Digital Communications and Networks xxx (xxxx) xxx

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Attacks and defences on intelligent connected vehicles: a survey

Mahdi Dibaei [a], Xi Zheng [a,*], Kun Jiang [b], Robert Abbas [c], Shigang Liu [d], Yuexin Zhang [d], Yang Xiang [d], Shui Yu [e]

[a] Department of Computing, Macquarie University, Sydney, NSW, Australia
[b] China State Key Lab of Automotive Safety and Energy, Tsinghua University, Beijing, China
[c] School of Engineering, Macquarie University, Sydney, NSW, Australia
[d] School of Software and Electrical Engineering, Swinburne University of Technology, Hawthorn, VIC, Australia
[e] School of Software, University of Technology Sydney, Australia

ARTICLE INFO

Keywords:
Intelligent vehicles
Vehicular networks
Software vulnerabilities
Deep learning
3GPP
Software defined security

ABSTRACT

Intelligent vehicles are advancing at a fast speed with the improvement of automation and connectivity, which opens up new possibilities for different cyber-attacks, including in-vehicle attacks (e.g., hijacking attacks) and vehicle-to-everything communicationattacks (e.g., data theft). These problems are becoming increasingly serious with the development of 4G LTE and 5G communication technologies. Although many efforts are made to improve the resilience to cyber attacks, there are still many unsolved challenges. This paper first identifies some major security attacks on intelligent connected vehicles. Then, we investigate and summarize the available defences against these attacks and classify them into four categories: cryptography, network security, software vulnerability detection, and malware detection. Remaining challenges and future directions for preventing attacks on intelligent vehicle systems have been discussed as well.

1. Introduction

The past decade has seen a rapid development of vehicular systems in various aspects. The complexity of current vehicular systems, with a dramatic increase in the use of electronic systems and wireless technologies, has changed the traditional concept of security in the automotive industry. Moreover, the growing interest in the development of vehicular networks and Intelligent Transportation Systems (ITS) has introduced new security challenges and vulnerabilities. Meanwhile, long-established computer security policies are not followed by the industry standards for in-vehicle and vehicular communications because of hardware constraints and differences in network configuration [1,2].

Previous reports have illustrated highly practical wireless attacks on core functions of vehicles, which can disengage engines and brakes [3–6]. For instance, by hijacking the steering and braking units in a Ford Escape and a Toyota Prius, Miller and Valasek [3] found that while a vehicle system is getting more advanced with appealing features, the system is also becoming a vulnerable target for attacks. In 2015, 1.4 million vehicles were subjects of a recall by Chrysler because hackers could remotely take control of a jeep's digital system over the Internet [4]. In another report, a team of hackers remotely hijacked a Tesla Model S from a distance of 12 miles [5]. In a recent study, researchers have found 14 vulnerabilities in the infotainment system in several Bavarian Motor Works (BMW) series [6]. Overall, these incidents proved that security in intelligent vehicular systems has become essential and must be treated with high priority.

At present, successful cybersecurity attacks on vehicles are mainly caused by information sharing and wireless communications. Consequently, information privacy, data privacy, securing data exchange, including input and output data as well as protecting Electronic Control Units (ECUs) inside the vehicle systems, are among the most significant security and privacy issues for intelligent vehicles [7].

In this paper, we encompass security with attacks, defences, and vulnerabilities. With this as the scope, we sorted out the most significant recent work related to our study and that these works are limited in attacks or vulnerabilities, but they do not focus too much on defence mechanisms. For instance, Mokhtar and Azab [8], Sakiz and Sen [9], and Hasrouny et al. [10]. have focused on security attacks on Vehicular Ad hoc NETworks (VANETs). In these papers, however, security defence mechanisms have not been classified explicitly. Moreover, although these studies have performed some

* Corresponding author.
E-mail addresses: dibyimahdi@yahoo.com (M. Dibaei), james.zheng@mq.edu.au (X. Zheng), jiangkun@tsinghua.edu.cn (K. Jiang), robert.abbas@mq.edu.au (R. Abbas), shigangliu@swin.edu.au (S. Liu), yuexinzhang@swin.edu.au (Y. Zhang), yxiang@swin.edu.au (Y. Xiang), Shui.Yu@uts.edu.au (S. Yu).

https://doi.org/10.1016/j.dcan.2020.04.007
Received 13 July 2019; Received in revised form 21 December 2019; Accepted 19 April 2020
Available online xxxx

good exploratory work on the network vulnerabilities in vehicular systems, they have largely missed the in-vehicle vulnerabilities (e.g., vulnerabilities of ECUs and software vulnerabilities). A survey by Bernardini et al. [11] covers security vulnerabilities in internal vehicle communications, including the ECU, and in gateways, including the On-Board Diagnostics (OBD), Tire Pressure Monitoring System (TPMS), electrical charging system, Remote Keyless System (RKS), and infotainment system. However, not too many details are covered for defence mechanisms.

In comparison, based on the detailed walk-through of the architecture of intelligent vehicle systems, we present an in-depth analysis of security attacks, challenges, and defence mechanisms in this kind of intelligent vehicle system.

The critical structures of the paper are illustrated in Fig. 1, which taxonomizes the security of intelligent vehicles according to the following attributes: (i) Intelligent vehicle system architecture: we give an overview of the electronic/electrical architecture of intelligent vehicle systems as well as the in-vehicle and inter-vehicle communication networks, the computation platform, and new sensors in intelligent vehicles. (ii) Security requirements and identified attacks: we discuss security requirements for vehicular systems in four categories (authentication, integrity, privacy, and availability) and present a classification of attacks on vehicles and vehicular networks. (iii) Defences against the attacks: we refer to a list of existing defence techniques, including cryptography, signature-based detection, anomaly-based detection, software vulnerability detection, and malware detection, which can be used to deal with security challenges in automotive systems. (iv) Future directions: we show the possible areas (e.g., lightweight authentication, software-defined security, deep learning) for further studies. Explicitly, this paper aims to answer four research questions:

- What are the state-of-the-art vehicle systems?
- What are the unique research challenges in securing vehicle systems?
- What are the main defences and their pros and cons?
- And what are promising solutions to improve security?

And this paper makes the following contributions:

- We provide a detailed description of system architecture for intelligent vehicles, which covers structure design, communication networks, computation platforms, and new sensors used.
- We raise the security requirements and identify possible security attacks to intelligent connected vehicles.
- Based on a detailed analysis of existing defence mechanisms against intelligent vehicle system attacks, we propose some promising research directions.

The remainder of this paper is divided into four sections: Section 2 gives an overall review of the state-of-the-art architectures of intelligent

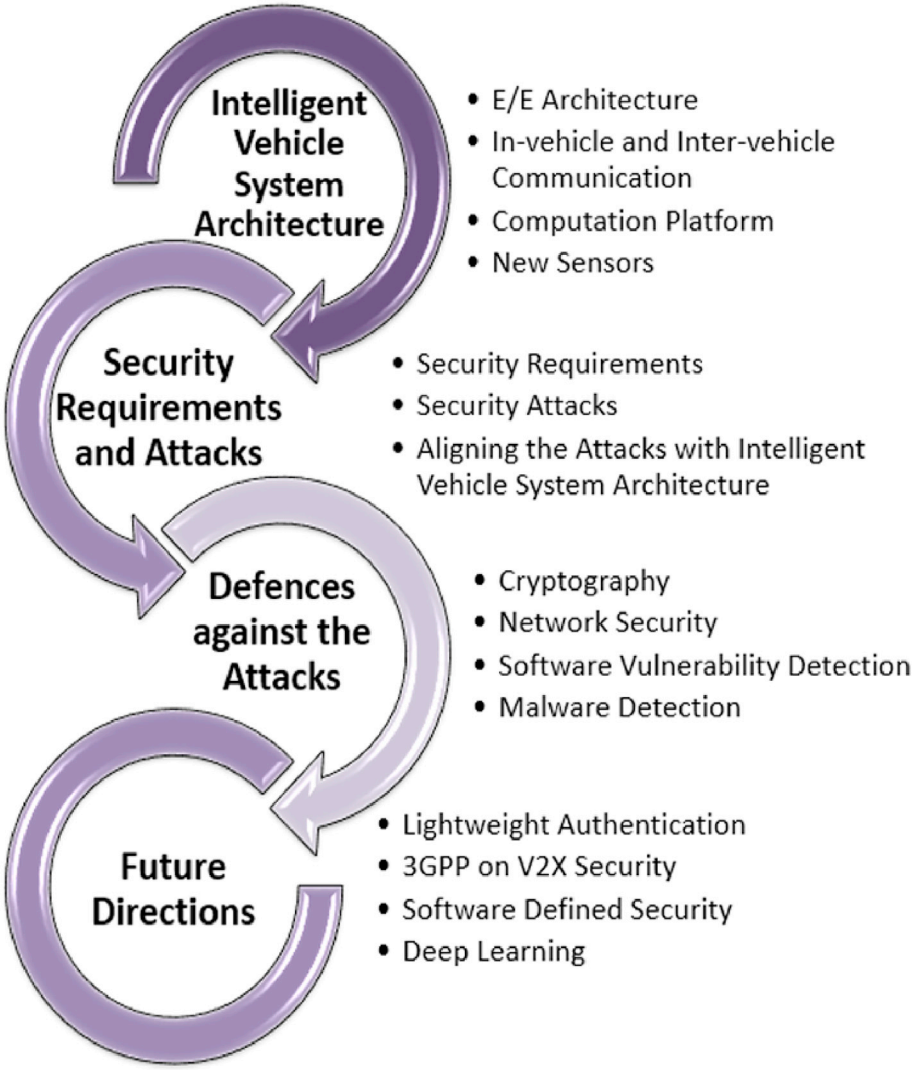

Fig. 1. Key structures of our technical contribution.

vehicle systems. Section 3 discusses the current security attacks and challenges faced by intelligent vehicle systems In Section 4, we highlight the best practices for dealing with these security challenges in intelligent vehicle systems. Section 5 discusses some promising future directions to address those security challenges in intelligent vehicle systems. Limitations and threats to the validity of this study are discussed in Section 6. Finally, Section 7 concludes this paper.

2. Intelligent vehicle system architecture

Intelligent Connected Vehicles (ICVs) are now an active research topic in the automotive industry. Many intelligent driving functionalities have been installed on passenger cars, such as Lane Keeping Assistance (LKA), Lane Departure Warning (LDW), and other assistance systems. Surely, a high-level intelligent vehicle should be able to accomplish all these functionalities. However, it is not feasible to integrate all these intelligent assistance systems by puttting them together, as the traditional Electrical/Electronic Architecture (EEA) was not designed to support so many intelligent functionalities. Notably, the required abilities of data acquisition and processing are beyond the limit of the traditional EEA. The next-generation EEA, which can support high-level ICVs, is the key to the ICV's series production. The next-generation EEA needs fundamental advancement in three parts: the overall structure design, the in-vehicle and inter-vehicle communication network, and the computation platform.

2.1. The overall EEA of intelligent vehicle

The topology design of the overall architecture is fundamental to improve the performance of EEA. The main task of the topology design is to ensure the data flow on the network matches the need of each node. As shown in Fig. 2, the traditional EEA topology is based on the Controller Area Network (CAN). Due to the characteristics of the CAN, every node in the network must share the bandwidth with each other. The bandwidth is like a bottleneck that limits the data processing ability of each ECU on the network. The core problem of the traditional EEA is the lack of space for a high computation power unit, which is necessary for intelligent driving. The topology of next-generation EEA should specify where the complex computation is realized and how the huge amount of data is transferred.

One feasible approach is the domain-based topology, which has been recently applied in the production of vehicles. Its concept is to divide the autonomous driving system into several domains. Its main difference with the traditional EEA is the occurrence of domain ECU, which is the core computation platform of each domain. The vehicle components can be classified into different domains according to their functionalities. Usually, the sensors and actuators that can be shared by different functionalities would be grouped as one domain. For example, the commonly used domains are the infotainment domain, the chassis domain, and the safety domain. The domain-based EEA is illustrated by Fig. 3. The domain-based topology has advantages over the traditional one. First of all, it can support more complex intelligent driving functions, as each domain ECU has more power in both communication and computation. The domain ECU can be directly connected to sensors in the domain without the problem of sharing the bandwidth. It is also a computation platform to integrate related simple control functions into a complex behavior control function [12]. Furthermore, the distributed computation strategy of the domain-based topology has the advantage of being more compatible with the traditional EEA system. The domains can be relatively independent from each other, only transmitting necessary information to other domains. The data flow within the domain will not occupy the bandwidth and other resources of the backbone.

The centralized architecture is another approach for the EEA of next-generation vehicles. In a centralized architecture, most of the computation tasks are executed in the central computation entity, as illustrated in Fig. 4, rather than distributed in different functional domains. Most of the components should be connected to the central computation entity, which could access all sensors and actuators. The benefit of a centralized topology is the ability to realize complete sensor fusion. In theory, when the central computation entity could combine more information, it has the potentials to make a better decision. However, a centralized topology has higher demands on the data communication capabilities. The centralized EEA needs to group the components into different sub-networks according to their physical placement or network properties to improve communication efficiency. The controller of the sub-network is called a zone controller in Ref. [13].

2.2. The in-vehicle and inter-vehicle communication network of intelligent vehicles

As mentioned above, one of the most significant challenges for the next-generation EEA is managing the high-speed communication among a vehicle's electronic components with a limited cost. The most successful communication network in the current automotive industry is the CAN protocol. The CAN protocol is developed by Bosch corporation, and it has been the most widely used standard in the field of vehicle hardware communication since its publication in 1986 [14]. Compared with other network technologies, the CAN has outstanding advantages in cost-efficiency and flexibility. A variant of the CAN is one with the Flexible Data rate (CAN-FD) [15,16] with a bandwidth of up to 8 Mb/s [17]. The CAN is a multi-master network in which every node could equally and independently receive and broadcast information. With this characteristic, the CAN is almost a plug-and-play system: new ECUs or

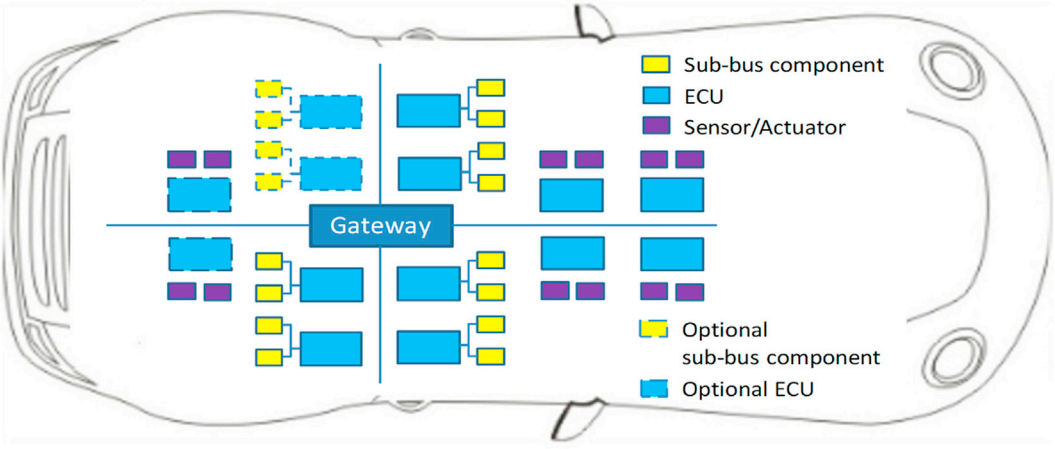

Fig. 2. Gateway-based E/E architecture.

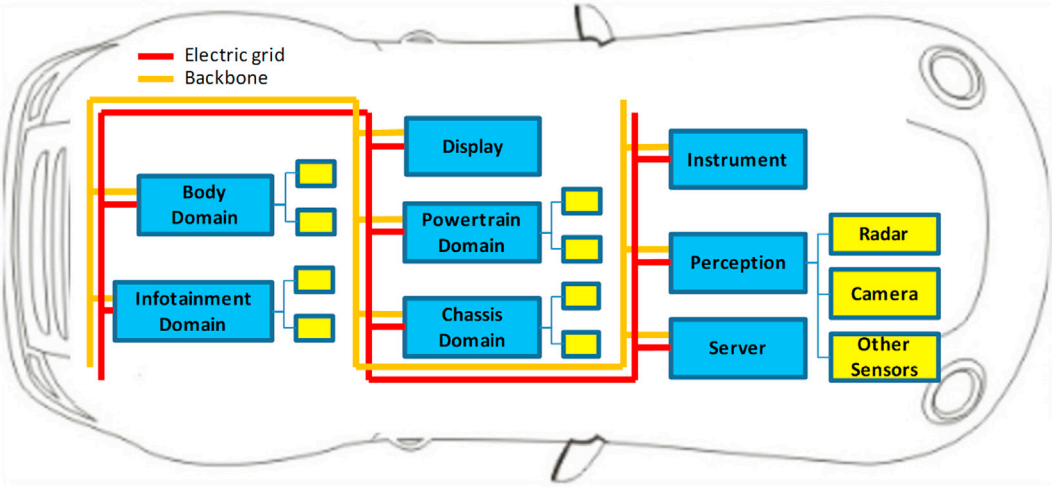

Fig. 3. Domain-based E/E architecture.

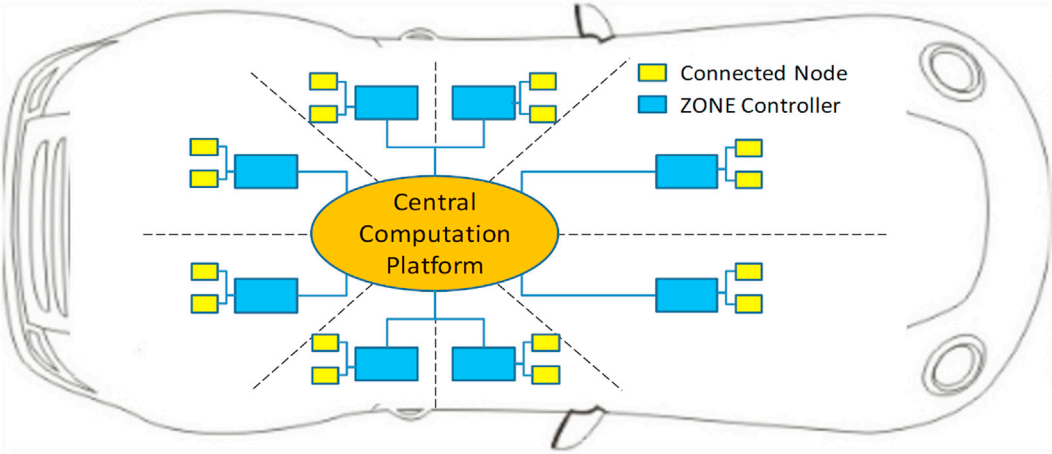

Fig. 4. Centralized E/E architecture.

diagnostic tools can be easily connected to the network without special modification of the network. Nevertheless, it also makes the communication system vulnerable to attacks.

In many subsystems of vehicles, different kinds of specialized communication networks are developed for specific automotive applications. Each of these networks has its own advantages. They will probably exist in vehicles for a long time. However, they are unlikely to be employed as the backbone communication network in the EEA of the next generation. A LIN (Local Interconnect Network) permits a low-cost and flexible wire harness and can be easily implemented without special support requirements. However, the bandwidth capacity of the LIN is only 20 kb/s. It is usually used in the switches and motors that roll windows and control seats. The FlexRay protocol was designed to support the use of full electric/electronic systems for performing the vehicle's safety-critical functions, including "brake-by-wire", "suspension-by-wire", "steer-by-wire", and in general "x-by wire" [18]. FlexRay can ensure real-time communication between safety-critical components with little time delay with a built-in mechanism of time synchronization. Media Oriented Serial Transport (MOST) is another in-vehicle network. MOST was developed to support infotainment devices and related applications in vehicles [19–21]. It employs plastic optical fibers as its physical layer, so the network is isolated from EMI (Electro-Magnetic Interference), preventing problems like buzzing sounds in the infotainment system.

A promising candidate for the backbone communication network is the Automotive Ethernet (AE) [22–24]. Though the Ethernet is not a new idea for data communication, it still needs a considerable amount of modification and research to be utilized by vehicles. It was until 2013 that the first application of AE appeared in producing vehicles when the BMW X5 used AE for connecting onboard cameras. A comparison between the AE and other networks is shown in Table 1. The main advantages of the AE are as follows: (1) Larger bandwidth. Currently, the bandwidth capacity of the AE protocol is 100 Mbps; and in the near future, it will be increased to 1 Gbps. (2) Improved security. The Ethernet employs an IP-based routing method, thus it prevents one compromised ECU from performing malicious attacks on the whole communication system. Moreover, the switches in the Ethernet can manage the information flow in the network, and avoid hi-jacked ECUs flooding overload data into the network.

The emergence of various wireless communication technologies enables the development of cooperative communication, in particular, the breakthrough of 4G Long Term Evolution(LTE) and 5G remote communication technologies, and the development of Dedicated Short-Range Communication(DSRC)-supported Vehicle-to-Everything (V2E) communications. The next important step is accident-free driving based on inter-vehicle communications and cooperative ITS [26]. Cooperative perception-based V2E provides an exciting opportunity for developing more reliable target recognition and tracking in the Field of View (FoV)

Table 1
Specifications of common vehicle buses [25].

	AE	CAN	FlexRay	MOST	LIN
Bandwidth (Mb/s)	1000 (developing)	1 or 10 (CANFD)	20	150	0.02
Maximum Number of Nodes	Number of switch ports	30	22	64	16
Messaging	IP based	Multi-master	Multi-master	Cyclic frames/ streams	Master-slave
Cost	High	Low	Low	High	Very Low
Availability	Growing	Many	Few	One	Many
Cabling	UTP	UTP	UTP	Optical, UTP	1-wire
Applications	Infotain-ment, Back-Bone (future)	General bus	Safety -critical, x-by-wire	Infotain -ment	Switches, doors

[27]. Furthermore, it can also provide an accurate perception of occluded objects [28–30] or objects outside the FoV by multimodal sensor data fusion [25,31,32].

2.3. The computation platform for intelligent vehicle

Traditionally, simple controllers such as MicroController Units (MCUs) and Digital Signal Processors (DSPs) were well established in vehicles for data processing of various functions, including taillights on and off [33], air-conditioning [34], powertrain [35], etc. Meanwhile, DSPs can execute more complicated applications, like onboard multimedia systems [36] and driver assistance functions [37,38], which require high integration and excellent processing capacity.

In high-level ICVs, more than hundreds of millions of lines of codes are expected to be executed by the processors to realize intelligent algorithms, including sensor fusion and deep learning. Therefore, a powerful computation platform with better hardware and software design is urgently needed. Both Graphics Processing Units (GPUs) and Field-Programmable Gate Arrays (FPGAs) are believed to have wide applications in the automotive industry in the near future. A GPU is specialized in massively parallel computation, and thus it is very good at image processing [39], which makes it ideal in self-driving vehicles for complex computational systems, such as obstacle detection systems and collision avoidance systems. Another option is FPGAs that are suitable for parallel computing and have less energy consumption.

The software system is another indispensable task of a computation platform. The software used in the automotive industry has its own requirements. Open Systems and their interfaces for the Electronics in Motor Vehicles/Vehicle Distributed eXecutive (OSEK/VDX) is a joint project that is developed by the European automotive industry. The aim of this project is to develop a real-time operating system for automotive applications [40]. Another important project is JASPAR (Japan Automotive Software Platform and Architecture) established in 2004 by Japan, and well-known corporations, including Toyota, Nissan, and Honda, are among its member companies. It should be mentioned that one major drawback of OSEK/VDX and JASPAR is that they fail to take the reusability and transferability demanded by the modern automotive electronics industry into account. The AUTomotive Open System ARchitecture(AUTOSAR) standard is developed to separate the application software from the associated hardware, and thus save development costs [41]. However, AUTOSAR still needs further development to support complicated perception algorithms and Artificial Intelligence (AI) applications.

Although general operating systems such as Linux and Android support highly complex algorithms, the major problem is that they cannot be used as automotive embedded software. It is necessary to develop a software platform that combines the advantages of both the automotive software system and the general operating system [42]. Currently, AUTOSAR as a global partnership for developing automotive software is standardizing the AUTOSAR adaptive platform. In particular, providing a stable programming interface as well as supporting the Ethernet-based EEA are the two major objectives of this software platform [43]. In software development, software update and security are two primary concerns. For an autonomous driving vehicle, it is necessary to update its software even after it has been sold, just like a smartphone. Over-the-air updates can bring lots of convenience and benefits to both consumers and manufacturers. The security during updates is quite important and is becoming a hot research topic [44].

2.4. New sensors in intelligent vehicles

To achieve full observations of both the vehicle's own state, the surroundings and even the situation beyond the visual range, the intelligent vehicle needs to be equipped with many new sensors. By comparing the sensors used in autonomous driving competitions [45–49] as shown in Fig. 5, we can see the current trends in perception technology. The fusion of multi-sensors is widely accepted as an essential method to ensure perception robustness. The sensor fusion for the high-level ICV mainly refers to the following sensors: LiDaR, radar, and intelligent cameras.

- **LiDaR:** LiDaR, which stands for Light Detection and Ranging, enables self-driving cars to observe the world. In fact, it is achieved by utilizing laser light pulses. High-definition LiDaR provides a 360-degree field of view with more than 16 laser channels. Regarding rotation mechanisms, LiDaR may be classified into three main categories: mechanical LiDaR, semisolid-state LiDaR, and solid-state LiDaR.
- **Radar:** Millimeter-wave radar is capable of penetrating non-transparent materials, such as smoke, dust, snow, and fog. In other words, the main advantage of millimeter-wave radar is its capability to handle small size, all-weather, and long detection distance. However, low horizontal resolution and low lateral detection accuracy are the most significant limitations of millimeter-wave radars [50,51]. Due to these shortcomings, millimeter wave radar needs to be fused with other sensors to improve the accuracy of the target perception system. One solution is the fusion of millimeter-wave radar and monocular camera [52–54].
- **Intelligent visual sensors:** The monocular visual system and the stereo vision system are the main intelligent visual sensors in intelligent vehicles. They are utilized in order to achieve semantic segmentation of the driving environment [50], target detection and tracking [55], ranging [56,57], driver distraction and fatigue detection [58], and so on [59,60]. AI technologies, such as deep learning, are deeply integrated into the visual sensors to provide more accurate detection results. However, visual sensors are unstable in changing light conditions. What is worse, the AI algorithm may be attacked, leading to a false detection result.

3. Security requirements and identified attacks

In recent years, we have seen an increasing amount of research related to vehicular networks, and fully automated vehicles are fast becoming a reality. They have a tremendous potential to increase efficiency and safety for their occupants, and they have already been implemented in trials in a number of locations around the United States and throughout Europe [61,62]. Understandably, as with any new technology, there is a certain amount of hesitation regarding self-driving vehicles. And this has been further enhanced by recent incidents in California and Arizona in the United States [63,64], where the self-driving vehicles have been involved in incidents with pedestrians. This has prompted a number of companies like Uber to slow down or suspend the deployment of self-driving vehicles [65], in an attempt to optimize the operation and restore public confidence. In addition to

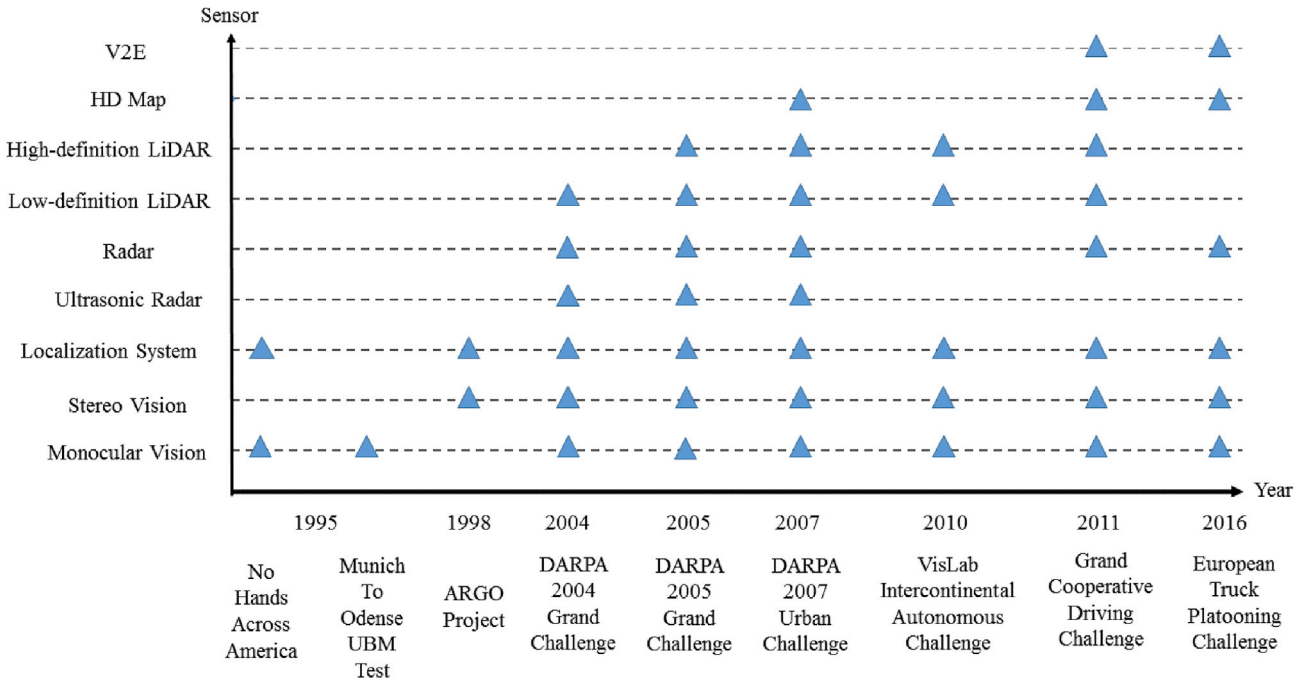

Fig. 5. Mainstream sensors used in autonomous driving competitions and projects.

unpredictable accidents, in-vehicle and inter-vehicle networks are susceptible to a number of malicious attacks and intrusions, where users are going to cause damage intentionally to the vehicles or their occupants.

In 2016, a group of Chinese security researchers from Keen Security Lab discovered a method to hack a Tesla CAN bus, which can be found in almost all intelligent cars and controls indicators and brakes [66]. They were able to remotely access the central control unit and adjust the mirrors, lock the doors, manipulate the dashboard, and even apply the brakes. This was reported to Tesla who quickly provided an update for its vehicles. However, this event clearly revealed that there was a real issue with the outdated software being used. Recently, another team from Keen Security Lab discovered 14 vulnerabilities in BMW cars [67]. They discovered that they were able to use a backdoor to gain access to the telematics control unit as well as the CAN bus. Similar to Tesla, BMW's response was to roll out upgrades for the affected models. These were made available over an air connection or for customers at the BMW dealerships. Similarly, researchers in the Netherlands discovered a method to get around the Radio Frequency IDentification (RFID)-based key immobilizers [68], which have been used as a primary security feature by many automotive manufacturers since 1996. The authors in Ref. [68] used a method that bypasses the cryptographic authentication, while it can be conducted in less than 6 min with no specialized hardware. The next section discusses some system-level security requirements for vehicular networks. The subsequent section details the various types of attacks to which intelligent vehicles are vulnerable.

3.1. Security requirements

Successful, safe and secure implementation of intelligent vehicular systems is dependent on designing and developing an extensive security framework. Therefore, vehicular systems must abide by strict security requirements. Identification of appropriate security requirements in the early stages of conceptual design and development plays a key role in ensuring that vehicles and occupants will remain safe and secure at all times. Throughout the literature, authentication, integrity, privacy, and availability among the most significant prerequisites need to be provided by a security system [69]. In this section, we discuss these four categories as key requirements for successful and secure integration of vehicular systems. Studying security requirements will provide deep knowledge of security attacks, security vulnerabilities, and security defences.

3.1.1. Authentication

Authentication in vehicular systems is an important attribute that needs to be considered carefully in the early stages of system design and implementation. It means that authorized users can only access data/information. In essence, only the intended parties should be able to have access to the message and retrieve its original contents. In order to meet the authentication requirements, key management and distribution must be efficient and accurate.

3.1.2. Integrity

In vehicular networks, it is essential to be able to validate that the message has not been corrupted during transmission by degradation factors such as noise and fading, as well as deliberately corrupted by an attacker.

3.1.3. Privacy

In the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) modes of communication, where vehicles employ different techniques for sharing information (e.g., information about their geographical locations) and creating a cooperation-oriented environment among vehicles and RSUs, the shared information can be used maliciously to track users [70]. Hence, privacy is another significant challenge in intelligent vehicle systems, and sensitive information must be protected by intelligent cars [11].

3.1.4. Availability

In vehicular communications, improving the chance of getting information by all targeted vehicles is of great importance. Vehicular networks are highly dynamic, and the network must be able to respond in real-time.

3.2. Security attacks

In addition to the requirements described above, in order for vehicular networks to be securely and successfully deployed, they must defend

against cyber threats. Threats to security must be mitigated whenever possible; in other words, a proactive approach to threats should be a key requirement that must be met. However, since it is impossible to predict all possible threats to the network, reactive approaches must be effective and deployed quickly and efficiently. It is important that users experience as little disruption as possible as a result of an attack. The following sections present a classification of attacks that affect vehicles. We will focus on the strategies of these attacks and also general mitigation techniques to give a comparative analysis in Table 2.

3.2.1. Denial-of-Service (DoS) attacks

DoS attacks involve flooding a host with an enormous amount of information in an attempt to overload it, effectively preventing it from receiving or processing information coming in from legitimate users. In vehicular networks, the primary target for attackers would be the Road-Side Unit (RSU). RSUs are a core component in vehicular networks as they authenticate, manage and update vehicles and their information. The simplest method to combat DoS attacks is to block the attacker's IP address. In traditional DoS attacks, a single attacker attacks a node or a channel using a single IP address, usually from a single vehicle. This often places a huge burden on the attacker's resources. As a result, attackers often use multiple IP addresses in distributed attacks, reducing the resource burden. Distributed DoS attacks are even harder to mitigate and combat because the incoming messages can come from a large number of vehicles. Therefore, it becomes useless to simply block a single IP address. Similar to the DoS attack, distributed DoS attacks can be performed on both RSUs and other vehicles on the network.

3.2.2. Black-hole attacks

In a black-hole attack on the vehicular network, an attacker drops packets instead of forwarding them to their destination, creating a hole where no packets can move through the network to other vehicles. A variant of the black-hole attack is called the grey-hole attack. In a grey-hole attack, the attacker only drops a percentage of packets. Attackers do this in order to avoid detection. One solution to the black-hole attack is adding sequence numbers to the packets.

3.2.3. Replay attacks

Replay attacks are a variant of the man-in-the-middle attacks in which a valid transmission data is repeated or delayed. In vehicular networks, replay attacks often target communications between the vehicle and the RSU. If an attacker intercepts a message between an RSU and a vehicle containing the encryption key or password, it would be able to authenticate itself later. Man-in-the-middle and replay attacks are difficult to mitigate effectively, as it is almost impossible for a vehicle or an RSU to know when it is under attack. In most cases, attackers are highly mobile and do not alter the packets in any way. Mitigation methods include the implementation of a strong encryption method, using virtual private networks, and using time-delay variation [71].

Table 2
Comparison of security attacks in vehicular networks.

Attacks	Strategy	General mitigation techniques
DoS	Flooding	Blocking IP
Black-Hole	Dropping	Adding sequence number to packets
Replay	Repeating/Delaying	Cryptography
Sybil	Operating multiple identities actively at the same time	Cryptography
Impersonation	Sending message on behalf of other nodes	Cryptography
Malware	Infection	Firewall, Reputation-based schemes
Falsified-Information	Spreading false information	Reputation-based schemes
Timing	Adding time slots to create delay	Fixed data rate

3.2.4. Sybil attacks

Sybil attacks, or pseudospoofing attacks as they are sometimes known, involve a user creating a large number of pseudonymous identities [72,73] to have a greater influence on the network. Sybil attacks can be used in vehicular networks to route traffic in a certain direction, for example, when an attacker creates a large number of pseudonymous identities at certain locations. The increase in the number of users at a certain location indicates that there is severe congestion at that location which would force other vehicles to change their own routing to avoid the congested areas. In vehicular networks, when Sybil attacks are performed with the assistance of Global Positioning System (GPS) spoofing attacks (where an attacker attempts to appear at a location where they are not), it would allow the attackers to ensure that they have a congestion-free route. A congestion-free route would be created because all other vehicles would attempt to route around problem areas. The most effective mitigation methods are identification and authentication based methods using cryptography.

3.2.5. Impersonation attacks

In vehicular networks, malicious nodes would impersonate RSUs in an attempt to trick users into divulging their authentication details. After the authentication information has been acquired, it can be used to access classified information or even as authentication with other parties. Attackers could also impersonate other vehicles to gain an advantage. For example, an attacker might choose to impersonate an emergency vehicle, which would give them a higher priority within the network and lead to less congestion. Methods based on encryption, localization, and clustering can be used to mitigate the effects of impersonation attacks.

3.2.6. Malware

Since vehicular networks are highly dynamic and will be changed and updated frequently, vehicles must ensure that updates and information that they receive come from a trusted source. If they don't, they become infected, risking losing personal information and, in some cases, having critical malfunctions. The easiest way to reduce malware attacks is to introduce a firewall that filters malicious messages from legitimate ones. However, additional methods are sometimes needed, as attacks have been known to find methods around firewalls [74]. In addition to firewall protection, reputation-based schemes are often introduced to ensure that only messages from trusted parties are accepted.

3.2.7. Falsified-information attack

Attackers can spread falsified information about the congestion on roads to effectively force other drivers to diverge to alternate routes. They can also create congestion by neglecting to report congestion or accidents on the road. This form of attack is often combated by using reputation-based schemes that reward drivers that send out legitimate information and punish drivers that send out falsified information.

3.2.8. Timing attacks

Time synchronization is a key aspect of intelligent connected vehicles. Vehicles move in and out of networks very rapidly, which introduces the need for real-time updates and information exchange between both RSUs and vehicles. Since time-critical message exchange in safety and warning applications is critical, any delay in messages can cause serious problems. Timing attacks are similar in many ways to black and grey hole attacks. However, instead of dropping all or part of the packets, a malicious node adds a time slot to introduce an intentional delay. This causes major problems, especially in autonomous vehicles where a delay in time-sensitive information can lead a major accident. One proposed solution for timing attacks in vehicular networks is to force all vehicles to send and receive packages at fixed data rates [75].

Table 2 lists security attacks and demonstrates their strategies and general mitigation techniques.

3.3. Aligning attacks with intelligent vehicle system architecture

This part of the paper aligns the above-mentioned attacks with different components of the intelligent vehicle system architecture identified in Section 2. Table 3 lists security attacks on different components in intelligent vehicles, including the overall EEA, communication network, computation platform, and new sensors. An intelligent vehicle with its components is shown in Fig. 6. Below, we demonstrate the identified attacks on these components.

- **Overall EEA:** As mentioned earlier, the in-vehicle networks (CAN, LIN, FlexRay, and MOST) are vulnerable to different cybersecurity attacks. Through an On-Board Diagnostics (OBD) port or a USB port, attackers can stop the engine or brakes of a vehicle and cause a fatal car crash [76]. Replay attacks and impersonation attacks on CAN buses are reported in Ref. [77]. Nilsson et al. [78] simulated a spoofing (Sybil) attack on the FlexRay bus by creating and injecting diagnostic messages. Another instance is the EEA of the Electrical Vehicle (EV). In recent years, the use of EVs that can be recharged from an external source of electricity has dramatically increased. The architecture of EV charging-station systems makes it possible for information exchange between EVs and Electric Vehicle Supply Equipment (EVSV) that may be used for payment systems for public charging stations. Consequently, EVs are subject to cybersecurity attacks by the charging-plug interface. The International Electrotechnical Commission (IEC) has defined the communication protocol between a charging station and an EV by the IEC 61851 and International Standardization Organization (ISO) 15118 standards [79].
- **Communication network:** DSRC, LTE, Wi-Fi, and Worldwide Interoperability for Microwave Access (WiMAX) are among the available communication standards and technologies for V2V and V2I data communications. V2E or inter-vehicle communications are wireless, and security is considered one of the most significant challenges of V2E technology [80]. Moreover, audio and video players, automotive navigation systems, USB and Bluetooth connectivity, Carputers, audio control, hands-free voice control, and general infotainment systems have increased security concerns about potential remote car hacking. In reviewing the literature, Sybil attack [81], black-hole attack [82], Dos attack, DDoS attack, replay attack, and timing attack [83] on the communication network of intelligent vehicle systems are found. In addition, V2V communications are susceptible to malware attacks [84].
- **Computational platform:** Malware can infiltrate software systems of intelligent vehicles. Additionally, DoS attacks can be launched to destroy the processing ability of a vehicle [85].
- **New sensors:** The TPMS is a warning system for measuring the air pressure of tires by pressure sensors or monitoring individual wheel rotational speeds and warning the driver when tires are underinflated. A TPMS notifies the driver when a vehicle's tire pressure is low. Under those circumstances, a security issue related to the TPMS is that a vehicle may be tracked using existing sensors along the roadways [85]. Another instance is RKS or smart key that is most widely used as an electronic authorization system in order to control access to the vehicle. Sensors in the vehicle are able to sense the received signal from the remote key. Along with this growth in using smart keys, however, there is an increasing concern over their security vulnerabilities. The most compelling evidence is a surveillance video released by West Midland police department in Birmingham, England, in 2017 that shows two hackers exploiting keyless technology to steal a Mercedes-Benz [86]. In Ref. [87], a falsified-information attack on the LiDaR system, which observes the surrounding environment of an intelligent vehicle, is reported.

All the requirements and attacks mentioned above lead to the conclusion that securing intelligent vehicles is of great importance. Thus, security solutions, mechanisms, and techniques should be used to deal with these attacks. In the next section, we will present some key findings and our analysis.

4. Existing defences against the attacks

In this section, we walk through a variety of existing defences (Fig. 7), which can be used as best practices to deal with the security attacks identified in Section 3 and analyze the pros and cons of these defences. Table 4 lists all security defences presented in this section and associates them with security requirements and security attacks.

4.1. Cryptography

This section provides an overview of cryptography-based algorithms used to enhance security for vehicular networks. In intelligent vehicular systems, encryption is an essential key to ensure safety. The section that follows outlines a number of existing security algorithms based on symmetric key encryption, asymmetric key encryption, and attribute-based encryption.

4.1.1. Symmetric encryption

In symmetric-key cryptology, a single key is used both to encrypt and decrypt data, as shown in Fig. 8. Traditionally, symmetric keys were seldom used in point-to-point communication. They were primarily used in retrieval situations, where the data was stored in a database at a central location. However, they gained popularity because they were simple and much faster than asymmetric keys.

In [88], a decentralized method is proposed to authenticate vehicles using hash functions. The Two-Factor LIghtweight Privacy-preserving (2FLIP) algorithm works in two steps to provide fast and accurate authentication. In the first step, a thematic device is used to identify the driver using fingerprints or face recognition. The key strength of using a biological password is nonrepudiation. In other words, driving evidence or sent messages are undeniable. This is denoted as a biological password and is needed along with the Certificate Authority (CA) for user authentication. The second step is the decentralization of the CA, which means that constant transmission of the CA is not needed for increasing overall efficiency. The authors claim that the new method has a large improvement in terms of computational complexity as opposed to existing schemes. The results of performance evaluation indicate that in the 2FLIP, the computation cost has been reduced 100–1000 times, and the communication overhead has been decreased between 55% and 77%. The reduction in overhead makes this method highly practical. A disadvantage of this algorithm is that all new drivers would have to be subjected to an authentication phase to add them to the list of authenticated drivers.

Pseudorandom authentication can also be used to authenticate a vehicle, both in V2V authentication and vehicle to RSU authentication. In

Table 3
Security attacks on components of intelligent vehicles.

	DoS	DDoS	Black-Hole	Replay	Sybil	Impersonation	Malware	Falsified-Information	Timing
Overall E/E architecture				✓	✓	✓			
Communication network	✓	✓	✓	✓	✓		✓		✓
Computation platform	✓						✓		
New sensors						✓		✓	

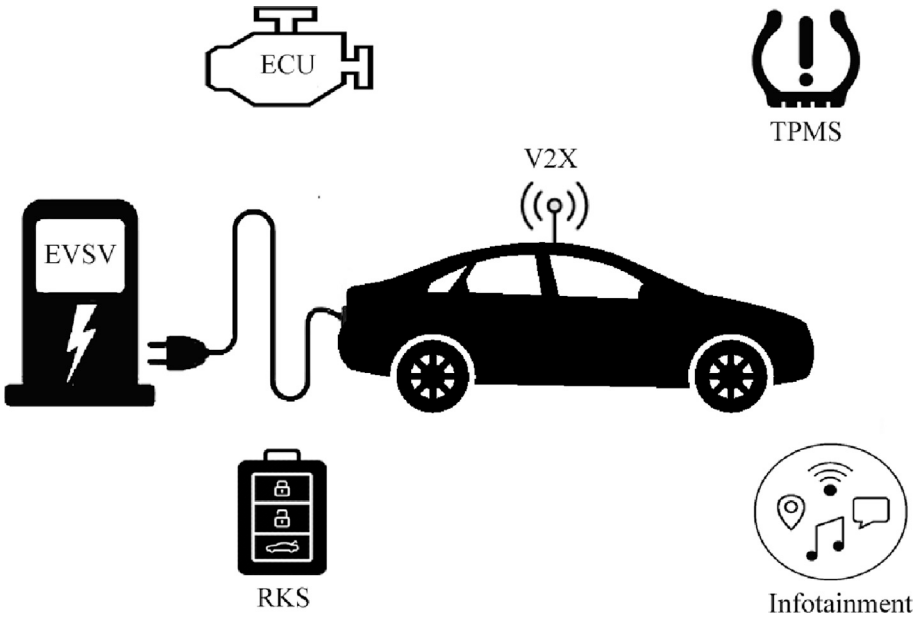

Fig. 6. Typical components of intelligent vehicles.

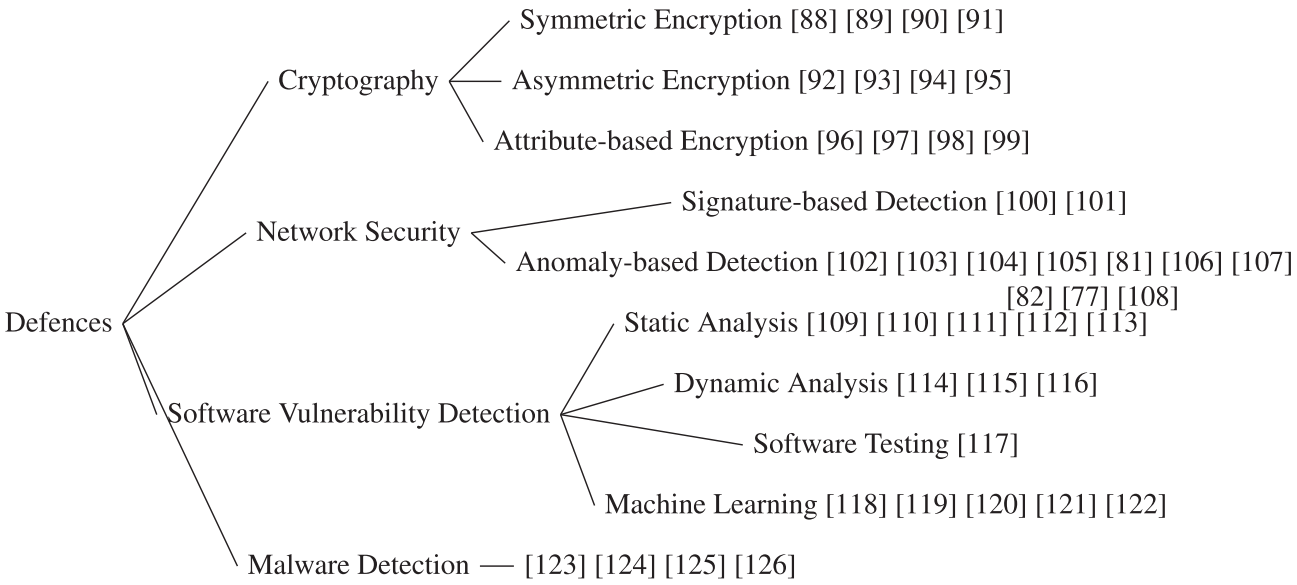

Fig. 7. Existing defences against the attacks.

Ref. [89], a pseudorandom method is used to authenticate users at the RSU. Each user is sent a pseudorandom key that no other vehicle on the network knows. This keeps the identity of each user hidden and known only by the RSU. Pseudonymous Authentication with Conditional Privacy (PACP) is used to generate pseudorandom keys. When the users register at the motor vehicle department, they are handed a ticket with a unique ID that authenticates them and generates a pseudorandom key. Although this scheme is effective, it has very high overhead and is prone to identity theft, as malicious nodes could possibly intercept or copy the ticket acquired at the motor vehicle department. A similar scheme is presented where the RSU sends out a large number of pseudorandom keys and matching certificates. These messages are sent to all users on the network. Then when a user wants to transmit, they would do so by using the pseudorandom key. When the message reaches the receiver, it can be authenticated using the corresponding certificate. Similar to the previous method, this algorithm needs a large amount of overhead. In Ref. [90], an Elliptic-Curve Digital Signature Algorithm (ECDSA)-based scheme is proposed. A typical ECDSA scheme works in three stages: the key generation, signature generation, and signature verification stages. In order for a vehicle to be authenticated, they must be able to generate a valid signature using a public key, whereas the signature generation phase has a low computational complexity associated with it. The highest computational complexity lies in the signature-verification phase, where the receiver must verify that the signature is legitimate from a large list of possible signatures. The method proposed in Ref. [90] introduces a scheme that implements an ECDSA verification engine that is able to verify up to 27,000 signatures per second. This presents a significant reduction in latency within the network. A latency of 37 μs for a single signature verification and an efficiency of 24.5 sGE are achieved, which is a significant improvement compared with previous methods. A Secure and Authenticated Key-Management Protocol (SAKMP) is presented in Ref. [91]. The SAKMP is a distributed key-management protocol that assigns public keys to users based on their geographic locations. The keys are generated using a function that ensures that each key is unique and

Table 4
Comparison of security defences based on security attacks and security requirements.

Category	Security solutions	main mitigated attacks	Authentication	Integrity	Privacy	Availability
Cryptography	2FLIP [88]	DoS	✓	✓	✓	Medium
	PACP [89]	Eavesdropping, replay, impersonation	✓		✓	Medium
	ECDSA [90]	All malicious attacks	✓			Medium
	SA-KMP [91]	DoS, replay, impersonation	✓	✓	✓	Medium
	Calandriello et al. [92]	DoS, jamming	✓	✓	✓	Limited
	PPGCV [93]	Collusion	✓		✓	Limited
	TACKs [94]	Eavesdropping, Sybil, correlation	✓		✓	Limited
	GSIS [95]	DoS	✓	✓	✓	Limited
	DABE [96]	Collusion	✓			Limited
	ABACS [97]	Collusion	✓			Limited
	Xia et al. [98]	Collusion, replay	✓		✓	Limited
	Bouabdellah et al. [99]	Black-hole	✓			Limited
Network Security	Biβmeyer et al. [100]	Sybil	✓	✓	✓	Medium
	REST-Net [101]	Impersonation, falsified information	✓	✓		N/A
	CIDS [102]	DoS, masquarade		✓		Limited
	Martynov et al. [103]	DoS				Good
	IDFVN [104]	Selective forwarding, black-hole				Medium
	Song et al. [105]	Message injection				N/A
	Zaidi et al. [81]	Sybil, falsified information	✓			Good
	OTIDS [106]	DoS, impersonation, fuzzy				N/A
	PES [107]	Sybil		✓	✓	Medium
	AECFV [82]	Black-hole, worme hole, Sybil		✓	✓	Limited
	Markovitz et al. [77]	Falsified information				Meduim
	PML-CIDS [108]	DoS, probing, unauthorized access			✓	Medium
Software Vulnerability Detection	Tice et al. [109]	Control-flow		✓	✓	Good
	Dahse and Holz [110]	XSS, remote code execution	✓		✓	Good
	PITTYPAT [111]	Control-flow	✓	✓	✓	Good
	DFI [112]	Buffer overflow	✓	✓	✓	Good
	FindBugs [113]	Buffer overflow		✓		Medium
	Generational Search [114]	Malware (Bug)		✓	✓	N/A
	TaintCheck [115]	Overwrite	✓	✓	✓	Medium
	Dytan [116]	Control-flow, data-flow, overwrte		✓	✓	Good
	GenProg [117]	DoS, overflow	✓	✓		Medium
	Shin et al. [118]	Malware (Bug)		✓	✓	Good
	Perl et al. [119]	Malware (Bug)		✓	✓	Good
	Zhou and Sharma [120]	DoS		✓	✓	Good
	Shar et al. [121]	Injection, file inclusion		✓	✓	Good
	VDiscover [122]	Malware		✓	✓	Good
Malware Detection	MSPMD [123]	Malware		✓	✓	Limited
	MRMR-SVMS [124]	Malware	✓	✓	✓	Limited
	Huda et al. [125]	Malware		✓	✓	N/A
	CloudIntell [126]	Malware		✓	✓	Variable

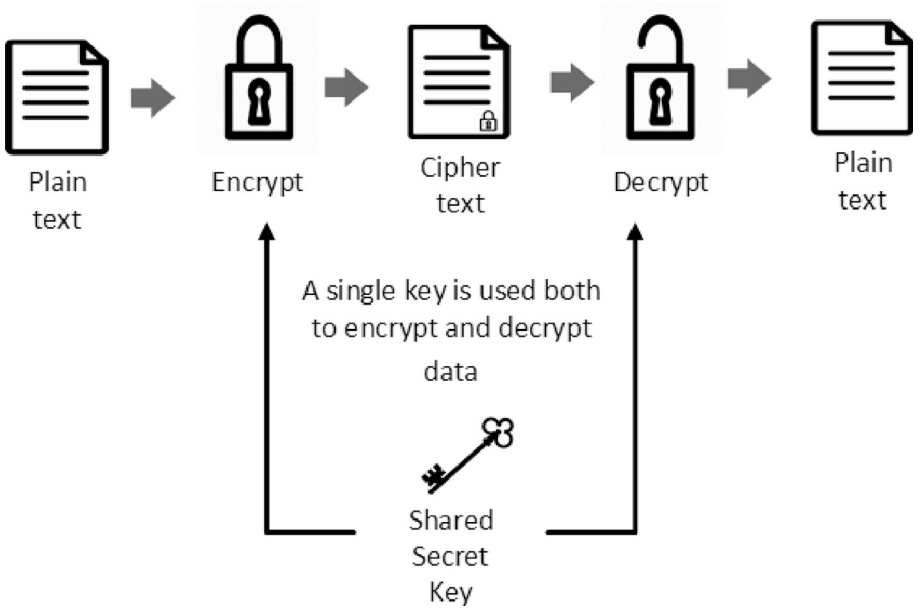

Fig. 8. Symmetric encryption.

dependents on the user's ID and location. The location of the user is obtained using GPS. In order for the algorithm to generate unique keys, a 3D position must be established. The key is generated using the x, y, and z coordinates. The algorithm is only concerned with secure communication between the RSU and the On-Board Units (OBUs). It would be challenging to implement this algorithm in V2V communication because of its dependence on location and the fairly complicated key generation function. Much like the other symmetric-encryption based methods, storing a large number of keys produces a very large overhead, especially for V2V communication.

4.1.2. Asymmetric encryption

Asymmetric cryptography is based on a two-key system (Fig. 9). One of its disadvantages over symmetric cryptography is that it is much slower because of the harder mathematical problems associated with encryption and decryption using separate keys. The keys must also be longer in order for asymmetric cryptography to be useful.

In [92], a pseudonym-based authentication method is used to secure communication in VANETs. A hybrid scheme that uses group signatures to generate on-the-fly pseudonym keys that allow vehicles to remain anonymous within the network is proposed. In this scheme, a vehicle registers within a group, at which point it is given the group public key that can be used to authenticate its messages. This method has low computational complexity and allows the vehicles to quickly authenticate their messages using a group dynamic key. Through the use of group public keys, the authors have reduced the amount of storage needed to execute this method. However, the use of group keys could lead to serious breaches in the security framework. If an attacker was able to gain access to the group keys, it would be able to authenticate the messages.

A Privacy-Preserving Group Communication Scheme for VANETs (PPGCV) is proposed in Ref. [93]. The algorithm works in two phases. In the first phase, each vehicle in the network is given a pool of keys which are randomly distributed. These keys are used for Key Encrypting Keys (KEKs). In order to ensure that the vehicles in the group can communicate, a group key is also established, which can be used to change the key pool to prevent key leakage. If a single vehicle on the network is compromised, the central authority assumes that all keys are compromised. This scheme has a comprehensive method for key relocation and, as such, has the advantage of being robust and hard to predict. But it does add overhead to the network. In addition, during key reallocation, vehicles are left with no encryption methods and cannot transmit data, further decreasing the network efficiency. This method also assumes that vehicles can keep track of which keys have been compromised, which puts an additional burden. If it is not managed properly, then revoked keys can be used by attackers.

A VANET key-management scheme based on Temporary Anonymous Certified Keys (TACKs) is introduced in Refs. [94]. In this method, users are grouped according to their locations. Users that are in close proximity are given a single group public key. Regional Authorities (RAs) are appointed within each group to distribute certificates. A TACK is a short-term certificate that is acquired from the RA. The TACK is used for signing messages. It is a method of authenticating each vehicle within the group. When a vehicle enters a new geographical area or after some set period of time, the TACK expires, and a new one is issued. This ensures that attackers are not able to associate any particular key with any particular user. The new key is generated randomly by any vehicle after its previous key has expired. The new key, along with the group user key, are sent out for authentication by the RA. The RA authenticates the key and updates its internal records accordingly. This scheme's main advantage is the minimal overhead associated with it, especially at the OBU. Most of the computational complexity and authentication are done at the RA. A disadvantage is that the scheme is very infrastructure-dependent and cannot be used in a distributed environment. Temporary Authentication and Revocation Indicator (TARI), an algorithm based on TACK, was proposed in Ref. [127]. It is based on the same security principles as TACK. TARI also uses group signatures that are dependent on the geographical locations of the OBUs. TARI has a different method of authentication. It uses an AI to authenticate OBUs after they have received a message. Each user is verified within its own group. The primary advantage of TARI over TACK is that it uses symmetric-key cryptography, which significantly reduces its overhead. However, it suffers from the same drawbacks of TACK, which makes it highly dependent on a centralized topology.

A method called Group Signature and Identity-based Signature (GSIS) is used to tackle security and conditional privacy in vehicular networks [95]. GSIS proposes to use another two-step process to ensure a high level of security. It groups vehicles into clusters based on their locations. Then, using a group structure, all vehicles are able to securely communicate with each other in a safe and secure manner. Users outside the cluster are ignored. A significant reduction in computational complexity is achieved, as only a single key has to be stored. This could present a problem: if an attacker is to acquire the public key, it would be treated as a part of the group. The communication between the RSU and the cars is achieved using ID-based cryptography. Each message is sent out with a digital

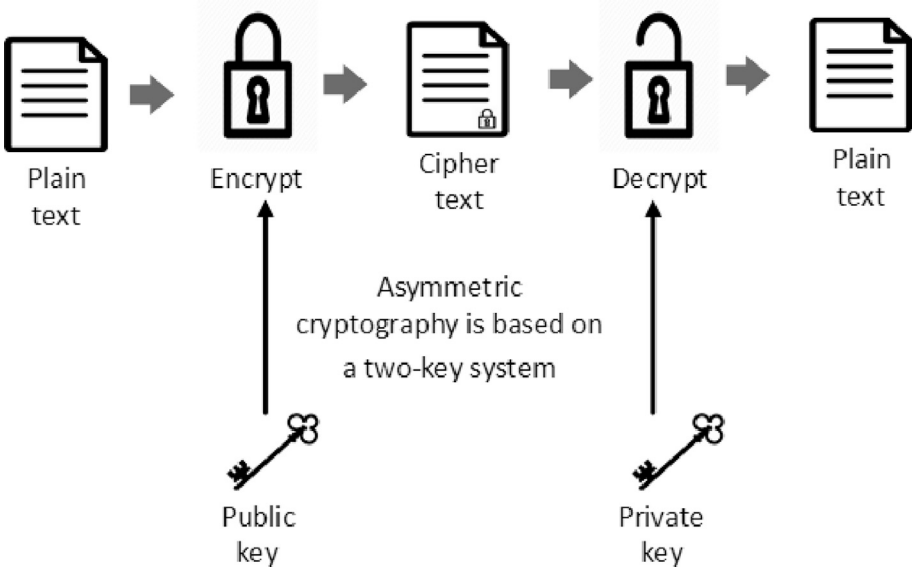

Fig. 9. Asymmetric encryption.

signature called an Identity (ID). The ID numbers for the RSUs are used as public keys, whereas the licence plates of the vehicles are used as their private keys. The main contribution of this paper is to propose a lightweight accurate algorithm, which can guarantee the high level authentication of vehicular communication. The drawback of this method is its susceptibility to man-in-the-middle-attacks, especially within the cluster configuration where vehicle-to-vehicle communication is conducted.

4.1.3. Attribute-based encryption

Compared with symmetric and asymmetric cryptography, Attribute-Based Encryption (ABE) is gaining popularity, especially in intelligent connected vehicles due to the adaptability of ABE to the dynamic networks [128]. The ABE is a form of encryption that uses specific attributes (or a set of attributes) to encrypt data. As such, in order to decrypt the data, one must have a satisfactory configuration/combination of attributes [129]. The ABE was first introduced in 2005 by Sahai and Walters in Refs. [130]. They presented ABE as an application of fuzzy identity-based encryption. This was later expanded in Refs. [131], where the authors present a general framework for the attribute-based cryptology, seen as a more flexible alternative to the rigid traditional public-private key cryptography. Instead of using fixed public and private keys, the encryption is done using specific attributes. The attributes are taken from a pool, which includes an entire library. Only users or groups of users with the same properties as the ones chosen are able to decrypt the message.

This form of encryption is quickly becoming very popular because of its flexibility, effectiveness, and efficiency. In Ref. [96], a secure, selective group broadcast in vehicular networks using dynamic attribute-based encryption is presented. In traditional attribute-based methods, key generation is based on a combination of certain attributes. The attributes selected depend on the policy of the sender. This again depends on what user/group of users the sender intends the message for. When an attribute expires or needs to be replaced, the entire set of attributes must be replaced. This causes considerable overhead and delay. This is especially a problem in vehicular-based networks, where the number of users within a network is highly dynamic. The authors in Ref. [96] propose an algorithm that uses the attribute-based cryptology where each attribute is treated independently, as opposed to a set. When a single attribute elapses or needs to be replaced for some other reasons, it is replaced independently and has no need to change other attributes. The main advantage of this method is the significant reduction in the overhead of the network. However, synchronization between users about which attribute is relevant and which has been changed presents a problem in practical implementation. A similar scheme is presented in Refs. [132], where the authors present an algorithm that looks to dynamically add and remove attributes without affecting the rest of the access control policy tree. In Refs. [132] a fading function is introduced to each attribute, making attributes dynamic and independent. Although this algorithm presents the problem and solution in a slightly different framework, it has very similar advantages and disadvantages.

In [97], an Attribute-Based Access-Control System (ABACS) is proposed to enable improved efficiency of emergency vehicles over VANETs. When an emergency occurs, it is important for the emergency vehicle to be able to get to the emergency site as quickly and efficiently as possible. The emergency vehicles must be able to communicate efficiently with RSUs. The RSUs must be able to identify which emergency vehicles are close by and which can respond to the emergency the fastest. The RSUs broadcast a message encrypted using attribute encryption that uses attributes, such as location, type of emergency vehicle (depending on the emergency, this would be a police car, an ambulance or a fire truck), and event type. The emergency vehicles that have these attributes are the only ones that are able to decrypt the message. When an emergency vehicle encrypts the message, it gets the relevant information and is able to respond. The algorithm presented by the authors offers high security and reduces the overhead since only a single broadcast message has to be sent. In Ref. [98], an adaptive multimedia data-forwarding method is proposed for privacy preservation in VANETs. The paper puts forward a scheme that reduces the overhead placed on on-board units in vehicles. It does this by allowing RSUs to perform a large portion of the overall encryption. Unlike conventional schemes, the paper presents a framework for not only short messages, but also multimedia applications such as social media. It does this by ensuring that the overhead is spread between the OBU and the RSU. Therefore, it is important for vehicles to effectively pick which RSU they are going to involve in the dissemination process. Since decryption takes time, it is important that the vehicle remains within the transmission range of the RSU; otherwise, they will receive partial or incomplete information. The attribute-based encryption is used by both the RSU and the OBU to ensure that users with the appropriate attributes are the only ones that receive the message. This method reduces the computational overhead on the RSUs, which enables them to be smaller and cheaper to implement. It relies heavily on the structure of the network. In large networks, there is a possibility that the RSU would be overwhelmed with large quantities of traffic, causing a bottleneck in the network. A distributed multi-hop algorithm is proposed in Ref. [99], where the authors present a protocol that can be utilized when there is no direct link between the vehicle and the RSU. This paper concentrates on the situations where the OBUs are out of the range of RSUs. The primary issue with relaying information across the network is that malicious users between the source and destination could have a large impact [133]. In order to tackle this, a scheme using attribute-based encryption is employed to ensure only users that have the right attributes receive the message and are able to read them, and a reputation-based function is used to ensure that the messages are passed over the safest possible path. The framework for the reputation/trust function is poorly defined. Additional storage and overhead are added in order to calculate the reputation and then store the reputation of each secondary user on the network. However, this scheme is not independent of a centralized topology. The OBUs are able to communicate in a distributed manner, which would be quite effective in more remote areas or when the RSU is under attack. A fine-grained privacy-preserving protocol is introduced in Ref. [134], which is used to allow service providers to offer certain services to certain vehicles within the network. The algorithm uses the attribute-based encryption to ensure that only authorized vehicles are able to access the offered services by the service providers. Different attributes allow users to access different services. To further add security, a secret sharing scheme is proposed to enforce the fine-grained access control requirements. The algorithm also allows vehicles to remain anonymous by using pseudonyms as unique ID-based signatures. This algorithm is well defined, and it is very effective in ensuring that the service providers only allow certain users to access their services. It also allows for vehicles to remain anonymous. However, there are some concerns that the algorithm would produce a high overhead in practical situations, especially in large networks.

4.1.4. Summarizing cryptographic defences

It is necessary here to compare the cryptography-based algorithms used to enhance the security of intelligent vehicles. Table 5 gives a comparative view of the above-mentioned cryptographic defences and focuses on their key ideas, advantages, and disadvantages. Cryptography in vehicular networks is key to providing safety and security for users and service providers. However, many of the existing cryptographical standards and practices are inadequate for the new generation of vehicles. The current cytological standards are often over complicated and place a high computational burden on the users. They are seldom suitable for high-speed real-time applications in vehicular networks. The latency or a delay in communications between the vehicle and the RSU could cause serious accidents for users. It is, therefore, crucial that cytological standards are lightweight but secure. It must be noted that security is paramount in vehicular networks, and even though real-time applications require low latency, security must also be considered as a priority. Therefore, the application of cryptology algorithms in next-generation vehicles must consider the tradeoff between the security of the

Table 5
Cryptographic defences.

Method	Key idea	Advantages	Disadvantages
2FLIP [88]	Uses decentralized CA and biological password	Reduces message delay, low message loss ratio	Telematics devices are required for all vehicles
PACP [89]	Motor vehicle department gives unique ID to the vehicles for authentication	Scalability	Prone to identity theft, high overhead
ECDSA [90]	Provides an implementation of ECDSA for a fast signature verification	Low latency	Proper implementation of ECDSA is difficult
SA-KMP [91]	Uses geographic information of the vehicle for key generation	Robust against DoS attack	Overhead of storing a large number of keys
Calandriello et al. [92]	Combines pseudonym-based approach with group signatures	Reduces overhead	serious breaches in the security framework
PPGCV [93]	A probabilistic key distribution approach	Preserving the privacy of the nodes, robust	Overhead of key relocation
TACKs [94]	Utilizes short-lived keys that are certified by regional authorities	Reduces overhead especially at the OBU	Low speed is the main disadvantage of asymmetric encryption
GSIS [95]	Integrates group signature and identity-based signature schemes	High level of authentication	Heavy verification procedure for large verification lists
DABE [96]	Allows users to change the attributes that are associated with their private keys	Reduces overhead	Synchronization, not applicable to unpredictable attribute changes
ABACS [97]	Utilizes attribute-based encryption for emergency services	Flexible and scalable access control	attribute revocation mechanism is a key challenge of ABE
Xia et al. [98]	Uses CP-ABE scheme for multi-hop multi-media data transmission in VANETs	Privacy-preserving, access control	It is heavily dependent on the structure of the network
Bouabdellah et al. [99]	Combines CP-ABE and trust management scheme for multi-hop V2V communication	Anonymity, access control	Overhead of calculating and storing trust and reputation values

network and the user against application-based parameters that enable low latency and delay.

To solve these problems, we propose a number of solutions throughout this paper. These include but are not limited to new 3rd Generation Partnership Project (3GPP) standards, software-defined networks, light authentication, and Block Chaining (BC). In the previous sections, we have discussed a number of lightweight authentications methods. In the sections that follow, we discuss 3GPP standards and software-defined networks. Another promising solution to the problems faced by VANETs is BC. As an illustration, the blockchain is a distributed data structure that can manage financial transactions without the need for a centralized authority. In other words, a genuine copy of a digital ledger is shared among the parties. Besides, in order to validate new transactions, the public-key cryptography is utilized for providing multi-signature protection [135]. In Ref. [135], an IoT-based BC method is discussed. The IoT requires similar attributes from security protocols as VANETs. They both require low latency and computational complexity, as well as a high level of security. It is concluded that the blockchain enhances the security of authentication and authorization and also provides a strong defence against IoT security attacks such as IP spoofing. This is primarily due to their high levels of security and scalability [135]. In Ref. [136], the authors present a framework for a lightweight algorithm that is secure and has low overhead. It is claimed that the fundamental security goals of confidentiality, integrity, and availability are considered and delivered using the approach presented in the paper. Significant reductions in overhead are achieved and confirmed through the simulation of a variety of scenarios. In Ref. [137], a similar algorithm is presented that is lightweight and preserves all security features of traditional blockchain algorithms. They proposed an architecture that uses distributed trust to reduce the block validation processing time. The experimentation and trials are conducted in a smart home setting that has similar goals and constraints of VANETs. The simulation of the proposed framework indicates that it has low packet overhead and low processing overhead.

4.2. Network security

Intelligent vehicles require cooperation from other devices and sensors to perform communications. These communications are implemented between the CAN and the ECUs, and security mechanisms have not been considered in these settings at all. The CAN and ECUs are valuable targets for adversaries. For example, a vehicle is connected to various devices such as smartphones, flash memory, and CD using different ports (e.g., USB, auxiliary) and various wireless communication technologies (e.g., 3G, 4G, 5G, WiFi). All of these make the car an open system. Therefore, it is very necessary to invent suitable countermeasures to relieve the security risks in the intelligent car. Since Intrusion Detection Systems (IDSs) are the most effective countermeasure and the most reliable approach [81,138,139] to protect vehicular networks or traditional computer networks, this section reviews related works using IDSs in intelligent cars.

As shown in Fig. 10, there are two main classes of IDSs, including the signature-based detection and the anomaly-based detection. Recently published works [140–142] have discussed ways to secure vehicles from remote attacks by assuming the defense strategy as a network intrusion detection problem. Recently, 3GPP is working on verifying that 5G systems are able to utilize 256-bit symmetric cryptography mechanisms inherited from legacy 4G systems. The handover from one system architecture to the next must remain seamless. As a matter of fact, legacy security visibility and configurability functionality are developing with the evolution of technology. And in the future, devices will be more reactive and flexible to various security configurations.

4.2.1. Signature-based detection

This method first stores various existing signatures of known attacks in a database for retrieving them and making a comparison. Then, it detects the intrusion attack by comparing oncoming cases from the Internet of Vehicle (IoV) with existing signatures of known attacks in the store.

Biβmeyer et al. [100] developed a signature-based IDS that utilizes a plausibility model for vehicle movement data. The proposed scheme is able to detect a single fake vehicle even if it uses a valid movement. Two kinds of attackers can be detected using the proposed algorithm: 1) a fake congestion attack; 2) a denial of congestion attack.

Tomandl et al. [101] introduced a novel IDS called REST-Net for VANETs to check fake messages. Different from previous solutions, REST-Net uses a dynamic engine to analyze and monitor the data, and it achieves very high detection rates and adaptive warning levels in case drivers are interrupted. It is also implemented with a concept that is used for recalling the fake message as long as an attacker is identified.

One of its disadvantages is that it usually causes high false-negative rates when facing unknown or new attacks. Another disadvantage is that the signature-based detection fails to detect intrusions with the development of onboard applications. For example, signature-based detection may be invalid sometimes as more and more additional devices, such as sensors, are integrated into vehicles.

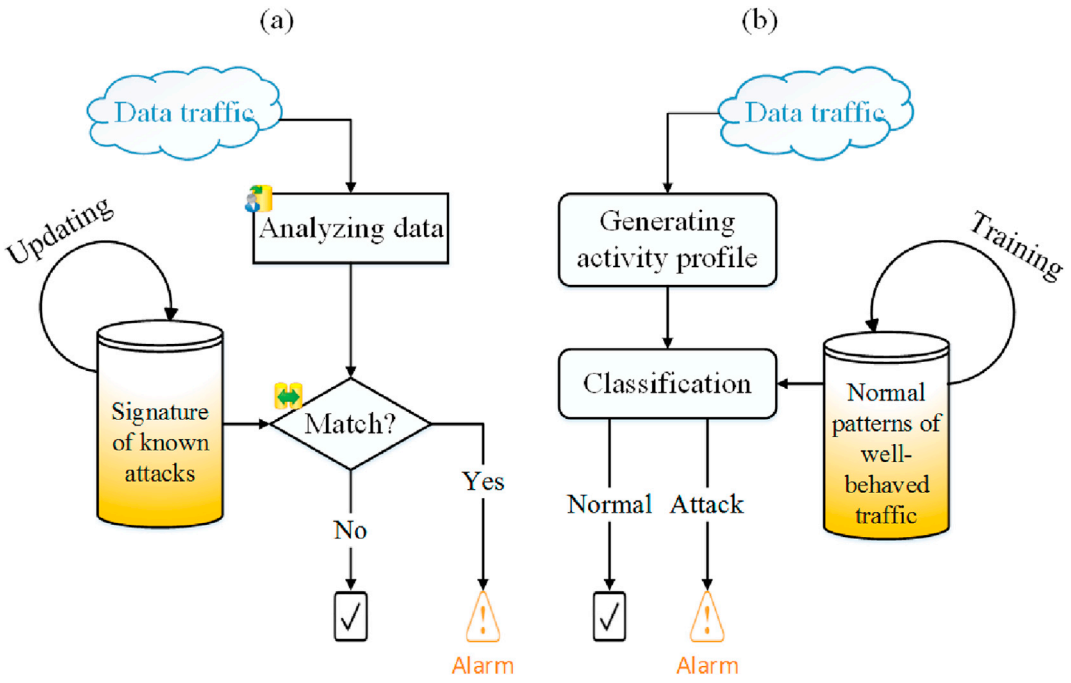

Fig. 10. (a) Signatute-based detection; (b) Anomaly-based detection.

4.2.2. Anomaly-based detection

Anomaly-based detection predefines the baseline of normal cases, then new types of attack can be identified once they are observed to have abnormal information beyond the baseline [143].

Cho and Shin [102] developed a Clock-based IDS (CIDS) for intrusion detection. CIDS constructs a baseline of the ECUs' clock behaviors based on the thus-derived fingerprints, which are extracted from the intervals of periodic in-vehicle messages. Then, CIDS employs cumulative sum to detect any abnormal shifts (i.e., signs of intrusion) in identification errors. Experiments showed that CIDS could achieve a low false-positive rate of 0.055%.

Martynov et al. [103] developed a software-based light-weight IDS based on properties selected from the signal database. Then, the authors studied the message cycle time and the plausibility of the messages and introduced two anomaly-based methods for the IDS. Experiments were conducted in terms of both simulation and real-world scenarios. Experimental results demonstrate that the proposed IDS can recognize some malicious events, such as injection of malformed CAN frames, unauthorized CAN frames as well as DoS attacks.

Sedjelmaci and Senouci [104] proposed a novel Intrusion Detection Framework for a Vehicular Network (IDFVN) utilizing detection and eviction techniques. IDFVN is implemented in two detection agents: a local intrusion-detection module and a global intrusion-detection module. Experiments demonstrate that the IDFVN exhibits a very high detection rate of more than 98% and a low false-positive rate of lower than 1.3%.

Song et al. [105] proposed a light-weight intrusion-detection strategy by analyzing time intervals of CAN messages. The authors first experimentally showed the differences between time intervals of messages in the normal status and the under-attack status. Then, experiments were conducted based on the CAN messages from the cars made by a famous manufacturer. The results showed the effectiveness of the proposed method.

Zaidi et al. [81] presented a statistical-technique-based IDS for anomalies and rogue-nodes detection using a traffic model. The proposed IDS can work independently without relying on any infrastructure. In order to use the proposed mechanism, network message congestion was controlled to avoid broadcast storms. Experiments showed that the proposed IDS could keep the network working even if up to 40% of nodes were malicious.

Lee et al. [106] studied the offset ratio and time interval of message response performance and proposed an intrusion-detection method. The proposed method assumes that the receiver node will respond to the remote frame immediately once a particular identifier is transmitted. It also assumes that the response performance should be different between an attack-free state and an attack state. In order to enhance the overall performance and accuracy of the proposed strategy, a novel algorithm was also proposed to monitor the change of in-vehicle nodes. Offset radio and Time interval-based Intrusion Detection System (OTIDS) can achieve very good performance without modifying the CAN protocol. Moreover, it can not only identify message injection attacks and impersonating node attacks but also can detect the types of messages in the injection attacks.

Yu et al. proposed a Presence Evidence System (PES) [107]. The PES is a statistical method for detecting Sybil attacks in VANETs. The authors have considered signal-strength distribution analysis of vehicles to estimate their physical positions because position verification is regarded as one of the best methods for the detection of Sybil attacks. When a claimer node broadcasts a beacon message at a beacon interval for neighboring discovery, an estimated position will be calculated for the claimer. The main idea is to improve estimating the position of a vehicle by using a RANdom-SAmple Consensus (RANSAC)-based method. It should be mentioned that the RANSAC algorithm is a well-known learning method in the field of computer vision for outliers detection. The main limitation of the PES, however, is that it cannot detect all Sybil attacks.

An accurate and Efficient Collaborative intrusion detection Framework to secure Vehicular networks (AECFV) is introduced by Sedjelmaci and Senouci [82]. AECFV includes intrusion-detection systems at three levels: (1) cluster members level; (2) Cluster Heads (CH) level; (3) RSU level. It should be noted that, along with a rule-based decision technique and a trust-based scheme [144], AECFV makes use of a Support Vector Machine (SVM) as a machine-learning method to detect anomalies at the cluster level. Furthermore, feature extraction, the training process, and the classification process are the three main components of the SVM in the proposed model. Moreover, the detection mechanism of AECFV against different and various types of attacks on VANETs has been discussed. AECFV is expected to suit scenarios such as a lightweight communication overhead as well as fast attack detection. However, inasmuch as AECFV needs to implement IDS on lots of vehicles as cluster members, it causes a high overhead in large-scale vehicular networks. In

the same way, other studies by Sharma and Kaul [145], Wahab et al. [146], and Sedmalci et al. [147] used SVMs for intrusion detection of vehicular networks.

Recent developments in the field of machine learning have also led to a renewed interest in designing intelligent IDSs for in-vehicle anomalies. One study by Markovitz et al. [77] involved designing a domain-aware anomaly detection system for the CAN traffic bus in which Ternary Content-Addressable Memories (TCAMs) have been used for detecting anomalies in CAN bus network traffic. It must be mentioned that TCAMs are special types of high-speed memories that modern switches and routers use them for fast route lookup and packet classification. At first, in the learning phase, the TCAM learns how to classify CAN packets into three categories: constant, multi-value, and counter/sensor. Then, in the testing phase, the TCAM classifier detects irregular messages that do not match the trained model. The authors evaluated the proposed scheme by simulated CAN bus traffic and also by real traffic data. It should be mentioned that the TCAM is implementable in both software and hardware.

Zhang et al. [108] proposed a Privacy-preserving Machine Learning based Collaborative Intrusion Detection System (PML-CIDS) against malicious nodes. The authors argued that privacy is a serious concern for the proposed approach, PML-CIDS, because vehicles may exchange sensitive information. PML-CIDS consists of different parts: The preprocessing engine is responsible for collecting and preprocessing data. The local detection engine is a logistic-regression classifier that is responsible for intrusion detection by analyzing the preprocessed data and determining malicious activities. The Privacy-preserving Collaborative Machine Learning (PCML) engine is responsible for updating the classifier. The main philosophy of PML-CIDS is decentralizing a centralized machine-learning approach. For solving this problem, a distributive optimization method called Alternating Direct Method for Multipliers (ADMM) has been used to decentralize regularized Empirical-Risk-Minimization (ERM) algorithms to achieve distributed training of large datasets. Moreover, PML-CIDS employs a privacy-preserving scheme of regularized ERM-based optimization called Dual-Variable Perturbation (DVP), which perturbs each vehicle's dual variable at every ADMM iteration. It should be noted that PML-CIDS is a distributive approach and decreases the overhead [148].

Anomaly detection can also be analyzed from the perspective of big data analysis with information theory. In this view, anomalies are considered as rare events with a small probability hidden in the total information of voluminous amounts of data. These rare events contain valuable information. In information theory, information measures such as entropy provide a probable solution for characterizing the distribution and highlighting the importance of rare events. Furthermore, dimension reduction of big data and analyzing the relationships among rare events are necessary to increase efficiency [149].

The disadvantages of anomaly-based detection are: 1) it may cause high false-positive rates; 2) it is usually hard to prepare proper metrics to determine the baseline. However, it is expected that data analysis techniques will improve performance in the future.

4.2.3. Summarizing network security defences

In this part of the paper, the most popular network security defences of vehicular networks are compared. Table 6 lists network security defences and compares their merits and demerits.

Table 6
Network security defences.

Method	Key idea	Advantages	Disadvantages
Biβmeyer et al. [100]	Uses position information of vehicles to detect message forgery	Additional hardware (radar, lidar, camera) are not required	Accuracy of GPSs, movements of vehicles, data transmission delays
REST-Net [101]	Utilizes data plausibility checks to analyze and detect an attacker's fake messages	High detection rate, high adaptability	Ineffective against unknown attacks
CIDS [102]	Estimates clock skew of CAN messages to detect intrusion	Evaluation in real conditions, low false positive rate	CIDS cannot detect irregular time sequence attacks
Martynov et al. [103]	Simulates anomaly-based detection against DoS attacks on wireless sensors	Protects nodes against unknown attacks	The simulation is performed on a limited number of fixed nodes
IDFVN [104]	Uses rule-based, learninig-based, and trust-based techniques to detect malicious nodes	High detection rate, low false positive rate	Overhead of using many techniques
Song et al. [105]	analyzes the frequency of CAN messages to detect message injection and DoS attack	Lightweight	Cannot guarantee protection against other types of attacks
Zaidi et al. [81]	Vehicles collect and analyze traffic information of other vehicles to train the IDS	High accuracy, low overhead	Dose not consider data communication attacks
OTIDS [106]	Considers offset and time intervals of CAN messages to detect three types of attacks	accurate, low detection time	IDS cannot detect attacks with irregular *remote frames*
PES [107]	Uses RANSAC to improve estimating physical position of vehicles	Robust estimation	RANSAC can only estimate one model for a particular dataset
AECFV [82]	Uses support vector machine at cluster heads	High detection rate, low false positive	High overhead
Markovitz et al. [77]	Uses TCAM for CAN packets classification	CAN packets are easy to represent as TCAMs, adaptable	Not tested against different attack scenarios
PML-CIDS [108]	Uses DVP approach to decentralize a centralized machine learning approach	Decreases overhead, provides a certain degree of privacy, scalable	Computational complexity

4.3. Software vulnerability detection

A well-known fact is that the software is a critical part of the intelligent vehicles, and the vulnerabilities in this software open up new possibilities to attackers. Therefore, it is important to keep the intelligent vehicles' system secure enough in order to prevent any potential threat, data theft, and even some accidents [150,151]. Many works have been proposed to identify potential vulnerabilities [152–154]. Static analysis [155,156], dynamic analysis [157,158], and concolic execution (i.e., dynamic symbolic execution) [159] are popularly used techniques for vulnerability discovery. In this section, we mainly review the works about vulnerability detection for intelligent vehicles because this is closely related to this work. For more work about software vulnerability detection, please refer to Refs. [154,160].

Intelligent vehicles, including aircraft, airplanes, and cars, have millions of lines of code (Table 7), and the software is responsible for many safety-critical functions of the vehicle. Drive-by-wire, brake-by-wire, suspension-by-wire, and in general X-by-wire (Fig. 11) in the automotive

Table 7
Software size in intelligent vehicles.

Manufacturer	Model	Software Size (lines of code)
Boeing	787	14 million
Lockheed	F-22	8 million
Mercedes-Benz	S series	20 million
Ford	GT	10 million
Ford	CES 2016	150 million

industry refer to the use of fully electric/electronic systems for performing vehicle functions, such as braking or steering, instead of mechanical or hydraulic systems [161]. Testing the flight control software is one of the safety-critical applications which receives the current altitude of the aircraft and uses this information for altitude switch. For example, NASA developed a fly-by-wire fixed-wing aircraft for the first time [162]. NASA Ames Research Center has also developed a software testing platform for testing the aircraft control software a few years ago [163].

Static and dynamic analyses are popularly used in software vulnerability detection. Static analysis is a set of program analysis methods to check and verify the properties of the program code without the need to execute it [164]. Dynamic taint analysis is a technique that aims to analyze the marked information flow when the program is executed, and this method could detect most of the software vulnerabilities [165]. Some Well-known automotive manufacturers (e.g. Toyota [166], Hyundai [167]) and airplane companies (e.g., Boeing [168]) use static, and dynamic analysis of software behavior in safety-critical missions to fix the bugs. There are several common techniques of static analysis, including lexical analysis [169], control-flow analysis [109,111,170], and data flow analysis [112,171]. The main advantage of static analysis is that it does not execute the code, so it has fast execution and high efficiency. In contrast to static analysis, dynamic analysis depends on running the program to examine whether it has errors and vulnerabilities. The two important dynamic analysis techniques are fuzzing [114, 172] and dynamic taint analysis [115,116,173]. Apart from static analysis and dynamic analysis, software testing techniques such as symbolic execution [163] and mutation testing [174] can be used for software vulnerability detection. For instance, symbolic execution has been used for testing the altitude switch used in the flight control software [163].

In addition, machine learning, especially deep learning, has been employed to automatically detect software vulnerabilities [118–122,122, 175,176]. For different methods, the key difference is feature selection. For the software vulnerability prediction model, software metrics that are degrees of some properties that are relative to the software are used as features to train machine-learning and deep-learning models. For a software vulnerability-pattern-recognition system, features are extracted from the software source code using traditional static and dynamic program analysis methods.

4.4. Malware detection

Malware detection is an important problem to be addressed in intelligent vehicles because attackers usually use malware as a key tool to launch campaigns. Even single incidences of malware can cause millions of dollars loss [177]. Therefore, this malware should ideally be found and stopped or at least expunged before it causes any loss.

Global computer security software companies such as McAfee emphasize today's connected cars' vulnerability to malware [7]. Whenever something new and as complex as an intelligent car or truck connects to the Internet, it is exposed to the full force of malicious activities. As depicted in Fig. 12, leaving an attack surface unprotected will expose vehicles to many security risks, including malware and trojans. MSPMD [123], Huda et al. [124], Huda et al. [125], and CloudIntell [126] are among significant and well-known intelligent malware detection approaches, which can be used in vehicular networks. They are compared with each other in Table 8. It demonstrates the key features and points of the above-mentioned malware detection defences, and their merits and demerits.

4.5. Comparision of existing security defence mechanisms

Security defences in intelligent vehicles are developed to protect the in-vehicle communication and communication between vehicles. The evaluation of a solution is required to know whether a particular solution has achieved its aims or not. The evaluation will reveal the effectiveness of security defences against malicious attacks. The challenge here is the fact that security defences are developed under different deployment configurations, which complicates the process of comparison. Herein, the experimental overviews of the above-mentioned existing security defences are compared with one another.

Generally, the challenges of the current main defence mechanisms are as follows:

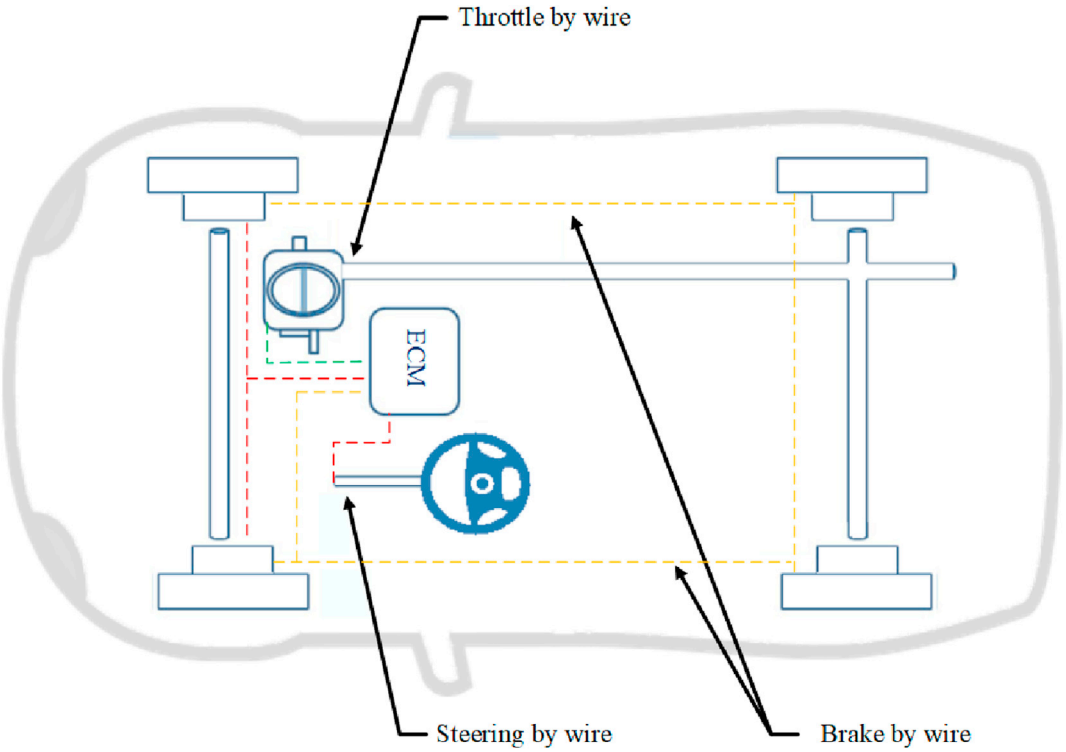

Fig. 11. X by wire.

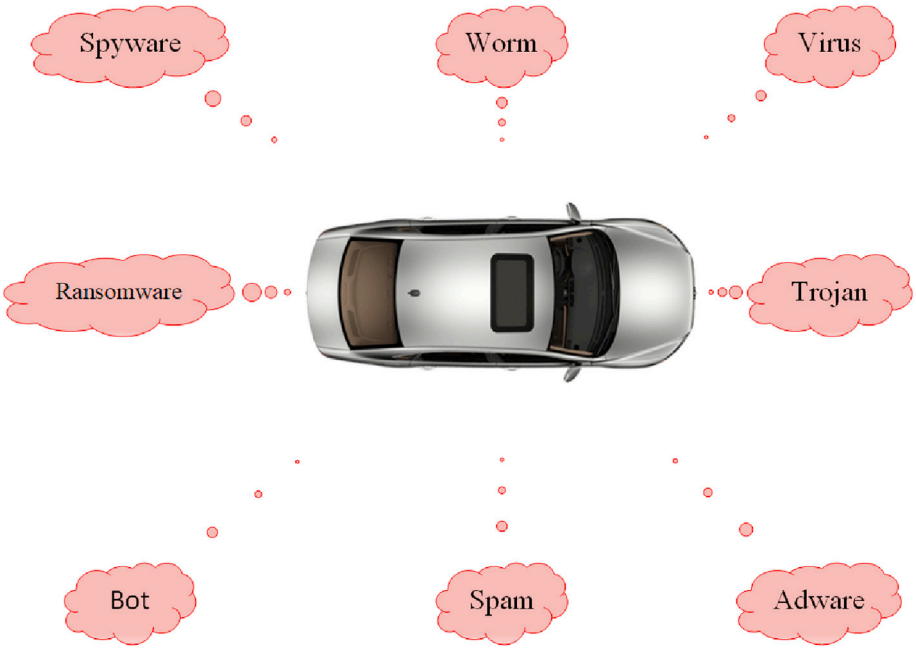

Fig. 12. Various types of malware attacks on intelligent vehicles.

Table 8
Malware detection defences.

Method	Key idea	Advantages	Disadvantages
MSPMD [123]	Uses a modified version of the k-nearest neighbor algorithm for malware detection	High detection rate	k-NN is a lazy learning algorithm
MRMR-SVMS [124]	Uses the combination of SVM wrapper with MRMR filter	Low false positive rate, low false negative rate	Collecting API calls is time-consuming
Huda et al. [125]	Uses semi-supervised technique with unlabeled data for dynamic feature extraction	Significant performance improvement	Complexity of database update procedure
CloudIntell [126]	Computation offloading using SVM, decision tree and boosting on decision tree	Energy efficiency, high detection rate	Continuous connectivity is required

- **Cryptography:** The main disadvantage of symmetric encryption is the problem of key transportation. This problem is solved in asymmetric encryption, and exchanging keys are not required. Thus, asymmetric encryption reduces the overhead. Moreover, they can provide undeniable digital signatures. However, public-key encryption is not fast enough, and it uses more computer resources. In the same vein, the attribute-based encryption, as a suitable mechanism for dynamic networks, is a type of public-key encryption with the same drawbacks. Provided that, the key problem with presented cryptographic methods is that they do not meet the performance requirement of vehicles. In other words, vehicles need light and real-time data transmission out of cities because of their fast-movement nature. On the other hand, over any congested area of the city with a traffic load of more than 100 vehicles in communication range, storing and computation of encrypted messages are really challenging [178].
- **Network security:** The main disadvantage of signature-based detection mechanisms is that they cannot detect zero-day attacks. In contrast, the anomaly-based detection methods have an advantage over the signature-based methods for detecting unknown attacks, but defining the rules is the main challenge of the anomaly-based detection methods.
- **Software vulnerability detection:** Static analysis is usually time-consuming, and finding trained professionals for dynamic testing is difficult. Automated machine learning techniques mitigate the problem. However, machine learning techniques for software vulnerability detection are not accurate enough, and more accurate defences are required. In separate regard, since X-by-wire systems are highly safety-critical, they must comply with safety standards such as ISO 26262. Moreover, software testing techniques must guarantee the traceability of an artifact [179]. Thus, a more intelligent learning defence for an accurate and precise software vulnerability detection is of great importance.
- **Malware detection:** Although using machine learning techniques for malware detection has improved the detection rate, it is still very difficult to detect all evasive malware by traditional *anti*-malware strategies, and more intelligent strategies are required.

The above-mentioned security solutions have been proposed to mitigate malicious attacks and increase the security of vehicles. Table 9 associates identified attacks with the defence mechanisms. It is apparent from this table that cryptographic and intrusion detection techniques are recognized as well-known and popular defence mechanisms for protecting intelligent vehicles while not enough attention has been paid to

Table 9
Security defences against security attacks.

	Cryptography	Network Security	Software Vulnerability Detection	Malware Detection
DoS	✓	✓	✓	
DDoS	✓	✓		
Black-hole	✓	✓		
Replay	✓			
Sybil	✓	✓		
Impersonation	✓	✓		
Malware	✓		✓	✓
Falsified Information	✓	✓		
Timing	✓			

other defences such as software vulnerability detection. As mentioned above in this section, software sizes in intelligent vehicles are growing dramatically, and therefore software vulnerability detection, and malware detection techniques for protecting software in vehicles require particular attention. In general, a specific defence mechanism is not adequate. For instance, the DoS attack on CAN bus is very different from the Dos attack on wireless vehicular communications. Therefore, a systematic approach that integrates complementary defence mechanisms is needed. Cryptographic approaches are usually employed for protecting wireless communications between RSUs and vehicles in inter-vehicle communications. Network security techniques are appropriate for protecting ECUs as well as intrusion detection in wireless communications. Software vulnerability detection techniques are suitable for the testing and analysis of software before installation on the vehicle, while malware detection techniques protect them against malware after installation.

Future research on securing intelligent vehicles against attacks should consider recent technologies and developments. The next section will focus on using lightweight authentication to improve cryptography, LTE advanced, 5G and software-defined security to improve network security, and deep learning to improve software vulnerability and malware detection. In fact, computational constraints and the requirement for real-time data transmission in intelligent vehicles are the main reasons for choosing lightweight authentication as a future direction. Besides, LTE advanced and 5G as new promising telecommunication standards for V2E security and software-defined security as an efficient, adaptable, and dynamic method for detecting and mitigating security attacks are other main directions for future studies. Finally, deep learning techniques are introduced because they outperform machine learning solutions in terms of attack detection accuracy. Therefore, we will consider these developments as future directions.

5. Future directions

The research to date in the field of securing vehicles against cybersecurity challenges has addressed a number of security issues and proposed many security solutions. However, there are still open challenges that need further investigation. Future studies on the current topic are therefore recommended. This section provides a discussion of open issues as well as available and possible methods and technologies to further secure, intelligent vehicles. This part of the paper aims to provide future directions for research and encourage future contributions. In this section, we outline four promising directions to further secure, intelligent vehicle systems: lightweight authentication to improve cryptography, LTE, and software-defined security to improve network security and deep learning to improve software vulnerability and malware detection.

Our main reasons for choosing these directions for future research are as follows:

- **Lightweight authentication:** In modern inter-vehicle communications, the efficiency of authentication has become a central issue because fast-moving vehicles need to authenticate each other as quickly as possible before exchanging any information. Thus, we will introduce lightweight authentication as the first future direction.
- **3GPP:** Resulting from the development of V2E communications, 3GPP Cellular-V2X (C–V2X) as an initial standard completed in early 2017 to provide reliable, scalable, and robust wireless communications for hazardous situations. With this in mind, C–V2X is the first step towards 5G and this area of study has been chosen for its role in the development of network security in the future.
- **Software-defined security:** Software-defined security is the automation of threat detection and the automatic mitigation of attacks. Therefore, SDS is a practical way of improving network security in vehicular networks. In general, design principles of vehicular software-defined networking is an open issue for future research.
- **Deep learning:** More recent attention has focused on using intelligent deep learning technologies in different applications such as self-driving vehicles. Deep learning methods are accurate. They outperform not only machine learning technologies but also humans in many tasks. Future studies on utilizing neural networks in software vulnerability detection, as well as mitigating malware attacks on vehicles, are therefore recommended.

5.1. Lightweight authentication

Achieving lightweight authentication is never a trivial task in intelligent vehicle systems. The reason is that the authentication in the systems should be secure and efficient, and it should be flexible to handle complicated transportation circumstances [180]. As a future research direction, more attention should be paid to lightweight authenticated key generation protocols using communication-media signals.

In this part of the paper, two types of lightweight authentication protocols, including key establishment protocols using the keyless cryptography technology and key distribution protocols using the Li-Fi technology, are reviewed.

5.1.1. Key establishment using keyless cryptography technology

Alpern and Schneider designed a key-establishment protocol in Ref. [181] using the keyless cryptography technology, and it was improved by Refs. [182–184]. In these protocols, the characteristics of the anonymous channel are utilized to establish secret keys. In the field of communication theory, the broadcast channel can be turned into the anonymous channel if the channel achieves source indistinguishability. Technically, source indistinguishability requires that the adversary cannot obtain a non-negligible advantage in identifying the source of the signals (transmitted over the channel) even using sophisticated signal-processing technologies.

5.1.2. Key distribution using light-fidelity technology

The rapid increase of wireless data communication makes the radio spectrum below 10 GHz insufficient. Thus, researchers respond to this challenge by utilizing the radio spectrum above 10 GHz. Light-Fidelity (Li-Fi) provides a promising perspective: it is demonstrated that Li-Fi can achieve high-speed wireless communication, at over 3 Gb/s, from a single LED (which uses the optimized DCO-OFDM modulation) [185, 186].

In recent years, there is an increasing interest in designing intelligent vehicle systems using Li-Fi technology. The related work includes [187–190]. However, the research is in its infancy, and more investigations need to be conducted. Specifically, it is critical and imperative to design key-distribution protocols using Li-Fi technology in order to ensure the security of Li-Fi communication in intelligent vehicle systems.

5.2. 3GPP on V2E security

3GPP is assigned to create technical specification services for LTE support of V2E (3GPP TS33.185 V15.0.0 (2018-06)) [191]. The 3GPP V2E standard will develop specifications for all aspects of LTE advanced and 5G networks, including the protocols' architecture, V2V, V2I, Vehicle to Network (V2N), Vehicle to Pedestrian (V2P) and all related security concepts for all V2E models (Fig. 13). An overview of the LTE enhancements is presented in Ref. [191] with an emphasis on the transport of V2E messages. This document also identifies some of the key threats to security in V2E networks as well as proposed mitigation methods. In addition, some preliminary security requirements are identified to enable safe and secure communication in V2E networks.

A key element in V2E communication is the ability for vehicles and RSUs to effectively and efficiently communicate. The 3GPP group outlines PC5 as the primary communication protocol used between two autonomous cars. In order to facilitate communication between the vehicle and the RSU, a protocol called Uu is used. The vehicle to RSU-server is carried over LTE-Uu

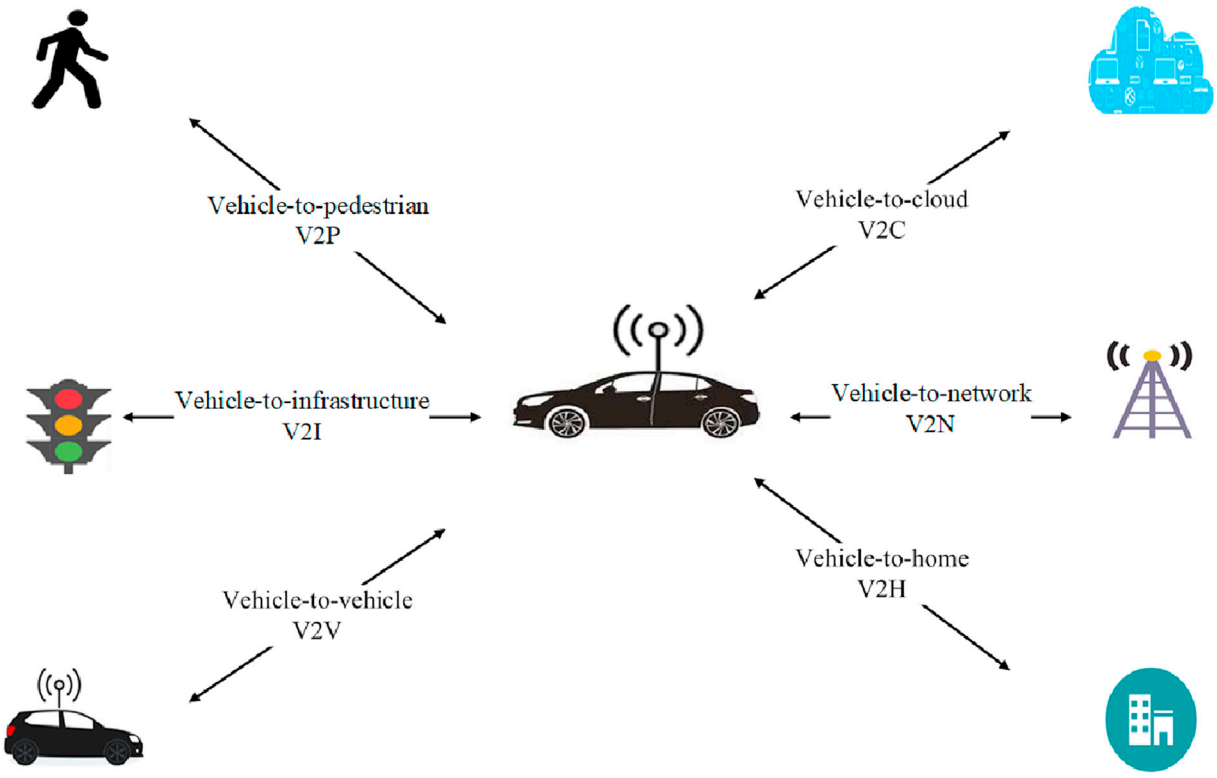

Fig. 13. V2E models.

in a payload of UDP/Ip packets. Emphasis on effective V2E messages is important. In order for vehicles and users to be safe, effective, and efficient exchange of information between vehicles must be achieved. Constant communication and message exchange must be conducted in real-time. Since vehicles are constantly evaluating their environment and their positions, real-time communication is important [191].

Most V2E research is based on the LTE standard. This technology is currently being utilized and has been proven to be effective, with excellent performance, high bandwidth, and low latency (up to 5 ms). 5G is the V2E enabling technology, and it provides ultra-low latency (as low as 1 ms). This allows a real-time response, which enables real-time warnings to be distributed to autonomous vehicles to avoid collisions in real-time. This is key to ensuring that autonomous vehicles provide safe and reliable transport for their users. The end-to-end latency that is required for all real-time V2E transmissions is less than 5 ms for message sizes of about 1600 bytes with a probability of 99.999%. This requirement must be guaranteed for all data traffic in real-time V2E communications [192].

Handover in and out of 5G coverage is illustrated in Fig. 14. It is an important aspect of supporting the V2E application with multiple Radio Access Technology (RAT) modems [193]. The User Equipments (UEs) are grouped into platoons (clusters) as they move through the network. Platoon-related messages must be transmitted between UEs with very low latency as per requirement. Thus, V2V messages needed to support platooning applications are exchanged between the UEs in the target cell using device-to-device communication in 5G New RAT (NR), even though there is no 5G coverage in the target cell [193]. In Ref. [193], intersection safety and provisioning for urban driving are discussed. Future applications lead to reduced traffic congestion as traffic is routed according to traffic incidents and conditions. A Local Dynamic Map (LDM) is used to express traffic signal information, and pedestrian and vehicle movement, direction, and location information. 3GPP utilizes the low latency capability of 5G communications to conduct real-time analysis of traffic conditions to reduce congestion. The concept of intersection safety information system is illustrated in Fig. 15.

3GPP is proposing a car Electronic Control Unit (ECU), which is a software module able to control the car's system electronics. Examples are wheel steering and brakes. The ECU has to be periodically software updatable. ECU software updates are very important for V2E and have to undergo major security testing.

5.3. *Software-defined security*

Software-defined security refers to the automation of threat detection, and automatic mitigation of threats using software-defined platforms by adopting an open flow protocol, Network Function Virtualization (NFV) and Software-Defined Networking (SDN) which utilizes the concept of a multi-layered open virtual switch with programmatic extension to enable automation on a large scale, in addition to the open stack standard as a platform to manage the cloud and distributed data centers.

Current systems take an unacceptably long time to recover from DDoS attacks because they require IT personal intervention to reconfigure major nodes settings and cannot be utilized in a V2E environment. The most promising solution is to automate the network configuration by applying SDN, which uses a central point of control and a decoupling control plan from the data plan to automate the configuration and settings for major nodes. Based on SDN, we can apply the concept of SDS, which would decouple the mitigation plan, from the detection plan to automate the security action and solution to mitigate attacks and threats to any node or component within the V2E system. The SDS has to allow legitimate traffic to pass through to the designated destination and the redirection of traffic with an abnormal signature to submit to a forensic analysis to extract as much as possible information about the attack characteristics and traffic parameters in order to create a patch file to mitigate the attack by pushing down the patch file along with the network major nodes and devices. Dynamically changing environments of V2E will require dynamic software and hardware for practical implementation. SDNs are a key piece of the V2E architecture, enabling dynamic mitigation of security threats on the V2E network.

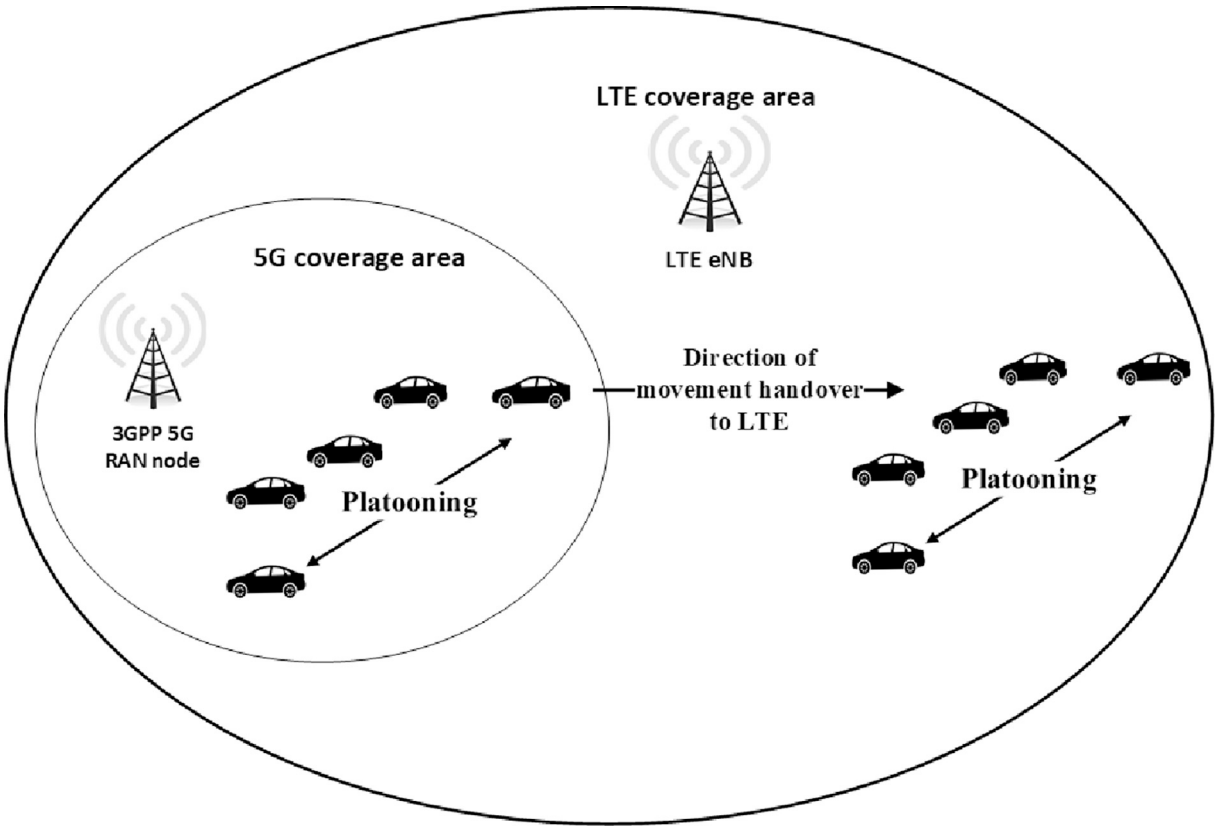

Fig. 14. Use case out of 5G coverage.

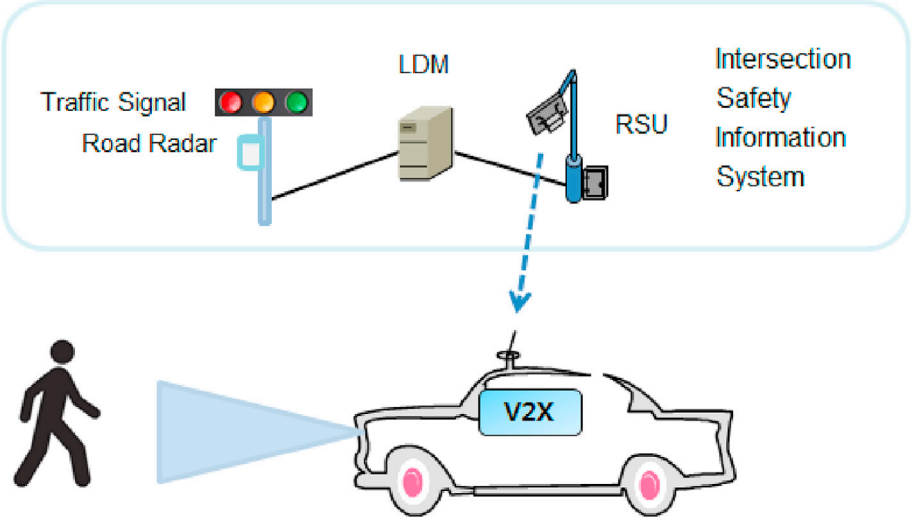

Fig. 15. Concept of intersection safety information system.

5.4. Deep learning

Deep learning models and techniques such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Deep Belief Networks (DBN), Deep Boltzmann Machines (DBM), MultiLayer Perceptron (MLP), autoencoder-based methods, and sparse coding-based methods are based on training neural networks with a training set. After training the neural network, it recognizes the patterns and classifies a different set of examples called a test set [194]. In deep-learning models, there are many layers between the input and output layers for finding features.

5.4.1. Real-time simulation and formal verification

In a separate regard, the industry is adopting real-time simulation and formal verification as part of a security compliance check for intelligent vehicles [76,195,196]. In real-time simulation, computer models are used to accurately re-create repetitive and flexible test environment for vehicular systems [197] while formal verification provides security guarantee [198,199]. As a promising future direction, deep learning-based models can be combined with real-time simulation and formal verification to provide more rigid yet accurate security assurance.

5.4.2. Deep learning on edge computing

As illustrated earlier, one of the main drawbacks of deep learning approaches is computational complexity. Due to more datasets, cloud computing is a convenient solution for deep learning approaches. However, a major problem with this kind of application is huge data traffic and latency. In general, therefore, it seems that the distribution of computation between nodes is a better idea. With this intention, in recent years, edge computing or fog computing for the IoT has been introduced [200]. The term "fog computing" was used by Cisco the first time and generally understood to mean extending cloud computing to the edge of the network. It should be noted that low latency, geographical distribution, real-time interaction, support of mobility, and wireless access are the most significant characteristics of fog computing networks [201].

In particular, exchanging safety-critical information in the IoV and its supporting platform [202] between connected vehicles and RSUs need to minimize latency. With this in mind, mobile edge computing provides an important opportunity for deep learning applications to extend the connected car cloud to be close to vehicles without sending data to distant servers [203].

5.5. Summarizing future directions

With the emerging and developing IoT and IoV, the biggest challenge for intelligent vehicles in the future is security. By comparing the proposed directions for future security solutions, it is obvious that they are usually light, fast, and intelligent. Therefore, they provide an appropriate environment for developing more adaptable and complicated security defences with high performance, meeting security requirements in the vehicles.

6. Validity discussion

In any study of this report, the validity of the results is always under threat. As a matter of fact, it is possible that some limitations may have influenced this review paper. Herein, some of these limitations and threats have been discussed:

- **Limitation of the approach:** Due to brevity, we only selected a few interesting and major security attacks. The scope of attacks is nowhere close to being exhaustive. But we hope the solutions for these attacks can provide generalizable solutions for other attacks that are not covered here.
- **Solutions covered:** Once again, our solutions chosen are nowhere exhaustive, but we have chosen them based on our research capabilities from all possible collaborations for the manuscript. We hope the solutions, though inevitably limited, can provide some research insight into securing the intelligent vehicle systems.

7. Conclusion

In this paper, we presented an overview of securing state-of-the-art intelligent vehicles. Firstly, we focused on security issues and stated the security requirements of intelligent vehicular networks. We also presented a number of security attacks on intelligent vehicle systems and challenges related to them. Secondly, we studied the security defences and classified them into four categories regarding their effectiveness against these identified attacks. Finally, we comprehensively reviewed and discussed the potential directions for the future to secure intelligent vehicle systems and their communications. Since the security problems regarding intelligent vehicles have raised increasing concerns among academia and industry, we hope this work can provide a good foundation for researchers interested in gaining insight into intelligent vehicles' security issues and working on the proposed solutions.

Funding

Australia Research Council LP *190100676*.

Declaration of competing interest

None.

References

[1] C. Patsakis, K. Dellios, M. Bouroche, Towards a distributed secure in-vehicle communication architecture for modern vehicles, Comput. Secur. 40 (2014) 60–74.
[2] M. Cheah, S.A. Shaikh, J. Bryans, P. Wooderson, Building an automotive security assurance case using systematic security evaluations, Comput. Secur. 77 (2018) 360–379.
[3] A. Greenberg, Hackers reveal nasty new car attacks–with me behind the wheel (video) [Online]. Available, https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#3901ab9a228c, 2013.
[4] A. Greenberg, The jeep hackers are back to prove car hacking can get much worse [Online]. Available, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/, 2016.
[5] O. Solon, Team of hackers take remote control of tesla model s from 12 miles away [Online]. Available, https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes, 2016.
[6] C. Miller, Researchers hack bmw cars, discover 14 vulnerabilities [Online]. Available, https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/, 2018.
[7] C. David, S. Fry, Automotive security best practices [Online]. Available, https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf, 2016.
[8] B. Mokhtar, M. Azab, Survey on security issues in vehicular ad hoc networks, Alexandria Eng. J. 54 (4) (2015) 1115–1126.
[9] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: vanets and iov, Ad Hoc Netw. 61 (2017) 33–50.
[10] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, Vanet security challenges and solutions: a survey, Vehicul. Commun. 7 (2017) 7–20.
[11] C. Bernardini, M.R. Asghar, B. Crispo, Security and Privacy in Vehicular Communications: Challenges and Opportunities, *Vehicular Communications*, 2017.
[12] W. Haas, P. Langjahr, Cross-domain vehicle control units in modern e/e architectures, in: *16*. Internationales Stuttgarter Symposium, Springer, 2016, pp. 1619–1627.
[13] S. Brunner, J. Roder, M. Kucera, T. Waas, Automotive e/e-architecture enhancements by usage of ethernet tsn, in: Intelligent Solutions In Embedded Systems (WISES), 2017 13th Workshop On, IEEE, 2017, pp. 9–13.
[14] W. Zeng, M.A. Khalid, S. Chowdhury, In-vehicle networks outlook: achievements and challenges, IEEE Commun. Surv. Tutor. 18 (3) (2016) 1552–1571.
[15] M.E. Afsin, K.W. Schmidt, E.G. Schmidt, C 3: configurable can fd controller: architecture, design and hardware implementation, in: Industrial Embedded Systems (SIES), 2017 12th IEEE International Symposium On, IEEE, 2017, pp. 1–9.
[16] F. Hartwich, et al., Can with flexible data-rate, in: *Proc. iCC*. Citeseer, 2012, pp. 1–9.
[17] R. Bosch, Can with Flexible Data-Rate Specification, *Robert Bosch GmbH*, Stuttgart, 2012.
[18] F. Consortium, Flexray Communications System Protocol Specification, vol. 3.0.1, *Version*, 2010, pp. 1–341, no. 1.
[19] S. Khurshid, C.S. Păsăreanu, W. Visser, Most150-development and production launch from an oems perstective, in: Presented at the 11th MOST Intercon-Nectivity Conf, Asis, Seoul, Korea, 2010, pp. 553–568.
[20] A. Grzemba, "Most Book from Most 25 to Most 150," *MOST Cooperation*, FRANZIS, 2011.
[21] E. Zeeb, "Optical data bus systems in cars: current status and future challenges," in *Optical Communication*, in: 2001. ECOC'01. 27th European Conference on, vol. 1, IEEE, 2001, pp. 70–71.
[22] K. Matheus, T. Königseder, Automotive Ethernet, Cambridge University Press, 2017.
[23] P. Hank, T. Suermann, S. Mueller, Automotive ethernet, a holistic approach for a next generation in-vehicle networking standard, in: Advanced Microsystems For Automotive Applications 2012, Springer, 2012, pp. 79–89.
[24] Ethernet in-vehicle networking to feature in 40% of vehicles shipping globally by 2020, london, u.k." *[Online] Available*: https://www.abiresearch.com/press/ethernet-in-vehiclenetworking-to-feature-in-40-of, accessed on Nov. 09, 2014.
[25] D. Yang, K. Jiang, D. Zhao, C. Yu, Z. Cao, S. Xie, Z. Xiao, X. Jiao, S. Wang, K. Zhang, Intelligent and Connected Vehicles: Current Status and Future Perspectives, *Science China Technological Sciences*, 2018, pp. 1–26.
[26] C. Weiß, V2x communication in europe–from research projects towards standardization and field testing of vehicle communication technology, Comput. Network. 55 (14) (2011) 3103–3119.
[27] M. Obst, L. Hobert, P. Reisdorf, Multi-sensor data fusion for checking plausibility of v2v communications by vision-based multiple-object tracking, in: Vehicular Networking Conference (VNC), 2014 IEEE, IEEE, 2014, pp. 143–150.

[28] S.-W. Kim, B. Qin, Z.J. Chong, X. Shen, W. Liu, M.H. Ang, E. Frazzoli, D. Rus, Multivehicle cooperative driving using cooperative perception: design and experimental validation, IEEE Trans. Intell. Transport. Syst. 16 (2) (2015) 663–680.
[29] W. Liu, S.-W. Kim, K. Marczuk, M.H. Ang, Vehicle motion intention reasoning using cooperative perception on urban road, in: Intelligent Transportation Systems (ITSC), 2014 IEEE 17th International Conference On, IEEE, 2014, pp. 424–430.
[30] S.-W. Kim, W. Liu, M.H. Ang, E. Frazzoli, D. Rus, The impact of cooperative perception on decision making and planning of autonomous vehicles, IEEE Intell. Transp. Syst. Magaz. 7 (3) (2015) 39–50.
[31] S. Luthardt, C. Han, V. Willert, M. Schreier, Efficient graph-based v2v free space fusion, in: Intelligent Vehicles Symposium (IV), 2017 IEEE, IEEE, 2017, pp. 985–992.
[32] K.Y. Leung, T.D. Barfoot, H.H. Liu, Decentralized cooperative slam for sparsely-communicating robot networks: a centralized-equivalent approach, J. Intell. Rob. Syst. 66 (3) (2012) 321–342.
[33] L.D.W. Shenjiang, The design of the controller on automobile taillight based on at89s52 [j], For. Electr. Meas. Technol. 8 (2010), 021.
[34] J. Xu, F.M. Zhong, Automotive Air Conditioning Control System Based on Stcl2c5a60s2 Singlechip, *Auto Electric Parts*, 2014, pp. 14–16.
[35] H.Y. Gan, J.Z. Zhang, Q.C. Lu, Study on Operating Mode Control of Hybrid Electric Vehicle Based on the High Performance 32- Bit Scm Mpc555, *Automobile Technology*, 2004, pp. 9–12.
[36] X.Q. Yu, B.B. Chen, T.K. Ji, Dsp software design for eq effect of car multimedia system, Microcomp. Appl. 30 (2011) 47–50.
[37] Y.J. Yu, Z.Z. Fu, L. Rao, et al., Dsp-based advancecollision warning system, Process Autom. Instrum. 30 (6) (2009) 11–13.
[38] J.Q. Yu, Z.Z. Chen, P. Liang, The design and implementation signal processing system of the automotive collision. avoidance based on tms320vc5402, Microcomp. Inform. 23 (2007) 266–267.
[39] E. Lindholm, J. Nickolls, S. Oberman, J. Montrym, Nvidia tesla: a unified graphics and computing architecture, IEEE Micro 28 (2) (2008).
[40] B.L. Liu, Y.B. Sun, Osek/vdx— an Open-Architectured Platform of Vehicle Electronics System, *Vehicle& Power Technology*, 2002, pp. 61–64.
[41] C. Guettier, B. Bradai, F. Hochart, P. Resende, J. Yelloz, A. Garnault, Standardization of generic architecture for autonomous driving: a reality check, in: Energy Consumption And Autonomous Driving, Springer, 2016, pp. 57–68.
[42] S. Aly, "Consolidating autosar with complex operating systems (autosar on linux),'' SAE Technical Paper, Tech. Rep. (2017).
[43] S. Fürst, M. Bechter, Autosar for connected and autonomous vehicles: the autosar adaptive platform, in: Dependable Systems And Networks Workshop, 2016 46th Annual IEEE/IFIP International Conference On, IEEE, 2016, pp. 215–217.
[44] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W.R. Harris, S. Jha, T. Peyrin, A. Poschmann, S. Chakraborty, Security challenges in automotive hardware/software architecture design, in: Proceedings Of the Conference On Design, Automation And Test In Europe, EDA Consortium, 2013, pp. 458–463.
[45] T. Jochem, D. Pomerleau, No Hands across america Official Press Release, *Carnegie Mellon University*, 1995.
[46] M. Maurer, R. Behringer, S. Furst, F. Thomanek, E.D. Dickmanns, A compact vision system for road vehicle guidance, in: *Pattern Recognition*, 1996., Proceedings of the 13th International Conference on, vol. 3, IEEE, 1996, pp. 313–317.
[47] M. Bertozzi, A. Broggi, G. Conte, A. Fascioli, R. Fascioli, "Vision-based automated vehicle guidance: the experience of the argo vehicle,'' *Tecniche di Intelligenza Artificiale e Pattern Recognition per la Visione Artificiale*, 1998, pp. 35–40.
[48] A. Broggi, M. Bertozzi, A. Fascioli, Architectural issues on vision-based automatic vehicle guidance: the experience of the argo project, R. Time Imag. 6 (4) (2000) 313–324.
[49] M. Campbell, M. Egerstedt, J.P. How, R.M. Murray, Autonomous driving in urban environments: approaches, lessons and challenges, Phil. Trans. Roy. Soc. Lond.: Math. Phys. Eng. Sci. 368 (1928) (2010) 4649–4672.
[50] D.G. Johnson, Development of a high resolution mmw radar employing an antenna with combined frequency and mechanical scanning, in: Radar Conference, 2008. RADAR'08. IEEE, IEEE, 2008, pp. 1–5.
[51] X. Wang, L. Xu, H. Sun, J. Xin, N. Zheng, Bionic vision inspired on-road obstacle detection and tracking using radar and visual information, in: Intelligent Transportation Systems (ITSC), 2014 IEEE 17th International Conference On, IEEE, 2014, pp. 39–44.
[52] S. Han, X. Wang, L. Xu, H. Sun, N. Zheng, Frontal object perception for intelligent vehicles based on radar and camera fusion, in: Control Conference (CCC), 2016 35th Chinese, IEEE, 2016, pp. 4003–4008.
[53] X. Wang, L. Xu, H. Sun, J. Xin, N. Zheng, On-road vehicle detection and tracking using mmw radar and monovision fusion, IEEE Trans. Intell. Transport. Syst. 17 (7) (2016) 2075–2084.
[54] T. Kato, Y. Ninomiya, I. Masaki, An obstacle detection method by fusion of radar and motion stereo, IEEE Trans. Intell. Transport. Syst. 3 (3) (2002) 182–188.
[55] S. Song, M. Chandraker, Robust scale estimation in real-time monocular sfm for autonomous driving, in: Proceedings Of the IEEE Conference On Computer Vision And Pattern Recognition, 2014, pp. 1566–1573.
[56] E. Dagan, O. Mano, G.P. Stein, A. Shashua, Forward collision warning with a single camera, in: Intelligent Vehicles Symposium, 2004 IEEE, IEEE, 2004, pp. 37–42.
[57] K.-Y. Park, S.-Y. Hwang, Robust range estimation with a monocular camera for vision-based forward collision warning system, Sci. World J. (2014) 2014.
[58] Y. Dong, Z. Hu, Driver inattention monitoring system for intelligent vehicles, in: Transportation Technologies For Sustainability, Springer, 2013, pp. 395–421.
[59] M. Bertozzi, A. Broggi, A. Fascioli, Vision-based intelligent vehicles: state of the art and perspectives, Robot. Autonom. Syst. 32 (1) (2000) 1–16.
[60] A. Tawari, S. Sivaraman, M.M. Trivedi, T. Shannon, M. Tippelhofer, Looking-in and looking-out vision for urban intelligent assistance: estimation of driver attentive state and dynamic surround for safe merging and braking, in: Intelligent Vehicles Symposium Proceedings, 2014 IEEE, IEEE, 2014, pp. 115–120.
[61] A. Davies, The wired guide to self-driving cars [Online]. Available, https://www.wired.com/story/guide-self-driving-cars/, 2018.
[62] P. Campbell, Eu motors ahead with rules for self-driving cars. [Online]. Available: https://www.ft.com/content/f3a76e4c-5772-11e8-b8b2-d6ceb45fa9d0, 2018.
[63] J. Stewart, Tesla's autopilot was involved in another deadly crash [Online]. Available, https://www.wired.com/story/tesla-autopilot-self-driving-crash-california/, 2018.
[64] A. Davies, The unavoidable folly of making humans train self-driving cars [Online]. Available, https://www.wired.com/story/uber-crash-arizona-human-train-self-driving-cars/, 2018.
[65] A. news, Uber suspends self-driving car tests after vehicle hits and kills woman crossing the street in Arizona [Online]. Available, http://www.abc.net.au/news/2018-03-20/uber-suspends-self-driving-car-tests-after-fatal-crash/9565586, 2018.
[66] A. Perrig, R. Canetti, J.D. Tygar, D. Song, The Tesla Broadcast Authentication Protocol, vol. 5, 2002, p. 11.
[67] Z. Zorz, Researchers hack bmw cars, discover 14 vulnerabilities [Online]. Available, https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/, 2018.
[68] R. Verdult, F. Garcia, J. Balasch, Gone in 360 Seconds: Hijacking with Hitag2, 01 2012, pp. 237–252.
[69] G. De La Torre, P. Rad, K.-K.R. Choo, Driverless Vehicle Security: Challenges and Future Research Opportunities, *Future Generation Computer Systems*, 2018.
[70] Q.G.K. Safi, S. Luo, C. Wei, L. Pan, G. Yan, Cloud-based security and privacy-aware information dissemination over ubiquitous vanets, Comput. Stand. Interfac. 56 (2018) 107–115.
[71] M.S. Al-kahtani, Survey on Security Attacks in Vehicular Ad Hoc Networks (Vanets), in: 2012 6th International Conference On Signal Processing And Communication Systems, Dec 2012, pp. 1–9.
[72] L. Wang, J. Kangasharju, Measuring large-scale distributed systems: case of bittorrent mainline dht, in: IEEE P2P 2013 Proceedings, Sept 2013, pp. 1–10.
[73] Real-world sybil attacks in bittorrent mainline dht, in: 2012 IEEE Global Communications Conference (GLOBECOM), Dec 2012, pp. 826–832.
[74] G. Smith, The new threats to firewalls [Online]. Available, https://www.computerworld.com/article/2569753/security0/the-new-threats-to-firewalls.html, 2003.
[75] P. Cencioni, R. Di Pietro, A mechanism to enforce privacy in vehicle-to-infrastructure communication, Comput. Commun. 31 (12) (2008) 2790–2802.
[76] L. Pan, X. Zheng, H. Chen, T. Luan, H. Bootwala, L. Batten, Cyber security attacks to modern vehicular systems, J. Inform. Secur. Appl. 36 (2017) 90–100.
[77] M. Markovitz, A. Wool, Field classification, modeling and anomaly detection in unknown can bus networks, Vehicul. Commun. 9 (2017) 43–52.
[78] D.K. Nilsson, U.E. Larson, F. Picasso, E. Jonsson, A first simulation of attacks in the automotive network communications protocol flexray, in: Proceedings Of the International Workshop On Computational Intelligence In Security For Information Systems CISIS'08, Springer, 2009, pp. 84–91.
[79] R. Leszczyna, A Review of Standards with Cybersecurity Requirements for Smart Grid, *Computers & Security*, 2018.
[80] K.C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, J. Martin, Vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) communication in a heterogeneous wireless network–performance evaluation, Transport. Res. C Emerg. Technol. 68 (2016) 168–184.
[81] K. Zaidi, M.B. Milojevic, V. Rakocevic, A. Nallanathan, M. Rajarajan, Host-based intrusion detection for vanets: a statistical approach to rogue node detection, IEEE Trans. Veh. Technol. 65 (8) (2016) 6703–6714.
[82] H. Sedjelmaci, S.M. Senouci, An accurate and efficient collaborative intrusion detection framework to secure vehicular networks, Comput. Electr. Eng. 43 (2015) 33–47.
[83] J. Cui, L.S. Liew, G. Sabaliauskaite, F. Zhou, A Review on Safety Failures, Security Attacks, and Available Countermeasures for Autonomous Vehicles, *Ad Hoc Networks*, 2018.
[84] L. Wei, H. Qin, Y. Wang, Z. Zhang, G. Yu, Virus-traffic coupled dynamic model for virus propagation in vehicle-to-vehicle communication networks, Vehicul. Commun. 14 (2018) 26–38.
[85] J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles, IEEE Trans. Intell. Transport. Syst. 16 (2) (2015) 546–556.
[86] S. Fussel, Watch thieves hack keyless entry to steal a mercedes in less than a minute [Online]. Available, https://gizmodo.com/watch-thieves-hack-keyless-entry-to-steal-a-mercedes-in-1820767189, 2017.
[87] M.H. Eiza, Q. Ni, Driving with sharks: rethinking connected vehicles with vehicle cybersecurity, IEEE Veh. Technol. Mag. 12 (2) (2017) 45–51.
[88] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2flip: a two-factor lightweight privacy-preserving authentication scheme for vanet, IEEE Trans. Veh. Technol. 65 (2) (Feb 2016) 896–911.
[89] D. Huang, S. Misra, M. Verma, G. Xue, Pacp: an efficient pseudonymous authentication-based conditional privacy protocol for vanets, IEEE Trans. Intell. Transport. Syst. 12 (3) (2011) 736–746.
[90] M. Knežević, V. Nikov, P. Rombouts, Low-latency ecdsa signature verification 2014;a road toward safer traffic, IEEE Trans. Very Large Scale Integr. Syst. 24 (11) (Nov 2016) 3257–3267.

[91] H. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang, P.H.J. Chong, A secure and authenticated key management protocol (sa-kmp) for vehicular networks, IEEE Trans. Veh. Technol. 65 (12) (Dec 2016) 9570–9584.
[92] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, Efficient and robust pseudonymous authentication in vanet, ser. VANET '07, in: Proceedings Of the Fourth ACM International Workshop On Vehicular Ad Hoc Networks, ACM, New York, NY, USA, 2007, pp. 19–28, https://doi.org/10.1145/1287748.1287752 [Online]. Available.
[93] A. Wasef, X. Shen, Ppgcv: privacy preserving group communications protocol for vehicular ad hoc networks, in: *2008* IEEE International Conference on Communications, May 2008, pp. 1458–1463.
[94] A. Studer, E. Shi, F. Bai, A. Perrig, Tacking together efficient authentication, revocation, and privacy in vanets, in: 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2009, pp. 1–9.
[95] X. Lin, X. Sun, P.H. Ho, X. Shen, Gsis: a secure and privacy-preserving protocol for vehicular communications, IEEE Trans. Veh. Technol. 56 (6) (Nov 2007) 3442–3456.
[96] N. Chen, M. Gerla, D. Huang, X. Hong, Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption, in: 2010 the 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net), June 2010, pp. 1–8.
[97] L.-Y. Yeh, Y.-C. Chen, J.-L. Huang, Abacs: an Attribute-Based Access Control System for Emergency Services over Vehicular Ad Hoc Networks, vol. 29, 03 2011, pp. 630–643.
[98] Y. Xia, W. Chen, X. Liu, L. Zhang, X. Li, Y. Xiang, Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks, IEEE Trans. Intell. Transport. Syst. 18 (10) (Oct 2017) 2629–2641.
[99] M. Bouabdellah, F.E. Bouanani, H. Ben-azza, A secure cooperative transmission model in vanet using attribute based encryption, in: 2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS), Oct 2016, pp. 1–6.
[100] N. Bißmeyer, C. Stresing, K.M. Bayarou, Intrusion detection in vanets through verification of vehicle movement data, in: *Vehicular Networking Conference (VNC), 2010 IEEE*, IEEE, 2010, pp. 166–173.
[101] A. Tomandl, K.-P. Fuchs, H. Federrath, Rest-net: a dynamic rule-based ids for vanets, in: Wireless And Mobile Networking Conference (WMNC), 2014 7th IFIP, IEEE, 2014, pp. 1–8.
[102] K.-T. Cho, K.G. Shin, Fingerprinting electronic control units for vehicle intrusion detection, in: USENIX Security Symposium, 2016, pp. 911–927.
[103] D. Martynov, J. Roman, S. Vaidya, H. Fu, Design and implementation of an intrusion detection system for wireless sensor networks, in: Electro/Information Technology, 2007 IEEE International Conference On, IEEE, 2007, pp. 507–512.
[104] H. Sedjelmaci, S.M. Senouci, A new intrusion detection framework for vehicular networks, in: *Communications (ICC),* 2014 *IEEE International Conference On*, IEEE, 2014, pp. 538–543.
[105] H.M. Song, H.R. Kim, H.K. Kim, Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network, in: Information Networking (ICOIN), 2016 International Conference On, IEEE, 2016, pp. 63–68.
[106] H. Lee, S. H. Jeong, and H. K. Kim, "Otids: A Novel Intrusion Detection System for In-Vehicle Network by Using Remote Frame.''.
[107] B. Yu, C.-Z. Xu, B. Xiao, Detecting sybil attacks in vanets, J. Parallel Distr. Comput. 73 (6) (2013) 746–756.
[108] T. Zhang, Q. Zhu, Distributed privacy-preserving collaborative intrusion detection systems for vanets, IEEE Trans. Signal Inform. Process. over Netw. 4 (1) (2018) 148–161.
[109] C. Tice, T. Roeder, P. Collingbourne, S. Checkoway, Ú. Erlingsson, L. Lozano, G. Pike, Enforcing forward-edge control-flow integrity in gcc & llvm, in: USENIX Security Symposium, 2014, pp. 941–955.
[110] J. Dahse, T. Holz, Static detection of second-order vulnerabilities in web applications, in: USENIX Security Symposium, 2014, pp. 989–1003.
[111] R. Ding, C. Qian, C. Song, B. Harris, T. Kim, W. Lee, Efficient protection of path-sensitive control security, in: 26th USENIX Security Symposium (USENIX Security 17), USENIX Association, Vancouver, BC, 2017, pp. 131–148.
[112] M. Castro, M. Costa, T. Harris, Securing software by enforcing data-flow integrity, in: Proceedings Of the 7th Symposium on Operating Systems Design and Implementation, USENIX Association, 2006, pp. 147–160.
[113] N. Ayewah, D. Hovemeyer, J.D. Morgenthaler, J. Penix, W. Pugh, Using static analysis to find bugs, IEEE Softw. 25 (5) (2008).
[114] P. Godefroid, M.Y. Levin, D.A. Molnar, et al., "Automated Whitebox Fuzz testing.'' in *NDSS*, vol. 8, 2008, pp. 151–166.
[115] J. Newsome, D.X. Song, "Dynamic Taint Analysis for Automatic Detection, Analysis, and Signaturegeneration of Exploits on Commodity software.'' in *NDSS*, vol. 5, Citeseer, 2005, pp. 3–4.
[116] J. Clause, W. Li, A. Orso, Dytan: a generic dynamic taint analysis framework, in: Proceedings Of the 2007 International Symposium on Software Testing and Analysis, ACM, 2007, pp. 196–206.
[117] C. Le Goues, T. Nguyen, S. Forrest, W. Weimer, Genprog: a generic method for automatic software repair, IEEE Trans. Software Eng. 38 (1) (2012) 54.
[118] Y. Shin, A. Meneely, L. Williams, J.A. Osborne, Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities, IEEE Trans. Software Eng. 37 (6) (2011) 772–787.
[119] H. Perl, S. Dechand, M. Smith, D. Arp, F. Yamaguchi, K. Rieck, S. Fahl, Y. Acar, Vccfinder: finding potential vulnerabilities in open-source projects to assist code audits, in: Proceedings Of the 22nd ACM SIGSAC Conference On Computer And Communications Security, ACM, 2015, pp. 426–437.
[120] Y. Zhou, A. Sharma, Automated identification of security issues from commit messages and bug reports, in: Proceedings Of the 2017 11th Joint Meeting On Foundations Of Software Engineering, ACM, 2017, pp. 914–919.
[121] L.K. Shar, L.C. Briand, H.B.K. Tan, Web application vulnerability prediction using hybrid program analysis and machine learning, IEEE Trans. Dependable Secure Comput. 12 (6) (2015) 688–707.
[122] G. Grieco, G.L. Grinblat, L. Uzal, S. Rawat, J. Feist, L. Mounier, Toward large-scale vulnerability discovery using machine learning, in: Proceedings Of the Sixth ACM Conference On Data And Application Security And Privacy, ACM, 2016, pp. 85–96.
[123] Y. Fan, Y. Ye, L. Chen, Malicious sequential pattern mining for automatic malware detection, Expert Syst. Appl. 52 (2016) 16–25.
[124] S. Huda, J. Abawajy, M. Alazab, M. Abdollalihian, R. Islam, J. Yearwood, Hybrids of support vector machine wrapper and filter based framework for malware detection, Future Generat. Comput. Syst. 55 (2016) 376–390.
[125] S. Huda, S. Miah, M.M. Hassan, R. Islam, J. Yearwood, M. Alrubaian, A. Almogren, Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data, Inf. Sci. 379 (2017) 211–228.
[126] Q.K.A. Mirza, I. Awan, M. Younas, Cloudintell: an intelligent malware detection system, Future Generat. Comput. Syst. (2017).
[127] R. Chen, D. Ma, A. Regan, Tari: Meeting Delay Requirements in Vanets with Efficient Authentication and Revocation, 01 2009.
[128] N. Chen, M. Gerla, Dynamic attributes design in attribute based encryption, in: Annual Conference Of ITA (ACITA), University of Maryland, MD, 2009.
[129] A. Alston, "Attribute-based encryption for attribute-based authentication, authorization, storage, and transmission in distributed storage systems,'' *CoRR*.
[130] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: R. Cramer (Ed.), Advances In Cryptology – EUROCRYPT 2005, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 457–473.
[131] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings Of the 13th ACM Conference On Computer And Communications Security, Ser. CCS '06, ACM, New York, NY, USA, 2006, pp. 89–98, https://doi.org/10.1145/1180405.1180418 [Online]. Available.
[132] N. Chen, M. Gerla, Dynamic Attributes Design in Attribute Based Encryption, 01 2009.
[133] M.T. Mamaghani, R. Abbas, On the Security and Reliability Performance of Two-Way Wireless Energy Harvesting Based Untrusted Relaying with Cooperative Jamming, *IET Communications*, 2018.
[134] L. Nkenyereye, B.A. Tama, Y. Park, K.H. Rhee, A fine-grained privacy preserving protocol over attribute based access control for vanets, JoWUA 6 (2015) 98–112.
[135] N. Kshetri, Can blockchain strengthen the internet of things, IT Profess. 19 (4) (2017) 68–72.
[136] A. Dorri, S.S. Kanhere, R. Jurdak, Towards an optimized blockchain for iot, in: 2017 IEEE/ACM Second International Conference on Internet-Of-Things Design and Implementation (IoTDI), April 2017, pp. 173–178.
[137] A. Dorri, S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for Iot Security and Privacy: the Case Study of a Smart Home, 03 2017.
[138] S. Dhaliwal, A.-A. Nahid, R. Abbas, Effective intrusion detection system using xgboost, Information 9 (7) (2018) 149.
[139] I. Butun, S.D. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 266–282.
[140] C. Miller, C. Valasek, A survey of remote automotive attack surfaces, Black Hat USA 2014 (2014).
[141] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, X. Cui, Attacks and countermeasures in the internet of vehicles, Ann. Telecommun. 72 (5–6) (2017) 283–295.
[142] S. Sharma, A. Kaul, A Survey on Intrusion Detection Systems and Honeypot Based Proactive Security Mechanisms in Vanets and Vanet Cloud, *Vehicular Communications*, 2018.
[143] H. Sedjelmaci, S.M. Senouci, M.A. Abu-Rgheff, An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks, IEEE Internet Things J. 1 (6) (2014) 570–577.
[144] M. Dibaei, A. Ghaffari, Tsis: a trust-based scheme for increasing security in wireless sensor networks, Majlesi J. Electr. Eng. 11 (4) (2017) 45–52.
[145] S. Sharma, A. Kaul, Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized ids for vanet, Vehicul. Commun. 12 (2018) 23–38.
[146] O.A. Wahab, A. Mourad, H. Otrok, J. Bentahar, Ceap: svm-based intelligent detection model for clustered vehicular ad hoc networks, Expert Syst. Appl. 50 (2016) 40–54.
[147] H. Sedjelmaci, S.M. Senouci, N. Ansari, A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks, IEEE Trans. Syst. Man Cybern.: Systems (2017).
[148] T. Zhang, Q. Zhu, Dynamic differential privacy for admm-based distributed classification learning, IEEE Trans. Inf. Forensics Secur. 12 (1) (2017) 172–187.
[149] R. She, S. Liu, S. Wan, K. Xiong, P. Fan, Importance of small probability events in big data: information measures, applications, and challenges, IEEE Access 7 (2019) 100 363–100 382.
[150] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H.M. Zhang, J. Rowe, K. Levitt, Security vulnerabilities of connected vehicle streams and their impact on cooperative driving, IEEE Commun. Mag. 53 (6) (2015) 126–132.
[151] A.D. Kumar, K.N.R. Chebrolu, S. Kp, et al., A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities, 2018 *arXiv preprint arXiv: 1810.04144*.

[152] S.A. Kumar, T. Vealey, H. Srivastava, Security in internet of things: challenges, solutions and future directions, in: 2016 49th Hawaii International Conference On System Sciences (HICSS), IEEE, 2016, pp. 5772–5781.
[153] E. Bertino, N. Islam, Botnets and internet of things security, Computer (2) (2017) 76–79.
[154] L. Xiao, X. Wan, X. Lu, Y. Zhang, D. Wu, Iot security techniques based on machine learning: how do iot devices use ai to enhance security? IEEE Signal Process. Mag. 35 (5) (2018) 41–49.
[155] J. Pewny, B. Garmany, R. Gawlik, C. Rossow, T. Holz, Cross-architecture bug search in binary executables, in: In Security And Privacy (SP), 2015 IEEE Symposium On, IEEE, 2015, pp. 709–724.
[156] S. Wen, Q. Meng, C. Feng, C. Tang, Protocol vulnerability detection based on network traffic analysis and binary reverse engineering, PloS One 12 (10) (2017), e0186188.
[157] A. Henderson, L.K. Yan, X. Hu, A. Prakash, H. Yin, S. McCamant, Decaf, A platform-neutral whole-system dynamic binary analysis platform, IEEE Trans. Software Eng. 43 (2) (2017) 164–184.
[158] M. Luo, O. Starov, N. Honarmand, N. Nikiforakis, Hindsight: understanding the evolution of ui vulnerabilities in mobile browsers, in: Proceedings Of the 2017 ACM SIGSAC Conference On Computer And Communications Security, ACM, 2017, pp. 149–162.
[159] N. Stephens, J. Grosen, C. Salls, A. Dutcher, R. Wang, J. Corbetta, Y. Shoshitaishvili, C. Kruegel, G. Vigna, Driller: augmenting fuzzing through selective symbolic execution, in: In NDSS, 16, 2016, pp. 1–16.
[160] S.M. Ghaffarian, H.R. Shahriari, Software vulnerability analysis and discovery using machine-learning and data-mining techniques: a survey, ACM Comput. Surv. 50 (4) (2017) 56.
[161] P. Sinha, Architectural design and reliability analysis of a fail-operational brake-by-wire system from iso 26262 perspectives, Reliab. Eng. Syst. Saf. 96 (10) (2011) 1349–1359.
[162] K.E. Hodge, Y. Kellogg, Proceedings of the F-8 Digital Fly-By-Wire and Supercritical Wing First Flight's 20th Anniversary Celebration, vol. 2, bibliography appendices, 1996.
[163] S. Khurshid, C.S. Păsăreanu, W. Visser, Generalized symbolic execution for model checking and testing, in: International Conference On Tools And Algorithms For the Construction And Analysis Of Systems, Springer, 2003, pp. 553–568.
[164] P. Emanuelsson, U. Nilsson, A comparative study of industrial static analysis tools, Electron. Notes Theor. Comput. Sci. 217 (2008) 5–21.
[165] T. Ji, Y. Wu, C. Wang, X. Zhang, Z. Wang, The coming era of alphahacking?: a survey of automatic software vulnerability detection, exploitation and patching techniques, in: 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), IEEE, 2018.
[166] Toyota itc benchmark — runtime verification match documentation [Online]. Available, https://runtimeverification.com/match/1.0-SNAPSHOT/docs/benchmark/, 2019.
[167] Mechatronics [accessed on 22-june-2019]. [Online]. Available, http://www.mobistc-na.com/rd/mechatronics/advanced.
[168] T. Hepher, Boeing says successfully tested new 737 max software in ceo flight [Online]. Available, https://www.reuters.com/article/us-ethiopia-airplane-boeing-test/boeing-says-successfully-tested-new-737-max-software-in-ceo-flight-idUSKCN1RF2MD, 2019.
[169] G. McGraw, Software security, IEEE Secur. Privac. 2 (2) (2004) 80–83.
[170] M. Abadi, M. Budiu, U. Erlingsson, J. Ligatti, Control-flow integrity, in: Proceedings Of the 12th ACM Conference on Computer And Communications Security, ACM, 2005, pp. 340–353.
[171] W. Wögerer, "A survey of static program analysis techniques,'' Citeseer, Tech. Rep. (2005).
[172] A. Takanen, J.D. Demott, C. Miller, Fuzzing for Software Security Testing and Quality Assurance, Artech House, 2008.
[173] E.J. Schwartz, T. Avgerinos, D. Brumley, All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask), in: Security And Privacy (SP), 2010 IEEE Symposium on, IEEE, 2010, pp. 317–331.
[174] L. Deng, J. Offutt, P. Ammann, N. Mirzaei, Mutation operators for testing android apps, Inf. Software Technol. 81 (2017) 154–168.
[175] D. Lin, J. Zhang, W. Luo, L. Pan, A. Xiang, O. De Vel, P. Mont, Cross-project transfer representation learning for vulnerable function discovery, in: IEEE Transactions on Industrial Informatics, 2018.
[176] Z. Li, D. Zou, S. Xu, X. Ou, H. Jin, S. Wang, Z. Deng, Y. Zhong, Vuldeepecker: A Deep Learning-Based System for Vulnerability Detection, 2018 *arXiv preprint arXiv: 1801.01681*.
[177] Q. Luo, J. Liu, Wireless telematics systems in emerging intelligent and connected vehicles: T hreats and solutions, IEEE Wireless Commun. (99) (2018) 1–7.
[178] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2flip: a two-factor lightweight privacy-preserving authentication scheme for vanet, IEEE Trans. Veh. Technol. 65 (2) (2016) 896–911.
[179] S. Maro, J.-P. Steghöfer, M. Staron, Software traceability in the automotive domain: challenges and solutions, J. Syst. Software 141 (2018) 85–110.
[180] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET, IEEE Trans. Veh. Technol. 65 (2) (2016) 896–911, https://doi.org/10.1109/TVT.2015.2402166 [Online]. Available.
[181] B. Alpern, F.B. Schneider, Key exchange using 'keyless cryptography', Inf. Process. Lett. 16 (2) (1983) 79–81, https://doi.org/10.1016/0020-0190(83)90029-7 [Online]. Available.
[182] C. Castelluccia, P. Mutaf, Shake them up!: a movement-based pairing protocol for cpu-constrained devices, June 6-8, 2005, , in: K.G. Shin, D. Kotz, B.D. Noble (Eds.), Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services, MobiSys 2005, , ACM, Seattle, Washington, USA, 2005, pp. 51–64, https://doi.org/10.1145/1067170.1067177 [Online]. Available.
[183] R.D. Pietro, G. Oligeri, ESC: an efficient, scalable, and crypto-less solution to secure wireless networks, Comput. Network. 84 (2015) 46–63, https://doi.org/10.1016/j.comnet.2015.04.006 [Online]. Available.
[184] Y. Zhang, Y. Xiang, T. Wang, W. Wu, J. Shen, An over-the-air key establishment protocol using keyless cryptography, Future Generat. Comput. Syst. 79 (2018) 284–294, https://doi.org/10.1016/j.future.2016.12.013 [Online]. Available.
[185] D. Tsonev, H. Chun, S. Rajbhandari, J.J. McKendry, S. Videv, E. Gu, M. Haji, S. Watson, A.E. Kelly, G. Faulkner, M.D. Dawson, H. Haas, D.O. Brien, A 3-Gb/s single-LED OFDM-based wireless VLC link using a gallium nitride μLED, IEEE Photon. Technol. Lett. 26 (7) (2014) 637–640.
[186] H. Haas, L. Yin, Y. Wang, C. Chen, What is LiFi? J. Lightwave Technol. 34 (6) (2016) 1533–1544.
[187] N.A. Abdulsalam, R.A. Hajri, Z.A. Abri, Z.A. Lawati, M.M. Bait-Suwailam, Design and implementation of a vehicle to vehicle communication system using Li-Fi technology, in: Information And Communication Technology Research (ICTRC), 2015 International Conference On, IEEE, 2015, pp. 136–139.
[188] P. Bhateley, R. Mohindra, S. Balaji, Smart vehicular communication system using LiFi technology, in: Computation Of Power, Energy Information And Commuincation (ICCPEIC), 2016 International Conference On, IEEE, 2016, pp. 222–226.
[189] M. Gupta, S. Sharma, Infrastructure-less vehicular communication system using Li-Fi technology, Int. J. Comput. 23 (1) (2016) 53–60.
[190] F.A. Dahri, H.B. Mangrio, A. Baqai, F.A. Umrani, Experimental evaluation of intelligent transport system with VLC vehicle-to-vehicle communication,'' *Wireless Personal Communications* [Online]. Available, https://doi.org/10.1007/s11277-018-5727-0, Apr 2018.
[191] 3GPP, 3rd generation partnership project; technical specification group services and system aspects; security aspect for lte support of vehicle-to-everything (v2x) services (release 15), 3GPP TS 33.185 16 (2018).
[192] P. Luoto, M. Bennis, P. Pirinen, S. Samarakoon, K. Horneman, M. Latva-aho, Vehicle clustering for improving enhanced lte-v2x network performance, in: Networks And Communications (EuCNC), 2017 European Conference On, IEEE, 2017, pp. 1–5.
[193] 3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Enhancement of 3gpp Support for 5g V2x Services (Release 16), vol. 16, 2018. *3GPP TS 33.185*.
[194] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (7553) (2015) 436.
[195] X. Zheng, Physically informed assertions for cyber physical systems development and debugging, in: Pervasive Computing And Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference On, IEEE, 2014, pp. 181–183.
[196] X. Zheng, C. Julien, M. Kim, S. Khurshid, Perceptions on the state of the art in verification and validation in cyber-physical systems, IEEE Syst. J. 11 (4) (2017) 2614–2627.
[197] X. Zheng, C. Julien, H. Chen, R. Podorozhny, F. Cassez, Real-time simulation support for runtime verification of cyber-physical systems, ACM Trans. Embed. Comput. Syst. 16 (4) (2017) 106.
[198] X. Zheng, C. Julien, R. Podorozhny, F. Cassez, T. Rakotoarivelo, Efficient and scalable runtime monitoring for cyber–physical system, IEEE Syst. J. 12 (2) (2018) 1667–1678.
[199] X. Zheng, C. Julien, R. Podorozhny, F. Cassez, Braceassertion: runtime verification of cyber-physical systems, in: Mobile Ad Hoc And Sensor Systems (MASS), 2015 IEEE 12th International Conference On, IEEE, 2015, pp. 298–306.
[200] X. Sun, N. Ansari, Edgeiot: mobile edge computing for the internet of things, IEEE Commun. Mag. 54 (12) (2016) 22–29.
[201] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proceedings Of the First Edition of the MCC Workshop on Mobile Cloud Computing, ACM, 2012, pp. 13–16.
[202] T. Zheng, X. Zheng, Y. Zhang, Y. Deng, E. Dong, R. Zhang, X. Liu, Smartvm: a Sla-Aware Microservice Deployment Framework, *World Wide Web*, 2018, pp. 1–19.
[203] Y.C. Hu, M. Patel, D. Sabella, N. Sprecher, V. Young, Mobile edge computing—a key technology towards 5g, ETSI White Pap. 11 (11) (2015) 1–16.