Connected Vehicles: Use Cases, Privacy Issues, and Defense Techniques

Barış Kaplan *, Ilter Erol Gurol†,
*Department of Computer Engineering, Koç University, Sariyer 34450, Istanbul, Turkey
†Department of Electrical and Electronics Engineering, Koç University, Sariyer 34450, Istanbul, Turkey
e-mail: bkaplan18@ku.edu.tr, igurol19@ku.edu.tr,

***Abstract*—Nowadays, with the development trend of smart cities, Internet of Things (IoT) technologies are on the rise. The automotive industry is no exception to this trend, where today's car can be referred to as an IoT grid, which is also referred to as the Internet of Vehicles (IoV). This shift in the automotive industry has significant impacts on the lives of the people, such as the ability to interact with the roads, traffic lights via IoV, and with other cars via Vehicle-to-Vehicle (V2V) Communication. Such connectivity with sensor networks leads to an increase in transportation safety and faster travel times, promotes mobility choices, reduces user costs by increasing fuel efficiency, etc. Despite all these advantages, Connected and Automated Vehicles (CAVs) come with several challenges. One of those challenges is to collect, process and send massive amount of data (25 GBs/h) to the cloud environment. In such a dense data-traffic environment between the CAVs and the outside environment, data breaches may likely to exist. Furthermore, malicious users are likely to exist, where they are able to implement various CAV attacks, which threaten the CAV security. Thus, this paper focuses on use cases of the CAVs with the aim of highlighting their privacy and security challenges, where up-to-date protection and defense techniques against these challenges are also discussed.**

***Index Terms*—Cybersecurity, Connected and Automated Vehicle Security (CAVs)**

I. Introduction

In the last decade, researchers, engineers, and scientists are becoming increasingly interested in sensor networks, Internet of Things (IoTs), smart cities, and Connected and Automated Vehicles (CAVs). All these technologies, and especially CAVs are believed to improve the efficiency and the safety of the transportation by utilizing the in-build sensor networks' ability to measure and share data such as position, speed, and movement [1], [2]. At the core of CAVs lie the sensor networks, IoT applications, and Vehicle-to-Vehicle (V2V) communication schemes. The desire to develop increasingly autonomous and connected vehicles inevitably require larger sensor networks, more IoT applications and more data to be shared over the V2V communication protocols. However, this desire requires an increase in the computational infrastructure, which may also lead to an increase in the complexity. As the complexity of the CAVs increase, they become more vulnerable to cyberattacks [3]. This also increases the risk of which an adversary can control a vehicle, or its surrounding devices [4]. As an example in [5], a vulnerability in the vehicle's infotainment system is discussed, where they were able to hack successfully into a Jeep Cherokee. Interestingly, as a result of this hack, adversaries were able to control the steering wheel, accelerator and etc. Similar to this, in [6], [7], many other examples of cyberattacks are covered, which mainly focus on IoT and embedded technologies, which indirectly threaten the CAVs.

All the above-mentioned security breach examples indicate and highlight the underestimation of cybersecurity issues in the system design. The lack of consideration of cybersecurity issues in the system design may lead to catastrophic results for the CAV industry. Therefore, it is essential to highlight and classify the cybersecurity-related issues for CAVs.

The security of CAVs can be classified into two main categories: intra-vehicle network security and inter-vehicle security. The former includes security issues related to the in-vehicle communication among the Engine Control Unit (ECU), other electro-mechanical parts, and sensors. On the other hand, the latter focuses on connectivity (base station (BS), external devices (EDs), Intelligent Transportation Systems (ITS)) and covers V2V communication [8]. Intra-vehicle communication is mainly built on CAN-Bus protocol, which does not consider security at all in the manner of confidentiality, integrity, and authentication. CAN architecture simply broadcasts messages to all components, very similar to a publish-and-subscribe model. This is due to the time it was developed. Since there were no CAVs related concerns, CAN-Bus architecture is designed for infotainment, power train, and chassis control. On the other hand, inter-vehicle networks are based on three different common schemes, with yet more to come. These standard interfaces for EDs are In-vehicle Infotainment (IVI) systems, containing the CD player, Bluetooth, and other infotainment interfaces. Secondly, the Onboard Diagnostic II (OBD-11) interface for diagnostics, repair, and reporting capabilities. Thirdly, the Telematics Box (T-BOX) and Telematic Server Providers (TSP) for vehicle data sharing and other capabilities. [9]. All these three forms of communication schemes with EDs offer limited security, where a single gateway filter is used to control and filter the malicious messages. However, this approach is far from optimal and may cause malicious messages to be reached to it's destination. Despite such a need, V2V or any communication with EDs are designed considering first the following aspects: scalability, low latency, and reliability. The main concern and the main challenge in such schemes are considered real-time communication with a large number of devices.

All the above-mentioned issues highlight the alarming cy-

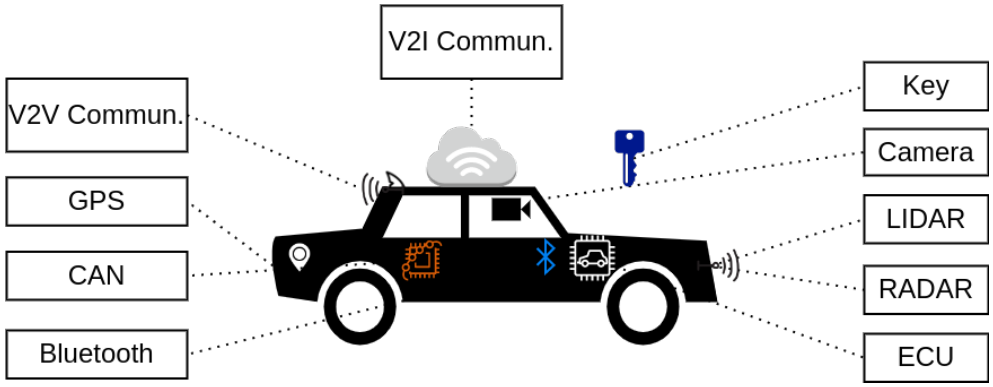

Fig. 1. Potential Security Flow Locations in CAVs.

bersecurity issues in CAVs. Therefore, Automotive cybersecurity standards, such as SAE (Society of Automotive Engineers) J3061 [10] are proposed to overcome these critical problems. In [10], the committee also involved high-level procedures for the purpose of security testing. Nonetheless, the proposed approaches are highly expensive and do not standardize the specific tests which are supposed to be performed for security evaluations. Against all that, our motivation in this paper is to state where the connected vehicles are used, analyze both intra- and inter-vehicle security issues, summarize them, and propose methodologies to patch the security issues in an abstract manner.

II. General Overview & Use Cases of CAVs

In this section, we provide a general overview of CAV-related technologies and provide their use cases, where we group CAV-related technologies under intra-vehicle technologies and inter-vehicle technologies.

A. Intra-Vehicle CAV Technologies

The CAVs are a complex system of systems (SoS), which employ semi-autonomous systems such as driver-assistance systems (DAS), brake assistants (BA), lane centering assistants (LCA), and adaptive cruise control (ACC) systems. These systems are packaged in such a way that they can work in harmony with each other. To achieve a flawless SoS, the systems have to communicate with each other. The communication among the above-mentioned technologies is achieved with intra-vehicle communication technologies, which is based on CAN-Bus architecture in the state-of-the-art CAVs. The CAVs are also able to collect, compare, verify and process the internal data with the received outer data coming from Vehicle-to-Infrastructure (V2I) and V2V communication technologies. For example, the speed of a CAV can automatically be adjusted by comparing the internal speed and velocity data with the estimated speed and distance data coming from the lidar and radar. This system is also commonly named ACC. Moreover, similar to ACC and BA, the location of the car can be automatically adjusted to the center of the lane; which is referred as LCA. Using such technologies, these driver-assistance systems result in having a safer and better travel experience with the connected vehicles in the traffic. However, they also cause a security overhead to be dealt with.

B. Inter-Vehicle CAV Technologies

As mentioned in Section II-A in Section II, CAVs have to manage the communication between both internal devices and have to provide outer interfaces to interact with the surroundings and environment. One of such outer interfaces is the Global Positioning System (GPS). The GPS data provided by GPS satellites in collaboration with the data collected via V2I and V2V communication schemes are used for the navigation and maneuver of the CAVs. In addition to the maneuver and navigation of the CAV, the navigation system is also capable of optimizing the path to the destination in such a way that both the cost and the time to the destination is reduced. As another side benefit of this process, the traffic density may be reduced, and this can also indirectly decrease the probability of traffic accidents. Additionally, in combination with the V2I communication schemes, CAV technologies can further impose further technologies on our daily life, where smart parking technologies and usage-based insurance can be utilized with CAVs [11]. As mentioned in [11], by using a telematics technology called ”GPS,” the insurance fee is determined by the amount of travel with the car and the driving behavior of the driver. Moreover, the connected vehicle data is used in the prediction depending on car maintenance systems. In addition to such telematic technologies, ML applications can be further utilized for predictions based on the collected big data from the CAVs [12].

C. Security Overhead Caused by Intra- and Inter-Vehicle Technologies

As mentioned in Section II-A and Section II-B in Section II, CAVs has to manage many different systems or subsystems under a SoS. Although such an architecture offers numerous benefits to our life, environment and etc., CAVs also come with a cost and a security overhead. Many technologies built into to CAVs or their interaction with their outer environment leaves some security gaps that can be exploited for the adversary’s benefit. Such potential security gaps are analyzed in the Section III.

III. The Potential Security Flow Locations In CAVs

As shown in Fig. 1, CAVs are vulnerable to many different kinds of attack surfaces since they employ many different

TABLE I
DIFFERENT CYBERATTACKS AND DEFENSE MECHANISMS AGAINST CAVS.

Attack Surface	Cyberattack(s)	Defense Mechanisms
LIDAR	Manipulate EM signals	Random Modulation of Output Signal
RADAR	Manipulate EM signals	Random Modulation of Output Signal
GPS	Manipulate GPS signals	Compare GPS signals from neighboring CAVs
CAN-Bus	Listen CAN-Bus channel CAN-Bus Poisoning	CAN-Bus must employ integrity, authenticity checks in hand with cryptography
Bluetooth	Attack on Commun. Protocol	Employing safe Bluetooth protocols commercially
ECU	ECU Flashing Code Change	Integrity Checks
ML Apps	Learning Attacks Data poisoning	Black-Box modeling
Entertainment System	DOS attacks Impersonating attacks Replay Attacks Routing Attacks Data falsification attacks Priority attacks Eavesdropping attacks	Integrity, authentication checks Black-Box modeling

automated technologies, which may be vulnerable to different kinds of cyberattacks. In this section, we will be analyzing different kinds of cyberattacks and defense mechanisms against these cyberattacks. The intra-vehicle attacks and their defense mechanisms are analyzed in Section III-A and inter-vehicle cyberattacks in collaboration with the defense mechanisms against them are analyzed in Section III-B.

A. Intra-Vehicle Security Issues in the Use Cases

In this section, we will be analyzing intra-vehicle communication and cyberattacks based on the employed intra-vehicle technologies in CAVs. The cyberattack types with their corresponding attack surfaces and defense mechanisms against them are given in Table I.

1) Attack & Defense Mechanisms (LIDAR): LIDAR system is part of autonomous cars, which is used for sensing applications, as well as for estimating the range between CAVs and detecting obstacles in the environment. This technology is based on sending and receiving electromagnetic (EM) waves with wavelengths between 1020-520 nm, depending on the laser type used. This technology is one of the key components of ACC and CAV for sensing reasons. However, it is easy to manipulate received signals by sending malicious signals from another laser at different time intervals to generate false obstacles, or even it can poison the estimation process by forcing CAVs to move in a specific direction. To perform such attacks, the attacker first has to analyze the frequency spectrum, and then the attacker has to analyze signal-defining words (EM signal parameters). Once the attacker knows the EM wave's parameters, the attacker then sends malicious signals.

On the other hand, protecting CAVs against such attacks requires time-consuming digital-signal-processing (DSP) techniques in time or frequency, or both. This method is usually not applicable to CAVs, since the real-time operation is considered one of the key design features. However, random modulation performed on the transmitted signals may help to distinguish the reflection of the modulated-transmitted signals from the signals sent by the adversary. Due to randomness, unless the seed is somehow known by the adversary, the CAV should be able to distinguish the signal. This method, however, may not be prone to repetition attacks in some scenarios. Despite that, it can still continue its operation in a safe way, where it can compare the estimation results with the data obtained from the other sensors (camera, radar, etc.).

2) Attack & Defense Mechanisms (RADAR): Radar application in CAVs follows a similar path to LIDAR applications. The main difference between radar and lidar is that the radar operates at a much lower frequency (usually FMCW Radar with 70 GHz). Since the radar's operation principle is very similar to lidar with much lower resolution, radar on CAVs may suffer from the same attacks against lidar, where the manipulation of the received EM signals is utilized. More details about such attacks are already given and analyzed in Section III-A1. Therefore, it is also possible to develop similar defense mechanisms mentioned in Section III-A1.

3) Attack & Defense Mechanisms (GPS): GPS is one of the main core components of CAVs. Without the location information, a CAV may be incapable of planning routes to the desired information. As a result of that, the overall experience and overall performance of the autonomous processes may be degraded. Therefore, GPS spoofing attacks may become extremely common. While implementing the GPS spoofing attacks, an adversary alters the obtained GPS signal arbitrarily inside the attacked surface [13]. To achieve a successful attack, the malicious GPS signal's received signal strength must be higher. If performed successfully, an adversary poison the location data, which can force CAV to change its trajectory.

To defend CAVs against GPS spoofing attacks, there are different strategies that can be followed. Some of these defence techniques are estimation range check [14], statistical test [15], velocities consistency check [16], and global navigation satellite system augmentation [17]. The methods mentioned in [14]–[17] relies on backtracking, consistency of the received information, statistics. However, to prevent such attacks, a V2V Network can also be utilized by sharing the GPS data information among the V2V network. This application, however is not straightforward since usually, when a GPS Spoofing attack is performed, neighboring CAVs will also be affected. Despite that, by comparing the GPS data with other CAVs in the network, the attack can be detected, and the location information can be obtained by taking another car's GPS data as a reference. Then, the location of the desired CAV can be computed by using other ranging metrics of the CAVs in the same V2V Network. Additionally, to prevent such attacks V2I networks can also be utilized, where reference GPS data can be pushed to the CAVs by the infrastructures built near the

environment.

4) Attack & Defense Mechanisms (CAN-Bus): CAN-Bus is the main communication protocol which is used by the car manufacturers. The CAN-Bus is designed to be simple and efficient. However, it does not consider security at all since it was not a concern at the time it was developed. The primary problem with the CAN-Bus architecture is the deficiency existing in the authentication and encryption processes [18]. This implies that an adversary can easily can join the network, listen to the communication and participate. In addition, CAN-Bus architecture is also vulnerable to the Denial-of-Service (DoS) attacks [19], as in CAN-Bus the arbitration mechanism permits the node having the higher priority to speak first [19]. Furthermore, CAN-Bus discards messages from parts if too many erroneous messages are received. This feature can also be exploited for attacks by the adversary.

To defend CAVs from the above-mentioned vulnerabilities following defense mechanism must be employed. CAN-Bus must be based on an encryption mechanism. Further, in [20], [21] authentication is employed on the CAN-Bus architecture.

5) Attack & Defense Mechanisms (Bluetooth): Bluetooth is a short-range communication protocol that operates between 2402 and 2480 MHz. Attacks that involve Bluetooth therefore require the adversary to be located near the CAV. However, this can also be exploited by malicious other CAVs, which is located near the target CAV. There are two main concerns related to Bluetooth security. First, the pin-paring mechanism does not employ encryption, which enables the opportunity for an adversary to eavesdrop on the Bluetooth pairing pin. The other main problem with Bluetooth is that a paired malicious device can be utilized to access and take control of the CAVs. Furthermore; it has been demonstrated that the Bluetooth control code involves a potential memory exploit, and this situation permits the code execution from any paired Bluetooth device. [22].

To fix the above-mentioned problems, cryptographic algorithms for Bluetooth are designed to provide authentication and encryption. However, due to efficiency concerns, these algorithms are currently not employed in commercial products. Despite that, they must be utilized for CAVs.

6) Attack & Defense Mechanisms (ECU): An ECU is responsible for the control of a car or a CAV. They lie in the core of any given car application, whether it is autonomous or not. The ECU is designed to be reprogrammable for future support, tweaks, and functionalities. However, this feature of ECUs creates a vulnerability, where an adversary can perform an ECU flashing attack [23].

To prevent a flashing attack on ECU, the ECU must employ encryption, integrity, and authentication checks [24]. These are easy tasks to employ, but these will definitely create a small overhead for the ECU.

7) Attack & Defense Mechanisms (ML Apps): In CAVs, it is expected that ML algorithms and applications will be utilized. These ML applications can also be extended to security and cyberattack estimations as well. However, against all these advantages, ML algorithms have a vulnerable phase, where data is collected, trained, and predicted. In these phases, there are different kinds of attacks that can be performed by an adversary. These attacks can be on the data, which is referred as data poisoning attacks [25]. Another attack can be performed on the ML library [26], and various other types of attacks.

To prevent an attack on ML systems, various methodologies such as differential privacy [27], algorithm robustness improvement, homomorphic encryption, and data sanitization [28] are proposed. It is important to implement these methodologies in ML-based systems to prevent vulnerabilities against cyberattacks. Lastly, black-box access to ML applications can prevent attacks as well.

8) Attack & Defense Mechanisms (Entertainment System): In CAVs, there are numerous third-party services. These services employ telediagnosis, entertainment, and remote software update. All these features and services create another point of failure. These services may be exploited to gain client-level access by utilizing malicious codes or phishing attacks.

To prevent CAVs from such attacks and point of failures, content filters can be employed. Moreover, virtualization could be a good alternative as well. It is worth noting that virtualization technologies can be employed both for hardware and software. Furthermore, supporting block-box access to these services may also prevent attacks if integrity and authentication checks are properly done.

B. Inter-Vehicle Security Issues in the Use Cases

In this section, we will be analyzing the inter-vehicle technologies, attack surfaces, and defense mechanisms. Inter-vehicle security is referred to as any communication of CAVs with the outer world.

1) Attack & Defense Mechanisms (V2V Communication): V2V communication is responsible for the communication among CAVs, where data is shared among the CAVs to provide more reliable data, safer travel, and better autonomous processes. To prevent unwanted access, eavesdropping, DoS, and any attacks related to Internet and Network security, the protocols must properly be designed.

As we all know, standard Internet Protocol allows limited support for cybersecurity, with the exception of IP-Sec. However, due to feasibility issues, it is not used in commercial network systems. This cannot be allowed in V2V communication protocols, and V2V networks since V2V applications are human-life critical. Therefore, it is important that the integrity, encryption, and authentication must be performed carefully for V2V networks and communication.

2) Attack & Defense Mechanisms (V2I Communication): V2I communication is referred to any communication between a CAV and any infrastructure but not with any other vehicle or CAV. To provide autonomous features, CAVs have to communicate and interact with the outer world, for example, with the smart city infrastructures, to provide better efficiency. To prevent unwanted access, eavesdropping, DoS, and any attacks related to the Internet and Network security, the protocols must properly be employed for V2I, like mentioned in Section

III-B1. Since we are speaking of a network, it is a must to employ integrity, encryption, and authentication checks in a safe-proven way. If not, human life could be put in danger. The prevention methods for V2I networks and protocols are very similar to V2I network defense techniques as mentioned in Section III-B1.

IV. Challenges And Future Problems

Despite the fact that there are partial solutions to the existing problems, several above-mentioned problems are left to open. Currently, there are several CAV security problems which need a solution in the future such as spectrum sharing, interference, proof of security issues, malware, trust levels and so on.

V. Conclusion

In the 21st century, connected vehicle technologies have become frequently seen. Utilizing these technologies have several benefits, including an increase in fuel efficiency, time efficiency, cost efficiency, traffic management efficiency, and a decrease in the delays of the vehicle travels. On the other hand, there are also some disadvantages of using connected vehicles. The software systems of the connected vehicles are constantly connected with the Internet, roads, other vehicles, and infrastructures. Furthermore, these connected vehicles constantly produce a huge amount of data (25 GBs/h) and send this data to the cloud environment. In this massive communication and data transaction environment, some CAV-related security attacks such as eavesdropping attacks and denial of service (DOS) attacks are highly likely to happen. From this paper, besides these pros and cons , we have learned the CAV communication technologies such as vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V); connected vehicle use cases such as prediction depended on car maintenance systems, usage-based insurance systems, and driver-assistance systems; some CAV attack surface types such as LIDAR, RADAR, Bluetooth, and GPS; some CAV-related cyberattack types such as denial of service (DOS) attacks, eavesdropping attacks, routing attacks; and some CAV-related defense mechanism types such as authentication checks, integrity checks, and Black-Box modeling. Moreover, we have learned the core systems of the connected vehicles, such as Telematics Box (T-BOX), and electronic control units (ECU). The knowledge that we learned in the class about the attack types such as eavesdropping attacks, routing attacks, spoofing attacks, and denial of service (DOS) attacks; and about the defense mechanism types such as integrity checks, authenticity checks, and authentication checks helped us with the understanding of the project topic. The hardest part of the project was understanding how the attacks are done on the connected vehicle components and how the defense mechanisms against these attacks are applied. Currently, there are some defense mechanisms that are applied against the discovered cyberattacks. In the future, with the rapid development trend of the connected vehicles, we think that the vulnerabilities of the connected vehicle systems, and thus the connected vehicle attacks, will decrease. Moreover, we think that connected vehicles will provide safer and faster travel and become the normal transportation method in the future.

References

[1] N. Lu *et al.*, "Conn. vehic.: Sol. and chal." *IEEE Internet of Things Jour.*, vol. 1, no. 4, pp. 289–299, 2014.

[2] M. Hebert *et al.*, *Intel. Unmanned Ground Vehic.: Auto. Nav. Res. at Carnegie Mellon*, M. Hebert, Ed. KluwerAcademic Pub., June 1997.

[3] A. Nanda *et al.*, "Internet of auto. vehic. commun. sec.: Overview, issues, and dir." *IEEE Wireless Communications*, vol. 26, no. 4, pp. 60–65, 2019.

[4] X. Sun *et al.*, "A surv. on cyber-sec. of conn. and auto. vehic. (cavs)," *IEEE Transac. on Intel. Trans. Sys.*, pp. 1–20, 2021.

[5] C. Miller and C. Valasek, "Hackers remotely kill a jeep on the hghway," *www.wired.com*, 2015.

[6] K. Zhao and L. Ge, "A survey on the internet of things sec." *2013 Ninth Inter. Conf. on Comp. Intel. and Se.*, pp. 663–667, 2013.

[7] S. Ravi *et al.*, "Sec. in embedded sys.: Design chal." *ACM Trans. Embedded Comp. Sys.*, vol. 3, pp. 461–491, 08 2004.

[8] I. E. Carvajal-Roca and J. Wang, "A semi-decentralized sec. framework for conn. and auto. vehic." in *2021 IEEE 94th Vehic. Tech. Conf. (VTC2021-Fall)*, 2021, pp. 1–6.

[9] Y. Xun *et al.*, "An experimental study towards the in-vehicle net. of intel. and conn. vehic." in *2018 IEEE Glob. Commun. Conf. (GLOBECOM)*, 2018, pp. 1–6.

[10] C. SVESS, "Sae j3061-cybersec. guidebook for cyber-physical automotive sys." *SAE-Society of Automotive Engineers*, vol. 3, 2016.

[11] A. Ashwini, "Conn. car practical use cases," *www.medium.com*, Mar. 2018.

[12] R. Prytz, "Machine learning methods for vehic. predictive maint. using off-board and on-board data," *Halmstad Univ. Press*, 9 2014.

[13] C. Rani *et al.*, "Sec. of unmanned aerial vehic. systems against cyber-phys. attacks," *The Jour. of Def. Model. and Sim.: App., Meth., Tech.*, vol. 13, 11 2015.

[14] Y. Liu *et al.*, "Impact assess. of GNSS spoofing attacks on INS/GNSS integrated nav. sys." *Sensors*, vol. 18, p. 1433, 05 2018.

[15] A. Kalantari and E. Larsson, "Stat. test for GNSS spoofing attack det. by using mult. receiver on a rigid body," *EURASIP Jour. on Adv. in Sig. Proc.*, vol. 2020, 02 2020.

[16] H. Tao *et al.*, "GNSS spoofing det. based on consist. check of vel." *Chinese Jour. of Elec.*, vol. 28, pp. 437–444, 03 2019.

[17] S. Jeong *et al.*, "CUSUM-based GNSS spoofing det. meth. for users of GNSS aug. sys." *Inter. Jour. of Aeronautical and Space Sci.*, vol. 21, 04 2020.

[18] M. Bozdal *et al.*, "A survey on CAN bus protocol: Attacks, chal., and poten. sol." *2018 Inter. Conf. on Comp., Elec. Commun. Eng. (iCCECE)*, pp. 201–205, 2018.

[19] A. Palanca *et al.*, "A stealth, sel., link-layer denial-of-service attack against automotive net." *Inter. Conf. on Det. of Intrusions and Malware, and Vul. Assess.*, pp. 185–206, 06 2017.

[20] B. Groza *et al.*, "Highly eff. auth. for can by identifier reallocation with ordered CMACs," *IEEE Trans. on Vehic. Tech.*, vol. 69, no. 6, pp. 6129–6140, 2020.

[21] B. Palaniswamy *et al.*, "An eff. auth. scheme for intra-vehic. cont. area net." *IEEE Trans. on Inf. Forensics and Sec.*, vol. 15, pp. 3107–3122, 2020.

[22] M. Dibaei *et al.*, "Attacks and defences on intel. conn. vehic.: a survey," *Dig. Commun. and Net.*, vol. 6, 5 2020.

[23] R. Brooks *et al.*, "Automobile sec. concerns," *Vehic. Tech. Mag., IEEE*, vol. 4, pp. 52 – 64, 07 2009.

[24] M. S. U. Alam *et al.*, "Sec. vehicle ecu commun. and stored data," *ICC 2019 - 2019 IEEE Inter. Conf. on Commun. (ICC)*, pp. 1–6, 2019.

[25] N. Baracaldo *et al.*, "Det. poisoning attacks on mach. learn. in iot env." *2018 IEEE Inter. Cong. on Inter. of Things (ICIOT)*, pp. 57–64, 2018.

[26] N. Papernot *et al.*, "Semi-supervised know. trans. for deep learn. from priv. train. data," 2016. [Online]. Available: https://arxiv.org/abs/1610.05755

[27] K. Mivule *et al.*, "Towards a diff. priv. and utility preserving mach. learn. class." *Procedia Comp. Sci.*, vol. 12, p. 176–181, 11 2012.

[28] P. Chan *et al.*, "Data sanitization against adversarial label contamin. based on data complex." *Inter. Jour. of Mach. Learn. and Cybernetics*, vol. 9, 06 2018.