and CAN packet payload manipulation attack further in the following subsection.

3.1.3 Attacks on CAN packet frequency

The time interval between the CAN packet IDs is fixed and periodic. Thus, the attacks that are involved in the CAN packet frequency is done by inserting an extra packet or erasing legitimate packet from the CAN bus traffic [22, 23, 41, 42, 45].

a. Packet insertion

Most attacks involved in causing cyber-physical effects on the vehicle are done by inserting extra CAN ID or, at the same time, can be combined with the insertion of modified CAN packet payload into the traffic. However, the inserted packet needs to be designed to be legitimate and valid for the vehicle to get affected. In addition to the CAN frequency attack, the packet is flooded with the highest priority ID of the CAN packet and is inserted within a short cycle. By occupying the CAN bus with priority-based protocol scheme and if the rate of insertion is faster enough, it could enable an ECU to

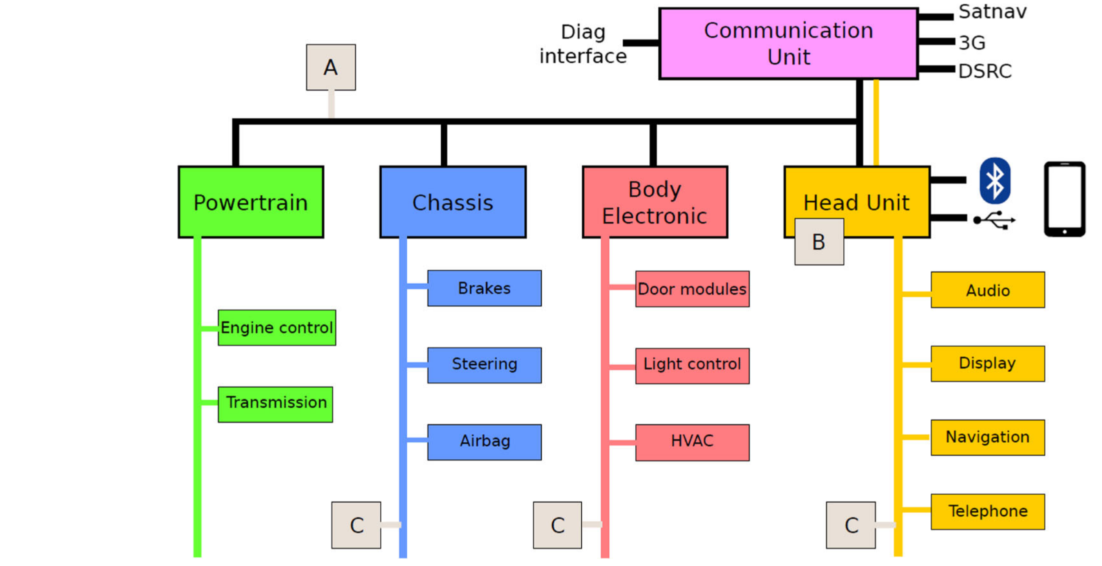

Fig. 4 Possible locations for IDS deployment in the CAN bus system. A) CAN, B) ECU, C) gateways [38]

constantly broadcast CAN packet with a dominant state [11]. As a result, it would cause other legitimate packets with a lower priority to back off (e.g., DoS attack).

b. Packet erasure

The absence of normal CAN packet which is expected to arrive at a fixed interval could allow attacks to manifest into the traffic. For instance, the adversary could take over the target ECUs and manipulate them to stop all legitimate CAN packet transmission [22]. When the victim ECU stops sending the intended packets, all packets transmitted from the impersonated ECU would be entirely removed from the CAN bus traffic. Finally, after the inserted packet is finished taking over the traffic, the missing packet stream will be resumed, and the phase would be probably different than before.

3.1.4 Attacks on CAN packet payload

The attack on CAN packet payload is done by manipulating or spoofing the data content of some CAN ID. The manipulated data may be transmitted within the new inserted packet on the traffic, or it may be included within the normal CAN packet stream. The spoofed CAN packet payload can be done by compromising the ECU externally in order to transmit the manipulated packets. This kind of attack is unlike the inserted packet, where it focuses on changing values within packet content and does not comprise inserting new packets. The manipulated packet content also must be valid; otherwise, it would not produce any effects on the vehicle. This type of attack consists of packet replay and manipulation of packet payload.

a. Packet replay

The packet replay attack is achieved by capturing real-time CAN packet traffic which is known to produce some effects on the vehicle. The captured packet is then replayed, in which the normal CAN packet in the traffic is replaced with the historical packet, to cause the historical effects. This attack is the easiest way to be performed as it does not require any understanding of how the traffic operates. Despite the fact that the replayed packet is a valid subsequence, however, the replaced packet is inconsistent with the prior packet sequence. As a result, it can lead to even serious problems such as non-stop requests of CAN packet transmission [46], violation of the deadline [47], and significant CAN arbitration priority scheme inversion [48]. Further, the sequence of the CAN packets would also change from the original and thus prevents the vehicle to operate properly as the packets are not transmitted sequentially and violate the protocol requirement. Even though the frequency of CAN packets remains the same, nevertheless, the problems stated above are critical which may, in turn, undermine the safety of the vehicle.

b. Packet payload modifications

The CAN packet modification is described as changing values within packet payload in order to perform unintended behavior. In this case, it may not be possible to define valid packet manipulation for this kind of attack. Moreover, the packet payload is manipulated either by setting the packet content with a constant value, i.e., minimum or maximum value, or random value. For example, packet payload modification like fuzzy attack works by changing values of CAN ID as well as CAN packet content randomly.

3.1.5 IDS technical challenges

There have been some challenges highlighted in previous works [31, 40, 49] that need to take into consideration when designing proposed solutions in the CAN bus network system: limited resources, the timing requirement, traffic patterns behavior, unstable connection size, weight, and cost.

1. Limited resources: all ECUs reside within a vehicle harbor several limitations concerning memory storage, computational power, and data transmission rate (bandwidth).
2. Real-time constraint: the CAN packets are transmitted from the ECUs to other node's work in real-time, thus delaying and queuing of packet buffers are too risky and intolerable. The CAN packet received from the vehicle's sensors has to be managed in real-time so that the actuators can perform a vehicle's function without imposed any delay. The real-time limitation needs to be taken into account when proposing any security solutions.
3. Traffic behavior: the CAN traffic protocol patterns for automotive communication system vary from conventional Internet Protocol (IP) networks. For instance, CAN packets are broadcasted in nature. Further, in order to perform firmware updates and wireless diagnostics on vehicles, a temporary connection from in-vehicle to V2I needs to be established which requires different solutions for communication models and traffic protocols. Hence, adopting IP network solution is not possible.
4. Unstable connections: since vehicles are moving, regardless of the speed, they may move into a region that does not have internet connections. Hence, IDS solutions for the automotive domain should be aware that the connection establishment to a third-party may not always available.
5. Size, weight, and cost: IDS solutions may vary in weight and size, and it may also need some minor or possibly major modification which will eventually affect the cost. As an example, removing a CAN bus network which adopts line topology, to be replaced with an Ethernet bus network which adopts different topology, requires an abundance of extra wiring and may be infeasible.

3.1.6 IDS detection approach

The intrusion detection method in the automotive domain depends on how the detection mechanism is utilized within the system. It comprises of four categories, which are anomaly-, signature-, specification- and hybrid-based. Compared to the signature- and specification-based technique, the anomaly-based IDS is the most common and promising approach used in the automotive IDS. The inclination towards the anomaly-based IDS in the CAN bus system compared to other IDS technologies are explained further in Section 4.

3.1.6.1 Anomaly-based approach Briefly, anomaly-based IDS [50] observes a real-time system's activities and compare it against a normal behavior that has been recorded into a profile. Whenever the deviation from normal profile behavior reaches a certain threshold, it will raise the alarm. This anomaly-based approach also can effectively detect new attacks after undergoing a training phase. Nevertheless, it is not necessarily a simple task, to begin with, as this approach considers anything that deviates from a normal behavior would be a signal of intrusions [51]. As a result, this approach poses a serious problem where it also generates false-positive alerts on normal packets. To build a profile of normal behavior, the most common techniques that have been employed by the previous researchers are frequency-based, machine learning-based, and statistical-based technique [52]. Meanwhile, a hybrid-based anomaly detection solution is still emerging [53, 54]. These techniques however require a lot of computational power [54] which may need to be considered before implementing into low capacity ECUs. Consequently, the anomaly-based approach should take this issue into account, in particular, for the CAN bus system in the automotive domain.

As far as anomaly-based IDS is concerned, numerous research articles proposed in the literature such as [22, 34, 36, 41, 55, 56] have been exploiting the timing interval of CAN traffic and the frequency of CAN packet sequences in identifying anomalies within the CAN bus network. This is due to the nature of CAN network traffic which constantly broadcasts the fixed CAN packet ID and payload to any listening ECUs at a fixed time interval and frequency. Thus, any deviation from the normal traffic may be an indication of attacks in the system. The following taxonomy of the anomaly-based IDS within the automotive domain is explained according to frequency-based, machine learning-based, statistical-based, and hybrid-based method.

3.1.6.2 Frequency-based method In [45], Miller and Valasek stated that to detect attacks in a CAN bus is very straightforward. This is due to the predictability of a normal CAN bus traffic which broadcasts packets at a fixed time interval. By observing the CAN behavior on which ECUs interact, they proposed that utilizing known CAN packet frequency between the packet sequences can detect anomalies. Nevertheless, relying on the predictability of CAN frequency alone cannot detect anomalies from irregular or unpredictable CAN packets in the traffic due to the noisy environment in CAN network [57].

As mentioned before in Section 3.1.1, Hoppe et al. were the first ones to introduce the IDS approach in the automotive domain. In [23, 36], they proposed an anomaly-based IDS solution as an exemplary short-term countermeasure in dealing with current automotive threats. To evaluate the method, four selected attack case studies targeting the vehicle control systems have been conducted. The targeted electric components consist of window lift, airbag control system, warning lights, and central gateway ECU. Systematic process analysis of the attacks was organized by using CERT taxonomy. Based on the CERT analysis, there were three characteristics of identified patterns that can be employed into IDS so as to address the 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 communication of the CAN bus. Based on the result, they could identify patterns that are relatively simple to be developed and deployed as well as very cost-effective.

Song et al. adopted a very light-weight algorithm based on the observance of CAN packets frequencies [57] inspired from [23, 45]. They simplified the detection algorithm so that it could react faster to the intrusion while, at the same time, computing power usage can be reduced. The method works by computing the time interval of the latest packets from its arrival time (usually lower than 0.2 ms). If the time interval is shorter than a given threshold, then the IDS will identify that intrusions are taking place. To evaluate the effectiveness of the algorithm, packet frequency attacks were performed using modified CAN packets captured from a well-known car manufacturer. The first type of attack was injecting packets having a single CAN ID. The second attack was injecting pre-ordered packets randomly with multiple CAN IDs and, finally, injecting high amounts of CAN packets similar to DoS attack. The overall experimental results presented a 100% accuracy of the detection without causing any false alarm. Despite high detection accuracy, however, it could not detect irregular incoming packets.

In [58], Ling et al. employed an algorithmic-based detection solution in dealing with major vulnerabilities occurred in CAN bus traffic: DoS attack and misuse of error flag. The DoS attack always wins priority-based arbitration ID as it flooded the network with a large number of high priority packets and dropped the lower priority legitimate packets. The error flag is exploited to disable the communication mechanism for the packets can be processed without discrimination. Further, the proposed system used threshold and resettable counters in monitoring legitimate and illegitimate CAN ID that broadcasted consecutively outside the predetermined thresholds. Although the design of the model is based on the CAN system capacity limitation, it could successfully detect malicious activity in the CAN network. Despite that, the author in [59] stated that the proposed algorithm and the alarm response towards the attack are not clear and, thus, undermine the report.

Gmiden et al. [60] proposed the anomaly-based detection method based on the time interval feature of the consecutive CAN packets. The concept of the proposed IDS is slightly similar to that in [58]. The only difference is that they calculated the arrival time of the packets and compared with the prior packets. Though the method did not require major modification in CAN protocol, however, they do not consider DoS attack and could not detect irregular packets.

The nature of the fixed interval between the CAN packets also has been made prominent by Moore et al. [61] to adopt time analysis in other vehicle models. The proposed method does not only base on the regularity of most parameter ID (PID), but also relies on the redundancy nature of PID signal broadcasted in the CAN traffic. They performed packet insertion attack in exploiting the regular-frequency nature normal CAN packet. While this method achieved significant progress in terms of high detection accuracy against the three types of packet frequency attack, however, automating algorithm parameters such as adjusting threshold and changing training time when experimenting with larger and wider variety of attacks is necessary.

3.1.6.3 Machine learning-based method Machine learning-based method usually falls into a supervised or unsupervised category, which is trying to learn the feature representation from the input data. A supervised category requires fully labeled data when training a model, whereas unsupervised category does not, in which the classes between the given inputs are defined based on their similarity. The difficulties in predicting and generating attack behavior in evaluating the CAN bus system, as well as the need of generalization that is appropriate with the proprietary environment of CAN protocol, thus encourage researchers to propose supervised or semi-supervised anomaly detection methods.

Kang et al. were the first ones to employed machine learning-based IDS, which is, in this case, semi-supervised deep neural network (DNN) [62] method for CAN bus network [63]. The packets exchanged between ECUs were acquired directly from a bitstream in the CAN bus lines before being decoded. Due to the non-linearity of

CAN packet features, the author proposed the restricted Boltzmann machine (RBM) in training the extracted parameters [64]. The algorithm gives the probability for every single class in the form of logistic value "1" and "0" to separate the normal from the malicious packets. To reduced time consumption, an off-line training was performed during the training phase, while the binary decision based on the trained features was executed against incoming new CAN packets in the detection phase. The authors validated the model using spoofed tire pressure monitoring system (TPMS) packets in order to display the wrong values of TPMS indicator on the dashboard. Despite the 99% detection ratio, however, the computational complexity, the training time, and the testing time increase as the amount layers were added.

Taylor et al. utilized a supervised one-class support vector machine (OCSVM) in detecting any deviations from normal frequencies of CAN packet [41]. The authors brought up a problem concerning the high rate of false alarm when evaluating CAN traffic. As an example, if the traffic is observed every 0.5 s, a rate of 10^{-4} false alarm will be raised every hour. As a result, the driver will ignore, assuming it useless. By understanding the method's practical limitations, the authors proposed an algorithm adapted in [65] by measuring statistics of the CAN bus traffic flows in terms of its frequencies and average packet changes. The obtained statistics then is compared against the historical values in determining the anomaly signal. The OCSVM [66], in this case, is used to classify the CAN traffic flows. The authors evaluated the proposed model by simulating packet insertion attack using modified pre-captured CAN packets extracted from a 5-min drive car at low speed. Briefly, the result showed that they detected a very small number of packet injections and reduced false alarm ratio.

Taylor et al. developed a supervised long short-term memory (LSTM) [67] to predict the next value for a given input sequence [43], since raw CAN packets contents are a string data type. The proposed algorithm is used to train the received CAN input in predicting the subsequent data field values broadcasted from each sender that attached to the CAN bus. Any errors that occurred in the input sequence are used to indicate anomalies. The authors used modified CAN packet to simulate attack traffic using three common techniques: packets are flooded into the bus, unusual data packets content appeared, and intended packets did not turn up. The experimental result presented that the anomalies could be detected with the lowest rate of false alarm. Nonetheless, it worked only for a single CAN ID and did not support online learning.

Wasicek and Weimerskirch considered a semi-supervised chip tuning-based method in detecting attacks that were trying to modify parameters or reflashing memories within the ECUs and integrating new hardware to make the CAN network traffic behave abnormally [68]. The author extracted five parameters from each feature, torque, revolutions per minute (RPM), and speed, to classify engine's power ECU behavior in diverse CAN traffic conditions. They also proposed to add time-shifting signals in reducing noise within the CAN bus system. The training process began with feeding the CAN input data into the bottleneck of the artificial neural network (ANN) model and trained them via backpropagation. Finally, they used root-mean-square error to combine the final output and to produce a single anomaly score. Despite the promising results in getting higher true-positive detection against false-positive rate, however, the diagonal ROC graph displayed in the paper is inclined to the line of no discrimination.

3.1.6.4 Statistical-based method The statistical-based IDS method compares the present statistical observation with the priorly determined statistical observation. For instance, [69, 70] used statistical properties, e.g., mean, variance, and standard deviation, in finding unusual behavior within the modeled system. In the CAN bus network IDS, the statistical-based method can be applied by utilizing a rolling window into the time series of the CAN bus traffic: univariate or multivariate time series. The univariate technique analyzes the CAN ID fields independently. However, in the case of multivariate technique analyses, it may be susceptible to timing intervals that involve CAN ID, but it may not be effective for CAN packet content. The reason is that it does not consider the contextual of strings in a CAN data sequence [49], due to automotive parameters being highly interdependent [45]. For example, the CAN data field content changes one bit at a time when the car accelerates. Thus, the multivariate technique may be appropriate in detecting intrusions only in the CAN packet data field content.

Marchetti et al. introduced the information-theoretic algorithm motivated by the entropy application implemented in [55] to detect anomalies in the CAN traffic [24]. The authors captured nearly 48 million of CAN packets for training the model and created a baseline for normal packets behavior built upon their statistical entropy level. For the evaluation part, several types of forged CAN packets were injected, targeting a vehicle's safety-relevant components while the car was driven at a high speed. Finally, the experimental results indicated that the entropy-based IDS approach is practical in detecting large numbers of malicious CAN packets. However, the method could only detect high rates of the packet but was less successful for a small volume of packet injection as it required several entropy computations assigned to each ID to be executed in parallel.

Marchetti and Stabili developed an algorithm in building a model based on the sequence of the transition between packet IDs observed in the CAN bus system [71]. The workflow of the proposed model is comprised of two main phases: training phase and a detection phase. The training phase involved gathering pre-captured CAN packet, and 20% of them were trained to structure a legitimate model in the form of the transition matrix. The resulting model which is composed of true or false caused an extremely low latency in getting into the transition value. The model is assessed using the CAN packet injection to perform realistic attacks. All in all, the results positively demonstrated that the proposed solution could detect stealth attack as well as high-probability attack without causing any false-positive alarm. However, it appeared to be ineffective in detecting a replay attack wherein normal packets are retransmitted.

Cho and Shin adopted a clock-based IDS (CIDS) in their proposal [22] based on their investigation of three typical attacks which occurred within in-vehicle CAN network, i.e., masquerade, suspension, and fabrication attacks. Based on their analysis, the masquerade attack could not be detected comprehensively as the sender's address in messages is not presented. Thus, the authors introduced to fingerprint each ECU's timestamp after observing the periodicity behavior of CAN packet timing intervals at the receiver's side. The baseline of the fingerprinted ECUs was constructed using recursive least squares (RLS) algorithm, while the cumulative sum (CUSUM) analysis is utilized to assess the error. The model is evaluated through the implementation of CIDS within a CAN bus network prototype. The authors validated the proposed model by reprogrammed the CIDS on three different vehicle models. The overall experimental result indicated that various types of attack could be detected with the lowest 0.055% of false-positive error and could identify the source of attack from the compromised ECUs.

Müter et al. presented the entropy-based applicability in detecting anomalies in the CAN bus system [55]. The entropy approach adopted the information-theoretic concept by measuring the coincidence that occurred from a given dataset and utilized the obtained result as an IDS specification behavior profile. Therefore, the increasing number of attacks would raise the number of entropies which indicated the intrusions that occurred in the CAN bus. The authors tested the practicality of the method using packet insertion attacks, flooded the CAN bus network with DoS attack, and disturbed the normal correlated events. The results demonstrated that the low randomness of traffic specification of the method could identify any violations from the normal behavior of the CAN bus networks. However, on the negative side, the entropy method did not seem to be able to give detailed information regarding the recognized attack.

Lee et al. proposed an OTIDS (offset ratio and time interval-based intrusion detection system) based on the examination of timing interval and offset ratio between the broadcasted request and response CAN remote frame in the CAN bus network [11]. They utilized these significant features: the correlation coefficient of time intervals and offsets, the instant and lost reply ratio, and the average response times in detecting fuzzy, DoS, and impersonation attacks. The results showed that the proposed method could detect any state of attack models quickly. As well, the attackers could not bypass the system because of the characteristics of the proposed detection features. However, the additional hardware integration to increase the communication caused the method to detect a relatively small amount of data compared to the actual amount of total data.

Tomlinson et al. exploited pre-determined average time intervals of CAN packet broadcasts and adopted Z score and autoregressive integrated moving average (ARIMA) methods in detecting timing changes within the CAN bus traffic [72]. The proposed methods were compared with the mean time interval supervise-based method. These methods were tested whether they can trigger high priority of dropped packets and injected packets. The performance results demonstrated that the two unsupervised Z score and ARIMA methods were degraded when injecting lower priority packets irregularly. However, they suggested that by exploring a more realistic attack packet, tweaking optimal threshold and optimizing model factors and parameters may improve performance.

Narayanan et al. [73] employed a hidden Markov model-based technique to predict the time series in the CAN bus traffic. Initially, they converted the input containing engine RPM, engine coolant temperature, speed, O_2 voltage, etc. into a time series observation. Instead of feeding the model using observation in the form of real value, they transformed them into gradients. The model has constructed transition probabilities (i.e., manage the transition from a current state to a new state) and emission probabilities (i.e., generate probability based on the observation in a current state). The CAN packet logs used for the experimentation consist of changes of a specific behavior in CAN traffic, such as reduction of RPM value during high-speed driving. The indication of these anomalous CAN packets is based on the posterior probability of a given prior input sequence in the determined sliding window. The model raised an alert if any observation probabilities were below the threshold value. The results reported that the model could successfully detect anomalies either in individual and combination of states or even unsafe states in CAN bus traffic, though it may be a significant improvement in the future by evaluating the model using realistic CAN attack packets.

3.1.6.5 Hybrid-based approach In the current desktop IT environment, hybrid-based IDS is also recognized as a distributed intrusion detection system (DIDS). It combines several IDS techniques (e.g., network-based IDS and host-based IDS) on a vast network that communicate with each other, monitored by the central server [74]. The hosted IDS components on the network collect and convert information concerning the monitored system to a standard format and send that information to a central system. The central system aggregates the received information from multiple IDS and processes them. Nevertheless, in contrast with the CAN bus environment, hybrid-based anomaly detection in CAN combines more than one method that takes into account the CAN ID field, CAN data payload, CAN specification, CAN timing interval, or its frequency in detecting attacks [53, 54].

Weber et al. deployed a combination of the specification-based system integrated with a detection mechanism based on machine learning specifically for embedded ECUs in CAN bus traffic [53]. This method is lightweight and also worked in an online manner like [54]. The specification-based part applied *static checks* at the initial stage, where it conducted payload property inspection statically described in the form of a communication matrix, whereas the machine learning-based part applied *learning checks* at the second stage for temporal behavior anomaly detection in the CAN time series. The *static checks* module forwarded selected data to the *learning checks* module to perform feature extraction using RNN, OCSVM, and lightweight on-line detector of anomalies (LODA) [75]. Each algorithm generated a binary value for the indication of an anomaly. The method is evaluated against five CAN modified packets with different types of attack, and the results exhibit an excellent minima anomaly score which is similar to the normal CAN specification.

Wang et al. developed a hybrid anomaly detection using hierarchical temporal memory (HTM) which is a memory-based system that can train a massive number of CAN time series input while at the same time learning CAN data field sequences [54]. The method worked in an online manner, which relied on the state of prior learning. The memory will be kept updated and continue learning whenever it received a new input stream of CAN packets. Also, the scoring mechanism in measuring the error of the predicted value is based on the log loss function; the error of each predicted CAN ID is derived and combined in order to produce a single decision. To evaluate the impact of the method, they used both packet insertion and packet modification attack with different sliding windows for detection respectively. Based on the result, the HTM algorithm is shown to be more reliable in detecting known and unknown attacks when compared with existing CAN IDS that adopted the RNN and HMM methods. However, if the model training time can be reduced and redundant in CAN fields can be removed, the overall performance of the model can be improved effectively.

3.1.6.6 Specification-based approach Specification normally is a set of thresholds and rules that describe the well-known behavior of components in the network, e.g., routing tables, protocols, and nodes. Specification-based approach [76] works by detecting attacks whenever an expected behavior of the network diverges from designated specifications. Hence, the purpose of the specification-based approach is the same as an anomaly-based approach: anything that deviates from the designated well-known behavior profile is indicated as anomalies. Still, the only significant difference between both methods is that each specification and rule needs to be defined manually by a human expert. However, a training phase for this approach is not required as it will work immediately once setting up specifications is finished. Additionally, specifying specifications manually could be error-prone and time-consuming as the system may find it hard to adjust with different domains [77].

Larson et al. explored the applicability of specification-based by obtaining relevant information from CAN version 2.0 and CAN open draft standard 3.01 protocols [30]. The aim was to construct security specifications for ECUs' communication behavior and communications protocol. Since the specification was derived from ECUs' behavior, thus, the anomaly detector does not need to be placed on each ECU. Instead, the security specification could enforce ECUs to check the validity of the sent and received CAN packets. The authors evaluated the method using six types of attacks derived from [78]: spoof, replay, read, modify, flood, and drop. The evaluation result showed that most of the derived attack models could be detected. However, the detection depends highly on the role of the ECU; if an attacker has modified the ECU behavior specification, then the anomaly detection would be impossible.

3.1.6.7 Signature-based approach The signature-based approach detects an attack by utilizing a set of identified signatures, malicious events, or rules stored in the database module of IDS [78]. This approach compares the network or system's activity against the attack patterns stored in IDS, and if it matches with the stored malicious patterns, it will trigger the alarm. The signature-based approach is promising as it is not sophisticated to build and can increase the accuracy in detecting known attacks effectively. Nonetheless, as this approach relies heavily on the attack signature database, it becomes ineffective in detecting unfamiliar or unknown attack [79]. Thus, it necessitates an IDS to update new attack signatures regularly. Further, unlike established signature-based IDS operated in the computer network domain, the attack signatures in the automotive field so far have not yet been documented publicly by any automotive manufacturers or scientific researchers [36].

Müter et al. implemented eight anomaly detection sensors which were derived from the CAN bus system properties to serve as attack signatures for IDS [80]. The signatures developed in the sensors contained specifications of CAN bus protocol, which defined allowed packets with respect to intended communication bus system, specifications of packets payload that complied with data range, approved packets frequency and interval behavior, correlation of packets on diverse bus system that met the specifications, valid communication challenge-response protocols, realistic data content of packet payload, and finally non-redundant vehicle data sources. The authors presented the sensors' applicability criteria which consist of working conditions, requirements, and consequences of each criterion to assist the evaluation phase. Based on the overall results, the sensors could successfully detect anomalies with zero false-positive alarm. However, the method could not detect injected attacks that are compliant with the normal behavior of CAN specification.

Studnia et al. extracted the attack signatures obtained from standard ECU specifications using finite-state automata (FSA) in detecting an anomalous sequence of CAN packets via the in-vehicle network [38]. The authors evaluated the proposed method by performing malicious packet injection, where the attack packets were simulated using modified CAN frames. Although the methods could successfully detect deviations from normal states of CAN behavior, however, the detection performance became ineffective when it emitted the first frames of the broadcasted attack packets.

4 Potential intrusion detection and prevention system (IDPS) in CAN bus network

In a desktop IT domain, the intrusion detection system is known as a passive monitoring system. As the name implies, the detection is designed not to produce any kind of response towards the intrusion. On the contrary, an IDPS or also known as preventive IDS reacts to the unusual activities occurred within the system. For instance, firewall rules or specifications are reprogrammed to block any packets in the network traffic that came from the suspicious source [81].

In a CAN bus automotive domain, Tobias et al. discussed a preventive IDS concept exploiting the car's multimedia system in supporting the technology of automotive IDPS in the near future [36, 56]. The concept introduced is based on the potential human-computer interface (HCI) approaches that can be employed into IDPS to assist drivers after the alert has been raised. The intrusion detection system serving as HCI should be carefully designed as its responses might endanger the safety of the drivers. However, the main focus in [6, 12] was not a user-supported or automated intrusion response system. Instead, the authors investigated the opportunities of a modern multimedia system which could be utilized as a platform in collecting and assessing the driver's reaction. Hence, this paper briefly discussed the three different methods for an IDPS to communicate with the driver through a range of haptic (e.g., force response ability components like ABS braking system), acoustic (e.g., sound subsystems component like media player, phone, audio), and visual (e.g., on-board video screen component like TV system) actuators provided in modern vehicles. As a result of using an array of modern vehicle's sensors as an input, the most appropriate interaction among the vehicle and its driver can be determined. The adaptive dynamic approach could be activated as soon as an intrusion has been identified. However, Hoppe et al. also discussed the problem of intrusion response system where it might not be allowed to actively make decisions in the vehicle due to legal requirements for safety-critical systems [36].

Another intrusion detection and prevention mechanism has been proposed by Miller and Valasek in [1]. They developed a small anomaly detector device that can directly be plugged into the vehicle's OBD-II port. The device then learned the communication bus traffic pattern and detected if any anomalies occurred. Once anomalies were identified, the CAN bus will be short-circuited, and all packets that traverse within the bus will be disabled. However, this introduced new problems in ensuring the designed and implemented embedded systems: multiple security and integrity features, real-time monitoring guarantee, and cost-effective [81].

5 Discussion and summary

In the previous section, we describe a study of a wide range of intrusion detection in the CAN bus system that has led several issues that we need to highlight in helping and shaping the future research for CAN bus IDS in the automotive domain.

We investigated that the inclination of CAN packet IDS towards the anomaly-based approach over other methods (shown in Fig. 5) is due to the constraints and limitations that it possesses. The proprietary characteristic of CAN protocol makes it difficult to adopt a signature- or specification-based approach, as these approaches required semantic knowledge of CAN

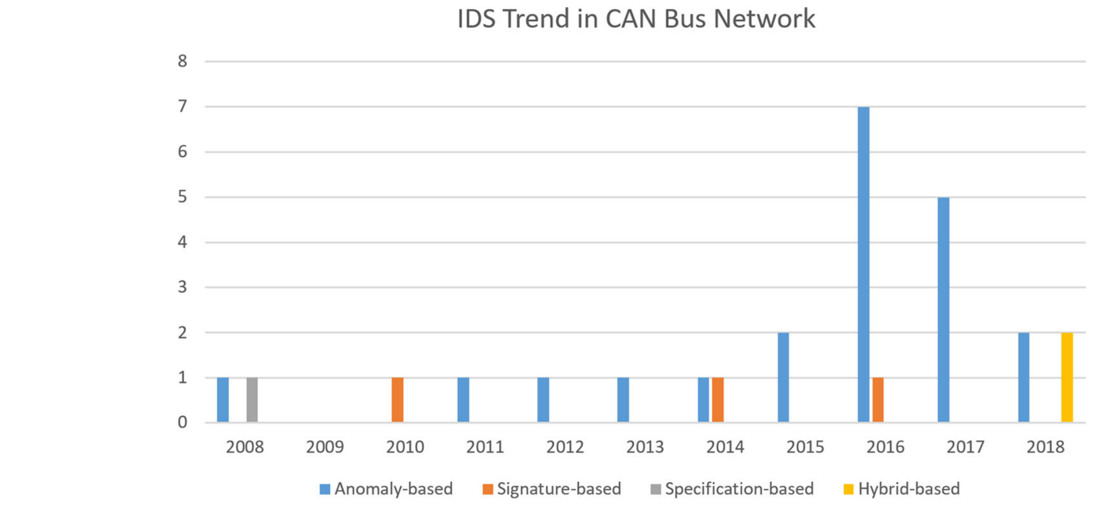

Fig. 5 Trends in CAN IDS from 2008 until 2018

packet, and the protocol may change frequently. Learning-based using anomaly detection may be a suitable detection method as it can learn from the examples and can intelligently adapt with the CAN environment regardless of the protocol, model, and year of the vehicle. Additionally, the anomaly-based approach can detect novel attack which is one of the significant features in IDS, as the outliers' characteristics are generally unknown in advance [82, 83].

Apart from that, most techniques illustrated above, especially those implementing machine learning-based anomaly detection, are deployed in a supervised or at least in a semi-supervised manner. Although these adopted techniques achieved high accuracy, however, it requires a completely labeled data. Obtaining a fully labeled data is impractical especially from a real-time CAN which generates a considerable volume of data in milliseconds. Also, it involves a human expert and is very time-consuming. Thus, using an unlabeled CAN data in an unsupervised manner is more desirable and is convenient for anomaly detection.

As a machine learning approach is emerging, the training efficacy can be improved in terms of pre-processing dataset techniques for the CAN bus system. Most methods in the discussed studies focus on improving the core model and the post-processing model but neglect on the examination of pre-processing parts. The IDS' overall performance is greatly influenced by the size of the data primarily for CAN as it broadcasts a large number of packets per second. Perhaps conducting a comparative review on the computational efficiency of the data pre-processing method is worth for future work study [84, 85].

Further, some of the frequency-based methods demonstrated above can effectively detect numerous kinds of attack within the CAN bus traffic. However, one of the challenges that we need to overcome is that most of the methods can only detect attacks from periodic malicious packets but not from aperiodic intrusions. Though it can detect the injected aperiodic malicious packets, yet, it still unable to identify where the attack originates. Perhaps in the future, those who adopted frequency-based IDS may need to integrate unsupervised recurrent methods like in [86] which are shown to be robust in detecting the unpredictable, predictable, aperiodic, and periodic attack.

In addition, it appears to be a new hurdle, especially when dealing with real-time response system as IDS monitors CAN bus network and requires an exception. Implementing the response system may need an extra tweaking on the design of separate IDS component. Whenever it detects something unusual, the response mechanism can activate the security mode immediately and allow the vehicle to be parked safely [1, 54]. This type of response system may be more challenging than enhancing the detection performance as it involves coordination from various components. Hence, the main aim in designing response system in IDS should instill intelligent human-vehicle interaction, integrated with immediate action mechanism.

Most of the research findings considered a single IDS module; however, it may not cover a holistic approach in serving the security needs of the vehicle communication system. It needs to be complemented with a more lightweight cryptography-based mechanism like message authentication method [72, 81].

Finally, despite the escalating interest in improving IDS methods for CAN bus system presented in Fig. 5, very few works have compared their proposed solutions with others that have similar conditions. It is necessary to evaluate and validate the significant differences of the proposed method among different methods so that the concerned method can achieve optimal performance [87].

6 Conclusion

In this paper, we examine some of the aspects regarding the behavior as well as the vulnerabilities that exist mainly in the CAN bus system. To grasp how CAN work, we present the standard CAN packet structure used in the automotive communication system. As well, we briefly illustrate various kind of possible attack surface in the CAN bus, from direct physical access to long-range wireless access in the existing literature. We also present some of the security countermeasures that have been proposed by researchers in combating this problem. As for conventional networks, the intrusion detection system is one of the most significant security mechanisms in providing holistic protection for the CAN communication system in the automotive domain. Thus, to extend the previous study in proposing various methods of security countermeasures, we investigate every possible research effort done on IDS in a literature survey specifically for in-vehicle CAN bus system. We have selected 25 research works in the literature that proposed numerous types of IDS techniques and strategies in detecting and mitigating the attacks. The selected papers are ranging from 2008 to 2018. We introduce a taxonomy in classifying these research papers according to these aspects: IDS detection approaches, deployment strategies, attacking techniques, and finally technical challenges. Based on our observation, the research works on IDS for the automotive domain is emerging. Nonetheless, we believe the issues discussed in this paper will give researchers some ideas in enhancing security solutions in this area. This necessitates security researchers to investigate comprehensively into a plethora of attacking techniques and methods to produce realistic data for training and testing.

Abbreviations

ACK: Acknowledge; CAN: Controller Area Network; CAN-FD: CAN flexible data-rate; CBC-MAC: Cipher block chaining message authentication code; CIDS: Clock-based intrusion detection system; CRC: Cyclic redundancy code; CUSUM: Cumulative sum; DNN: Deep neural network; DoS: Denial of service; ECU: Electronic control unit; EOF: End of frame; IDS: Intrusion detection system; IP: Internet Protocol; LIN: Local Interconnect Network; LSTM: Long short-term memory; MAC: Message authentication code; MOST: Media Oriented Systems Transport; OBD-II: On-board diagnostics; OCSVM: One-class support vector machine; OTIDS: Offset ratio and time interval-based intrusion detection system; PIPS: Parallel intrusion prevention system; RLS: Recursive least squares; ROC: Receiver operating characteristic; RTR: Remote transmission request; SG: Secure gateway; SOF: Start of frame; TPMS: Tire pressure monitoring system; USB: Universal Serial Bus; V2I: Vehicle-to-infrastructure; V2V: Vehicle-to-vehicle

Acknowledgments

Not applicable

About the authors

Siti Farhana Binti Lokman received her B.Sc. degree in Computer Science from the International Islamic University of Malaysia in 2013 and M.Sc. degree from The University of Manchester in 2016. She also had some industrial experience in Digital Forensic. She is currently attending the University of Kuala Lumpur to pursue her PhD degree in Engineering Technology (Information Technology). Her current research interests include network information security especially in automotive domain as well as intelligent information processing.

Abu Talib Bin Othman is a Professor of Electrical and Electronics Section from Universiti Kuala Lumpur, Malaysian Spanish Institute. He received the B.Sc. degree in Statistics from the National University of Malaysia, M.Sc. degree in Control Engineering and Ph.D. in Computer Network from the University of Bradford. He has various experiences in information technology industries especially in the field of computer network and security in desktop computer as well as electric vehicle domain.

Muhamad Husaini Bin Abu-Bakar received the B.E., MSc., and Ph.D. degrees in Advanced Manufacturing Technology from the Universiti Sains Malaysia, Penang, Malaysia in 2007, 2012, and 2017, respectively. In 2008, he joined the Underwater Robotic Research Group, Universiti Sains Malaysia as a research engineer. Currently, he is a senior lecturer in the University of Kuala Lumpur, Malaysian Spanish Institute, and Head of System Engineering and Energy Laboratory (SEElab). His research interests cover energy, smart material, computational mechanics, and smart manufacturing.

Authors' contributions

SF carried out a comprehensive overview of IDS implementation specifically for CAN bus network system in automotive domain, proposed an in-depth investigation of IDS found in CAN bus system literature based on the following aspects: detection approaches, deployment strategies, attacking techniques, and finally technical challenges. AT participated in categorizing the anomaly-based IDS for CAN bus network system in automotive domain according to these methods: frequency-based, machine learning-based, statistical-based, and time-based. MH conceived of the study by providing advice as from industry to direct the research. All authors read and approved the final manuscript.

Funding

This work was supported by the Short Term Research Grant (grant number str17001), which was provided by the Center for Research and Innovation, Universiti of Kuala Lumpur.

Availability of data and materials

Not applicable

Competing interests

The authors declare that they have no competing interests.

Received: 9 January 2018 Accepted: 30 May 2019
Published online: 19 July 2019

References

1. C. Miller, C. Valasek, in *Black Hat USA, 2014*. A survey of remote automotive attack surfaces (2014), p. 94
2. M. Wolf, A. Weimerskirch, T. Wollinger, State of the art: Embedding security in vehicles. EURASIP J. Embed. Syst. **2007**(1), 074706 (2007)
3. T. Nohet, H. Hanssont, L.L. Bello, in *IEEE Symposium on Emerging Technologies and Factory Automation*. Automotive Communications-past, Current and Future (Catania, 2005)
4. C. Miller, C. Valasek, in *Black Hat USA, 2015*. Remote exploitation of an unaltered passenger vehicle (2015), p. 91
5. S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network. J. Netw. Comput. Appl. **37**, 380–392 (2014)
6. P. Papadimitratos, A.L. Fortelle, K. Evenssen, R. Brignolo, S. Cosenza, Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE Commun. Mag. **47**(11), 84–95 (2009)
7. A. Humayed, J. Lin, F. Li, B. Luo, Cyber-Physical Systems Security—A Survey. IEEE Internet Things J. **4**(6), 1802–1831 (2017)
8. F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Netw. **61**, 33–50 (2017)

9. J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. **16**(2), 546–556 (2015)
10. N. Lyamin, A. Vinel, M. Jonsson, J. Loo, Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks. IEEE Commun. Lett. **18**(1), 110–113 (2014)
11. H. Lee, S.H. Jeong, H.K. Kim, in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame (Calgary, 2017), pp. 57–5709
12. Carsten, P., Andel, T. R., Yampolskiy, M., & McDonald, J. T. In-vehicle networks: Attacks, vulnerabilities, and proposed solutions. In Proceedings of the 10th Annual Cyber and Information Security Research Conference. Oak Ridge. (p. 1). (2015).
13. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, in *2010 IEEE Symposium on Security and Privacy*. Experimental security analysis of a modern automobile (Berkeley/Oakland, 2010), pp. 447–462
14. H.A. Boyes, A.E.A. Luck, *A security-minded approach to vehicle automation, road infrastructure technology, and connectivity* (2015)
15. S. Woo, H.J. Jo, D.H. Lee, A practical wireless attack on the connected car and security protocol for in-vehicle CAN. IEEE Trans. Intell. Transp. Syst. **16**(2), 993–1006 (2015)
16. K. Han, A. Weimerskirch, K.G. Shin, Automotive cybersecurity for in-vehicle communication. IQT Q. **6**(1), 22–25 (2014)
17. O. Hartkopp, R.M. SCHILLING, in *Escar Conference*. Message authenticated can (Berlin, 2012)
18. B. Groza, S. Murvay, A. Van Herrewege, I. Verbauwhede, Libra-can: a lightweight broadcast authentication protocol for controller area networks Proc. 11th Int. Conf. Cryptology and Network Security, CANS, Darmstadt, 2012
19. C.J. Szilagyi, Low cost multicast network authentication for embedded control systems Doctoral dissertation, Carnegie Mellon University (2012)
20. D.K. Nilsson, U.E. Larson, E. Jonsson, in *2008 IEEE 68th Vehicular Technology Conference*. Efficient in-vehicle delayed data authentication based on compound message authentication codes (Calgary, 2008), pp. 1–5
21. A. Van Herrewege, D. Singelee, I. Verbauwhede, in *CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus*. ECRYPT Workshop on Lightweight Cryptography (Vol. 2011) (2011)
22. K.T. Cho, K.G. Shin, in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. Fingerprinting electronic control units for vehicle intrusion detection (Austin, 2016), pp. 911–927
23. T. Hoppe, S. Kiltz, J. Dittmann, in *International Conference on Computer Safety, Reliability, and Security Springer, Berlin, Heidelberg*. Security threats to automotive CAN networks–practical examples and selected short-term countermeasures (2008), pp. 235–248
24. M. Marchetti, D. Stabili, A. Guido, M. Colajanni, in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*. Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms (Bologna, 2016), pp. 1–6
25. V. Verendel, D.K. Nilsson, U.E. Larson, E. Jonsson, in *2008 IEEE 68th Vehicular Technology Conference*. An approach to using honeypots in in-vehicle networks (Calgary, 2008), pp. 1–5
26. K. Lemke, C. Paar, M. Wolf, *Embedded security in cars* (Springer-Verlag, Berlin Heidelberg, 2006), pp. 3–12
27. Arilou Cyber Security. (2016). [Online] https://www.nng.com/arilou-cyber-security/
28. Argus Cyber Security. (2013). [Online] https://argus-sec.com/
29. J. Berg, J. Pommer, C. Jin, F. Malmin, J. Kristensson, A.B. Semcon Sweden, in *13th Embedded Security in Cars (ESCAR'15)*. Secure gateway-a concept for an in-vehicle IP network bridging the infotainment and the safety critical domains (Stuttgart, 2015)
30. U.E. Larson, D.K. Nilsson, E. Jonsson, in *Intelligent Vehicles Symposium, 2008 IEEE*. An approach to specification-based attack detection for in-vehicle networks (2008), pp. 220–225
31. D.K. Nilsson, U. Larson, A defense-in-depth approach to securing the wireless vehicle infrastructure. JNW **4**(7), 552–564 (2009)
32. P. Kleberger, T. Olovsson, E. Jonsson, in *2011 IEEE Intelligent Vehicles Symposium (IV)*. Security aspects of the in-vehicle network in the connected car (Baden-Baden, 2011), pp. 528–533
33. 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
34. R.A. Kemmerer, G. Vigna, Intrusion detection: a brief history and overview. Computer **35**(4), supl27–supl30 (2002)
35. J.R. Vacca, *Computer and information security handbook. Newnes* (Amsterdam, 2012), pp. 47–60
36. T. Hoppe, S. Kiltz, J. Dittmann, Applying intrusion detection to automotive it-early insights and remaining challenges. J. Inform. Assur. Secur. **4**(6), 226–235 (2009)
37. B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in Internet of Things. J. Netw. Comput. Appl. **84**, 25–37 (2017)
38. I. Studnia, E. Alata, V. Nicomette, M. Kaâniche, Y. Laarouchi, A language-based intrusion detection approach for automotive embedded networks. Int. J. Embed. Syst. **10**(1) (2018) United Kingdom
39. L. Apvrille, R. El Khayari, O. Henniger, Y. Roudier, H. Schweppe, H. Seudié, B. Weyl, M. Wolf, Secure automotive on-board electronics network architecture FISITA World Automotive Congress, Budapest,8 2010
40. T. Bécsi, S. Aradi, P. Gáspár, in *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. Security issues and vulnerabilities in connected car systems (Budapest, 2015), pp. 477–482
41. A. Taylor, N. Japkowicz, S. Leblanc, in *2015 World Congress on Industrial Control Systems Security (WCICSS)*. Frequency-based anomaly detection for the automotive CAN bus (London, 2015), pp. 45–49
42. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, et al., Comprehensive experimental analyses of automotive attack surfaces. In USENIX Security Symposium (2011)
43. A. Taylor, S. Leblanc, N. Japkowicz, in *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*. Anomaly detection in automobile control network data with long short-term memory networks (Montreal, 2016), pp. 130–139
44. H. Lee, K. Choi, K. Chung, J. Kim, K. Yim, in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*. Fuzzing can packets into automobiles (2015), pp. 817–821
45. C. Miller, C. Valasek, Adventures in automotive networks and control units. Def. Con. **21**, 260–264 (2013) 54. Miller, C., & Valasek, C. Adventures in automotive networks and control units. DEF CON, 21, 260–264. (2013)
46. R.I. Davis, S. Kollmann, V. Pollex, F. Slomka, in *2011 23rd Euromicro Conference on Real-Time Systems*. Controller area network (can) schedulability analysis with fifo queues (Porto, 2011), pp. 45–56
47. 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
48. 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)
49. L. Pike, J. Sharp, M. Tullsen, P.C. Hickey, J. Bielman, in *Proc. Int. Conf. Embedded Security Cars*. Securing the automobile: A comprehensive approach (2015), pp. 1–14
50. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, E. Vázquez, Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput. Secur. **28**(1), 18–28 (2009)
51. R. Mitchell, I.R. Chen, A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. (CSUR) **46**(4), 55 (2014)
52. I. Butun, S.D. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutorials **16**(1), 266–282 (2014)
53. M. Weber, S. Klug, E. Sax, B. Zimmer, in *9th European Congress on Embedded Real Time Software and Systems*. Embedded hybrid anomaly detection for automotive CAN communication (2018)
54. C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, X. Cheng, A distributed anomaly detection system for in-vehicle network using HTM. IEEE Access **6**, 9091–9098 (2018)
55. M. Müter, N. Asaj, in *2011 IEEE Intelligent Vehicles Symposium (IV)*. Entropy-based anomaly detection for in-vehicle networks (Baden-Baden, 2011), pp. 1110–1115
56. Hoppe, T., Kiltz, S., & Dittmann, J. Adaptive dynamic reaction to automotive it security incidents using multimedia car environment. In 2008 The Fourth International Conference on Information Assurance and Security, Naples. (pp. 295-298). (2008).
57. Song, H. M., Kim, H. R., & Kim, H. K. 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), Kota Kinabalu. (pp. 63-68). (2016).
58. 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)

59. P. Carsten, T.R. Andel, M. Yampolskiy, J.T. McDonald, in *Proceedings of the 10th Annual Cyber and Information Security Research Conference*. In-vehicle networks: Attacks, vulnerabilities, and proposed solutions (Oak Ridge, 2015), p. 1
60. 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
61. M.R. Moore, R.A. Bridges, F.L. Combs, M.S. Starr, S.J. Prowell, in *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*. Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection (Oak Ridge, 2017), p. 11
62. L. Deng, D. Yu, Deep learning: Methods and applications. Foundations and Trends®. Signal Process. **7**(3–4), 197–387 (2014)
63. M.J. Kang, J.W. Kang, Intrusion detection system using deep neural network for in-vehicle network security. PLoS One **11**(6), e0155781 (2016)
64. 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)
65. A. Valdes, S. Cheung, in *2009 IEEE Conference on Technologies for Homeland Security*. Communication pattern anomaly detection in process control systems (Boston, 2009), pp. 22–29
66. C. Cortes, V. Vapnik, Support-vector networks. Mach. Learn. **20**(3), 273–297 (1995)
67. S. Hochreiter, J. Schmidhuber, Long short-term memory. Neural Comput. **9**(8), 1735–1780 (1997)
68. A. Wasicek, A. Weimerskirch, in *SAE Technical Paper*. Recognizing manipulated electronic control units (No. 2015-01-0202) (2015)
69. A. Avalappampatty Sivasamy, B. Sundan, A dynamic intrusion detection system based on multivariate Hotelling's T2 statistics approach for network environments. Sci. World J., 1–9 (2015, 2015)
70. A. Qayyum, M.H. Islam, M. Jamil, in *Proceedings of the IEEE Symposium on Emerging Technologies*. Taxonomy of statistical based anomaly detection techniques for intrusion detection (Islamabad, 2005), pp. 270–276
71. M. Marchetti, D. Stabili, in *2017 IEEE Intelligent Vehicles Symposium (IV)*. Anomaly detection of CAN bus messages through analysis of ID sequences (Los Angeles, 2017), pp. 1577–1583
72. A. Tomlinson, J. Bryans, S.A. Shaikh, H.K. Kalutarage, in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. Detection of Automotive CAN Cyber-Attacks by Identifying Packet Timing Anomalies in Time Windows (Luxembourg City, 2018), pp. 231–238
73. S.N. Narayanan, S. Mittal, A. Joshi, in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*. OBD_SecureAlert: An anomaly detection system for vehicles (St. Louis, 2016), pp. 1–6
74. D. Krishnan, M. Chatterjee, in *International Conference on Security in Computer Networks and Distributed Systems*. An adaptive distributed intrusion detection system for cloud computing framework (Springer, Berlin, Heidelberg, 2012), pp. 466–473
75. T. Pevný, Loda: Lightweight on-line detector of anomalies. Mach. Learn. **102**(2), 275–304 (2016)
76. C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, K. Levitt, in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. A specification-based intrusion detection system for AODV (2003), pp. 125–134
77. J.P. Amaral, L.M. Oliveira, J.J. Rodrigues, G. Han, L. Shu, in *2014 IEEE International Conference on Communications (ICC)*. Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks (Sydney, 2014), pp. 1796–1801
78. C. Kruegel, T. Toth, in *International Workshop on Recent Advances in Intrusion Detection*. Using decision trees to improve signature-based intrusion detection (Springer, Berlin, Heidelberg, 2003), pp. 173–191
79. J.D. Howard, T.A. Longstaff, A common language for computer security incidents. Sandia Natl. Lab. **10**, 751004 (1998)
80. H.J. Liao, C.H.R. Lin, Y.C. Lin, K.Y. Tung, Intrusion detection system: A comprehensive review. J. Netw. Comput. Appl. **36**(1), 16–24 (2013)
81. M. Müter, A. Groll, F.C. Freiling, in *Information Assurance and Security (IAS)*. A structured approach to anomaly detection for in-vehicle networks (Atlanta, 2010), pp. 92–98
82. 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
83. S. Omar, A. Ngadi, H.H. Jebur, 0020`Machine learning techniques for anomaly detection: An overview. Int. J. Comput. Appl. **79**(2), 975–8887 (2013). https://doi.org/10.5120/13715-1478
84. N.M. Nawi, A.S. Hussein, N.A. Samsudin, N.A. Hamid, M.A.M. Yunus, M.F. Ab Aziz, The Effect of Pre-Processing Techniques and Optimal Parameters selection on Back Propagation Neural Networks. Int. J. Adv. Sci. Eng. Inf. Techn. **7**(3), 770–777 (2017)
85. S.A. Alasadi, W.S. Bhaya, Review of Data Preprocessing Techniques in Data Mining. J. Eng. Appl. Sci. **12**(16), 4102–4107 (2017)
86. P. Malhotra, A. Ramakrishnan, G. Anand, L. Vig, P. Agarwal, G. Shroff, LSTM-based encoder-decoder for multi-sensor anomaly detection. arXiv preprint arXiv 1607, 00148 (2016)
87. H. Ji, Y. Wang, H. Qin, Y. Wang, H. Li, Comparative performance evaluation of intrusion detection methods for in-vehicle networks. IEEE Access **6**, 37523–37532 (2018)
88. J. Li, in *Presentation slides on Hack In The Box Security Conference (HITBSecConf)*. CANsee-An Automobile Intrusion Detection System (2016) [Online] http://conference.hitb.org/hitbsecconf2016ams/materials/D2T1%20-%20Jun%20Li%20-%20CANSsee%20-%20An%20Automobile%20Intrusion%20Detection%20System.pdf

7 Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.