Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

# Cybersecurity for autonomous vehicles: Review of attacks and defense

*Kyounggon Kim*[a,c], *Jun Seok Kim*[a], *Seonghoon Jeong*[a], *Jo-Hee Park*[b], *Huy Kang Kim*[a,*]

[a] *School of Cybersecurity, Korea University, Seoul, Republic of Korea*
[b] *TMS security TFT, Hyundai Motor Company, Republic of Korea*
[c] *Department of Forensics Science, Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia*

ARTICLE INFO

*Article history:*
Received 11 February 2020
Revised 19 August 2020
Accepted 10 December 2020
Available online 5 January 2021

*Keywords:*
Smart city
Smart mobility
Autonomous vehicle artificial intelligence security survey

ABSTRACT

As technology has evolved, cities have become increasingly smart. Smart mobility is a crucial element in smart cities, and autonomous vehicles are an essential part of smart mobility. However, vulnerabilities in autonomous vehicles can be damaging to quality of life and human safety. For this reason, many security researchers have studied attacks and defenses for autonomous vehicles. However, there has not been systematic research on attacks and defenses for autonomous vehicles. In this survey, we analyzed previously conducted attack and defense studies described in 151 papers from 2008 to 2019 for a systematic and comprehensive investigation of autonomous vehicles. We classified autonomous attacks into the three categories of autonomous control system, autonomous driving systems components, and vehicle-to-everything communications. Defense against such attacks was classified into security architecture, intrusion detection, and anomaly detection. Due to the development of big data and communication technologies, techniques for detecting abnormalities using artificial intelligence and machine learning are gradually being developed. Lastly, we provide implications based on our systemic survey that future research on autonomous attacks and defenses is strongly combined with artificial intelligence and major component of smart cities.



## 1. Introduction

With the rapid development of technology, traditional cities are becoming smarter. The components of a smart city include smart mobility, smart living, smart environments, smart economy, smart governance, and smart people (Khatoun and Zeadally, 2016). Smart mobility is a crucial factor in smart cities. Cyber threats of smart mobility are increasing at a quickening pace. Two security researchers showed critical vulnerabilities for autonomous cars in 2005. The researchers could control the key features of a self-driving Jeep remotely. They could stop the car remotely on the highway. A security research lab, Keen Lab of the Tancent Group, presented their offensive security research to Tesla and BMW autonomous vehicle in 2017 and 2019, respectively, (Keen Security Lab of Tencent, 2017; Cai et al., 2019). Keen Lab also controlled vulnerable features of Tesla and BMW self-driving cars though Wi-Fi and browser vulnerabilities using 0-day exploits. Such tampering with autonomous vehicles is very disruptive to a person's life. For this reason, research on attacks and defenses against autonomous vehicles has continued. However, even though there are many papers related to attacks and defenses

* Corresponding author.
*E-mail addresses:* anesra@korea.ac.kr (K. Kim), seonghoon@korea.ac.kr (S. Jeong), cenda@korea.ac.kr (H.K. Kim).
https://doi.org/10.1016/j.cose.2020.102150

**Table 1 – Counts of selected papers from 2008 to 2019.**

| Category | Subcategory | Method | Count | Total |
|---|---|---|---|---|
| Attack | Automatic control system | ECU attacks | 7 | |
| | | In-vehicle network attacks | 14 | |
| | | Automotive key related attacks | 4 | |
| | Autonomous Driving | Sensor attacks | 5 | |
| | System Components | Mobile app attacks | 6 | 77 |
| | V2X Communications Technologies | VANET attacks | 8 | |
| | | Infotainment attacks | 5 | |
| | Risk assessment | Risk assessment | 15 | |
| | Threat modeling | Attack tree and method | 8 | |
| | | Review | 5 | |
| Defense | Security architectures | CAN/ECU security | 15 | |
| | | VANET security | 6 | |
| | | Design, process, and framework | 9 | |
| | Intrusion Detection System | IDS for CAN | 21 | 74 |
| | | IDS for VANET | 5 | |
| | | ML and DL | 15 | |
| | Artificial Intelligence using Big Data | Cloud and big data | 3 | |
| Total | | | | 151 |

regarding autonomous vehicles, comprehensive surveys are lacking.

In this present study, we reviewed literature from 2008 to 2019 and focused on attacks and defenses technologies related to autonomous vehicles. We focused on research outcomes that meet specific criteria. We searched for specific keywords in Google Scholar, such as “autonomous vehicles,” “connected-car,” “cyber,” “V2X,” “autonomous,” “attack,” “autonomous,” and “security.” We chose additional recently published papers for the categories of attack and defense. A summary of the papers we selected is presented in Table 1. Our review is aimed at readers who are researching in the areas of attack and defense against autonomous vehicles.

The contributions of this report are as follows:

- Research conducted for attacks and defenses against autonomous cars is organized in a chronological order, indicating the technologies that have been used over time concisely.
- 151 papers from 2008 to 2019 on attacks and defenses against autonomous vehicles are summarized.
- Through a comprehensive investigation of attacks on autonomous vehicles, it can be observed that, in the future, attacks on autonomous vehicles will increasingly target vehicle-to-everything (V2X) technology related to communication rather than other simpler elements of the vehicles.
- The research trend in autonomous vehicle security indicated that artificial intelligence with big data has been used to defend autonomous vehicle attacks.

The remainder of this paper is organized as follows. Section 2 addresses the major elements of autonomous vehicles, such as automotive control systems, autonomous driving systems components, and V2X communication technology. In Section 3, we summarize cyber-attack papers involving autonomous vehicles and V2X. Section 4 describes cyber-defense techniques in autonomous vehicles. Finally, Section 5 summarizes our observations and concludes the paper.

## 2. Key elements of autonomous vehicles

To investigate the security aspects of autonomous vehicles, we identified three key elements, as depicted in Fig. 1:(i) automotive control systems, (ii) autonomous driving system components, and (iii) V2X.

### 2.1. *Automotive control systems*

An automotive control system consists of an in-vehicle network that connects the main device and the other devices. The key parts of automotive control systems used in autonomous vehicles are classified as units and networks. The most important units are electronic control units (ECU). The ECU controls the state of the automatic transmission of the vehicle engine and manages the sensors inside the vehicle. Some representative types of ECUs are body control modules and powertrain control modules. Body control modules include modules for the door, seat, power lock, airbag, air condition system, and light control. Powertrain control modules include an anti-lock brake system (ABS), an engine control unit, and a transmission control unit. ECUs include the central timing module, central control module (CCM), brake control module, transmission control module, powertrain control module, engine control module, suspension control module, general electronic module, and body control modules (Yoshiyasu Takefuji, 2018; Koscher et al., 2010). Typically, small- and medium-sized vehicles include approximately 50 ECUs (Tettamanti et al., 2016), and at least 70 ECUs are included in luxury cars (Kim et al., 2008). Some cutting-edge vehicles have up to 80 ECUs due to new functionality (Takefuji, 2018).

An in-vehicle network interconnects the ECUs and transfers the data among them. This network includes

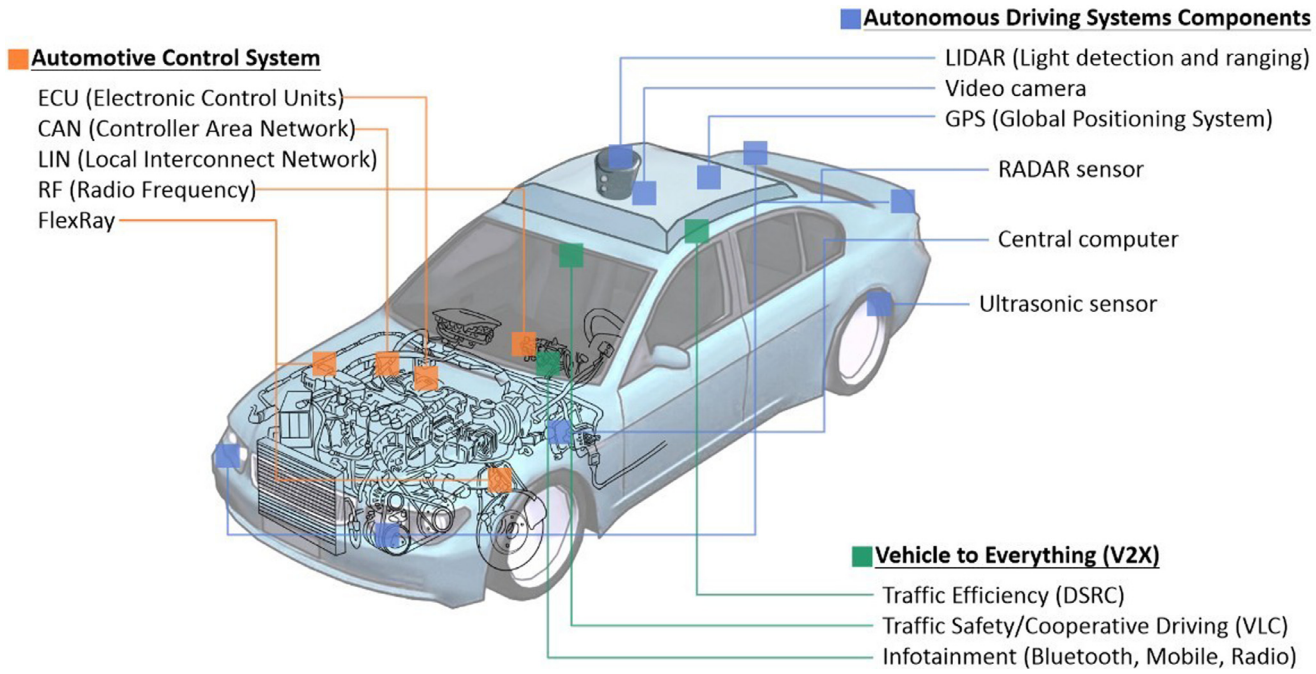



**Fig. 1 – Key elements of autonomous vehicles.**

**Table 2 – Inter-vehicle wired interconnection technologies in autonomous driving (Wang et al., 2018).**

| Network | CAN | LIN | Domestic digital bus | FlexRay | Ethernet | Media-oriented systems transport | Interface description block | Low-voltage differential signaling |
|---|---|---|---|---|---|---|---|---|
| Maximum date rate | 1 Mb/s | 19.2 Kb/s | 11.2 Mb/s | 20 Mb/s | 100 Mb/s | 150 Mb/s | 400 Mb/s | 655 Mb/s |
| Topology | Linear bus, star, ring | Linear bus | Ring | Linear bus, star, or hy-brid | Linear bus, star | ring | Linear bus, star, ring | Point to point |
| Cost | Medium | Low | High | High | Medium | High | High | High |

the controller area network (CAN), local interconnect network (LIN), domestic digital bus, FlexRay (Makowitz, 2006), Ethernet, media-oriented systems transport, interface description block, and low-voltage differential signaling, as listed in Table 2.

The CAN protocol is a data communication ISO standard and is registered as ISO 11,898 (ISO, 2015). Robert Bosch GmbH invented the CAN bus protocol in 1986; it was originally designed for automobiles (Voss, 2008; Herrewege et al., 2011). In 1988, the BMW 8 series was the first production vehicle to adopt the CAN-based communication system (Learning About Electronics, 2018). It uses the CAN as a core network for body systems, engine management, and transmission. The CAN ID (identifier) is an 11-bit framework and can be divided into IDH and IDL or combined to be used as a single ID. If the CAN ID is 02B3, the IDH is 02 and the IDL is B3. The LIN was invented in 1998 based on a consortium of automotive companies, such as Audi, BMW, Daimler-Chrysler, Volcano, Volvo, Volkswagen, and Motorola. The LIN 1.1 standard was introduced in 2000 and adapted in the first production vehicle in 2001. The LIN 2.0 standard was developed in 2003 (Nolte et al., 2005). LIN is a low-speed single-master network commonly used for door locks, climate controls, seat belts, sunroof, and mirror controls. FlexRay is a next-generation automotive bus technology that provides high-speed and fault-tolerant communications. Kukkala et al. (2017) studied the introduction of FlexRay into jitter-aware message scheduling in automotive networks.

### 2.2. *Autonomous-Driving-System components*

The key components of autonomous driving systems are light detection and ranging (LIDAR) sensor, video camera, Global Positioning System (GPS), radio detection and range (RADAR) sensor, central computer, and ultrasonic sensor (Kong et al., 2017; The Economist, 2013).

LIDAR is a technology that uses light to detect objects and measure distances. LIDAR uses a shorter wavelength laser to achieve higher measurement accuracy and better spatial resolution than RADAR. Video cameras read traffic lights and road signs and monitor pedestrians and obstacles. The GPS receiver collects signals transmitted from three or more GPS satellites to determine the position of the receiver. Once the

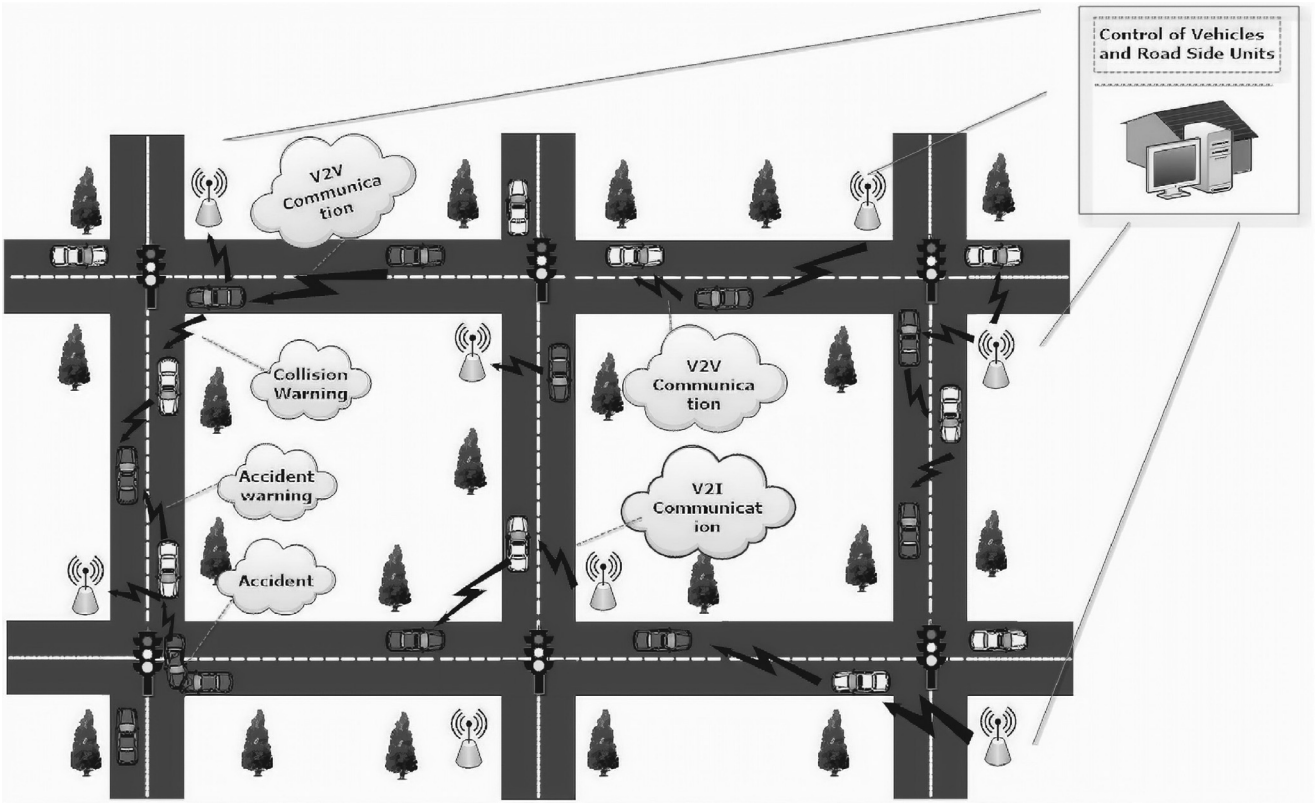



**Fig. 2 – Illustration V2X communications (Malhi et al., 2020).**

receiver knows the distance to at least three satellites and the position of each satellite, the position of the receiver can be calculated using trilateration. RADAR refers to a detection system that measures the distance, direction, angle, and velocity of a target using radio waves. RADAR in an autonomous vehicle is used to recognize environment of a vehicle in real time. The central computer receives information from all sensors and manages steering, accelerator, and brakes. Central computer software interprets regular or irregular road conditions. Ultrasonic sensors are used to measure the position of very close objects such as curves and nearby vehicles.

### 2.3. *V2X communication technologies*

The network communication between the car and the external terminal is referred to as V2X. V2X technology consists of vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-network communications, as illustrated in Fig. 2.

Vehicle ad-hoc networks (VANETs) are an area of significant interest for researchers of V2X communications. VANET uses dedicated short-range communications (DSRC). It is based on the IEEE 802.11p standard for wireless access in vehicular environments. IEEE 1609 is a higher layer standard based on IEEE 802.11p, and defines the standards, architecture, and interfaces for secure V2V and V2I communications. DSRC includes an on-board unit inside the vehicle and infrastructural road-side units (RSU) outside the vehicle. The on-board unit is composed of a communication control unit, routing table, and local dynamic map: (i) the communication control unit is a unit for communication between the interior and exterior of the vehicle; (ii) the routing table stores neighboring vehicle information and timestamps; (iii) the local dynamic map is a map database that stores information on road conditions and traffic surrounding the vehicle. The RSU is a device for V2I communication. It communicates with location servers through a wired/wireless network for tracking information on all vehicles. The service infrastructure of a RSU includes the traffic-management system, public-key infrastructure, and RSU management center (Lee et al., 2014).

Another communication structure required for V2X is the mobile cellular network, referred to as Cellular V2X (C-V2X), which currently uses the long-term evolution technology. C-V2X is superior to DSRC in terms of communication over a wider area, existing infrastructure environment, and security factors. In addition to DSRC and C-V2X, V2X communications use technologies such as satellite radio and Bluetooth for V2X applications. V2X communication technologies have several security vulnerabilities that will be explained in Section 3.

## 3. Attacks on autonomous vehicles

In this section, we investigate cyber-attacks for autonomous vehicles based on the components of autonomous vehicles and the historical timeline. We classified attack research on autonomous vehicles as automotive control systems, autonomous driving systems components, V2X communication, and risk assessment, as depicted in Fig. 3.

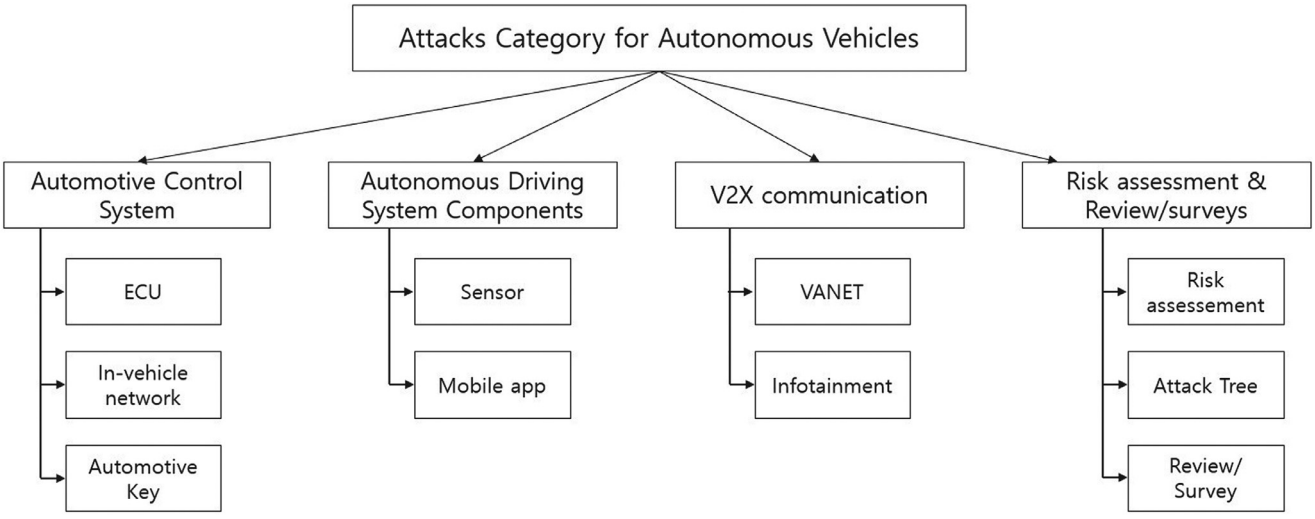



**Fig. 3 – Categories of Attack Research on Autonomous Vehicles.**

**Table 3 – Research on automotive control systems.**

| Attack category | Authors | Year | Approach and experiment |
|---|---|---|---|
| ECU attacks | Koscher et al. (2010) | 2010 | Experimental result regarding modern automobile hacking |
| | Ishtiaq Roufa et al. (2010) | 2010 | Vulnerability in tire pressure monitoring system case |
| | Salfer et al. (2014) | 2014 | On-board networks attack forest construction |
| | Shukla (2016) | 2016 | Vulnerability analysis of automotive software (ECU) |
| | Burakova et al. (2016) | 2016 | Experimental analysis of the SAE standard |
| | Nie et al. (2017) | 2017 | Full attack chain to CAN BUS and ECU remote controls |
| | Halahan & Chen (2017) | 2017 | Wireless for TPMS, ECU |
| In-vehicle network attacks | Hoppe & Dittman (2007) | 2007 | Sniffing/replay attacks on CAN buses |
| | Hoppe et al. (2008) | 2008 | Conducting four empirical tests on the automotive control system |
| | Larson & Nilsson (2008) | 2008 | Analyzing automotive wireless communication security problem |
| | Nilsson et al. (2009) | 2009 | Describing two attacks in FlexRay bus-read and spoof |
| | Miller & Valasek (2013) | 2013 | Practical ECU remote code execution. |
| | Smith (2016) | 2016 | Published “The Car Hacker’s Handbook" for penetration tester |
| | Palanca et al. (2017) | 2017 | Denial-of-Service attack for link-layer automotive |
| | Pan et al. (2017) | 2017 | Attack scenario from a malicious smartphone application to CAN |
| | Fowler et al. (2017) | 2017 | Prepared testbed and built for a CAN simulator |
| | Martinelli et al. (2017) | 2017 | Fuzzy neural network algorithm to identify CAN protocol communication |
| | Fröschle & Stühring (2017) | 2017 | Analyzing the capabilities of the CAN attacker |
| | Li et al. (2018) | 2018 | Attack via ECU (Reversing ECU, side-channel attack) |
| | Fowler et al. (2019) | 2019 | Fuzz testing for CAN prototypes |
| | Payne (2019) | 2019 | Step-by-step attack procedure through detailed CAN Bus Protocol analysis |
| Automotive Key related attacks | Francillon et al. (2011) | 2011 | Relay attacks on passive keyless entry (Risk of PKES system) |
| | Verdult et al. (2012) | 2012 | Demonstrate Hijacking with Hitag2 |
| | Verdult et al. (2013) | 2013 | Cipher authentication protocol and key-update mechanism |
| | Garcia et al. (2016) | 2016 | ECU/Remote keyless entry system vulnerability |

### 3.1. *Attacks on automotive control systems*

Attacks on automotive control systems typically target the ECU, in-vehicle network, and automotive key. Research papers related to this area are listed in Table 3.

#### 3.1.1. *ECU attacks*

In 2010, Koscher et al. (2010) published a study that identified the key ECUs in detail, as listed in Table 4. They investigated security challenges faced by the CAN, including the lack of authentication fields, weak access control, and denial-of-service (DoS) vulnerabilities. They performed CAN packet sniffing, target probing, reverse-engineering, and fuzzing to verify the attack methodology. They attempted to attack the ECU and found that fuzzing is very effective method to find vulnerabilities for CAN. These attacks allow an attacker to load firmware without authorization into major ECUs, such as remote-control door lock receivers and telematic devices. The authors found that an attacker can maliciously manipulate a car’s speed and display information through a compromised telematics unit, as depicted in Fig. 4. The authors evaluated the real-time performance of the modern automobile CAN network and proved the vulnerability of the structure.

**Table 4 – Key ECU components and functionality associated with CAN bus.**

| Component | Functionality | Low-Speed Comm. bus | High-Speed Comm. bus |
|---|---|---|---|
| ECM | *Engine control module*. Uses information from sensors to determine the amount of fuel, ignition timing, and other engine parameters. | | V |
| EBCM | *Electronic break-control module*. Controls the anti-lock brake system pump motor and values, preventing brakes from locking up and skidding by regulating hydraulic pressure. | | V |
| TCM | *Transmission control module*. Controls electronic transmission using data from sensors and from the engine control modules to determine when and how to change gears. | | V |
| BCM | *Body control module*. Controls various vehicle functions, provides information to occupants, and acts as firewall between two subnets. | V | V |
| Telematics | *Telematics module*. Enables remote data communication with vehicles via a cellular link | V | V |
| RCDLR | *Remote-control door lock receiver*. Receives the signal from the car's key to lock and unlock doors and trunk. It also receives data wirelessly from the tire pressure monitoring system sensors. | V | |
| HVAC | *Heating, ventilation, and air conditioning*. Controls the cabin environment. | V | |
| SDM | *Inflatable restraint sensing and diagnostic module*. Controls airbags and seat belt pretensioners. | V | |
| IPC/DIC | *Instrument panel cluster/driver information center*. Displays information to the driver about speed, fuel level, and various alerts about car's status. | V | |
| Radio | *Radio*. In addition to regular radio functions, funnels and generates most of the in-cabin sounds (beeps, buzzes, and chimes) | V | |
| TDM | *Theft-deterrent module*. Prevents vehicle from starting without legitimate key. | V | |


**Fig. 4 – Displaying arbitrary message and false speedometer reading on Driver Information Center. (Koscher et al., 2010).**

This study is meaningful in that it is the earliest study that identifies the EUC in detail and directly attacks the ECU.

Ishtiaq Roufa et al. (2010) described a tire pressure monitoring system (TPMS) that could sniff personal information, which could be leaked to an attacker while wirelessly communicating status information. The authors highlighted the TPMS as the first wireless network in the vehicle. This study substantially evaluated TPMS through experiments. It also contributed significantly to the verification of the impacts that can be generated on privacy and security through the modified TPMS. The TPMS does not use any cryptographic mechanisms; it sends fixed sensor IDs to each packet, and it is highly possible to track vehicles through it. In addition, there is no authentication for the transmitted message, and the vehicle's ECU also does not verify the input value. This allows the attacker to use a malformed message to display a tire pressure warning to the next car on the highway or to disable the TPMS ECU.

To automate the assessment of vulnerability, Salfer & Eckert (2015) proposed a methodical and automated measurement method based on ECU development data and software images. The metrics of this methodology were designed for ease of evaluation, such as code review and penetration testing. The attack interface includes a diagnostic protocol, an external interface such as a USB, a user interface through the driver, and a low-level hardware interface.

Shukla (2016) explained the weaknesses of typical ECU software, the procedure to attack networks such as CAN, and existing security countermeasures available in tricore architecture. He further explained a method of exploiting vulnerabilities in the ECU software. His-study described the software framework of the Automotive Open System Architecture (AUTOSAR) standard for intelligent mobility. A tricore microcontroller analyzes the vulnerabilities in the ECU to understand and exploit further vulnerabilities using the already discovered ones.

Burakova et al. (2016) experimented on Class-8 semi-tractors and school buses. This experiment highlights how simple it is to attack vehicles that are sold in the real world. Above all, it proves that the same attack can be repeated on all other vehicles that comply with the SAE J1939 vehicle security standard. The authors demonstrated their awareness

of vehicle safety (trucks and buses) using the same standards and illustrated specific attacks that can affect critical systems (ECU, CAN, etc.). They warn that the attacks can be carried out broadly, irrespective of the target, as they focus on the SAE J1939 network standard.

Tesla revealed an entry-level electric vehicle model in 2017. As Tesla entered the automotive market, electric vehicles such as Tesla became the main target of attacks. Nie et al. (2017) focused on discovering new security vulnerabilities that were not known in Tesla vehicles. They experimentally demonstrated how the ECU can be controlled remotely by sending arbitrary CAN packets to a Tesla vehicle updated with the latest firmware. They tested the vulnerabilities of Tesla models S P85 and P75, the latest versions at that time. First, after searching for browser vulnerability, the vehicle was attacked by attracting users to the Wi-Fi hotspot. They damaged many in-vehicle systems, such as integrated circuit and gateways, via wireless (Wi-Fi/cellular) technology and then injected malicious CAN messages. After this discovery, Tesla vehicles were updated using the over-the-air (OTA) mechanism, and code signing protection was applied.

Halahan & Chen (2017) explored how a vehicle can potentially be hacked. They divided process of hacking a car into three steps: (i) the first is to remotely compromise, (ii) the second is to inject messages via cyber or physical components, and (iii) the final step is to allow the ECU to perform the tasks desired by the attacker. Hacking types include indirect physical access, short-range and long-range wireless communications, and dongle-based attacks. Hacking threats include data collection and eavesdropping. They suggested that the countermeasures against attacks are to design secure vehicle, considering the risks and threats. They also addressed that continuous monitoring and communicating suspicious activity is necessary to develop a secure vehicle network.

#### 3.1.2. *In-vehicle network attacks*

Initially, there were attack studies on internal networks such as CAN and FlexRay (Hoppe and Dittman, 2007; Nils- son et al., 2009). Hoppe & Dittman (2007) performed sniffing and replay attacks to CAN bus networks in automotive control systems. Hoppe et al. (2008) explored vehicular security threats on the CAN bus. Based on their test environment, the authors presented a classification on four scenarios. For each scenario, they specified the objective of the attack, mode of the attack, and related vulnerabilities. Larson et al. (2008) proposed a conceptual network topology for the CAN bus, including a gateway. In the attack model, the attackers mentioned six types of attacks, including passive (such as reading messages) and active attacks (particularly injection attacks, such as flood, replay, and spoof).

In 2009, Nilsson et al. (2009) analyzed the FlexRay protocol and evaluated its functionality to verify whether it can withstand cyber-attacks. Their study described experiments where the ECU on the FlexRay bus was attacked. The authors defined and described two attacks, reading and spoofing, that, in the FlexRay network, can be conducted from any ECU. On the FlexRay bus, there is no encryption of data; therefore, an attacker can read all the data sent to the bus. The attacker can also create and insert an unauthenticated message in the data flow that is sent to the bus. Messages flowing on the bus can thus be spoofed by an attacker, and any targeted ECU can be deceived.

The year 2013 was important in the history of car hacking. Miller & Valasek (2013) presented an outstanding research result on offensive security. They demonstrated its application to the technological accessories embedded in the Ford Escape and the Toyota Prius. The experiment demonstrated that the vehicle's ECU can allow remote code execution through a variety of interfaces, such as Bluetooth and telematics devices. The authors also proposed mechanisms to detect various types of attacks. They used the OBD-II connector shell available from obd2allinone.com. The CAN message implemented in the Toyota Prius contains a message checksum at the end of the data byte. Only the most important CAN packets contain a checksum. The experiment was conducted by sending a proprietary message to the ECU. The Ford engine used in the experiment is a well-established vehicle, which is set to not operate when too much or too little gas or air is injected. This is the specific routine control set in Ford 4044. For example, the packet sent by the attacker is

*IDH: 07, IDL: E0, Len: 08, Data: 05 31 01 40 44 FF 00 00*

Each parameter presented here is a bit field. In this test, because the CAN was overloaded with the CAN packet, service was denied, as depicted in Fig. 5.

The year 2016 and 2017 were the most active periods for research on car attacks. Smith (2016) published a book titled *The Car Hacker's Handbook: A Guide for the Penetration Tester*. This handbook describes various points of attack methodologies and attack processes that can be used to hack vehicles. Beginning with detailed explanations of the concepts and related policies of vehicle security, it goes on to explain the methods of security and threat testing on vehicles. It is also demonstrated how hardware vulnerabilities can be drawn and tested. This book contains information related to automotive buses, CAN networks, vehicle diagnostic and logging methods, CAN bus reverse engineering, ECU-related concepts, and other attack threat models.

Palanca et al. (2017) demonstrated that selective DoS attacks are possible for vehicles communicating via CAN. They also emphasized that such an attack cannot be detected at the frame level. This attack is based on the vulnerability of the CAN protocol, which is vulnerable irrespective of the manufacturer. The authors illustrated the concept by experimenting with cars that are currently in use and proved how easy such an attack is. Pan et al. (2017) explained various scenarios of attacks on vehicles. They also explained the dangers vehicle damaged by an attack through a CAN bus. Direct examples illustrate various attack scenarios, emphasizing that a malicious attacker can attack the CAN bus, disturb the vehicle control system, and cause physical harm to drivers and passengers in the vehicle.

Fowler et al. (2017) proposed attacks via a CAN simulator. Using on-board diagnostic (OBD) scanners, which are readily available after a vehicle is purchased, CAN vulnerabilities have been demonstrated and verified. The authors have been implemented according to the J3061 guidelines commonly used by the automotive industry to design security. Martinelli et al. (2017) conducted research using the fuzzy neu-


**Fig. 5 – Instrument cluster indicating that something is definitely wrong (Miller and Valasek, 2013).**

ral network algorithm to identify CAN protocol communication attacks of four types (DoS, fuzzy, spoofing the drive gear, and spoofing the RPM gage). The authors proposed a method for detecting attacks targeting the CAN protocol. They verified that the actual data embedded in the CAN packet was used as a feature vector. They also showed that each fuzzy classification algorithm can achieve a precision of 0.85 to 1 in an attack aimed at CAN protocol identification. Fröschle & Stühring (2017) explained vehicle network security based on a systematic understanding of the CAN protocol. They developed an invulnerable security concept for the CAN. They derived an abstract model from the attacker's perspective that targets the CAN. To accurately verify the derived model, they attempted to improve the demonstration of the attack model by considering the potential impact on the actual vehicle.

Li et al. (2018) attacked the mounted infotainment system in a vehicle. The infotainment system is vulnerable to attacks because it can control the CAN buses of the vehicle, ECUs, etc. The authors used ECU reversing and side-channel attacks as attack methods, which proved to be successful in real experiments. They described the attack surface of modern vehicles and provided a deep analysis of the CAN frame. The side-channel attack method used in the study determined the key using leaked signal information in the process of encryption or a replay attack.

In 2019, a representative fuzzing technique for automobile attacks was introduced. Fowler et al. (2019) used fuzzy-testing to investigate the vulnerability of CAN prototypes. They conducted black-box fuzzy testing of display ECUs for experimental vehicles, demonstrating the weakness of the vehicle system design. Fuzzing is a typical method used to detect software vulnerabilities. The distinction is that a CAN packet is used for the display ECU. Payne (2019) described a clear step-by-step process for hacking cars through a detailed analysis of the CAN bus protocol. It was mainly targeted at faculty, students, and researchers with the necessary tools, such as the curriculum and practice environment required to implement vehicle hacking. For as little as $100, it introduces tools for reverse engineering CAN bus messages as well as related CAN-to-USB bus cables or wireless connector combinations.

ECUs and CANs continue to be the targets of attacks. Initially, they were physically connected and attacked, but recently, advanced techniques such as side-channel and fuzzing have been applied together.

#### 3.1.3. *Automotive-Key-Related attacks*

Francillon et al. (2011) attacked passive keyless entry and start (PKES) systems, which are widely used in modern cars. They demonstrated the relay attack method by duplicating the existing signal. They proved that wireless attacks are possible via transceivers. Furthermore, the authors conducted a risk assessment of ten vehicle models from eight vehicle manufacturers. They emphasized the impacts of relay attacks, suggested alternatives to prevent them.

Verdult et al. (2012) analyzed real-world vulnerabilities in cryptographic designs applied to automobiles. They demonstrated a real attack using wireless communications to recover private keys. The authors introduced malleability and time-memory trade-off attacks against Hitag2. Malicious attacks exploit the unique weaknesses of Oracle by randomizing the key stream lengths. One of the weaknesses of Oracle is the time-memory trade-off. This approach is also applicable to linear-feedback shift register-based stream ciphers with sufficient continuous key streams. Cryptanalytic attacks combine two weaknesses, dependency between sessions and low degree of filter functionality. This attack allows the attacker to recover a secret key after collecting the key from the car through a few authentication attempts. The strongest attacks can recover the secret key from a car within six minutes using common hardware.

Verdult et al. (2013) reverse-engineered the security mechanism of transponders used for encryption authentication. To this end, the key value was obtained or duplicated using the weak points of the cryptographic design and authentication protocol. The vulnerability of the key transponder update mechanism was exploited when updating or changing the key. The authors proved that the encryption key used for authentication is set such that it is too weak for the actual vehicle. They experimented with the vulnerability of the transponder and suggested possible challenges.

**Table 5 – Research on autonomous driving system components.**

| Attack category | Authors | Year | Approach and experiment |
|---|---|---|---|
| Sensor attacks | Wyglinski et al. (2013) | 2013 | New form of vulnerability into critical infrastructure sensors |
| | Amoozadeh et al. (2015) | 2015 | Cooperative adaptive cruise control (CACC) |
| | Yan et al. (2016) | 2016 | Attacks for RADAR, cameras, and ultrasonic sensors |
| | Lim et al. (2018) | 2018 | Attack simulation for ultrasonic sensor |
| | Yeh et al. (2018) | 2018 | Security risks automotive for RADAR and DSRC |
| Mobile app attacks | Woo et al. (2015) | 2015 | An attack with malicious smart-phone app |
| | Jafarnejad et al. (2015) | 2015 | Remotely critical systems control of the vehicle |
| | Yan (2015) | 2015 | Survey on security challenges in automotive threat for 2 years |
| | Mazloom et al. (2016) | 2016 | Security analysis for in-Vehicle-infotainment systems (IVI) |
| | Tod Beardsley (2017) | 2017 | Hyundai Blue Link cleartext communications |
| | Eriksson et al. (2019) | 2019 | Static tool for code analysis |

Garcia et al. (2016) described the vulnerability of a vehicle immobilizer (key) used primarily by vehicle manufacturers and original equipment manufacturers. First, they recovered encryption algorithms and keys to and from the immobilizer. Next, a VW Group remote-control signal was transmitted using the recovered key, and the signal sent from the vehicle was eavesdropped upon to allow arbitrary access to the vehicle. This attack can recover the encryption key and replicate the remote-control key with four to eight rolling codes and a short calculation time. The results of this study affected millions of vehicles worldwide and are now considered a significant component of physical vehicle security.

### 3.2. *Attacks on autonomous driving system components*

Attacks on autonomous driving components are clearly different from traditional automobile. In this section, we investigate studies that focus on attacks on the main components of autonomous vehicles. Research papers related in this field are listed in Table 5.

#### 3.2.1. *Sensor attacks*

Wyglinski et al. (2013) provided insights into the challenges and security aspects of autonomous vehicles. This study suggested better opportunities in terms of sensors that can be applied to vehicles with more complex embedded computing. The authors performed a case study on automotive computing and sensing. They analyzed the LIDAR sensors, wireless access, autopilots and navigators, sensors, and actuator controls as components of autonomous vehicles. They also addressed steganographic attacks, hardware and firmware attacks, information leakage eavesdropper attacks, sensor attacks, and physical chip-tampering attacks.

Amoozadeh et al. (2015) discussed security attacks on the communication channels used in vehicles and studied the sensor operation of connected vehicles that can perform cooperative adaptive cruise control (CACC). CACC is an extended concept of adaptive cruise control. The simulation results presented in this study proved that insider attacks can cause serious problems in CACC vehicle networks. It presented alternatives to downgrading to the existing adaptive cruise control mode instead of CACC or other countermeasures. Yan et al. (2016) explained that sensor security is a crucial issue in autonomous vehicles and is a real challenge from a safety standpoint. They studied automated driving systems for Tesla vehicles and three essential sensors: (i) ultrasonic sensor, (ii) millimeter wave RADAR, and (iii) cameras deployed for use with autopilots. The results indicated that radio interference and spoofing attacks were possible.

Lim et al. (2018) emphasized the significance of ultrasonic sensors applied to autonomous vehicles. They described possible vulnerability assessment methods applicable to obstacle detection devices for commonly used sensors. Possible attack scenarios were derived through ultrasonic sensors and were proven experimentally by simulation. They pointed out the inaccuracy of attempting to detect an obstacle using ultrasonic sensors applied to a vehicle. Experimental results indicated that nearby attackers could intercept or randomly remove the ultrasonic sensor. They emphasized that these attacks were very easy to carry out and were easily available at low cost. Yeh et al. (2018) presented the unique security flaws of automotive RADAR and DSRC technologies. The author emphasized removing security risks as quickly as possible by simulating various attacks on this technology.

#### 3.2.2. *Mobile app attacks*

In 2015, Woo et al. (2015) reported that in a connected vehicle environment, a malicious smartphone app can carry out long-range wireless attacks. They analyzed CAN vulnerabilities and designed a security protocol applicable to vehicles after demonstrating the attack model. Based on Secure-ECU and CANoe, which is comprehensive software tool for the development, testing, and analysis of ECUs, they conducted a security and performance analysis of the proposed security protocol. Jafarnejad et al. (2015) developed a platform that allowed them to access a vehicle's internal systems. Through this platform, they could remotely access the interior and manipulate the actual vehicle. This is referred to as the open vehicle monitoring system. The authors had access to a Sevcon Gen4 controller to operate the vehicle. They developed a web interface and Android mobile application for smooth vehicle operation. All these tests were conducted on real vehicles, which emphasized the possible risks. Yan (2015) conducted a two-year survey on problems in autonomous vehicle security. The research report covered nearly all types of connected cars from cloud platforms, and OBD dongles to auto apps, proving to be the most comprehensive report on the current connected-car-threat situation. The author provided a guide to help au-

tonomous vehicle companies in identifying vulnerabilities in their products and services.

Mazloom et al. (2016) proved that vehicle attacks were possible through a vehicle driver's smartphone. First, an attacker who steals the control of a smartphone from a driver sends a malicious message to the vehicle's internal network using the MirrorLink protocol. Thereafter, the attacker can send CAN packets. Thus, it was established that attacks are possible, and the vulnerabilities of the MirrorLink protocol and IVI implementation were highlighted. The attack method illustrated in the experiment demonstrated that the message causes a heap overflow to manipulate the vehicle.

Tod Beardsley (2017), from the security company Rapid7, announced a vulnerability in Blue Link, a vehicle control application. He discovered that the Blue Link vulnerability impacted Hyundai Motors in Korea. An attacker could extract the username, password, and personal identification number (PIN), while the Blue Link app sent personal information to Hyundai. In addition, the attacker could exploit this vulnerability to launch a fatal attack that could be initiated remotely by unlocking the vehicle.

Eriksson et al. (2019) investigated vulnerability with a focus on Android car apps developed by car manufacturers. They considered road safety and security factors that affect users. They investigated the attack surface and vulnerability of in-vehicle apps and suggested countermeasures for fine-grained permission, API control, system support, and information flow. They also developed AutoTame, a static tool for code analysis.

As we have seen so far, attacks on autonomous driving elements have mainly focused on attacks on sensors and attacks through mobile apps. As the control function of autonomous vehicles through smartphones is strengthened, mobile devices, which are relatively vulnerable to attack, are expected to become the main targets for attack.

### 3.3. *Attacks on V2X communications technologies*

The most active research area for attacks on autonomous vehicles is in the V2X field. Research papers related to this area are listed in Table 6.

#### 3.3.1. *VANET attacks*

Attacks on VANET is a major field that has been continuously researched since 2008. Larson & Nilsson (2008) analyzed a security problem for wireless communication transmission from the outside. They used a defense-in-depth view of the wireless communication segment. They also analyzed security issues for each of the prevention, detection, deflection, countermeasure, and recovery layers for the autonomous vehicle. Brooks et al. (2009) discussed system stakeholders, including manufacturer, private customer, fleet owners and leasing companies, service providers and dealer. They also summarized vehicle and communication use-cases. They suggested modified CERT taxonomy for the automotive security domain. The attack on VANETs covered the man-in-the-middle attack, bogus information attack, DoS, location tracking, malicious codes, and replay attacks. The types of ECU flashing attacks include modifying codes, phishing attacks, fuzzing attacks, and reverse engineering. For the integration of business service attacks, they described brute force, social attacks, DoS, malicious codes, and reverse-engineering.

Checkoway et al. (2011) insisted that they are the first researchers to identify attack surfaces from outside rather than inside the vehicle, and they actually experimented with attacks. They demonstrated two types of hacking: (i) technical hacking and (ii) Operational hacking. Technical hacking is an attack that modulates various electrical input and output signals to the internal elements of a vehicle. It also intercepts and modulates various communication signals between external networks, such as automobiles and internet connections. Operational hacking is an attack that introduces malicious signals into the communication between the interior and exterior of the car. The authors identified four classes of vulnerability: short-range wireless, long-range wireless, direct physical, and indirect physical.

Al-Kahtani (2012) published a survey paper for VANET security attack. This paper described security attacks and defenses against VANETs. The author used the defense mechanisms of VANETs to present various security and privacy infringement attacks and classified these mechanisms. The existing security and privacy schemes for VANETs were classified into public key, symmetric and hybrid, certificate revocation, and identity-based encryption.

**Table 6 – Research on V2X communication attacks.**

| Attack category | Authors | Year | Approach and experiment |
|---|---|---|---|
| VANET attacks | Larson & Nilsson (2008) | 2008 | Analyzing automotive wireless communication security problem |
| | Brooks et al. (2009) | 2009 | Automotive Security taxonomy by CERT |
| | Checkoway et al. (2011) | 2011 | Analyzing automotive wireless communication security problem |
| | Al-Kahtani (2012) | 2012 | Survey on vehicular ad hoc network's security issues |
| | Parul and Deepak (2014) | 2014 | Different types of fifty security attacks in VANET |
| | Miller & Valasek (2015) | 2015 | Culmination of three years of research into automotive security |
| | Bariah et al. (2015) | 2015 | Surveying the state-of-the-art of VANET security |
| | Hasrouny et al. (2017) | 2017 | A survey on VANET security challenges and countermeasures |
| Infotainment and Bluetooth attacks | Foster et al. (2015) | 2015 | Security analysis of a telematics control unit (TCU) |
| | Cheah et al. (2016) | 2016 | Bluetooth-enabled automotive infotainment unit |
| | Cheah et al. (2017) | 2017 | Two case studies for Bluetooth connection and diagnostics device. |
| | Bacchus et al. (2017) | 2017 | Security analysis for wireless and Bluetooth |
| | Cai et al. (2019) | 2019 | Attack using external I/O (USB, OBD-II, and cellular network) |

Parul and Deepak (2014) examined the various security threats of VANETs and analyzed their impacts and implementations on the VANET security architecture. They compared various types of VANET security attacks with attacker types. Several examples and theoretical structures have been used to mitigate the instability of VANETs. Their study also described major security vulnerabilities in VANETs and their countermeasures.

Miller & Valasek (2015) demonstrated remote attacks that can be carried out against any Fiat-Chrysler vehicle. Remote attacks have been shown to affect certain physical systems, such as steering and braking. The D-Bus service was exposed and vulnerable. The authors were able to reprogram a V850 chip to send arbitrary CAN messages from an open multimedia applications platform chip. The D-Bus was also accessible over the cellular network, not just over Wi-Fi. The D-Bus system can be accessed anonymously and is used for communication among processes. The D-Bus was exposed through the network, which was exploited by an attacker to cause security threats, including code injection and memory corruption. Bariah et al. (2015) provided a comprehensive and systematic overview of the latest research on security threats, vulnerabilities, and security services related to VANETs. They focused on important aspects, such as VANET security simulation tools, that are not well documented in the general literature.

In 2017, Hasrouny et al. (2017) comprehensively identified security problems, causes, and existing solutions related to VANETs. In addition, they described the security standards and protocols related to the latest security architecture. The authors focused on classifying and resolving various known attacks. They explained that VANET can effectively implement a system that can secure a vehicle and protect it from malicious nodes.

#### 3.3.2. *Infotainment system and bluetooth attacks*

As the functions of autonomous vehicles have developed, infotainment technology has also become important, and research has been done on infotainment system attacks. Foster et al. (2015) reviewed the telematics control unit (TCU) connected to an automotive vehicle through the standard on-board diagnostic port (OBD-II in the United States, EOBD in Europe, and JOBD in Japan). They demonstrated that this device can be remotely discovered and attacked. They described the local and remote attack surfaces of the telematics control unit. For the local attack surface, web, telnet console access, NAND dump, and SSH service methods were explained. The attackers discovered that they were bound to all the network interfaces as well as short-message-service-based functions from remotely accessible web, telnet consoles, and attack junctions, such as SSH servers.

Cheah et al. (2016) introduced a method for enhancing the security of composite systems without requiring the user to have complete knowledge of commercially sensitive subcomponents. They applied this method to Bluetooth-enabled vehicle infotainment devices and identified legitimate Bluetooth functions that lead to system instability. They discovered weaknesses in structured security testing and demonstrated how security requirements can be inferred. They also demonstrated a case study that illustrated that a file system can be mounted via Bluetooth.

Cheah et al. (2017) proposed a framework for conducting a systematic security test on a Bluetooth interface and conducted a vehicle test through the implementation of a proof-of-concept tool. They identified Bluetooth vulnerability in the vehicle, based on which vehicle manufacturers emphasized the need to consider how legacy pairing in Bluetooth technology can be replaced. They were able to test for vulnerable discovery and security practices in accordance with the structured procedures presented. The tools developed in their study emphasized that manufacturers could evaluate the status of the implementation of their security practices. Bacchus et al. (2017) discussed various systems in cars, types of known attacks, and methods to defend against such attacks. They built in-vehicle networks that use Bluetooth technology to connect both the automotive CAN bus system and the media system reliably with one system.

Cai et al. (2019) demonstrated a remote attack using multiple vulnerabilities that exist in the NBT head Unit (in-vehicle infotainment) and telematic communication box to BMW cars. They prepared a fake mobile network with an HTTP payload and short message service. The authors performed reverse-engineering on the firmware of infotainment and telematic box. They obtained root privileges with the execution of bash commands.

### 3.4. *Risk assessment and threat modeling*

A study of attacks was also conducted from a systematic point of view on autonomous vehicles. From a systematic perspective, there are threat modeling, risk assessment, and attack-tree perspectives. Research papers related to these subjects are listed in Table 7.

#### 3.4.1. *Risk assessment*

In recent years, a lot of attack studies have been conducted from the perspective of risk assessment for autonomous vehicles. Henniger et al. (2009) described the security requirement analysis process in automotive on-board network architecture. The analysis process included identifying threats, identifying security requirements, evaluating the risks, and prioritizing security requirements based on the acceptable risk. The authors identified the potential attack scenarios and probabilities by applying the analysis process. In 2013, Ward et al. (2013) developed a process similar to functional safety risk analysis for the analysis of cybersecurity threats. The authors explained how the guidelines were developed based on the approach described in ISO 26,262 and the motor industry software reliability association safety analysis guidelines. There were significant differences in understanding the severity of security attacks and the factors that lead to the likelihood of successful attacks. The authors investigated potential directions such as whether threat analysis and risk assessment can provide warranty support for cybersecurity.

Othmane et al. (2014) conducted case studies to determine the likelihood of seven threats closely related to autonomous vehicles. Experts rated six of the seven threats as “very unlikely” and one as “almost impossible.” The case study showed that the attacks were difficult because they were required to be carried out quickly and by a profoundly knowledgeable expert. However, cyber-attacks on autonomous vehicles are in-

**Table 7 – Research on risk assessments and threat modeling.**

| Attack category | Authors | Year | Approach and experiment |
|---|---|---|---|
| Risk | Henniger et al. (2009) | 2009 | Evaluating the risks associated with the threat |
| Assessment | Ward et al. (2013) | 2013 | Threat analysis and risk assessment in automotive |
| | Othmane et al. (2014) | 2014 | Likelihoods of threats to connected vehicles (OBD-II, CAN) |
| | Petit & Shladover (2015) | 2015 | Threats on autonomous automated vehicles |
| | Bayer et al. (2015) | 2015 | Automotive security evaluation assurance levels (ASEAL) |
| | Macher et al. (2016) | 2016 | Risk assessment techniques for automotive |
| | Islam et al. (2016) | 2016 | Demonstrate viability use-case and risk assessment framework |
| | Alcaraz et al. (2017) | 2017 | Threat scenarios related Open Charge Point Protocol (OCPP) |
| | Rubio et al. (2018) | 2018 | Man-in-the-Middle attacks between the CP and the CS |
| | Cheah et al. (2018) | 2018 | Method of security testing for automotive Bluetooth. |
| | Zhang et al. (2018) | 2018 | Proposed evaluation method of cybersecurity testing (108 items) |
| | Morris et al. (2018) | 2018 | Threats of the car and countermeasure strategies |
| | Bolovinou et al. (2019) | 2019 | cybersecurity framework known as threat analysis and risk assessment |
| | Xiong & Lagerström (2019) | 2019 | Meta attack language compiler for privacy |
| | Zoppelt & Kolagari (2019) | 2019 | Cloud-based attack modeling for autonomous vehicles |
| Attack tree and methodology | Salfer et al. (2014) | 2014 | On-board networks attack forest construction |
| | Thing & Wu (2016) | 2016 | A taxonomy on attacks and defenses for autonomous vehicle |
| | Lim et al. (2016) | 2016 | Infrastructure, ECU |
| | Dürrwang et al. (2018) | 2018 | Attack tree STRIDE model for airbag control unit |
| | Karray et al. (2018) | 2018 | Attack tree construction |
| | Strandberg et al. (2018) | 2018 | Systematic approach using the start, predict, mitigate, and test method |
| | Sheehan et al. (2018) | 2018 | classification framework for possible cyber-attacks |
| | Maple et al. (2019) | 2019 | Attack area analysis using a reference architecture |
| Review | Miller & Valasek (2014) | 2014 | A survey on automotive attack surfaces (20 cars) |
| | Liu et al. (2017) | 2017 | In-vehicle network attacks and countermeasures |
| | Parkinson et al. (2017) | 2017 | Reviews vulnerabilities revealed from white hat hackers |
| | Pekaric et al. (2019) | 2019 | Selected 39 papers focus on the lifecycle |
| | Miller (2019) | 2019 | Lessons Learned from hacking a car |

deed feasible, and it has been demonstrated that it is possible to attack these vehicles even using cheap equipment and scripts.

Petit & Shladover (2015) investigated vulnerability to autonomous driving and studied cyber-attacks. They identified and analyzed threats to autonomous vehicles. The most important task in developing a vehicle automation system is to identify potential security vulnerabilities before they are required. This study identified challenges by considering both autonomous and smart vehicles that communicate alert to a human driver. They used these together with current vehicle-related threats and alternatives to mitigate them. Bayer et al. (2015) introduced dangerous vulnerabilities and possible threats from the perspective of vehicle security and categorized the attacks. They analyzed the elements embedded in security evaluations based on the following three subcategories: (i) security analysis, (ii) practical security testing, and (iii) verifiable security validation. They insisted on the important of documenting a security analysis procedure prior to performing the actual analysis. This documented security analysis includes a vehicle design analysis, potential threat derivation, and corresponding risk analysis. The next step, a practical security test, includes the four categories of functional testing of vehicle modules, exploitation of actual vulnerabilities, fuzzing, and penetration testing with various inputs. Verifiable security validation used was based on the NIST FIPS-140 and common criteria. The authors introduced more details regarding the practical security testing model. They defined a security test level for each of the four categories and named it "automotive security assurance level" or "ASEAL."

Macher et al. (2016) presented ways of classifying cybersecurity threats by reviewing various risk-assessment techniques that apply to the automotive sector. This approach can provide countermeasures against threats and risks. The authors also provided an integrated approach to safety and security that can be introduced during initial product development. Islam et al. (2016) developed a framework to systematically solve security risks through threat analysis and risk assessment for embedded systems in automobiles. This framework can also be used by non-security experts. ISO 26,262 allows automotive engineers to adequately meet security requirements through a detailed description of the "safety level" of a car. This framework uses systematic guidelines and existing standards to conduct systematic assessments of security risks.

Alcaraz et al. (2017); Rubio et al. (2018) studied the communication protocol between the energy management system and the charging point in an electric vehicle. The authors identified security elements based on the Open Charge Point Protocol (OCPP) scenario, especially among the protocols. In addition, the security risk of man-in-the-middle attacks between Charge Point and Central Server in OCPP was also described.

Cheah et al. (2018) used a systematic security assessment to enumerate all undesirable behaviors to which severity ratings could be assigned in a semi-automated manner. They demonstrated vehicle vulnerability exposure, comparison methods, and severity classification. They presented a

methodology with basic concepts and demonstrated the use of native Bluetooth connectivity and aftermarket diagnostics in automotive head units. Zhang et al. (2018) presented evaluation methods for testing the cyber security of cars. First, a threat analysis for vehicle security was performed and 108 security test items were determined. Then, a methodology to build and test evaluation systems based on product testing, automobile advancement levels, and company emergency responses, was designed. The authors shared the level of vulnerability and described an example of a vehicle security assessment. Morris et al. (2018) described the cyber security threat and identified strategies that can be applied by the automotive industry to respond to it.

Bolovinou et al. (2019) presented a cybersecurity framework known as threat analysis and risk assessment (TARA) for the cybersecurity analysis model of level 3 automated driving systems. Through the TARA framework, the authors quantified the likelihood and impact of attacks. Four factors were selected to quantify the likelihood of an attack's expertise, knowledge of the target, required equipment, and window of opportunity. This study differed from previous studies in that it attempted to quantify the attack potential and impact based on the methodology called TARA +. Xiong & Lagerström (2019) examined privacy issues in vehicle security. They focused on the fact that the various existing threat models did not address privacy issues in vehicle data. To evaluate threat modeling related to privacy, they proposed the meta attack language compiler. It features threat modeling and data analysis for vehicle data in terms of privacy. Zoppelt & Kolagari (2019) reviewed cloud-based attack modeling for autonomous vehicles using the security abstraction model for automotive software. The authors also explain how the security abstraction model and the security scoring system (e.g., common vulnerability scoring system) can be used together. They demonstrated the application of the new security abstraction model version for cloud attacks through an actual case study that investigated attack modeling for the combination of a car and a cloud.

#### 3.4.2. *Attack tree and methodology*

Salfer et al. (2014) formulated an attacker and system model to analyze on-board automotive network security efficiently. They proposed a search algorithm that can create a reasonable attack path and an efficient attack tree. It is possible to create attack trees for large system models on thousands of nodes in just a few minutes. These become easy to implement as the required input values become more detailed.

Thing & Wu (2016) proposed a holistic attack and defense classification scheme to identify how autonomous vehicles can be effectively attacked and defended. The authors created an autonomous vehicle attack taxonomy with the categories of attacker, attack vector, target, motive, and potential consequences. Autonomous vehicle defenses were classified into preventive defense, passive defense, active defense, and collaborative defense.

Lim et al. (2016) analyzed security threats to autonomous vehicles and infrastructure. The authors proposed the development and analysis of countermeasures that focus on possible attack scenarios and their impacts on vehicles. They analyzed the research and development status of security technologies to cyber secure autonomous vehicles and infrastructure as well as research and development strategies. In addition, they identified the deployment status of attacks against domestic and foreign countermeasures. They also presented technological developments as well as research and development strategies to secure operations and cybersecurity for autonomous vehicle infrastructure.

Dürrwang et al. (2018) presented verification methods through penetration testing. The proposed verification methodology was intended to improve automotive security testing. They systematically explained how test cases can be derived before security validation. They demonstrated the feasibility of applying a security verification methodology to an ECU. The airbag control device was used in the experiment as an essential element for vehicle safety. The vulnerabilities considered in the experiment caused the explosion of the airbag artificially through ECU manipulation. Karray et al. (2018) studied cyber-physical attacks, focusing on car structure and state changes. The attacks were used to assess the overall risk posed to the vehicle system, thereby creating an attack tree. An attacker would need to disable the ECU-related privileges for exception handling and various other options at the user input level. They showed that an attacker would be able to display, modify, and even destroy the desired message under certain conditions.

Strandberg et al. (2018) introduced a systematic approach for testing vehicular security using the start, predict, mitigate, and test (SPMT) method. They provided pseudo-code to demonstrate SPMT, suggesting possible scenarios after the vehicles were released, and integrated them into the V-model process. To illustrate the SPMT phases, they enumerated potential attacks in the start phase. They applied the spoofing, tampering, repudiation, information disclosure, DoS, and escalation of privileges method in the prediction phase, and tested unveiled vulnerabilities and threats in the mitigating phase. In the possible scenario of released vehicles, the authors demonstrated how SPMT works with the V-model software process and concluded their work.

Some studies have applied deep-learning technology to attacks on autonomous vehicles. Sheehan et al. (2018) introduced a classification framework for possible cyber-attacks on connected and autonomous vehicles. They classified cyber-risk and illustrated testing phases using their model and the US National Vulnerability Database. They used a Bayesian network classification model and achieved a high accuracy with 9794 cases of cyber risks.

Maple et al. (2019) performed attack area analysis using a reference architecture for connected autonomous vehicles. Attack surface analysis was performed on elements such as devices, edges, and cloud systems, which interact with the connected autonomous vehicles. Based on this, a reference architecture was proposed from the perspective of hybrid communication. The authors also used attack trees in two case studies to investigate attacks on autonomous vehicles.

#### 3.4.3. *Review and survey papers regarding car hacking*

Miller & Valasek (2014) surveyed remote attack surfaces on various vehicles. They checked the location of the ECUs that handle external inputs as well as those that can physically

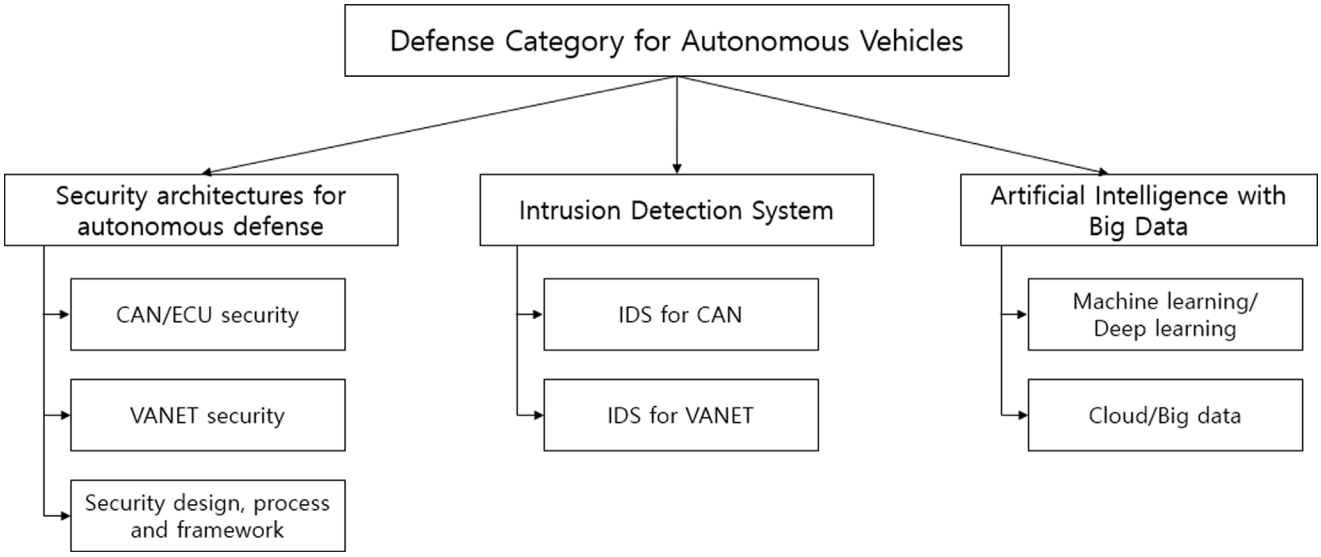



**Fig. 6 – Categories of defense on autonomous vehicles.**

change the vehicle. They examined the internal network architecture of each vehicle. They identified physically controllable features. The nature of these attacks necessitates an in-depth defense strategy, including the detection of message injection, as the attack proceeds through multiple steps.

Liu et al. (2017) reviewed various research findings to describe the vulnerabilities of in-vehicle networks and summarized the method by which they can be attacked. They presented countermeasures against such attacks and pointed out future issues and directions. They investigated the environment, interface, attack methodology, and contribution of related papers (Hoppe and Dittman, 2007; Hoppe et al., 2008; Koscher et al., 2010; Checkoway et al., 2011; Woo et al., 2015). Parkinson et al. (2017) reviewed previous studies, particularly those on vulnerabilities revealed by white hat hackers, and mitigation techniques for connected and autonomous vehicles.

Pekaric et al. (2019) conducted security tests on various software-based vehicle IT components. They selected 39 papers on systematic mapping, investigating security test techniques, AUTOSAR hierarchy investigations, AUTOSAR functional interfaces, vehicle lifecycles, and attacks. They focused on the lifecycle of the application and service layers of the AUTOSAR architecture. Miller (2019) demonstrated in 2015 that it was possible to attack a Jeep Cherokee remotely. After three years, they declared that the code signing required for software verification on ECUs is crucial. As an example, it has been claimed that the Tesla Model S could only be attacked because it does not verify unsafe code. Therefore, if the code is properly verified during software verification, carrying out the attack would be difficult. Another example is that no matter how perfect the security solution of a car is, it is not safe from being hacked. Vehicle security requires that one must not rely only on attack prevention but design a system that can detect possible attacks and undertake appropriate measures against them. Thus, Miller suggested that vehicles must be protected through thorough verification, focusing on the security mechanisms already known rather than those based on new ideas.

## 4. Defense of autonomous vehicles

With regard to the security of autonomous driving vehicles, we divided the literature on defense into the following categories: (i) security architecture, (ii) intrusion detection system, and (iii) artificial intelligence with big data, as depicted in Fig. 6.

### 4.1. *Security architectures for autonomous defense*

Initially, research was conducted in terms of the security of each element of autonomous vehicles. Various security aspects of CAN and ECU have been studied, and gradually, research on malware and VANETs has also been conducted. Research papers related to this area are listed in Table 8.

#### 4.1.1. *CAN/ECU security*

Many studies on the security architecture for CAN and ECU have been presented. In 2008, Oguma et al. (2008) presented a security architecture for secure communication within a vehicle. Remote authentication systems using trusted platform module to prevent ECU tampering cannot be applied to time-constrained vehicle systems; thus, it cannot be realized in real-world vehicle systems. The authors presented a new proof-based security architecture for in-vehicle communications that meet the flexibility requirements of software configuration authentication, encryption communications, and switching. Nilsson et al. (2008) proposed a method of effectively delaying data using complex message authentication code. The authentication factor is delayed because the message with the authentication code is calculated as a composite element of consecutive messages and is transmitted along with the next message. The method considered real-time traffic in the vehicle network, the CAN frame structure, and the limited resources of the ECU. The message authentication code (MAC) computes the message to provide guarantees of integrity and reliability. In addition, delayed data authenti-

**Table 8 – Defense research related to security architectures for autonomous defense.**

| Defense category | Authors | Year | Approach and experiment |
|---|---|---|---|
| CAN/ECU security | Oguma et al. (2008) | 2008 | Attestation-based security architecture |
| | Nilsson et al. (2008) | 2008 | Method to delay data by using complex message authentication code |
| | Groll & Ruland (2009) | 2009 | Trusted Communication Groups |
| | Schulze et al. (2009) | 2009 | Data Management System (DMS) |
| | Herrewege et al. (2011) | 2011 | CAN authentication protocol |
| | Lin & Sangiovanni-Vincentelli (2012) | 2012 | Security mechanism (message-based counter, pair-wise secret key) |
| | Hazem, 2012 | 2012 | Lightweight message source authentication protocol for CAN |
| | Groza & Murvay (2013) | 2013 | Secure broadcast protocol for CAN |
| | Wang & Sawhney (2014) | 2014 | VeCure, a security framework identifying injected CAN message |
| | Yadav et al. (2016) | 2016 | Two-way authentication method for legitimate ECUs |
| | Groza et al. (2017) | 2017 | Lightweight broadcast authentication |
| | Kornaros et al. (2019) | 2019 | TrustNet based CAN communication protection |
| | Andel et al. (2019) | 2019 | Proposal of countermeasures against attacks through priority |
| | Agrawal et al., 2019 | 2019 | Communication security architecture between ECUs on different channels |
| | Woo et al. (2019) | 2019 | CAN ID shuffling method using a network address shuttle (NAS) |
| VANET security | Dardanelli et al. (2013) | 2013 | A security session layer for Bluetooth communication |
| | Engoulou et al. (2014) | 2014 | VANET security surveys |
| | Islam et al. (2018) | 2018 | A group-key agreement protocol for vehicular networks |
| | Lu et al. (2018) | 2018 | Survey on trust management models in VANET |
| | Talib et al., 2018 | 2018 | Literature review on Internet-of-Vehicles communication (90 references) |
| | Shrestha & Nam (2019) | 2019 | Design of regional blockchains used in VANETs |
| Security design, process and framework | Bécsi et al. (2015) | 2015 | Demonstrating the significance of careful system security design |
| | Yağdereli et al. (2015) | 2015 | Suggesting automatic defensive measure |
| | Khurram et al. (2016) | 2016 | Scalable security architecture |
| | Zheng et al. (2016) | 2016 | Framework for cross-layer modeling on connected vehicles |
| | Berlin et al. (2016) | 2016 | Security management system with use cases |
| | Reger (2016) | 2016 | V2X Communications, NFC, Ultra-Wideband ranging |
| | Mawonde et al. (2018) | 2018 | Survey on vehicle security systems (14 references) |
| | El-Rewini et al. (2019) | 2019 | Hierarchical framework for security threats targeting vehicles |
| | Nasser & Ma (2019) | 2019 | HSM-based attack detection method in AUTOSAR |

cation is introduced to prevent the interruption of real-time traffic.

Groll & Ruland (2009) explained that the lack of reliability and confidentiality in CAN is the most crucial for the security risks of in-vehicle communications. They insisted that an effective solution must be provided using a reliable communication group to enable confidential communication among the vehicle's components. They also emphasized that manufacturers must prove that they belong to a closed communication group by holding a signed certificate. Schulze et al. (2009) considered the need for data management for the dozens of ECUs that compose an autonomous system. They proposed three types of data-management systems based on design aspects as well as example scenarios: (i) a central driver monitoring systems (DMS) relies on a single ECU, having pros (e.g., simple, easier management, and updates) and cons, including the bottleneck problem; (ii) a distributed DMS works with multiple ECUs, having the opposite pros and cons; (iii) a novel hybrid DMS consisting of a single DMS on each sub-network of a vehicle. Although they did not discuss how a DMS might be implemented, the consideration is relevant because many intrusion detection methods require in-vehicle status at sensors, actuators, and ECUs.

Herrewege et al. (2011) proposed CANAuth, an authentication protocol for broadcast communication, particularly applicable to the CAN bus. A benefit of this concept is that modification of the existing nodes is not required to maintain compatibility. The limited size of payload in a CAN message makes it difficult to implement defense mechanism, including authentication. To bypass this problem, the authors used the CAN+ protocol, which extends to the available bits. Thereafter, they adopted a hash-based MAC (HMAC), demonstrating the adversarial model, potential attacks, and transmission overheads. This proposed methodology allows ECUs to defend against several injection attacks.

Lin & Sangiovanni-Vincentelli (2012) also proposed a message authentication mechanism for CAN, which requires a pre-shared pairwise key, ID table, and message-based counter. They presented experimental results of the application of the methodology. In the experiment, the attacker model performed replay and modification attacks. The result was based on message latency and bus load, indicating affordable overheads. Hazem (2012) proposed a lightweight message source authentication protocol for CAN. The protocols have detailed phases by state against the attackers, including initialization, channel setup, data exchange, synchronization, and refreshing chain. Even though the protocol was not tested on commercial vehicles, it was implemented within a microcontroller. The authors also mentioned that single-pair Ethernet and FlexRay technologies can adapt their protocol.

Groza & Murvay (2013) provided a secure broadcast protocol for CAN, which does not require a pre-shared, public,

or private keys. In the protocol, the key is updated on every broadcast (i.e., transmission of a single message in the CAN bus). The authors optimized some parameters on their embedded test-bed to maximize the efficiency of communication. Wang & Sawhney (2014) proposed VeCure, a security framework identifying injected CAN messages by calculating the latency of the message from sender to the receiver. They implemented a proof of the concept on an embedded system, reporting a process delay of 50 $\mu$s. Experiments have shown that they can effectively respond to injection and replay attack. Yadav et al. (2016) summarized entry points that can be used for attacks, including physical access, and wireless system such as Bluetooth and TPMS. The authors also focused on threats to the OBD-II and CAN buses. The key idea is that only legitimate ECUs can be connected to the diagnostic system. They applied a two-way authentication method described in a step-by-step manner.

Groza et al. (2017) introduced LiBrA-CAN, a secure protocol for broadcast authentication using symmetric primitives. The protocol was implemented on CANoe and the result, including computational costs, bus load, and execution time, were described in their study. The authors also addressed the concern of feasibility degradation owing to the small payload size of a CAN message. One suggestion is to use the CAN+ protocol for additional data. However, a limitation is that the protocol is not suitable for the pre-built CAN bus, which is used in almost all vehicles.

Kornaros et al. (2019) proposed a technique that allows the use of both virtual and unreliable channels over the same CAN network. Referring to it as TrustNet, they proposed a means to protect the communications of the CAN bus with minimal overhead and full legacy system support. That is, they proposed an integrated approach to ECU authentication and network security that can easily be deployed in legacy infrastructure. Andel et al. (2019) used the inherent features of CAN arbitration, error detection and signaling, and fault confinement mechanisms. They invalidated packets coming into the attack through access control and message priority thresholds at the CAN data-link layer. Thus, they proposed a means to mitigate the impact on the normal node from attacks that attempt to manipulate messages at priority levels. Agrawal et al. (2019) proposed a communication security architecture among ECUs on different channels through one of the units acting as a gateway. He proposed a secure communication scheme for a CAN with flexible data rate. Additionally, he claimed that AEGIS, the proposed encryption scheme, provides better performance than applying individual primitives for encryption and authentication. His-experiments have also demonstrated that this schema is superior to AES counter with a cipher block chaining message authentication code.

Woo et al. (2019) proposed the CAN ID shuffling method using a network address shuttle as a moving target defense method in the CAN network environment of a vehicle. A practical security solution is to make it difficult for attackers to easily find information, such as the CAN ID, data frame saving cycle, and data field formats. It has also been claimed that this method is practical because it can be implemented without changing the protocol format or the specific fields in the existing CAN standard.

#### 4.1.2. *VANET security*

Dardanelli et al. (2013) proposed a security session layer applicable to Bluetooth communication to protect the connection between a smartphone and a vehicle. Owing to the evolution of the infotainment system, most vehicles support Bluetooth services and allow access to the in-vehicle network. After the smartphone and vehicle share their symmetric session key through the elliptic-curve Diffie-Hellman scheme, they communicate through encrypted messages with a randomly generated key. The experiment demonstrated the feasibility of the proposed method. Engoulou et al. (2014) focused on security in VANETs, presenting security issues, requirements, and challenges as well as the categorization of these issues. The authors proposed a security architecture for VANETs from a global point of view. Islam et al. (2018) proposed a password-based conditional privacy-preserving authentication and group-key generation. A group-key agreement protocol for vehicular networks preserves privacy while exchanging traffic data using a hash function. Their study includes security analysis, the number of potential attacks on vehicles, and analyses of computation and communication costs. The discussion shows that their protocol resists attacks, such as impersonation, modification, and offline password-guessing attacks, on the VANET.

Lu et al. (2018) presented a survey on trust management models in VANETs and summarized VANET simulators that can be used to research VANETs. The authors enumerated properties of trust management that should be considered: decentralization, real-time constraint, information sparsity, scalability, privacy, and robustness. Talib et al. (2018) surveyed the literature on communication security for the Internet-of-Vehicle, published between 2010 and 2018. They described various attacks on the Internet of Vehicles, countermeasures for those, and the results of such countermeasures. The authors summarized future legal and technical considerations for developing the Internet of Vehicles platform.

Shrestha & Nam (2019) examined the design of regional blockchains used in VANETs and illustrated how regional blockchains are safe against "51% percent attack." They determined that, to reduce the attack success rate below 51%, the number of benign and malicious nodes, message-delivery time, puzzle calculation time, and certain conditions need to be considered. They experimented with various simulations to determine these conditions. They found that being able to deliver benign nodes in the shortest time plays a significant role in improving the stability of the local blockchain. If the message delivery time between benign nodes is sufficiently short, it is unsafe for malicious nodes to attack. The authors also proposed a method for decreasing the message delays between the superior nodes of a VANET.

#### 4.1.3. *Security design, process, and framework*

Bécsi et al. (2015) described the impact of connectivity on vehicles. They demonstrated the significance of careful system security design, with linked functions modifying the vehicle structure and presenting the vulnerability of each element. The application security of information and communications technology has emphasized the already well-understood security principles.

Yadereli et al. (2015) suggested that a variety of autonomous vehicle systems can become vulnerable owing to software and hardware defects as well as defects in the development process. Due to these risks, the authors emphasized that vehicles must have automatic defensive measures in place. They also investigated the security vulnerabilities of autonomous vehicle systems and identified the threats and attacks that exploit them. Further, they discussed the development guidelines and mitigation methods available for autonomous vehicle systems.

Khurram et al. (2016) presented a security framework for connected car security architecture - multiple modules in various layers that comprised the OTA update system. Zheng et al. (2016) developed CONVINCE, which is a framework for cross-layer modeling on connected vehicles. CONVINCE encompasses intra-vehicle and inter-vehicle communication. CACC was used to evaluate the effectiveness of the framework in a case study. The authors carried out flooding attacks on an NS3-based vehicle network simulator to measure the packet-loss rate and evaluate the performance of their work. Berlin et al. (2016) introduced a security management system. This system uses the use-case concept. The use-cases included a special event of an attack and stolen credentials.

Reger (2016) addressed the concepts of Ethernet, V2X communications, car RADAR, NFC, ultra-Wideband (UWB) ranging, and security. At the highest levels of privacy and system security, reliable wireless and wired communication technologies combined with powerful data-processing capabilities are critical. The author discussed what it takes to realize securely connected cars of the future. He asserted that, as opposed to an afterthought, security must become an integral part of the design process. This calls for security-by-design and privacy-by-design approaches.

Mawonde et al. (2018) presented an analysis of numerous studies and approaches that exist in the literature. They performed an in-depth comparative analysis of the type of technology implemented and the strengths and weaknesses of the proposed systems. Based on their findings, the authors concluded that there are some strong contenders to the augmentation of current vehicle security. They reviewed 14 existing papers to create a summary of the proposed vehicle security technologies.

El-Rewini et al. (2019) proposed a hierarchical framework for security threats targeting vehicles. The proposed framework consists of three layers: sensing, communication, and control. The sensing or detection layer consists of environmental sensors vulnerable to eavesdropping, jamming, and spoofing attacks. The communication layer consists of in-vehicle communication and V2X communication and is primarily exposed to eavesdropping, spoofing, man-in-the-middle, civil attacks, etc. The control layer includes autonomous driving functions, including vehicle speed, braking, and steering automation. They used this framework to investigate attacks and threats related to the communication layer and suggested countermeasures.

Nasser & Ma (2019) determined that AUTOSAR-based safety systems are vulnerable to code reuse attacks and studied countermeasures against these. They proposed a method to protect the shared RAM buffer between a hardware security module and the host from a vulnerability that could be manipulated. The experiment used the vehicle's diagnostic protocol to implement routine control services related to vehicle safety. They mentioned that the hardware-security-module-based monitoring systems can protected against malicious attacks.

### 4.2. *Intrusion detection system*

There have been many attempts to incorporate the most representative and basic network security solutions, firewall and intrusion detection systems, into the autonomous vehicle. Research papers related to this area are listed in Table 9.

#### 4.2.1. *Intrusion detection system for CAN*

Hoppe et al. (2009) proposed the adoption of intrusion detection in the automotive domain. The special requirements for achieving this were analyzed considering the technical challenges. They also developed a prototypical automotive IDS component.

Müter et al. (2010) discussed a structured approach based on sensor intelligence. The authors provided certain applicability criteria for sensors as well as the parameter values. Furthermore, they suggested the integration of sensor result to build the concept of IDS in the vehicular domain. Kleberger et al. (2011) conducted research on the in-vehicle network and security of connected cars. They stated existing problems with in-vehicle network and architectural security features. They also introduced IDS and honeypots to defense attacks.

Müter & Asaj (2011) suggested an information-theoretic intrusion detection method for the CAN bus. Their idea was to calculate the entropy of CAN messages on the binary, signal, and protocol levels. The authors measured the entropy based on three measures: i) conditional self-information, ii) entropy, and iii) relative entropy. As the calculation is based on each CAN ID, a specific ECU can be identified as being attacked. A test vehicle was used to measure the value while driving.

Ling & Feng (2012) proposed a malicious detection algorithm applicable to a CAN bus. The proposed algorithm detects attacks using the frequencies calculated by the CAN IDs of the messages. A list of CAN IDs used in the bus is obtained in advance. An attack can be detected early by watching out for the appearance of a CAN ID that has not been used before. The algorithm was implemented in the CANoe simulator using a CAN access programming language. Studnia et al. (2013) introduced a brief overview of possible attacks that are already known and experimented against vehicles and certain protection mechanisms. The key idea was to deploy a gateway and use it as an IDS. However, applying a gateway to the CAN bus can cause problems due to unintended performance degradation.

Song et al. (2016) proposed a lightweight algorithm to detect an injection attack on an in-vehicle network based on the time intervals of CAN messages. In the implementation, the authors measured and calculated the period of a message by the CAN ID with normal status. The results were used as thresholds to identify intrusions. The limitation of this study is that the detection algorithm must have prior knowledge about the intervals of receiving "*Arbitration_ID*" values for each

**Table 9 – Defense research related to intrusion detection systems.**

| Defense category | Authors | Year | Approach and experiment |
|---|---|---|---|
| IDS for CAN | Hoppe et al. (2009) | 2009 | Anomaly-based IDS for the CAN protocol |
| | Müter et al. (2010) | 2010 | Eight attack detection sensors |
| | Kleberger et al. (2011) | 2011 | Surveys for network, architectural, IDS, honeypots, threats, and attacks. |
| | Müter & Asaj (2011) | 2011 | Information theoretic intrusion detection method for CAN bus |
| | Ling & Feng (2012) | 2012 | Consecutively broadcast ID threshold count |
| | Studnia et al. (2013) | 2013 | Experimented against vehicles and some protection mechanism |
| | Song et al. (2016) | 2016 | Time intervals of CAN messages for in-vehicle network |
| | Boudguiga et al. (2016) | 2016 | ECU Intrusion Detection (ECU DoS, replay and impersonation attacks). |
| | Gmiden et al. (2016) | 2016 | Time intervals between matching CAN IDs |
| | Cho & Shin (2016) | 2016 | Anomaly-based intrusion detection system-Clock based IDS (CIDS) |
| | Rizvi et al. (2017) | 2017 | State-fully hybrid adaption of distributed firewall system |
| | Lee et al. (2017) | 2017 | Offset ratio and time-interval-based IDS (OTIDS) |
| | Marchetti & Stabili (2017) | 2017 | Detection algorithm measuring sequence of CAN ID |
| | Choi et al. (2018) | 2018 | Using low-level communication characteristics. Detect bus-off attack |
| | Studnia et al. (2018) | 2018 | A language-based intrusion detection approach |
| | Kneib & Huth (2018) | 2018 | Signal-characteristic-based sender identification |
| | Lokman et al. (2019) | 2019 | Survey and review of IDS in CAN bus system environment |
| | Longari et al. (2019) | 2019 | CopyCAN intrusion detection |
| | Zhou et al. (2019) | 2019 | Bit-time-based CAN bus monitor (BTMonitor) |
| | Luo & Hou (2019) | 2019 | Software-based firewall |
| | Olufowobi et al. (2019) | 2019 | Proposal of IDS of ECU reboot mechanism using message cycle |
| IDS for VANET | Maglaras (2015) | 2015 | Architectural concept of DIDS designed for VANET |
| | Straub et al. (2017) | 2017 | Four layers (vehicle-level, network, traffic management, and coordination) |
| | Li et al. (2017) | 2017 | Regression learning approach |
| | Sharma & Kaul (2018) | 2018 | Surveyed and classified IDS in VANET |
| | Hamad et al. (2019) | 2019 | Proposal of red-zone-based intrusion response system |

vehicle. They published the dataset used in this study on their website.

Boudguiga et al. (2016) proposed an intrusion detection method for a CAN bus. The main idea was that the microcontrollers monitor the CAN messages traveling in the bus to detect malicious frames. To do this, the method requires a hardware security module embedded in each ECU. The authors performed an experiment with their CAN attacker model, performing DoS, impersonation, and isolation attacks. Each ECU identifies whether a message is normal, based on the MAC, and classifies illegal messages as intrusions. Gmiden et al. (2016) proposed a simple IDS based on the time intervals between CAN messages. The advantages of this method are that it does not require any modification of the existing hardware or CAN buses, and it can identify attacks through only a single monitor.

Cho & Shin (2016) proposed an ECU-fingerprinting methodology based on analyzing the message arrival time. The authors overcome the limitation that the transmission source was unknown, as CAN messages do not contain such information. The authors' idea was to measure the travel time required for a message until it is received by the ECU. They extended the study to build an IDS that identifies the exact attacked nodes. Three attack scenarios were evaluated on a testbed and two commercial sedans. One limitation of their study was that the IDS cannot locate the attackers who send messages only periodically.

Rizvi et al. (2017) studied threats to in-vehicular networks by introducing existing vulnerabilities and attacks on autonomous cars. They argued that DoS and replay attacks are harmful and should be addressed by understanding the existing vulnerabilities and threats to the in-vehicle network. To this end, they suggested a hybrid security system and a distributed firewall that deployed a filter for each sensor and communication module such as GPS, Bluetooth, and Wi-Fi. Lee et al. (2017) suggested OTIDS, which is an IDS based on the offset ratio and time interval using the requests and responses of remote frames. Under normal driving conditions, the interval and offset between the request and response are fixed, but when a message injection attack occurs, it varies. The experiment was conducted on a commercial vehicle, and the dataset used in the study was released on the author's website. Marchetti & Stabili (2017) suggested a detection algorithm to measure the sequence of CAN IDs. In the method, the sequence potentially follows the CAN ID or IDs, which are referred to by the detection model upon transmission of each CAN message.

In 2018, Choi et al. (2018) proposed VoltageIDS, which detects intrusions on the side-channel of CAN messages. VoltageIDS was the first IDS developed for vehicles that can distinguish between errors and bus-off attacks. The IDS capture an electrical CAN signal to identify an ECU. An advantage of this proposal is that it does not require any modification of the system. The authors presented a prototype of the CAN bus and the results of an experiment on a real vehicle while driving. Studnia et al. (2018) presented a network IDS, using language theory to build attack signatures and detect malicious messages sequences. The authors detailed the methodology and experiments conducted using collected CAN traffic.

Kneib & Huth (2018) proposed Scission, an IDS fingerprinting ECU that captures the voltage of the CAN bus. The advantage of monitoring the side-channel is that the attacker's position can be determined beyond the limits of the CAN protocol. The experiment was conducted on two commercial vehicles. A comparison of three similar studies, including the authors', was provided. The result was that Scission achieved 99.85% accuracy and a 0% false positive rate. The authors mentioned that the method can distinguish between added ECUs and unknown ECUs.

In 2019, Lokman et al. (2019) conducted a survey and review of the IDSes in a CAN bus system environment. Their goal was to conduct literature research on proposed IDS detection methods, deployment strategies, and attack techniques. Based on the IDS detection methods described in detail, these were categorized as frequency-based, machine-learning-based, statistical, and hybrid-based methods.

Longari et al. (2019) proposed CopyCAN intrusion detection, which monitors the CAN network to determine whether the node is disconnected from the current network based on the error counter of the ECU. This approach is advantageous when an attacker spoofs a message. It can also detect how to isolate the normal ECUs and attack the malicious node. CopyCAN can detect spoofed messages, even if the information streams do not match. In the existing network environment, IDS-implemented ECUs can be installed to monitor and comply with existing CAN standards. Zhou et al. (2019) proposed a new intrusion detection system called BTMonitor (bit time-based CAN bus monitor) to address the weaknesses caused by the lack of message authentication in the CAN protocol. The system indicated that experiments in vehicles have an average of 99.76% chance of correctly identifying the sender, which can help detect intrusions and find attackers. The detection method used the measurable discrepancies of bit times in the CAN frame to indicate the fingerprint of the ECU in the outgoing packet. The authors proposed a method for detecting intrusions and detecting attackers using the fingerprints generated by each sender.

Luo & Hou (2019) proposed a firewall and a security mechanism based on a hardware platform to protect against vehicle-borne cyber security threats. The authors proposed a packet filter mechanism, which was categorized according to protocol security requirements. CAN with a flexible data rate was implemented as a packet filter mechanism. The authors also designed and proposed DoS defense and access control mechanisms. They proposed a network firewall mechanism that can be applied based on each attack vector. The firewall was based on a microcontroller unit using the hardware security module to implement the encryption function. The authors also suggested a possible network firewall implemented in the central gateway.

Olufowobi et al. (2019) proposed an algorithm that detects and repairs messages spoofed by an attacker using the vehicle's CAN network. The proposed recovery process works by remotely rebooting the damaged ECU. Therefore, an IDS was proposed to switch off the abnormal node to the bus so that only normal communication is possible. The criteria were applied by setting a threshold of approximately 6 ms rather than the normal message frame period.

#### 4.2.2. *Intrusion detection system for VANET*

Maglaras (2015) presented an architectural concept of a distributed IDS designed for VANETs. The modules of the proposed distributed IDS were installed in a RSU and in a vehicle. The authors mainly focused on performance issues that can occur during implementation rather than on attack-detection methods.

Straub et al. (2017) presented a collaborative intrusion detection system that works on VANETs. The proposed system is composed of four parts: (i) the vehicle-level IDS works on each vehicle, detecting attacks without the cooperation of the external system; (ii) the vehicle area network IDS works with VANET with several vehicles that share their status with each other; (iii) a system on the RSU takes responsibility for the secure communication of the local VANET, and (iv) the central system processes all data from the VANETs and identifies anomalies.

Li et al. (2017) presented an IDS based on sensor data, applied to the regression-learning approach, estimating parameters with correlated and redundant data. The authors used the following sensor data from the vehicle: engine speed, acceleration, brake pedal position, yaw rate, angle of steering wheel, and gear position. Experiments were conducted using actual vehicles and demonstrated that an accuracy of 90% or more was obtained when the vehicle speed was used.

In Sharma & Kaul (2018), the authors surveyed IDSes in VANETs. The authors conducted research on the papers that proposed each IDS based on the following criteria: placement strategy, detection method, security threat, validation strategy, and highlighting features. In addition, the IDSes were classified as follow: (i) reaction type: active IDS, passive IDS, and real-time detection IDS; (ii) detection methodology: signature-based, anomaly-based, cross-layer-based, hybrid IDS, and watchdog-based; (iii) validation strategy: simulation, empirical, hypothetical, and theoretical; and (iv) deployment location: centralized RSU-based IDS, distributed individual-node IDS, cluster head-based IDS, and hybrid IDS.

Hamad et al. (2019) proposed a situational evaluation mechanism to determine the optimal response in a vehicle using intrusion response systems (IRSes), which are used not only in the vehicle sector but also in other areas. They investigated the requirements for applying the IRS mechanism to vehicles. They also proposed an IRS based on the red-zone principle according to the identified requirements. The IRS uses the red-zone time to implement the response strategy. It is designed to evaluate and respond to a predefined security policy through a framework already established through the IRS during the red-zone period. The authors had already verified the security policy strategy and countermeasures predefined in the previous study before proposing the IRS-based IDS framework.

### 4.3. *Artificial intelligence using big data*

With the development of artificial intelligence and the activation of big data, research on autonomous vehicle security combining artificial intelligence and big data technology has become an important trend in recent years. Research papers related to this area are listed in Table 10.

**Table 10 – Defense research related to artificial intelligence using big data.**

| Defense category | Authors | Year | Approach and experiment |
|---|---|---|---|
| ML and DL | Taylor et al. (2015) | 2015 | Flow-based anomaly detector for CAN bus |
| | Han et al. (2015) | 2015 | Detection method by using a statistical method |
| | Marchetti et al. (2016) | 2016 | LSTM to determine anomaly detection in CAN bus data |
| | Kang & Kang (2016) | 2016 | Deep learning structure with deep belief network |
| | Narayanan et al. (2016) | 2016 | Using hidden Markov model with OBD SecureAlert |
| | Taylor et al. (2016) | 2016 | Measured entropy of CAN messages using information-theoretic method |
| | Moore et al. (2017) | 2017 | Data-driven anomaly detection algorithm |
| | Tomlinson et al. (2018b) | 2018 | CAN IDS survey (43 references) |
| | Han et al. (2018) | 2018 | Anomaly detection based on survival analysis |
| | Tomlinson et al. (2018a) | 2018 | Measured packet timing of CAN messages within time window |
| | Al-Khateeb et al. (2018) | 2018 | Recursive Bayesian estimation |
| | Seo et al. (2018) | 2018 | GAN based IDS |
| | Ahmad et al., 2019 | 2019 | Machine learning techniques to detect relay attacks |
| | Song et al. (2019) | 2019 | Deep convolutional neural network (DCNN) based IDS |
| | Tang et al. (2019) | 2019 | Classified machine learning as communications, networking, and security |
| Cloud and Big data | Zhang et al. (2014) | 2014 | Cloud-assisted vehicle malware defense framework |
| | Eiza & Ni (2017) | 2017 | Latest vehicle cyber security threats and defending mechanisms (17 references) |
| | Gupta & Sandhu (2018) | 2018 | Authorization framework for secure cloud assisted |

#### 4.3.1. *Machine learning and deep learning*

Research has been conducted to introduce artificial intelligence concepts into autonomous vehicle security since mid-2010.

Taylor et al. (2015) presented a flow-based anomaly detector for the CAN bus. The motivation was that most normal packets arrive at a fixed frequency. The proposed method compares the historical packet timing over a sliding window. The authors tested their method with data captured from two CAN buses on a 2011 Ford Explorer and evaluated the performance on a one-class support vector machine. Han et al. (2015) proposed a detection method using one-way analysis of variance. They used several sensor data values captured via an OBD-II scanner. A homogeneity test was performed on parking, driving with constant speed, and driving in downtown situations. The authors suggested that the method should be targeted at IoT devices that are connected while driving, and an external device should be able to identify the anomalies.

Marchetti et al. (2016) measured the entropy of CAN messages using the information-theoretic method. The simple idea was that an attack is detected when the entropy drops below a certain threshold value. The entropy value is calculated for each time window. In the experiment, an attack model was injected at regular intervals.

Kang & Kang (2016) proposed a DNN-based IDS working on a CAN bus. The goal of their research was to detect malicious packets injected into the CAN bus. Due to the time consumption of the training phase, the authors assumed that the training phase occurs outside the vehicle. However, they mentioned that the model provides results immediately in the detection phase. The experiment was performed on a simulator using a packet generator, open car testbed, and network experiments. Narayanan et al. (2016) proposed OBD-SecureAlert to determine abnormal activities that occur during driving. The system architecture is divided into three sections. In the data collection phase, CAN messages are collected via the OBD-II port that exists in almost all United States vehicles. In the model generation phase, the system builds a hidden Markov model that expresses time-series data. Using the model, anomalous behavior is detected in the anomaly-detection phase. In their experiment, the authors used RPM and velocity data to test their model.

Deep-learning and machine-learning techniques have been studied in autonomous security. Taylor et al. (2016) used long short-term memory (LSTM) to detect anomalies in CAN bus data. The LSTM predicts the next payload of CAN messages based on prior messages. The model identified abnormal messages that were injected, modified, or even dropped. The authors claimed that the method shows low false-alarm rates.

Moore et al. (2017) proposed an anomaly detection algorithm based on time interval, taking less than 5 s to train the model. The authors described that 1) the normal message and signal have a regular frequency, and 2) an attacker injects repetitive messages to trigger an effective attack on the vehicle. The authors determined the intrusion using simple threshold.

Tomlinson et al. (2018b) studied anomaly detection methods and technologies for CAN. They also considered the implications of these in terms of practicability and requirements. The authors categorized anomaly detection methods as follows: i) signature-based, ii) statistical-based, iii) knowledge-based, and iv) modeling algorithms, including clustering, support vector machines, neural networks, and the hidden Markov model.

Han et al. (2018) used the survival analysis model to detect intrusion in vehicular networks. The goal of their study was to identify malicious CAN messages accurately without knowledge of traffic information. They tested their detection model on three different types of vehicles. The experiment was performed with flood, fuzzy, and malfunctioning attacks. The result included accuracy and f-measure on each vehicle and attack, and the detection speed depends on the number of CAN IDs used with a car.

Tomlinson et al. (2018a) measured the packet timing of CAN messages within a time window and offered various experimental results with changed thresholds. Two measurements, Z-score and auto-regressive integrated moving average, are normally used to determine the likelihood of an attack. The authors demonstrated that the proposed method could identify dropped or injected packets. The features used in the performance evaluation were recall, specificity, and accuracy, and the results varied depending on the window size.

Al-Khateeb et al. (2018) used Bayesian estimation techniques for the insider-threat prediction model. They assumed a hijacking attacker who can not only acquire communication between the vehicle and command and the control system, but also perform a man-in-the-middle attack. To detect the attack, they used the following features: vehicle speed, geolocation information including elevation, orientation, timestamp, and IPv6 address. They insisted that the Bayesian model can predict a vehicle's next possible state, which is used to identify an attacker's intervention.

Seo et al. (2018) built a CAN message classifier using a generative-adversarial-network-based IDS (GIDS). The significance of GIDS is that it can detect intrusion using a model built from normal data. GIDS generates fake messages for training purposes instead of attacks, which allows the model to detect attacks that have never been seen before. The experiment was performed using four types of attacks: DoS, fuzzy, RPM modification, and gear position modification. The performance was measured with 100% accuracy on the first discriminator and 98% accuracy on the second discriminator.

Ahmad et al., 2019 studied the introduction of machine-learning techniques to detect relay attacks against PKES systems. For the experiment, the decision tree, support vector machine, and k-nearest neighbors methods were compared using a three-month log of the PKES system. Song et al. (2019) proposed an IDS based on a deep convolutional neural network to protect the CAN bus. They compared machine-learning algorithms (LSTM, artificial neural network, support vector machine, k-nearest neighbors, naive Bayes, and decision tress) for DoS, gear spoofing, RPM spoofing, and fuzzy attack. The authors experimented on the proposed model with four categories of message injection attacks. Tang et al. (2019) presented a survey paper related to the secure vehicular network-applied machine-learning approach. The authors classified machine-learning techniques in a vehicular network as communication, networking, and security perspective. They also highlighted the future of vehicle network that include 6 G and artificial intelligence techniques.

#### 4.3.2. *Cloud and big data*

Zhang et al. (2014) focused on defending malware targeted at vehicles. They introduced potential inflow ports, including the OBD-II port, OTA update system, on-board web browser, multimedia port (e.g., USB port), and third-party equipment. As several infotainment systems are operated using the Linux OS, malware can harm the in-vehicle system. The authors proposed some frameworks to protect the in-vehicle system from malware, such as cloud-assisted detection framework and on-board inspection procedure.

Eiza & Ni (2017) illustrated cybersecurity threats on vehicles, including malware and vulnerabilities in OBD and automobile applications. New cyber threats come along with new technologies, including autonomous driving technology and V2X communication. The authors introduced an automotive network architecture, corresponding cyber threat vectors, and certain defensive mechanisms against these. To challenge attacks via communication channels, the authors suggested three solutions: i) secure OTA update solution delivering the code with cryptographic verification, ii) a cloud-based solution, and iii) a layer-based solution.

Gupta & Sandhu (2018) studied an authorization framework, an extended access control oriented architecture for VANET and vehicular clouds. The proposed architecture focuses mainly on the object and virtual object layers. The authors introduced a method to deal with sensitive information in the cloud environment and provided a real use-case. The research topics proposed in the study are: external interactions, in-vehicle interactions, cross-cloud interaction, and cloud data.

## 5. Summary and conclusion

There has been a clear flow in the attacks against vehicles and their defenses over time. Regarding attacks, research on CAN and ECU was actively conducted before 2017. Recently, the design of risk and possible attack scenarios for vehicles has been studied (e.g., attack tree, STRIDE, and evaluation method). Research on automobile attacks has been conducted on a variety of attack surfaces, beginning with the studies by (Hoppe et al., 2008) and (Nilsson et al., 2008) up to the recent study conducted by (Maple et al., 2019). The first car attack was primarily an attack on the interior of the car involving the ECU and CAN. In recent years, autonomous driving technology has advanced, and attacks on external communications, such as on V2X, have been studied extensively.

As attack techniques for autonomous vehicles continues to emerge, defensive methods are also being studied. Defense has been steadily researched in areas such as security of CAN networks, security of authentication protocols, and intrusion detection. We know that the networks and protocols currently in use in vehicles are insecure, but we are restrained by the fact that it is difficult to respond quickly to attacks. Therefore, methods of detecting attacks have been steadily researched, and in recent years, artificial intelligence techniques with big-data analysis are being considered to improve the specifications of ECUs. Security research on autonomous vehicles has led to the method of specification-based detection as proposed by (Hoppe et al., 2008) and has been continuously studied since then. This has led to the proposal of machine-learning techniques in (Ahmad et al., 2019). Autonomous vehicle security models have been studied, from IDS, which is a traditional security model, to security models combining artificial intelligence, machine learning, and deep learning technologies, such as a Bayesian network and a deep-belief networks.

With the present technology, the future of automobiles will be combined with fully autonomous vehicle functions. The major automobile brands Volkswagen, BMW, Mercedes-Benz, Nissan, Hyundai, and Toyota are developing autonomous driv-

ing technologies, as are IT companies such as Google, Apple, and Samsung.

In this situation, cyber-attacks on autonomous vehicles will be further intensified, and the aftermath will have a grave impact on the safety of human life and that of the city. The research contents of Alcaraz & Lopez (2012) who studied security requirements in Critical Infrastructure are also helpful in constructing the security elements of future autonomous vehicles. The world we live in will evolve into one made of smart cities, and autonomous vehicles will be at the center of smart mobility. With the aim of making the world we live in more secure; we hope this survey paper will be helpful to all researchers working on attacks and defenses associated with autonomous vehicles.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

The study was funded by Institute for Information and communications Technology Promotion (Grant No. 2020-0-00374, Development of Security Primitives for Unmanned Vehicles). Also, this study was supported by a Korea University Grant.

## REFERENCES

Al-Kahtani Mohammed Saeed. In: 2012 6th International Conference on Signal Processing and Communication Systems. Survey on security attacks in Vehicular Ad hoc Networks (VANETs) *Pages 1–9 of*. IEEE; 2012.

al-Khateeb Haider, Epiphaniou Gregory, Reviczky Adam, Karadimas Petros, Heidari Hadi. Proactive threat detection for connected cars using recursive bayesian estimation. IEEE Sens J 2018;18(12):4822–31.

Agrawal Megha, Huang Tianxiang, Zhou Jianying, Chang Donghoon. CAN-FD-Sec: Improving Security of CAN-FD Protocol, 11552 Page 77 of. Springer; 2019. Revised Selected Papers.

Ahmad Usman, Song Hong, Bilal Awais, Alazab Mamoun, Jolfaei Alireza. Securing smart vehicles from relay attacks using machine learning. J Supercomput 2019:1–18.

Alcaraz Cristina, Lopez Javier. Analysis of requirements for critical control systems. International journal of critical infrastructure protection 2012;5(3–4):137–45.

Alcaraz Cristina, Lopez Javier, Wolthusen Stephen. OCPP protocol: security threats and challenges. IEEE Trans Smart Grid 2017;8(5):2452–9.

Amoozadeh Mani, Raghuramu Arun, Chuah Chen-Nee, Ghosal Dipak, Zhang H Michael, Rowe Jeff, Levitt Karl. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine 2015;53(6):126–32.

Andel Todd R, McDonald J Todd, Brown Adam J, Trigg Tyler H, Cartsten Paul W. In: 2019 IEEE International Conference on Consumer Electronics (ICCE). Towards Protection Mechanisms for Secure and Efficient CAN Operation Pages 1–6 of. IEEE; 2019.

Bacchus, Mark, Coronado, Alexander, Gutierrez, Maria A. 2017. The insights into car hacking.

Bariah Lina, Shehada Dina, Salahat Ehab, Yeun Chan Yeob. In: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall). Recent Advances in VANET Security: A Survey Pages 1–7 of. IEEE; 2015.

Bayer Stephanie, Enderle Thomas, Oka Dennis-Kengo, Wolf Marko. Security crash test-practical security evaluations of automotive onboard it components. Automotive-Safety & Security 2015;2014.

Bécsi Tamás, Aradi Szilárd, Gáspár Péter. In: Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2015 International Conference on. Security issues and vulnerabilities in connected car systems *Pages 477–482 of*. IEEE; 2015.

Berlin Olga, Held Albert, Matousek Matthias, Kargl Frank. In: 2016 IEEE Vehicular Networking Conference (VNC). Poster: anomaly-based misbehaviour detection in connected car backends *Pages 1–2 of*. IEEE; 2016.

Bolovinou Anastasia, Atmaca Ugur-Ilker, Sheik Al Tariq, Ur-Rehman Obaid, Wallraf Gerhard, Amditis Angelos, et al. In: IEEE Intelligent Vehicles Symposium (IV). TARA+: controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems Pages 8–13 of: 2019. IEEE; 2019.

Boudguiga Aymen, Klaudel Witold, Boulanger Antoine, Chiron Pascal. In: IEEE International Conference on Communications (ICC). A simple intrusion detection method for controller area network Pages 1–7 of: 2016. IEEE; 2016.

Brooks Richard R, Sander Sam, Deng Juan, Taiber Joachim. Automobile security concerns. IEEE Vehicular Technology Magazine 2009;4(2):52–64.

Burakova Yelizaveta, Hass Bill, Millar Leif, Weimerskirch André. In: In: 10th USENIX Workshop on Offensive Technologies (WOOT 16). Truck Hacking: an Experimental Analysis of the SAE J1939 Standard. ACM; 2016.

Cai Zhiqiang, Wang Aohui, Zhang Wenkai, Gruffke M, Schweppe H. 0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars. Black Hat USA 2019;2019:39.

Cheah Madeline, Shaikh Siraj A, Bryans Jeremy, Nguyen Hoang Nga. Combining Third Party Components Securely in Automotive Systems. Pages 262–269 of: IFIP International Conference on Information Security Theory and Practice. Springer, 2016.

Cheah Madeline, Shaikh Siraj A, Haas Olivier, Ruddle Alastair. Towards a systematic security evaluation of the automotive Bluetooth interface. Vehicular Communications 2017;9:8–18.

Cheah Madeline, Shaikh Siraj A, Bryans Jeremy, Wooderson Paul. Building an automotive security assurance case using systematic security evaluations. Computers & Security 2018;77:360–79.

Checkoway Stephen, McCoy Damon, Kantor Brian, Anderson Danny, Shacham Hovav, Savage Stefan, Koscher Karl, Czeskis Alexei, Roesner Franziska, Kohno Tadayoshi, et al. In: USENIX Security Symposium. Comprehensive Experimental Analyses of Automotive Attack Surfaces San Francisco; 2011.

Cho Kyong-Tak, Shin Kang G. In: 25th USENIX Security Symposium (USENIX Security 16). Fingerprinting Electronic Control Units for Vehicle Intrusion Detection Pages 911–927 of. USENIX; 2016.

Choi Wonsuk, Joo Kyungho, Jo Hyo Jin, Park Moon Chan, Lee Dong Hoon. VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System. IEEE Transactions on Information Forensics and Security 2018;13(8):2114–29.

Dardanelli Andrea, Maggi Federico, Tanelli Mara, Zanero Stefano, Savaresi Sergio M, Kochanek R, Holz T. A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth. IEEE Embed Syst Lett 2013;5(3):34–7.

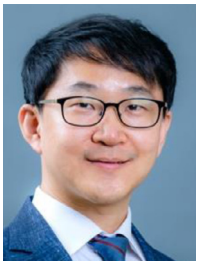
Dürrwang Jürgen, Braun Johannes, Rumez Marcel, Kriesten Reiner, Pretschner Alexander. Enhancement of Automotive Penetration Testing with Threat Analyses Results. SAE International Journal of Transportation Cybersecurity and Privacy 2018;1(11–01–02–0005):91–112.
Eiza Mahmoud Hashem, Ni Qiang. Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. IEEE Vehicular Technology Magazine 2017;12(2):45–51.
El-Rewini Zeinab, Sadatsharan Karthikeyan, Selvaraj Daisy Flora, Plathottam Siby Jose, Ranganathan Prakash. Cybersecurity challenges in vehicular communications. Vehicular Communications 2019.
Engoulou Richard Gilles, Bellaïche Martine, Pierre Samuel, Quintero Alejandro. VANET security surveys. Comput Commun 2014;44:1–13.
Eriksson Benjamin, Groth Jonas, Sabelfeld Andrei. On the road with third-party apps: security analysis of an in-vehicle app platform. Proc. 5th Int. Conf. Vehicle Technology and Intelligent Transport Systems (VEHITS), 2019.
Foster Ian, Prudhomme Andrew, Koscher Karl, Savage Stefan. In: WOOT. Fast and Vulnerable: a Story of Telematic Failures. USENIX; 2015.
Fowler Daniel S, Cheah Madeline, Shaikh Siraj Ahmed, Bryans Jeremy. In: 2017 IEEE International Conference on Software Testing, Verification and Validation (ICST). Towards a Testbed for Automotive Cybersecurity Pages 540–541 *of*. IEEE; 2017.
Fowler Daniel S, Bryans Jeremy, Cheah Madeline, Wooderson Paul, Shaikh Siraj A. In: Pages 1–8 of: 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C). A Method for Constructing Automotive Cybersecurity Tests, a CAN Fuzz Testing Example. IEEE; 2019.
Francillon Aurélien, Danev Boris, Capkun Srdjan. Relay attacks on passive keyless entry and start systems in modern cars. Proceedings of the Network and Distributed System Security Symposium (NDSS). Department of Computer Science, 2011.
Fröschle Sibylle, Stühring Alexander. In: Pages 464–482 of: European Symposium on Research in Computer Security. Analyzing the capabilities of the CAN attacker. Springer; 2017.
Garcia Flavio D, Oswald David, Kasper Timo, Pavlidès Pierre. In: USENIX Security Symposium. Lock It and Still Lose It-on the (In) Security of Automotive Remote Keyless Entry Systems; 2016.
Gmiden Mabrouka, Gmiden Mohamed Hedi, Trabelsi Hafedh. In: 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA). An intrusion detection method for securing in-vehicle CAN bus Pages 176–180 of: 2016. IEEE; 2016.
Groll Andre, Ruland Christoph. In: 2009 IEEE Intelligent Vehicles Symposium. Secure and authentic communication on existing in-vehicle networks Pages 1093–1097 of. IEEE; 2009.
Groza Bogdan, Murvay Stefan. Efficient protocols for secure broadcast in controller area networks. IEEE Transactions on Industrial Informatics 2013;9(4):2034–42.
Groza Bogdan, Murvay Stefan, Herrewege Anthony Van, Verbauwhede Ingrid. LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks. ACM Transactions on Embedded Computing Systems (TECS) 2017;16(3):90.
Gupta Maanak, Sandhu Ravi. Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things. *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*. SACMAT '18. ACM, 2018.
Halahan Jennifer, Chen Weifeng. Wireless Security Within New Model Vehicles. Journal of Information Warfare 2017;16(3):51–62.
Hamad Mohammad, Tsantekidis Marinos, Prevelakis Vassilis. In: the 5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS). Red-Zone: towards an Intrusion Response Framework for Intra-Vehicle System; 2019.
Han Mee Lan, Lee Jin, Kang Ah Reum, Kang Sungwook, Park Jung Kyu, Kim Huy Kang. In: International Conference on Internet of Vehicles. A statistical-based anomaly detection method for connected cars in internet of things environment *Pages 89–97 of*. Springer; 2015.
Han Mee Lan, Kwak Byung Il, Kim Huy Kang. Anomaly intrusion detection method for vehicular networks based on survival analysis. Vehicular communications 2018;14:52–63.
Hasrouny Hamssa, Samhat Abed Ellatif, Bassil Carole, Laouiti Anis. VANet security challenges and solutions: a survey. Vehicular Communications 2017;7:7–20.
Hazem Ahmed, Fahmy HA. LCAP - A Lightweight CAN Authentication Protocol for Securing In-Vehicle Networks. 10th escar Embedded Security in Cars Conference. Escar, 2012.
Henniger Olaf, Apvrille Ludovic, Fuchs Andreas, Roudier Yves, Ruddle Alastair, Weyl Benjamin. In: 9th International Conference on Intelligent Transport Systems Telecommunications,(ITST). Security requirements for automotive on-board networks Pages 641–646 of: 2009. IEEE; 2009.
Herrewege Anthony Van, Singelée Dave, Verbauwhede Ingrid. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus, 2011. ECRYPT; 2011.
Hoppe Tobias, Dittman Jana. Sniffing/Replay Attacks on CAN Buses: a simulated attack on the electric window lift classified using an adapted CERT taxonomy. Proceedings of the 2nd workshop on embedded systems security (WESS), 2007.
Hoppe Tobias, Kiltz Stefan, Dittmann Jana. In: International Conference on Computer Safety, Reliability, and Security. Security threats to automotive CAN networks–practical examples and selected short-term countermeasures *Pages 235–248 of*. Springer; 2008.
Hoppe Tobias, Kiltz Stefan, Dittmann Jana. Applying intrusion detection to automotive IT-early insights and remaining challenges. Journal of Information Assurance and Security (JIAS) 2009;4(6):226–35.
Roufa Ishtiaq, Millerb Rob, Mustafaa Hossen, Taylora Travis, Ohb Sangho, Xua Wenyuan, Gruteserb Marco, Trappeb Wade, Seskarb Ivan. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. *Pages 11–13 of*. 19th USENIX Security Symposium 2010.
Islam Mafijul Md, Lautenbach Aljoscha, Sandberg Christian, Olovsson Tomas. A risk assessment framework for automotive embedded systems. Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security. ACM, 2016.
Islam SK Hafizul, Obaidat Mohammad S, Vijayakumar Pandi, Abdulhay Enas, Li Fagen, Reddy M Krishna Chaitanya. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Generation Computer Systems 2018;84:216–27.
ISO. 2015 (November). *ISO 11898-1:2015, Road vehicles – Controller area network (CAN)*. online, accessed 4/11/19. https://www.iso.org/standard/63648.html.
Jafarnejad Sasan, Codeca Lara, Bronzi Walter, Frank Raphael, Engel Thomas. In: Globecom Workshops (GC Wkshps), 2015 IEEE. A car hacking experiment: when connectivity meets vulnerability *Pages 1–6 of*. IEEE; 2015.
Kang Min-Joo, Kang Je-Won. Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE 2016;11(6).
Karray Khaled, Danger Jean-Luc, Guilley Sylvain, Elaabid M Abdelaziz. In: Cyber-Physical Systems Security. Attack Tree Construction and Its Application to the Connected Vehicle Pages 175–190 of. Springer; 2018.
Keen Security Lab of Tencent. 2017 (July). *New Car Hacking Research: 2017, Remote Attack Tesla Motors Again*. online,

accessed 7/27/17. https://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-Remote-Attack-Tesla-Motors-Again/.
Khatoun Rida, Zeadally Sherali. Smart cities: concepts, architectures, research opportunities. Commun ACM 2016;59(8):46–57.
Khurram Muzaffar, Kumar Hemanth, Chandak Adi, Sarwade Varun, Arora Nitu, Quach Tony. In: 2016 International Conference on Connected Vehicles and Expo (ICCVE). Enhancing connected car adoption: security framework *Pages 27–28 of*. IEEE; 2016.
Kim Seung-Han, Seo Suk-Hyun, Kim Jin-Ho, Moon Tae-Moon, Son Chang-Wan, Hwang Sung-Ho, Jeon Jae Wook. In: Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on. A gateway system for an automotive system: LIN, CAN, and FlexRay Pages 967–972 of. IEEE; 2008.
Kleberger Pierre, Olovsson Tomas, Jonsson Erland. In: 2011 IEEE Intelligent Vehicles Symposium (IV). Security aspects of the in-vehicle network in the connected car. IEEE; 2011.
Kneib Marcel, Huth Christopher. Scission: signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018.
Kong Linghe, Khan Muhammad Khurram, Wu Fan, Chen Guihai, Zeng Peng. Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: overview, design, and challenges. IEEE Communications Magazine 2017;55(1):62–8.
Kornaros George, Bakoyiannis Dimitris, Tomoutzoglou Othon, Coppola Marcello, Gherardi Giovanni. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). TrustNet: ensuring Normal-world and Trusted-world CAN-bus Networking *Pages 1–6 of*. IEEE; 2019.
Koscher Karl, Czeskis Alexei, Roesner Franziska, Patel Shwetak, Kohno Tadayoshi, Checkoway Stephen, McCoy Damon, Kantor Brian, Anderson Danny, Shacham Hovav, et al. In: Security and Privacy (SP), 2010 IEEE Symposium on. Experimental security analysis of a modern automobile *Pages 447–462 of*. IEEE; 2010.
Kukkala Vipin Kumar, Pasricha Sudeep, Bradley Thomas. JAMS: jitter-Aware Message Scheduling for FlexRay Automotive Networks. Proceedings of the Eleventh IEEE/ACM International Symposium on Networks-on-Chip. ACM, 2017.
Larson Ulf E, Nilsson Dennis K. Securing vehicles against cyber attacks. Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead. ACM, 2008.
Larson Ulf E, Nilsson Dennis K, Jonsson Erland. In: 2008 IEEE Intelligent Vehicles Symposium. An approach to specification-based attack detection for in-vehicle networks Pages 220–225 of. IEEE; 2008.
Learning About Electronics. 2018
Lee ByungKwan, Jeong EunHee, Jeong YiNa. Message Propagation based on Three Types of Density Classification for Smooth and Secure Vehicular Traffic Flow. International Journal of Multimedia and Ubiquitous Engineering 2014;9(12):383–404.
Li Huaxin, Zhao Li, Juliato Marcio, Ahmed Shabbir, Sastry Manoj R, Yang Lily L. Poster: intrusion detection system for in-vehicle networks using sensor correlation and integration. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017.
Lee Hyunsung, Jeong Seong Hoon, Kim Huy Kang. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST). OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame Pages 57–5709 of. IEEE; 2017.
Li Xiangxue, Yu Yu, Sun Guannan, Chen Kefei. Connected Vehicles' Security from the Perspective of the In-Vehicle Network. IEEE Netw 2018;32(3):58–63.
Lim Bing Shun, Keoh Sye Loong, Thing Vrizlynn LL. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). Autonomous vehicle ultrasonic sensor vulnerability and impact assessment *Pages 231–236 of*. IEEE; 2018.
Lim Dohyun, Park Kitaek, Choi Dongjun, Seo Jungtaek. In: International Conference on Broadband and Wireless Computing, Communication and Applications. Analysis on Attack Scenarios and Countermeasures for Self-driving Car and Its Infrastructures *Pages 429–442 of*. Springer; 2016.
Lin Chung-Wei, Sangiovanni-Vincentelli Alberto. In: Cyber Security (CyberSecurity), 2012 International Conference on. Cyber-security for the Controller Area Network (CAN) communication protocol *Pages 1–7 of*. IEEE; 2012.
Ling Congli, Feng Dongqin. In: 2012 National Conference on Information Technology and Computer Science. An algorithm for detection of malicious messages on CAN buses. Atlantis Press; 2012.
Liu Jiajia, Zhang Shubin, Sun Wen, Shi Yongpeng. In-vehicle network attacks and countermeasures: challenges and future directions. IEEE Netw 2017;31(5):50–8.
Lokman Siti-Farhana, Othman Abu Talib, Abu-Bakar Muhammad-Husaini. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP J Wirel Commun Netw 2019;2019(1):184.
Longari Stefano, Penco Matteo, Carminati Michele, Zanero Stefano. CopyCAN: an Error-Handling Protocol based Intrusion Detection System for Controller Area Network. Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy, 2019.
Lu Zhaojun, Qu Gang, Liu Zhenglin. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Transactions on Intelligent Transportation Systems 2018:1–17.
Luo Feng, Hou Shuo. Tech. rept. SAE Technical Paper; 2019.
Macher Georg, Armengaud Eric, Brenner Eugen, Kreiner Christian. Threat and risk assessment methodologies in the automotive domain. Procedia Comput Sci 2016;83:1288–94.
Maglaras Leandros A. A novel distributed intrusion detection system for vehicular ad hoc networks. International Journal of Advanced Computer Science and Applications (IJACSA) 2015;6(4):101–6.
Makowitz Rainer, Temple Christopher. FlexRay-A communication network for automotive control systems. 2006 IEEE International Workshop on Factory Communication Systems. IEEE, 2006.
Malhi Avleen Kaur, Batra Shalini, Pannu Husanbir Singh. Security of vehicular ad-hoc networks: a comprehensive survey. Computers & Security 2020;89.
Maple Carsten, Bradbury Matthew, Le Anh Tuan, Ghirardello Kevin. A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. Applied Sciences 2019;9(23):5101.
Marchetti Mirco, Stabili Dario. In: 2017 IEEE Intelligent Vehicles Symposium (IV). Anomaly detection of CAN bus messages through analysis of ID sequences *Pages 1577–1583 of*. IEEE; 2017.
Marchetti Mirco, Stabili Dario, Guido Alessandro, Colajanni Michele. In: 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI). Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms *Pages 1–6 of*. IEEE; 2016.
Martinelli Fabio, Mercaldo Francesco, Nardone Vittoria, Santone Antonella. In: 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). Car hacking identification through fuzzy logic algorithms Pages 1–7 of. IEEE; 2017.

Mawonde Kudakwashe, Isong Bassey, Lugayizi Francis, Abu-Mahfouz Adnan M. In: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society. A Survey on Vehicle Security Systems: approaches and Technologies *Pages 4633–4638 of*. IEEE; 2018.
Mazloom Sahar, Rezaeirad Mohammad, Hunter Aaron, McCoy Damon. In: *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. A security analysis of an in-vehicle infotainment and app platform. USENIX; 2016.
Miller Charlie. Lessons learned from hacking a car. IEEE Design & Test 2019;36(6):7–9.
Miller Charlie, Valasek Chris. Adventures in automotive networks and control units. Def Con 2013;21:260–4.
Miller Charlie, Valasek Chris. A survey of remote automotive attack surfaces. black hat USA 2014;2014:94.
Miller Charlie, Valasek Chris. Remote exploitation of an unaltered passenger vehicle. Black Hat USA 2015;2015:91.
Moore Michael R, Bridges Robert A, Combs Frank L, Starr Michael S, Prowell Stacy J. Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection. Proceedings of the 12th Annual Conference on Cyber and Information Security Research. ACM, 2017.
Morris David, Madzudzo Garikayi, Garcia-Perez Alexeis. Cybersecurity and the auto industry: the growing challenges presented by connected cars. International journal of automotive technology and management 2018;18(2):105–18.
Müter Michael, Asaj Naim. In: 2011 IEEE Intelligent Vehicles Symposium (IV). Entropy-based anomaly detection for in-vehicle networks. IEEE; 2011.
Müter Michael, Groll André, Freiling Felix C. In: 2010 Sixth International Conference on Information Assurance and Security. A structured approach to anomaly detection for in-vehicle networks. IEEE; 2010.
Narayanan Sandeep Nair, Mittal Sudip, Joshi Anupam. In: 2016 IEEE International Conference on Smart Computing (SMARTCOMP). OBD_SecureAlert: an anomaly detection system for vehicles. IEEE; 2016.
Nasser Ahmad, Ma Di. Defending AUTOSAR Safety Critical Systems Against Code Reuse Attacks. Proceedings of the ACM Workshop on Automotive Cybersecurity. ACM, 2019.
Nie Sen, Liu Ling, Du Yuefeng. Free-Fall: hacking Tesla from Wireless to Can Bus. Briefing, Black Hat USA 2017.
Nilsson Dennis K, Larson Ulf E, Jonsson Erland. In: 2008 IEEE 68th Vehicular Technology Conference. Efficient in-vehicle delayed data authentication based on compound message authentication codes. IEEE; 2008.
Nilsson Dennis K, Larson Ulf E, Picasso Francesco, Jonsson Erland. A first simulation of attacks in the automotive network communications protocol flexray. Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISISâAZ08. Springer, 2009.
Nolte Thomas, Hansson Hans, Bello Lucia Lo. Automotive communications-past, current and future, 1 *Pages 8–pp of*. IEEE; 2005.
Oguma Hisashi, Yoshioka Akira, Nishikawa Makoto, Shigetomi Rie, Otsuka Akira, Imai Hideki. In: IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference. New attestation based security architecture for in-vehicle communication Pages 1–6 of. IEEE; 2008.
Olufowobi Habeeb, Hounsinou Sena, Bloom Gedare. Controller Area Network Intrusion Prevention System Leveraging Fault Recovery. Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy, 2019.
Othmane L Ben, Fernando Ruchith, Ranchal Rohit, Bhargava BHARAT, Bodden Eric. Likelihood of threats to connected vehicles. International Journal of Next-Generation Computing (IJNGC) 2014;5(3):1–14.
Palanca Andrea, Evenchick Eric, Maggi Federico, Zanero Stefano. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. A stealth, selective, link-layer denial-of-service attack against automotive networks *Pages 185–206 of*. Springer; 2017.
Pan Lei, Zheng Xi, Chen HX, Luan T, Bootwala Huzefa, Batten Lynn. Cyber security attacks to modern vehicular systems. Journal of information security and applications 2017;36:90–100.
Parkinson Simon, Ward Paul, Wilson Kyle, Miller Jonathan. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE transactions on intelligent transportation systems 2017;18(11):2898–915.
Tyagi Parul, Dembla Deepak. In: 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI). Investigating the security threats in vehicular ad hoc networks (VANETs): towards security engineering for safer on-road transportation. IEEE; 2014.
Payne Bryson R. Car Hacking: Accessing and Exploiting the CAN Bus Protocol. Journal of Cybersecurity Education, Research and Practice 2019;2019(1):5.
Pekaric Irdin, Sauerwein Clemens, Felderer Michael. Applying Security Testing Techniques to Automotive Engineering. Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019.
Petit Jonathan, Shladover Steven E. Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems 2015;16(2):546–56.
Reger Lars. In: 2016 IEEE International Solid-State Circuits Conference (ISSCC). 1.4 The road ahead for securely-connected cars. IEEE; 2016.
Rizvi Syed, Willet Jonathan, Perino Donte, Marasco Seth, Condo Chandler. A threat to vehicular cyber security and the urgency for correction. Procedia Comput Sci 2017;114:100–105.
Rubio Juan E, Alcaraz Cristina, Lopez Javier. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). Addressing Security in OCPP: protection Against Man-in-the-Middle Attacks Pages 1–5 of. IEEE; 2018.
Salfer Martin, Eckert Claudia. Attack surface and vulnerability assessment of automotive Electronic Control Units, 4 Pages 317–326 of. IEEE; 2015.
Salfer Martin, Schweppe Hendrik, Eckert Claudia. In: International Conference on Information Security. Efficient attack forest construction for automotive on-board networks Pages 442–453 of. Springer; 2014.
Schulze Sandro, Pukall Mario, Saake Gunter, Hoppe Tobias, Dittmann Jana. On the Need of Data Management in Automotive Systems, 144 Pages 217–226 of; 2009.
Seo Eunbi, Song Hyun Min, Kim Huy Kang. In: 2018 16th Annual Conference on Privacy, Security and Trust (PST). GIDS: GAN based Intrusion Detection System for In-Vehicle Network. IEEE; 2018.
Sharma Sparsh, Kaul Ajay. A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. Vehicular Communications 2018;12:138–64.
Sheehan Barry, Murphy Finbarr, Mullins Martin, Ryan Cian. Connected and autonomous vehicles: a cyber-risk classification framework. Transportation Research Part A: *Policy and Practice* 2018.
Shrestha Rakesh, Nam Seung Yeob. Regional blockchain for vehicular networks to prevent 51% attacks. IEEE Access 2019;7:95021–33.
Shukla Siddharth. Embedded Security for Vehicles. ECU Hacking; 2016.
Smith Craig. The Car Hacker's Handbook: A Guide For the Penetration Tester. No Starch Press; 2016.

Song Hyun Min, Kim Ha Rang, Kim Huy Kang. In: 2016 international conference on information networking (ICOIN). Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. IEEE; 2016.
Song Hyun Min, Woo Jiyoung, Kim Huy Kang. In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications 2019;21.
Strandberg Kim, Olovsson Tomas, Jonsson Erland. Securing the connected car: a security-enhancement methodology. IEEE vehicular technology magazine 2018;13(1):56–65.
Straub Jeremy, McMillan John, Yaniero Brett, Schumacher Mitchell, Almosalami Abdullah, Boatey Kelvin, Hartman Jordan. In: 2017 12th System of Systems Engineering Conference (SoSE). CyberSecurity considerations for an interconnected self-driving car system of systems. IEEE; 2017.
Studnia Ivan, Nicomette Vincent, Alata Eric, Deswarte Yves, Kaâniche Mohamed, Laarouchi Youssef. In: SAFECOMP 2013-workshop CARS (2nd workshop on critical automotive applications: robustness & safety) of the 32nd international conference on computer safety, reliability and security. Security of embedded automotive networks: state of the art and a research proposal; 2013.
Studnia Ivan, Alata Eric, Nicomette Vincent, Kaâniche Mohamed, Laarouchi Youssef. A language-based intrusion detection approach for automotive embedded networks. International Journal of Embedded Systems 2018;10(1).
Takefuji Yoshiyasu. Connected Vehicle Security Vulnerabilities [Commentary]. IEEE Technology and Society Magazine 2018;37(1):15–18.
Talib Manar Abu, Abbas Sohail, Nasir Qassim, Mowakeh Mohamad Fouzi. Systematic literature review on Internet-of-Vehicles communication security. International Journal of Distributed Sensor Networks 2018;14(12).
Tang Fengxiao, Kawamoto Yuichi, Kato Nei, Liu Jiajia. Future Intelligent and Secure Vehicular Network Toward 6G: *machine-Learning Approaches*. Proceedings of the IEEE 2019.
Taylor Adrian, Japkowicz Nathalie, Leblanc Sylvain. In: 2015 World Congress on Industrial Control Systems Security (WCICSS). Frequency-based anomaly detection for the automotive CAN bus. IEEE; 2015.
Taylor Adrian, Leblanc Sylvain, Japkowicz Nathalie. In: 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA). Anomaly detection in automobile control network data with long short-term memory networks. IEEE; 2016.
Tettamanti Tamás, Varga István, Szalay Zsolt. Impacts of autonomous cars from a traffic engineering perspective. Periodica Polytechnica. Transportation Engineering 2016;44(4):244.
The Economist. 2013 (April). *How does a self-driving car work?*online, accessed 12/05/15. https://www.economist.com/blogs/economistexplains/2013/04/economist-explains-how-self-driving-car-works-driverless.
Thing Vrizlynn LL, Wu Jiaxi. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Autonomous vehicle security: a taxonomy of attacks and defences. IEEE; 2016.
Tod Beardsley. 2017 (April). *R7-2017-02: hyundai Blue Link Potential Info Disclosure (FIXED)*. online, accessed 25/04/17. https://blog.rapid7.com/2017/04/25/r7-2017-02-hyundai-blue-link-potential-info-disclosure-fixed/.
Tomlinson Andrew, Bryans Jeremy, Shaikh Siraj Ahmed, Kalutarage Harsha Kumara. In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Detection of Automotive CAN Cyber-Attacks by Identifying Packet Timing Anomalies in Time Windows. IEEE; 2018a.
Tomlinson Andrew, Bryans Jeremy, Shaikh S. Towards Viable Intrusion Detection Methods For The Automotive Controller Area Network. Proc. 2nd Computer Science in Cars Symposium-Future Challenges in Artificial Intelligence Security for Autonomous Vehicles (CSCS 2018), 2018b.
Verdult Roel, Garcia Flavio D, Balasch Josep. Gone in 360 s: hijacking with Hitag2. *Pages 237–252 of: Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*. USENIX, 2012.
Verdult Roel, Garcia Flavio D, Ege Baris. In: USENIX Security Symposium. Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer Pages 703–718 of. USENIX; 2013.
Voss Wilfried. A Comprehensible Guide to Controller Area Network. Copperhill Media; 2008.
Wang Jiadai, Liu Jiajia, Kato Nei. Networking and Communications in Autonomous Driving: a Survey. IEEE Communications Surveys & Tutorials 2018.
Wang Qiyan, Sawhney Sanjay. In: 2014 International Conference on the Internet of Things (IOT). VeCure: a practical security framework to protect the CAN bus of vehicles Pages 13–18 of. IEEE; 2014.
Ward David, Ibarra Ireri, Ruddle Alastair. Threat analysis and risk assessment in automotive cyber security. SAE International Journal of Passenger Cars-Electronic and Electrical Systems 2013;6(2013–01–1415):507–13.
Woo Samuel, Jo Hyo Jin, Lee Dong Hoon. A practical wireless attack on the connected car and security protocol for in-vehicle CAN. IEEE Transactions on Intelligent Transportation Systems 2015;16(2):993–1006.
Woo Samuel, Moon Daesung, Youn Taek-Young, Lee Yousik, Kim Yongeun. CAN ID Shuffling Technique (CIST): Moving Target Defense Strategy for Protecting In-Vehicle CAN. IEEE Access 2019;7:15521–36.
Wyglinski Alexander M, Huang Xinming, Padir Taskin, Lai Lifeng, Eisenbarth Thomas R, Venkatasubramanian Krishna. Security of autonomous systems employing embedded computing and sensors. IEEE micro 2013;33(1):80–6.
Xiong Wenjun, Lagerström Robert. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). Threat Modeling of Connected Vehicles: a privacy analysis and extension of vehicleLang. IEEE; 2019.
Yadav Aastha, Bose Gaurav, Bhange Radhika, Kapoor Karan, Iyengar Nc, Caytiles Ronnie D. Security, vulnerability and protection of vehicular on-board diagnostics. International Journal of Security and Its Applications 2016;10(4):405–22.
Yadereli Eray, Gemci Cemal, Akta§ A Ziya. A study on cyber-security of autonomous and unmanned vehicles. The Journal of Defense Modeling and Simulation 2015;12(4):369–81.
Yan Chen, Xu Wenyuan, Liu Jianhao. Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle. In: DEF CON; 2016. p. 24.
Yan Wei. In: Connected Vehicles and Expo (ICCVE), 2015 International Conference on. A two-year survey on security challenges in automotive threat landscape. IEEE; 2015.
Yeh Enoch, Choi Junil, Prelcic Nuria G, Bhat Chandra R, Heath Robert W, et al. Tech. rept. University of Texas at Austin. Data-Supported Transportation Operations; 2018.
Zhang Yanan, Shi Peiji, Dong Changqing, Liu Yangyang, Shao Xuebin, Ma Chao. In: 2018 IEEE International Conference on Computational Science and Engineering (CSE). Test and Evaluation System for Automotive Cybersecurity *Pages 201–207 of:*. IEEE; 2018.
Zheng Bowen, Lin Chung-Wei, Yu Huafeng, Liang Hengyi, Zhu Qi. In: 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). CONVINCE: a cross-layer

modeling, exploration and validation framework for next-generation connected vehicles. IEEE; 2016.
Zhou Jia, Joshi Prachi, Zeng Haibo, Li Renfa. BTMonitor: bit-time-based Intrusion Detection and Attacker Identification in Controller Area Network. ACM Transactions on Embedded Computing Systems (TECS) 2019;18(6):1–23.
Zoppelt, Markus, & Kolagari, Ramin Tavakoli. 2019. UnCle SAM: modeling Cloud Attacks with the Automotive Security Abstraction Model.



**Kyounggon Kim** received his B.S. degree in computer science from Soongsil University in 2008, and M.S. degree and Ph.D. in School of Cybersecurity from Korea University in 2015 and 2020, respectively. He is currently an Assistant Professor at the Department of Forensics Sciences, Naif Arab University for Security and Sciences (NAUSS). He has performed penetration testing for over 130 clients in various industries when he worked for Deloitte, PwC, and boutique consulting firms during over 15 years. He was awarded 6th place at DefCon CTF in 2007 and a first prize at the First Hacking Defense Contest hosted by the Korea Information Security Agency. He has authored a book on Internet hacking and security and has translated numerous security books. His research interests include cybercrime and network forensics, vulnerability analysis, smart city security, and CPS and IoT security.

**Jun Seok Kim** received the B.S. degree in computer science from Sejong University in 2015, and M.S. degree in cybersecurity from Korea University in 2019. He joined Deloitte through 2014 to 2017 and ESCRYPT through 2019 to 2020 as cybersecurity consultant. Currently, he is a research engineer in Hyundai Motor Company. His research interests are reverse engineering, protocol fuzzing and wireless network in vehicle cybersecurity.

**Seonghoon Jeong** obtained his M.S. degree in Information Security from Korea University, Seoul, Republic of Korea, in 2017. He is currently a Ph.D. candidate studying at Korea University. His research interests are in the areas of data-driven security and network security, especially on in-vehicle networks.

**Jo-Hee Park** received a B.S. degree in Information Security from Seoul Women's University in 2014. She joined Ernst & Young and worked as a cybersecurity consultant from 2014 to 2016. Currently, she is a research engineer in Hyundai Motor Company. Her research interests include hardware hacking, reverse engineering, wireless network and in-vehicle cybersecurity.

**Huy Kang Kim** received a B.S. degree in Industrial Management, M.S. degree in Industrial Engineering and Ph.D. degree in Industrial and System Engineering in Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea. He is a serial entrepreneur; he founded A3 Security Consulting in 1999 and AI Spera, the data-driven cyber threat intelligence service company in 2017. Currently, he is a professor in the School of Cybersecurity, Korea University. His recent research is focused on anomaly detection in the intelligent transportation system, online gaming and internet banking by using data analytics and machine learning techniques.