Hindawi
Journal of Advanced Transportation
Volume 2020, Article ID 6873273, 15 pages
https://doi.org/10.1155/2020/6873273

Research Article

Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles

Qiyi He,[1] **Xiaolin Meng**,[1] **and Rong Qu**[2]

[1]*Nottingham Geospatial Institute, University of Nottingham, Nottingham, UK*
[2]*School of Computer Science, University of Nottingham, Nottingham, UK*

Correspondence should be addressed to Qiyi He; qiyi.he@nottingham.ac.uk

Received 12 January 2020; Revised 29 May 2020; Accepted 21 August 2020; Published 3 September 2020

Academic Editor: Zeyang Cheng

CAV (connected and autonomous vehicle) is a crucial part of intelligent transportation systems. CAVs utilize both sensors and communication components to make driving decisions. A large number of companies, research organizations, and governments have researched extensively on the development of CAVs. The increasing number of autonomous and connected functions however means that CAVs are exposed to more cyber security vulnerabilities. Unlike computer cyber security attacks, cyber attacks to CAVs could lead to not only information leakage but also physical damage. According to the UK CAV Cyber Security Principles, preventing CAVs from cyber security attacks need to be considered at the beginning of CAV development. In this paper, a large set of potential cyber attacks are collected and investigated from the aspects of target assets, risks, and consequences. Severity of each type of attacks is then analysed based on clearly defined new set of criteria. The levels of severity for the attacks can be categorized as critical, important, moderate, and minor. Mitigation methods including prevention, reduction, transference, acceptance, and contingency are then suggested. It is found that remote control, fake vision on cameras, hidden objects to LiDAR and Radar, spoofing attack to GNSS, and fake identity in cloud authority are the most dangerous and of the highest vulnerabilities in CAV cyber security.

1. Introduction

Connected and autonomous vehicle (CAV), as a subset of the Intelligent Transportation System, makes use of different hardware, e.g., electronic control units (ECUs) and sensors, software, e.g., entertainment system and decision-making units, and data fused from multiple sources to conduct driving tasks with different levels of automation. With these components, CAVs could not only drive without human involvement but also communicate with surroundings to navigate and take appropriate reactions. The automation of CAVs is supported by the sensors installed around the vehicle body which gather information of surrounding environments to make decisions. The connectivity is achieved by the communication with other vehicles, infrastructures, and pedestrians on the road to navigate and take relevant reactions.

Currently, a large number of companies investigate and focus on the research and development of CAVs. In China, one of the biggest IT companies Baidu released an open source autonomous driving platform named Apollo, aiming to address the challenging issues of precise sensing and decision-making [1]. In USA, Tesla released their Autopilot for assistant driving and Summon system for assistant parking in 2015 and 2016, respectively [2]. The latest news on Tesla official website [3] introduces the enhanced Autopilot system, which supports autonomous driving in certain scenarios such as highways. Google is also a leading player in connected and autonomous driving. Its subcompany Waymo, set up in 2009, has been focusing on the research and development of CAVs and finished more than 2 million miles road test [4]. Taxi-hailing company Uber also tests their own CAVs on public roads in Arizona [5]. In Europe, traditional vehicle manufactures including Audi and

Mercedes Benz also announce their initiatives on CAVs. Audi already conducted 550 km on-road test, based on their own autonomous vehicle "Jack" [6]. Mercedes Benz started to develop CAVs in 1980s; now, their latest S-class Benz vehicles completed 100 km road trials in Germany [7].

To accelerate the CAV development, governments also publish relevant regulations and principles. In USA, regulations and laws on CAV are built at the state level [8]. Chinese government also released a ten-year plan "Made in China 2025" plan, which aims to master the key CAV technologies by 2025 [9]. In addition, Chinese government launched an abundance of CAV demonstration projects and set up Jiading district in Shanghai as the first public test field for CAVs [10]. Moreover, CAV competitions among academic organizations have been held successfully several times around the world. These include the US DARPA Urban Challenge in 2007 and DARPA Grand challenge in 2004 [11]. In China, the Future Challenges of Intelligent Vehicles competition has been held since 2008, sponsored by the National Natural Science Foundation of China [12]. With the participation of an increasing number of research organizations, these competitions not only provide platforms for researchers to communicate but also raise public interests on CAV developments. According to a survey conducted by Boston Consulting Group, 55% of public would like to try an autonomous vehicle or even buy one [13].

However, all the CAV research works mentioned above focus on the functions of either automation or connectivity. The cyber security of CAVs is not being sufficiently addressed. As a fundamental part of the CAV development, cyber security plays a crucial role on the function safety of CAVs, which will influence public trust and CAV commercialization directly. According to the newly released UK CAV Cyber Security Principles [14], CAV cyber security should be considered at the early stage of CAV development from the design phase, based on which the whole supply chain could then prevent CAVs from cyber security risks and issues in the following phases.

Comparing to traditional networks, mobile network or traditional automobile network, CAV cyber security has specific characteristics including large amount of data, complex functions, and fatal consequences, as shown in Table 1. These differences indicate that the cyber security of CAVs should be considered specifically and in different ways compared to the cyber security strategies in traditional networks or automobile networks.

The main aim of this paper is to investigate different potential cyber attack points of CAV. The specific characteristics of CAV are analysed and potential attack points of CAV are listed. The authors also present new criteria to evaluate the potential attacks to CAVs. The severity of each attack is then analysed and mitigation methods are then suggested.

The main contributions of this paper are listed as below:

(1) Definitions and categorization of all the potential attacks for CAVs: the attack categories cover both the autonomous elements such as the in-vehicle system and sensors on the vehicles, and the connected parts or functions such as V2X communication in CAVs. The paper also identifies the gaps and the limitations of current studies. For example, there is a lack of research and developments on cyber security for the connectivity elements of CAVs. In addition, those papers in the literature discussing the attacks to CAVs focus on only some specific attack types. The missing types of attacks require further research. By defining the initial set of all potential attacks to CAVs within a structured category and of different severities, additional unexpected new attacks to CAVs could be added in the future research. That is, the categories of the potential attacks and criteria apply to new attacks; thus, the set of attacks is extendable to include new attacks.

(2) A new severity assessment on potential attacks to CAVs: the assessment criteria used in engineering and information technology are adopted to define the criteria suitable for assessing CAVs attacks. This is a new adoption of such criteria assessing the severity of different CAV attacks.

(3) A new categorization of mitigation methods to CAV attacks: the recovery and protection mechanisms are key issues in cyber security of CAVs. Defining mitigation methods presents guidance to future research, including intrusion detection or encryption to protect the overall CAV systems. The mitigation category method categorizes the mitigation methods into prevention, production, acceptance, transference, and contingency. With the establishment of test environments, this categorization could be adopted to respond to different attacks.

The paper is structured as follows. Section 2 introduces the related works on cyber security in CAVs and also the related subject of Vehicular Ad hoc Network. Section 3 then describes the methodology to define different criteria to assess the risk of different attacks. In Section 4, the potential cyber attacks are listed to analyse each of their severity with the criteria listed in Section 3. Mitigation methods of cyber security attacks on CAVs are then recommended in Section 5. Section 6 summarizes the paper and discusses the future challenges faced by CAV cyber security research.

2. Related Work

The SAE International defined "driving automation" as that the system could conduct part of or all DDT (Dynamic Driving Tasks) continuously [20]. DDT are defined as three different levels by the SAE J3061 standard, namely, operational functions, tactical functions, and strategic functions. The relations of these three functions are illustrated in Figure 1. Operational functions include basic motion control such as lateral and longitudinal motion controls. Tactical functions include all the operational functions plus OEDR (Object and Event Detection and Response). In the current DDT performance, the strategic functions such as destination and waypoint planning are not included.

Table 1: Comparison of CAVs/traditional vehicles/mobile networks.

Compared to traditional vehicles	Compared to computer network/mobile network
1. There are more ECUs and more codes in CAVs [15], which means more data to be processed	1. In addition to information leakage, cyberattacks to CAVs could cause physical damage or even fatal injuries
2. There are multiple communication protocols in CAVs, such as CAN [16], 5G, and DSRC [17]; different communication protocols lead to multiple data formats, which require more preprocessing time	2. CAVs require higher detection accuracy as well as shorter data processing time; in the Europe Metis project, the latency is expected to be less than 5 ms and the accuracy is expected to be 99.999% when transmitting a 1600 bytes data package [18]
3. There are more connected functions, meaning the number of potential attack points is also increasing [19]	3. The application scenarios are more complicated; CAVs are more likely to drive in unregulated areas such as parking lots, highways, and rural areas

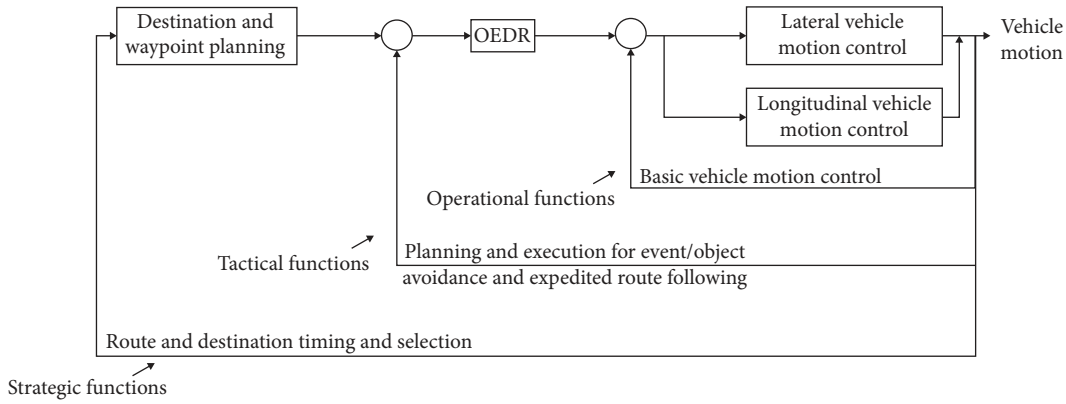

Figure 1: Schematic view of driving tasks [20].

The response by either users or the system to perform DDT when a system failure happens is defined as DDT fallback by SAE International. ODD (Operational Design Domain) is considered as the driving system which requires a specific running environment including environmental, geographical, or time restrictions. For example, some autonomous driving vehicles only operate in a closed environment [21], which indicates that the vehicle is still designed under a limited ODD. Based on the DDT performance, DDT fallback, and ODD, SAE International then defines the vehicle automation into 6 different levels, as shown in Table 2.

Besides the automation taxonomy, there are attempts to discuss CAV cyber security. In [22], the authors discussed the possible cyber security attacks on autonomous vehicles. After listing all the possible attacks, the authors then provided mitigation solutions to each attack. It is recommended that it is important to keep sufficient redundancy in autonomous vehicles. Sufficient sensor data could help vehicles to know the surroundings and positions. Among all these attacks, they believed that GNSS spoofing and fake message injection are the most threatening risks, both of which will threaten passengers' lives. It is believed that antispoofing hardware and authentication methods are needed in autonomous vehicles.

In [23], the authors discussed cyber security in connected vehicles and believed that the vehicles would be more vulnerable with the increasing connectivity. This paper described the possible attack scenarios including USB update attacks, communication attacks, and malicious application installation. A system using machine learning methods is then built to detect the anomaly behaviours in CAN-Bus (Controller Area Network) and the operating system.

In [24], the authors attempted to use the categories of cyber security in computer science to describe the possible attacks in CAVs. The possible attacks are divided into passive attacks and active attacks. The passive attacks are easy to prevent but difficult to detect, while the active attacks are easy to detect but difficult to prevent. Feasible mitigation methods including authentication and encryption were recommended.

In [25], the authors assumed that connected vehicles are similar to all the Internet devices and cyber security should be considered as a fundamental part of their development. The authors then discussed the potential cyber attacks on V2I (Vehicle-to-Infrastructure) Communication and proposed a novel cyber security architecture called CVGuard to detect the attacks in V2I. The CVGuard reduced 60% DDoS (Distributed Denial of Service) attacks which might cause vehicle conflicts.

In [19], it is pointed out that modern cars are already new targets for hackers. Engines, doors, and brakes could all be possible vulnerable points. In addition, nowadays, the attackers do not need to approach the target vehicle physically. All the vehicles in the communication range could be hacked. The authors also listed OBD (On-Board Diagnostics) threat, DSRC communication, Malware, and

Table 2: SAE automation levels [20].

Level	Name	DDT		DDT fallback	ODD
		Sustained motion control	OEDR		
0	No driving automation	Driver	Driver	Driver	N/A
1	Driver assistance	Driver and system	Driver	Driver	Limited
2	Partial driving automation	System	Driver	Driver	Limited
3	Conditional driving automation	System	System	Fallback-ready user (becomes the driver during fallback)	Limited
4	High driving automation	System	System	System	Limited
5	Full driving automation	System	System	System	Unlimited

automobile apps as the most vulnerable parts on vehicles. The authors then offered the solutions to address the cyber security issues including OTA solution, cloud based solution, and layer-based solution.

There are also research attempts in simulation environments to examine the influence of cyber attacks to CAVs. In [26], simulated slight attacks were made to study longitudinal safety of CAVs, i.e., on the positions and speed via GPS communications. An empirical model named PATH CAV from a field test [27, 28] and a RCRI (Rear-end Collision Risk Index) based on stopping distance was used to evaluate the safety. The authors found that the slight attacks to the CAV positions are severer than they are to the speed. The slight cyber attacks will also make severer impacts on decelerating than accelerating. In addition, the slight attacks to multiple CAVs are more dangerous than attacks of higher severity to fewer number of vehicles. This research will help to find a more efficient mitigation method to the attacks to V2V communications.

In [29], four possible attack points of the vehicle have been discussed, including signal controllers, vehicle detectors, roadside units, and onboard units. The focus was on the attacks to infrastructures. The authors attacked the traffic signal control systems by sending spoofed data, which showed to increase the delay. Some attacks in the experiments also showed to cause severe congestion. Based on the attacks, an approach was devised to identify this kind of attacks by analysing the attack locations, which helps to design a more stable transportation network.

As a fast emerging research topic, CAV cyber security has just started attracting increasing research attention. In addition to the limited research on cyber security in CAVs, research on VANET (Vehicular Ad hoc Networks) may contribute to the research on the connected functions of CAVs. VANET uses V2V communication and V2I communication to help vehicles gathering traffic information [30], while CAVs extend the boundaries to the wider V2X (Vehicle-to-Everything) communications.

VANET is a mobile ad hoc network, where the vehicles are the mobile nodes [31]. In [31], the authors listed the possible privacy and security challenges to the safety of VANET including the attacks on confidentiality, integrity, or data trust. They claimed that encryption is important to VANET.

In [32], the authors concluded that VANET has three specific characteristics, which are frequent vehicle movement, time critical response, and hybrid architecture. Other attacks listed include bogus information, DoS attacks, Masquerade, and GPS spoofing. The authors also propose several mitigation methods including public key, certificate revocation approaches, and ID-based cryptography.

Research in [33] focused on threats and attacks to vehicular communication. The authors built a three-layer framework and pointed out the potential threats and attacks to V2X communication such as remote communication protocols including DSRC or Bluetooth. It also suggested machine learning and block chain as countermeasures to detect attacks.

In the literature listed above, the majority of the researchers believe that cyber security is a fundamental part in CAV developments, which demands urgently more research and investigations. The majority of researchers agreed that the increasing connected and autonomous functions will increase the possibilities of cyber attacks. However, existing research mainly focused on the cyber security of autonomous functions. The potential attacks should be considered from both the autonomous and connected aspects. There are attempts to discuss the most severe attacks, but there is a lack of systematic evaluation criteria in the literature. Some research discussed the mitigation methods including encryption or authentication, but there are still the needs of further investigations to identify comprehensive and systematic mitigation methods to categorized cyber attacks. Overall, the literature on CAV cyber security is limited and requires more investigation and research efforts. Awareness of cyber security in CAV should be raised as well.

This paper significantly extends the existing research by defining potential attacks to both connectivity and autonomy, as well as both in-vehicle and intervehicle potential cyber attacks. Moreover, severity evaluation criteria for cyber attacks are defined and the severity level of each attack is also evaluated based on the criteria defined in this paper. Corresponding mitigation methods are then suggested at the end. This research aims to raise cyber security awareness of consumers, OEMs, researchers, and manufactures and also present a starting point to develop the detection and prevention methods towards CAV cyber attacks.

3. Potential CAV Cyber Attack Criteria

The potential attack points or attack ports are analysed firstly. For each potential attack, the following criteria will then be adopted to assess its severity.

The new CAV assessment criteria are defined based on the widely used formula in engineering risk assessment in different areas including transportation and infrastructure [34], information technology system [35], and civil aviation [36]:

$$\text{Risk} = \text{Asset} * \text{Vulnerability} * \text{Threat}. \quad (1)$$

The new assessment criteria evaluate three aspects of cyber attacks, namely, the asset of the possible attack targets, vulnerability of the possible risks to the attack targets, and threat of the possible consequences. As mentioned in Section 1, due to several key differences between traditional automobile network cyber security and CAV cyber security, some extra criteria are adapted to our new CAV cyber security assessment. For example, to evaluate the severity of the risk, the assessment criteria of CAVs should consider not only the level of information leakage but also the level of physical damage.

3.1. Asset of the Attacked Targets

(1) Asset name: in computer security, ISO/IEC 13335-1: 2004 defines that assets include all the hardware or software components on computers which are exposed to an attack target, e.g., a dataset and one piece of hardware or software code [37]. CAVs are equipped with a large number ECUs and sensors and are thus vulnerable to an abundance of possible attacks. More detailed assets will be explained in Section 4.

(2) Asset importance: the importance of each asset is categorized into three levels:

- (a) Low: the breakdown of this asset will not affect the operational and tactical functions of the whole CAV system. In the SAE J3016 standard [20], operational functions include lateral and longitudinal vehicle motion control, including the most basic functions of starting, stopping, driving, and controlling [38]. The tactical functions include the OEDR as introduced in Section 2.
- (b) Medium: the breakdown of this asset might influence tactical functions of the vehicle, however would not have direct impacts on the operational functions. In addition, the asset function could be replaced or covered by other assets on the vehicle. For example, if cameras on CAV breakdown, the vehicle could still use other sensors to detect the surroundings.
- (c) High: the breakdown of this asset may cause damage to operational functions of the vehicle directly. For example, the in-vehicle system, which sends instructions to ECUs to maintain the vehicle speed or stop the vehicle in certain situations, is of high importance.

3.2. Vulnerability of the Attacked Targets

(1) Risk name: each asset may be exposed to more than one risk. This criterion assesses specific risks to each asset; more details are presented in Section 4.

(2) Difficulty of conduction: the difficulty of conducting an attack varies depends on its characteristics. Some attacks may require sufficient expertise from the attackers in specific areas such as GPS spoofing or fake identification. Some devices, such as GNSS satellites, are securely protected by the governments. Hacking into these devices needs not only knowledge but also sufficient time and money. The difficulty of conduction is considered based on the knowledge, time, and budget needed and can be graded into three levels listed as below:

- (a) Low: attackers do not need to acquire relevant knowledge to conduct the attack or the target asset is easy to be obtained/bought on the market. The attack is not time consuming.
- (b) Medium: attackers only need to spend a short time (weeks/months) to learn the required knowledge. Hacking into the target asset needs to be purchased at a high price, or the hacking process is time consuming.
- (c) High: attackers need to have extensive knowledge on the target asset or need to spend years to learn relevant knowledge. The target asset is difficult to find in the market or costs an astronomical figure.

(3) Detection possibilities: this criterion defines the level of possibilities detecting attacks by the users or the CAV system. In computer science, the attacks are divided into two main categories, namely, passive attacks and active attacks [39]. Passive attacks do not interrupt the system but will monitor or eavesdrop it to access information. Active attacks will interrupt the system functions directly by methods such as injecting fake message. In general, passive attacks are difficult to detect but easy to defend, while active attacks are difficult to defend but easy to detect [24]. Although passive attacks may not cause harms on system functions, the information loss could also be a severe risk because CAVs will be the ultimate personal mobile device in the future [40], storing sensitive data including personal home address, contact numbers, and financial information. It is essential to evaluate the detection possibilities of different attacks. The levels of detection possibilities are categorized into three levels as listed below.

- (a) Low: the attacks will not affect any function (whether operational or tactical functions) of the CAV system. It is difficult to detect the attack in normal use. The best solution is to prevent the attacks from happening in advance with encryption or authentication.
- (b) Medium: the attacks will not affect the operational functions of the CAV system so the users would not notice the attacks immediately. However, the attacks would affect some parts of the tactical or strategic functions. The system will detect the abnormal behaviour afterwards and warn users.

(c) High: the attacks will influence the operational function immediately so the users could notice them immediately. For example, if the vehicle suddenly stopped on the road, the users would notice the abnormal situation immediately. In addition, if the cameras around the vehicle breakdown, the system will notice this abnormal situation promptly.

3.3. Consequences of the Attacks

(1) Consequence name: to each possible risk, there may be more than one consequence. The consequences will be listed and then be analysed; more details are presented in Section 4.

(2) Severity of information leakage: information leakage has been a major cyber security issue in computer science. Information leakage attacks usually damage the confidentiality, integrity, and availability of the system [37]. The severity is based on the scale and importance of the leaked information.

(a) Low: the attack will not leak any private information.
(b) Medium: the attack will leak nonconfidential personal information or unimportant information at a small scale. For example, the attacker may know the preference of the passenger on choosing routes or on the entertainment system. This type of information leakage will not cause further harm directly.
(c) High: the attack will leak highly important confidential information such as the financial information, the home address, or the personal ID. With this information, the attackers could conduct further harmful actions to the victims. In other situations, this information leakage would cause larger scale information leakage such as personal data stored in the cloud.

(3) Severity of physical damage: compared with traditional networks, cyber attacks to CAVs could lead to physical damage or even fatalities directly. Tesla vehicle has already caused fatalities on a straight road with good visibility and in a good weather [41]. On March 2018, an Uber autonomous vehicle struck and killed a pedestrian crossing the road in Arizona, USA [42]. The Uber test vehicle failed to detect the pedestrian in the environment of low visibility and failed to conduct any corresponding actions. As a large machine, CAV could cause hazards or even be exploited as a weapon. With the possible consequences, the severity of physical damage can be categorized as below.

(a) Low: the attacks are not likely to cause physical damage to human or other vehicles, and infrastructures
(b) Medium: the attacks are likely to cause small hazards and damage to infrastructures or vehicles, but would not cause fatal injuries to people
(c) High: the attacks have a high possibility to cause fatal injuries

(4) Combined severity level: a method evaluating the combined severity is adapted from risk management in the information system [35]. In the information system, the risks are determined by the likelihood and impact. To determine the combined severity levels to CAVs, a new severity matrix is built based on the severity of information leakage and physical damage, as shown in Table 3. If the severity of information leakage and physical damage are at the same level, then the combined severity will be at the same level as well. However, considering its importance, if the severity of physical damage is high, the combined severity level will be high as well.

(5) Recovery time: this criterion evaluates the time needed to recover to normal situation after the attack has been detected.

(a) Low: after the detection, the damage caused by the attack can be fixed in a timescale of seconds
(b) Medium: after the detection, the damage caused by the attack can be fixed in a timescale of minutes to hours
(c) High: after the detection, the damage caused by the attack can be fixed in a timescale of hours to days

Based on these criteria, possible attacks in different scenarios are analysed in Section 4. It should also be noticed that this paper aims to discuss the possible cyber security attacks to a full CAV (Level 5), where all the possible attacks could be conducted via wireless communication remotely. The physical access of attacks is not considered when evaluating the severity. These criteria may not be comprehensive and exclusive, however could be further refined and extended. This research presents the initial attempt to define and rank the severity of possible attacks in CAV scenarios. This also aims to encourage further research developments to raise public and CAV practitioners' awareness towards CAV cyber security.

4. Possible Attacks

In this section, possible attacks of CAVs are listed and categorized, as shown in Table 4. Following the criteria defined in Section 3, severity of each attack will be analysed. CAV developments concern mainly two streams of research, which are connectivity and automation, covering in-vehicle and intervehicle components. Detailed potential attacks will be analysed within these two streams.

Different autonomous levels may be exposed to different attacks of different possibilities. This paper focuses on the attacks to a fully automated vehicle (i.e., level 5) according to the SAE automation level [20]. Level 5 CAV is capable of all the DDT under all circumstances. It is also assumed that all the vehicles on the road are CAVs. In real-world situations, there will be a mix of CAVs of different automation and traditional vehicles for a certain period of time. In addition,

Table 3: Combined severity level matrix (adapted from [35]).

Information leakage/physical damage	Low	Medium	High
Low	Low	Low	High
Medium	Low	Medium	High
High	Medium	High	High

it is known that CAVs will keep evolving and adapting more technologies. This paper only discusses attacks with existing CAV technologies. However, as the attacks are categorized on automation and connectivity in-vehicle and intervehicle, the list of possible attacks could be extended if new technologies are adapted to CAVs.

4.1. Automation in CAVs. In the current CAV development, all the vehicles from different companies have installed multiple sensors. The mainstream sensors include LiDAR, Radar, and camera [43, 44]. For example, Google Waymo vehicles are installed with a 360 degree camera on the roof as the vision system and several LiDAR sensors and Radar sensors around the vehicle body [45]. There are also supplemental sensors such as the sound detection sensors.

The possible attack target assets are analysed as below.

(1) Audio/entertainment devices: audio devices have already been widely used in modern automobiles. It evolved to a colorful touchable screen showing more information in vehicles [46]. In CAVs, the audio/video system could be used to warn users about anomaly or abnormal behaviours detected in the system or surrounding environments.

  (a) Loud volume: the first possible attack is to suddenly increase the volume of the voice such as background music on board. This attack could distract the passengers' attention or even cause panic in certain situations. The severity of information of leakage is low but the severity of physical damage is medium, which means that the overall severity is low.

  (b) Fake sound: the attacker could use the audio system to make fake noise such as a crash sound. This attack might cause passengers' panic as well, although is not likely to cause information leakage.

  (c) Remote control: this attack already happened in real world. Two white hackers in the USA hacked into a Jeep Great Cherokee from 10 miles away and then stopped the vehicle on a highway road through the entertainment system [47]. This is because the vehicle CAN and the entertainment system are combined together. If an attacker could control the vehicle remotely through the audio/entertainment system, the severity of physical damage could be high. In addition, the risk of information leakage will also be severe because the attackers could send remote instructions to gather private information. Moreover, in CAVs, the remote-control attacks might happen on other components leading to severe risks.

(2) Cameras: cameras provide the vision data, an indispensable part in CAV. To detect the surrounding objects and position the vehicle, camera is a fundamental sensor on CAVs. However, the camera's function could be replaced by other sensors when they break down; thus, camera is of medium importance. There are already successful attacks to cameras to fool vehicles already [48].

  (a) Blind vision: blind vision attack could be easily achieved by physical access. However, with the connectivity of the vehicle, it is even easier for the attackers. The attackers could disable the camera by controlling a strong light resource remotely. The attack would not leak the private information of the vehicle. However, this attack would not cause fatal injuries as well because it is easy to be detected, and CAV contains multisensors' data. If the cameras break down, other sensors could still help to 'see' the environment. Based on this, the overall severity level of the attack is low.

  (b) Mislead camera (fake images): by controlling the cameras remotely, the attackers could inject fake image information to mislead the cameras. This attack is more dangerous than the blind vision attack because the detection possibility is lower. For blind vision attack, the system or the user could easily detect the abnormal situation. While in the mislead camera attack, it may take longer time to detect. In addition, the system might make decisions based on the fake images, the severity of physical attack is thus higher, and the overall severity is high.

(3) Battery system: currently, the number of electric vehicles on road is increasing. As an environment-friendly transportation method, it is believed that the future CAVs would be electric vehicles. The vehicles' battery system would also then be an attack target.

The most possible attack to the battery system is the DoS (Denial of Services) attack. In computer science, the aim of DoS attack is to exhaust all the resources of the target to make the computer, server, or communication channel unavailable. In CAVs, the DoS attack could target the energy sources to exhaust the power sources including heating the seats on the vehicle. DoS attacks could be really dangerous to the battery system. It could trigger different parts to consume battery power in a short time. Sudden battery loss could cause damage to the basic functions of the vehicle. The severity of physical damage is medium, and the combined severity level is medium as well.

Table 4: Possible attacks in CAV.

	Asset name	Importance	Risk name	Difficulty of conduction	Detection possibilities	Consequences	Severity of information leakage	Physical damage	Severity level	Recovery time
Automation	Audio/video devices	Low	Loud volume	Medium	High	Distract passenger's attention	Low	Medium	Low	Low
			Fake sound	Medium	High	Cause passenger's panic	Low	Low	Low	Low
	Cameras	Medium	Remote control	High	Medium	Take control of the vehicle	High	High	High	Medium
			Blind vision	Low	High	Block the vision of vehicles	Low	Medium	Low	Low
			Mislead cameras (fake vision)	Low	Medium	Wrong reactions of vehicles	Low	Medium-high	High	Low
	Battery system	High	DoS	High	Medium	Consuming battery energy	Low	Medium	Medium	High
	Lidar	Medium	Jamming	Medium	Medium	Decreasing the performance of LiDAR	Low	Medium	Low	Medium
			Hidden objects	Medium	Medium	Wrong reactions of vehicles	Low	Medium-high	High	Medium
			Fake objects	Medium	Medium	Wrong reactions of vehicles	Low	Medium	Medium	Medium
	Radar	Medium	Jamming	Medium	Medium	Decreasing the performance of radar	Low	Medium	Low	Medium
			Hidden objects	Medium	Medium	Wrong reactions of vehicles	Low	Medium-high	High	Medium
			Fake objects	Medium	Medium	Wrong reactions of vehicles	Low	Medium	Medium	Medium
	GNSS	Medium	Spoofing	High	Low	Wrong position	Medium	High	High	High
			Jamming	Medium	Low	Signal lose	Low	Medium	Low	Medium
	In-vehicle system	High	Injection	Medium	Medium	Information leakage and wrong reaction	Medium	Medium	Medium	Medium
			Eavesdropping	Medium	Low	Leakage of personal information	High	Low	Medium	Low
			Traffic analysis	Low	Low	Leakage of daily usage	High	Low	Medium	Low
			Modification	High	Medium	Wrong message received	Medium	Medium	Medium	Medium

Table 4: Continued.

	Asset name		Importance	Risk name	Difficulty of conduction	Detection possibilities	Consequences	Severity of information leakage	Physical damage	Severity level	Recovery time
Connectivity	With other vehicles		Medium	DoS	Low	High	Block vehicle communication channel	Low	Medium	Low	High
				Modification message	Medium	Medium	Wrong reactions of vehicles	Medium	Medium	Medium	Medium
				Fake/ghost message	Medium	Medium	Wrong reactions of vehicles	Medium	Medium	Medium	Medium
	With infrastructure	Infrastructure	Low-medium	Change infrastructure sign	Low-medium	Medium	Wrong reactions of vehicles	Low	Medium	Medium	Low
				Block/remove sign	Low	Medium	No reaction in specific position	Low	High	Medium	Low
		Road	Low-medium	Road line/ infrastructure changing	Low	High	Wrong reactions of vehicles	Low	Medium	Low	Low
		Authority	Medium	Fake identity	High	Medium	Identity leakage	High	Medium	High	Medium
	Cloud system	Cloud database	Medium	Injection	High	Medium	Wrong message received	Medium	Medium	Medium	Medium-high
				Modification	High	Medium	Wrong information from cloud	Medium	Medium	Medium	Medium-high

(4) LiDAR (light detection and ranging): LiDAR is the most fundamental sensor in CAVs to support localization and parking assistance [49]. It uses light point cloud to detect the distance and boundaries of surrounding obstacles and environments [50]. The importance of LiDAR is medium. There are successful attempts to attack the LiDAR by using strong lights in a simulation environment [48].

(a) Jamming: this attack jams the LiDAR by using strong lights to reflect the origin light. The attackers could not gather any information through this attack. However, it may lead to physical damage because the detection performance of LiDAR will decrease.

(b) Hidden objects: because LiDAR uses the reflection of light to detect the surrounding environments, the attackers may use special materials to absorb the light to avoid detection. This attack would not cause any information leakage directly. However, in some situations, for example, if the object is covered by special reflection materials, the vehicle would not observe it. This could cause physical damage or even fatal injuries to the target vehicle. The combined severity of this attack is high as it may lead to fatal accident.

(c) Fake objects: the attackers could use light reflection to simulate a fake object, e.g., a barrier in front of the vehicle. The target vehicles would stop or change direction based on the false detection. If multiple vehicles detect this fake object, it could cause severe traffic congestion. Moreover, if there are multiple fake objects on the roads, this attack could cause physical damage when CAVs try to avoid those fake objects. With the other detection methods on the vehicle, however, the possibility of fatal injuries of this attack exists but is low. The severity of physical damage is medium and the combined severity is medium as well.

(5) Radar: unlike LiDAR in CAVs, radar uses radio waves instead of light to detect the surroundings. Currently, there are two types of Radar on CAVs, millimeter Radar [51], and Ultrasonic Radar [52]. The millimeter radar is used on object detection [53], and the ultrasonic radar is used in short distance scenarios such as parking assistance system [54]. This is because the speed of ultrasonic radar is slow, which would lead to poor detection rate in high speed movements. Radar is also of medium importance.

(a) Jamming: this attack is similar to the LiDAR jamming attack. In radar jamming attack, the attackers would use noise to degrade the signal of radar. The attacked radar system might not work properly and the vehicle could not detect the surrounding environments. If the noise source influences multiple CAVs, the traffic flow would be disturbed or it could even cause traffic collisions. This attack would not cause information leakage directly but might cause physical damage. The combined severity of this attack is medium.

(b) Hidden objects: currently, existing technologies are able to hide objects from radar detection and have been already adapted in the area of military aerospace [55]. The planes or the objects hide themselves by changing the regular reflection shape or using radar absorbing materials. In military, the mitigation method is already developed, which is called Radar Antistealth Technology [55]. This technology will strengthen the radar signal. This attack would not cause information leakage but might cause physical damage, or even hurt people directly. The combined severity level of this attack is high.

(c) Fake objects: the attackers broadcast fake radar signals to conduct the attack. Other vehicles would then detect the false signal and take corresponding reactions. This attack would not cause information leakage, however, might cause physical damage to infrastructures, e.g., collisions when vehicles are trying to avoid fake objects. The combined severity of this attack is medium.

(6) GNSS (Global Navigation Satellite System): the most widely used GNSS system is GPS (Global Positioning System) from the USA [56]. Currently, other countries are developing their own GNSS such as Beidou from China, Galileo from Europe Union, and Glonass from Russia [57]. The GNSS system could help to locate and navigate the vehicle. Hacking into this system requires high-level knowledge. The GNSS system is a major resource for positioning and navigation, but as the positioning and navigation are cooperated via V2V communication, the importance of GNSS system is thus medium.

(a) Spoofing: GNSS spoofing attack sends similar GNSS signals to mislead the receivers of the target CAVs. The attackers could use these devices to lead the vehicle to false location or wrong route. In 2013, researchers from the University of Texas at Austin successfully fooled an 80 million dollar super-yacht by their GPS spoofing devices [58]. Compared to the GNSS jamming attack, GNSS spoofing attack would be more dangerous. Without the GNSS signals, CAVs would use other methods such as V2V communication or SLAM (Simultaneous Localization and Mapping) to navigate and avoid the possible hazards such as collisions. However, if the information is wrong and not detected, CAVs would trust the wrong GNSS information and take wrong reactions, which may lead to collisions and fatal injuries. In addition, a vehicle that has been spoofed successfully could respond with private

information such as the location information and historic route information to the attackers, which would also cause information leakage. In that case, the severity of information leakage is medium and the severity of physical damage is high.

(b) Jamming: in the GNSS jamming attack, the attackers will send stronger power signal to the CAV receiver. The GNSS signal is normally weak when they approach the receivers, and it could be easily covered by the jamming signal. The real GNSS signal will then be ignored. In addition, it is also difficult to detect the jamming attack because the GNSS signal is likely to decrease due to interference or limited number of satellites [59]. CAVs could not navigate and locate without the GNSS signal. However, V2V communication could help to navigate coordinately as a backup method. The severity levels of both information leakage and physical damage are medium.

(7) In-vehicle system: in-vehicle system contains the microcontrollers and communication instructions in the vehicle sent by CAN (Controller Area Network) or other communication methods such as WiFi and Bluetooth. The in-vehicle system is related to all the operational functions, thus is of high importance.

(a) Injection: the attackers would inject nonexisting information or even malware to the system through ports such as USB ports. With the fake information, CAVs might make wrong decisions leading to physical damage. As an active attack, injection could also cause leakage of sensitive data. The combined severity of this attack is medium.

(b) Eavesdropping: eavesdropping is a passive attack and is difficult to be noticed. The main objective of this attack is not to cause physical damage but to gain access to valuable data. Thus, the severity of information leakage is high and the severity of physical damage is low.

(c) Traffic analysis: traffic analysis is also a passive attack. The attackers will monitor and observe the data and then try to identify the pattern in the data flow. As a passive attack, the traffic analysis attack would not cause physical damage directly and the scale of information leakage is limited. The combined severity of this attack is low.

(d) Modification: this attack modifies the messages sent between different components and units. The wrong messages could lead to the wrong decision and action of the vehicle. The severity of this attack is medium.

4.2. Connectivity in CAVs. There are three main types of vehicle communication in CAV network. V2V (Vehicle-to-Vehicle) communication is between vehicles via wireless network. V2I (Vehicle-to-Infrastructure) communication is between vehicles and infrastructures via wireless network and V2X (Vehicle-to-Everything) includes V2V, V2I, and communications between vehicles and other entities such as cloud database or pedestrians [60]. Compared with traditional automobiles, these communication methods could help to improve the accuracy of location in rural area and prevent accidents efficiently. Meanwhile, some computer cyber attacks might also happen in CAV environment. For example, in a network cyber attack benchmark KDD99 [61], cyber attacks such as DoS attack could be adapted into V2V communication. Nowadays, many communication technologies are being used in CAV network, e.g., DSRC (Dedicated Short Range Communication), LTE (Local Thermal Equilibrium), and 5G [62].

The possible attack target assets of connectivity are analysed as below.

(8) V2V Communication (with other vehicles): V2V communication is a crucial part in future CAVs. However, there are no general adapted communication standards for V2V communication. Currently, the V2V communication standard in the USA is DSRC, which is based on IEEE 802.11p standard [63]. In Europe, there is ITS-G5 for V2V communication [64]. V2V communication could help to navigate or warn vehicles of potential hazards.

(a) DoS: in addition to the battery system, DoS attack could also happen in the V2V communication. The attackers could send huge amount of data to block the communication channel of the target vehicle from receiving external information. This attack would not cause information leakage but might cause physical damage especially in the rural area, where the V2V communication is the main data source for vehicle planning.

(b) Modification on message/fake message: the communication between vehicles would send different types of information including position coordinates, speed, and head angle. If the attackers send fake messages, the target vehicle would take wrong reactions. In addition, if the target vehicle trusts the fake message, it may respond to the attacker with private information. Based on this, the overall severity is medium.

(c) Hidden vehicle: this attack is also a type of passive attack. The attackers would disable their own message sender to hide their activities. This would not cause information leakage directly, but might cause physical damage if the vehicle hide its activities and approach the target vehicle silently.

(9) V2I communication (with infrastructure): nowadays, there are some initial uses of V2I communication. For example, the ETC (Electronic Toll Collection) on roads and bridges use RFID (Radio Frequency Identification) to charge vehicles [65].

Table 5: Categories of severity of attacks.

Level	Description	Attack types
1	Critical	Remote control (audio/video devices); mislead cameras/fake vision (cameras); hidden objects (LiDAR); hidden objects (radar); spoofing (GNSS); fake identity (cloud authority)
2	Important	Fake objects (LiDAR); fake objects (radar); DoS attack (battery system); injection (in-vehicle system); modification (in-vehicle system); modification (V2V communication); fake/ghost message (V2V communication); change infrastructure sign (V2I communication); injection (cloud dataset); modification (cloud dataset)
3	Moderate	Blind vision (cameras); jamming (LiDAR); jamming (radar); jamming (GNSS); eavesdropping (in-vehicle system); traffic analysis (in-vehicle system); DoS attack (V2V communication); block/remove sign (infrastructure sign); road line changing (road)
4	Minor	Loud volume (audio/video devices); fake sound (audio/video devices)

Apart from the communication channel, which is similar to the V2V communication, there are other attack types in V2I communication.

(a) Change infrastructure sign: the infrastructure signs in transportation help vehicles to navigate, locate, or control speed. CAVs could 'read' the sign and take corresponding actions. If the attackers change infrastructure signs such as the road direction sign, it will lead the vehicle to wrong route. In addition, if multiple traffic lights are changed intentionally, it could cause severe traffic congestion or even traffic collisions.

(b) Block/remove sign: the infrastructure signs could also be blocked or removed physically or remotely. If an emergency alert sign is removed intentionally, this could cause traffic congestion and accidents. However, this attack will not cause information leakage. The combined severity of this attack is medium.

(10) V2X communication (mainly on cloud).

(a) Cloud ID dataset: authority is important in CAV network. Each CAV would be assigned a unique ID such as an electronic plate. In order to confirm the reliability of the communication, only the information from the trusted CAVs in the dataset could be accepted. All the communication and information exchange are based on the authority from the CAV cloud.

(b) Cloud real-time traffic database: cloud database collects the traffic data to provide transportation guidance. It includes the real-time traffic congestion data and accident data to inform all the CAVs to avoid certain areas. If the attackers inject fake messages or modify messages, all the vehicles in the cloud database would receive wrong information. In addition, the attackers could also access valuable information in the dataset.

With the severity criteria, all the attacks are then grouped into four categories, as shown in Table 5. It can be seen that the critical attacks contain remote control, fake vision on cameras, hidden objects to LiDAR and Radar, spoofing attack to GNSS, and fake identity in cloud authority. It could be summarized that all the critical attacks are related to spoofing and falsify messages. These attacks are difficult to realize and they could all lead to wrong reaction or even fatal injuries.

5. Mitigation Methods

For each of the attacks analysed in Section 4, the mitigation methods will be different. By adapting the mitigation methods in information security [35], the main types of mitigation methods could be grouped into five categories. To CAVs, the mitigation methods could be similar but need to be considered based on specific CAV characteristics.

(1) Prevention: these methods prevent the attack from influencing the whole vehicle system negatively. In potential attacks to CAVs, the prevention is for passive attacks such as eavesdropping by encrypting the communication channel and messages. In addition, all the CAV users could be authorized with the credibility of the messages. For example, to the eavesdropping attacks in in-vehicle system, if the communication channel and messages are encrypted, it is much more difficult for attackers to make use of the information.

(2) Reduction: reduction methods reduce the possibility or feasibility of the attack. It could also reduce the possible impacts of the attacks to a controllable level. In CAVs, the reduction methods include the redundant sensors. If one sensor breaks down, the vehicle could still rely on the data from other sensors to reduce the impact of each sensor. For example, to reduce the impact of the blind vision attack to the camera, the vehicle could use other sensors after detecting abnormal attacks.

(3) Transference: transference shares the possible risks with others, such as a reliable third-party organization including governments and insurance companies. For example, in the Cloud of V2X communication, the authority of each CAV's identity should be assigned by the government or relevant legitimate organizations. All the CAVs information should also be stored safely and monitored by the trusted third-party. Not all the

attacks could be resolved by transference. In CAVs, this mitigation method could only be used when a single vehicle manufacturer or a supplier could not handle all the information safely.

(4) Acceptance: acceptance is to retain the risks caused by those attacks with limited negative impacts on CAVs. The attack might not have a proper countermeasure and the impact is at an acceptable level. For example, to the traffic analysis attack in in-vehicle communication, the leaked information could only be the size and timing of the communication package, which is not likely to cause physical damage. In addition, the traffic analysis attack, which is a passive attack, could not be prevented by message and communication channel encryption. In that case, the traffic analysis attack could be tolerated.

(5) Contingency: contingency considers the possible reactions if the attacks happen. A contingency plan needs to be prepared to recover the system once attacked. If the CAV system detects an abnormal battery loss due to the DoS attack, it could pull up the CAV to a safe place.

6. Conclusion

CAV is a fundamental part of intelligent transportation systems and has started attracting increasing research attention in the last few years. Given the importance of CAVs in relation to personal information, physical damages, and passengers' lives, cyber security of CAVs are thus becoming highly important in research developments.

This paper has identified some of the most important cyber attacks to CAVs. For each identified cyber attack, the target asset, the possible risks, and the consequences have been analysed. The severity level of information leakage and physical damage are then estimated and considered based on a new criteria adapted from engineering and software developments. Possible mitigation methods are then categorized and suggested to resolve these attacks.

Among the attacks identified in this paper, the spoofing and falsify messages attacks including remote control, fake vision on cameras, hidden objects to LiDAR and Radar, spoofing attack to GNSS, and fake identity in cloud authority have been identified as the most dangerous attacks to CAVs. All of these attacks would cause severe consequences to information leakage and physical damage.

However, it should also be noticed that CAV technologies are fast evolving. This paper discusses the potential cyber attacks in the existing CAVs technologies and derives the potential attacks based on the traditional cyber attacks. Within the scope of CAV hardware, software, and data, the possible attacks listed in Table 4 will be further extended to reflect the latest developments in CAVs. Meanwhile, the overall severity of each attack is only judged by the listed criteria. It could be further discussed based on other criteria. Due to the emerging infrastructures under construction at different countries, and the unique characteristics of real-world environments required, there is a lack of readily complete testing environments compliant to generally adopted standards available in research and practice. Apart from defining and categorizing the potential cyber attacks, it should also be stressed that the evaluations of the severity of each type of attacks also need to be defined and justified carefully based on real-world field tests. Furthermore, the severity assessment of the listed potential attacks only considers single sensor. For example, in real-world tests, if the cameras fail to recognize an obstacle on the road, the LiDAR and Radar might complement and help to recognize and avoid the obstacle. In some extreme situations, all the sensors or backup elements/functions might be ineffective or fail. The assessment of the severity for different attacks should consider and evaluated the integration of multiple sensors and would also be an interesting topic for future research. In addition, the advantage, disadvantage, and application scenarios of each mitigation method are not the focus in this paper. The presented mitigation methods will be extended and refined further in future research on CAVs cyber security.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors would like to thank Nottingham Geospatial Institute and the School of Computer Science University of Nottingham.

References

[1] H. Fan, Z. Fan, C. Liu et al., *Baidu Apollo Em Motion Planner*, arXiv preprint arXiv:1807.08048, 2018.

[2] M. Dikmen and C. M. Burns, "Autonomous driving in the real world: experiences with tesla autopilot and summon," in *Proceedings of the 8th International Conference on Automotive User Interfaces and Interactive Vehicular Applications Automotive'UI 16*, pp. 225–228, New York, NY, USA, 2016.

[3] Tesla, *Future of Driving*, Tesla, Inc., San Carlos, CA, USA, 2018, http://www.tesla.com/model3.

[4] L. Jones, "Driverless cars: when and where?" *Engineering & Technology*, vol. 12, no. 2, pp. 36–40, 2017.

[5] B. J. Cottam, "Transportation planning for connected autonomous vehicles: how it all fits together," *Transportation Research Record*, vol. 2672, no. 51, pp. 12–19, Article ID 0361198118756632, 2018.

[6] B. Schoettle and M. Sivak, *A Preliminary Analysis of Real-World Crashes Involving Self-Driving Vehicles*, University of Michigan Transportation Research Institute, Ann Arbor, MI, USA, 2015.

[7] K. Bimbraw, "Autonomous cars: past, present and future a review of the developments in the last century, the present scenario and the expected future of autonomous vehicle technology," in *Proceedings of the 12th International*

Conference on Informatics in Control, Automation and Robotics-Volume 1 (ICINCO), pp. 191–198, Colmar, France, 2015.

[8] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," *Transportation Research Part A: Policy and Practice*, vol. 77, pp. 167–181, 2015.

[9] X. Xu and C.-K. Fan, "Autonomous vehicles, risk perceptions and insurance demand: an individual survey in China," *Transportation Research Part A: Policy and Practice*, vol. 124, pp. 549–556, 2019.

[10] X. Kuang, F. Zhao, H. Hao, and Z. Liu, "Intelligent connected vehicles: the industrial practices and impacts on automotive value-chains in China," *Asia Pacific Business Review*, vol. 24, no. 1, pp. 1–21, 2018.

[11] J. Guanetti, Y. Kim, and F. Borrelli, "Control of connected and automated vehicles: state of the art and future challenges," *Annual Reviews in Control*, vol. 45, pp. 18–40, 2018.

[12] D. Li and H. Gao, "A hardware platform framework for an intelligent vehicle based on a driving brain," *Engineering*, vol. 4, no. 4, pp. 464–470, 2018.

[13] World Economic Forum, *Self Driving Vehicles in an Urban Context*, World Economic Forum, Cologny, Switzerland, 2015.

[14] GOV UK, *The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles*, 2018, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles#contentsThe access date is 06/08/2019.

[15] J. Cui, L. Shen Liew, G. Sabaliauskaite, and F. Zhou, *A Review on Safety Failures, Security Attacks, and Available Countermeasures for Autonomous Vehicles*, Ad Hoc Networks, Jaipur, India, 2018.

[16] H. M. Song, R. K. Ha, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in *Proceedings of the 2016 International Conference on Information Networking (ICOIN)*, pp. 63–68, Kota Kinabalu, Malaysia, January 2016.

[17] H. Zhou, W. Xu, Y. Bi, J. Chen, Q. Yu, and X. S. Shen, "Toward 5G spectrum sharing for immersive-experience-driven vehicular communications," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 30–37, 2017.

[18] L. Liang, H. Ye, and G. Y. Li, "Toward intelligent vehicular networks: a machine learning framework," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 124–135, 2019.

[19] M. H. Hashem Eiza and Q. Ni, "Driving with sharks: rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017.

[20] SAE, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE, Warrendale, PA, USA, 2018.

[21] J. Levinson, J. Askeland, J. Becker et al., "Towards fully autonomous driving: systems and algorithms," in *Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV)*, pp. 163–168, Baden-Baden, Germany, June 2011.

[22] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[23] M. Levi, A. Yair, and A. Kontorovich, "Advanced analytics for connected car cybersecurity," in *Proceedings of the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pp. 1–7, Porto, Portugal, June 2018.

[24] Q. He, X. Meng, and R. Qu, "Survey on cyber security of cav," in *Proceedings of the 2017 Forum on Cooperative Positioning and Service (CPGP)*, pp. 351–354, Harbin, China, May 2017.

[25] M. Islam, M. Chowdhury, H. Li, and H. Hu, "Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2672, no. 19, pp. 66–78, 2017.

[26] Y. Li, Y. Tu, Q. Fan, C. Dong, and W. Wang, "Influence of cyber-attacks on longitudinal safety of connected and automated vehicles," *Accident Analysis & Prevention*, vol. 121, pp. 148–156, 2018.

[27] V. Milanes, S. E. Shladover, J. Spring, S. E. Shladover, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 296–305, 2014.

[28] V. Milanés and S. E. Shladover, "Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data," *Transportation Research Part C: Emerging Technologies*, vol. 48, pp. 285–300, 2014.

[29] Y. Feng, S. Huang, Q. A. Chen, H. Liu, and Z. Mao, "Vulnerability of traffic control system under cyberattacks with falsified data," *Transportation Research Record: The Journal of the Transportation Research Board*, vol. 2672, no. 1, pp. 1–11, Article ID 036119811875688, 2018.

[30] D. Satyajeet, A. R. Deshmukh, and S. S. Dorle, "Heterogeneous approaches for cluster based routing protocol in vehicular ad hoc network (vanet)," *International Journal of Computer Applications*, vol. 134, no. 12, pp. 1–8, 2016.

[31] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[32] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (vanets)," in *Proceedings of the 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–9, Gold Coast, Australia, December 2012.

[33] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, Article ID 100214, 2020.

[34] J. Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*, Library of Congress Washington DC Congressional Research Service, Washington DC, USA, 2005.

[35] G. Stoneburner, Y. Alice, and A. Feringa, "Risk management guide for information technology systems," Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2002.

[36] G. Tamasi and M. Demichela, "Risk assessment techniques for civil aviation security," *Reliability Engineering & System Safety*, vol. 96, no. 8, pp. 892–899, 2011.

[37] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013.

[38] W. F. Powers and P. R. Nicastri, "Automotive vehicle control challenges in the 21st century," *Control Engineering Practice*, vol. 8, no. 6, pp. 605–618, 2000.

[39] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education Ltd., London, UK, 6th edition, 2014.

[40] C. Garling, *Why Cars Will Become the Ultimate Mobile Device*, 2017, https://builttoadapt.io/why-cars-will-become-the-ultimate-mobile-device-33dbaad40118The access date is 10/08/2019.

[41] H. C. Barbosa, D. A. Lima, A. M. Neto et al., "The new generation of standard data recording device for intelligent vehicles," in *Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 2669–2674, Rio de Janeiro, Brazil, November 2016.

[42] P. Kohli and A. Chadha, *Enabling Pedestrian Safety Using Computer Vision Techniques: A Case Study of the 2018 Uber Inc. Self-Driving Car Crash*, arXiv preprint arXiv:1805.11815, Texas A&M University, College Station, TX, USA, 2018.

[43] C. J. Jacobus and H. Douglas, "All weather autonomously driven vehicles," US Patent 9,989,967, 2018.

[44] M. Konrad and M. Schramm, "Validation of ADAS by sensor fusion," *ATZ Worldwide*, vol. 120, no. 6, pp. 56–59, 2018.

[45] Waymo, *Waymo Safety Report: On the Road to Fully Self-Driving*, Waymo, Mountain View, CA, USA, 2017.

[46] C. Wang, L. Yu, and H. Yanan, *Automotive Usability: Human Computer Interaction in the Vehicle*, Rensselaer Polytechnic Institute, Troy, NY, USA, 2012.

[47] T. Ring, "Connected cars—the next targe tfor hackers," *Network Security*, vol. 2015, no. 11, pp. 11–16, 2015.

[48] J. Petit, B. Stottelaar, M. Feiri, and K. Frank, "Remote attacks on automated vehicles sensors: experiments on camera and lidar," *Black Hat Europe*, vol. 11, 2015.

[49] R. Kummerle, D. Hahnel, D. Dolgov, S. Thrun, and W. Burgard, "Autonomous driving in a multi-level parking structure," in *Proceedings of the 2009 IEEE International Conference on Robotics and Automation ICRA'09*, pp. 3395–3400, Kobe, Japan, May 2009.

[50] André Ibisch, S. Stümper, H. Altinger et al., "Towards autonomous driving in a parking garage: vehicle localization and tracking using environment-embedded lidar sensors," in *Proceedings of the 2013 Intelligent Vehicles Symposium (IV)*, pp. 829–834, Gold Coast, Australia, June 2013.

[51] L. Kong, M. K. Khan, F. Wu, G. Chen, and P. Zeng, "Millimeter-wave wireless communications for iot-cloud supported autonomous vehicles: overview, design, and challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 62–68, 2017.

[52] U. Farooq, M. Amar, E. Ul Haq, M. Usman Asad, and H. Muhammad Atiq, "Microcontroller based neural network controlled low cost autonomous vehicle," in *Proceedings of the 2010 Second International Conference on Machine Learning and Computing (ICMLC)*, pp. 96–100, Bangalore, India, February 2010.

[53] J. Choi, V. Va, N. Gonzalez-Prelcic, R. Daniels, C. R. Bhat, and R. W. Heath, "Millimeter-wave vehicular communication to support massive automotive sensing," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 160–167, 2016.

[54] W.-J. Park, B.-S. Kim, D.-E. Seo, D.-S. Kim, and K.-H. Lee, "Parking space detection using ultrasonic sensor in parking assistance system," in *Proceedings of the 2008 Intelligent Vehicles Symposium*, pp. 1039–1044, Eindhoven, Netherlands, June 2008.

[55] K. Zikidis, A. Skondras, and C. Tokas, "Low observable principles, stealth aircraft and anti-stealth technologies," *Journal of Computations & Modelling*, vol. 4, no. 1, pp. 129–165, 2014.

[56] J. Jackson, R. Saborio, S. A. Ghazanfar, D. Gebre-Egziabher, and B. Davis, *Evaluation of Low-Cost, Centimeter-Level Accuracy OEM GNSS Receivers*, Minnesota Department of Transportation, Saint Paul, MI, USA, 2018.

[57] B. Hofmann-Wellenhof, L. Herbert, and E. Wasle, *GNSS–Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and More*, Springer Science & Business Media, Berlin, Germany, 2007.

[58] M. L. Psiaki, T. E. Humphreys, and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectrum*, vol. 53, no. 8, pp. 26–53, 2016.

[59] D. Margaria, E. Falletti, and T. Acarman, "The need for GNSS position integrity and authentication in its: conceptual and practical limitations in urban contexts," in *Proceedings of the 2014 IEEE Intelligent Vehicles Symposium Proceedings*, pp. 1384–1389, Dearborn, MI, USA, June 2014.

[60] S. Zhang, J. Chen, F. Lyu, N. Cheng, W. Shi, and X. Shen, "Vehicular communication networks in the automated driving era," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 26–32, 2018.

[61] National Conference of State Legislatures, *UCI Kdd Cup 1999 Data Data Set*, National Conference of State Legislatures, Washington, DC, USA, 1999.

[62] R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: a new 5G technology for short-range vehicle-to-everything communications," *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 30–39, 2017.

[63] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[64] L. Chen and C. Englund, "Cooperative ITS—EU standards to accelerate cooperative mobility," in *Proceedings of the 2014 International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 681–686, Vienna, Austria, November 2014.

[65] Z. Ren and Y. Gao, "Design of electronic toll collection system in expressway based on RFID," in *Proceedings of the 2009 International Conference on Environmental Science and Information Application Technology*, pp. 779–782, Wuhan, China, July 2009.