IoT-enabled Adaptive Control Systems for Cyber-Physical Security in Autonomous Vehicles

By Dr. Li Guo

Professor of Computer Science, Nanyang Technological University (NTU), Singapore

1. Introduction

In the AV era, driving behavior changes drastically, as control over the steering (and other devices) is taken over by autonomous agents, and driving commands are no longer generated by human–machine interactions [1]. This leads to the heavily interconnected cyber-physical aspects of AV environment (also known as autonomous CPS) to be exposed to potentially unknown hardware/software faults or adversarial influences. This also poses serious confidentiality and availability concerns on sensed data gathered from many onboard and sensing devices. This work adopts a black-box view by assuming the sensors as the devices and environment as the physical entity to control.

The introduction of autonomous vehicles (AVs) makes human drivers irrelevant in the driving loop, thereby enforcing the centrality of security and safety from both physical and cyber angles [2]. This work emphasizes the essential security measures in AVs and focuses on ensuring that an AV begins to take care of invalid and fake sensor data generated by adversaries or due to hardware/software faults [3]. Furthermore, this work proposes a computational model to ensure vehicle-to-infrastructure as well as vehicle-to-vehicle (collectively, V2X) communication security using the heuristic and formal aspects.

1.1. Background and Motivation

Autonomous vehicles—defined as vehicles capable of navigating and driving from point A to point B without driver input—have already become a hot topic. Considering the rapid evolution of connected and driverless—especially inter-vehicle communication and inter-vehicle interfacing systems—several security vulnerabilities (e.g., data interception, data tampering and data fabrication) that can be exploited to abuse normal V2V-relaying functions have been discovered [4]. Similarly, several recent research attacks on the V2X system work through a decade-old known idea, they still do tangibly exist. The more autonomous vehicle technology advances, the more scope there is to improve the driving experience, making safety and security a central holist notion. As a result, the security of IoT-enabled and autonomous vehicle technologies remains a very crucial exploration domain for researchers.

The recent advancement of the Information and Communication Technology (ICT) era has introduced the concept of an Internet-of-Things (IoT) to our daily lives. In recent years, the rapid development in the IoT industry along with the connectivity of all electronic sensors, tools, and devices has made our lives more convenient in various fields. The smart transportation industry, including the automotive, has transformed dramatically with the current rise in advanced driver-assistance systems (ADAS) and autonomous vehicles [5]. However, it has been shown that the success of any IoT system is highly dependent on the performance of its cloud service provider. The IoT cloud is central to the operation and value proposition of a spectrum of upcoming services in automotive, health care, sports and entertainment, finance, etc. [6]. Thus, the security and availability of connected services, in general, and the cloud infrastructure that supports these services in particular, are of paramount importance. In an IoT cloud, security mitigation involves challenges related to data privacy, data integrity, data authenticity, and data reliability. As a result, enhancing the safety and reliability of the IoT framework has become a crucial discussion.

1.2. Research Objectives

[4] The adaptive learning-based access control layer will dictate who and what accesses configuration parameters, which will be used in both defense and reconfigurable sensor systems. The data integrity and confidentiality models are designed for integrity checks, with the help of scales, torque sensors, visual sensors, and inertial sensors in both defense and reconfigurable sensor systems. All security components will share a heart-beat mechanism to detect inconsistency in the sensed data collected from all defense and reconfigurable sensors. A three-tire security architecture, dynamic filtering, and adaptive reconfiguration are defined and simulated in Hands-On Program for Cyber Physical System security for defense and reconfigurable sensor systems using.[7] The fast increasing ubiquity of "smart objects" in urban areas means that it is increasingly possible to share private information through the use of IoTs (Internet-Of-Things). Consequently, smart environments could be easily monitored and private information exposed to strangers, thus affecting privacy of citizens and the

feasibility of more and more applications, such as mobile payment or university submissions. With the aim of protecting the privacy of data sources with as much as possible, we propose a solution in the direction of privacy-preserving crowdsourced mobile data collection in the context of IoTs-based smart cities. This privacy-preserving crowdsourced data collection system, composed by a cluster of mobile devices and a set of server-back-ends and accessible only to authorized servers, is designed to protect citizens' personal life, avoiding disclosure of the route they are covering in smart cities.

1.3. Scope and Organization of the Work

However, smart transportation systems are not without their risks, particularly cyber-physical risks. As seen in different sectors of the economy (utilities; industry advanced manufacturing), the adoption of the Internet of Things (IoT), including Autonomous Vehicles (AV), recognizes cyber-physical risks as growing key threats. By integrating numerous nodes of IP-enabled sensors, a fully networked infrastructure enables traffic control in the case of an AV, as well as route selection. Recital 46 of the GDPR suggests that data protection requirements should be taken into account during the definition and construction of IT systems. Furthermore, the integration of the much broader additional set of sensors and actuators in a modern (self-checking, self-monitoring, self-healing) cyber-physical world means that, more than traditional digital security measures, the carefully planned integration of more than just digital technologies is needed for the planned integration of digital and physical security incidents in a CPS. It has particularly drawn attention to demonstrations on AV that current digital security services require significant improvement if they are to successfully withstand likely CPS attacks for fleet management and transport control [8].

Autonomous vehicles have proliferated with the recent advancements of artificial intelligence and sensing technologies, and its anticipated impact on society includes enhanced efficiencies, saved transportation costs, and improved road safety. The integration of autonomous vehicles will influence a variety of top-tier sectors, such as ride-sharing, public transportation, and commercial shipping solutions. Also, there is a clear global trend toward low-emission and zero-emission transport, particularly around urban centres where pollution is a significant concern. The use of GPS and tracking devices can notify authorities immediately in case of a road accident and reduce the time for repair of a vehicle. Geofencing technology could notify vehicles and automatically reduce speeds to safe limits in residential neighbourhoods or around schools [4]. Moreover, the widespread adoption of more efficient electric vehicles is improving overall fuel efficiency and reducing carbon dioxide emissions.

2. Foundations of Cyber-Physical Systems

Cyber-Physical systems have become an indispensable part of the fourth industrial revolution, integrating computing with physical processes to bridge the cyber and physical worlds seamlessly. The components of modern cyber-physical systems are operations-technology-driven fulfilling most of the new industrial standards of Industry 4.0. Cyber-Physical Systems encompass a very broad ideality of systems and technologies, from smart grids to smart homes, water management systems, self-sensed machines, intelligent structures, and of course, autonomous vehicles. Cyber-Physical Systems are able to adapt to the state of the system, compensate for disturbances, and respond to the various impacts of environment and vehicle forces. Vehicle sensors can express a variety of attributes including timeliness, resolution, spectral, spectrum, and so on. The time counter for the control device generally stores the actual vehicle time, besides to the UID of the device which defined by the supplier protection, will be set to zero after restarting the car. the most authentic information at the time for the controller, can be found in the instruments panel, it is important to compare the available instruments information with real values periodically, and update it. Results of experiments provide acceptable precision [4].

Autonomous vehicles are an integral part of the fourth industrial revolution. Besides the autonomous control itself, these vehicles provide perception, decision making capabilities, and adaptability in the field of interaction with the outer world. These functions require embedded and IoT systems in the vehicle system, which can open new potential threats to the vehicles themselves and the system elements they interact with. The IoT part of the vehicle already includes the vehicle web server, security systems, infrastructure servers, and other vehicles in the form of pattern and exchange models. The interconnected mesh can enhance the existing electromechanical system itself and possibly pose a major threat to a huge number of input systems [9].

2.1. Overview of Cyber-Physical Systems

Communication technologies between worms have many applications, including wireless sensor networks, drones, self-driven cars, and so on, that can significantly improve their in navigation accuracy. For example, the Global Positioning System, and other many navigation applications, have brought the satellite navigation technology on the End user device. In indoor and urban navigation areas, the effectiveness of satellite signals is limited and the accuracy of route navigation is too rough. Therefore, participating in vehicles other than a GPS satellite as in the case of the use of self-run self-moving cars leads the accuracy of our transport to defect level ([10]).

Cyber-Physical Systems (CPS) have been an active area of research dedicated to the design of computing-based control systems that interact with the physical environment to support manners of high-level control ([4]). These systems are used to manage interconnected physical and computational resources learned from big data to make the best decisions based on the available information. This approach has resulted in a plethora of CSS applications, many of which use a combination of deterministic control frameworks combined with statistical and computational approaches for decision making with real-time data ([11]). For example, in the aviation sector, dynamic Bayesian networks are used for software security, fault detection, fault diagnosis, and software reliability improvement. In the health sector, high-level control is performed by combining intuitive optimization methods with data, such as statistical data, patient monitor data, and hospital data. This integration can allow hospital communication and internal security.

2.2. Key Components and Architectures

Table 10 shows the major optional features that are found in connected automated drive-by-devices/automation platforms and in the basic technologies that can intrinsically, consistently be used for means of achieving the desired features in the car and its driver environment. As it will be shown in Section 4 (Scenarios and requirements), the implementations of automated features in a Vehicular Ad-hoc Network (VANET) ecosystem will cover a broad spectrum. The communications scenario can also unfold in multiple network iterations ranging from fully cooperative and connected (fC-C) scenarios to vanilla VANET. We assume very basic features like a common (geo-localised) network address both for the vehicle's VANET and in the private 5G-network (tethering) infrastructure that is currently assumed to positively precede the future vehicle 5G-communication ecosystem.

[12] The ecosystem of an IoT-enabled CPS can be divided into a number of components driven by different middle-wares, software agents and fault recovery systems. It is enabled by both

artificial intelligence (AI) and machine learning (ML). Highly automated and autonomous vehicles naturally have to be integrated into larger connected vehicle systems. These will also be part of IoT-supervised and sustained urban infrastructures that autonomously manage smart city resources. The smart home and the smart office are just additional elements of these global, IoT-driven autonomic service infrastructures. The impact of IoT is currently the most tangible in customised automotive services and in Industry 4.0 business initiatives.

3. Internet of Things (IoT) Technologies

Thanks to IoT, these systems are taking the concepts above to the next level, making possible a lot of new applications which refer to many fields such as: transportation [13], healthcare, robotics and energy management. In IoT systems there are, generally, two main ends: a device that senses and collects data from the physical world - the IoT device - and a system able to initially process, then store, display, deliver remote actions and, finally, (autonomously) take decisions based on these data. This paper presents the investigation and development of architectures and procedures put into practice in two IoT-based control systems leading to various issues related to cyber security in general and to privacy preservation in particular.

The Internet of Things (IoT) paradigm is now gaining a great deal of attention from engineers and researchers, mostly due to the large number of possible applications in various fields such as medical, environmental monitoring, automotive, smart homes and buildings, transportation, etc. This new approach is significantly changing the traditional concept of "network". In fact, the IoT lets any object connect to the Internet, share real-time data and be controlled remotely, thanks to Internet Protocol Suite (TCP/IP) standard use [14]. The new paradigm of IoT has led to the widespread availability of smart devices that are equipped with different sensors for both the measurement of physical quantities and position data. All these devices, instrumented with right sensing systems, are often used to create cyber-physical systems (CPS), where the remote control and/or configuration aspects can also be included. CPS are, generally speaking, systems where information technology connected devices (cyber part) interact with the real world (physical part) to accomplish specific tasks.

3.1. Fundamentals of IoT

Wirele Communication System is a key concern area for upcoming Vehicular Networks. Intelligent route choices, based on the thorough knowledge of the region by each connected vehicle, can be taken in order to enhance the effectiveness and reliability of communication. The proposed protocols are based on ad hoc and plant-vehicle communication (PLC) technologies. These protocols listen to radio wave transmissions for the purpose of identifying important information sources. However, traditional approach to disseminate messages in IoV suffers from a number of limitations. For instance, even though the messages carry relevant information, they have limited priority or limited lifetime, however, vehicles do not know this information and still deliver them. When a vehicle receives a life-saving message, the vehicle prior to dissemination must verify the validity of the information. Aware of the potential problem, in this paper, we examine for safety messages the current efficient communication protocols in the IoT domain and offer a leading improvement to effectively disseminate, theoretically model the messages and gauge the relative performance of the systems under examination.

[15] [16]Given the extreme drive in the evolution of vehicular networking, the Internet of Vehicles (IoV) has surfaced in recent years as an effective approach to convert vehicles into intelligent terminals that form a core component of the Internet of Things (IoT). The main motivating factor is to improve driver's comfort and road safety via cutting-edge information, communication, and control technologies. In essence, vehicular networks are meant for cooperative inter-vehicular communication, that can be used to share various information such as event warning, traffic conditions, and location-based services. Principle building blocks of the Internet of Vehicles (IoV) include in-vehicle on-board units (OBUs), roadside units (RSUs), and other infrastructure. Their inclusion is underpinned by the requirement of efficient dissemination of life-saving messages generated by roadside infrastructure and the vehicles in the vicinity which is vital. Two categories of life-saving messages for vehicles on expressway include safe and unsafe zones. Safe zones, generally, denote good road conditions. In contrast, unsafe zones pertain to hazardous and accident-prone areas, where drivers must take necessary action.

3.2. IoT in Cyber-Physical Systems

IoT-enabled adaptive awareness and control can significantly improve the cyber-physical resilience of autonomous vehicles [10]. Overly aggressive filtering or simply denying access to information without offering a "reasoned confidence"-based analysis of real-time monitoring can be detrimental to an autonomous car's safety. An IoT filtering platform aims to address the above challenges by efficiently associating raw sensory data and environmental factors with threat intelligence obtained from public/global and private/local cybersecurity feeds and maintain a FC boundary throughout the vehicle's journey. In addition, the adaptive part of the IoT platform leverages continuous machine (deep) learning to quickly adjust its security policies with high accuracy to address the FC drift due to new knowledge gained by sensors from the known to the unknown states [4].

The movie industry is filled with examples of autonomous vehicles gone rogue. In Maximum Overdrive, a mysterious alien force causes the Earth's technology to possess its own will, and trucks start terrorising a group of survivors. In well-documented reports Tesla vehicles have been known to lurch abruptly during autonomous driving, leading to accidents. A common theme in many of these movies and news articles is the fear of an autonomous vehicle mishap.

4. Adaptive Control Systems

It extends classic Intrusion Detection Systems (IDS) by engaging the physical interaction of the system with the environment, turning them into Intrusion Detection and Localization Systems (IDLS) to increase dependent security by detecting the cyber-physical anomalies and pinpointing their origin. Still, this broader focus turns IDLS into complex, multi-domain and yet incomplete constructs as they often leave aside other general requirements such as relevance to a particular system behaviors, a prompt resolution of all anoma lies, a decision of whether to trust some abnormalities or a disruption of the normal behavior to cause it to yield less information to an attacker. Therefore, here we extend it in two ways. First, we narrow down the focus by making the IDLS adaptive cyber-security subparts that get the multiple competing objective of an IDLS more in line with its domain of application. Such general insights are developed and exemplified with a specific anchor applied to automotive driving systems but they automatically extend to other applications that share the same cyber-physical security challenges.

As these vulnerabilities and the associated conceptual components continue to emerge, detecting such cyberattacks on autonomous driving becomes increasingly difficult [17]. Recognizing this challenge, we envision an integrated and automated Intrusion Detection System (IDS) that not only seeks to identify the occurrence of cyberattacks, but also works towards localizing and characterizing that attack in order to appropriately respond to it [18]. Moreover, with the advent of vehicular connectivity and increasing amounts of over-the-air

(OTA) updates, the attack surface of an autonomous driving system simply increases, making it all the more important to ensure applications and APIs are hardened and that the security of external infrastructure is also duly considered. To that end, we discuss strategies to integrate external communication security features into the management and distribution of attack detection information.

4.1. Concepts and Principles

Experience has proven indispensable and necessary to forecast and identify the planned events, in order to cooperate directly from a driver's smartphone to the vehicle. The driver not only needs to be transported from one point to another but also to plan all the activities for the day while commuting. As a result, the proposed technological solutions have been designed for two critical modeling ranges that allow to cooperate the vehicles and infrastructure components among them. A vehicle equipped with a diverse range of intelligent features, which can achieved an important increase in quality of information and services being transferred back to the driver, is capable to make more flexible and autonomous collective technical movements. An increased amount of information in the form of nuisance alerts should be quickly verified thanks to the multitude of flags used. All such included algorithms and models finally are able to provide more accurate predictions for vehicles [3].

Vehicular networks can be viewed as complex systems that provide cybersecurity and big data challenges [19]. A vehicle has been equipped with a variety of Key Life Cycle Devices (KLDs) dealing with secure driving services such as recognizing the basic movement of neighboring vehicles, applying the cooperative adaptive cruise control systems, all up to forecasting fault events (see . Consequently, the broadcasting of precise road events is being done with the aim of turning out an integral part of the functioning of each modern vehicle. It provides utmost future improvements to the safety of operation of modern intelligent transport systems. Today Internet of Things (IoT) vehicular systems provide an attractive opportunity to improve this situation, such platforms are capable to reach in the full-scale potential improvements in the domain of experiences and possibilities for driving and gaining a lot of energy savings and road safety. Car fleet is being turned into a powerful network-innovation education for numerous services [20].

4.2. Types of Adaptive Control Systems

Cyber-physical systems (CPSs) integrate autonomous vehicles (AVs) with physical components and network control to make roads smarter and safer. In an intelligent interactive environment, AVs constitute a significant force to constantly sense the environment and operate the controllers to enhance road capacity. The key characteristic of the synergy of CPS and Internet of Things (IoT) is that IoT and IP-enabled sensors/actuators and among the biggest opportunities at the horizon is the avenue defined by the CPS + IoT combination [4]. By integrating internet protocol (IP) microcontroller units (MCU) and sensors, the boundary between IoT and CPS is blurred, and a number of security challenges are significantly accentuated as the lightweight communication protocol suites that have been inherent to IoT connectivity are cast aside for mature offerings from the IT and network world. Moreover, since vehicle owners convenience and ease in their handling, and vehicle performance can not drastically differ from todays cars and transportation infrastructures, security-by-design for CPS environment has to envelop and involve a much larger, highly complex and highly sophisticated range of mechanisms and controls, such as of varying natures and addressing varying characteristics. AVs are one of the most critical forms of Cyber-Physical Systems (CPS). Their distributed and centralised components communicate with one another by integrating hardware, software, network, and communication technologies for real-time operation. The virtual cyber-world of automotive network systems and the physical action of the individual vehicles which constitute a part of the transportation infrastructure, effectively bring CPS's to life. i.e., vehicles represent a significantly rich source of data with, distributed and simultaneous occurrence of both data sources be fused by the CPS. Cyber attacks typically aim at incapacitating some, or all of the autonomous operating protocol by hijacking it or mitigating it to colluding aim or else, attacking the attackable components of the AVs as an aim to divert, delay or disable the individual or fused system components from being able to fullfill their purpose fulfilled. In this regard, the research invariably over that past two decades has continuously raised alarms through publications on just how vulnerable automotive networks and hence the individual operating vehicles are to attacks and tampering and hijacking of their electronic modules. Using CAN as an example, it offers zero internal security measures, worse yet it has been discarded by the standardization panels an it's replacement revision have no inherent security measures often relying on higher layers TLS tunnels to secure the network. Recreational and commercial vehicles have been demonstrated to be in a large series of demonstrations since2010th, which have been demonstrated to be overridable so that almost complete control over a vehicle can be taken by a malicious third person on a remote basis [2]. Networking the physical components of an AV on turn makes the car susceptible to non-physical events, e.g., cyber-attacks on it in an attempt to affect its behaviour directly.

5. Cyber-Physical Security in Autonomous Vehicles

In the connected vehicle the externally commanded control by the embedded controllers will serve the real-time signals, representing involved system states along with. Most control variables, that are destination and departure co-ordinates, current position of the vehicle, expected path direction are computed by the hosting server for ensuring the safe driving. So, the embedded controller can immediately acts the instantaneous control command with no feedback [4]. Generally, in a generic PID controller the proportional, integral, and derivative are the parameters of the controller. So, the possibility of tuned un-optimized Kp, Ki, and Kd controller parameters can limit the driving in the safe physical environment of partially controlled and semi-autonomous cars. Due to this imprecise range of first derivative of time integral input signal there are various common security attacks on the road. Together, real world actors are also the intelligent models that understand the moving pattern of individual vehicles and the priorities, timely, and deliberate avoidance from the on-road obstacles.

Autonomous vehicles or drones, by and large, are a set of sensors, actuators, and computational mechanisms that are engaged with vehicles, both land, air and sea, enabling the automatic exploitation of several control functions for physical or non-physical processes. These communication modules have to significantly comply with the interfaces, understanding of messages, and decapsulation of payloads for decoding during payload transmission [2]. The data of the developed interface of a connected vehicle is collected by the embedded controllers and is forwarded to the server side on demand of the development team, installed at back office. So, when the connected vehicle system gains information from its embedded sensors and actuators systems, the vehicle is converted into a huge source of data center machines, once it regulates to return the derived data for other systems (communication, utilization of data like controlling, network integration etc.) of the global system, it turns into an Internet of Things sensor. When it is passed, visual communication enables the transferred sensor data turns into Machine to Machine Communications. When the above steps are followed, a vehicle becomes one part of the IoT system [21].

5.1. Challenges and Threats

In order to make driving more secured and efficient, the located infrastructure must include the latest intelligent transport systems (ITS) solutions. The mass of cyber-attacks on vehicles are directly imputed to the fact that AVs do not prevent Intelligent Attacks, which increases the massive risk to the public and the economy. Having detected and isolated cyber-enabled threats, AVs should dynamically adjust their control law due to adaptation to unknown attack characteristics. [22]. Cybersecurity in communication protocols, AI-based secure channel access, and AI-based cybersecurity solutions for multi-zoom intelligent traffic lights are key research areas. To tackle the above-mentioned challenges and threats to the APS and AVS, a broad research effort is anticipated and being enforced.

Security of Cyber-Physical Systems (CPS) in autonomous vehicles is a major concern, as these vehicles rely on various technologies and infrastructures that are vulnerable to cyberattacks [16]. With the increasing number of electronic systems and connectivity in cars, cyberattacks on transportation systems have become serious threats [23]. The potential cyberattacks on vehicles include diverse cyber-enabled threats at different layers, such as sensor data spoofing, false data injection, network attacks, Geographic Intrusion Detection System (GIDS) attacks, and shortage of knowledge in multi-sensor integration. Recently, autonomous vehicles (AVs) have been adopted as a means for self-driving to provide high driving performance and high mobility. However, the growing reliance on inter-disciplinary technologies that are vulnerable to cyberattacks creates significant threats. Currently, modern vehicles and AVs have the ability to communicate with and inform infrastructure.

5.2. Security Measures and Best Practices

The public infrastructure of a vehicle, consisting of backend servers, third-party service providers and other partner companies, introduces new challenges: Other than in a classic.monolithic backend server, here each component is often operated by a different entity and requests data or services from components of other entities. Additionally, serving as the backend for many different actors receiving a multitude of different types of queries means that the server infrastructure has to act as a gatekeeper, intelligently route queries to the right components, and then hide behind a firewall preventing unauthorized access to all other components. Ideally, each component has a firewall, such that the potential damage a successful attack can cause is limited. But after compromising a single component, attacks should not be able to easily jump. Across all previously mentioned concerns, there is a hybrid security measure across both software and hardware that can be beneficial for ensuring security [4].

Autonomous vehicles (AV) are reshaping the automotive industry with their countless advantages and promises [24]. However, crucial questions related to these technologies are still unanswered, despite efforts to address security threats related to this kind of transportation, and it is imperative to address them systematically [25]. The elements of a vehicle are interconnected through a combination of V2V, V2I, and V2X communications with different architectures, connectivity solutions, dynamic network topology, public infrastructure, and a varying set of boundary conditions. Building reliable and secure systems that act in an environment of constantly changing actors and environments is a challenging task. The complexity of the task increases with each individual component that is involved in the decision-making process or has an impact on actual road traffic.

6. Integration of IoT and Adaptive Control Systems

Nevertheless, this architecture allows to consider the integration of the edge intelligence and the localization by cloud technologies, conceived as promising for future research frontier, as well as the study of the privacy and security issues by integration of the IoT security system and the cybersecurity [26]. In fact, the extension to edge and cloud architectures will make possible the introduction of control and location functions on board of the vehicle and on the cloud site, even with reduced communication delays. The privacy issue is the major for the CPS of AVs, which is able by the use of appropriate mechanism for the sensitive data encryption, for the anonymous identification and for nondisclosure of confidential information without consent of the user. Moreover, the security is fundamental for the IoTs of the AV for potential cyber attacks, as well as physical attacks, particularly if the control systems are infringed and can lead to accidents and incidents.

The IoT- enabled adaptive CPSs for AVs, whose development is intended by this article, can be potentially applied for future road and public transport systems, as shown in [21]. The cyber-physical support of AVs is an essential asset of the smart city, contributing to the optimization of the traffic management and the guidance to wirelessato- wireless communication and the security systems, as well as manoeuvres to be taken in emergency cases of safety and security, not only on the basis of the actions suggested by first level control systems but also of the indications or proposals by second level control systems. For these reasons, the safety of AVs depends essentially on the control system efficiency and on the communication reliability, particularly in urban scenarios due to the increase variability of the environment and the unpredictability of the user behavior [ref: Model references].

6.1. Benefits and Opportunities

We maintain that advanced vehicular control and safety assurance through adaptive control development must seamlessly incorporate cyber-physical security within a unified methodology. As reflected by the publications on optimizing fuel efficiency, driving economics, minimizing emissions and other such topics, significant research momentum exists around enhancing different aspects of connected and autonomous vehicle systems designed in isolation without direct consideration of vehicular cyber and physical security [3], [19]. The major challenge numerous such works face remains the distinct consideration of the attacker's actions and goals or the lacking realization of the interdependence between the vehicular cyber and physical layer. Our research strives to fill these glaring gaps by offering a uniform treatment of interconnected physical vehicular performance, multi-objective adaptive control design and cyber security in the presence of an adaptive adversary.

Connected and autonomous transportation systems could significantly diminish road fatalities and crashes, while augmenting the efficiency of traffic flow and the conduct of human and economic activity. Fully embracing the advanced technologies that powers battery electric vehicles, connected vehicles, high fidelity mobility models, cloud, and analytics, to name a few, will help realize these societal improvements. A number of astute innovators and corporations have begun to buy into the concept of connected and autonomous vehicles, while national governments worldwide are increasingly knowledgeably conducting research, education activities and policy innovation to make the connected, autonomous vehicle dream a reality. However, according to [27], robust cyber-physical assurance for these systems is still a significant missing piece in the grand puzzle of safe and trustworthy autonomous transportation.

6.2. Challenges and Limitations

In IoT, the constant transfer of data "on the fly" among different "smart" interfaces and inside a given smart interface is a challenging service from the security perspective. Autonomous cars must "upload" for collection their current context to the IoT interface when certain unforeseen cooperation becomes necessary. Also, the car has to request assistance and context updates from server edge computing servers, local crowd, or cloud through physical access points, Wi-Fi, or mobile networks [17]. Random requests can be security hazardous. Attacker readings of such information can reveal where the vehicle carries valuable payload or humans. For network integrity of a VDA system, any sudden security "obstacles" are inherently sinister for preoccupying and spoiling the vehicle IoT sensor space by humans or hacking entities, such as unexpected traffic jam, inserted bad drivers, fake IKEA bike, sketched holes on roads, and wacky traffic lights. For advancing and integrating spare of secure computation, the expense of privacy over security becomes a challenge.

In an ITS like autonomous cars, communication is performed by wireless IoT platforms for data acquisition, edge and cloud computing, and cyber-physical connectivity, respectively [12]. Consequently, security is a serious consideration for privacy, data protection, car autonomy, and network integrity as well as vehicle safety. Further, vehicle autonomy and the responsive interactions between autonomous vehicle systems and systems operating with human driver–performed steering/wheel-brake-accelerate functions require strict security procedures to avoid accidents and misuse [28].

7. Case Studies and Applications

The above-mentioned problems, by focusing on cybersecurity problems, bring into consideration the evolution of cyber-attacks in this context. These new kind of attacks leads us to think of the development of new advanced systems to be able to counteract with them and also the development of new transport paradigm. To address and solve these problems, the RISE-ITN EU project aimed at the realization and at developing of an end-to-end serious vehicular cyberphysical Software Defined Controller (SDC)-based System-Software Defined Car (SDC) solution, specifically thought for automotive applications and enabled by the introduction of IoT architectures paving the way for developing cooperative and connected vehicles IoT architectures at the base of a complete automotive pinpointed IoT electronic architecture [6]. In this context, the proposed solution consists of the realization of a multi-agent software defined controller system designed to be run on top of an IoT-like infrastructure to guarantee federated control for the cyberphysical, cooperative, and connected, vehicles and architectures. The integration with IoT devices (cameras/RFID/nodal-on-car sensors) to be carried into experiments on ADAS and autonomous-driving features are also thought. A first home robotics IoT of the shelves 4.0 hardware platform is also used to inspire the potential users and students with application of the proposed system.

Self-driving cars are well known as next-generation advanced vehicle systems that are set to solve several security issues and to present mobility solutions. As they start advancing towards higher levels of autonomy levels, several technological challenges need to be overcome. One of the key technology solutions enabling these types of vehicles is the use of multi-agent, autonomous, adaptive, and cyberphysical systems that can also feature autonomous decision-making strategies [21]. Such vehicular settings should be developed to leverage the possibility of the Industry 4.0 approach to also enable lending to them common Internet of Things (IoT) functionalities. However, this will also pave the way for all the connected vehicle problems that currently involve them, for example, enabling physical hacking strategies, sensor hacking attacks, OBD-II theft of services (TOS)-like hacks, and so forth.

7.1. Real-world Implementations

In this chapter, three real-time implementations of optimized ACSs into a modern CAV are presented. One of the SAE Level 2+ experimental vehicles where the control system (i.e., the case-based ACS (CBCS)) has been finally integrated can handle multi-lane highway and busy road traffic. The second vehicle is a new ready-to-market electric CAV, initially fitted with EGO adaptive control that has been replaced by the adaptive secure CBCS. Conclusive road test campaigns showed the efficiency of the approached secure ACS in highways' multi-lanes and even in unstructured parking scenarios. New real-time experiments show that the adaptive cybersecurity CBCS developed on real attacks in a test road becomes efficient within conventional IT environment. These real experiments lead to a conclusion in the "hot-topic" use-case of Intrusion-tolerance-inspired IDM in the IoT-CPS (where IDM stands for Intelligent Driving Module).

State of the art cybersecurity concerns have led various researchers and industrialists to study the possible vulnerabilities of connected and autonomous vehicles (CAVs) [16]. One particular approach is related to prediction and adaptive control systems (ACS) based on available data from sensors that monitor vehicle intrinsics and environmental datasets, including pervasive and advanced IoT sensors [18]. Pallengottla et al. recently proposed a novel adaptive secure

ACS based on multiobjective optimization that uses a physical interaction force model of a vehicle to adapt fast to new Cyber-threats [28].

7.2. Use Cases in Autonomous Vehicles

Once IoT data (user behavior, user driving statistics) is collected, expected scenario analysis can be possible with the machine learning algorithm. This will help to recommend some good facilities to the user. We added a file with real-time event details sent by vehicle IoT for adding safety for passenger and pedestrian by warning about potential harmful event prediction. That in turn will help to make all application form base on that IoT device's real-time event data. With the help of this user personality base, the vehicle can suggest a person to go near by some hospitals in case s/he get injured or in case of any normal transportation system in case will book a movie or will suggest a place to go. The second use case is in V2X communication security architecture with the help of blockchain in which Intelligent Transportation System (ITS) systems have been to re-engineered to adequately cater the complexities of the future provisioning of the V2V and V2I services in the domain of C-ITS using blockchain technology. A smart car can drive itself without the need for human assistance. [29]

[22] [21] Several use cases can benefit from the IoT-enabled ACS for cyber-security protection in the AVs, such as behavioral analysis using IoT for detecting driver/passenger attributes, detecting and mitigating tampering attacks using OSG technology, secure provisioning using OTA secured in-car networks for navigation and traffic navigation systems, and cyber-security compliant AVPaaS and MaaS platforms. The very first use case is the vehicle-behavioral analysis by using an IoT-enabled solution. Vehicles can have multiple "personalities" depending on the user. The personality can be of driver using vehicle navigation. The driver may want to drop the vehicle to pick up the bread on the way back home OR may want to find hotels, cinemas, memorable places to park, etc. using navigation system services and sensors. The personality can also be of passengers of vehicle. The passenger of vehicle can be of different ages (e.g., children), physical limitations (e.g., diseased, writing injury, broken leg and fingerament, etc.). Therefore, the vehicle should have a mechanism to identify a person existing in it and suggesting corresponding options to each individual accordingly. One feasible available solution is vehicle senses and send them to the processing server using Inter of Things (IoT) devices.

8. Future Directions and Emerging Trends

Provably, all these smart-connected IoT devices allow an autonomous and automated driving vehicle mainly for: 1) better localization and mapping; 2) better understanding about the environment and therefore better ability to plan the trajectory, 3) better answer to allowed user and 4) augmented reality in mobility support (parking assistance, traffic navigation and possibility of warning about potential risks and communication in two directions to indicate its position). Most of traffic signaling systems are composed by signal traffic lights to regulate the traffic and to ensure transport efficiency, safety and improve road transportation system (RTS) management. In the future, the communication between connected pedestrians and vehicle should also be done in order to allow autonomous vehicle to announce its arrival at an intersection to the pedestrians [30]. The information exchanged can also take the form of demand signaling from pedestrians to vehicles about their intention to cross.

Connectivity is essential in the coordinated and synchronized operation of AV [21]. This includes on-road infrastructure (intelligent traffic signs and smart traffic light systems), cyber-physical systems (such as autonomous hilltop-less small railway vehicles) and the integration to and with pedestrians and bicycle riders, in outside as well as in enclosed urban and peri-urban spaces. This is achieved through electronic IoT (such as RFIDs, NCF transceivers and other contactless devices) that keep environmental properties or population paths. When referring about mobility of AV through smart IoT foreseen environments, we certainly (but not exclusively) refer to green infrastructure, avoiding or reducing the risks, obtained mainly from the knowledge of the environment (NFC tags multiple signals & scattered coverage).

8.1. Advancements in Technology

Meta Id: Seymour PapertAutonomous vehicles making decision for broad domains such situated robotics and security of cyber-physical technology. Modern day autonomous vehicles are cyber-physical systems being equipped with intelligent computation and communication capabilities. As a result, they have representation in the form of cyber-physical systems (CPS) unlike any other autonomous vehicle of literature. This chapter presents a survey of elegant closed-loop results, algorithms, and strategies that bridge from traditional optimal control theoretical advancements in cyber-physical technology within autonomous vehicles framework. Resilient cyber-physical Autonomous Vehicle (AV) technology for advanced control, sharing security down to the vehicle layer to prevent potential vulnerabilities is rigorously considered at every finer granularity level of expression.

[26] The advancement of technology has been making rapid progress across the globe owing to the Internet of Things, Artificial Intelligence, Machine Learning, Big Data, Cloud Computing, and 5G wireless communication technologies. All these technologies have been playing a crucial role in the advancement of the field of Vehicle Safety, Control, and Monitoring. In this review chapter, we have reviewed the recent advancements in the fields of Adaptive Control, Optimal Control, and Model Predictive Control in Cyber-Physical Security framework for Autonomous Vehicles. Additionally, most of the fundamental theories have been modified and extended so that these can be incorporated in the use-case scenarios of Autonomous Vehicles.[22] With the aims of reinforcing the road safety and reducing driving stress, many automotive Original Equipment Manufacturers (OEMs) are moving toward the production of fully autonomous vehicles. These vehicles demand worldwide real-world datasets in which they can operate and find strategic decisions. Given this context, researchers must barricade the vehicle security against numerous cyber threats, including signal falsification and smart sensor repudiation. When these threats are not controlled, they can impose huge risk to human life and cause very serious or even catastrophic accidents. This chapter reflected on three of such important foundational threats of cyber security.istinguishing feature of this chapter include a historic perspective trace back to historic events and publications, an overview of participant research and relevant technologies. This is followed by dedicated sections on network security, system security, and signal falsification. In this chapter, policies are also reviewed that take an integrated outlook toward the vehicular production ecosystems. Subsequently, time-delayed discrete-time Markov jump systems and overall matching system state function are newly defined and established as wagner function.

8.2. Research Opportunities

Cyber-Physical (Autonomous, Self-Driving) Systems (CPS) and Internet of Things (IoT) based data infrastructures' mutual cyber-world vs physical world risks identified [17]. Connected Electronic Devices (CED [and other IoT Devices) and Network Nodes : A malfunction or bad programming by a TBI [Temporary Build Influence] can result in bad or inadequate physical inventory management. In a smart environment (SE), the electronic devices (EDs) being used have access to the integrated inventory management soft system(s), enabling the devices to take real-time decisions to maintain the inventory as per the threshold, ensuring the availability of the desired item at an appropriate place and time to avoid the deficiency of the desired product (Kirginc, Dereli, & Rauch, 2021). Such a controlled environment enables intelligent traffic strategies to work precisely for the transportation of evacuated goods at the sublevel of smart healthcare (e.g., based on a specific emergency) or the macro level (especially important for vaccination campaigns) (Afsi & Ghonaimy, 2021).

Semi-structured cognitive maps (including the OWA [Ordered Weighted Averaging] based extension) for prioritizing security needs, both subdomain level and overall or general [21]. Yearly updates and reviews comparing autonomous vehicle (and cyber-physical system) security need prioritizations. Semi-structured cognitive maps are a relational form of knowledge representation, useful when there is only a vague understanding of what the future need weighs are in any area, including socio-mechanical subdomains (like security). Major subdomains including Industry Security (IS) needs, Privacy Needs in Autonomous Vehicle (AV) (and other systems vehicles), and Cyber Security (CS) needs. OWA prioritization as normative and descriptive, define needs and heuristics for safety regulator and industry programmers to consider when designing, programming, and regulating autonomous vehicles and cyber-physical systems.

9. Conclusion

The adaptive control system for the autonomous vehicle is highly reliant on the inception and execution of the telecommunication infrastructure, cloud computing, sensor devices and software framework. Concomitantly, we are spearheading the number of cyber attacks that are impinging on different levels of the vehicle control continuum i.e. Intra-vehicle security, Vehicular communication and interdependent infrastructure domains has also come under severe scrutiny for this research trail. Present day security policies, precautionary protocols and regulatory enforcements in the midst of the AI and ML for cyber-physical articulations to sustain the present day threats are widely acknowledged, although this work is positing the contemporary domain of the adaptive security measures for autonomous transportation system with novel IoT solutions in its cyber physical integrity.

The Internet of Things (IoT-Enabled) Adaptive Control Systems (ACSs) are integral components of self-driving cars that rely heavily on diverse functionalities such as lidar, GPS, cameras, and vehicle-to-vehicle/vehicle-to-everything (V2X) communication [31]. The ACSs integrate the excessive physical level to control the interactive command parameters with the mechanical systems and provide the force profile for a successful execution plan. This necessitates an intricate essence wherein the physical layer is stringently connected to the cyber layer, as well as remains largely vulnerable and thus prone to cyber attacks. This paper thus tries to synthesize, systemize and offer exhaustive understanding and endorsement of established security measures that curbs the contemporary vulnerabilities of ACS [ref: ead000b4,5a9c2ec0]

9.1. Summary of Key Findings

Also, it has emphatically argued that vehicles are not only treatable as simple transportation units but in an entirely new context: as living space. The proposed cybersecurity mechanisms have also been found to enhance adaptive control initiation, operation, and communication mechanisms for RVs. Furthermore, an early realization of a cybersecurity mechanism can be carried out in the first instance by using RVs for ensuring controlled traffic signals (known as Green wave), adopting less infrastructure support, needing less communication, and avoiding any possible confusion among RVs due to new settings in the infrastructure, which may not be well known to one or more RVs. No loss of control of the later positions (network security) has been explained in great detail in this chapter. Finally, the experimental layout of the entire security framework has been described in an elaborate manner, explaining all the aspects of the system in a comprehensive manner.

[32] [33] [21]The chapter discussed the current security concerns in the AV era and has made a comprehensive review of the existing cybersecurity mechanisms and corresponding countermeasures. Specifically, it has carefully proposed several cybersecurity countermeasures (e.g., access control, intrusion detection, behavioral analysis, and defense strategies) and also sensors to safeguard transportation systems for passenger vehicles that are empowered with the Internet of Things (IoT) devices (i.e., LIDAR, RADAR, camera, IMU, and etc.), which are widely used across the globe for security enhancements. It has also explained the capabilities of the proposed security technologies to autonomously detect, interpret, and react to an attack. It has elaborated on the robustness of the proposed system by emphasizing on the theoretical and experimental analysis of its service provisioning platform (road infrastructure) and the onboard system (RVs). It has proved that the proposed

cybersecurity mechanisms autonomously enhance the context-aware cybersecurity of the RVs.

9.2. Implications and Recommendations for Future Research

The IoT ecosystem can facilitate the exchange of vital safety messages proactively, and prospective accidents and subsequent injuries, lives, and property can be averted. 5G/6G technology trees by engaging in ultra-reliable and low-latency communication can also provide security and threat warnings to AVs in a timely and secure manner. Technologies have a substantial potential to address these goals. Nevertheless, because all these technologies are infrastructureless, fully or partially distributed and have slow-to-high latency figures, effectively they become the ideal targets for security and privacy breaches. Therefore, threats and vulnerabilities must be assessed proactively and cautionary measures ought to be followed [12].

Connectivity is essential for the synchronized operation of Autonomous Vehicles (AVs), achieved through IoT electronic devices. IoT sensors enable self-driving vehicles to transition from manual to fully autonomous operation, assisting with sensory mechanisms, actuators, and real-time decision-making [21]. In addition, IoT facilitates augmented mobility assistance, ensuring smart and safe vehicle operation for passengers and pedestrians. It also enables traffic navigation and supports the development of completely autonomous driving mechanisms [25]. Smart transportation is expected to transform cities to smart cities as well. “IoT + V2X” will be a significant technological boon for AVs, since vehicles will communicate with each other, traffic lights, and traffic signs by sharing information among them. In addition, they will share the information regarding the immediate surroundings of the vehicle, enabling them to detect dangers before they actually occur.

Reference:

1. Tatineni, Sumanth, and Anirudh Mustyala. "Advanced AI Techniques for Real-Time Anomaly Detection and Incident Response in DevOps Environments: Ensuring Robust Security and Compliance." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 88-121.

2. Biswas, A., and W. Talukdar. “Robustness of Structured Data Extraction from In-Plane Rotated Documents Using Multi-Modal Large Language Models (LLM)”. *Journal of Artificial Intelligence Research*, vol. 4, no. 1, Mar. 2024, pp. 176-95, https://thesciencebrigade.com/JAIR/article/view/219.
3. Bojja, Giridhar Reddy, and Jun Liu. "Impact of it investment on hospital performance: a longitudinal data analysis." (2020).
4. Vemoori, Vamsi. "Towards a Driverless Future: A Multi-Pronged Approach to Enabling Widespread Adoption of Autonomous Vehicles-Infrastructure Development, Regulatory Frameworks, and Public Acceptance Strategies." *Blockchain Technology and Distributed Systems* 2.2 (2022): 35-59.
5. Tillu, Ravish, Muthukrishnan Muthusubramanian, and Vathsala Periyasamy. "Transforming regulatory reporting with AI/ML: strategies for compliance and efficiency." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.1 (2023): 145-157.
6. Bayani, Samir Vinayak, Ravish Tillu, and Jawaharbabu Jeyaraman. "Streamlining Compliance: Orchestrating Automated Checks for Cloud-based AI/ML Workflows." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023): 413-435.
7. Tomar, Manish, and Vathsala Periyasamy. "Leveraging advanced analytics for reference data analysis in finance." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.1 (2023): 128-136.
8. Abouelyazid, Mahmoud. "Advanced Artificial Intelligence Techniques for Real-Time Predictive Maintenance in Industrial IoT Systems: A Comprehensive Analysis and Framework." *Journal of AI-Assisted Scientific Discovery* 3.1 (2023): 271-313.
9. Prabhod, Kummaragunta Joel. "Leveraging Generative AI and Foundation Models for Personalized Healthcare: Predictive Analytics and Custom Treatment Plans Using Deep Learning Algorithms." Journal of AI in Healthcare and Medicine 4.1 (2024): 1-23.
10. Tatineni, Sumanth. "Applying DevOps Practices for Quality and Reliability Improvement in Cloud-Based Systems." *Technix international journal for engineering research (TIJER)*10.11 (2023): 374-380.
11. Shahane, Vishal. "Harnessing Serverless Computing for Efficient and Scalable Big Data Analytics Workloads." *Journal of Artificial Intelligence Research* 1.1 (2021): 40-65.

12. Shanmugam, Lavanya, Ravish Tillu, and Manish Tomar. "Federated learning architecture: Design, implementation, and challenges in distributed AI systems." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*2.2 (2023): 371-384.