Adaptive Cybersecurity Measures for Autonomous Vehicle Communication Networks

By Dr. Eric Verschueren

Professor of Electrical Engineering, Ghent University, Belgium

1. Introduction

[1] A CAV (Connected Autonomous Vehicle) is a representative of the intelligent vehicle in the era, integrating vehicle electronics, V2x (Vehicle to Everything) communication, and artificial intelligence. According to the sensor data, vehicle state data and vehicle control commands, V2x communication, and system, subsystem and component characteristics and limitations, the network security detection, response and repair optimization in the adaptive cybersecurity defense of CAV are described. This work connected uplink intrusion detection and response in the CAV network from the broad aspects of detection technology, recognition and isolation of intrusion source, response and repair time optimization. The purpose of this work is to study the adaptive network security defense of CAV from the aspects of off-vehicle and on-vehicle human-machine interfaces.[2] The core of the CAV is to automatically connect vehicles with each other and various living and working objects through wireless communication technology, and use perception technology to realize environmental perception with various on-board sensors. The adaptive cybersecurity defense method and system based on V2x communication network is designed. When the vehicle detects abnormal network traffic and single-element performance state data, generates an alert and reports to the IDaaS(N) system as attack or fault source information, the IDaaS(N) system sends judgment and defense command to the V2x communication network elements and network drivers for the detection and response tool VNS countermeasures, the VNS countermeasures modify the driver of network elements as needed, reconfigure network topologies, and isolate the intrusion; when the abnormal network traffic continues for a certain time period, the adaptive cybersecurity defense system generates an intrusion report, alarm and response command for the human–machine interface, and judges the probability.

1.1. Background and Significance

[3] The automotive industry is currently undergoing a digital transformation. Mobility services and autonomous driving are only two examples that are impacting the traditional role of automotive manufacturers. In addition, the increasing digitalization and IT-like environments of vehicles require new vehicle architectures. And the convergence of applications of have an impact on the vehicle real-time system. Increasing connectivity of vehicles on the other hand leads to a huge attack surface as we trust everything is connected which will not necessarily be the case. Additional to the pure cyber attacks, the vehicle is impactable of being exposed to physical attacks. With this new environment it is essential to focus on automotive cybersecurity as Automotive is becoming Smart Mobility. In this work we will focus on in-vehicle network and will not concentrate on the ODD itself. Therefore, MindTrack is not part of our research in terms of indirect consequences of autonomous driving vehicles on automotive cybersecurity have therefore been neglected in this article, too.[4] Recent modern autonomous vehicles not only share road with each other, but also share road and infrastructure information to enhance safety, traffic efficiency, and reduce frustration via wireless communication. How to provide secure and safety vehicular recreation and highway system becomes a very crucial social public requirement. Wireless communications enable remote physical attacks like wireless jamming and applications run on communication devices introduce security threats such as cyber-attacks. Cyber-attacks in autonomous vehicles can lead to catastrophic threats. For increasing traffic efficiency, physical and digital shared-road information is becoming very popular. CAVs need to share map, signal phase, distance to signal and intersection status over time to know others' maneuver, get suggestion in case of human-driven vehicles, and take decision in a phase-based adaptive–cruise lifecycle, respectively in context to CAVs-to-signal and CAVs-to-signal and signal-to-CAVs. Rise of these applications increase exposure of cyber-threats both in road traffic and traffic lights and emergency preemption system controls. This work considers vehicular ad-hoc network and park highway system with mobility models from real open sources data. We vary the network densities to represent rural to urban road.

1.2. Research Objectives

[5] Autonomous vehicles employ numerous electronic control units (ECUs) within a network to manage their functions. However, this makes it more vulnerable to hacking or exploiting such trust by, for example, using a rogue ECU for spear phishing.[Link] These can impact not just privacy, but physical harm too. Notably, in 2015, two white hat hackers successfully

controlled a Jeep Cherokee remotely through the Internet, leaving the driver helpless. Hence, hacker's malicious control on the vehicle would result in loss of tens of thousands of aviation fatalities that's why it is the most harrowing of all cyber- physical system security challenges. Indeed, It takes out driver's control of strategic systems responsible for perception, planning and control, and works as a physical weapon. Consequently, the attacker can cause physical harm to many occupants, and/or suffer financially [6].ftse.qut.edu.au/wp-content/uploads/sites/26/08R-1835_M_Mougoue_African-Human-Robot-Interaction.pdf[7] To exploit the issue, an attacker uses the network to send a form of message containing some corrupt file or command. Once the attacked ECU opens the message, it triggers the corrupt files or command to the point of crashing the ECU. The dangerous outcome is either the vehicle spontaneously stops suddenly, or it becomes incapable of detecting ot detecting having error messages, perilous situations. The attacker will send another message to the ECU that was vulnerable to the attack or corrected automatically after the crash to instruct it to create more traffic using the message to move on like nothings happen.The attacker undertakes traffic jam operations under the corrupt message production instruction, and the rest of the vehicle expose fake news messages, and each vehicle can produce it. Similarly, the rest of the vehicle will send out redundant fake traffic jam messages and appear silent. In contrast, the ECU on the road side can produce fake traffic jam messages like vehicles on the road side in the road.

1.3. Scope and Limitations

The cybersecurity of AVs and their communication networks has attracted especially high attention when autonomous deterrence is included in the communication systems. We discovered that this deterrence should provide three main attributes: integrity, authenticity, and confidentiality. Subsequent to the effects of different cyber-attacks on these attributes through the degradation of the security of the CAN and LoRa systems, we also identified the different types of cyber-attacks and predicted that developing access control along with the use of encryption would be effective in providing data security [8].

Compared to traditional automotive systems, where testing and simulation have been identified as the main approaches to validate and verify new functionality [9], AV systems additionally incorporate aspects related to computer science while adding sensors from varying vendors and mechanisms for interconnected activation on a broader scale. While

these cannot be extensively examined at multiple levels, such as software, hardware, and communication, in use-case test drives and real-life scenarios, advanced testing models are necessary to account for the complexity. It is also important to research the issue of security in communication networks, especially with the increased use of these systems in challenging traffic situations [10].

2. Autonomous Vehicle Communication Networks

During the beginning of contemporary vehicular networks, its communication component examination was perceived as intertwined and weakly-designed thoughts. So, the analyst and the operators have set rigorous safety constraints in all levels of the network as vehicular grids are considered critical for technical infrastructure documents and the systems to which they are related [11]. The enhancement of the security catalogue for vehicular networks needs a consideration of real information technologies, legal, cyber-forensic, and cyber-crime issues, thus the involved technical, financial problems, and consumer rights should be integrated in campaign planning and the computation boost. The vehicular networks have now evolved to present us with new prospects like the requirement for alternative modes such as the rail roads, pipeline networks, airspace, and IoT channels. The vehicular grids are presumably capable of yielding more vehicular optimisations and innovations such as tolerance against natural contingencies, formations according to the presence, limitations on several technical, cyber-forgiving, and recovery procedures.

Vehicular communication networks (VANETs) is a dynamic area of research for the intelligent transportation system (ITS). While several key challenges have been addressed in this field such as safety, precise navigation, environmental impact, and on-board infotainment services providing higher comfort levels, the area of cybersecurity is often neglected [12]. Holding interconnected and vehicular links throughout could introduce several severe risks to the travel system. The risk includes the distribution unwelcome adware and adware in addition to concentrating on the theft of significant personal details, which probably disrupts the entire V2V and V2I framework. Consequently, the evaluation of safe connections in the vehicular ad-hoc grids will gain together broadcast and on-board systems for both present and upcoming self-driven automobiles. We cover present instances of eavesdropping, hits of fake information, and dissent-deterring techniques, cryptography sketches, reliability

applications, Digital Personal Helpers (DPNs), and bottom-up and top-down descriptions in this periodical.

2.1. Overview of Autonomous Vehicles

Over the last few decades, the secure communication between a few on-road vehicles and roadside infrastructure was based on transponder/obu with a dedicated short-range communications interface, such as ATSC and DSRC. Oftentimes, this vehicle arrangement is called the electronic toll collection, dedicated short-range communications (ETC-DSRC). For these requests, the transponder sends a predetermined signed cryptogram in response. Hence, in this approach, if a transponder cryptogram can be accessed away from the legit vehicle, then it might be abused to do various frauds. So, a more sophisticated vehicle-to-infrastructure security is designed based on the attribute-based public key cryptosystem in this case and some additional frequent secure as possible distance statistics are used to further prevent misuse of this kind.

An autonomous vehicle (AV), also known as a driverless or self-driving vehicle, has the capability to navigate and implement multiple functions typically associated with human driving. According to widely accepted levels of driving automation [13], the discussed levels range from having no automation capability (level 0) to full automation capability, with no human involvement (level 5). Such advanced communications, computing, and control systems can offer numerous advantages in terms of enhanced safety, energy efficiency, driving comfort, and convenience. Some of these capabilities involve the use of onboard sensors, local situational awareness, data management as well as vital intervehicle and road–infrastructure communications. Currently, an AV relies significantly on cloud-connected, high-speed, ratified, and 4G/5G-based reliable communications with the other surrounding vehicles, of roadside infrastructure, and of mobility services (e.g., eCall-based accident notification, dynamic route guidance, OTA updates). All these communication-based services are grouped into three main categories, (1) vehicle-to-everything (V2X) and vehicle-to-infrastructure (V2I) communications, collectively known as I2X communication, (2) point-to-point (P2P) communication, and (3) vehicle internal communication (INCOM) [6]. INCOM is a highly heterogeneous communication landscape comprising several in-vehicle sub-networks supporting infotainment, safety, performance, energy management and so on. Most of the data are confidential at least whereas other can involve safety-critical control messages-

propagating over digital communication media like Controller Area Network (CAN) buses [12].

2.2. Communication Protocols and Technologies

Vehicular network communications and control systems have developed to ensure safe and efficient operation of vehicles and driving for the passengers. Because of their potential to advocate high mobility, high traffic, the limited short-term horizon of data, and the imperative need for safe operations, vagaries of these systems may result in serious safety problems for V2X systems. The communication of the vehicles and external support is vulnerable owing to different attacks over this communication link, including jamming attacks on the RF communication channel, node capture, and DOS attacks This is why secure reliability solution studies have typically concentrated on real-time operations and detection of attackers to supply safe and correct timely input to the driving function.

Vehicular networks rely on multi-technology and can connect vehicles (i.e. in-vehicle networks, IVNs) and vehicles to external entities (i.e. vehicle-to-everything, V2X) [12]. Generally, four types of multi-technologies are used in vehicular networks, such as: (i) vehicle-to-vehicle (V2V) communications, which can support direct wireless connections between vehicles, (ii) vehicle-to-infrastructure (V2I) communications, which can connect vehicles with the road side units, (iii) vehicle-to-nomadic device (V2N) communications, which can connect vehicles with mobile stations or personal digital assistants, and (iv) vehicle-to-internet (V2I+) communications, which can connect vehicles with the internet except for vehicle's nomadic devices, the road infrastructure, and other vehicles [14]. The basis protocols of V2X communications include various technologies, such as IEEE 802.11brp, IEEE 802.11p, LTE-V2X, 4G-V2X, 5G-CV2X [372,373] and 6G-V2X. For V2X, security and privacy are more crucial [2].

2.3. Vulnerabilities and Threats

As demonstrated by Ghimire, et al. [15], some attacks a malicious party can launch against AVs are: backdoor attacks altering vehicular communications, which could result in physical accidents; penetration testing using specific hardware tools to connect to the internal network of the car; and the exploitation of weaknesses in the software of the AVs. These attacks involve numerous mechanisms that can violate the reliability, privacy, and safety properties we found

in related to the computation, communication, and the operation of the cars. If a vehicle can communicate and react autonomously to triggers managed by a remote command and control server, it will expose itself to threats as if it were a static infrastructure component [16].

Vehicular ad-hoc networks (VANETs) are fundamental to intelligent transportation systems, enabling vehicles to communicate with one another and with the infrastructure. However, VANETs are exposed to various attacks, like eavesdropping, impersonation, and attacks from non-authentic nodes. Therefore, to facilitate secure VANETs, an authentication system is required to protect them and enable legitimate nodes to communicate with each other, thus allowing the security and safety of the whole vehicular communication mechanism [17].

3. Cybersecurity Fundamentals

Cybersecurity of autonomous vehicle (AV) systems has recently gained significant attention, due to the rising demand for intelligent transportation systems and the ever-increasing number of cyber threats. (ref: e8630618-9e11-48f1-8edb-293061b3203e) In line with this, the use of the autosar (automotive open system architecture) standard is recommended as well, placing strong emphasis on the employment of secure software systems. The key-points associated with the discussion have been categorized in four categories: (i) the comparison of AV cybersecurity measures of the automotive industry; (ii) the employment of the multi-layer model to elevate security of AVs to a novel level; (iii) the external/internal cyber threats that are magnifying the vulnerability position of AVs; and (iv) a range of cybersecurity measures that can be employed to rebuild and improve the security maturity of AVs. In the analysis that follows, the cybersecurity measures that are capable of elevating the position of AVs in the face of a range of devastating cyber threats are discussed in the context of the employment of the multi-layer model. A variety of key-points associated with cybersecurity of AV systems has been examined, with the aim of repositioning them from their current poor security maturity to another level, where the security maturity of AVs would be remarkably boosted.

Autonomous vehicles (AVs) have gained notable popularity owing to their significant ability to improve mobility, reduce accidents, and enhance fuel efficiency. (ref: a9265296-08fb-4fa8-a304-6a9d12beea7b) However, as AVs are typically employed in open and interconnected cyber-physical systems, they are indeed exposed to a variety of cybersecurity threats. The exposure of AVs to cybersecurity risks is due to their employment of wireless communication to interact with other entities on the road and infrastructure around them. The automotive

industry suggests the employment of a multi-layer cybersecurity model for AVs to lower cybersecurity risks. The primary layer of the cyber-related security measures for AVs is named the perimeter security layer. Actually, in this layer, client/server authentication and data verification would be undertaken using cryptographic algorithms and blockchain technologies, respectively. Furthermore, the proper design and implementation of secure wireless communication systems and also the development and application of secure wireless communication protocols play significant roles in strengthening the cyber-related security position of AVs. In next layer, which is recognized as an internal network security layer, a variety of cybersecurity measures are required to be applied to enhance the security maturity of the IVN of AVs. Moreover, public-key infrastructure and firewall technologies are typically used in the third layer of the multi-layer cybersecurity framework to elevate the security of cloud-based data storage facilities. This requires the suitable design and implementation of intrusion detection and geographical-based access control systems (basically for real-time cyber threat response) in the fourth layer of the multi-layer cybersecurity framework.

3.1. Key Concepts and Definitions

Self-driving vehicles (SDVs) or fully autonomous vehicles (AVs) are equipped with advanced sensors, cameras, radar and lidar, GPS-based systems, data-communication units, and computer units such as embedded systems and control units for executing specific tasks. External data communication over a wireless network is crucial for many self-driving-car subtasks. For example, this allows cars to connect to cloud platforms, access software repositories, exchange vehicle data with other cars for the purpose of making safety and traffic optimization decisions, and exchange data with infrastructure environments for guidance, traffic-lights control, and surveillance. All of these have become important components of operational solutions based on different levels of autonomous driving. Therefore, in self-driving cars, the problems of cybersecurity or attacks/governance impact self-driving cars in many dimensions and at varying levels of autonomy [18]. An increasing number of original research papers and review and survey papers have been published that discuss various aspects of self-driving cars, vehicular ad hoc networks, security, their problems, and potential solutions. This creates a need to systematically classify the main aspects of the problem of autonomous vehicles and their security and then capture them into one place.

The effort to maintain security in the communication network of vehicles implies a set of strategies and techniques for monitoring vehicle-behavior, identifying deviation from the normal behavior, and protecting the data and information across the network from unauthorized and nefarious behavior [7]. Different cryptographic methods and diversity-based techniques are proposed for protecting communications over the VANET at different OSI layers. Network-based attacks have been addressed through intrusion detections, as they are identified in different layers of VANET communication stacks [12]. The existing or proposed solutions typically include methods and approaches that require a change in the security infrastructure of the VANET, incur communication overhead, and involve some management complexity. This is due in part to VANET security and the centralization of servers. There has been an effort to secure the existing infrastructure and data. The main idea is to limit the applications that are available to access data; the only access request allowed is from a vehicle or infrastructure. Any access that comes from a user cannot be trusted and is considered inauthentic.

3.2. Threat Modeling and Risk Assessment

To guarantee secure communication among processing systems (ECUs) on IVNs, extensive research is initially being carried at utilizing software, sound design, and process evaluation on diverse inertial models. This letter explains why it cannot be effectively protected by present techniques based on the spectrum model and presents a Multi-Layer Security Structure (MLSS) model for automotive data applications. This model primarily includes data alternate and safety monitoring approaches with data travel and interfaces [1]. This article offers surge-implants encryption, cover-generated based alternative, and Amanda as alternative options. The complete composition and function of the automotive utility pilot scheme developed in this data abstract will also be defined.

The in-vehicle communication of autonomous vehicles has become a critical security concern due to the increasing level of vehicle automation [5]. In-vehicle communication systems mainly consist of in-vehicle networks (IVNs). The present traffic control systems regulate vehicle movement with the help of prescribed rules and regulations through traffic lights, zebra crossing, etc. [12]. With the inclusion of automation, their role is gradually fading. Intelligent Traffic Control System (ITCS) and Internet of Vehicles (IoV) have been developed to have a more useful and comfortable environment. IoV has numerous applications including

traffic control systems, autonomous vehicles and project safety measures, and environmental protection.

4. Adaptive Cybersecurity Approaches

Dynamic cybersecurity prevention is based on the rapid intervention of anomalies and cyberattacks at the beginning of the residence time, e.g. before their establishment. Indeed, limiting the effects of potential cyberattacks and protecting in-vehicle ECUs as quickly as possible in addition to their detection, once established, is mandatory for autonomous vehicles [19]. As a result, an embedded cybersecurity cooperation protocol will be necessary to encourage a natural response to the existence of cyberattacks and anomalies. The presented solution aims to quickly build a secure residence with all the neighboring 'trustful' ECUs and drastically reduce the propagation of cyberattacks. When the cooperative and active-responding (demand) of parameters to potential cyberattacks are reached, then the DDoS, network, and physical layers of the in-vehicles should be secured from the starting times of the attacks.

Cybersecurity attacks on individual in-vehicle Electronic Control Units (ECUs) can pose threats to the safety of non-managed vehicles' point-to-point communication in the future. As the ECU's bandwidth reaches its capacity limit and/or the network becomes crowded, communication between the various in-vehicle Electronic Control Units (ECUs) can encounter challenges. These problems could potentially be due to various reasons, where cybersecurity attacks and anomalous behaviors are only a few examples [20]. Although the integrity and availability of communications between the wireless vehicular network and smart infrastructure or other vehicular networks in the mentioned situation may depend on cybersecurity in-vehicle networks, these issues are not directly addressed in this domain so far. Thus, it will be necessary to develop a dynamic cybersecurity solution in relation to having congestion problems in in-vehicle communications between the lean and smart devices.

4.1. Machine Learning and AI in Cybersecurity

To ensure the security of the Internet of Vehicles (IoV), many scholars have proposed a lot of methods. The first feasible idea for the security and privacy of IoV was based on the applied support vector machine (SVM) and multilayer perception (MLP) in order to classify the traffic which is taking into queue and decides the domain Name system (DNS) traffic and IoT traffic

of an heterogeneous vehicular network. The most effective methods for this proposition are models presented from the classical clustering and classification techniques as well as novel communication methods. Training through network-based artificial neural systems itinerary and HMAC analysis techniques were used for ensuring the security in the drone communication system. In order to compliance with privacy and security requirements and to optimize predictive data mining efficiency in autonomous driving applications, an edge-based online learning system was placed under the control of an intelligent SVM scheme using reinforcement learning and executed by means of an adaptive deep learning-based agrevate learning agents.

The machine learning and artificial intelligence

[2] [15] Autonomous vehicles' reliance on external networks results in complex and new security issues in the connected autonomous vehicle (CAVs) communication networks. The spread of COVID-19 has emphasized the importance of autonomous vehicles, as they provide safer transportation by reducing human interactions. The adoption and development of autonomous vehicles are expected to accelerate in the post COVID-19 era. Despite many advantages, CAVs have some issues like connectivity, safety, and the price of the autonomous vehicles. To reduce the collision and fatalities probability of accidents, the implementing of vehicular networks connected to vehicle (V2V) and infrastructure (V2I) communication technologies and Automated Driver Assistance Systems (ADAS) made some subexchangesal step in the development of CAVs. However, different cyber or physical attacks harm the communication between vehicles and infrastructure. The violation of safety critical communication, which cyber or physical attacks are allowed for occurrence, may lead accidents that has fatal results for human health and human disabilities. Therefore, to provide security for CAVs, some changes must be occurred in the traditional security processes. The traditional conclusion of the digital signatures, message authentication code (MAC) and countermeasures is very fast and makes changes for cyber and physical attacks. The conclusion trying to find a function for traditional cyber and physical attacks are shown in the artificial intelligence solutions which make updates itself against attacked and make makes more difficult to the attacker about determining its target.

4.2. Dynamic Threat Detection and Response

Least of all the enormous potential of the connected vehicles for future smart mobility if their protection against adversarial attacks can not be adequately ensured. Here, the properties of connected and fully-automated vehicles themselves and the associated vehicles communication network, which is composed of a large number of individual interconnected ECUs and is therefore also known as an individual ECU, can be hindered by other components individually. Therefore, for the purposes of timely responding to detected security vulnerabilities on the individual ECU, it would make sense to use a Threat Detection & Response (TDR) functionality [21]. This should not only be able to identify and categorize security vulnerabilities but also to implement appropriate countermeasures autonomously or provide information about the need for manual intervention by the End User.

To provide protection against dynamically evolving threats, measures have to be in place to detect security vulnerabilities and respond proactively [22]. This motivates the introduction and adoption of dynamic threat detection approaches as well as concrete countermeasures in autonomous vehicle communication networks. A thorough overview of security measures deployed in the automotive industry was presented by Robin Moll (Moll, 2001) [8], and Unger defines intelligent detection and precise response procedures as the crucial features of comprehensive security routines in the automotive industry.

5. Case Studies and Examples

Our second case study is devoted to vehicle applications that also exhibit real-time requirements . Xu and Rudin, in (Xu and Rudin, 2021) discussed the issue of truth discovery in autonomous vehicles (AV) having the ability to communicate via vehicle-to-everything (V2X) communication. AVs operating in V2X environments collect information from multiple sources, such as V2I, V2V, and V2P, in order to make the necessary navigational decisions and also equipped with sensors like LiDAR or camera hardware can measure the location and its environment. The authors indeed discuss how the communication process becomes a crucial part of the broader decision-making process in the new AV ecosystem. They argue that communication sourcing, not the only accuracy but also the sender's intent and truthfulness change based on the sender's privacy preferences, and the time it takes to gather the data are crucial to make correct decisions about the sender's intent. They therefore proposed the Efficient and Privacy-Preservation Truth Discovery (EPPTD) method and compared it with the existing methods. EPPTD leverages reputation, credibility, and privacy feedback

mechanisms orchestrated in order to efficiently and accurately discover the truth and reduce the privacy-preserving constraints in a lessinvasive and infallible fashion. Their extensive experimental evaluations over two real, large-scale datasets demonstrate that EPPTD achieves lower root mean square errors (RMSE) with up to 39.69% improvement.

Our first case study involves the security of autonomous drones. In a study that Schlachter and Bremer published in (Schlachter and Bremer, 2021), they investigated the security of autonomous drones. They thoroughly tested and compared three contemporary real-time operating systems (RTOS) for their feasibility in drone systems with real-time security requirements. The authors demonstrated a concept and an implementation for continuously monitoring and periodically determining the safety state of the drone during its operation. This ensures safe actions if an attacker is able to inject faults. They compared the implementation complexity of the concept for all RTOSs and showed a detailed comparison of code size, execution time, worst-case stack usage, worst-case execution times, and energy consumption. They further discussed the implications of the results regarding autonomous vehicles in general. One can think about drones, with their proprietary standards, as the first generation of autonomous vehicles. These can be used for investigating the safety properties and pros of transportation technologies without being bound to realworld restrictions like street-legal vehicles.

In Section 4, we discussed security requirements, challenges, and attacks in autonomous vehicles [2]. In this section, we illustrate security mechanisms through case studies. We also present some examples and discuss potential future research directions for vehicle security research.

5.1. Real-world Attacks on Autonomous Vehicles

The systemic vulnerabilities present in the current controllers, processors, sensors, actuators, and communication networks enable potential cyber attacks on the AV [23]. Cyber-physical attacks on sensing perception can render the AV system blind during the critical time of operation, therefore resulting in the vehicle deviating from its expected trajectory and causing accidents. Disruptive attacks on data distribution, caused either by communication network disturbances or by data manipulations, can potentially results in formation of wrong conclusions, a wrong robotic reasoning and, eventually, incorrect actions [10]. M. T. Vo and W. Elmenreich [15] discussed common cyber-attacks and exploits on autonomous vehicles

manually or by use of simulated instances like Car2X-environment-based V2V, V2P, or V2I communication. Security is an oft-neglected aspect of autonomous vehicle research, but it is an area receiving an increasing amount of attention. While surveys of vulnerabilities present in the software of modern cars are available through prior art, and software to exploit such vulnerabilities often are publicly available, the security-related challenges are rarely mentioned in the detailed requirements for autonomous vehicles. Nevertheless, autonomous vehicles need to be robust against a variety of potential attacks and be prepared to react robustly if an attack would succeed despite its defensive measures.

6. Regulatory and Ethical Considerations

This is particularly relevant for AVs, since they will also have to be navigable without Internet access and rapid response times will be crucial. Therefore, the adaptiveness of cybersecurity measures implemented in AVs will be an even more restricting factor. Moreover, the collection, storage and analysis of large amounts of sensitive data comprising personal and environmental information in the context of autonomous vehicles raise significant concerns. The trade-offs between anonymization and identifiability will be particularly difficult. The integration of cryptographic measures for data encrypting and handling of personally identifiable information into the adaptive cybersecurity measures of AVs could thus be crucial. There are multiple value-laden trade-offs between privacy and security that will need to be considered. We have our doubts as to whether it is possible, ethically, to provide full access to all V2X services for every stakeholder, under any circumstances without any form of discrimination. Mechanisms of access control should be taken into consideration regarding the provisioning of V2X services, because it raises issues of digital security justice to consider digital inequalities. A flat approach treating all requests from entities for certain resources in the same manner will instead buttress existing inequalities in society. The essence of the ethics of digital security has not been thoroughly discussed—we intend to introduce the importance of security as a requirement within the discourse of justice [ref: article_id 70320a48-476a-4891-ad51-a6ab72943242].

During our review of the literature and the current state of the art, we focused mainly on machine learning, anomaly detection, and blockchain technology as adaptive cybersecurity measures for V2X communication. However, many other solutions and potential threats have been proposed in the literature and need to be considered. One key aspect we would like to

address is the question of patch management in security-critical vehicular systems. Although we could not identify solutions in the literature aiming specifically at the patch management for autonomous vehicles, we would like to highlight the relevance of the issue and its ethical implications. The discussion of the ethical and regulatory implications of autonomous security-enhancing measures is only just beginning, but it should also be addressed from a research standpoint [ref: article_id 26e2619b-3ab1-4d67-baf2-40c2b2d9869a]. Existing work will also need to be reviewed, focusing on its potential legal, social, and political implications, in addition to its technological relevance. The call for integrated analytical frameworks for governing the Internet of Things and increased emphasis on security we observed in our literature review could also play a role [ref: article_id 39941539-5611-4974-bafd-0e690996fdad].

7. Future Trends and Research Directions

Blockchain technology can find numerous applications in Connected and Autonomous Vehicle (CAV) networks. Blockchain is a leading-edge technology that has shown promising outcomes with decentralized trust-based secure communication, and has the resiliency for counter-future cryptographic threats. Our thoughtful representation of secure adaptive is to E3-automate the whole security interface of the Vehicle based network interconnected system. We evaluated the performance of both decision block and model descriptor based machine learning models (out of 32 architectures variants (of dense, farms and recurrent networks with various hidden layers) with around 70 hyper-parameters) over TIMIT recording dataset scenario for voice, image, voice-over-image and key-stroke environment for all environment that created theft and further distributed 100 cases each to all accuracy distribution for DNN Block based or pre-trained compact classifiers. (e.g., SVM, LDA, GMM, GMM super vector, OMP and k-NN). When the experimental results were evaluated, the overall compact model produced excellent results with an overall accuracy of 92%-95%. Overall, the results of this study suggest reasonable performance of efficient participating server in both noisy and noise-free recording datasets [24]. A comprehensive review of the presented techniques can be found in [7].

The development of autonomous vehicle communication networks has a significant potential for future growth. By 2035, 5G first phase deployments will cover 40% of the world's population to support billions of connected devices, including smart vehicles powered with

enhanced autonomous capabilities [21]. Through these V2X channels, the connected and autonomous vehicles could interact with other vehicles, pedestrians, infrastructure, distant clouds and Digital Twins. However, security remains the key barrier for the wide acceptance and deployment of CAV technology. In addition, cybersecurity is hard to maintain when our networking techologies are advancing with the advent of 5G and MQTT - a publish-subscribe based messaging protocol, when it comes to fault tolerance, called out by the things connected where the vehicles prominently called as moving edge computing nodes. Although innovative connections to the cloud-based cybersecurity systems like VANET-cloud and Digital Twins are shared, their functionalities are not explicitly designed to provide an ex-ante or ex-post protection against the advanced persistent attacks. In future, need of the communication with the clouds, while some ports are still literally open, is resulting in the immediate need for new techniques to protect the network.

7.1. Emerging Technologies in Cybersecurity

The trend of making vehicles more autonomous has created a numerous challenges. The primary among those challenges being the cyber security, which according to Q. Silon et al. is the weakest link in the autonomous era. It is especially the wireless communication medium mobility, OMNeT++ proved that made man-in-middle attack much possible. Intelligent Transport Systems (ITSs) are not new in the automotive world and even revolutionizing the transportation systems by transforming the traditional vehicles into the connected autonomous vehicles (CAV). The purpose of this every vehicle community is to reduce the traffic congestion and increase safety environment for all the road users with the spreading of 5G and V2X technologies. The massive potential inflow of data and traffic is definitely going to increase the size of attack vectors. A classified taxonomy of cyber-physical threats has already been studied in,. Moreover, to improve the entertainment and comfort, the number of eased connectivity will also be adopted in the vehicle system. A connected vehicle is just like a big computer on the move, which is going to contain plenty of personal data, are subject to privacy issue as well. The automotive system has completely different constraints in terms of power, real-time and wireless connectivity. So, while employing some of the security measures taken from the classical computer domain could also deteriorate some operational functionality; for instance, frequent scan and fire-wall program possibly parcel the network severely necessary data. Therefore, the constraints must be placed during the hacking.

[16] [5]With the publication of SAE J3016 a few years ago, the level of research and investment in driverless cars saw an exponential growth. Multiple automotive events over the last decade, especially patents related to autonomous vehicle technology, demonstrate that the trend is here to stay. From 5G to V2X, the vehicle-to-everything technology is continuously getting upgraded. This implies an increasing trend in the interconnectivity and communication technology in the vehicles. The telematic technology has facilitated a considerable amount of data, network and communication traffic to support the convenience and comfort of the driver. However, the technology push may force the deployable autonomous vehicles to operate in a more connected environment than the actual perspective with a connected autonomous vehicle (CAV) perspective desires.

8. Conclusion and Recommendations

The proactive network security intelligence hints to methodological cybersecurity techniques that could be taken into account within development and operation planning. Crucial for that are not just the physical security of the communication channel shunts (arrow in Figure 1) and the involved vehicles themselves but that also includes the required secure software development process with a more detailed classification of the affected surface as well as in-house procedure through proactively and reactively cooperation with potential external attackers. A monitoring and alerting system would enable proactive identification of an insufficiently secured component (something holds true for all device categories from hydraulic shovels, to routers, to injectable insulin pumps) across the affected layers [25].

Although the security technology to narrow these attack surfaces exists, subjects concerned with the conveyance of autonomous vehicle control signals, Internet of Vehicles (IoV) or Vehicle-to-Anything software updates, or merely entertainment content moved to the automobile is risky. These attacks would contemplate the manipulation of the sensorial layers in which the attackers gain distressing control of the vehicle's motion control systems or simply misinform the owners with manipulated navigation instruction. With the release of smartphone apps such as the Android OBD—VAG vehicle diagnostics (Ross-Tech.com LLC, Landshut, Germany), similar to other vehicle data access solutions, the prognosis of maintenance and diversion interventions has been made more accessible [5].

8.1. Summary of Key Findings

This review explored, identified, and analyzed the research papers, which have contributed to security management, in which response and countermeasures, such as the latest systems and security management implemented and evaluations have been reported. This review only included journal/ conference/ workshop articles and diagnostics & imaging papers published in the last 10 years and written in English. The articles were found using PubMed, Scopus, and Google Scholar bibliographic databases, and only the publications matching the specific criteria were included. 1,275 articles were found by this search methodology and the relevant articles were numbered as 1–279. Articles that provided a simple explanation of exiting paper reviews, while the reviews' paper for security establishment, reaction and countermeasures', a systematic mapping study was used as a type of review. The research direction may refer to the cyber-physical mode' printing and industry like the pharmaceutical and aerospace industry, because these companies' information security similar to next generation vehicle of the 21st century. Cybersecurity in this mode ranged from securing business enterprises to securing transportation system. Security functions are vital to securing the TR vehicles from different vehicles attacks, in terms of semantic-based addressing and vehicle reputation.

The rapid advancement in connected and autonomous vehicular systems has transformed conventional vehicular networks into complex cyber-physical systems, also initiating new security issues and vulnerabilities [16]. Comprehensive IDS techniques are essential to enhance vehicular security in potentially non-robust VN environments. Despite some promising goals and challenges, transportation systems' security aspects are not always included in systems' design and development. This study presented a critical review of security and privacy in the growing number of proposed security features and suggested future vehicular security challenges, as well as the possible research directions for overcoming existing and future vehicular security threats and challenges [23].

8.2. Practical Recommendations for Industry

These are the only practical activities we should carry out for vehicles which are equipped with advanced electrical/electronic systems. Japan, South Korea and Germany with is currently the state-of-the-art data and information exchange in vehicle only uses with all types of vehicles. Such a step increases significantly the costs for entire car repair services, where the single setting have to be modified each time car is being serviced. Each separate standard

could be useful for securing one or more protocol level, present, or future cryptographic algorithms, assuming that they will be exposed to attacks during their lifecycle and hacker tactics will evolve.

1) They are capable of performing only a limited number of operations specific for their instance and EV, however customization for software-based solutions can make them versatile. For better communication of each layer of the network a defense-in-depth approach needs to be utilized. The first layer could be protected using ECU software where rapid diagnostic fault detections are implemented. Middle layers could be protected with cryptographic techniques, whereas installation of AI/ML has proven to be proficient for quite various applications. However, applied in the author has come to a conclusion regarding some weaknesses and threats-e.g. in the application of artificial intelligence and/or machine "vital" data/ lines are before the cyber attacks can affect the whole service system of vehicle [3]. Each algorithm should be carefully studied so that the input data themselves would not become exploited during the learning process. The final layer encompasses the artisans whose only task is anomaly detection, therefore, themselves should be monitored, and their booting should be secure. 2) Reliability, latency, and bandwidth are the most important challenges in wireless V2X communication [16]. In order to successfully implement security in the V2X network, we need to ensure that we have a secure interoperable and standardized implementation. It is important to study the market/ technologies that are already applied to cybersecurity, reliable and latency in communication and data exchange in the whole vehicle with attention paid to traditional computer security systems and the effectiveness of proposed solutions. Such technologies answer almost every challenge that the vehicle could face and it leverages the knowledge already gained for wireless communication.

The above-mentioned approaches emphasize some unsolved and unresolved problems. Therefore, here we provide some practical recommendations for industry in order to mitigate these challenges before implementing in new autonomous vehicle communication networks [5].

9. References

1. [1] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
2. [2] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov
3. [3] S. N. Saadatmand, "Finding the ground states of symmetric infinite-dimensional Hamiltonians: explicit constrained optimizations of tensor networks," 2019. [PDF]
4. [4] Y. Baek and S. Shin, "CANon: Lightweight and Practical Cyber-Attack Detection for Automotive Controller Area Networks," 2022. ncbi.nlm.nih.gov
5. [5] R. Singh Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," 2022. ncbi.nlm.nih.gov
6. [6] J. Manuel Lozano Domínguez and T. Jesús Mateo Sanguino, "Review on V2X, I2X, and P2X Communications and Their Applications: A Comprehensive Analysis over Time," 2019. ncbi.nlm.nih.gov
7. [7] D. Haileselassie Hagos and D. B. Rawat, "Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives," 2022. ncbi.nlm.nih.gov
8. [8] V. Linkov, P. Zámečník, D. Havlíčková, and C. W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," 2019. ncbi.nlm.nih.gov
9. Tatineni, Sumanth. "Compliance and Audit Challenges in DevOps: A Security Perspective." *International Research Journal of Modernization in Engineering Technology and Science* 5.10 (2023): 1306-1316.
10. Vemori, Vamsi. "From Tactile Buttons to Digital Orchestration: A Paradigm Shift in Vehicle Control with Smartphone Integration and Smart UI–Unveiling Cybersecurity Vulnerabilities and Fortifying Autonomous Vehicles with Adaptive Learning Intrusion Detection Systems." *African Journal of Artificial Intelligence and Sustainable Development*3.1 (2023): 54-91.
11. Shaik, Mahammad, Leeladhar Gudala, and Ashok Kumar Reddy Sadhu. "Leveraging Artificial Intelligence for Enhanced Identity and Access Management within Zero Trust Security Architectures: A Focus on User Behavior Analytics and Adaptive

Authentication." *Australian Journal of Machine Learning Research & Applications* 3.2 (2023): 1-31.

12. Tatineni, Sumanth. "Security and Compliance in Parallel Computing Cloud Services." *International Journal of Science and Research (IJSR)* 12.10 (2023): 972-1977.
13. [13] S. Dolev, Łukasz Krzywiecki, N. Panwar, and M. Segal, "Vehicle Authentication via Monolithically Certified Public Key and Attributes," 2015. [PDF]
14. [14] S. Ali Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki et al., "Towards a Machine Learning Driven Trust Management Heuristic for the Internet of Vehicles," 2023. ncbi.nlm.nih.gov
15. [15] A. Dinesh Kumar, K. Naga Renu Chebrolu, V. R, and S. KP, "A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities," 2018. [PDF]
16. [16] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
17. [17] S. Bharati, P. Podder, M. Rubaiyat Hossain Mondal, and M. Robiul Alam Robel, "Threats and Countermeasures of Cyber Security in Direct and Remote Vehicle Communication Systems," 2020. [PDF]
18. [18] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]
19. [19] M. Hamad, A. Finkenzeller, M. Kühr, A. Roberts et al., "REACT: Autonomous Intrusion Response System for Intelligent Vehicles," 2024. [PDF]
20. [20] S. Park and J. Y. Choi, "Hierarchical Anomaly Detection Model for In-Vehicle Networks Using Machine Learning Algorithms," 2020. ncbi.nlm.nih.gov
21. [21] M. Chowdhury, M. Islam, and Z. Khan, "Security of Connected and Automated Vehicles," 2020. [PDF]
22. [22] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and The Way Forward," 2019. [PDF]
23. [23] K. Bakhsh Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Vehicle Security: Risk Assessment in Transportation," 2018. [PDF]
24. [24] G. Cui, W. Zhang, Y. Xiao, L. Yao et al., "Cooperative Perception Technology of Autonomous Driving in the Internet of Vehicles Environment: A Review," 2022. ncbi.nlm.nih.gov

25. [25] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov