Cybersecurity attacks on CAN bus based vehicles: a review and open challenges

Faten Fakhfakh
ReDCAD Laboratory, University of Sfax, Sfax, Tunisia
Mohamed Tounsi
ReDCAD Laboratory, University of Sfax, Sfax, Tunisia and
Common first year Deanship, Umm Al-Qura University, Mecca, Saudi Arabia, and
Mohamed Mosbah
CNRS, Bordeaux INP, LaBRI, University of Bordeaux, Talence, France

Received 18 January 2021
Revised 29 April 2021
Accepted 16 June 2021

Abstract

Purpose – Nowadays, connected vehicles are becoming quite complex systems which are made up of different devices. In such a vehicle, there are several electronic control units (ECUs) that represent basic units of computation. These ECUs communicate with each other over the Controller Area Network (CAN) bus protocol which ensures a high communication rate. Even though it is an efficient standard which provides communication for in-vehicle networks, it is prone to various cybersecurity attacks. This paper aims to present a systematic literature review (SLR) which focuses on potential attacks on CAN bus networks. Then, it surveys the solutions proposed to overcome these attacks. In addition, it investigates the validation strategies aiming to check their accuracy and correctness.

Design/methodology/approach – The authors have adopted the SLR methodology to summarize existing research papers that focus on the potential attacks on CAN bus networks. In addition, they compare the selected papers by classifying them according to the adopted validation strategies. They identify also gaps in the existing literature and provide a set of open challenges that can significantly improve the existing works.

Findings – The study showed that most of the examined papers adopted the simulation as a validation strategy to imitate the system behavior and evaluate a set of performance criteria. Nevertheless, a little consideration has been given to the formal verification of the proposed systems.

Originality/value – Unlike the existing surveys, this paper presents the first SLR that identifies local and remote security attacks that can compromise in-vehicle and inter-vehicle communications. Moreover, it compares the reviewed papers while focusing on the used validation strategies.

Keywords Vehicles, CAN bus, Attacks, Review, Cybersecurity, Validation

Paper type Literature review

1. Introduction

In the last decades, vehicles have become highly computerized due to the continuous development of information and communication technologies. Connected vehicles play an important role in smart cities because they aim to minimize transportation problems due to congested roads (Sun *et al.*, 2018; Chang *et al.*, 2020). Smart city is a new trend that is developed due the rapid growth of the Internet of things. It aims to make life more comfortable by providing various services enabling the monitoring and the management of remote devices (Moreno *et al.*, 2016). However, vehicles of smart cities are very sophisticated systems as they are equipped with many on-board micro-controllers. They consist of different networked components such as sensors, electronic control units (ECUs), actuators and communication devices (Zeng *et al.*, 2016). The ECUs represent the fundamental unit of computation since they aim to control the vehicle subsystems including airbags, braking systems, etc. ECUs are not only connected to internal vehicle's ECUs but also to other vehicles' ECUs. The communication between ECUs can use different protocols such as Ethernet (Pedreiras and Almeida, 2002), Local Interconnection Network (LIN) (Ruff, 2003),

Library Hi Tech

0737-8831
DOI 10.1108/LHT-01-2021-0013

FlexRay (Consortium *et al.*, 2005), Controller Area Network (CAN) (Standard, 2003) and Media Oriented Systems Transport (MOST) (Lee *et al.*, 2012). CAN bus is the most widely used protocol in automotive applications thanks to its main characteristics such as low cost, fault tolerance and real-time transmission between vehicles.

1.1 Scope of the survey

Despite the different advantages of CAN, connected vehicles are vulnerable to several attacks since they suffer from some security features, including the broadcast dissemination and the absence of message authentication (Choi *et al.*, 2018). Thus, adversaries can penetrate the network and perform malicious tasks as the CAN bus does not check the source of messages. Attacks in vehicle systems can not only disclose sensitive personal information but also threaten humans' lives. Thus, protecting vehicles against these attacks is currently a significant challenge as vehicles have been designed without taking into account all security requirements. Since security of connected vehicles is critical, it is essential to identify potential attacks and specify the existing defense solutions. In this paper, we present an end-to-end review starting from the scenarios of security attacks while addressing two ways of gaining access to the CAN bus. In fact, these attacks can be introduced in the CAN bus through a local access or via remote access. Local access attacks consist in accessing the vehicle physically and remote access attacks can take place using wireless communication interfaces. We attempt also to categorize the existing solutions, which have been provided by earlier works, to cope with automotive attacks. Then, we investigate the validation strategies adopted to check whether the proposed system is operating as expected and offering the envisaged accuracy level.

1.2 Sate-of-art surveys

There are a number of useful surveys which have been conducted to emphasize the security attacks in automotive networks based on the CAN bus.

Wu *et al.* (2019) analyze the vehicle attacks based on three layers: physical layer, data-link layer and application layer. In addition, they discuss the vulnerabilities related to each layer. Furthermore, a classification of the intrusion detection methods for in-vehicle networks has been presented with an emphasis on the implementation techniques. In another study, Lokman *et al.* (2019) discuss the existing works which focus on intrusion detection systems (IDSs). The IDS is one of the most significant security mechanisms in providing protection for the CAN communication system in the automotive domain. Also, the authors introduce taxonomy in classifying these research papers according to the following aspects: detection approaches, deployment strategies, attacking techniques, and finally, technical challenges. Likewise, in Al-Jarrah *et al.* (2019), present a detailed review of IDSs for in-vehicle networks. They classify them according to the used detection techniques. They also analyze each work based on different comparison metrics such as innovation, benchmark models, performance criteria, evaluation data, etc. Similarly, a description of several methods and approaches for applying IDSs to protect automotive systems on the CAN bus has been introduced in Young *et al.* (2019). The scope of the survey papers already mentioned is limited to secure in-vehicle networks using IDS mechanisms while ignoring other potential solutions. Additionally, Gmiden *et al.* (2019) provide a survey of the existing approaches interested in protecting CAN bus. Nonetheless, this work focuses only on cryptography based solutions. So, the authors introduce some of these solutions and evaluate them according to a set of requirements such as authentication, integrity, confidentiality, backward compatibility and performance. The study of Studnia *et al.* (2013) presents a survey in which they introduce a classification of security menaces in embedded automotive networks. They explain how the opportunities of attackers can be improved through the new communication abilities of connected vehicles. The authors also point to

some techniques which have been used to improve security. However, no description of the attack scenarios has been presented. Also, the paper does not provide an exhaustive list of the potential solutions aiming at mitigating these attacks. In the same context, the survey of Dibaei *et al.* (2019) provides valuable insight about the major security attacks which can hamper connected vehicles. Moreover, a classification and a comparison of the defense mechanisms against the security attacks have been presented. Nevertheless, this survey is not intended only for approaches based on CAN bus protocol. In another review study, Bozdal *et al.* (2020) present a detailed survey in which they focus on physical and remote attacks that have been implemented on the CAN bus network. In addition, they introduce an in-depth analysis of some defense mechanisms which have been used to secure the CAN bus. However, the research challenges which have been shown are insufficient and do not provide any improvement of the existing works.

To help position the contributions of this research with regard to the existing published surveys, we present a comparison table (see Table 1) based on some criteria including:

(1) Network: The considered network can be classified into two types: in-vehicle and inter-vehicle network.

(2) Attack scenarios: This criterion indicates whether the considered paper gives a description of the attack scenarios that compromise CAN bus based vehicles.

(3) Solutions: This criterion identifies the defense mechanisms which have been used to deal with automotive attacks. These solutions will be detailed in section 5.

(4) Validation strategies: This criterion indicates if the survey paper has discussed the different validation strategies (such as simulation, formal verification and real experiments) adopted to evaluate the proposed solutions.

(5) Years range: It represents the years' range of the studied papers.

(6) Review type: This criterion is used to identify whether the considered paper carries out a simple survey or it follows the systematic literature review (SLR) methodology (Kitchenham *et al.*, 2009) that can provide rigorous review of the literature.

(7) Open issues: This criterion indicates whether some future directions have been mentioned in the studied paper.

The symbol "±" indicates that only some security attacks (or solutions) have been taken into account. No doubt there are other criteria that can be considered (such as performance metrics, benchmark model, etc.), but the presented ones are sufficient for the scope of this research.

Based on this overview of the existing survey studies, we notice that the literature is missing an SLR that identifies local and remote security attacks, which are related respectively to in-vehicle and inter-vehicle communications. Unlike the aforementioned surveys, we introduce a thorough, comprehensive and systematic review of the different attacks scenarios that compromise connected vehicles. We also classify the selected papers (ranging from 2010 to July 2020) according to the existing solutions against these attacks. Additionally, we detail some selected papers while focusing on their validation strategies. Furthermore, we explore the open issues that can be studied in the future.

1.3 Organization of the paper

The remainder of this paper will be divided into the following sections: In section 2, we introduce an overview of the CAN bus protocol. Section 3 describes the research methodology applied to our survey paper. In section 4, a list of the different attack types is presented. In section 5, we outline the best practices to deal with these attacks. In section 6, we review some selected papers by classifying them according to the adopted validation strategies. In section 7,

Table 1.
A Comparison of our paper with the existing surveys

Ref		Studnia *et al.* (2013)	Al-Jarrah *et al.* (2019)	Lokman *et al.* (2019)	Young *et al.* (2019)	Wu *et al.* (2019)	Dibaei *et al.* (2019)	Gmiden *et al.* (2019)	Bozdal *et al.* (2020)	Our paper
Network	In-vehicle	+	+	+	+	+	−	+	+	+
	Inter-vehicle	−	−	−	−	−	+	−	+	+
Attack scenarios		−	±	−	−	−	±	−	−	+
Solutions	IDS	±	+	+	+	+	+	−	+	+
	Cryptography	±	−	−	−	−	+	+	−	+
	Others	−	−	−	−	−	−	−	+	+
Validation strategies		−	−	−	−	−	−	−	−	+
Years range		2008–2012	2007–2018	2008–2018	2010–2018	2010–2018	2009–2018	2008–2017	2011–2020	2010–2020
Review type		Survey	Survey	Survey	Survey	Survey	Survey	Survey	Survey	SLR
Open issues		−	+	−	−	+	+	−	−	+

we provide a rich analysis of the existing approaches and we identify a set of possible future directions. Finally, the last section sums up the paper.

2. CAN bus protocol: an overview

CAN is a message-based protocol which allows electronic components of a vehicle to communicate with each other. These components include sensors, ECUs, actuators, microcontrollers, etc. In a connected vehicle, a typical CAN network includes 20 to 100 ECUs. The goal of an ECU is to handle all core and additional vehicle functions. In Figure 1, we present the CAN frame structure which consists of:

(1) Start of frame (SOF): It represents the start of a CAN message with a dominant bit and informs all ECUs of the beginning of the CAN message transmission.

(2) Arbitration: It consists of 11 bits and can be extended up to 29 bits' format. The arbitration identifier (ID) field associated with each transmitted CAN frame specifies the priority of packets. The packet having the higher priority corresponds to the lowest bit value of the ID. The CAN protocol aims to prevent collisions within the CAN bus traffic.

(3) Control: It gives more information for the receiver to verify whether all packets are received successfully.

(4) Data: It includes actual information for CAN nodes to achieve actions. It can be between 0 and 8 bytes.

(5) CRC: This field contains 15 bits for the fault detection mechanism which verifies the validity of packets.

(6) Acknowledge (ACK): This field guarantees that the receiver nodes obtain the CAN packets. If it detects an error during the dissemination process, the sender will be informed instantly by the receiver to transmit the data packets again. This field is also called "confirmation field".

(7) End of frame (EOF): It specifies the end of the CAN frame using a recessive bit's flag.

The CAN protocol provides several benefits over other communication protocols:

(1) Low cost and lightweight network: The CAN bus protocol is based on a unique wire connecting to actuators, sensors and ECUs in a vehicle and can transmit data with high speed. Its implementation decreases an important amount of complex wiring, which leads to a lower cost of the system.

(2) Robustness: CAN bus systems have a reliable communication network which is based on mechanisms for detecting failures. When a failure is discovered, all nodes in the network are informed. In addition, the CAN bus line is resistant to electrical disturbances.

(3) Flexibility: In the CAN bus protocol, nodes are not identified by information which characterizes them. Then, they can be easily inserted or eliminated according to the system requirements.

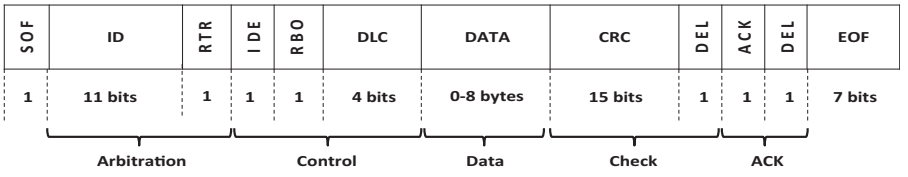

Figure 1.
The structure of CAN data frame

All these advantages motivate the use of CAN bus as a standard for vehicle networking. Nevertheless, it has been recognized that CAN is exposed to various cyberattacks. The main reasons of such attacks are:

(1) Lack of authentication: A CAN frame does not include any information of the sender and the receiver address. So, the CAN protocol is not able to differentiate between the fake frame and the valid one. Otherwise, the attacker can take control of the vehicle components by transmitting spoofed messages since any illegal device can be connected to the CAN bus. Thus, several functions can be performed such as interrupting the engine, deactivating the break, etc.

(2) Lack of confidentiality: Each message transmitted on CAN is sent to every node of the network. So, a malignant node can easily listen on the bus and read the message content.

(3) Lack of availability: Data transmission in CAN bus is based on the arbitration ID which defines the priority of messages. Thus, an ECU can overflow the bus with high priority messages and prevent any transmission of other ECUs.

(4) Lack of integrity: CAN bus uses the CRC field to verify whether a message has been altered. However, this is not enough to inhibit an attacker from changing an accurate message or fabricating a fake message, because it is possible to falsify a valid CRC for a false message.

(5) Lack of non-repudiation: It is not possible to verify whether a legitimate ECU has not transmitted or received a specific message.

The issues already mentioned make connected vehicles unsafe and poorly equipped in discovering nodes which have led to the attacks. Consequently, protecting vehicles against cyberattacks is a significant challenge.

3. Research selection method

The present review paper follows the guidelines of systematic reviews in software engineering research proposed by Kitchenham *et al.* (2009). The goal of this methodology is to interpret and evaluate all research relevant to a topic area. It is also an efficient approach when searching for a critical discussion on problems from similar perspectives. Following these guidelines, an SLR consists of three main steps as shown in Figure 2. A clear description of each step will be described in the rest of this section.

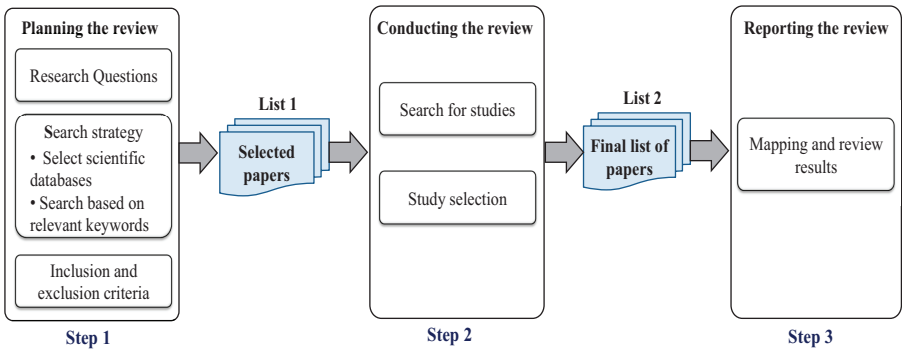

Figure 2.
Description of the SLR process

3.1 Planning the review

The first step of a SLR consists of defining the research questions (RQs), specifying the search strategy and identifying the inclusion and exclusion criteria.

3.1.1 Research questions. The goal of the present paper is to identify the relevant literature which focuses on the automotive security attacks. For this purpose, we have defined a set of RQs in order to analyze the reviewed publications:

RQ1. What are the attacks studied in the existing works ?

RQ2. Which solutions are implemented to prevent the different attacks ?

RQ3. Which strategies are used to validate the proposed solutions ?

3.1.2 Search strategy. In this part, we explain the search strategy adopted for selecting the relevant publications from several sources. Our search consists in using the known scientific databases: ACM Digital Library (http://dl.acm.org), IEEE Xplore (http://ieeexplore.ieee.or), Springer (http://www.springer.com), Elsevier Scopus (https://www.elsevier.com/) and Wiley (http://onlinelibrary.wile).

We have conducted an extensive search using the following query which uses synonyms and various words of the main features:

((“CAN bus” OR “CAN protocol”) AND (“security”) AND (“attack” OR “threat”) AND (“vehicle” OR “car”)).

Based on this stage, we collect only the papers published between 2010 and July 2020. These papers are stored in List 1.

3.1.3 Inclusion and exclusion criteria. In the second stage, we have refined the studies already collected using a manual search in order to identify those related to our RQs. To this end, we have determined the inclusion and exclusion criteria which are required to assess each study. In what follows, we present the list of these criteria:

(1) Only long publications written in English from peer reviewed journals and conferences were considered.

(2) Studies in the form of short papers, book chapters, tutorial papers and poster papers were discarded because they did not give sufficient information.

(3) Studies presented reviews and survey papers were excluded.

3.2 Conducting the review

This step involves two main phases: search for studies and study selection.

3.2.1 Search for studies. Through the search strategy already presented, we retrieved a new set of papers. After that, we removed duplicated papers as they appeared in different databases.

3.2.2 Study selection. The selected papers were analyzed based on their abstracts and keywords. The remaining papers were fully examined after a complete text reading. Finally, we ended up with a new set of candidate papers (List 2) for the next step of the SLR.

3.3 Reporting the review

In this step, we use the three RQs already presented. The first question RQ1 is so useful as it aims to identify the different attack types of the CAN bus. The answer to RQ2 illustrates the solutions proposed to deal with the attacks in question. These solutions can be classified into five main types: cryptography, message authentication, firewall, IDS and honeypots. Finally, in the last RQ RQ3, we categorize the strategies enacted by the researchers to validate their proposed solutions.

4. Security attacks

4.1 Classification of attacks

Although there is a great progress in the automotive field, vehicles are susceptible to many cyberattacks with different security degrees. In fact, there are two ways to gain access to the CAN bus: local access and remote access (see Figure 3). In the local access attacks, the adversary should access the vehicle physically. However, remote access attacks are implemented via wireless communication interfaces (Checkoway *et al.*, 2011).

4.1.1 Local attacks. They require direct or indirect access to the CAN bus network. Direct access can be obtained by using the On Board Diagnostic (OBD) port which is adopted in the CAN network to identify and collect diagnostic data. The OBD port represents a particular port entry for attackers to monitor and transmit frames on the bus. For example, an attacker can disseminate control information to other ECUs on the bus. After the attacker intervention, the vehicle will be in a compromised state. As concerns indirect access, attacks need a physical object to be inserted into the vehicle. For example, a vehicle can have multimedia devices like a CD/DVD player for entertainment and USB for saving and reading files from nomadic devices. In this context, a potential scenario consists in connecting a compromised device (like a smartphone) that can achieve an attack against the ECU which is connected to it.

4.1.2 Remote attacks. They are performed without having physical access to bus systems. Vehicles use different wireless networks like Bluetooth, Wifi, global navigation satellite system (GNSS) (Wang, 2012), 3G/4G, etc. We classify these attacks into two types according to the range of wireless access:

(1) *Short range attacks*: This type includes attacks which are based on communication technologies having short range wireless access such as remote key, Bluetooth, Wi-Fi, dedicated short-range communications (DSRC), etc. For example, the conductor can connect his phone via Bluetooth and use his sound system in hands free kit. Nevertheless, using these technologies in vehicles can be defective. In fact, this can induce the possibility of listening to conversations and the recovery of data saved in the communication unit.

(2) *Long range attacks*: This type incorporates attacks which are worn on long range wireless communication technologies (a distance greater than 1 km (den Hartog *et al.*, 2018)) including cellular technologies (from 2G to 5G) and GNSS. In some connected vehicles, users can select a set of downloadable applications for the multimedia unit. An attack on the online store or a program sold on a store actually incorporating a Trojan horse can have dangerous effects. The remote attack surface of connected vehicles is important due to the increasing connectivity in vehicles.

Remote security attacks can deal with vehicle to vehicle (V2V), vehicle to infrastructure (V2I) and vehicle to pedestrian (V2P) communications.

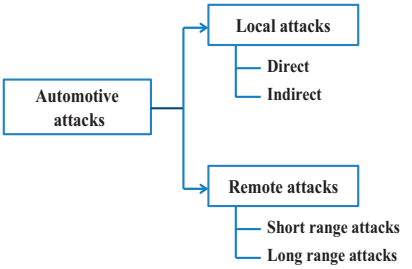

Figure 3.
Classification of automotive attacks

4.2 Attack types

In what follows, we present several attack scenarios that can affect the CAN bus either in the same vehicle (local access) or inter-vehicle (remote access).

4.2.1 Denial-of-service (DoS) attack. DoS is a well-known attack which has been widely used to disrupt communication by flooding the network with huge volume of false data. As already mentioned, the operation of the CAN protocol is based on the message priority. In fact, the message having the high priority can access to the CAN bus before the message with low priority. During the arbitration process, if there are messages having the highest priority on the CAN bus, nodes are not authorized to send messages. In order to implement DoS attacks, the attackers can simply command the malicious node to transmit periodically messages with the highest priority.

Another scenario of the DoS attack can takes place by stopping the communication network created by a road side unit (RSU) or a vehicle. This can be achieved by transmitting numerous request messages, leading to encumbering the RSU and its incapacity to exchange data. In this situation, safety messages (such as alert messages and road condition) cannot be shared causing in disastrous effects.

4.2.2 Distributed denial of service (DDoS) attack. This attack represents an improved type of DoS. It is more robust and effective than DoS since it adopts several IP addresses. It is difficult to remedy DDoS attacks because the entering messages can arrive from a huge number of users.

4.2.3 Suspension attack. It is considered as a kind of DoS attack. The adversary declines some disseminated messages which can contain urgent information for the receiver. The purpose of such an adversary is to prohibit insurance and registration authorities from knowing the transmitted collision reports. For example, the adversary may remove a congestion alert and use it again. This can lead to serious effects.

4.2.4 Black hole attack. It involves a malicious node (called Black hole) which introduces itself for belonging to the shortest path, so that it can intercept the sent packets or keep them. This type of attack is also known drop attack.

4.2.5 Gray hole attack. It is considered as an extension of Black hole attack. In fact, the attacker can drop packets in a selective technique. For instance, the malicious node can choose to transmit all types of packets, with the exception of requests related to the prediction of energy-consumption or the traffic-safety packets.

4.2.6 Sybil attack. It is a common attack orchestrated by a malicious node that introduces itself under several identities. Its goal is to insert wrong information in the network. Then, it can have an influence on conductors' decision. This attack can take place in one vehicle. In this case, a malicious ECU creates several ECUs having the same identity so as to attain its illegal objectives of attack.

Another scenario of the Sybil attack resides in the fact that the attacker can simulate complex traffic situations involving many virtual vehicles which are perceived as real by legitimate conductors. So, victims can be redirected to the desired location. There are two types of Sybil attack: static and dynamic. The static Sybil attack generates faked nodes having fixed positions. However, the second type prepares Sybil nodes for each vehicle.

4.2.7 Man-in-the-middle (MITM) attack. This type of attack consists in inserting a third party that interrupts and supervises the communications between two other parties. In the case of in-vehicle communication, this attack can take place by introducing an attacker between an ECU and the CAN bus in order to listen, disseminate and intercept messages.

Another scenario can be envisaged by introducing an attacker between two vehicles (the transmitter and the receiver) that communicate together. The attacker monitors the message dissemination between the two victims.

4.2.8 Masquerade (or spoofing or impersonation) attack. We distinguish two scenarios of this attack. The first one can deteriorate in-vehicle functions since it aims to manipulate an

ECU. The adversary requires two ECUs, one is called a strong attacker and the other is called a weak attacker. During the time interval $[0, T_{max}]$, the adversary controls the messages which are transmitted by its weaker attacker as well as its frequency. If the message identifier and its frequency have been learned, the adversary breaks the dissemination of its weak attacker and uses its strong attacker to create and inject malicious messages having the same identifier. In the second scenario, the adversary modifies its identity and transmits wrong information to other vehicles. This genre of attacks can take place by a malicious node that tries to act as an emergency vehicle in order to deceive other vehicles.

The spoofing attack can aim to hide the position of the attacker and give an illusion to other nodes that its vehicle is in other location. This can be achieved by modifying the location table of the global positioning systems (GPS). So, the attacker can secure itself against the actions that can be taken if an accident has been produced or a traffic signal has not been respected (Sun *et al.*, 2019).

4.2.9 Fabrication attack. As its name indicates, the goal of this attack is to damage the integrity of a message by altering or omitting its existing data. Two scenarios can be envisioned according to the access way to the CAN bus. The first one consists in creating a message by an adversary and injecting it with fake ID, DLC and DATA. The goal of this attack is to cancel the transmission of messages by a legitimate ECU. Then, the ECUs receiving the fabricated massage cannot operate properly.

In the second scenario, the fabrication attack is carried out by transmitting fake data in the network. It consists in fabricating messages by greedy drivers and initiating the attack by disseminating massages into the network. We distinguish two possible cases of this attack. The first one can be done by transmitting fake information about the attacker's location, speed and ID to other vehicles or RSUs. In the second case, the attacker introduces itself as an emergency vehicle in order to be able to drive at high speed.

4.2.10 Malware attack. The main objective of this attack is to gather confidential information. It can exist in different forms such as worms, viruses and spyware, which can be injected into vehicles to trigger malicious attacks. We distinguish two scenarios depending on whether the attack is local or remote. In the first one, an attacker inserts a malware within a legal software program such as music files. By downloading and installing the software, the malware will be installed. It runs and transmits hurtful messages into the CAN bus of the vehicle. Another way to affect vehicles with malware is to ask the user to install false updates.

In the second scenario, the malware attack can be inserted into vehicle systems via the installed software components. We consider a vehicle which requests to update its software while communicating with an RSU affected by attackers. Thus, a virus will be injected in the operating system of the vehicle. In this case, the network behavior will be disrupted.

4.2.11 Replay attack. In this attack, the adversary saves a message already transmitted at a certain time and utilizes it at next steps. Here, two scenarios can be considered. In the first one, a malicious ECU sniffs the CAN network to store the content of valid messages associated to various functionalities (such as the speedometer reading). Afterward, it transmits these messages on the network at any time to handle the vehicle operation. Furthermore, it can modify the data in the CAN message. This attack can cause critical problems such as deadline violation, infinite requests for message dissemination, etc.

Another scenario of the replay attack can target the communication between a vehicle and a RSU in a vehicular network. The adversary can interrupt and record the exchanged messages to propagate them through the network and fulfill malicious goals.

4.2.12 Eavesdrop attack. With this attack, the adversary can eavesdrop the messages sent over the network. We distinguish two scenarios that can be summarized as follows:

In the first one, this attack consists in snooping on the CAN bus to determine the precise format and content of a message to monitor an ECU. The attacker can steal some private information, including location and speed of vehicles.

In the second scenario, this attack is performed by collecting sensitive data of the network. In fact, an adversary quietly monitors the network traffic, the motion and the position of a vehicle. It is difficult to detect such attack since it does not have a reaction in the network.

4.2.13 Fuzzy attack. In such type of attack, the adversary randomly generates identifiers and injects arbitrary data to the network. So, a lot of messages are received by the network nodes. This can induce an unexpected behavior of a vehicle (or vehicles) and interruption of data dissemination.

4.2.14 Timing attack. The time synchronization is a key concept in vehicular networks. In fact, any delay in the exchange of critical information can lead to dangerous consequences. The timing attack consists in adding a delay slot by a malicious node to block the message transmission. For example, a malicious node acquires a critical message indicating that an accident has taken place between two vehicles. It can add some delays to message reception. So, the other vehicles cannot change their route.

5. Potential solutions

This section provides the existing defense mechanisms which have been adopted as best practices to cope with the automotive attacks identified in section 4.

5.1 Cryptography

It is one the popular solution which has been adopted by the researchers to address security issues in a CAN network. It guarantees that the CAN data frame transmitted from one node to another is authorized. In the following, we distinguish three types of security algorithms which nodes are used in the cryptography mechanism.

5.1.1 Symmetric-key cryptography. It consists in using a single key both for the encryption and decryption of data. Besides, it requires the installation of a secure channel in order to exchange keys safely.

In Lu *et al.* (2019), introduced an encryption and authentication protocol which ensures the security of in-vehicle networks. This protocol is based on two mechanisms. The first one is responsible for the key management. A secure ECU generates periodically the session keys and transmits them to each pair of ECUs communicating together. In the second mechanism, each pair of these ECUs uses the shared key to ensure the confidentiality and authentication of the CAN messages.

Similarly, in Lakshmanan and Natarajan (2019), the authors proposed an ECU authentication scheme which is based on International Data Encryption Algorithm (IDEA). The symmetric-key cryptography is adopted in this scheme to generate an authentication code and facilitate the key exchange and update operations. Its main goal is the need of small resource requirements due to its repetitive nature.

Additionally, in Wang and Sawhney (2014), a security framework for vehicular systems, called VeCure, was proposed to resolve the message authentication issues of the CAN bus. This framework is based on trust groups where nodes share a symmetric key to generate an authenticated code for each outgoing message and check obtained messages.

5.1.2 Asymmetric cryptography. This type of cryptography is more secure than the first one since it consists in using two keys: public key and private key. A given node sends a public key to each node of the network. This key is used by other network nodes to transmit encrypted messages to the reference node. Only the original node can decrypt the message using the private key.

In Mundhenk *et al.* (2017), introduced a lightweight authentication protocol to secure in-vehicle networks while respecting real-time constraints and resources requirements. The proposed approach consists in using primitives which rely on asymmetric cryptography.

In fact, each ECU is configured with a set of trusted Certification Authorities (CAs) and saves a key pair signed by one of the CAs. The communication between ECUs can be ensured by interchanging symmetric session keys. Moreover, the vehicle that can cancel invalid certificates contains a specialized ECU.

5.2 Firewall

A firewall is a security system which controls entering and outgoing network traffic using several rules. It distinguishes untrusted regions and trusted ones and blocks illegitimate entities. The implementation of a firewall is performed in the security gateway.

To ensure safe automobile networks and reduce potential types of intrusions, Rizvi *et al.* (2017) introduced a security system which includes different layers of security where each one contains many modules. These layers ensure flexibility for manufacturers who need further security for their vehicles. In order to filter harmful content, distributed firewalls have been put in each module and ECU.

In another proposal, Kornaros *et al.* (2018) proposed a security solution which ensures hardware-assisted protection against software attacks. This solution consists of an authentication method and configuration rules written to the firewall. The main goal of these rules is to guarantee that each application uses the devices already specified.

5.3 Intrusion detection system (IDS)

IDS aims at preventing attacks by detecting them at an early stage. Whenever an attack is fired, several warnings can be generated. We distinguish five detection methods which are detailed in what follows.

5.3.1 Signature-based method. It consists in saving a set of existing signatures in IDS database. These signatures are associated with malicious events of popular attacks. Then, it makes a comparison between the system's behavior and the attack patterns already stored. This method requires periodic updates to consider new attacks.

In this context, Studnia *et al.* (2018) presented a signature-based solution for detecting intrusions in vehicular network. In this method, the behavior of popular attack signatures and authorized ECUs are modeled. Its goal is to generate prohibited messages sequences (i.e. signatures) which are useful to detect intrusions.

5.3.2 Anomaly-based method. It is called also behavior based detection. It consists in observing the system behaviors and comparing it with the baseline of normal cases. If abnormal information has been detected, an alarm will be triggered. Compared to signature-based, this method can detect unknown attacks. However, its accuracy is usually lower than the signature-based method. In signature-based IDS, intrusions are detected by comparing monitored behaviors with pre-defined intrusion patterns, while anomaly-based IDS focuses on knowing normal behavior to identify any deviation.

In Sagong *et al.* (2018), introduced an anomaly-based IDS which takes into consideration several voltage-based attacks to protect the CAN protocol. The proposed IDS aims to identify unpredictable deviations from their behaviors and monitor physical properties (such as clock skew, message periodicity, voltage, etc.). It includes fuses or circuit breakers that are connected the CAN bus and the microcontroller's analog pins.

An IDS for in-vehicle networks was introduced in Müter *et al.* (2010). It contains a set of anomaly detection sensors (such as correlation sensor, range sensor, location sensor, etc.), related to the behavior of the CAN bus, which enable the identification of threats during the vehicle operation without engendering fake positives.

5.3.3 Statistic-based method. This method is based on using statistical properties (such as variance and mean) of normal tasks to establish a normal profile and utilize statistical tests. Its goal is to verify whether the observed tasks differ a lot from the norm profile. In contrast to

signature-based method and anomaly-based method, statistic-based approaches identify intrusions based on probabilities and statistics and compare them to predefined thresholds. They can use multiple options depending on the characteristics of the used dataset. In Narayanan *et al.* (2016), presented a new attempt to detect abnormal activities in the CAN bus traffic. They collected CAN messages data of vehicles from several automotive manufactures, including load, speed, values of physical sensor, etc. Then, they adopted Hidden Markov Models to analyze event sequences for malicious behaviors and generate transition probabilities. The purpose of the proposed technique is to generate alerts if an abnormal state is detected while supervising CAN messages.

Another intrusion detection algorithm was proposed by Marchetti and Stabili (2017) to discover malicious messages injected by attackers in the CAN bus. The identified anomalies have small memory and computational footprints. The proposed algorithm consists of two different steps. The first one uses CAN bus logs to produce a data structure. The latter includes all transitions between successive identifiers in CAN traffic traces that do not contain any attack. This step has a transition matrix as output. The second step takes this matrix and the traffic traces to examine them and identify attacks.

5.3.4 Hybrid method. Security attacks in CAN bus can take various forms and can be under many conditions. Adopting only one IDS method is sometimes insufficient to detect different types of unsafe CAN messages. Therefore, some research efforts suggest combining more than one type of IDS methods.

Grimm *et al.* (2018) introduced a hybrid detection system for ECUs to enhance the security of vehicles. This system incorporates anomaly detection and machine learning methods to identify irregularities. It consists of two steps. The first one evaluates the signals and the protocol headers whenever a message is transmitted or received. In the second step, pertinent information is derived from messages and forwarded to learning checks.

Another trend aims at introducing hybrid IDS algorithms which can detect both anomalous events and attack signatures. In this context, the authors of Song *et al.* (2016) presented a lightweight algorithm which consists in analyzing time intervals of CAN messages and detecting the attacks related to data injection in few time. These attacks can have diagnostic and standard messages.

5.3.5 Machine learning-based method. One of the most used methods for intrusion detection is based on learning techniques which have recently gained a great attention to enhance systems security. In fact, researchers have explored machine learning (Jordan and Mitchell, 2015) with an emphasis on deep learning algorithms (Shrestha and Mahmood, 2019) to detect intrusions and identify unusual behaviors in the CAN bus.

Chockalingam *et al.* (2016) studied several machine learning algorithms. They compared their ability to identify abnormal behaviors when an attacker is attempting to execute malicious commands. The comparison consists in using different types of unusual behaviors.

In Zhang *et al.* (2018), the authors proposed an IDS which consists of two steps. The first one uses some detection rules to reduce the time-consuming in the second step. The latter is based on deep learning techniques to detect, in real time, sophisticated attacks which violate CAN traffic. It is based on two components: the discriminator and the generator.

6. Validation strategies

The validation strategies indicate how a proposed protocol is validated in terms of correctness and performance criteria. This consists in ensuring whether a protocol is operating as expected. In the literature, different validation strategies have been adopted for evaluating the proposed protocols. In what follows, we provide an overview of each strategy and a brief description of some related works.

6.1 Simulation strategy

Simulation is a widely used validation strategy. It provides a free environment which can imitate the system behavior and the conditions of a real environment. Using simulation, experiments can be easily replicated and controlled. A vast amount of works has been conducted based on this strategy.

In Zheng *et al.* (2016), proposed a cross-layer framework for modeling, exploring and validating connected vehicles. To illustrate the efficiency of this framework, the authors adopted a case study to analyze the timing and the influence of security attacks in V2V applications.

In another proposal, Cros and Chênevert (2019) introduced a hashing protocol in CAN bus which consists in hashing each message with a key. In fact, computing this key is less costly than the encryption and the decryption of a message. The proposed protocol consists in altering the CAN header to split between ID representation and hash storing. In order to evaluate this protocol, the authors built a CAN bus simulator. They performed some simulations scenarios on different network sizes to estimate the average delay between errors.

The work presented in Avatefipour *et al.* (2019) tackled the problem of detecting malicious attack behaviors in CAN traffic by proposing a new anomaly detection model. This model is based on the Bat algorithm (Yang, 2011) and it aims to optimally adjust the parameters allowing to increase its efficiency. In order to evaluate the performance of this model, it is compared to two competitive CAN bus anomaly detection algorithms. The simulation experiments are based on two CAN bus traffic dataset and a data gathered from a vehicle.

Another attempt to protect vehicles against cyberattacks was introduced by Levi *et al.* (2018) using machine learning techniques. The proposed approach aims at supervising the basic vehicle interfaces (CAN, network and operating system). It allows obtaining pertinent information using configurable rules and transmits it to a trained model to discover deviations from normal behavior. Training the model using events produced by a rule-based engine is an important task to control the different interfaces. The authors used a dynamic threshold which is suitable for their temporal setting. In order to evaluate their solution, the authors adopted the SUMO tool (Krajzewicz *et al.*, 2012) to simulate a set of vehicles. Each event produced in the vehicle is sent to the backend. Several experiments were achieved to simulate the implemented algorithms and analyze the performance of the dynamic threshold for an anomaly.

6.2 Experimental strategy

It is an important strategy which consists in using real experiments based on dedicated physical testbed to evaluate the behavior of a system. In the following, we highlight some research studies adopting this strategy.

In Woo *et al.* (2014), proposed an attack model for the vulnerability of CAN bus in a vehicle. They analyzed this model based on a connected vehicle environment containing a malicious smartphone application and a real vehicle. Moreover, they proposed a security protocol for CAN and they evaluated its feasibility through a DSP-F28335 microcontroller and a CANoe software [1].

The contribution of the approach cited in Cho and Shin (2016) introduced an anomaly-based IDS which aims to detect in-vehicle attacks. To do so, the authors used intervals of periodic messages to identify fingerprinting ECUs. The performance of the proposed system has been shown using a CAN bus prototype and three real vehicles. Also, the presented experiments demonstrate the capability of the system in detecting some basic attacks such as masquerade, fabrication and suspension attacks.

In Ying *et al.* (2019), developed a scheme which ensures safe authentication of ECUs on the CAN bus. It can detect attacks which can break the dissemination of normal CAN messages

and the attacks in which adversaries fail to produce legitimate authentication messages. They evaluated its performance through extensive experiments using real vehicle datasets. The testbed contains UW EcoCAR [2] and two testbed ECUs connected via the OBD port.

Additionally, the approach proposed in Wang and Sawhney (2014) introduced a security framework which aims to protect vehicular systems against attacks resulted by the injection of spoofed messages. The authors incorporated a new protocol to resolve problems of authentication messages in the CAN bus. This protocol is based on cryptographic functions that consist in using a key which is known to authorized nodes. To validate the proposed framework, a new prototype was implemented by adopting Freescale's automotive development boards.

6.3 Formal verification

The use of a formal foundation to describe a system is very useful for checking its correctness. Indeed, formal verification provides an effective way for the designer to evaluate the behavior of a system and prevent errors before the implementation. It consists in describing the properties to be proven without worrying about the possible scenarios. In the literature, only few research studies have been proposed to address the correctness of intrusion detection protocols.

The approach proposed in Lu *et al.* (2019) suggested an authentication protocol and an encryption mechanism to prevent vulnerabilities in the CAN bus. To ensure the correctness of their solution, the authors theoretically prove some properties which guarantee the security against four attacks (eavesdrop, replay, masquerade and flooding). To do so, they adopted handwritten proofs.

In another proposal, Patsakis *et al.* (2014) presented architecture for in-vehicle communication that considers two aspects. The first one is the mutual authentication of ECUs. The second one is the different access roles and rights of users. These aspects allow reducing different vehicle attacks and triggering suitable alarms to detect and mitigate them. To this end, an authentication protocol has been proposed and formally verified using Scyther tool (Cremers, 2008).

7. Discussion and research challenges

7.1 Discussion

We present in this section a detailed analysis related to the studied approaches of security attacks in automotive networks based on CAN bus. In addition, we give the remarks that we have made about the RQs introduced in section 3.

In order to answer to RQ1 "*What are the attacks studied in the existing works?*", we identified two types of attacks as mentioned in section 4. The first type is called local attacks which need to access the vehicle physically and require direct or indirect access to the CAN bus network. The second one is called remote attacks which are implemented via wireless communication interfaces. They are performed without having physical access to bus systems. They can be classified according to the range of wireless access. Also, a set of attack types were listed while describing two scenarios: in-vehicle (local attack) and inter-vehicle (remote attack). In addition, we notice that most of the studied research papers are interested in attacks targeting the integrity or availability of automotive systems (Cho and Shin, 2016). Moreover, the existing proposals concentrate mostly on protecting vehicles from DoS (Rizvi *et al.*, 2017; Zhang *et al.*, 2018) and replay attacks (Cros and Chênevert, 2019; Wang and Liu, 2018; Gao *et al.*, 2019). According to the reviewed papers, we also observe that there is no work which aims at detecting the maximum attack types at the same time. Gmiden *et al.* (2016) is the only paper declaring that its proposed solution could be extended to detect more than the treated attacks.

With regards to RQ2 "*Which solutions have been implemented to prevent the different attacks?*", we identified a set of security mechanisms as shown in section 5. We notice that a great attention has been paid to IDSs (Studnia *et al.*, 2018; Sagong *et al.*, 2018; Müter *et al.*, 2010; Narayanan *et al.*, 2016; Marchetti and Stabili, 2017). In fact, IDSs can detect unexpected behaviors with time guarantee. Also, they provide precise information to prevent damage from malicious adversaries. Some papers (Lu *et al.*, 2019; Lakshmanan and Natarajan, 2019; Wang and Sawhney, 2014; Mundhenk *et al.*, 2017) focus on cryptography method to ensure the network security. This method is one the popular solution which guarantees that the CAN data frame transmitted from one node to another is authorized. However, this method cannot satisfy the real-time requirement and other constraints (such as cost and bandwidth) related to CAN bus based networks (Chakraborty *et al.*, 2016; Wasicek *et al.*, 2014). For instance, it is difficult to produce message authentication for a CAN bus due to the insufficient space available for adding the message code. Besides, only two works (Rizvi *et al.*, 2017; Kornaros *et al.*, 2018) have been established based on the firewall mechanism which blocks access to illegitimate entities. Nevertheless, this mechanism does not generate an alarm message to take corrective actions, as is the case with IDS.

In Table 2, we present a classification of some studied works according to their security solutions, as well as the treated attacks (NM: Not mentioned).

Although different solutions have been proposed to secure connected vehicles, they still face several constraints that must be considered during their design and implementation. In what follows, we present some of these constraints:

(1) *Response time*: ECUs in connected vehicles are characterized by a limited computational power. However, vehicle software should satisfy real-time constraints to guarantee the protection of drivers and vehicles. So, any defense

Table 2.
Comparison of security solutions based on security attacks and requirements

Reference	Treated attacks	Security solutions	Class of attacks	
			Local	Remote
Lu *et al.* (2019)	(1) Eavesdropping (2) Replay (3) Masquerade (4) Flooding	Symmetric-key cryptography	✓	
Cho and Shin (2016)	(1) Fabrication (2) Suspension (3) Masquerade	IDS (anomaly-based method)	✓	
Rizvi *et al.* (2017)	(1) DoS	Firewall		✓
Wang and Sawhney (2014)	(1) Spoofing (2) Replay attack	Symmetric-key cryptography		✓
Studnia *et al.* (2018)	NM	IDS (Signature-based method)	✓	
Narayanan *et al.* (2016)	NM	IDS (Statistic-based method)		✓
Marchetti and Stabili (2017)	(1) Replay	IDS (anomaly-based method)	✓	
Chockalingam *et al.* (2016)	(1) Fuzzy attacks	IDS (Machine learning-based method)	✓	
Zhang *et al.* (2018)	(1) Replay (2) Spoofing (3) Fuzzing (4) DoS (5) Black hole	IDS (Machine learning-based method)	✓	
Chen *et al.* (2019)	(1) DoS (2) Fuzzy (3) Impersonation	IDS (Machine learning-based method)	✓	

mechanism should not impact vehicle performance and must meet requirements related to response time.

(2) *Hardware*: Vehicle's embedded software has limited memory resources and computational power. Thus, security mechanisms cannot achieve advanced features (such as strong cryptographic functions). Nevertheless, the adversary's hardware does not suffer from these limitations.

(3) *Cost*: Decreasing hardware cost can give enterprises further benefits since they can have a significant production of vehicles. The manufacturing cost of vehicles becomes quite important once the design of defense mechanisms needs the change of ECUs hardware. Therefore, these mechanisms are subject to cost constraints.

Regarding to RQ3 "*Which strategies are used to validate the proposed solutions?*", we observe that three strategies have been adopted: simulation, experimentation and formal verification. A vast amount of works (Cho and Shin, 2016; Wang and Sawhney, 2014; Ying *et al.*, 2019; Song *et al.*, 2020; Nasser and Ma, 2020) have been validated based on experimentation which are very important to show the solution efficiency in a real world. Also, some research attempts (Cros and Chênevert, 2019; Levi *et al.*, 2018; Avatefipour *et al.*, 2019) have adopted simulation to imitate the system behavior and evaluate a set of performance criteria. However, a little consideration has been given to the formal verification which provides an effective way for the designer to evaluate the behavior of a system and prevent errors before the implementation (Lu *et al.*, 2019; Patsakis *et al.*, 2014; Wang and Liu, 2018; Woo *et al.*, 2019). We distinguish three formal verification methods: handwritten proofs (Mendes and Ferreira, 2018), model checking (Baier and Katoen, 2008) and theorem proving (Cook, 1971). The first one does not require time and effort to master a formal language. Nevertheless, it is error-prone especially in the case of complex systems. So, a minor error can have serious consequences on the system operation. As concerns the model checking, it is a powerful verification method which provides a platform for proving the correctness of systems. The main drawback of this method is the state space explosion problem. We also notice the absence of theorem proving based approaches despite the effective correctness of this method which can deal with complex formalisms and handle infinite state spaces. Some research studies are based on two strategies (simulation and formal verification) to validate their proposed solutions such as (Mundhenk *et al.*, 2017; Lu *et al.*, 2019). Other works do not provide validation results like (Müter *et al.*, 2010; Matsumoto *et al.*, 2012). However, it is necessary to fix validation metrics in each work to compare it with existing solutions.

To the best of our knowledge, there is no published study which has adopted testing (Brenner *et al.*, 2007; Sohal *et al.*, 2018) as a validation strategy for automotive systems based on the CAN bus. Testing is a robust method that consists in executing a system with the intent of detecting errors which can induce software failure.

In Table 3, we present a comparison of some reviewed papers regarding the following criteria: treated attacks, validation strategy, evaluation size and evaluation environment.

7.2 Research challenges

Ensuring the security of connected vehicles against cyberattacks has become a subject of intensive researches. Then, numerous defense mechanisms have been proposed in the literature. However, with the help of our critical and comparative study presented in our paper, we notice that this research field still faces several challenges. In what follows, we present a list of open issues that need to be further investigated in the future:

7.2.1 Proving the correctness of defense mechanisms. Formal verification is extremely important for preventing design errors of defense mechanisms and then ensuring the security properties defined by the designer. Although few works, such as Lu *et al.* (2019),

Year	Reference	Treated attacks	Validation strategy	Evaluation size	Evaluation environment
2014	Patsakis *et al.* (2014)	(1) DoS	Formal verification	One vehicle	Scyther
2016	Zheng *et al.* (2016)	(1) Flooding	Simulation	50 vehicles + a road of length 300 m	VENTOS + NS-3
2016	Mundhenk *et al.* (2016)	NM	Simulation	100 ECUs and 500 messages	IVNS
2016	Cho and Shin (2016)	(1) Masquerade (2) Fabrication (3) Suspension	Experimentation	3 vehicles (Honda Accord, Toyota Camry and Dodge)	Real vehicles
2017	Mundhenk *et al.* (2017)	NM	Formal verification	60 to 100 ECUs	Scyther
2018	Wang and Liu (2018)	(1) DoS (2) Eavesdropping (3) Replay	Simulation + Formal verification	NM	Finite state machine (FSM) + MATLAB Simulink
2019	Cros and Chênevert (2019)	(1) Replay attacks (2) DoS	Simulation	From 3 to 15 nodes	NM
2019	Lu *et al.* (2019)	(1) Eavesdrop (2) Replay (3) Masquerade (4) Flooding	Experimentation + Formal verification	One vehicle	Real vehicle
2019	Gao *et al.* (2019)	(1) Replay (2) DoS (3) Flooding	Experimentation	One vehicle	Real vehicle
2019	Takada *et al.* (2019)	(1) DoS	Experimentation	One vehicle	Real vehicle
2019	Olufowobi *et al.* (2019)	(1) Fuzzy (2) Spoofing (3) DoS	Experimentation	6 vehicles	Real vehicles
2019	Woo *et al.* (2019)	(1) Impersonation (2) Replay (3) DoS	Simulation + Formal verification	One vehicle	CANoe
2020	Song *et al.* (2020)	(1) DoS (2) Spoofing (3) Fuzzy	Experimentation	One vehicle	Real vehicle
2020	Nasser and Ma (2020)	(1) Masquerading	Experimentation	One vehicle	Real vehicle

Table 3.
Summary of some papers based on their validation strategies

Patsakis *et al.* (2014), addressed the correctness of these mechanisms, they still in very early stages. So, more efforts need to be made for specifying and verifying the solutions which are proposed to cope with automotive attacks. In addition, timing constraints have to be considered to ensure the safety of conductors and vehicles. Achieving this need will require an efficient modeling method and a tool that can specify time-related properties.

7.2.2 Securing connected vehicles using blockchain. Blockchain is a distributed data structure containing blocks that are chained together cryptographically in chronological

order (Saranti *et al.*, 2018). For instance, this technology is used in Alam *et al.* (2019) to secure communication data between intra-vehicular ECUs. Also, it can be exploited in V2X communication systems to facilitate the secure distribution of basic safety messages between vehicles and RSUs and/or the Cloud platform (Shrestha *et al.*, 2020). To our knowledge, few attempts (Liem *et al.*, 2017) have explored the Blockchain potential to overcome the security challenges. Then, developing a suitable Blockchain model remains as a promising option to satisfy the conditional anonymity and ensure the authenticity of the broadcast messages in the automotive platform.

7.2.3 Using machine learning/deep learning to hunt cybersecurity. Securing connected vehicles using Blockchain cybersecurity solutions based on classical statistical models and rule-based logic will not be able to fully use data at the automotive platform and Cloud (El-Rewini *et al.*, 2019). In Liang *et al.* (2018), Ye *et al.* (2018), the authors mention the grow-up of research interest in applying machine learning and deep learning (Goodfellow *et al.*, 2016) for developing cybersecurity solutions. For example, machine learning models are applied in Taylor *et al.* (2016) to secure the network and detect anomalies during information exchange between automotive system components. Despite their success, the use of machine learning to develop cybersecurity solutions faces many challenges (El-Rewini *et al.*, 2019) such as protecting machine learning models against adversarial attacks and optimizing model architectures.

7.2.4 Improving simulation based approaches. A number of works (Zheng *et al.*, 2016; Cros and Chênevert, 2019; Avatefipour *et al.*, 2019; Levi *et al.*, 2018) have attempted to evaluate their proposed solutions against attacks based on simulation. However, there is a dearth of efforts trying to compare their solutions with others that have similar conditions (Mundhenk *et al.*, 2016; Avatefipour *et al.*, 2019). The evaluation of the adopted methods among the other one is an important task to help researchers make the best decisions in accordance with their primary goal.

7.2.5 Improving security solutions for 5G technology. The fifth generation (5G) (Gohil *et al.*, 2013) has emerged as a promising mobile technology for intelligent transportation systems. It ensures low latency and real-time monitoring of data. According to Pan *et al.* (2017), the use of 5G technology with automotive networks produces new features for vehicles which can lead to more attacks. This can bring new issues to cybersecurity defense mechanisms intended for the CAN bus network. In fact, the current mechanisms become obsolete if they are not adapted to the new requirements of 5G (Liao *et al.*, 2018).

7.2.6 Adopting design patterns. A vast amount of security solutions have been proposed to deal with attacks on CAN bus networks such as cryptography, IDS, firewall, etc. Using design patterns (Gamma *et al.*, 1993) for securing automotive networks is a promising topic. In fact, formalizing a common problem and security solutions into design patterns guarantees rigorous development practices and is very helpful for design reuse. To the best of our knowledge, only the work of Cheng *et al.* (2019) attempts to propose some design patterns for cybersecurity requirements on CAN bus. However, this work has considered only IDS based strategies. Therefore, many open issues still worthy of exploration to obtain better solutions for such challenge.

7.2.7 Adopting detection approach based on honeypots. Honeypot (Spitzner, 2003) is a potential solution that can be used to collect and analyze attacker behaviors. In vehicular networks, many proposals (Gantsou and Sondi, 2014; Patel and Jhaveri, 2017; Sharma and Kaul, 2018) relied on the honeypot to deal with security attacks. To date, we have identified only an old work (Verendel *et al.*, 2008) which introduces a placement strategy of a honeypot within a driving vehicle based on CAN bus. However, this work has not been implemented in a realistic setting. Therefore, the literature still lacks an effective solution to overcome the security attacks using honeypots. This challenge will be the trend of future research.

8. Conclusion

Connected vehicles based on CAN bus are exposed to a vast number of security attacks that can be used by adversaries to affect the behavior of vehicles. So, securing automotive networks against these attacks is emerging as a fundamental concern for vehicles. In this paper, we present a comparison between the existing surveys focusing on cybersecurity attacks. Unlike the aforementioned surveys, our paper is the first SLR which deals with local and remote security attacks with a comprehensive discussion. We have conducted our SLR based on a set of selected papers ranging from 2010 to July 2020. In this paper, a holistic view about the different attacks scenarios has been introduced. Afterward, we have addressed an overview of the possible solutions aiming to cope with automotive attacks. Furthermore, we have presented a description of the validation strategies attempting to check the accuracy and the correctness of the reviewed proposals. The benefits and the drawbacks of these strategies have been examined. Our survey paper provides also a rich discussion related to the studied approaches based on the RQs. Finally, a set of open challenges that can significantly improve the existing works have been emphasized.

As a future work, we believe that improving validation strategies is one of the most important needs. More specifically, we plan to extend the proposed defense mechanisms by ensuring the correctness of temporal properties (such as liveness properties). Furthermore, we plan to guarantee rigorous development practices by specifying common problems and security solutions into design patterns.

Notes

1. https://www.vector.com/int/en/products/products-a-z/software/canoe/
2. https://uwecocarcom.wixsite.com/website

References

Al-Jarrah, O.Y., Maple, C., Dianati, M., Oxtoby, D. and Mouzakitis, A. (2019), "Intrusion detection systems for intra-vehicle networks: a review", *IEEE Access*, Vol. 7, pp. 21266-21289.

Alam, M.S.U., Iqbal, S., Zulkernine, M. and Liem, C. (2019), "Securing vehicle ecu communications and stored data", *IEEE International Conference on Communications (ICC)*, IEEE, pp. 1-6.

Avatefipour, O., Al-Sumaiti, A.S., El-Sherbeeny, A.M., Awwad, E.M., Elmeligy, M.A., Mohamed, M.A. and Malik, H. (2019), "An intelligent secured framework for cyberattack detection in electric vehicles' can bus using machine learning", *IEEE Access*, Vol. 7, pp. 127580-127592.

Baier, C. and Katoen, J.-P. (2008), *Principles of Model Checking*, MIT Press, London.

Bozdal, M., Samie, M., Aslam, S. and Jennions, I. (2020), "Evaluation of can bus security challenges", *Sensors*, Vol. 20 No. 8, p. 2364.

Brenner, D., Atkinson, C., Malaka, R., Merdes, M., Paech, B. and Suliman, D. (2007), "Reducing verification effort in component-based software engineering through built-in testing", *Information Systems Frontiers*, Vol. 9 Nos 2-3, pp. 151-162.

Chakraborty, S., Al Faruque, M.A., Chang, W., Goswami, D., Wolf, M. and Zhu, Q. (2016), "Automotive cyber–physical systems: a tutorial introduction", *IEEE Design and Test*, Vol. 33 No. 4, pp. 92-108.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S. and Koscher, K. (2011), "Comprehensive experimental analyses of automotive attack surfaces", *20th USENIX Security Symposium*, Vol. 4, pp. 447-462.

Chang, V., Sharma, S. and Li, C.-S. (2020), "Smart cities in the 21st century", *Technological Forecasting and Social Change*, Elsevier, Vol. 153 No. C.

Chen, Y., Hu, W., Alam, M. and Wu, T. (2019), "Fiden: intelligent fingerprint learning for attacker identification in the industrial internet of things", *IEEE Transactions on Industrial Informatics*.

Cheng, B.H., Doherty, B., Polanco, N. and Pasco, M. (2019), "Security patterns for automotive systems", *ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, IEEE, pp. 54-63.

Cho, K.-T. and Shin, K.G. (2016), "Fingerprinting electronic control units for vehicle intrusion detection", *25th USENIX Security Symposium*, pp. 911-927.

Chockalingam, V., Larson, I., Lin, D. and Nofzinger, S. (2016), "Detecting attacks on the can protocol with machine learning", *8th Annual EECS Security Symposium*.

Choi, W., Joo, K., Jo, H.J., Park, M.C. and Lee, D.H. (2018), "Voltageids: low-level communication characteristics for automotive intrusion detection system", *IEEE Transactions on Information Forensics and Security*, Vol. 13 No. 8, pp. 2114-2129.

Consortium, F., *et al.* (2005), "Flexray communications system protocol specification", *Version*, Vol. 2 No. 1, pp. 198-207.

Cook, S.A. (1971), "The complexity of theorem-proving procedures", *3rd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 151-158.

Cremers, C.J. (2008), "The scyther tool: verification, falsification, and analysis of security protocols", *20th International Conference on Computer Aided Verification (CAV)*, Springer, pp. 414-418.

Cros, O. and Chênevert, G. (2019), "Hashing-based authentication for can bus and application to denial-of-service protection", *3rd International Conference on Cyber Security in Networking (CSNet)*, IEEE.

den Hartog, J., Zannone, N., *et al.* (2018), "Security and privacy for innovative automotive applications: a survey", *Computer Communications*, Vol. 132, pp. 17-41.

Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., Zhang, Y., Deng, Y., Wen, S., Zhang, J., Xiang, Y. and Yu, S. (2019), "An overview of attacks and defences on intelligent connected vehicles", CoRR, Vol. abs/1907.07455, arXiv preprint.

El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J. and Ranganathan, P. (2019), "Cybersecurity challenges in vehicular communications", *Vehicular Communications*, Vol. 23, p. 100214.

Gamma, E., Helm, R., Johnson, R. and Vlissides, J. (1993), "Design patterns: abstraction and reuse of object-oriented design", *European Conference on Object-Oriented Programming*, Springer, pp. 406-431.

Gantsou, D. and Sondi, P. (2014), "Toward a honeypot solution for proactive security in vehicular ad hoc networks", *Future Information Technology*, Springer, Berlin, Heidelberg, pp. 145-150.

Gao, L., Li, F., Xu, X. and Liu, Y. (2019), "Intrusion detection system using soeks and deep learning for in-vehicle security", *Cluster Computing*, Vol. 22 No. 6, pp. 14721-14729.

Gmiden, M., Gmiden, M.H. and Trabelsi, H. (2016), "An intrusion detection method for securing in-vehicle can bus", *17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, IEEE, pp. 176-180.

Gmiden, M., Gmiden, M.H. and Trabelsi, H. (2019), "Cryptographic and intrusion detection system for automotive can bus: survey and contributions", *16th International Multi-Conference on Systems, Signals and Devices (SSD)*, IEEE, pp. 158-163.

Gohil, A., Modi, H. and Patel, S.K. (2013), "5G technology of mobile communication: a survey", *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, IEEE, pp. 288-292.

Goodfellow, I., Bengio, Y., Courville, A. and Bengio, Y. (2016), *Deep Learning*, Vol. 1, MIT press Cambridge.

Grimm, D., Weber, M. and Sax, E. (2018), "An extended hybrid anomaly detection system for automotive electronic control units communicating via ethernet - efficient and effective analysis using a specification- and machine learning-based approach", *4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS)*, pp. 462-473.

Jordan, M.I. and Mitchell, T.M. (2015), "Machine learning: trends, perspectives, and prospects", *Science*, Vol. 349 No. 6245, pp. 255-260.

Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J. and Linkman, S. (2009), "Systematic literature reviews in software engineering–a systematic literature review", *Information and Software Technology*, Vol. 51 No. 1, pp. 7-15.

Kornaros, G., Tomoutzoglou, O. and Coppola, M. (2018), "Hardware-assisted security in electronic control units: secure automotive communications by utilizing one-time-programmable network on chip and firewalls", *IEEE Micro*, Vol. 38 No. 5, pp. 63-74.

Krajzewicz, D., Erdmann, J., Behrisch, M. and Bieker, L. (2012), "Recent development and applications of sumo-simulation of urban mobility", *International Journal On Advances in Systems and Measurements*, Vol. 5 Nos 3 and 4.

Lakshmanan, M. and Natarajan, S.K. (2019), "Security enhancement in in-vehicle controller area networks by electronic control unit authentication", *Science and Technology*, Vol. 22 Nos 3-4, pp. 228-243.

Lee, S.-Y., Park, S.-H., Choi, H.-S. and Lee, C.D. (2012), "Most network system supporting full-duplexing communication", *14th International Conference on Advanced Communication Technology (ICACT)*, IEEE, pp. 1272-1275.

Levi, M., Allouche, Y. and Kontorovich, A. (2018), "Advanced analytics for connected car cybersecurity", *87th IEEE Vehicular Technology Conference (VTC Spring)*, IEEE, pp. 1-7.

Liang, L., Ye, H. and Li, G.Y. (2018), "Toward intelligent vehicular networks: a machine learning framework", *IEEE Internet of Things Journal*, Vol. 6 No. 1, pp. 124-135.

Liao, D., Li, H., Sun, G., Zhang, M. and Chang, V. (2018), "Location and trajectory privacy preservation in 5g-enabled vehicle social network services", *Journal of Network and Computer Applications*, Vol. 110, pp. 108-118.

Liem, C., Abdallah, E., Okoye, C., O'Connor, J., Alam, M.S.U. and Janes, S. (2017), "Runtime self-protection in a trusted blockchain-inspired ledger", *15th Escar Europe*.

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* No. 1, p. 184.

Lu, Z., Wang, Q., Chen, X., Qu, G., Lyu, Y. and Liu, Z. (2019), "Leap: a lightweight encryption and authentication protocol for in-vehicle communications", *22nd IEEE Intelligent Transportation Systems Conference (ITSC)*, IEEE, pp. 1158-1164.

Marchetti, M. and Stabili, D. (2017), "Anomaly detection of CAN bus messages through analysis of ID sequences", *IEEE Intelligent Vehicles Symposium*, IEEE, pp. 1577-1583.

Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K. and Oishi, K. (2012), "A method of preventing unauthorized data transmission in controller area network", *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, IEEE, pp. 1-5.

Mendes, A. and Ferreira, J.F. (2018), "Towards verified handwritten calculational proofs", *9th International Conference on Interactive Theorem Proving (ITP)*, Springer, pp. 432-440.

Moreno, M.V., Terroso-Sáenz, F., González-Vidal, A., Valdés-Vela, M., Skarmeta, A.F., Zamora, M.A. and Chang, V. (2016), "Applicability of big data techniques to smart cities deployments", *IEEE Transactions on Industrial Informatics*, Vol. 13 No. 2, pp. 800-809.

Mundhenk, P., Mrowca, A., Steinhorst, S., Lukasiewycz, M., Fahmy, S.A. and Chakraborty, S. (2016), "Open source model and simulator for real-time performance analysis of automotive network security", *ACM Sigbed Review*, Vol. 13 No. 3, pp. 8-13.

Mundhenk, P., Paverd, A., Mrowca, A., Steinhorst, S., Lukasiewycz, M., Fahmy, S.A. and Chakraborty, S. (2017), "Security in automotive networks: lightweight authentication and authorization", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 22 No. 2, pp. 1-27.

Müter, M., Groll, A. and Freiling, F.C. (2010), "A structured approach to anomaly detection for in-vehicle networks", *6th International Conference on Information Assurance and Security (IAS)*, IEEE, pp. 92-98.

Narayanan, S.N., Mittal, S. and Joshi, A. (2016), "Obd_securealert: an anomaly detection system for vehicles", *2nd IEEE International Conference on Smart Computing (SMARTCOMP)*, IEEE, pp. 1-6.

Nasser, A.M. and Ma, D. (2020), "Secmonq: an hsm based security monitoring approach for protecting autosar safety-critical systems", *Vehicular Communications*, Vol. 21, p. 100201.

Olufowobi, H., Young, C., Zambreno, J. and Bloom, G. (2019), "Saiducant: specification-based automotive intrusion detection using controller area network (can) timing", *IEEE Transactions on Vehicular Technology*.

Pan, L., Zheng, X., Chen, H., Luan, T., Bootwala, H. and Batten, L. (2017), "Cyber security attacks to modern vehicular systems", *Journal of Information Security and Applications*, Vol. 36, pp. 90-100.

Patel, P. and Jhaveri, R. (2017), "A honeypot scheme to detect selfish vehicles in vehicular ad-hoc network", *Computing and Network Sustainability*, Springer, pp. 389-401.

Patsakis, C., Dellios, K. and Bouroche, M. (2014), "Towards a distributed secure in-vehicle communication architecture for modern vehicles", *Computers and Security*, Vol. 40, pp. 60-74.

Pedreiras, P. and Almeida, L. (2002), "Flexibility, timeliness and efficiency over ethernet", *1st International Workshop on Real-Time LANs in the Internet Age*.

Rizvi, S., Willett, J., Perino, D., Vasbinder, T. and Marasco, S. (2017), "Protecting an automobile network using distributed firewall system", *2nd International Conference on Internet of things, Data and Cloud Computing (ICC)*, pp. 1-6.

Ruff, M. (2003), "Evolution of local interconnect network (LIN) solutions", *IEEE 58th Vehicular Technology Conference (VTC)*, IEEE, Vol. 5, pp. 3382-3389.

Sagong, S.U., Ying, X., Poovendran, R. and Bushnell, L. (2018), "Exploring attack surfaces of voltage-based intrusion detection systems in controller area networks", *ESCAR Europe Conference*, pp. 1-13.

Saranti, P.G., Chondrogianni, D. and Karatzas, S. (2018), "Autonomous vehicles and blockchain technology are shaping the future of transportation", *4th Conference on Sustainable Urban Mobility*, Springer, pp. 797-803.

Sharma, S. and Kaul, A. (2018), "A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud", *Vehicular Communications*, Vol. 12, pp. 138-164.

Shrestha, A. and Mahmood, A. (2019), "Review of deep learning algorithms and architectures", *IEEE Access*, Vol. 7, pp. 53040-53065.

Shrestha, R., Bajracharya, R., Shrestha, A.P. and Nam, S.Y. (2020), "A new type of blockchain for secure message exchange in Vanet", *Digital Communications and Networks*.

Sohal, A.S., Sandhu, R., Sood, S.K. and Chang, V. (2018), "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments", *Computers and Security*, Vol. 74, pp. 340-354.

Song, H.M., Kim, H.R. and Kim, H.K. (2016), "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network", *International Conference on Information Networking (ICOIN)*, IEEE, pp. 63-68.

Song, H.M., Woo, J. and Kim, H.K. (2020), "In-vehicle network intrusion detection using deep convolutional neural network", *Vehicular Communications*, Vol. 21, p. 100198.

Spitzner, L. (2003), "Honeypots: tracking hackers", *IEEE Network*, IEEE, Vol. 17, pp. 5-5.

Standard, I. (2003), *Road Vehicles–Controller Area Network (CAN)–part 1: Data Link Layer and Physical Signalling*, ISO, Vol. 11898, p. 1.

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M. and Laarouchi, Y. (2013), "Survey on security threats and protection mechanisms in embedded automotive networks", *43rd Annual*

IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), IEEE, pp. 1-12.

Studnia, I., Alata, E., Nicomette, V., Kaâniche, M. and Laarouchi, Y. (2018), "A language-based intrusion detection approach for automotive embedded networks", *International Journal of Embedded Systems*, Vol. 10 No. 1, pp. 1-12.

Sun, G., Yu, M., Liao, D. and Chang, V. (2018), "Analytical exploration of energy savings for parked vehicles to enhance vanet connectivity", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 20 No. 5, pp. 1749-1761.

Sun, G., Cai, S., Yu, H., Maharjan, S., Chang, V., Du, X. and Guizani, M. (2019), "Location privacy preservation for mobile users in location-based services", *IEEE Access*, Vol. 7, pp. 87425-87438.

Takada, M., Osada, Y. and Morii, M. (2019), "Counter attack against the bus-off attack on can", *14th Asia Joint Conference on Information Security (AsiaJCIS)*, IEEE, pp. 96-102.

Taylor, A., Leblanc, S. and Japkowicz, N. (2016), "Anomaly detection in automobile control network data with long short-term memory networks", *3rd IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, IEEE, pp. 130-139.

Verendel, V., Nilsson, D.K., Larson, U.E. and Jonsson, E. (2008), "An approach to using honeypots in in-vehicle networks", *IEEE 68th Vehicular Technology Conference (VTC)*, IEEE, pp. 1-5.

Wang, J.J. (2012), "Antennas for global navigation satellite system (GNSS)", *Proceedings of Te IEEE*, Vol. 100 No. 7, pp. 2349-2355.

Wang, L. and Liu, X. (2018), "Notsa: novel obu with three-level security architecture for internet of vehicles", *IEEE Internet of Things Journal*, Vol. 5 No. 5, pp. 3548-3558.

Wang, Q. and Sawhney, S. (2014), "Vecure: a practical security framework to protect the can bus of vehicles", *4th International Conference on the Internet of Things (IOT)*, IEEE, pp. 13-18.

Wasicek, A., Derler, P. and Lee, E.A. (2014), "Aspect-oriented modeling of attacks in automotive cyber-physical systems", *51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, IEEE, pp. 1-6.

Woo, S., Jo, H.J. and Lee, D.H. (2014), "A practical wireless attack on the connected car and security protocol for in-vehicle can", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16 No. 2, pp. 993-1006.

Woo, S., Moon, D., Youn, T.-Y., Lee, Y. and Kim, Y. (2019), "Can id shuffling technique (CIST): moving target defense strategy for protecting in-vehicle can", *IEEE Access*, Vol. 7, pp. 15521-15536.

Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J. and Li, K. (2019), "A survey of intrusion detection for in-vehicle networks", *IEEE Transactions on Intelligent Transportation Systems*.

Yang, X. (2011), "Bat algorithm for multi-objective optimisation", *International Journal of Bio-Inspired Computation*, Vol. 3 No. 5, pp. 267-274.

Ye, H., Liang, L., Li, G.Y., Kim, J., Lu, L. and Wu, M. (2018), "Machine learning for vehicular networks: recent advances and application examples", *IEEE Vehicular Technology Magazine*, Vol. 13 No. 2, pp. 94-101.

Ying, X., Bernieri, G., Conti, M. and Poovendran, R. (2019), "Tacan: transmitter authentication through covert channels in controller area networks", *10th ACM/IEEE International Conference on Cyber-Physical Systems*, pp. 23-34.

Young, C., Zambreno, J., Olufowobi, H. and Bloom, G. (2019), "Survey of automotive controller area network intrusion detection systems", *IEEE Design and Test*, Vol. 36 No. 6, pp. 48-55.

Zeng, W., Khalid, M.A. and Chowdhury, S. (2016), "In-vehicle networks outlook: achievements and challenges", *IEEE Communications Surveys and Tutorials*, Vol. 18 No. 3, pp. 1552-1571.

Zhang, L., Shi, L., Kaja, N. and Ma, D. (2018), "A two-stage deep learning approach for can intrusion detection", *The Ground Vehicle Systems Engineering and Technology Symposium (GVSETS)*, pp. 1-11.

Zheng, B., Lin, C.-W., Yu, H., Liang, H. and Zhu, Q. (2016), "Convince: a cross-layer modeling, exploration and validation framework for next-generation connected vehicles", *35th IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, IEEE, pp. 1-8.

Corresponding author
Faten Fakhfakh can be contacted at: faten.fakhfakh@redcad.org