Revisiting Attacks and Defenses in Connected and Autonomous Vehicles

Ziyan Fang[1,2(✉)], Weijun Zhang[1,2], Zongfei Li[3], Huaao Tang[3], Hao Han[1,2(✉)], and Fengyuan Xu[3]

[1] College of Computer Sciences and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
542897592@qq.com, 807301949@qq.com, hhan@nuaa.edu.cn
[2] Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing 210093, China
[3] State Key Laboratory for Novel Technology, Nanjing University, Nanjing 210046, China

Abstract. With the development of the automotive industry, the security of connected and autonomous vehicles (CAVs) has become a hot research field in recent years. However, previous studies mainly focus on the threats and defending mechanisms from the networking perspective, while newly emerging attacks are targeting the core component – AI of CAVs. Therefore, the defense methods against these attacks are urgently needed. In this paper, we revisit emerging attacks and their technical countermeasures for CAVs in a layered inventory, including in-vehicle systems, V2X, and self-driving. We believe that this survey provides insights on defending adversary attacks on CAVs and will shed light on the future research in this area.

Keywords: Connected and autonomous vehicles · V2X · In-vehicle network · Vehicle security · Autonomous vehicle algorithms

1 Introduction

The automotive industry is undergoing massive digital transformation towards connected and autonomous vehicles (CAVs). Compared with traditional cars, CAVs have great potential to achieve extended driving automation with strengthened environment awareness improved by vehicle connectivity. The Association of Automotive Engineers (SAE) definitions for levels of automation divide vehicles into 6 levels. However, only cars in L4 and L5 are considered autonomous vehicles. The L4 has fully automated driving feature in specific environments, while L5 can do all the driving in all circumstances.

Their self-driving capability is achieved through three layers: perception, cognition and execution as shown in Fig. 1. The perception layer is used to capture vehicle's internal and surrounding status via in-vehicle sensors and environmental sensors. With assistant of V2X communication, the cognition layer recognizes

G. Wang et al. (Eds.): SpaCCS 2020, LNCS 12382, pp. 104–117, 2021.
https://doi.org/10.1007/978-3-030-68851-6_7

vehicle's motion states and external threats based on the perception layer, and then determines the trajectory of the vehicle through deep learning algorithms. Finally, the execution layer controls the vehicle by issuing commands to Electronic Control Units (ECUs) and actuators through in-vehicle networks (e.g., CAN bus, FlexRay, MOST).

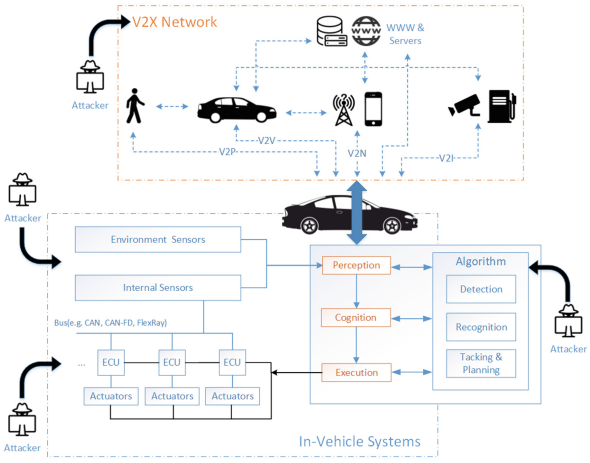

Fig. 1. The structure of connected and autonomous vehicles

Modern cars are quite insecure and vulnerable from an information system perspective. Although some security mechanisms have been adopted by automotive suppliers after a 2014 Jeep Cherokee was hacked by Miller and Valasek [26], new vulnerabilities continue to rise every year. A large number of studies show that the attack surface of CAVs is broad. A set of features in in-vehicle systems, V2X communication, autonomous algorithms might allow misuse of or a breach into CAVs, resulting in much more profound and widespread effects. Therefore, it is important of protecting future CAVs from hackers and cyberattacks.

In literature, there are many survey papers about automotive security. For example, work [3] study vulnerabilities and defenses in Controller Area Network (CAN) bus with more focus on authentication. Work [44] summarize the V2X technology and its protocol vulnerabilities, as well as corresponding defense measures. Work [43] discusses the security issues of connected vehicles from three categories, and introduces the trend of network attacks and the protection requirements that should be developed for networked services. Work [34] provides an overview of the security issues in AV but with emphasis on attacking sensors and iris recognition systems. However, those surveys are not specific to CAVs and mainly focus on the networking aspect rather than the system and algorithm perspective.

In this paper, we review potential attacks and their technical countermeasures for CAVs in a layered inventory: in-vehicle systems, V2X and autonomous

algorithms corresponding to execution, cognition and perception layers, respectively. We summarize the attack threats in each layer. Compared with the threats in traditional vehicles, attackers not only attack ECU and CAN networks, they also attack environmental sensors and autonomous vehicle algorithms in CAVs. Later in this survey, we provide insights on corresponding defense approaches to address those attack threats. In summary, the contributions of this paper include:

- To our best understanding, this survey is the first to study the attack surface and defensive mechanisms for CAVs from the perspective of the system and algorithms, while previous study mostly is network-oriented. This will shed light on the future research in this area.
- We explore new potential attacks for emerging CAVs along with existing vulnerabilities in E/E architecture, and categorize the various security approaches from 3 layers, including in-vehicle systems, V2X and autonomous driving algorithms.
- We discuss the possible directions for future research works on security and privacy issues in CAVs.

The rest of this paper is structured as follows: Sect. 2 specifically introduces the architecture of connected and autonomous vehicles. Section 3 describes the attacks that may be realized at each layer of the CAVs. Section 4 introduces the corresponding defense methods in detail for possible attacks. Section 5 describes the possible directions for future research works on security and privacy issues in CAVs, followed by the summary of the paper. Section 6 summarizes this survey.

2 Background

CAVs include not only autonomous driving but also the connection between the vehicle and the surrounding environment. In this section, we briefly present the main components of CAVs, which are typical targets of modern vehicle attacks discussed in next section.

2.1 In-Vehicle Networks

The in-vehicle network of CAVs connects sensors, Electronic Control Units (ECUs) and actuators of the car with a point-to-point connection into a complex network structure. They together are the guarantee for the normal and security vehicle driving, and are the critical components of the vehicle. The failure of any one may cause the abnormal driving of the vehicle, and even a traffic accident in a serious situation.

Sensors in CAVs can be divided into two categories: internal sensors and external sensors. The former, arranged inside a car, is used to check the function of the vehicle. For example, the oxygen sensor monitors the content of exhaust gases for the proportion of oxygen. Sensors in the latter category provide the car visuals of its surroundings and help it detect the speed and distance of nearby

objects, as well as their three-dimensional shape. Three primary external vehicle sensors are camera, radar and LiDAR.

Electronic Control Units (ECUs) are used to enable computer-based control of a vehicle. Based on the information sent by vehicle sensors, ECUs determine the running states and control the vehicle to work together. A modern car may have up to 70 ECUs - and each of them is assigned a specific function (e.g., engine control). Typically, ECUs are grouped into several subnetworks according to their functions. For example, the ECUs in charge of steering and braking are grouped together.

Bus networks, like the nervous system of the human body, interconnect ECUs and enable the information sensed by one part to be shared with other parts of the vehicle. The autopilot system in CAVs use such networks to transmit control commands. Example bus networks include Controller Area Network (CAN), CAN-FD, FlexRay, and automotive Ethernet. Among them, CAN is the standard for in-vehicle communications today in fact. The detail of CAN can be found in many good surveys such as [19].

2.2 Vehicle-to-X Communication (V2X)

V2X which stands for vehicle-to-everything technology enables cars to communicate with their surroundings and makes driving safer and more efficient. V2X covers Vehicle to vehicle (V2V), Vehicle to infrastructure (V2I), Vehicle to Network(V2N), Vehicle to Pedestrian (V2P) and others. Working together, they provide a guarantee for the security driving of vehicles. In CAVs, V2X offers an additional means to sense environment conditions other than typical sensors, e.g., retrieving traffic information and other vehicle's location for route planning.

Currently, there are two main types of communication technologies used for V2X: Dedicated Short Range Communication (DSRC) and Long Term Evolution for V2X (LTE-V2X). The DSRC system consists of a series of IEEE and SAE standards. DSRC uses IEEE 802.11p protocol which is also called Wireless Access in the Vehicular Environment (WAVE), at the physical layer and media access control (MAC) layer, while its network architecture and security protocols are defined in IEEE 1609 WAVE.

2.3 Autonomous Algorithms

Autonomous driving requires the car to be like human to recognize something that appears in surrounding environment and to forecast the changes that are possible to these surroundings. A deep neural network with various autonomous algorithms is equivalent to a human brain. Based on their tasks, those algorithms can be broadly grouped into three categories as follows:

– **The detection of an object:** Object detection based on deep learning is often used in the detection of traffic signs/lights and other vehicles in the proximity. Based on the data provided by environmental sensors attached to the vehicle, object detection algorithms can pinpoint the location of traffic

signs/lights and other vehicles. Together with other autonomous algorithms, the autopilot system will make a decision whether the car needs to slow down or stop. The state-of-the-art learning-based object detection algorithms include Faster R-CNN, etc.

– **The recognition of an object:** Object detection is typically coupled with the task of object recognition which is used to identify the class of objects, e.g., whether an object is a traffic sign, vehicle, or pedestrian. Common recognition algorithms are alexnet and senet.
– **The tracking of an object and trajectory planning:** Trajectory planning is based on path planning and obstacle avoidance planning. At present, it is mainly based on reinforcement learning and time series algorithms to achieve high standards of unmanned driving technology. In particular, reinforcement learning is widely used in automatic driving trajectory decision-making.

3 Attack Surface for CAVs

In this section, we revisit the attack surfaces of CAVs and identify three key components: in-vehicle systems, V2X communication, and autonomous algorithms. We separate them primarily into two categories: *remote* and *internal* as shown in Fig. 2.

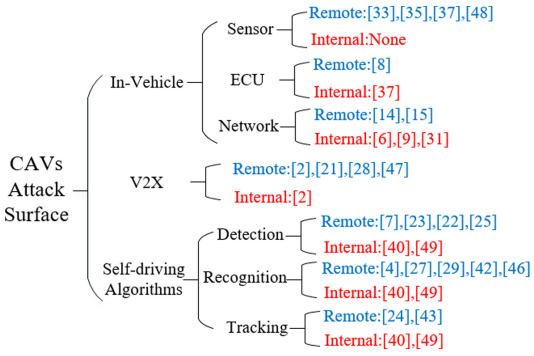

Fig. 2. Example of potential attacks by various research groups

3.1 Attacks Against In-Vehicle Systems

In-vehicle systems consist of three major components: sensors, ECUs and bus networks. Each of them may be compromised with both remote and internal attacks. Remote includes primarily any form of wireless communications interface. Internal includes both physical access such as the USB or OBD-II port,

and internal elements of the in-vehicle system interconnected on the network or the network itself.

Network: The CAN network is an important attack surface. Due to the broadcast nature of CAN as well as a lack of encryption, an attacker with access to internal network can monitor and reverse engineer the network architecture, collect personally sensitive information, or perform DoS attacks. Access to the network can be obtained through a physical interface or through a variety of wireless attack vectors.

The attacks on wireless interfaces are almost remote attacks. Work [14] analyzed relay attacks on Passive Keyless Entry and Start (PKES) systems used in modern cars. Work [15] proposed that by recovering the cryptographic algorithms and keys from ECUs, an adversary can gain unauthorized access to a vehicle. There are many internal attacks on CAN. For example, the attackers can eavesdrop CAN data by installing interceptors on the CAN network [6]. The eavesdropping attack is the starting point for many attacks, such as spoofing attacks, Dos attacks [6,31] and replay attacks. Work [9] discussed two kinds of spoofing attacks, which are masquerade attack and fabrication attack.

ECU: Compromising an ECU can also provide access to other shared secrets (such as cryptographic keys) which allow an attack to extend to other components on the vehicle.

One of the remote attacks is proposed by work [8] named battery drain attack due to the ECU wake-up mechanism. On the other hand, an attacker can physically internal attack the ECU through voltages, currents, and other physical means, such as overcurrent attacks [37]. This attack makes the microprocessor fail or burn out by exceeding the maximum rating of the microprocessor.

Sensor [33,37]**:** Sensors can be manipulated directly to achieve a particular effect. By modifying the physical property detected by a sensor, tampering with the sensor hardware, or through electromagnetic attacks, the input for which an ECU will make a decision can be modified directly.

Attacks on sensors are mostly remote attacks, such as jamming attacks [47] and spoofing attacks [47]. Noise can change sensor data to provide malicious input to components using the data. The tire pressure sensor in the TPMS (Tire Pressure Monitoring System) can be used for observation and tracking purposes and as an activation trigger for other attacks [35].

3.2 Attacks Against V2X Communication

Vehicles across different manufacturers share DSRC as a common attack surface since they communicate with each other on the same V2X system. Separate from the remote code execution risk, false data provided through a V2X system can cause disruptions in traffic flow and pose a risk to personal safety through physical effects. In addition, any vulnerability may have the potential to spread to other vehicles or infrastructure quickly.

Most of the attacks on V2X are remote attacks which are carried out through the **V2X communication protocols** such as IEEE 802.11p. These attacks

include [28]:1) *Black hole attack*: The compromised node will not relay the data packet to adjacent nodes, and the data packet will be intercepted and discarded by the attacker [2]. 2) *Flooding attack*: By flooding the MAC, the attacker will send countless data packets to make the victim node unusable. 3) *Jamming attack*: By using a jammer to identify the data packet and launch attack, the attacker can broadcast signals to destroy the data or block the channel, etc. [21]. 4) *Sybil attack*: The attacking station will send false V2X messages, which will simulate fake sites on the road and prevent other sites from sending real messages.

Vehicle ransomware [46] is also a remote attack but it is based on **terminal nodes**, such as mobile phones and the vehicle-mounted security vulnerabilities. Attackers can indirectly infect botnets to vehicles through smartphones, navigation, etc. and through vulnerabilities such as the Bluetooth buffer overflow vulnerability of in-vehicle infotainment units to lock the key parts of the vehicle.

Eavesdropping attacks [2] can be internal attacks or remote attacks. In the internal attack, attackers can collect information anywhere without permission, such as the data management system. In the remote attack, attackers can eavesdrop on vehicle information due to the plaintext transmission.

3.3 Adversarial Attacks Against Autonomous Algorithms

If autonomous algorithms are attacked, the autopilot system may make an adverse decision, resulting in devastating consequences. Similar to Sect. 2.3, we divide algorithm-related attacks into three tasks.

Attacks on Object Detection Algorithms [7,23,39,48]**:** They are mostly based on three techniques: *feature extraction region*, *iterative optimization*, and *Generative Adversarial Network (GAN)*. Since target detection algorithms need to extract the region of interest, attackers corrupt the extracted region by interference. DPATH attack [25] is to make the region where the adversarial patches exists as the only valid region of interest, while potential proposal region are ignored. BPATH attack [22] generates and refines the adversarial background patches in the overall loss optimization iterations.

Attacks on Object Recognition Algorithms [4,27,41,45]**:** Three categories as shown below. Because there are few cases of classification algorithm, however they are the most classical in the field of deep learning vision, simply mention it as a category.

- *Fast Gradient Sign based Adversarial attacks:* Iterative Targeted Fast Gradient Sign Method which is based on FGSM algorithm applies the target FGSM multiple times for a more powerful example of confrontation.
- *Optimization based Approach:* In this way, the adversary samples are obtained by solving optimization problems. By replacing the class variables in the antidisturbance with target class with the lowest recognition probability, the least likely class iterative methods are obtained.

– *Universal Adversarial Perturbation:* Universal advanced perturbations computed by Moosavi-Dezfooli et al. [29]. can generate any image attack disturbance, which is also almost invisible to human beings.

Attacks on the Trajectory Algorithms [42,48]**:** Trajectory algorithms are mainly attacked by *strategical time attack* and *enhancing attack* [24]. Strategically time attack is a traditional and conventional learning method. Enhancing attack's goal is to induce the agent to go to a specified state makes the performance of agent worse.

4 Survey of Technical Defense

This section will provide an overview of existing defensive approaches in response to the attack model presented in Sect. 3.

4.1 Defensive Approaches for In-Vehicle Systems

Authentication-Based Countermeasures: The lack of authenticity within automotive networks is a prime cause of the failure of today's automotive security. We admit that cryptography and key management is a requirement for any system that attempts to implement authentication. However, implementation of any form of cryptography on the car's resource constrained ECUs performing real-time control may not be practicable. Therefore, securing the external gateways and communications paths to the CAN bus may prove more valuable and workable than securing the individual nodes through cryptography.

One method of adding authentication between CAN nodes is through the use of Message Authentication Codes (MACs). For example, work [18] proposed the IA-CAN (Identity-Anonymized CAN) protocol. This scheme randomizes the CAN ID on a frame-by-frame basis to provide sender authentication and prevent attackers from injecting fake messages. In work [12], Parrot system was proposed to defend against the spoofing attack. The ECU equipped with Parrot System can identify spoofing messages on the bus that impersonate one of its own IDs.

In addition, there are other authentication-based defense methods. Work [30] have summarized some defenses and evaluated them through custom security testing standards. Therefore, in these paper we will not repeat them.

Fingerprint-Based Countermeasures: Fingerprint-based access control prevents attackers from accessing certain resources by verifying them as unauthorized nodes. Certain physical characteristics/uniqueness such as the voltage, the signal rising and falling edge characteristics and the clock frequency are utilized to recognize legitimate ECUs, so this type of approaches can prevent spoofing attacks. For example, work [10] firstly proposed the voltage profile of the ECU as its specific fingerprint to identify the attacker ECU by measuring and using the voltage on the vehicle network and implemented the corresponding detection

tool called Viden. Work [20] improved Viden by only measuring the dominant voltage of the ECU as a signaling feature, and using high and low signals rather than differential signals which would make it more error-prone in identifying attacker ECUs.

To prevent bus-off attacks (i.e., a type of denial-of-service attacks), work [11] proposed VoltageIDS, an intrusion detection system based on voltage characteristics. VoltageIDS uses electrical characteristics which is the time when the status of the signal changes from 0 to 1 and 1 to 0 as the fingerprint characteristics of the CAN message.

Furthermore, the defensive approaches for in-vehicle systems are not limited to ECU-based "fingerprints". Work [36] developed a motion-based IDS (MIDS). This method determines whether the data is normal or has been tampered based on the fingerprint characteristics of the vehicle's behavior correlation at a certain time, such as wheel speed, vehicle speed, etc.

IDS-Based Countermeasures: The intrusion detection method in the automotive domain depends on how the detection mechanism is utilized within the system. The anomaly-based IDS is the most common and promising approach used in the automotive IDS compared to the signature- and statistical-based technique. As mentioned above, Work [9] proposed the clock-based intrusion detection system (CIDS). It exploited the timing interval of CAN traffic and the frequency of CAN packet sequences in identifying anomalies within the CAN bus network.

The signature-based approach detects an attack by utilizing a set of identified signatures, malicious events, or rules stored in the database module of IDS. For example work [40] extracted the attack signatures obtained from standard ECU specifications using finite-state automate (FSA) in detecting an anomalous sequence of CAN packets via the in-vehicle network.

Other Defensive Approaches: There are other defense methods and are not based on the three categories above. Work [35] provided some defense guidance against TPMS attacks which is encrypting TPS packets and placement of additional password checksums, such as message authentication codes, before CRC checksums. Besides, Mehmet Bozdal, et al. [6] have been made a survey on the other defensive approaches and we will not repeat in this paper.

4.2 V2X Security Defense

V2X attacks are mostly remote attacks, so this section will focus on security defense methods against them.

Remote attacks are usually completed through protocol vulnerabilities. Many researchers have found methods to against them. The model proposed in work [1] uses advanced encryption standards to achieve user privacy. Using the randomness of channels in a vehicle network to share keys solves the key distribution problem of advanced encryption standards. Work [5] proposed a secure and

intelligent routing protocol where they use double encryption on packets and use the authentication scheme to measure the trust of nodes. However, this method increases processing time and adds network overhead. Work [49] proposed a new method to create passwords based on one-time authentication asymmetric group key protocols Mixed zones to protect against malicious eavesdropping. Security information is encrypted using group keys to improve vehicle privacy.

In particular, for the Sybil attack, work [16] used directional antennas to identify the source of the message. If a malicious vehicle broadcasts a large number of messages, it will be discovered by other vehicles.

4.3 Defensive Measures for Autonomous Algorithms

Countermeasures for Object Detection and Recognition: To improve the performance of the machine learning models against adversarial attacks, existing solutions developed in other domains may not be directly used for autonomous driving. For example, the detection of adversarial attacks may not be useful. However, there exist suitable solutions to help the CAVs defend against adversarial attacks in literature.

These approaches include but not limited to: 1) *data augmentation*, using image processing methods to help augment the quantity and diversity of the training set; 2) input transformation, using image processing methods to disturb or even remove the adversarial perturbations; 3) *adversarial training* [17]; and 4) *defensive distillation* [32];

Input transformation through image processing methods(e.g. JPEG compression) is considered to be the potential defensive measure. Work [50] discussed that input transformation may not be useful if the adversarial samples are generated with various transformations and random noise.

Adversarial training was discussed in work [38,50]. The idea of adversarial is producing adversarial samples during the training process and injecting them to the training set. Work [50] discussed that adversarial training can be bypassed through transferability or generating new adversarial samples against the improved models. Besides adversarial training, defensive distillation was also evaluated in work [13].

Countermeasures for Object Tracking and Trajectory Algorithms: To defend attacks on object tracking and trajectory, since object tracking and trajectory is now mainly based on reinforcement learning and time series algorithm, common defensive measures against adversarial attacks might be useful, such as adversarial training, defensive distillation, and data augmentation.

Objective function plays a pivotal role in reinforcement learning algorithm, and changing the objective function might also help to defend attacks on the object tracking and trajectory such as adding stability term and adding regularization term. By measuring the difference of the output produced from different input of versions of perturbations, the purpose of adding stability term is to help DNN generate similar output against natural perturbations. The idea of adding

regularization term to defend is adding the norm of adversarial perturbations to the objective function, thus attenuating the effect of adversarial perturbations.

5 Discussion

The security issues of CAVs are still considered to be open research areas, and many issues need to be resolved. This section will discuss some of these issues. As CAVs are becoming more popular, people are now getting concerned if it is necessary to regulate their use. For example, in 2018 in Arizona (USA) the first case of an autonomous car killing a pedestrian has been registered. In this case, who should be considered to be at fault? The problem is related to whether the driver in the car controls the vehicle at the moment of the accident. Is the car manufacturer at fault, or should the attackers who hacked self-driving take the responsibility. Identifying or fingerprinting drivers is one of proposed approaches to answer these questions. There have been many studies on combining vehicle network data with machine learning in recent years, collecting vehicle data to learn the driver's behavioral characteristics, as each driver's unique "fingerprint", and successfully identifying the driver during driving. However, there is no solution to determine whether is automatic driving or human driving. We believe that each driver's style of driving the vehicle, is different, including the AI driver. In this way, by collecting enough in-vehicle data, it is possible to determine whether the car was driven autonomously or artificially when a car accident occurs. Yet it needs further investigation.

In addition, certain vehicle attacks currently do not have effective solutions, such as the battery exhaustion attack against the ECU wake-up mechanism, the interference attacks faced by environmental sensors, and fast gradient sign based adversarial attacks on sensors that process images, etc. Some of them are mentioned above. These attacks have received a lot of in-depth research, but few countermeasures are available. Therefore, the CAVs security is still long way to go.

6 Conclusion

In this survey, we systematically discuss attacks and defense methods for connected and autonomous vehicles, as well as security of CAVs algorithms. In order to better present the most current research in this area, we divide CAVs into three layers: in-vehicle network, V2X, and autonomous vehicle algorithms. Besides, we divide the attacks on each layer into two categories: remote attacks and internal attacks, and list examples of each type of attack in the form of a table. Then we synthesize and summarize existing defenses to determine their effectiveness against these identified attacks. Finally, we provide further discussion on the security of CAVs. This survey provides a good foundation for researchers interested in the connected and autonomous vehicles and provide a systematic overview of the security issues for them.

Acknowledgement. We sincerely thank reviewers for their insightful feedback. This work was supported in part by NSFC Award #61972200.

References

1. Abdelgader, A.M., Shu, F.: Exploiting the physical layer security for providing a simple user privacy security system for vehicular networks. In: International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), pp. 1–6. IEEE (2017)
2. Alnasser, A., Sun, H., Jiang, J.: Cyber security challenges and solutions for V2X communications: a survey. Comput. Netw. **151**, 52–67 (2019)
3. Avatefipour, O., Malik, H.: State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vulnerabilities. arXiv preprint arXiv:1802.01725 (2018)
4. Baluja, S., Fischer, I.: Adversarial transformation networks: learning to generate adversarial examples. arXiv preprint arXiv:1703.09387 (2017)
5. Bhoi, S.K., Khilar, P.M.: SIR: a secure and intelligent routing protocol for vehicular ad hoc network. IET Netw. **4**(3), 185–194 (2014)
6. Bozdal, M., Samie, M., Jennions, I.: A survey on can bus protocol: attacks, challenges, and potential solutions. In: International Conference on Computing, Electronics & Communications Engineering (ICCECE), pp. 201–205. IEEE (2018)
7. Chen, S.-T., Cornelius, C., Martin, J., Chau, D.H.P.: ShapeShifter: robust physical adversarial attack on faster R-CNN object detector. In: Berlingerio, M., Bonchi, F., Gärtner, T., Hurley, N., Ifrim, G. (eds.) ECML PKDD 2018. LNCS (LNAI), vol. 11051, pp. 52–68. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-10925-7_4
8. Cho, K.T., Kim, Y., Shin, K.G.: Who killed my parked car? arXiv preprint arXiv:1801.07741 (2018)
9. Cho, K.T., Shin, K.G.: Fingerprinting electronic control units for vehicle intrusion detection. In: USENIX Security Symposium (USENIX Security), pp. 911–927 (2016)
10. Cho, K.T., Shin, K.G.: Viden: attacker identification on in-vehicle networks. In: ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1109–1123 (2017)
11. Choi, W., Joo, K., Jo, H.J., Park, M.C., Lee, D.H.: VoltageIDS: low-level communication characteristics for automotive intrusion detection system. IEEE Trans. Inf. Forensics Secur. (IEEE T INF FOREN SEC) **13**(8), 2114–2129 (2018)
12. Dagan, T., Wool, A.: Parrot, a software-only anti-spoofing defense system for the CAN bus. In: Embedded Security in Cars Europe (ESCAR), p. 34 (2016)
13. Deng, Y., Zheng, X., Zhang, T., Chen, C., Lou, G., Kim, M.: An analysis of adversarial attacks and defenses on autonomous driving models. arXiv Signal Processing (2020)
14. Francillon, A., Danev, B., Capkun, S.: Relay attacks on passive keyless entry and start systems in modern cars. In: Proceedings of the Network and Distributed System Security Symposium (NDSS) (2011)
15. Garcia, F.D., Oswald, D., Kasper, T., Pavlidès, P.: Lock it and still lose it -on the (in)security of automotive remote keyless entry systems. In: USENIX Security Symposium (USENIX Security) (2016)

16. Golle, P., Greene, D., Staddon, J.: Detecting and dorrecting malicious data in VANETs. In: ACM International Workshop on Vehicular Ad Hoc Networks (VANET), pp. 29–37 (2004)
17. Goodfellow, I.J., Shlens, J., Szegedy, C.: Explaining and harnessing adversarial examples. In: International Conference on Machine Learning (ICML) (2015)
18. Han, K., Weimerskirch, A., Shin, K.G.: A practical solution to achieve real-time performance in the automotive network by randomizing frame identifier. In: Embedded Security in Cars Europe (ESCAR), pp. 13–29 (2015)
19. Ishak, M.K., Leong, C.C., Sirajudin, E.A.: Embedded ethernet and controller area network (CAN) in real time control communication system. In: Zawawi, M.A.M., Teoh, S.S., Abdullah, N.B., Mohd Sazali, M.I.S. (eds.) 10th International Conference on Robotics, Vision, Signal Processing and Power Applications. LNEE, vol. 547, pp. 133–139. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-6447-1_17
20. Kneib, M., Huth, C.: Scission: signal characteristic-based sender identification and intrusion detection in automotive networks. In: ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 787–800 (2018)
21. Laurendeau, C., Barbeau, M.: Threats to security in DSRC/WAVE. In: Kunz, T., Ravi, S.S. (eds.) ADHOC-NOW 2006. LNCS, vol. 4104, pp. 266–279. Springer, Heidelberg (2006). https://doi.org/10.1007/11814764_22
22. Li, Y., Bian, X., Lyu, S.: Attacking object detectors via imperceptible patches on background. Computing Research Repository (CoRR) (2018)
23. Li, Y., Tian, D., Bian, X., Lyu, S., et al.: Robust adversarial perturbation on deep proposal-based models. arXiv preprint arXiv:1809.05962 (2018)
24. Lin, Y.C., Hong, Z.W., Liao, Y.H., Shih, M.L., Liu, M.Y., Sun, M.: Tactics of adversarial attack on deep reinforcement learning agents. arXiv preprint arXiv:1703.06748 (2017)
25. Liu, X., Yang, H., Song, L., Li, H., Chen, Y.: DPatch: attacking object detectors with adversarial patches. Computing Research Repository (CoRR) (2018)
26. Miller, C., Valasek, C.: Remote exploitation of an unaltered passenger vehicle. Black Hat USA **2015**, 91 (2015)
27. Milton, M.A.A.: Evaluation of momentum diverse input iterative fast gradient sign method (M-DI2-FGSM) based attack method on MCS 2018 adversarial attacks on black box face recognition system. arXiv preprint arXiv:1806.08970 (2018)
28. Mokhtar, B., Azab, M.: Survey on security issues in vehicular ad hoc networks. Alex. Eng. J. (AEJ) **54**(4), 1115–1126 (2015)
29. Moosavi-Dezfooli, S.M., Fawzi, A., Fawzi, O., Frossard, P.: Universal adversarial perturbations. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1765–1773 (2017)
30. Nowdehi, N., Lautenbach, A., Olovsson, T.: In-vehicle CAN message authentication: an evaluation based on industrial criteria. In: IEEE Vehicular Technology Conference (VTC-Fall), pp. 1–7. IEEE (2017)
31. Palanca, A., Evenchick, E., Maggi, F., Zanero, S.: A stealth, selective, link-layer denial-of-service attack against automotive networks. In: Polychronakis, M., Meier, M. (eds.) DIMVA 2017. LNCS, vol. 10327, pp. 185–206. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60876-1_9
32. Papernot, N., McDaniel, P., Wu, X., Jha, S., Swami, A.: Distillation as a defense to adversarial perturbations against deep neural networks. In: IEEE Symposium on Security and Privacy (S&P), pp. 582–597. IEEE (2016)
33. Petit, J., Stottelaar, B., Feiri, M., Kargl, F.: Remote attacks on automated vehicles sensors: experiments on camera and lidar. Black Hat Eur. **11**, 2015 (2015)

34. Raiyn, J.: Data and cyber security in autonomous vehicle networks. Transp. Telecommun. J. **19**(4), 325–334 (2018)
35. Rouf, I., Miller, R.D., Mustafa, H.A., Taylor, T., Seskar, I.: Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: USENIX Security Symposium (USENIX Security) (2010)
36. Sagong, S.U., Poovendran, R., Bushnell, L.: Inter-message correlation for intrusion detection in controller area networks. Technical report, Washington University (2019)
37. Sagong, S.U., Ying, X., Poovendran, R., Bushnell, L.: Exploring attack surfaces of voltage-based intrusion detection systems in controller area networks. In: Embedded Security in Cars Europe (ESCAR) (2018)
38. Sitawarin, C., Bhagoji, A.N., Mosenia, A., Chiang, M., Mittal, P.: DARTS: deceiving autonomous cars with toxic signs. arXiv Cryptography and Security (2018)
39. Stewart, J.: Self-driving cars use crazy amounts of power, and it's becoming a problem. wired.com, Transportation (2018)
40. Studnia, I., Alata, E., Nicomette, V., Kaâniche, M., Laarouchi, Y.: A language-based intrusion detection approach for automotive embedded networks. Int. J. Embed. Syst. (IJES) **10**(1), 1–12 (2018)
41. Su, J., Vargas, D.V., Sakurai, K.: One pixel attack for fooling deep neural networks. IEEE Trans. Evolu. Comput. (TEVC) **23**(5), 828–841 (2019)
42. Sun, J., et al.: Stealthy and efficient adversarial attacks against deep reinforcement learning. arXiv preprint arXiv:2005.07099 (2020)
43. Takahashi, J.: An overview of cyber security for connected vehicles. IEICE Trans. Inf. Syst. **101**(11), 2561–2575 (2018)
44. Wang, J., Shao, Y., Ge, Y., Yu, R.: A survey of vehicle to everything (V2X) testing. Sensors **19**(2), 334 (2019)
45. Wiyatno, R., Xu, A.: Maximal Jacobian-based saliency map attack. arXiv preprint arXiv:1808.07945 (2018)
46. Wolf, M., Lambert, R., Enderle, T., Schmidt, A.: Wanna drive? Feasible attack paths and effective protection against ransomware in modern vehicles. In: Embedded Security in Cars Europe (ESCAR) (2017)
47. Yan, C., Xu, W., Liu, J.: Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle. DEFCON **24**(8), 109 (2016)
48. Zang, S., Ding, M., Smith, D., Tyler, P., Rakotoarivelo, T., Kaafar, M.A.: The impact of adverse weather conditions on autonomous vehicles: how rain, snow, fog, and hail affect the performance of a self-driving car. IEEE Veh. Technol. Mag. **14**(2), 103–111 (2019)
49. Zhang, L.: OTIBAAGKA: a new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. **12**(12), 2998–3010 (2017)
50. Zhao, Y., Zhu, H., Liang, R., Shen, Q., Zhang, S., Chen, K.: Seeing isn't believing: towards more robust adversarial attack against real world object detectors. In: ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1989–2004 (2019)