Ad Hoc Networks 90 (2019) 101823

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

A review on safety failures, security attacks, and available countermeasures for autonomous vehicles

Jin Cui*, Lin Shen Liew, Giedre Sabaliauskaite*, Fengjun Zhou

iTrust Centre, Singapore University of Technology and Design, Singapore 487372, Singapore

ARTICLE INFO

Article history:
Received 3 May 2018
Revised 14 November 2018
Accepted 6 December 2018
Available online 7 December 2018

Keywords:
Autonomous vehicle
Safety
Security
Failures
Attacks
Countermeasures
V2X communications
VANET
ITS

ABSTRACT

Autonomous vehicles (AVs) attract a lot of attention recently. They are expected to assist/replace the human drivers in maneuvering the vehicle, thereby reducing the likelihood of road accidents caused by human error, as a means to improve the road traffic safety. However, AVs have their inherent safety and security challenges, which have to be addressed before they are ready for wide adoption. This paper presents an overview of recent research on AV safety failures and security attacks, as well as the available safety and security countermeasures.

1. Introduction

Many people get seriously injured or even lose lives in road accidents due to human errors, including drivers' errors (e.g., driver's inattention and distraction, reckless driving, and poor driving skills), and other road users' errors (e.g., violations of traffic rules) [1]. Moreover, vehicle malfunction (e.g., brake failure), or environmental circumstances (e.g., insufficient road information or lack of security infrastructure) affect traffic safety as well [2]. To improve road traffic safety, a new type of vehicles has been introduced, known as Autonomous Vehicle (AV), which enables a driving automation system to replace human driver to control the vehicle with better recognition, decision and driving skills [3,4]. Furthermore, AVs can communicate with other vehicles, infrastructure and pedestrians, as they are enabled with the vehicle to everything (V2X) communication technology. Thus, the AVs, once widely deployed, are expected to reduce human errors, optimize traffic flow, and ultimately enhance overall safety and experience of road users [5,6].

AVs play significant role in assuring the safety of transportation systems. However, AVs have their inherent safety and security challenges. If one component of AV fails or is attacked, the in-vehicle network is impacted; then, the on-board computer ('brain' of AV) may issue the wrong command, and directly compromise traffic safety [7]. For example, failed or tampered GPS (Global Position System) data affects the localization of AV, and leads to traffic disturbance or crash hazard [8]. Furthermore, the wrong information will be exchanged between nearby AVs, which would be hazardous. Thus, safety and security are crucial in AVs. Any failures (safety issues) and/or attacks (security issues) may lead to major safety losses [9]. Adequate safety and security countermeasures (CMs) have to be implemented to prevent and/or mitigate failures and attacks.

The motivation behind this paper is to provide and in-depth analysis of the issues and available solutions related to AV safety and security in order to identify challenges and future research directions of AVs. The paper:

- provides and overview of AV safety failures and security attacks;
- reviews available safety and security countermeasures, applicable to AVs;
- identifies open issues, challenges, and future research directions.

AV safety and security is a broad topic. Therefore, admittedly, this work may not have fully or thoroughly covered all safety and security aspects of AV. More in-depth discussion on VANETs (Vehicular ad hoc networks) related security challenges and solutions

* Corresponding authors.
E-mail addresses: jin_cui@sutd.edu.sg (J. Cui), giedre@sutd.edu.sg (G. Sabaliauskaite).

https://doi.org/10.1016/j.adhoc.2018.12.006
1570-8705/

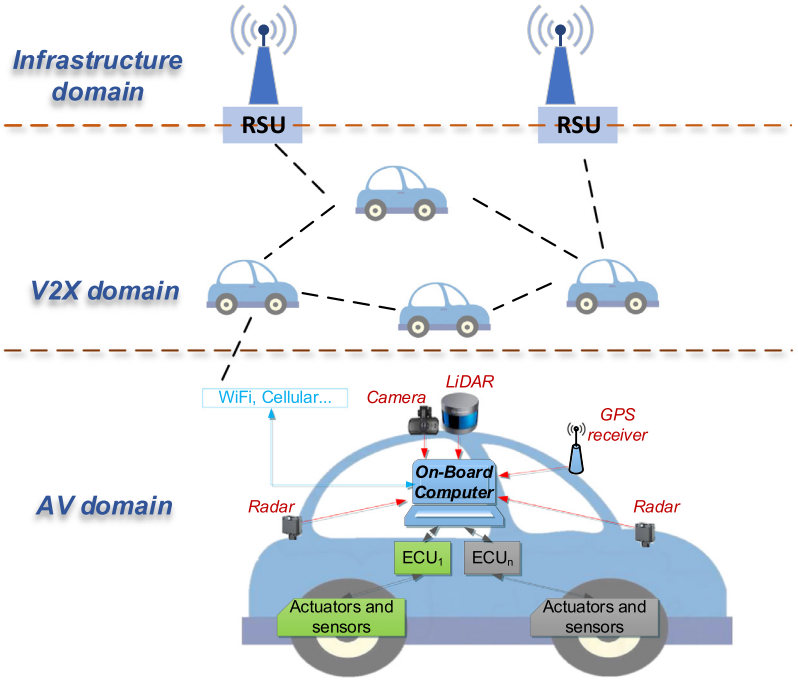

Fig. 1. AVs and their communications. (RSU - Road Side Unit; LiDAR - Light Detection and Ranging; ECU - Electronic Control Unit; GPS - Global Position System.).

can be found elsewhere [10–15]. ITS (Intelligent Transportation System) related problems and the corresponding cryptographic solutions are detailed in [16]. In [17], various cyberattacks on AV are investigated in terms of feasibility, severity, preventability, etc. Besides providing an overview of the AV related cybersecurity vulnerabilities and mitigation efforts, [18] also presents a list of knowledge gaps which may be used as a road-map to addressing the cybersecurity challenges in the connected and autonomous vehicle sector.

The aforementioned works mainly focus on security issues. However, in AVs, security and safety are inter-related, as both the failures and the attacks may lead to the safety losses. Thus, we discuss the safety failures, security attacks, and corresponding countermeasures collectively to provide a more comprehensive overview of state of the art and challenges of AVs as compared to the other studies.

The rest of paper is organized as follows. Section 2 describes the AVs and their communication networks. Section 3 summarizes the potential failures of AVs and describes the corresponding safety countermeasures. Section 4 presents the potential attacks on AVs and the associated countermeasures. Section 5 addresses the open issues, challenges, and future research direction, and finally, Section 6 concludes the paper.

2. Autonomous vehicle and its communication networks

According to standard SAE J3016 [19], there are six levels of autonomy to classify self-driving cars; these levels, which are basically a progression of self-driving features, range from 0 (having no self-driving features at all) to 5 (fully-autonomous driving). In general, AVs differ from conventional vehicles in the following ways: 1) relatively more sensors are equipped on AVs to perceive the surrounding environments; 2) the computer is to assume the role of the human driver in maneuvering the vehicle; 3) via V2X technology, AVs could communicate with any compatible systems including AVs, infrastructure and pedestrians. Note that the term V2X encompasses V2V, V2I and V2P; V2V refers to Vehicle-to-Vehicle; V2I - Vehicle-to-Infrastructure; V2P - Vehicle-to-Pedestrian [20].

Fig. 1 illustrates the major components of an AV as well as the communication between AVs and other systems (e.g., Roadside Unit). The AV's sensors such as radar, camera, and LiDAR (Light Detection and Ranging) are responsible for sensing vehicle's dynamics (e.g., location and speed) as well as its immediate environment (e.g., distances to neighboring vehicles, road traffic conditions, and traffic signs) [21,22]. The on-board computer processes this information and then commands the ECUs, which control their corresponding actuators accordingly to achieve desired movement speed and direction. The connections between on-board computer, external sensors, ECUs, and actuators form an in-vehicle network (also called the on-board network). Global Navigation Satellite System (GNSS) is often used by AVs to obtain accurate location information.

As AVs are network-enabled, the failures and attacks on an AV could also affect the connected ones. The network formed among vehicles and infrastructure via V2V and V2I communications is known as VANET (Vehicular ad hoc network) [23,24]. VANET enables the information to be relayed among the connected cars and infrastructure.

VANETs are key parts in the Intelligent Transportation System (ITS) framework [25,26]. The ITS shall integrate and analyze the shared information in order to optimize the traffic management for improved safety, efficiency and mobility of the transportation system. For example, ITS can dispatch vehicles away from congested areas, and dynamically adjust the road speed limits at on-peak and off-peak times.

3. Potential failures of AVs and available safety countermeasures

The failures that may jeopardize the AVs and the road users can be categorized into two groups [27,28]: 1) failures related to AV components (VF); 2) failures related to infrastructure (IF). Fig. 2 shows the composition of VF: *VF1* - hardware system failures (e.g., integration platform failure, sensor failures, actuator failure and controller failure), *VF2* - software failures, *VF3* - vehicle mechanical failures, *VF4* - failures of the communication system

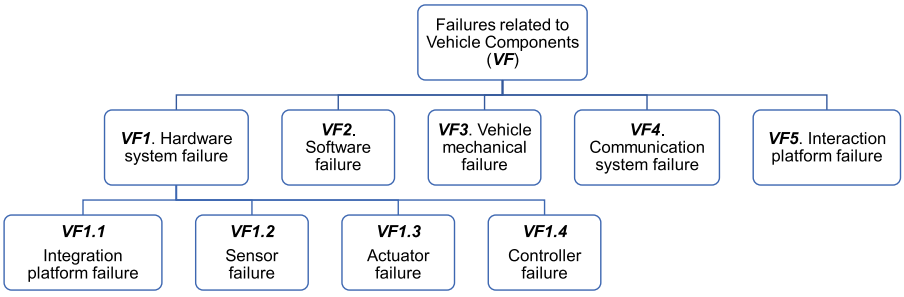

Fig. 2. Failures related to AV components.

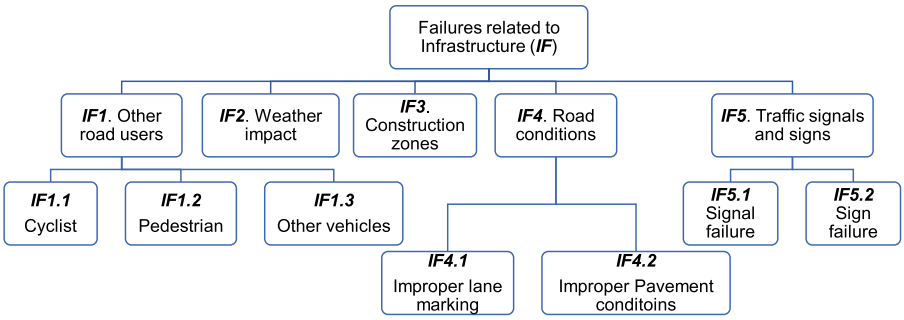

Fig. 3. Failures related to transportation infrastructure.

(e.g., V2X communication system, in-vehicle communication system), and *VF5* - interaction platform failure (e.g., wrong human command, or system fails to detect human command). *VF*s affect the AV performance and could endanger road users' safety.

Based on the traffic safety information analysis [29–31], failures related to infrastructure, *IF*, include the failures of *IF*1 - other road users (e.g., cyclist, pedestrian, other vehicles on the road), *IF*2 - weather, *IF*3 - construction zones, *IF*4 - road conditions (e.g., improper lane marking, and improper pavement conditions), and *IF*5 - traffic signals and signs (e.g., traffic signal failure, and traffic sign failure), as shown in Fig. 3. *IF* affects the driving environments, such as reducing visible area, bad pavement conditions, and unsafe traffic signs, thereby increasing the possibility of road accidents. Safety countermeasures (CMs) are the technologies or policies, which may reduce the likelihood of safety failures, or mitigate the failures. CMs can be classified into two groups: 1) CMs that can be applied on the infrastructure; 2) CMs that can be applied on the vehicle. AV safety failures and the corresponding countermeasures are shown in Fig. 4. The following subsections describe safety countermeasures in more detail.

3.1. Safety countermeasures applicable to infrastructure

[32–35] describe several safety CMs that have been proposed and/or implemented. Based on the countermeasure location, this type of CM can be further classified into intersection-based and segment-based countermeasures [36]. Fig. 4 shows the safety countermeasures and related failures.

3.1.1. Segment-based countermeasures

Segment-based CMs include the safety measures that can be achieved on the road segment:

- Speed limit reduction: Lowering the speed limit could reduce the likelihood of speeding. This can be a CM for *IF5.2* traffic sign failure.
- Pedestrian barrier is installed on the roadway medians or verges to prevent the pedestrian from crossing the roadway recklessly. This can be a CM for *IF1.2* pedestrian misbehavior.
- Bus lane, a separate lane for bus, which could improve the bus travel by reducing the delays caused by other traffic. This can be a CM for *IF1* other road user misbehavior (i.e., bus misbehavior). In addition, reasonable bus lane is proper lane marking to lessen conflict/interaction between buses and cars and lessen traffic congestion, which improve the road conditions (CM for *IF*4).
- Bike lane could ease the cyclists by reducing the delays caused by other traffic. This can be a CM for *IF*1.1 cyclist misbehavior. Similar to bus lane, bike lane can also be considered as CM for *IF*4.
- Speed bump, which is intended to vertically deflect the vehicle, thereby reducing its movement speed. If a road-side sign of slow speed is broken or missing, the speed bump can be considered as alternative sign for vehicles, i.e., a CM to mitigate the impact of *IF*5.2 sign failure.
- Construction zone sign is intended to notify and keep the road users away from the construction zone. This sign is necessary for *IF*3 construction zone. More construction zone signs along road side is helpful to decrease the impact of *IF*5.2.

3.1.2. Intersection-based countermeasures

Intersection-based CMs are the safety measures, which can be achieved on intersection [37]:

- Split phase timing: the division of a signal phase of one direction shared by through traffic, turning vehicles, and crossing pedestrians into two protected phases: a protected pedestrian crossing phase and a protected vehicle turning phase. This measure is used for mitigating *IF*1.2 pedestrian misbehavior, and decreasing the impact of *IF*5.2 traffic signal failure.
- Left-turn phase, which changes the signal phasing from permissive to protected/permissive or protected-only, which can be considered to ease *IF*1.2 pedestrian misbehavior, and reduce the impact of *IF*5.1 signal failure.
- Increasing pedestrian crossing time: an increase in the length of signal phases on the main and/or cross streets so that pedestrians have more time crossing streets. This way can be used to

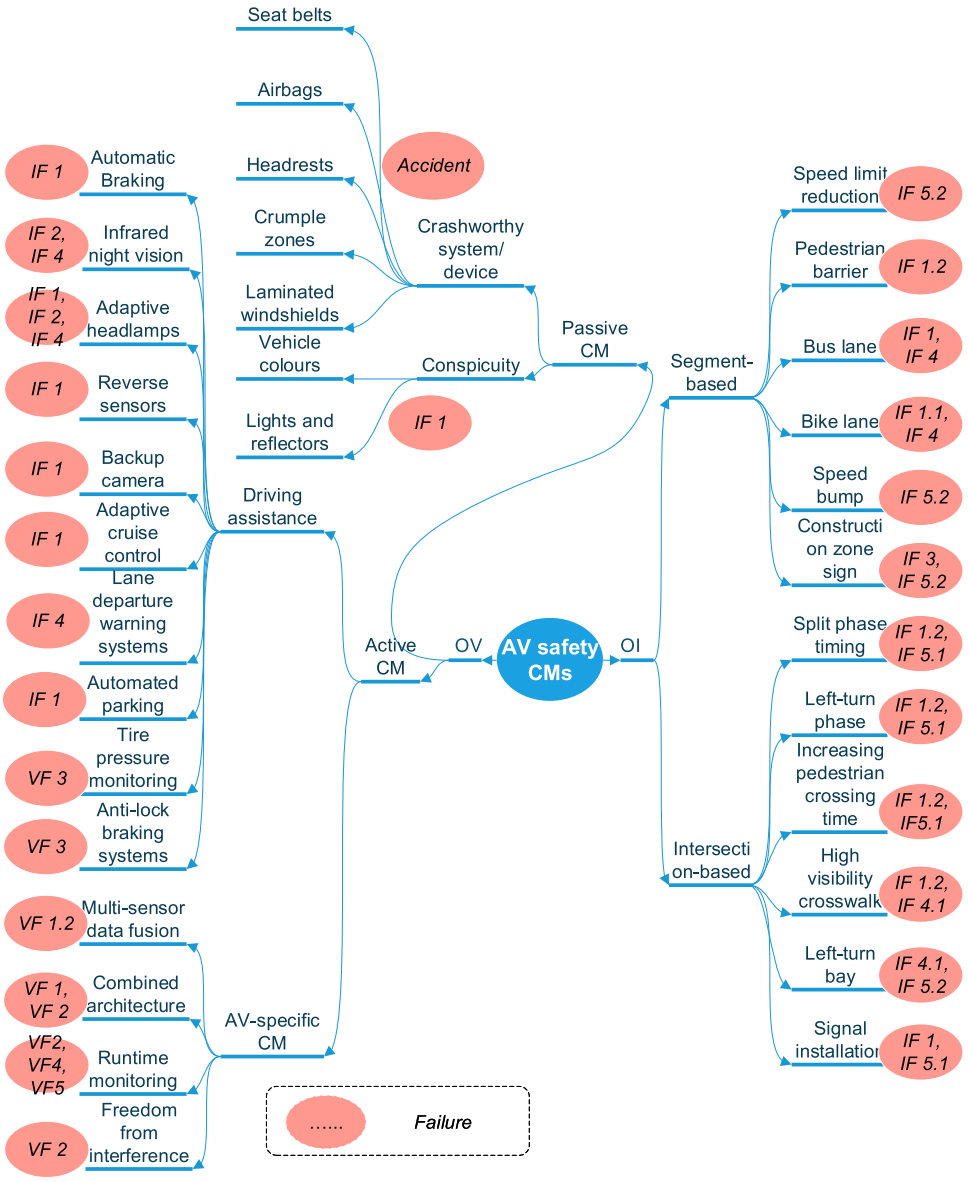

Fig. 4. AV safety countermeasures and the corresponding failures. (VF - vehicle component failures; IF - infrastructure failures; OV - countermeasures applied On Vehicle; OI - countermeasures applied On Infrastructure).

mitigate *IF*1.2 pedestrian misbehavior, and conquer *IF*5.1 traffic signal failure.

- High visibility crosswalk. A crosswalk with series of longitudinal white stripes, intended to increase awareness of pedestrians at intersections by using highly visible marking patterns. This CM is used for mitigating *IF*1.2 pedestrian misbehavior, and improving road condition to lighten *IF*4.1.
- Left-turn bay: a storage area of some length for left-turning vehicles at an intersection, reducing the need for through traffic to decelerate or change lanes near the intersection in order to by-pass left-turning vehicles. This bay can make the road marking better to overcome *IF*4.1 improper lane marking and *IF*5.2 traffic sign failure.
- Signal installation can reduce the likelihood of *IF*1 road users misbehavior. Reasonable and dense signal installation can decrease the probability of *IF*5.1 traffic signal failure.

3.1.3. Effectiveness of infrastructure safety countermeasures

The US highway safety manual [38] points out that proper countermeasures applied on the infrastructure can effectively reduce road accidents. For example, pedestrian barrier and high visibility crosswalk reduce 71% of crashes involving pedestrians walking along roadways. Left-turn bay and phase reduce 54% in injury and fatal crashes in Missouri [39] and 30% in intersection-related injury crash rate [40]. Split phase timing and increasing pedestrian crossing time brings 60% reduction in pedestrian-vehicle crashes at intersections [41].

3.2. Safety countermeasures applicable to vehicle

Corresponding to active safety and passive safety, the countermeasures applied on the vehicle also can be classified into active and passive ones, as shown in Fig. 4. Active CMs provide active safety features, which aim to prevent the vehicle from crashing, while passive CMs serve to protect the vehicle users during a crash. Active CMs include several driving assistance methods and AV specific countermeasures. Passive CMs consist of crash-worthy system or devices and the conspicuity of vehicle.

Table 1
Description of several driving assistance methods.

CM	Description of CM	Targeted failures
Automatic braking [49]	Activate the vehicle's brake system automatically when necessary	*IF1*
Night-vision system [50]	Uses a thermo-graphic camera to improve the visibility on the things ahead of the vehicle especially in darkness and poor weather	*IF2*, *IF4*
Adaptive headlamps [51]	Adjust the headlamps' angle automatically for better visibility on the road	*IF1, IF2, IF4*
Reverse sensors [52]	Notify the driver when there is an obstacle behind the vehicle during reversing	*IF1*
Backup camera [53]	Improve rear visibility to avoid collision while reversing	*IF1*
Adaptive cruise control [54]	Adjust surrounding vehicle's speed and distance accordingly to keep the vehicle at a safe distance from the traffic ahead and neighboring	*IF1*
Lane departure warning systems [55]	Alert the driver when the vehicle leaves the lane unintentionally	*IF4*
Automatic parking [56]	Help maneuver the vehicle from a traffic lane into a parking spot to perform parallel, perpendicular, or angle parking	*IF1*
Tire pressure monitoring [57]	Notify the drive when the pneumatic tire of the vehicle is significantly under-inflated	*VF3*
Anti-lock braking system [58]	Avoid the vehicle from uncontrolled skidding by preventing its wheel from locking up while braking	*VF3*

3.2.1. Active countermeasures

Active countermeasures can be classified into driving assistance methods and AV-specific methods, as shown in Fig. 4. Driving assistance technologies can be used for conventional vehicles and AVs. Table 1 demonstrates several driving assistance methods and their targeted failures.

Besides the driving assistance technologies, AV-specific countermeasures are also proposed. As discussed in [42], no single type of sensors (e.g., radar, camera, and LiDAR) should work well in sensing the surroundings in all kinds of conditions, thus additional/redundant sensors/data would lead to more reliable estimation. Thus, multi-sensor fusion is required in AVs [43,44]. With redundant information, measurement precision can be enhanced. In addition, with multi-sensor fusion, *VF*1.2 sensor failure can be mitigated to some extent. To achieve multi-sensor fusion on AVs, combined centralized and distributed architectures for hardware and software are needed [45]. Such architectures can also help alleviate *VF*1 hardware failure and *VF*2 software failure. Freedom From Interference (FFI) can be a CM for *VF2*, as it ensures that a fault in a less safety critical software component would not cause a fault in a more safety critical component. FFI can be achieved by applying task monitors, watchdog timer, or some other software [46]. Runtime Monitoring observes and checks if there is any violations of some well-defined properties in the system; the detected violations ought to be tackled accordingly, thus it can be used to detect software failures (as CM for *VF*2), communication system failure (as CM for *VF*4), and interaction platform failure (as CM for *VF*5) [47,48].

3.2.2. Passive countermeasures

Passive CMs aim to provide passive safety features, e.g., to keep the driver and passengers protected within the vehicle from various crash forces [59]. Modern vehicles contain what engineers sometimes refer to as a life space. The life space is a protected area around vehicle users (i.e., driver or passengers) within which the chances of escaping a crash with minimal injuries are more likely [60]. Passive CMs work to ensure that this life space is as safe as possible, and that vehicle users remain in this space throughout the crash. Crash-worthy system/device is one type of passive CMs. Crumple zone, seat belt, airbag, headrest and laminated windshield are common examples of crash-worthy system/devices. Crumple zone help to absorb and distribute crash forces before they reach the passenger and driver's seat. Similarly, seat belts, airbags, and headrests help keep the driver and passengers stationary within the life space of the vehicle. Laminated glass is strong enough to keep flying objects from penetrating a vehicle's windshield and hurting vehicle users.

Vehicle conspicuity, such as vehicle's color, lights and reflectors, is another type of passive CMs. The conspicuity can make other road users aware of the vehicle, committed to reducing other road users' error. Thus, conspicuity can be CM for *IF*1. Underwood et al. study how conspicuity influences drivers' attention and manoeuvring decisions in a T-junction [61], and point out that high saliency vehicles make the road users have higher percentage of decisions that it would be safety to pull into the junction, and with less decision time.

3.3. Higher level insights into AV safety

From the overview of safety failures and corresponding safety countermeasures, presented in this section, we can derive the following insights:

- current research focuses mostly on regular vehicles, while the safety of AV is not adequately addressed yet. In particular, more effort should be paid on analysis of AV software failures and possible consequences;
- most of the currently available safety countermeasures are applicable to AVs. However, there is a lack of information on their effectiveness. We were able to find some information on the effectiveness of infrastructure safety countermeasures (see Section 3.1.3), however the effectiveness of the countermeasures applicable to AVs is not evaluated yet;
- AV manufacturers are responsible for development of safety countermeasures applicable to AVs. However, the development of countermeasures applicable to infrastructure requires more effort from governments and regulators. Finally, as the road users, the public should obey the traffic signs and rules, jointly maintaining the traffic safety.

4. Potential attacks on AVs and available security countermeasures

In-vehicle communication and V2X communication are crucial to ensure the functionality of AV. However, they are vulnerable to various security attacks. Fig. 5 shows the channels by which the attacks could land on the AV. Apparently, the attack surface increases as the network expands. In Fig. 5, all the connections to V2X network can be attacked. Regarding the in-vehicle communication, the connections under controller network (e.g., the connections between CAN Bus and ECUs, the ECUs inter-connections, the connections between ECUs and actuators, and internal sensors and actuators themselves) can be attacked. Moreover, the connections to on-board computer, which include physical connections (e.g., Ethernet, USB to sensors, HMI and brought-in devices) and wireless connections (e.g., WiFi to other devices/interfaces), cause a greater possibility of attack. Relevant attacks and corresponding countermeasures are discussed in the following subsections.

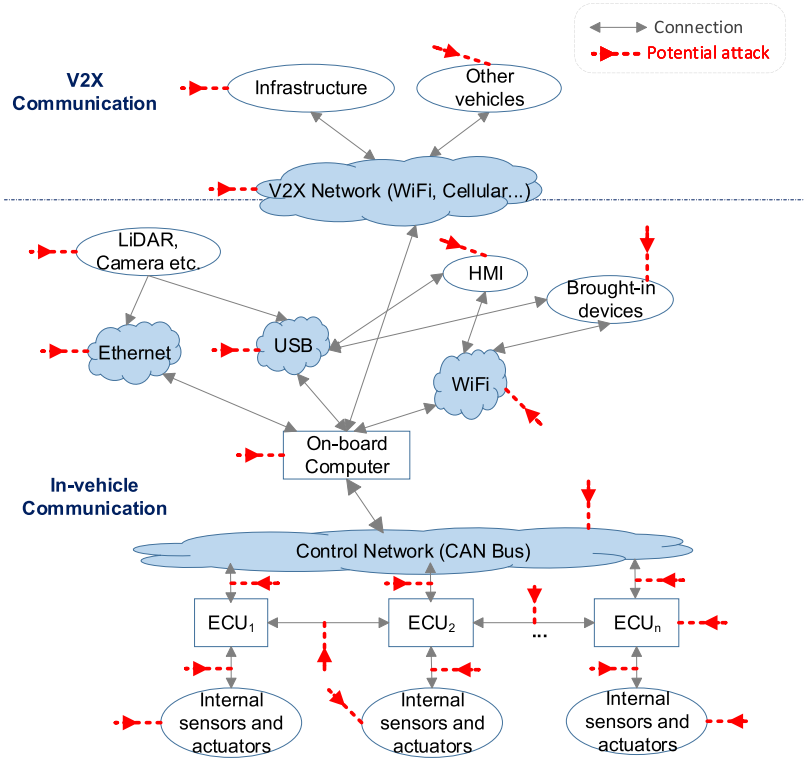

Fig. 5. Potential attacks on AV and AV communication networks.

The main security requirements with respect to AVs, VANETs and ITS are as follows [62–65]:

1) Authenticity/identification. The user, source and location must be authentic. User authentication is to prevent falsified entities attacks. Source authentication is to ensure that the data are generated by legitimate entities. Location authentication is to ensure the integrity and relevance of the received information.
2) Availability. The exchanged or shared information must be processed and made available in real time.
3) Data integrity/data trust. The received data must be free from malicious or unauthorized modification, manipulation or deletion during transmission.
4) Confidentiality/privacy. The exchanged data must not be disclosed to malicious or unauthorized users.

The attackers may be active or passive, external or internal, and malicious or rational, as described in [66]. Active attacker sends malicious packets to harm other nodes in the network, while passive attacker often eavesdrop on the communication inside the network to obtain useful information. External attackers are usually not authenticated, and and they mainly aim to compromise the confidentiality and availability of the system, whereas internal attackers are parts of the network and can perpetrate any kinds of attacks. Malicious attackers seek no personal benefits but would employ any means to jeopardize the network, while rational attackers seek personal benefit and their attack means and targets are relatively predictable.

4.1. Security attacks on AV network and corresponding countermeasures

The V2X communication technology enables the AVs to exchange/share information among themselves and any compatible systems, but also introduce security vulnerabilities. In this section, we discuss the attacks for AV communication networks and corresponding countermeasures.

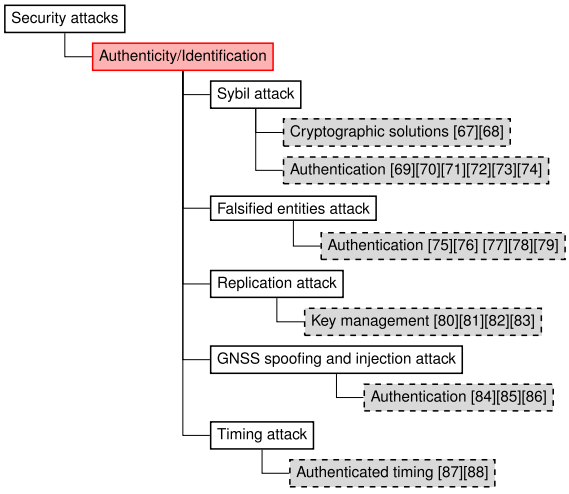

Fig. 6. Security attacks on Authenticity/identification and their corresponding countermeasures.

4.1.1. Authenticity/identification attacks and related countermeasures

Authenticity is a prime requirement in AV networking to ensure the protection of the legitimate in-network entities against several attacks, including spoofing and replay attacks. The common countermeasure for such attacks is authentication and cryptographic scheme. Any flaws in the process of authentication/identification may cause serious consequences to the entire network. Cryptographic scheme allows the receivers to verify the origin of the exchanged data. Some examples of authenticity attacks and their corresponding countermeasures (as shown in Fig. 6) are as follows:

- *Sybil attack*: In the context of VANETs, sybil attack [89–91] means that a malicious vehicle transmits the various messages with multiple fake or stolen source identities to other

nodes (e.g., AVs, or RSUs) in the network. Therefore legitimate/authenticated nodes consider the malicious messages to be legitimate and cannot detect the real identities of the attackers. To overcome this attack, the truth of an attribute of a single piece of message claimed true by any entity, should be confirmed using cryptographic scheme [67,68]. Moreover, the authentication process should be further strengthened [69–74]. For example, in [74], public-key cryptography is introduced into the pseudonym generation so that the legitimate third parts can obtain the vehicles' real IDs.

- *Falsified entities attack* means that the attacker passes information to the legitimate nodes through a valid network identifier [92]. The network identifier is the certificate of AV/RSU required for exchanging data in the network. Thus, the falsified entities construct a violation of the authentication process. This attack can be prevented by using more powerful authentication schemes, such as [75–79]. In [75], the RSU is utilized in verifying the message and notifying the results to the vehicle. Horng et al. [76] improves secure and privacy enhancing communication schemes to achieve security and privacy together. Lin and Li [93] proposes that the vehicles within the VANET must provide the authentication proofs and somewhat contribute to the cooperative authentication protocol before they are allowed to benefit from other vehicles' information. Hao et al. [94] and Shen et al. [95] present cooperative message authentication protocols to alleviate vehicle's computation burden.
- *Replication attack* means one or more nodes claiming an legitimate identity with duplicate keys/certificates [96]. Several key management schemes have been proposed, such as [80–83]. Taking [80] as an example, the key is generated by pairing-free certificated-less hybrid subscription scheme, which supports key update and revocation with forward and backward key secrecy.
- *GNSS spoofing and injection attack* is to falsify the location information with counterfeit signals. Moreover, successful GNSS spoofing attack can facilitate other attacks. This type of attack can be prevented by using encryption-based technology, signal-process based methods and authenticated location information [84–86].
- *Timing attack* is to delay the transmission of the message. A delayed message is hazardous especially for time-critical applications [67,97]. This attack can be prevented by using authenticated timing methods [87,88]. Based on the concept of transitive trust relationships, [87] propose a lightweight authentication scheme to mitigate timing attack.

4.1.2. Availability attacks and related countermeasures

The requirement of availability is mandatory to ensure the safety of the involved drivers and vehicles. Due to the major impact on the network resources, DoS attacks are commonly recognized as the most serious threat to the availability of vehicle-related systems. Authentication, detection and cryptographic solutions are usually employed to counter such attacks. In the following, several attacks on availability (as shown in Fig. 7) and their corresponding CMs are described.

- *Jamming attack* is to emit an interference signal to disrupt the communication channel [104]. Countermeasures for this attack include channel switching, technology switching, frequency hopping and utilizing multiple radio transceiver [86], and detection [98].
- *Flooding attack* is to impede the communication channel by flooding it with a huge volume of dummy messages generated by malicious nodes [105]. Authentication schemes are typically employed to fend off the malicious nodes, thereby preventing the flooding attack [64].

Fig. 7. Security attacks on availability and their corresponding countermeasures.

- *Malware attack* is to jeopardize the network or software components of the system (e.g., AV and RSU) via any form of hostile or intrusive software like computer viruses [106]. Such attack can be mitigated by using anti-malware software and firewall [99].
- *Spamming attack* is to send unsolicited message in bulk through the network, thereby increasing the transmission latency [106]. This attack can be mitigated by using appropriate authentication and detection schemes [97].
- *Denial of Service (DOS) attack*: major purpose behind a DoS attack is to prevent legitimate entities from accessing the network services and resources [107]. The aforementioned spamming attack and flooding attack are example types of DoS attack. It can also be known as DDOS (Distributed Denial of Service), when multiple computers and/or Internet connections are used to launch the attack. Authentication and packet filtering can limit the effects of DoS attacks [100]. He et al. propose a pre-authentication scheme, which taking advantage of the one-way hash chain and a group re-keying method to mitigate DoS attack in [101]. Verma et al. designs a data structure to filter packets and detect abrupt change, thereby avoiding DoS attack in [102].
- *Wormhole attack* means that the packets captured at one region of the network are transmitted to another region of the network. This would confuse the routing mechanisms where the accuracy of the distance between entities inside the network is crucial [108]. To counter such attack, Safi et al. [103] propose a way to restrict the packet's maximum allowed transmission distance, which would ensure that the recipient of the packet is within reasonable range of the sender.

4.1.3. Data integrity/data trust attacks and related countermeasures

Data integrity refers to the fact that the data must be intact and unchanged throughout its lifecycle. The attackers especially those having authenticated entities could easily alter the data or create false data. Thus, secure communication and information encryption are necessary to prevent/mitigate the attacks on data integrity. In the following, several attacks on data integrity (shown in Fig. 8) and their corresponding CMs are described.

- *Masquerading attack* means any attack that uses a forged identity to gain unofficial access to the system [120]. For example, a malicious node disguises itself as an emergency vehicle, and so the surrounding vehicles are tricked into slowing down, changing lane, etc. in order to give way to it. Effective detection of

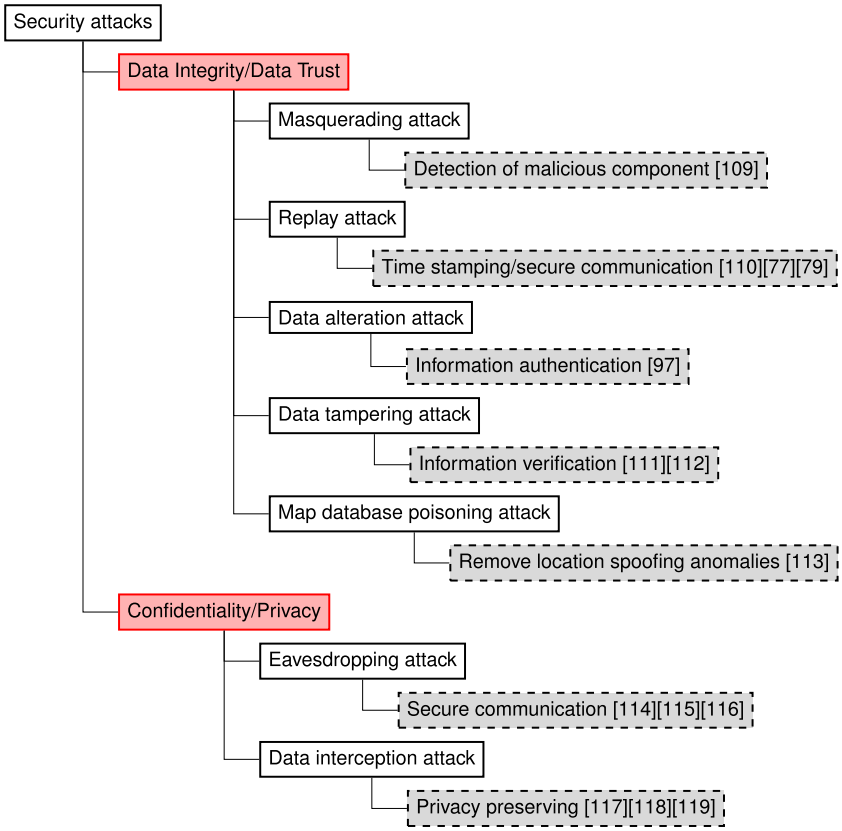

Fig. 8. Security attacks on data integrity/data trust, confidentiality/privacy and their corresponding countermeasures.

malicious component and authentication can be CMs to such attacks [109].

- *Replay attack*: aka Playback attack, means that the data is fraudulently repeated or delayed [120]. Duplicated data can be prevented by making use of the sequence number, time-stamp and secure communication [77,79,110].
- *Data alteration attack*: this type of attacks breaks the data integrity by modifying, deleting or altering the contents, which may inject false messages [67]. Ensuring the authentication between AVs and for signing in-network messages can be used to overcome data alteration attack [97].
- *Data tampering attack*: legitimate node may perform this attack by fabricating and broadcasting false messages [121]. The main countermeasure is to sign and verify the transmitted messages [111,112]. In [112], RSUs are responsible for distributing private keys and managing vehicles in a localized manner, and a hash message authentication code is used to ensure the integrity of message.
- *Map database poisoning attack*: in vehicle network, local map database is maintained by each AV. This type of attack is committed to sending malicious message to impact the accuracy of the map database [122]. The main countermeasure is verifying the signatures of the received map database messages and detecting and blacklisting the misbehaving nodes [113].

4.1.4. Confidentiality/privacy attacks and related countermeasures

The attacks on confidentiality/privacy may not affect safety as previous mentioned attacks do. Nevertheless, the sensitive information exchanged in network, e.g., AVs' location, ITS safety messages and drivers' personal information, should be protected. Information encryption and secure communication can be used to avoid information leak. Some examples of attacks on Confidentiality as well as their corresponding countermeasures are as follows (as shown in Fig. 8):

- *Eavesdropping attack* is an attempt to steal information (e.g., location) by snooping on the network communications [92]. Eavesdropping may not impact network resources and availability, but the sensitive information (e.g., location information) is leaked. Secure communication can be used to against eavesdropping [114–116]. To maximize both security and privacy to VANETs, a security credential management system is presented in [116]. It issues digital certificates to vehicles for establishing trust, and facilitate efficient revocation while providing privacy against attacks from insiders.
- *Interception attack*: this attack consists of listening to the network for a certain duration and then tries to analyze the data to extract the useful information [123]. The privacy preserving methods can be adopted to mitigate data interception attack [117–119]. Chim et al. [118] provides a software-based solution which makes use of two shared secrets to satisfy the privacy requirement, and gives lower message overhead than previous solutions in the message verification phase using the bloom filter and the binary search techniques (through simulation study).

4.2. Security attacks on AV itself and available countermeasures

In this section, we discuss the attacks that are specific for AV and the associated countermeasures. Tables 2 and 3 list some examples of attacks for AV on authenticity, availability, data integrity and confidentiality/privacy.

GPS spoofing is a typical attack on authenticity, which aims to distort the location information of the AV [124,125]. Professional attacker may perform GPS spoofing by replicating signals and providing false locations [126]. To detect this attack, Meuer et al. [127] use Direction-Of-Arrival (DOA) measurement; [128] uses the cross-correlation of unknown encrypted signals between two GPS receivers; [129] utilizes spatial phase delay

Table 2
Specific authenticity and availability attacks on AV and their corresponding countermeasures.

Attack Type	Attack	Countermeasure	
Authenticity	GPS spoofing	Detection	Montgomery et al. 2009 [127] Meuer et al. 2012 [134] Psiaki et al. 2013 [128] Magiera et al. 2015 [129] Anouar et al. 2016 [130]
		Anti-spoofing methods	Ledvina et al. 2010 [131] Tippenhauer et al. 2011 [132] Shepard et al. 2012 [135] Jafarnia et al. 2012 [136] Jwo et al. 2013 [133] stubberud et al. 2014 [137]
Availability	GPS jamming	Anti-jamming technique	Dixon et al. 2012 [138] Hancke et al. 2014 [139]
	Radar/LiDAR jamming	Filtering data/using other source of data	Petit et al. 2015 [140]
	Malware injection	Separate infotainment system	Zhang et al. 2014 [141]
		Intrusion detection	Müter et al. 2010. [142] Müter et al. 2011 [143] Alheeti et al. 2015 [144] Alheeti et al. 2016 [145]
		Installing anti-virus /firewall	Cui et al. 2018 [7]

Table 3
Specific integrity and privacy attacks on AV and corresponding countermeasures. CAN, Controller Area Network.

Attack type	Attack	Countermeasure	
Data integrity	Replay attack on Radar /LiDAR	Filtering data/using other source of data	Petit et al. 2015 [140]
	Radar/LiDAR confusion	Filtering data/using other source of data	Petit et al. 2015 [140]
	Inject CAN message	Intrusion detection	Song et al. 2016 [147] Salem et al. 2016 [148] Hymayed et al. 2017 [149]
		CAN security	Van et al. 2011 [150] Wolf et al. 2011 [151] Groza et al. 2012 [152] Hartkopp et al. 2012 [153] Lin et al. 2012 [154] Mundhenk et al. 2015 [155] Woo et al. 2015 [156]
	Map server poisoning	Authenticated map server	Yan et al.2014 [122]
Confidentiality/Privacy	Eavesdropping	In-vehicle security	Schweppe et al. 2012 [157] Maurer et al. 2016 [158] Pan et al. 2017 [159]

measurements; [130] considers the location information provided by the authenticated RSU. To prevent GPS spoofing, [131] develops a RF device that connects between a GPS antenna and a legacy civil GPS receiver; [132] identifies the minimal precision of signals needed to spoof the receivers; [133] uses Interacting Multiple Model Nonlinear filters to improve the GPS accuracy.

In terms of attacks on integrity, jamming attack cannot be ignored. The detection of GPS jamming can be challenging because the GPS signals may be unavailable owing to the environment constraints. Nonetheless, there exist some anti-jamming techniques like [138,139]. As for mitigating the Radar/LiDAR jamming, filters or other sources (e.g., camera data) could be used. Besides, some components of AV like infotainment system and on-board computer are vulnerable to malware injection. Anti-virus/firewall could be used to prevent the malware [146]. In [143], the anomaly is detected by observing an increased entropy. By training and testing of different system scenarios, Alheeti et al. compares the network status to the trained result to detect whether there is intrusion in [145].

Some example of attacks on data integrity are listed in Table 3. Replay attack and Radar/LiDAR Confusion (using reflective material interfere Radar/LiDAR) can be mitigated by using some filters, alternative data sources (e.g, camera images) [140], and multi-sensor fusion (a safety countermeasure presented in Section 3.2) [18]. The intrusion on CAN bus can detected by analyzing the time intervals of CAN message [147]. In [148], anomalies are identified based on the metrics derived from inter-arrival curves of normal set of CAN messages. In [149], when an DOS attack is detected, the ECU shall use a set of alternative IDs so that the malicious frame (sent by the attacker) is rendered ineffective. For secure CAN Bus, [150] propose a broadcast authentication protocol to ensure the security of CAN message. Lin et al. [154] proposes a software-based security mechanism that can be used to retro-fit the CAN protocol to protect CAN from replay attacks. A lightweight authentication scheme [155] for automotive networks is used to guarantee CAN security. Woo et al. [156] demonstrates an replay attack model using a malicious smart phone app in the connected car environment, and designs a security protocol to mitigate such attack. Map server poisoning should also be concerned since location is of crucial for AVs. Authenticated map server can be used to mitigate map poisoning, as described in Section 4.1.3.

Eavesdropping is an attack on confidentiality/privacy not only for vehicle networking, but also for AV itself. For example, eavesdropping tire pressure, Bluetooth, or CAN message are examples of attacks on confidentiality for AVs. Pan et al. [159] and Glancy [160] point out the importance of confidentiality/privacy for modern vehicular systems. In-vehicle security can be a CM for eavesdropping on AV, as shown in Table 3. Schweppe et al. [157] uses taint tracking tools into vehicle communication system to monitor data and to elevate security and privacy.

4.3. Higher level insights into AV security

The following insights can be derived from the material, presented in this section:

- there are numerous AV security vulnerabilities and possible attacks. However, few security countermeasures are currently available for detecting and mitigating each type of attacks;
- there is a lack of research into security countermeasure effectiveness;
- security and safety are inter-related, e.g., security attacks could lead to AV failures. Thus, the consequences of security attacks with respect to AV safety have to be analyzed. This would help in developing appropriate safety and security countermeasures to simultaneously improve AV safety and security.

5. Open issues, challenges, and future research direction

Are AVs safe and secure? Not yet. Unfortunately, the first fatal crash of an AV including pedestrian has been reported in March 2018 [161]. This increased the worldwide attention on the urgent need to assure AV safety and security to prevent such accidents from reoccurring.

AV development is an emerging area, and most of information on AVs is confidential. Furthermore, there are no international standards for AV development, safety, and security available yet. This makes the research into AV safety and security extremely difficult.

Alongside the development of AVs, more personal devices and infrastructures will be introduced into the AV network, which potentially will expose AVs to more vulnerabilities.

The following are several open issues, which should be addressed in the future.

1. In-vehicle security In-vehicle security is still a big challenge for AVs. A car hacking experiment, reported in [162], demonstrates that electric vehicles could be easily remotely controlled by mobile applications, forcing the vehicles to go forward of backward, limiting the speed, etc. In addition, the battery state, location and other private readings of the vehicle could be obtained by attackers. Future research should focus on protecting AV in-vehicle systems from outside attacks.

2. Security challenges in smart cities Versatile connections in smart cities provide more services to AVs, but at the same time introduce more challenges. Ensuring V2X communication security is extremely important, because attacks on AVs could spread to smart infrastructures and vice versa. For example, an attack on electric vehicle could spread to the power grid infrastructure through the electric charging equipment up to the utility system [163]. Developing secure communications [164] and defense mechanisms [165] are examples of future research in this area.

3. Safety and security countermeasure consistency Vehicle safety analysis and security analysis are often performed separately, consequently, safety and security countermeasures are designed and developed independently. In most cases, safety and security countermeasures complement or strengthen each other. For example, runtime monitoring (safety CM, described in Section 3.2) checks the system properties, and can help to detect the intrusion (security CM, described in Section 4.2). However, there is a possibility of antagonism between countermeasures, as described in [166]. Thus, there is a need of future research into the inter-relationships and consistency between AV safety and security countermeasures.

4. Safe and secure mixed traffic systems On public roads, AVs need to interact and cooperate with other automated and non-automated road users, such as regular vehicles, cyclists, and pedestrians, in order to reach an agreement about safe future motion plans [167]. Furthermore, AVs have to communicate with on-board users. Future research into safe and secure integration of AVs into mixed traffic environments and human-AV interaction is urgently needed.

6. Conclusions

The development of AVs is largely driven by the desire to produce quicker, more reliable, and safer vehicles. However, AVs still have numerous unsolved safety and security challenges.

This paper presents an introductory study into the issues and solutions related to safety and security of AVs. It includes an overview of current research on AV failures, attack, and safety and security countermeasures. Furthermore, it identifies open issues and future research directions.

References

[1] National Highway Traffic Safety Administration, Traffic safety facts, a brief statistical summary: critical reasons for crashes investigated in the national motor vehicle crash causation survey, National Center for Statistics and Analysis U.S. Department of Transportation, Washington, D.C, 2016. DOT HS 812 115.
[2] National Highway Traffic Safety Administration, 2016 Fatal motor vehicle crashes: overview, National Center for Statistics and Analysis U.S. Department of Transportation, Washington, D.C, 2017. DOT HS 812 456.
[3] D.J. Fagnant, K. Kockelman, Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations, Transp. Res. Part A 77 (Supplement C) (2015) 167–181, doi:10.1016/j.tra.2015.04.003.
[4] J.M. Anderson, K. Nidhi, K.D. Stanley, P. Sorensen, C. Samaras, O.A. Oluwatola, Autonomous Vehicle Technology: A Guide for Policymakers, Rand Corporation, 2014.
[5] B. Schoettle, M. Sivak, A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia (2014).
[6] K. Sjoberg, P. Andres, T. Buburuzan, A. Brakemeier, Cooperative intelligent transport systems in europe: current deployment status and outlook, IEEE Veh. Technol. Mag. 12 (2) (2017) 89–97, doi:10.1109/MVT.2017.2670018.
[7] J. Cui, G. Sabaliauskaite, US^2: an unified safety and security analysis method for autonomous vehicles, IEEE FICC, Singapore, 2018, doi:10.1007/978-3-030-03402-3_42.
[8] J. Cui, G. Sabaliauskaite, On the alignment of safety and security for autonomous vehicles, IARIA CYBER, Barcelona, Spain, 2017.
[9] M.H. Eiza, Q. Ni, Driving with sharks: rethinking connected vehicles with vehicle cybersecurity, IEEE Veh. Technol. Mag. 12 (2) (2017) 45–51, doi:10.1109/MVT.2017.2669348.
[10] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, Vanet security challenges and solutions: a survey, Veh. Commun. 7 (2017) 7–20, doi:10.1016/j.vehcom.2017.01.002.
[11] R.S. Raw, M. Kumar, N. Singh, Security challenges, issues and their solutions for Vanet, Int. J. Netw. Secur. Its Appl. 5 (5) (2013) 95, doi:10.5121/ijnsa.2013.5508.
[12] W. Liang, Z. Li, H. Zhang, S. Wang, R. Bie, Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends, Int. J. Distrib. Sens. Netw. 11 (8) (2015) 745303, doi:10.1155/2015/745303.
[13] R. Mishra, A. Singh, R. Kumar, Vanet security: Issues, challenges and solutions, in: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), IEEE, 2016, pp. 1050–1055, doi:10.1109/ICEEOT.2016.7754846.
[14] A. Vaibhav, D. Shukla, S. Das, S. Sahana, P. Johri, Security challenges, authentication, application and trust models for vehicular Ad Hoc network-a survey, Int. J. Wirel. Microw. Technol. 3 (2017) 36–48, doi:10.5815/ijwmt.2017.03.04.
[15] N. Lu, N. Cheng, N. Zhang, X. Shen, J.W. Mark, Connected vehicles: solutions and challenges, IEEE Internet Things J. 1 (4) (2014) 289–299, doi:10.1109/JIOT.2014.2327587.
[16] E.B. Hamida, H. Noura, W. Znaidi, Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures, Electronics (Basel) 4 (3) (2015) 380–423.
[17] J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles, IEEE Trans. Intell. Transp. Syst. 16 (2) (2015) 546–556, doi:10.1109/tits.2014.2342271.
[18] S. Parkinson, P. Ward, K. Wilson, J. Miller, Cyber threats facing autonomous and connected vehicles: future challenges, IEEE Trans. Intell. Transp. Syst. 18 (11) (2017) 2898–2915, doi:10.1109/TITS.2017.2665968.
[19] Society of Automotive Engineers (SAE), SAE-J3016: Taxonomy and definitions for terms related to driving automation systems for on-Road motor vehicles, 2016.
[20] C. Wei, V2x Communication in Europe from research projects towards standardization and field testing of vehicle communication technology, Comput. Netw. 55 (14) (2011) 3103–3119, doi:10.1016/j.comnet.2011.03.016.
[21] F. Zhang, D. Clarke, A. Knoll, Vehicle detection based on lidar and camera fusion, in: International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2014, pp. 1620–1625, doi:10.1109/ITSC.2014.6957925.

[22] M. Zhao, A. Mammeri, A. Boukerche, Distance measurement system for smart vehicles, in: 7th International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2015, pp. 1–5, doi:10.1109/NTMS.2015.7266486.

[23] Y. Toor, P. Muhlethaler, A. Laouiti, Vehicle Ad Hoc networks: applications and related technical issues, Commun. Surv. Tuts. 10 (3) (2008), doi:10.1109/COMST.2008.4625806.

[24] E.C. Eze, S. Zhang, E. Liu, Vehicular ad hoc networks (vanets): current state, challenges, potentials and way forward, in: 20th International Conference on Automation and Computing (ICAC), IEEE, Philadelphia, PA, USA, 2014, pp. 176–181, doi:10.1109/IConAC.2014.6935482.

[25] G. Dimitrakopoulos, P. Demestichas, Intelligent transportation systems, IEEE Veh. Technol. Mag. 5 (1) (2010) 77–84, doi:10.1109/MVT.2009.935537.

[26] M. Alam, J. Ferreira, J. Fonseca, Introduction to intelligent transportation systems, in: M. Alam, J. Ferreira, J. Fonseca (Eds.), Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety, Springer International Publishing, Cham, 2016, pp. 1–17, doi:10.1007/978-3-319-28183-4_1.

[27] P. Bhavsar, P. Das, M. Paugh, K. Dey, M. Chowdhury, Risk analysis of autonomous vehicles in mixed traffic streams, Transp. Res. Record (2625) (2017) 51–61, doi:10.3141/2625-06.

[28] G.S. Aoude, V.R. Desaraju, L.H. Stephens, J.P. How, Driver behavior classification at intersections and validation on large naturalistic data set, IEEE Trans. Intell. Transp. Syst. 13 (2) (2012) 724–736, doi:10.1109/TITS.2011.2179537.

[29] N.H. traffic Safety Administration, Pedestrians, Traffic Safety Facts 2014 Data, Report No. DOT HS 812 270, Washington, DC: National Highway Traffic Safety Administration, 2016.

[30] N.H. traffic Safety Administration, Bicyclists and Other Cyclists, Traffic Safety Facts 2014 Data, Report No. DOT HS 812 282, Washington, DC: National Highway Traffic Safety Administration, 2016.

[31] N.H. traffic Safety Administration, Traffic Safety Facts 2015, Report No. DOT HS 812 384, Washington, DC: National Highway Traffic Safety Administration, 2015.

[32] L. Chen, C. Chen, R. Ewing, C.E. McKnight, R. Srinivasan, M. Roe, Safety countermeasures and crash reduction in new york city experience and lessons learned, Accid. Anal. Prev. 50 (2013) 312–322, doi:10.1016/j.aap.2012.05.009.

[33] Z. Yang, Y. Zhang, O. Grembek, Combining traffic efficiency and traffic safety in countermeasure selection to improve pedestrian safety at two-way stop controlled intersections, Transp. Res. Part A 91 (2016) 286–301, doi:10.1016/j.tra.2016.07.002.

[34] H. Huang, X. Wang, G. Hu, Traffic safety in china: challenges and countermeasures, Accid. Anal. Prev. 95 (2016) 305–307. Traffic Safety in China: Challenges and Countermeasures, doi: 10.1016/j.aap.2016.07.040.

[35] L. Sasidharan, E.T. Donnell, Application of propensity scores and potential outcomes to estimate effectiveness of traffic safety countermeasures: exploratory analysis using intersection lighting data, Accid. Anal. Prev. 50 (2013) 539–553, doi:10.1016/j.aap.2012.05.036.

[36] V.V. Dixit, S. Chand, D.J. Nair, Autonomous vehicles: disengagements, accidents and reaction times, PLoS ONE 11 (12) (2016) e0168054, doi:10.1371/journal.pone.0168054.

[37] M. Hülsen, J.M. Zöllner, C. Weiss, Traffic intersection situation description ontology for advanced driver assistance, in: 2011 IEEE Intelligent Vehicles Symposium (IV), 2011, pp. 993–999, doi:10.1109/IVS.2011.5940415.

[38] K. Kolody, D. Perez-Bravo, J. Zhao, T. Neuman, Highway Safety Manual User Guide, Technical Report, 2014.

[39] P.K. Edara, C. Sun, S. Breslow, et al., Evaluation of J-Turn Intersection Design Performance in Missouri, Technical Report, Mid-America Transportation Center, University of Nebraska-Lincoln, 2013.

[40] J. Reid, L. Sutherland, Parsons-Brinckerhoff, B. Ray, et al., Median U-Turn Informational Guide, Technical Report, 2014.

[41] A. Fayish, F. Gross, Safety effectiveness of leading pedestrian intervals evaluated by a before-after study with comparison groups, Transp. Res. Record (2198) (2010) 15–22.

[42] W.C. Partners, Beyond the headlights: adas and autonomous sensing, WCP Rep. (2016).

[43] K. Chitnis, M. Mody, P. Swami, R. Sivaraj, C. Ghone, M. G Biju, B. Narayanan, Y. Dutt, A. Dubey, Enabling functional safety asil compliance for autonomous driving software systems, Auton. Veh. Mach. 2017 (2017) 35–40, doi:10.2352/ISSN.2470-1173.2017.19.AVM-017.

[44] M. Rezaei, R. Sabzevari, Multisensor data fusion strategies for advanced driver assistance systems, I-Tech Education and Publishing, 2009.

[45] M. Aeberhard, N. Kaempchen, High-level sensor data fusion architecture for vehicle surround environment perception, in: Proc. 8th Int. Workshop Intell. Transp, 2011.

[46] A. Goebel, R. Mader, O. Tripon, Performance and freedom from interference-a contradiction in embedded automotive multi-core applications? in: Proceedings of 30th International Conference on Architecture of Computing Systems, ARCS, VDE, Vienna, Austria, 2017, pp. 1–9.

[47] A. Kane, O. Chowdhury, A. Datta, P. Koopman, A case study on runtime monitoring of an autonomous research vehicle (arv) system, in: 6th Intenational Conference on Runtime Verification, RV,Vienna, Austria, 2015, pp. 102–117, doi:10.1007/978-3-319-23820-3_7.

[48] P. Koopman, M. Wagner, Challenges in autonomous vehicle testing and validation, SAE Int. J. Transp. Saf. 4 (1) (2016) 15–24.

[49] C.G. Keller, T. Dang, H. Fritz, A. Joos, C. Rabe, D.M. Gavrila, Active pedestrian safety by automatic braking and evasive steering, IEEE Trans. Intell. Transp. Syst. 12 (4) (2011) 1292–1304, doi:10.1109/TITS.2011.2158424.

[50] Y. Luo, J. Remillard, D. Hoetzer, Pedestrian detection in near-infrared night vision system, IEEE Intelligent Vehicles Symposium (IV), La Jolla, CA, 2010, doi:10.1109/IVS.2010.5548089.

[51] W.T. Prasetyo, P. Santoso, R. Lim, Adaptive cars headlamps system with image processing and lighting angle control, in: Proceedings of Second International Conference on Electrical Systems, Technology and Information 2015 (ICESTI 2015), Springer, 2016, pp. 415–422, doi:10.1007/978-981-287-988-2_45.

[52] M. Edirisinghe, Y. Dilhani, K. Kangara, Performance capabilities and detection efficiency of vehicle backup proximity sensors for narrow objects, Int. Lett. Chem. Phys.Astron. 52 (2015) 134–146. doi:10.18052/ http://www.scipress.com/ILCPA.52.134.

[53] D.G. Kidd, A. Brethwaite, Visibility of children behind 2010–2013 model year passenger vehicles using glances, mirrors, and backup cameras and parking sensors, Accid. Anal. Prev. 66 (2014) 158–167, doi:10.1016/j.aap.2014.01.006.

[54] V. Milanés, S.E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, M. Nakamura, Cooperative adaptive cruise control in real traffic situations, IEEE Trans. Intell. Transp. Syst. 15 (1) (2014) 296–305, doi:10.1109/TITS.2013.2278494.

[55] R.N. Mahajan, A. Patil, Lane departure warning system, Int. J. Eng. Tech.Res. 3 (1) (2015) 120–123.

[56] T. Lin, H. Rivano, F. Le Mouël, A survey of smart parking solutions, IEEE Trans. Intell. Transp. Syst. 18 (12) (2017) 3229–3253, doi:10.1109/TITS.2017.2685143.

[57] R.M. Ishtiaq Roufa, H. Mustafaa, S.O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, I. Seskarb, Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study, 19th USENIX Security Symposium,Washington, DC, 2010.

[58] N.K. Arzumanyan, M.A. Smirnova, M.N. Smirnov, Synthesis and modeling of anti-lock braking system, in: 2015 International Conference on “Stability and Control Processes” in Memory of VI Zubov (SCP), IEEE, Saint-Petersburg, Russia, 2015, pp. 552–554, doi:10.1109/SCP.2015.7342222.

[59] R.H. Grzebieta, D. Young, A. McIntosh, M.R. Bambach, B. Frechede, G. Tan, T. Achilles, Rollover crashworthiness: the final frontier for vehicle passive safety, J. Australas. Coll. Road Saf. 20 (2) (2009) 46–55.

[60] U. Seiffert, L. Wech, Automotive Safety Handbook, 2003.

[61] G. Underwood, E. Van Loon, K. Humphrey, How conspicuity influences drivers attention and manoeuvring decisions, Increasing Motorcycle Conspicuity (2017) 67.

[62] A.M. Malla, R.K. Sahu, Security attacks with an effective solution for dos attacks in Vanet, Int. J. Comput. Appl. 66 (22) (2013), doi:10.5120/11252-6467.

[63] R.G. Engoulou, M. Bellache, S. Pierre, A. Quintero, Vanet security surveys, Comput. Commun. 44 (Supplement C) (2014) 1–13, doi:10.1016/j.comcom.2014.02.020.

[64] S.S. Manvi, S. Tangade, A survey on authentication schemes in vanets for secured communication, Veh. Commun. 9 (Supplement C) (2017) 19–30, doi:10.1016/j.vehcom.2017.02.001.

[65] L.B. Othmane, H. Weffers, M.M. Mohamad, M. Wolf, A Survey of Security and Privacy in Connected Vehicles, in: Wireless Sensor and Mobile Ad-Hoc Networks, Springer, 2015, pp. 217–247, doi:10.1007/978-1-4939-2468-4_10.

[66] M. Raya, J.-P. Hubaux, Securing vehicular Ad Hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.

[67] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on Vanet security challenges and possible cryptographic solutions, Veh. Commun. 1 (2) (2014) 53–66, doi:10.1016/j.vehcom.2014.05.001.

[68] M. Rahbari, M.A.J. Jamali, Efficient detection of sybil attack based on cryptography in vanet, CoRR abs/1112.2257 (2011).

[69] N. Vighnesh, N. Kavita, S.R. Urs, S. Sampalli, A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks, in: IEEE Symposium on Wireless Technology and Applications (ISWTA), Langkawi, Malaysia, 2011, pp. 96–101, doi:10.1109/ISWTA.2011.6089388.

[70] H. Lu, J. Li, M. Guizani, A novel id-based authentication framework with adaptive privacy preservation for vanets, in: Computing, Communications and Applications Conference (ComComAp), 2012, IEEE, HongKong, China, 2012, pp. 345–350, doi:10.1109/ComComAp.2012.6154869.

[71] K.-A. Shim, Cpas: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. 61 (4) (2012) 1874–1883, doi:10.1109/TVT.2012.2186992.

[72] N.B. Bhavesh, S. Maity, R.C. Hansdah, A protocol for authentication with multiple levels of anonymity (amla) in vanets, in: 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, Barcelona, Spain, 2013, pp. 462–469, doi:10.1109/WAINA.2013.4.

[73] T. Zhou, R.R. Choudhury, P. Ning, K. Chakrabarty, P2dapsybil Attacks detection in vehicular Ad hoc networks, IEEE J. Sel. Areas Commun. 29 (3) (2011) 582–594, doi:10.1109/JSAC.2011.110308.

[74] J. Li, H. Lu, M. Guizani, Acpn: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets, IEEE Trans. Parallel Distrib. Syst. 26 (4) (2015) 938–948, doi:10.1109/TPDS.2014.2308215.

[75] C. Zhang, X. Lin, R. Lu, P.-H. Ho, X. Shen, An efficient message authentication scheme for vehicular communications, IEEE Trans. Veh. Technol. 57 (6) (2008) 3357–3368, doi:10.1109/TVT.2008.928581.

[76] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, M.K. Khan, B-specs+: batch verification for secure pseudonymous authentication in Vanet, IEEE Trans. Inf. Foren. Secur. 8 (11) (2013) 1860–1875, doi:10.1109/TIFS.2013.2277471.

[77] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity-based security system for user privacy in vehicular ad hoc networks, IEEE Trans. Parallel Distrib. Syst. 21 (9) (2010) 1227–1239, doi:10.1109/TPDS.2010.14.

[78] L. Zhang, Q. Wu, A. Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, IEEE Trans. Veh. Technol. 59 (4) (2010) 1606–1617, doi:10.1109/TVT.2009.2038222.
[79] A. Wasef, X. Shen, Emap: expedite message authentication protocol for vehicular Ad Hoc networks, IEEE Trans. Mob. Comput. 12 (1) (2013) 78–89, doi:10.1109/TMC.2011.246.
[80] S.-H. Seo, J. Won, S. Sultana, E. Bertino, Effective key management in dynamic wireless sensor networks, IEEE Trans. Inf. Foren. Secur. 10 (2) (2015) 371–383, doi:10.1109/TIFS.2014.2375555.
[81] J.-L. Huang, L.-Y. Yeh, H.-Y. Chien, Abaka: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 60 (1) (2011) 248–262, doi:10.1109/TVT.2010.2089544.
[82] Y. Hao, Y. Cheng, C. Zhou, W. Song, A distributed key management framework with cooperative message authentication in vanets, IEEE J. Sel. Areas Commun. 29 (3) (2011) 616–629, doi:10.1109/JSAC.2011.110311.
[83] L. Song, Q. Han, J. Liu, Investigate key management and authentication models in Vanets, in: International Conference on Electronics, Communications and Control (ICECC), IEEE, 2011, pp. 1516–1519, doi:10.1109/ICECC.2011.6067807.
[84] M.L. Psiaki, T.E. Humphreys, Gnss spoofing and detection, Proc. IEEE 104 (6) (2016) 1258–1270, doi:10.1109/JPROC.2016.2526658.
[85] A. Studer, F. Bai, B. Bellur, A. Perrig, Flexible, extensible, and efficient vanet authentication, J. Commun. Netw. 11 (6) (2009) 574–588, doi:10.1109/JCN.2009.6388411.
[86] R. Engoulou, Sécurisation des VANETS par la méthode de réputation des noeuds, Ph.D. thesis, École Polytechnique de Montréal, 2013.
[87] M.-C. Chuang, J.-F. Lee, Team: trust-extended authentication mechanism for vehicular ad hoc networks, IEEE Syst. J. 8 (3) (2014) 749–758, doi:10.1109/JSYST.2012.2231792.
[88] G. Guette, C. Bryce, Using tpms to secure vehicular ad-hoc networks (vanets), in: IFIP International Workshop on Information Security Theory and Practices, Springer, Berlin, Heidelberg, 2008, pp. 106–116, doi:10.1007/978-3-540-79966-5_8.
[89] D. Shrivastava, A. Pandey, A study of sybil and temporal attacks in vehicular ad hoc networks: types, challenges, and impacts, Int. J. Comput. Appl. Technol. Res. 3 (2014) 284–291, doi:10.7753/IJCATR0305.1002.
[90] K. Rabieh, M.M. Mahmoud, T.N. Guo, M. Younis, Cross-layer scheme for detecting large-scale colluding sybil attack in vanets, in: IEEE ICC, London, UK, 2015, pp. 7298–7303, doi:10.1109/ICC.2015.7249492.
[91] C. Kumar Karn, C. Prakash Gupta, A survey on vanets security attacks and sybil attack detection, Int. J. Sens. Wirel.Commun. Control 6 (1) (2016) 45–62, doi:10.2174/2210327905999151103170103.
[92] B. Mokhtar, M. Azab, Survey on security issues in vehicular ad hoc networks, Alex. Eng. J. 54 (4) (2015) 1115–1126, doi:10.1016/j.aej.2015.07.011.
[93] X. Lin, X. Li, Achieving efficient cooperative message authentication in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 62 (7) (2013) 3339–3348, doi:10.1109/TVT.2013.2257188.
[94] Y. Hao, T. Han, Y. Cheng, A cooperative message authentication protocol in vanets, in: IEEE GLOBECOM, Anaheim,CA,USA, 2012, pp. 5562–5566, doi:10.1109/GLOCOM.2012.6504006.
[95] W. Shen, L. Liu, X. Cao, Y. Hao, Y. Cheng, Cooperative message authentication in vehicular cyber-physical systems, IEEE Trans. Emerg. Top. Comput. 1 (1) (2013) 84–97, doi:10.1109/TETC.2013.2273221.
[96] T. Dimitriou, E.A. Alrashed, M.H. Karaata, A. Hamdan, Imposter detection for replication attacks in mobile sensor networks, Comput. Netw. 108 (2016) 210–222, doi:10.1016/j.comnet.2016.08.019.
[97] G. Samara, Y. Al-Raba'nah, Security issues in vehicular ad hoc networks (Vanet): a survey, CoRR abs/1712.04263 (2017).
[98] L. Mokdad, J. Ben-Othman, A.T. Nguyen, Djavan: detecting jamming attacks in vehicle ad hoc networks, Perform. Eval. 87 (2015) 47–59, doi:10.1016/j.peva.2015.01.003.
[99] D. Shukla, A. Vaibhav, S. Das, P. Johri, Security and attack analysis for vehicular ad hoc network: A survey, in: International Conference on Computing, Communication and Automation (ICCCA), IEEE, GREATER NOIDA, India, 2016, pp. 625–630, doi:10.1109/CCAA.2016.7813797.
[100] K.D. Thilak, A. Amuthan, Dos attack on vanet routing and possible defending solutions-a survey, in: International Conference on Information Communication and Embedded Systems (ICICES), IEEE, 2016, pp. 1–7, doi:10.1109/ICICES.2016.7518892.
[101] L. He, W.T. Zhu, Mitigating dos attacks against signature-based authentication in vanets, in: IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 3, 2012, pp. 261–265, doi:10.1109/CSAE.2012.6272951.
[102] K. Verma, H. Hasbullah, A. Kumar, Prevention of dos attacks in vanet, Wirel. Pers. Commun. 73 (1) (2013) 95–126, doi:10.1007/s11277-013-1161-5.
[103] S.M. Safi, A. Movaghar, M. Mohammadizadeh, A novel approach for avoiding wormhole attacks in vanet, in: Second International Workshop on Computer Science and Engineering, WCSE, 2, IEEE, 2009, pp. 160–165, doi:10.1109/WCSE.2009.787.
[104] A. Benslimane, H. Nguyen-Minh, Jamming attack model and detection method for beacons under multichannel operation in vehicular networks, IEEE Trans. Veh. Technol. 66 (7) (2017) 6475–6488, doi:10.1109/TVT.2016.2645478.
[105] 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, doi:10.1016/j.adhoc.2017.03.006.
[106] I.A. Sumra, H.B. Hasbullah, J.-l.B. AbManan, Attacks on security goals (confidentiality, integrity, availability) in Vanet: a survey, in: Vehicular Ad-Hoc Networks for Smart Cities, Springer, 2015, pp. 51–61, doi:10.1007/978-981-287-158-9_5.
[107] M. Shabbir, M.A. Khan, U.S. Khan, N.A. Saqib, Detection and prevention of distributed denial of service attacks in vanets, in: International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, Las Vegas, Nevada, 2016, pp. 970–974, doi:10.1109/CSCI.2016.0186.
[108] A.-S.K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET, CRC press, 2016.
[109] J.T. Isaac, S. Zeadally, J.S. Camara, Security attacks and solutions for vehicular Ad Hoc networks, IET Commun. 4 (7) (2010) 894–903.
[110] W. Li, H. Song, Art: an attack-resistant trust management scheme for securing vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2016) 960–969, doi:10.1109/TITS.2015.2494017.
[111] C. Ponikwar, H.-J. Hof, Overview on security approaches in intelligent transportation systems, arXiv preprint arXiv:1509.01552 (2015).
[112] X. Zhu, S. Jiang, L. Wang, H. Li, Efficient privacy-preserving authentication for vehicular ad hoc networks, IEEE Trans. Veh. Technol. 63 (2) (2014) 907–919, doi:10.1109/TVT.2013.2294032.
[113] L. Dolberg, J. Francis, T. Engel, Tracking spoofed locations in crowdsourced vehicular applications, in: IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 2014, pp. 1–9.
[114] K. Pll, H. Federrath, A privacy aware and efficient security infrastructure for vehicular ad hoc networks, Comput. Stand. Interfaces 30 (6) (2008) 390–397, doi:10.1016/j.csi.2008.03.007. Special Issue: State of standards in the information systems security area
[115] M. Abuelela, S. Olariu, K. Ibrahim, A secure and privacy aware data dissemination for the notification of traffic incidents, in: 69th Vehicular Technology Conference, VTC Spring, IEEE, 2009, pp. 1–5, doi:10.1109/VETECS.2009.5073340.
[116] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, A security credential management system for v2v communications, in: IEEE Vehicular Networking Conference (VNC), 2013, pp. 1–8. doi:0.1109/VNC.2013.6737583.
[117] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, X. Shen, Tsvc: timed efficient and secure vehicular communications with privacy preserving, IEEE Trans. Wirel. Commun. 7 (12) (2008) 4987–4998, doi:10.1109/T-WC.2008.070773.
[118] T. Chim, S. Yiu, L.C. Hui, V.O. Li, Specs: secure and privacy enhancing communications schemes for vanets, Ad Hoc Netw. 9 (2) (2011) 189–203. Advances in Ad Hoc Networks (I), doi: 10.1016/j.adhoc.2010.05.005.
[119] F.M. Salem, M.H. Ibrahim, I. Ibrahim, Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks, in: International Conference on Networking and Services (ICNS), IEEE, 2010, pp. 156–161, doi:10.1109/ICNS.2010.28.
[120] 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, doi:10.1109/MCOM.2015.7120028.
[121] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey on vehicular cloud computing, J. Netw. Comput. Appl. 40 (2014) 325–344, doi:10.1016/j.jnca.2013.08.004.
[122] G. Yan, D.B. Rawat, B.B. Bista, L. Chen, Location Security in Vehicular Wireless Networks, in: Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, IGI Global, 2014, pp. 108–133, doi:10.4018/978-1-4666-4691-9.ch006.
[123] L. Bariah, D. Shehada, E. Salahat, C.Y. Yeun, Recent advances in vanet security: a survey, in: 82nd Vehicular Technology Conference (VTC Fall), IEEE, Boston, MA, 2015, pp. 1–7, doi:10.1109/VTCFall.2015.7391111.
[124] V.L. Thing, J. Wu, Autonomous vehicle security: a taxonomy of attacks and defences, IEEE CPSCom, ChengDu, China, 2016, doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.
[125] S.C. Stubberud, K.A. Kramer, Threat assessment for GPS navigation, in: IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA) Proceedings, Alberobello, Italy, 2014, pp. 287–292, doi:10.1109/INISTA.2014.6873632.
[126] M. Thomas, J. Norton, A. Jones, A. Hopper, N. Ward, P. Cannon, N. Ackroyd, P. Cruddace, M. Unwin, Global navigation space systems: reliance and vulnerabilities, R. Acad. Eng. Lond. (2011).
[127] P.Y. Montgomery, T.E. Humphreys, B.M. Ledvina, A multi-antenna defense: receiver-autonomous GPS spoofing detection, Inside GNSS 4 (2) (2009) 40–46.
[128] M.L. Psiaki, B.W. O'Hanlon, J.A. Bhatti, D.P. Shepard, T.E. Humphreys, Gps spoofing detection via dual-receiver correlation of military signals, IEEE Trans. Aerosp. Electron. Syst. 49 (4) (2013) 2250–2267, doi:10.1109/TAES.2013.6621814.
[129] J. Magiera, R. Katulski, Detection and mitigation of GPS spoofing based on antenna array processing, J. Appl. Res. Technol. 13 (1) (2015) 45–57, doi:10.1016/S1665-6423(15)30004-3.
[130] B. Anouar, B. Mohammed, G. Abderrahim, B. Mohammed, Vehicular navigation spoofing detection based on V2Icalibration, in: 4th IEEE International Colloquium on Information Science and Technology (CiSt), 2016, pp. 847–849, doi:10.1109/CIST.2016.7805006.
[131] B.M. Ledvina, W.J. Bencze, B. Galusha, I. Miller, An in-line anti-spoofing device for legacy civil GPSreceivers, in: Proceedings of the 2010 international technical meeting of the Institute of Navigation, 2010, pp. 698–712.
[132] N.O. Tippenhauer, C. Pöpper, K.B. Rasmussen, S. Capkun, On the requirements for successful GPS spoofing attacks, in: Proceedings of the 18th ACM confer-

ence on Computer and communications security, ACM, Chicago, IL, USA, 2011, pp. 75–86, doi:10.1145/2046707.2046719.
[133] D. Jwo, F. Chung, K. Yu, Gps/ins integration accuracy enhancement using the interacting multiple model nonlinear filters, J. Appl. Res. Technol. 11 (4) (2013) 496–509, doi:10.1016/S1665-6423(13)71557-8.
[134] M. Meuer, A. Konovaltsev, M. Cuntz, C. Hättich, Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses raim, in: Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), American Institute of Navigation (ion. org), Nashville, TN, USA, 2012.
[135] D.P. Shepard, T.E. Humphreys, A.A. Fansler, Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks, Int. J. Crit. Infrastruct. Prot. 5 (3) (2012) 146–153, doi:10.1016/j.ijcip.2012.09.003.
[136] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle, Gps vulnerability to spoofing threats and a review of antispoofing techniques, Int. J. Navig.Obs. 2012 (2012), doi:10.1155/2012/127072.
[137] S.C. Stubberud, K.A. Kramer, Analysis of fuzzy evidence accrual security approach to GPS systems, in: 10th International Conference on Communications (COMM), IEEE, Bucharest, Romania, 2014, pp. 1–6, doi:10.1109/ICComm.2014.6866695.
[138] C. Dixon, C. Hill, M. Dumville, D. Lowe, Gnss vulnerabilities: testing the truth, Coord. Mag. (2012).
[139] G.P. Hancke, Security of Embedded Location Systems, Springer New York, New York, NY, pp. 267–286. 10.1007/978-1-4614-7915-4_11.
[140] J. Petit, B. Stottelaar, M. Feiri, F. Kargl, Remote attacks on automated vehicles sensors: experiments on camera and lidar, Black Hat Europe 11 (2015) 2015.
[141] T. Zhang, H. Antunes, S. Aggarwal, Defending connected vehicles against malware: challenges and a solution framework., IEEE Internet Things J. 1 (1) (2014) 10–21.
[142] M. Müter, A. Groll, F.C. Freiling, A structured approach to anomaly detection for in-vehicle networks, in: International Conference on Information Assurance and Security (IAS), IEEE, Atlanta, GA, USA, 2010, pp. 92–98, doi:10.1109/ISIAS.2010.56 04050.
[143] M. Müter, N. Asaj, Entropy-based anomaly detection for in-vehicle networks, in: IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 2011, pp. 1110–1115, doi:10.1109/IVS.2011.5940552.
[144] K.M.A. Alheeti, A. Gruebler, K.D. McDonald-Maier, An intrusion detection system against malicious attacks on the communication network of driverless cars, in: IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2015, pp. 916–921, doi:10.1109/CCNC.2015.7158098.
[145] K.M.A. Alheeti, K. McDonald-Maier, Hybrid intrusion detection in connected self-driving vehicles, in: International Conference on Automation and Computing (ICAC), IEEE, Colchester,UK, 2016, pp. 456–461, doi:10.1109/IConAC.2016.7604962.
[146] C. Miller, C. Valasek, A survey of remote automotive attack surfaces, Black Hat USA 2014 (2014).
[147] 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: International Conference on Information Networking (ICOIN), IEEE, Kota kinabalu, Malaysia, 2016, pp. 63–68, doi:10.1109/ICOIN.2016.7427089.
[148] M. Salem, M. Crowley, S. Fischmeister, Anomaly detection using inter-arrival curves for real-time systems, in: 28th Euromicro Conference on Real-Time Systems (ECRTS), IEEE, Toulouse, France, 2016, pp. 97–106, doi:10.1109/ECRTS.2016.22.
[149] A. Humayed, B. Luo, Using id-hopping to defend against targeted dos on can, in: Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles, in: SCAV'17, ACM, New York, NY, USA, 2017, pp. 19–26, doi:10.1145/3055378.3055382.
[150] A. Van Herrewege, D. Singelee, I. Verbauwhede, Canauth-a simple, backward compatible broadcast authentication protocol for can bus, ECRYPT Workshop on Lightweight Cryptography, 2011, 2011.
[151] M. Wolf, T. Gendrullis, Design, implementation, and evaluation of a vehicular hardware security module, in: International Conference on Information Security and Cryptology, Springer, Seoul, South Korea, 2011, pp. 302–318, doi:10.1007/978-3-642-31912-9_20.
[152] B. Groza, S. Murvay, A. Van Herrewege, I. Verbauwhede, Libra-can: a lightweight broadcast authentication protocol for controller area networks, in: International Conference on Cryptology and Network Security, Springer, 2012, pp. 185–200, doi:10.1007/978-3-642-35404-5_15.
[153] O. Hartkopp, R.M. SCHILLING, Message authenticated can, in: Escar Conference, Berlin, Germany, 2012.
[154] C.-W. Lin, A. Sangiovanni-Vincentelli, Cyber-security for the controller area network (can) communication protocol, in: International Conference on Cyber Security (CyberSecurity), IEEE, Washington,DC,USA, 2012, pp. 1–7, doi:10.1109/CyberSecurity.2012.7.
[155] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S.A. Fahmy, S. Chakraborty, Lightweight authentication for secure automotive networks, in: Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, EDA Consortium, Grenoble, France, 2015, pp. 285–288.
[156] S. Woo, H.J. Jo, D.H. Lee, A practical wireless attack on the connected car and security protocol for in-vehicle can, IEEE Trans. Intell. Transp. Syst. 16 (2) (2015) 993–1006, doi:10.1109/TITS.2014.2351612.
[157] H. Schweppe, Y. Roudier, Security and privacy for in-vehicle networks, in: International Workshop on Vehicular Communications, Sensing, and Computing (VCSC), IEEE, Seoul, South Korea, 2012, pp. 12–17, doi:10.1109/VCSC.2012.6281235.
[158] M. Maurer, J.C. Gerdes, B. Lenz, H. Winner, et al., Autonomous driving, Springer, 2016.
[159] L. Pan, X. Zheng, H. Chen, T. Luan, H. Bootwala, L. Batten, Cyber security attacks to modern vehicular systems, J. Inf. Secur. Appl. 36 (2017) 90–100, doi:10.1016/j.jisa.2017.08.005.
[160] D.J. Glancy, Privacy in autonomous vehicles, Santa Clara L. Rev. 52 (2012) 1171.
[161] The Guardian, Self-driving uber kills Arizona woman in first fatal crash involving pedestrian, 2018.
[162] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, T. Engel, A car hacking experiment: when connectivity meets vulnerability, in: IEEE Globecom Workshops (GC Wkshps), San Dieg, CA, USA, 2015, pp. 1–6, doi:10.1109/GLOCOMW.2015.7413993.
[163] M. Amjad, A. Ahmad, M.H. Rehmani, T. Umer, A review of evs charging: from the perspective of energy optimization, optimization approaches, and charging techniques, Transp. Res. Part D 62 (2018) 386–417, doi:10.1016/j.trd.2018.03.006.
[164] V.T. Kilari, S. Misra, G. Xue, Revocable anonymity based authentication for vehicle to grid (v2g) communications, in: IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, Australia, 2016, doi:10.1109/SmartGridComm.2016.7778786.
[165] S. Mousavian, M. Erol-Kantarci, L. Wu, T. Ortmeyer, A risk-based optimization model for electric vehicle infrastructure response to cyber attacks, IEEE Trans. Smart Grid 9 (6) (2018) 6160–6169, doi:10.1109/TSG.2017.2705188.
[166] L. Piètre-Cambacédès, M. Bouissou, Cross-fertilization between safety and security engineering, Reliab. Eng. Syst. Saf. 110 (Supplement C) (2013) 110–126, doi:10.1016/j.ress.2012.09.011.
[167] interACT prject, Designing cooperative interaction of automated vehicles with other road users in the mixed traffic environments, 2018.

Jin Cui received her Ph.D. degree in Computer Science from the Institut National des Sciences Appliquées de Lyon, France, in 2016, following her B.Eng. and M.E degrees in Computer Science and Technology from the Northwestern Polytechnical University, China, in 2009 and 2012, respectively. She is currently a postdoctoral research fellow at the Singapore University of Technology and Design. Her research interests are in data aggregation of sensor networks, and security of autonomous vehicle.

Lin Shen Liew received the B.Eng. degree in Robotics and Mechatronics Engineering and the Ph.D. degree from Swinburne University of Technology, Australia, in 2011 and 2017, respectively. He is currently a postdoctoral research fellow at Singapore University of Technology and Design. His research interests are in indoor tracking and localization systems, and cybersecurity of autonomous systems.

Giedre Sabaliauskaite received Ph.D. degree in Software Engineering from the Osaka University, Japan, in 2004, following her BSc and MSc degrees in Information Systems from the Kaunas University of Technology, Lithuania. She is a research scientist at the Singapore University of Technology and Design. Giedre is interested in cross-disciplinary and emerging complex topics in relation to the organizations, the design and management of complex systems, the role of customers, and the strategies to deal with increasingly uncertain environments. Her current research focuses on safety and security of autonomous vehicles.

Fengjun Zhou received his Ph.D. degree in Vehicle Engineering from Beijing Institute of Technology, China, in 2014, following his bachelors degree from Shandong University of Technology, China. Then he worked in Institute of Beijing Automotive Industry Company and was responsible for ABS and ESP development as an engineer in Chassis Department. After that, he worked in China Automotive Engineering Research Institute CO., LTD. Currently, he is a research fellow in SUTD and mainly focused on Autonomous Vehicle Safety.