Adaptive Threat Response Mechanisms for Cybersecurity in Autonomous Vehicle Networks

By Dr. Kin-Man Lam

Professor of Computer Science, The University of Hong Kong (HKU), Hong Kong

1. Introduction

To address the dynamic, sophisticated, and undetectable cyberattacks the solution to stabilize the CAV platoons can be mainly divided into two mitigation directions. The first mitigation direction is to construct a new research method to suppress the control effect of cyberattack. This direction is usually based on designing a robust and resilient control strategy for the active vehicle. [1] The second mitigation direction is to detect and remove the threats from the platoon structure to secure and stabilize the following teammates. It is naturally considered as the design problem of the monitoring sensor for the individual vehicle. Both the first and second mitigation methods aim to secure the number of relatively stable and beatifully-preceding and following teammates in the CAV platoon.

Autonomous vehicle technology has advanced to the point where vehicles have the ability to communicate with one another and interact with the environment around them. This hasty proliferation of vehicle communication technologies allows an immense number of vehicles to interact, however, unfortunately it exposes those vehicles to new and often undeterred threats from cyber espionage, cyberattacks, etc. A secure and reliable communication network is vital for safe and efficient vehicle operation. The design of a vehicular network is crucial, and should allow the detection and adaptation to cyber threats. On the other hand, a robust control strategy should be aggregately designed with a communication control system to resist cyber threats that affect driving safety and traffic fluidity. [2] With both methods, the accurate topology information can be achieved and compared with the desired topology information to determine the vehicle control.

1.1. Background and Significance

Reliable cryptographic systems are necessary but not sufficient to protect the connected vehicles from various cyber-attacks. Other components of security that need our immediate attention are secure localization algorithms to rely back for network security. Machine learning- techniques can provide the best results with the proper amount of training and testing data. Further, machine learning-driven trust management schemes can provide a good resistance against all types of insider and outsider cyber-attacks. This makes these network particularly vulnerable to Sybil attacks, collusion attacks, and selfish node attacks. Trust can be mismanaged in an IoV environment affected by packet drop attacks, Eavesdropping, Sybil attacks, Sinkhole, Selective forwarding, and Jamming and Deception. Cyber-attacks on V2V communications can lead to adverse packet dropping, incorrect routing and man-in-middle attacks. Cyber-attack on V2I communications disruptions vehicle connections and reduce information integrity. Cyber-attacks including Sybil attack and DoS cause trust management inefficiency image sensor capture, communications, Proving non-data trust could lead to inaccurate localization after a lack of correct GPS or interconnections dropped by an outsider.

Connected vehicles are part of the IoT, so cybersecurity challenges are similar [3]. Vehicles' proprietary protocols for Vehicle to External (V2X) communications have insecure communication and ECUs, leading to more attack surface [4]. Infotainment functions in vehicles are not well isolated from critical functions, enabling potential attackers to take control of the vehicle rudimentary by compromising the infotainment protocols. Also, many critical capabilities of vehicles, e.g., diagnostics, can be turned on remotely. This further opens the possibility of critical vehicle systems being compromised by an attacker. Beason et al proposed to use blockchain and check the event logs but did not describe further [5].

1.2. Research Objectives

To explore and analyze the applications of game theory in order to enable the understanding of the cybersecurity aspect from the perspective of a threat model; To explore a comprehensive review of the existing state-of-the-art cybersecurity threat response methodologies within the cyber-physical autonomous vehicle network environment; To identify existing malware propagation models and, based on the available dataset and specific environmental constraints present in the local autonomous vehicle network, it will develop custom transfer, latency and multiple actuation architectures; To establish a signature-free dynamic anomaly-based cyber threat detection system for the intelligent autonomous vehicle network

environment by incorporating architectural level adaptive intrusion detection algorithms, software based packet encapsulation, behavior based anomaly intrusion detection and reinforcement learning; To explore and develop a distributed collaborative approach for the communication protocol of connected and automated autonomous vehicles using time division multiple access -based real-time frame while making use of sharing intelligent decisions by vehicles in congruence with dynamic traffic state.

[6] [7]The overall objective of the research is to investigate the potential applications of game theory in the design, development and deployment of an adaptive cybersecurity threat response system in the autonomous vehicle network environment. Within this overarching research domain, the specific research objectives are as follows:

1.3. Structure of the Work

To address these exploitation methods, a two-tier, context aware, and adaptive defense mechanism is proposed to monitor the internal and vehicular specifics of an automotive system and reconfigure the system according to the requirements of the current threat scenarios [8]. The reconfiguration is employed through secondary communication, which ensures the adaptability and robustness of the responses even under attack and also prevents the attacker from accurately gauging their impacts of an attack. This mechanism is capable of monitoring the threat and detecting the attacks early, which is in accordance with the cybersecurity best practices and meets the SAE cybersecurity requirement to respond in the safe state during a cyber attack. We rely on an analytical model to determine the optimal defense reconfiguration strategies necessary to the following adaptive response mechanisms. These analytic model can be used to evaluate the proposed guidelines for the adaptive response mechanism, and give the system designer feedback on how to make the system secure without significantly degrading its normal, non-malicious intelligence. By simulating attacker-defenders interactions, we present experimental results aiming at quantifying the different trade-offs in these guidelines so that it can be used as recommendations for any vehicle having autonomous features.

The paper is structured as follows. Section 2 scrutinizes the growing prevalence of cyber threats and the strategies to address these threats in the automotive industry. Here, several cyber security mechanisms are presented, followed by an analysis of security threats to autonomous vehicle networks [5]. This section also covers an evaluation of the components

of autonomous vehicle communication systems and the security threats to these components. Besides, in Section 3, the techniques to protect autonomous vehicle networks from these threats are discussed. The taxonomy and solutions to minimize cyber security threats to autonomous vehicle networks are also dealt with in this section. In Section 4, the proposed contribution is extensively described, whereas the simulation environment and the results of simulation are presented in Section 5. The next section has the discussion and conclusion. The real-world issues and the significance of solving them, the implementation of the contribution in the real-world, and the limitations are discussed in the next section, followed by a section of conclusion.

2. Fundamentals of Cybersecurity in Autonomous Vehicle Networks

Based on the security requirements proposed by the automotive industry and the advantages of the hard real-time processing abilities of neural networks, the potential solutions highlighted in this paper points to the use of deep learning based security solutions for the automotive sector to realize intuitive deep learning based solutions for automotive security against passive, active and covert attacks. Research outputs will generate practical security solutions for automotive electronics in its entirety, in addition to the CAN network. To realize an end-to-end deep learning based bonding solution for cybersecurity to secure automotive components and ECUs, research outputs will target Cortex-M, Arduino, ESP866, and AVR microcontrollers in both standalone and networked environments. This solution will ensure that deep learning based security can be integrated with access, fragment, authentication, and intrusion layers and IoT devices to form a safe and secure smart automotive ecosystem. To improve the efficiency of the security solutions, future work will aim at realizing a hardware software co-design solution that will drive the deployment of deep learning based automotive security solution from being only active detection system designed during the research to a fully integrated system for bonding and detection of cyberattacks.

Self-driving vehicles or autonomous vehicles have gradually developed in various parts of the world [9]. As a new carrier for commuting worldwide, the rapid changes in the development of such vehicles have played excellent effect in various scenarios such as managing traffic, finding parking space, and assisting autonomous vehicles in traffic accident avoidance. The advent of autonomous vehicles fundamentally fits into the occurrence of ICT [Information and Communication Technology] technologies. It combines AI technology, big

data analysis, Internet of Things (IoT), cloud computing, 5G communication technology, and other high-tech to control vehicles and achieve autonomous control of vehicles just like the human brain. This work breaks tradition. We utilize self-driving intelligent vehicles, which are both traffic participants and wireless mobile hosts in vehicular networks. Through wireless communication between different intelligent vehicle networks, a vehicle cluster-based security mechanism is designed to ensure network security of the intelligent vehicle network, which fundamentally solves the shortcomings of traditional tracking security measures, and improves communication interception during communication. The network security functions are realized through relevant new systems, modules, and software platforms and other research technical means.

2.1. Overview of Autonomous Vehicle Networks

The highway is a holy grail for a driver where the featureless terrain and less distractions facilitate cognitive functions. The autonomous driving (AD) task pertains to robust and reliable performance in the challenge of AD and multi-robot system coordination for safe operation and minimal problem resolution time in case of a failure [10]. The onboard sensors such as Light Detection and Radar, Cameras, and Inertia Measurement Units process the live signals and send them via a local wireless network which is protected by standard UMTS, GPRS, GSM, or LTE over a SIM modem. The wireless back-haul (WiMAX, Long-Term Evolution (LTE), or usage of dedicated frequencies for Uplink and Downlink) networks are used for network establishment for centralized and/or edge computing applications. For example, LTE based manufacturers of automotive industries provide the authorized manufacture options further as data consumption options, i.e., unlimited, 3GB, or 5GB, and it also provides information on the data usage to the user for connectivity management purposes. For autonomous driving in the public space, it must not cause privacy invasion of bystanders. The major disadvantage is that the data cannot be aggregated and correlated across the multiple vehicles. This approach is inefficient and has security implications on Data-Consumption [11].

Autonomous Vehicle Networks (AVNs) are a novel concept that does not have an established architecture similar to the traditional TCP/IP protocol stack. AVNs are made up of three main parts, namely Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) communication interfaces with Device-to-Cloud (D2C) gateways. The core functionality of AVNs is to provide navigation through interconnected links, perform data

processing and smart sensing, and automate the decision-making tasks for the passengers [12].

2.2. Cyber Threat Landscape in Autonomous Vehicle Networks

Information is sent in two ways between ECU's in networks which belong to two different Abstracted Physical Layer (APL) categories, namely, not extended – APL_C and extended – APL_A. Both of these layers are backward compatible to the Classical CAN. Hence, network segregation and use of the functional constraints can provide base layer security against known APL limitations. Safety is the core design in autonomous vehicle networks, but the core problem is then at obstruction, defense and mitigation levels. The detection, identification and verification of admissible input is not identified before a decision is taken. This imposes an opportunity window for an attacker not only to attack the network but also the decision making process. Microlevel Detection and Defense (MDD-D) 2 has considered navigation system attack by the jamming of GPS signals. But both subsystems are sound when they work, and the at- tween, relevance of the detection and defense layers has not been explored. Vehicular re-routing challenges and security challenges in the absence of integrity checks in sensor inputs using a CCN, are also challenges that still need to be addressed in multicore integrated electrified autonomous vehicles [13].

The evolving cyber threat landscape in autonomous vehicle networks can impact vehicular safety, encompassing sensor-level attacks, network level threats and attacks on networked vehicles. The automotive industry is heavily influenced by external factors such as strong competition among industry stakeholders and the introduction of autonomous driving technologies. Hence, security is typically addressed using existing legal standards and regulations. An additional fear is that the technology is affected by vulnerabilities and, hence, can be attacked. Physically actuated attacks are possible through sensors and actuators based on radar, LiDAR or cameras. Over-the-air attacks are possible by radio frequency vulnerabilities and via V2X technology. The society is influenced and more vulnerable due to the adoption of more semi-autonomous and fully autonomous vehicles into public networks as attackers can impact multiple targets. Cybersecurity threats will remain for a few centuries to come and, hence, it's a case of when an attack will occur rather than if an attack occurs [5].

Adaptive Threat Response Mechanisms for Cybersecurity in Autonomous Vehicle Networks Sections 1.1– 1.4 provide a concise overview of the evolving cybersecurity requirements in modern vehicles [14].

2.3. Key Principles of Cybersecurity

[8] In-vehicle networks are used for communications between typical electronic control units (ECUs) within a vehicle to perform specific functions, such as controlling an engine, and are systematically specified via the standard called Controller Area Network (CAN). This standard is designed to support in-vehicle real-time and safety-critical communication by broadcasting information to all receivers effectively and flawlessly. However, CAN is considered to be vulnerable to different types of attacks due to its basic design to minimize the complexity of a standard and to ensure compatibility among different manufacturers' products. Therefore, it is crucial to offer comprehensive security services through making the communication secure, establishing enhanced security services like authenticity, confidentiality, data origin, and data integrity, and offering suitable cyber-attack detection and prevention schemes.[15] With the need for additional bandwidth and the trend in integration toward complex applications, current in-vehicle networks face a bottleneck of insufficient bandwidth for handling high traffic bulks, especially with an increase of onboard advanced driver assistance systems of modern vehicles. The new in-vehicle networks are expected to provide additional bandwidth and improve data stream management for handling those future applicative requirements beyond the challenges with the traditional in-vehicle networks. The future networks are also expected to provide comprehensive services towards security and safety assurances due to the fact that out of vehicle networks are becoming increasingly interconnected with a huge number of heterogeneous entities. Homogeneously, cybersecurity becomes an established challenge in-state-of-the-art in-vehicle networks and in future in-vehicle networks. The primary communication protocol for future in-vehicle networks is automotive Ethernet, which is deterministic, is capable of integrating different traffic classes over a single link, allows direct connectivity to external networks through TCP/IP and UDP/IP protocols, and covers the basic requirement of confidentiality and integrity by basic protocol extensions towards Unique IDentifier (UID)-based security. Though, new requirements for Vehicle-to-Everything (V2X) standards and in-vehicle autonomous driving call for network designs with the integration of real-time traffic, mission-

critical traffic, and best-effort traffic of diverse traffic patterns which are not supported by automotive Ethernet in its current form.

3. Adaptive Threat Response Mechanisms

Moreover, the completion of one cycle of a series of probe, mitigate, and classify responses will elicit a response log for the adversary and all the system states before, and after the appeasements were neutralized, i.e. system states achieved after applying the adaptive response. This selection of two adjacently logged system-states as responded and pre-responded states respectively in the system-context, will enable the creation of separate classification methodologies based on the system log being evolved and non-evolved giving each of them an equal chance to depict the statistics. This classification will provide us tools to expose the lurking adversarial response which has a chance to be overlayed with the normal intrinsics i.e., if, the computer adversary starts to jam the communication signals upon signal flow detection, ambiguities might arise due to dominance of other normal system response on the confusion matrix of the classifier. Hence, we should empirically get the handling by decision criterium for system ambiguity cases by running the AdaBoost classifier that assigns weights to the risky misclassified class, i.e., updates according to the higher false positive response. Also, alternatives can be used to do damage control and eliminating the noisy false positive response from the output of the classifier using the katalable approach in the evolved log of the simulated environment.

[4] Once a cybersecurity attack has been detected in an autonomous vehicle, it is of paramount importance to respond to the same in an extremely swift and reactive manner. It is imperative that the adaptive threat response mechanisms that are put into place beforehand must effectively respond accurately to the threat by initially taking evasive actions which isolate the threat from causing further modifications and damages to the autonomous system and finally an intricate probing can be invoked to delve deep into the vulnerabilities which were rendered susceptible by the adversarial exploit. The prominent challenge in developing responsive countermeasures in this adaptive threat response system is to ensure minimal side effects and false positives [7]. An effective methodology to achieve this would be simulating these response mechanisms together with the vehicle systems to fine-tune the lower-level vehicle systems in such a way that the effect of the mitigations on the normal operation of the vehicle will not have any significant side-effects. A time-delayed and lowered-risk set of

response mechanisms would enable the designers to continually probe at the lower underlying flaws that were exploited by the attacker in the adversarial exploits.

3.1. Real-Time Threat Detection

Not just the assumed semi-privacy issues and importance of quick online communication in traffic make it necessary today to connect personal vehicles, but it requires it more technically and directly is involved in the highway-safety subsystems. In reality-UN High-level experts have experiences about vulnerabilities in the interconnected and nearly-automated I-o-T highway systems that have not only driver assistance systems, but problems in their algorithms are more dangerous than human drivers. The companies that manage automated system risk management express more than once that although H-VAC or EMC failure can be handled with well-prepared, the system'd cybersecurity is harder to reveal and solve, and such systems cost much more for companies. Still, international corporations all agree in an already started innovation-accelerated () race towards the uprise the prices of the systems and applications enhancing automotive system cyber-resilience [16].

Current computing infrastructures and software systems are augmented with so many interconnected systems that are necessary to work with minimized human supervision, like public cloud systems, web 2.0/3.0, I-o-T and ironically, the automotive industry required most of these requirements long ago [4]. It requests changing software and system architectures, the new productivity standards, algorithm improvement to satisfy the energy limitations, and the main point, making redundancy and replacing human monitoring to computer-based continuously-learning risk estimation, avoidance and even incident response systems testing presented operational defined, standardised methods. This paper is only a short elemen-tary sketch to start discussing the aspect, how to roll out a new and integrated application and infrastructure level computer-generator security support for Level 4 autonomous vehicles [17].

3.2. Dynamic Threat Analysis

Dynamic actions, modification of the knowledge which is required is a good option in autonomous vehicle systems to stop the arrogance of the intensity of the attack. If the threshold has reached a level then software can trigger with automatic action. Moving Target Defense (MTD), Cyberspace Mimic Defense (CMD) and Cyber Deception are mainly used paradigms for vibrant defense mechanisms [18].-decisive action which is performed silence

and quickly which cannot be active with 5G, SDN, IoV & IoNT rough macro primary devices. What our thought model must have the security refinements for both certified the dynamic stability of secure multi- Identifier Networks.

Security mechanism that is developed should be driven based on uncertainty. Risk should be controlled and managed in the new emerging system. In autonomous vehicle, it is a must to have a system that can respond to decrease and notify the potential chances of threats [19]. Dynamic model can be applied in cyber security risk assessment to obtain the effectiveness of the overall process to check if it is suitable for the autonomous vehicle system to control and manage the risks. From the set of best methodology and local models there can be nice selection of those systems who can resist the cyber-attacks. The dynamic defense mechanism with proper risk measures should be engaged in the system. The protection need to be done based on multi-identifier network addressing paradigms. The system has to take its own decisions in response to the new cyber-attacks.

Adaptive threat response mechanism in which real-time cybersecurity threats are analyzed and immediate actions are taken to defend the system in an autonomous manner is essential for the flourishing of autonomous vehicles technologies. The autonomous vehicle must continuously assess the risks, implement necessary actions, and update the knowledge in real-time scenario. Applying the In-Motion Cybersecurity (IMC) concept we presented an approach in where the security algorithms enhancements are done dynamically in real time. This type of dynamic enhancements can provide a very strong adaption identifying and fixing vulnerabilities in run time effectively [20].

3.3. Adaptive Response Strategies

A hijacker wishes to increase his level of power by taking maximum possible control over as many vehicles as possible in [17] the network, causing at the end of one scenario different threat levels (from less serious to more serious); first, with 7 vehicles at risk, it can be stolen informational data such as vehicle identities and traffic data, but vehicles stability and comfort are guaranteed; with 1 or 2 risk at level 2, it is possible to take control of the programmed destination or take some brake or steer actions that even lead to a collision; when 89 vehicle are under control, all movement capabilities are affected pushing collision happening, for the highest level of 5 that her attacker can be made to pay diverting the vehicles towards high density places as for the sidewalk. In previous sections, physical, traffic and network related

threat levels were discussed together to evaluate their safety level, respectively. The analyzed scenarios start from the assumption that the attacker is able to control the entire V2V network, even though this is not technically possible. However, in basic safety messages, there are no authentication, encryption and integrity mechanisms. Therefore, every node is assumed to be trusted and is not able to detect false information carried by malignant messages (Sybil attack), making them open to all possible network attacks concerning physical threats. In [21] the scenario of a MAC layer DDoS attack aimed at causing a channel saturation, with the subsequent difficulty to send/receive real warning or message. In [18], moving along the system flow, the resilience and response mechanisms proposed are only defensive: the control unit is consequently oriented only to minimizing the impact of the consequences of the thread. It is important to underline that, the main technical characteristics, advantages and disadvantages of protocols are meta-features that constitute the system exposure to cyber security threats. Consequently, an opaque analysis and a high level considerations in the future can stress this assembling of responses because, if responses to threats have originated from systemic features, also other consequences (backfire) related to the use of adaptive responses could emerge to generate possible more potentially relevant threats [5, 66].

4. Case Studies and Experiments

Among the 15 major attacks that are mentioned in the, the Denial of Service attack (DoS) affects the network connectivity of vehicle directly and affect the driver's safety too. With other words, this type of cyber threat can affect the driver's experience directly and considerably. As has been stated in the DoS attack, the jamming of the system has been occurred by sending the multiple collision of packets to the switches and result in the loss of desired routing information where can significantly affect the reliability of the autonmous vehicle to road networks. Therefore, it is critical to have an adaptive threat response mechanism protocol that can respond to different cyber-threats in IVN and mitigate the impact of attacks immediately. There are three ingredients main mechanism that all of them are based on the challenging research questionnaire in adaptive cybersecurity design for autonomous vehicles [22].

Intelligent connected vehicles (ICVs) are expected to be an inevitable trend of future development. As ICVs are equipped with advanced communication technology, computational ability, and controllers, research evidence showed that In-Vehicle Networks

(IVN), Vehicle-to-Vehicle (V2V) communication, and Vehicle-to-Infrastructure (V2I) communication are more frequently become skeleton ground for potential cyber-attacks where the main motivation is to invade the confidentiality, availability, and integrity of the systems that finally underline the reliability of the one of the most important components of smart and intelligent transportation system. The most important part of the autonomous vehicles cybersecurity is the detection mechanisms or countermeasures that is built-in and continuous monitor the IVN of the driving system. Therefore, due to the high volume of packet that is transferred in a very small time and the limitation in the CPU and memory areas of ECUs, by considering the hardware limitation and cyber threats' nature, the design novelty becomes the main part of the cybersecucrity developed for autonomous vehicles [23].

4.1. Simulation Environments

The research represented in reference [24] featured a minimal SystemC environment for connected vehicles with three different modes: normal, attack (IDS), and response. In the IDS mode, the attack detection time is fixed at 100 ms, while in the response mode, the anomaly detection time is modified based on the adaptation algorithm. Attack detection is based on a specially designed watermark in the data packets. Once an anomaly is detected, one of the fictional responses (releasing the smoke, notifying the network components, and receiving response from the authorities) and two authentic responses (false data modification) are randomly selected and applied to the environment. Characteristics can be added to analyze the effect of the network size, number of vehicles in the network, real-world traffic patterns, and realistic attacks by generating a more realistic dataset through Man-In-The-Middle (MITM) attacks and using an enhanced attack and response model.

The research featuring in reference [25] has disclosed an open-source testbed for connected vehicles, where various realistic threat scenarios can be simulated to evaluate different anomaly detection techniques. This testbed can be used for quantitatively evaluating the performance of different adaptation mechanisms, such as receiving response from the authorities, releasing false smoke, notifying the network components including the other vehicles and roadside units through the security operation centers, and modifying the network component's behavior [17]. Therefore, this testbed can be used to answer the research question of how to measure the performance of different adaptation algorithms in terms of different type of response? What are their trade-offs, and how can we quantify and combine different performance measures over time and/or space?

4.2. Experimental Setup

In our experiments presented, our main objective was to investigate the extension to our prior work where we compare different methods to deploy a network robust consensus protocol in a recursive manner over an important case study: the leader election problem for a network of Autonomous Vehicles [19]. The simulator model is based on the "pyAIV" simulation platform, that implements a complete autonomous vehicle multi-agent based system, and uses SUMO to model the roadway system and integrates route control algorithms to support AVs controlled mobility. In future directions, the behavior of recursive protocols in the presence of competing adversaries will be part of the two-steps robustness evaluation of such protocols, the sum of a previously developed network level reachability study [2]. Moreover, The dependence of the robust leader election algorithms proposed by the authors on the graph characteristics of the initial network is being currently minimized.

Cybersecurity in autonomous vehicle networks should be considered from a network context, i.e., madly distributed, inherently heterogeneous, and restrictive in terms of communication and energy resources [16]. A highly distributed defense system can be considered, but this requires a central management and control system, which is fragile. In fact, the failure of a single control entity can lead to a general failure of the entire defensive network. Therefore, in the good architectural defense system process, an accidental attacker should have the central structure operational on ad hoc devices. If the replication mechanism generates only as many subaccurate systems as necessary according to the state of the attack, making the attacker as confused as possible about the logical and geographical position of the defensive structures, this can be considered an optimum strategy is the fluidity of the attack, which requires real-time dynamic response both in the network and in the node of the devices, capable of communicating with external components (peripheral transactional systems).

5. Evaluation Metrics and Results

The helper system works on punctual, circumstantial conditions, taking carefully scheduled action in the event of an adversarial attack, characterized by JFR (Section Sundials with the cyberphysical formulation in System Set-Up) or TopD Cyb (Oppositional Odds with the incorporated RNN-LSTM networks in Section We approach the Helper System task functionality from a data-driven standpoint in Methods, where we offer a delicate bottom-up deep learning approach.\helpersystem). Therefore, we deploy sets of formulations frequently

used in the contemporary control literature and plausibly accessible empirical data. Lastly, we observe that our perturbations are perturbations about the eager solutions, even though we use a rudimentary set-up.

This helper system steadies headways between the ego vehicle of the system and the preceding vehicle in the absence of adversarial attacks. However, as soon as an adversarial act is cast, the system demographics, separately characterized as JFR attacks, or Cyb attacks, instantly respond by changing the observable variables (the d, d_t, and dʊ states). For Dynamic Situational Awareness (DSA) to act on them, these cases are propagated down to it, where they are resolved. Finally, in the presence of time headways, relative velocity, and the acceleration calculated from the stable information, the default Adaptive Cruise Control (ACC) controller finalizes the target acceleration as the input for the cyberphysical vehicle model.

The proposed network defense mechanisms for autonomous vehicles with a known threat and attack goal start by configuring the set of parameters P for our experiment. The list of parameters, i.e., P, is given in Table 8. These parameters cover various functionalities from the original CACC controller and our proposed sensor and control resolver-based defense mechanisms (for both JFR and Cyb parameters), as well as our top-down and bottom-up DSA approaches. For each configuration of P, our evaluation study initializes the attack road parameters (from Table 9) and our model-based perturbations as discussed in our extended defense mechanisms in Sections 3.4 and 3.5. The evaluation study begins by launching the vehicle in a closed-loop simulation, modelled in our cyberphysical simulation environment, within a 5 km long highway with open boundaries. The We decouple these sections using the autonomous vehicle following traffic stream study.

5.1. Performance Metrics

Collective threat intelligence measures the effectiveness and success rate of cyber threat analysis and response. In the era of autonomous and automated systems, self-defending critical infrastructures require advanced cyber-threat intelligence adapted with artificial intelligence. Adaptation of real-time cyber threat response in automated information systems may generate proactive and adaptive cyber-security behavior. This work provides a futuristic study on the potential methodology to build an adaptive approach for the analysis and response protocol to curtail the multi-directional cyber threats affecting the operation of

critical systems [19]. Due to the future hypothesis of the automotive vertical industry, Autonomous Vehicles (AVs) require to operate without any human interventions, such as intervening the Autonomous Vehicle Network (AVN), preventing the future possibility for more innovation and more frequent accidents. This contribution focuses on an architectural and analytical survey that involves the recent challenges in the automotive vertical industry, models the potential cyber attacks on cellular network-based communication, and thoroughly migrates the use cases and results in the open-source software-based network simulation environment (SDNB

Protection and security are currently two main aspects of future systems such as Autonomous Vehicle Networks (AVNs) as they are prone to malicious attacks, leading to complex, already known or even new vulnerabilities [26]. An effective way to protect AVNs from this attack is through the use of adaptive threat detection and response mechanisms, where the system can adaptively adjust to its environment by analyzing, monitoring, and sharing information efficiently about security threats [27]. There is a gap in the literature where all the open-source software-defined network-based architectures have been proposed for an AVN with an adaptive threat detection and response mechanism. This article provides a comprehensive survey to address this gap by first, a discussion of a few recent attacks against the communication networks in an autonomous vehicle system, and second, a resettling the existing state-of-the-art schemes in a unified framework.

5.2. Case Study Results

In these case studies, we simulate four scenarios using two ADASs (including co-ADASs, hierarchical ADASs) and a software program (SW-theft) on a controller area network (CAN) network to emulate four representative situations of autonomous vehicle networks. Among the scenarios, the initial attacks on adaption mechanism and functional safety on ADASs are the major goals and, to implement the attack, active injectors are utilized. Where the two kinds of scenarios are categorized as: synchronic Scenario between ADASs (SADS); collaborative Attacks on ADASs (CAADAS). Also, we developed the two semantic hierarchies outer for SADS and CAADAS in section 4.5.3 and give the results and analysis in section 4.6. In this section, we will explain the simulation environment in detail, which is followed by implementation of attack scenarios and application of the adaptiveness and threat response mechanisms [25].

Text: To verify the effectiveness of the five proposed adaptive mechanisms, we perform four related case studies in Section 5.2. In the case studies, we use two advanced driver assistance systems (ADASs) and a software program on a controller area network (CAN) network to emulate four representative scenarios of autonomous vehicle networks. The attack both the adaption and the functional safety of the ADASs, and we opt for two kinds of scenarios to verify the effectiveness of the proposed mechanisms.

6. Discussion and Future Directions

Then, standard SIR-model to allegorize the interaction process between information and epidemics, through power structure topology networks, makes one wonder about the correlation existing between disseminators and responders nodes. Nevertheless, topologies with a known origin i.e., regular lattices, in practice often fall into communication issues because of their reduced variance and the small amount of compatible possibility events for message routing [19]. So, one can then think about whether or not large-scale network epidemic spread are always bound to be strong spread on small-worlds. Disconnecting the small world network information diffusion process, different influence activities of the two classes of nodes are not correlated for any value of γ. As convergence transitions for a susceptible node can be related to a vanishing epidemic threshold and, indirectly, to the collective behavior, we complete this study by investigating different strategies including greedy path strengthening.

The most novel contribution of the paper lies in endowing the distributed DAE with the ability to respond to unreliable network channel messages using DRMMLEs. By small worldness, we mean that the responder nodes collect trajectories of data about the surrounding network nodes for making response decisions, either through hierarchical activity or collectively through parallel computing [28]. Moreover, the regular lattices show a moderate adaptation range, i.e., only neighboring nodes are involved in message exchange. On the other hand, actual small world networks evidence know-how for different γ comparable to small world networks. Moving deeper, the mechanism is observed to be a critical capability, which allows nodes to adapt their strategies many small world networks use stochastic mechanisms for the movement rules on simple random walkers.

6.1. Challenges and Limitations

One substantial challenge in developing adaptive security mechanisms involves the challenges in collecting real-time oriented reliable data in extremely dynamic and uncertain threat environments; traumatic domain experts experience are mostly not capable of providing true reflections of adaptive security suitable for autonomous vehicle networks due to their limited abilities to handle and comprehend this volume of data and variation. Another dimension brings to light the challenge associated with randomness of cyber-attacks and managing its severity and swift transitioning stance in autonomous network systems. [17] A major limitation of the response procedures configured in conventional cybersecurity systems is that they are often pre-defined and rely on known attack scenarios and response patterns available in the databases (if any). The ability to modify response procedures dynamically, based on intrusions that occur in real-time, is poorly defined in the adaptive cybersecurity field yet is critically important.

[29] [10] Despite being able to leverage robust threat intelligence methodologies, conventional cybersecurity solutions face several limitations in relation to fielding effective security mechanisms able to detect and respond to a continuously evolving and stealthy threat environment. Adaptive measures for autonomous vehicles are even more critical since they do not have the luxury of human intervention, in the midst of automotive cybersecurity incidents. Moreover, the use of adaptive measures can greatly minimize the need for redundant infrastructure footprint, allowing the autonomous vehicle to operate with smaller security implant while maximizing operational security. Implementing and deploying an adaptive system assures faster vehicle recovery time which is extremely critical.

6.2. Future Research Directions

In the domain of finding a secure connected vehicle network, the work of present deep learning is very integral. The vehicle security attacks are one of the remarkable domains that newly transformed the cities with the aim of smart cities in the various domains. In conclusion, a thoroughly understanding of each issue has been addressed in the domain of connected autonomous vehicles and identified the latest security challenges and protection measures. Safety challenges: Ensuring that the autonomous drone system will offer physical safety and affordance requirements in normal and dangerous settings and privacy requirements need to be designed. [11] IOT technology in adverse conditions like human abuse, such as tampering and hijacking, demands the rectification. Doubtful functional requirements for these ideas can

be included in the class of developing secured real-time processes, trustworthiness assessment, communication techniques that circumvent eavesdropping, and privacy preservation frames. Additionally, CAE technology can address security issues at the vehicle and supply chain level, and concern at the data collection factor, which can also be included. In the future, technical issues related to vehicle security and incident anticipation should be performed and experimented with, with additional emphasis on intervention mechanisms and smart private data management taking into account consumer protection agendas.

The transformation from modern automation technologies to autonomous systems has made a drastic impact in the domain of technological advancements leading to considerable changes in the domain of numerous services and investigating alternatives for unmet enhanced revolutionized concepts. [12] The connected autonomous vehicles provide remarkable benefits, such as assessing all the possible feasible routes to evade unwanted circumstances and high congestion. However, the associated technological advancements lead to new security issues and vulnerabilities. The connected autonomous vehicles network converging communication and control architectures makes it access from the treasure for the attackers and makes it highly vulnerable to various attacks such as automated driving attacks, autonomous physical layer attacks, jamming, and eavesdropping. In the context of urban smart mobility, the group of autonomous cars engaged in vehicular networks is one of the remarkable domains that got significant interest from the research community. However, the connected car vehicles are highly vulnerable to various security attacks. Consequently, the objective of this domain of autonomous connected cars is to strengthen the mechanism for securing the network solution in terms of preserving the security, privacy, and security of the autonomous vehicles.

7. Conclusion

The framework presented in [10] consists of a reconnaissance phase where an attacker scans the network of the target vehicle system, a penetration phase where the attacker tries to exploit vulnerabilities, a lateral movement phase where the attacker moves from one service to another in the network and, finally, the second phase of exploitation where the attacker tries to affect the connection between vehicles or the vehicle and its infrastructure. Additionally, an evaluation of the classification abilities of each IDS/ICA is carried out under F-measure, Precision, Recall evaluation criteria. The claimed use-case of this framework, especially in

terms of the consolidated approach of using an IDS with an anomaly-based and a statistical feature and predicting results through an ICA, is also shown to have an efficient performance; further shown through the tests that the hybrid IDS outperforms the individual and traditional as well as the established systems through advanced machine learning and classification techniques.

Since the implementation of autonomous vehicles is progressing rapidly, it is important to give cybersecurity measures a proportionate emphasis, as these operate in a highly dynamic environment with real-time data sharing, leading to increasing risks of cyber-attacks. Given the expanding attack surface with a potential to threaten safety, the responsible strategy is to drive the principle of resiliency, by moving from a pure preventive to a preventive-detective-adaptive response approach. Therefore, it is especially important that critical systems are shielded to be able to resist anticipated failure modes, attaining a given level of performance under cyber-attack. While classical sensor fusion algorithms diminish sensibility to sensor failures in a traditional approach, any loss of critical sensory information in a sensor attack might not be recognized as an attack, since the abnormality-based fault detection might not be able to figure out the location of malfunctions in case of overlapping issues [17]. Collaborating development of secure autonomous systems, SOTAs in cybersecurity of connected and autonomous vehicles is provided in a recent survey in terms of learning and recognizing attack patterns using machine learning-based security capture solutions.

7.1. Summary of Findings

The proposed CoorAP or CoAES could potentially be adopted for implemented in vehicular communication systems in the future. However, the Human-in-the-Loop aspect must be carefully considered to avoid creating a singl orve trust a single points of compromise with any decision-making algorithms being implemented. [29]. To ensure data privacy and security, safe and secure communications across vehicle networks must be guaranteed between vehicles using different intrinsic features or global positioning system (GPS) based localization algorithms in order to dispatch law enforcement officers in the event of an ongoing hijacking cyberattack. Data captured by the RTTI security system has comprised the following: detection of cyber-attacks and unwanted attacks; the bandwidth consumed by each cyber-attack; and the patterns of cyber traffic during normal and abnormal conditions [30].

Security measures during communications in V2V/V2I and allowed communications only between trusted parties [31]. Use of AI/ML incr inventory demands. Threat Attack Victim Network Violations Example CyberAttack Network Traffic Online Traffic Resources Privileged Actions Data Crash Tamper Black/Gray Box No No Depending on the Attack Type Partial Denial-of-Service, Loss of Network Communication when Vehicl Collision Can Happen Identification of the Victims Based on Cyber Attacks and Classified as Ctrl, Sensing, Illegal request or Snrs, Vehicles, Traffic systems Lot of Trust is Consumed Insecure/Patient When the Attacks Break some Critical Ding Data, then It Is Considered as the Victim.

7.2. Implications and Recommendations

In [10], it is argued that the race among automotive companies and suppliers on releasing newer and smarter vehicles should be thoughtfully balanced with security risks that appear at the same pace. As numbers of modern vehicles become connected, intelligent, and eventually autonomous, existing and new threats make the cyber security of vehicular systems a very challenging domain. Collaborative and connected adaptive threat response mechanisms for ensuring security of autonomous vehicles as part of vehicular networks, particularly scenario specific and context specific, are briefly demonstrated using a global perspective in [12].

[29] In this paper, we have discussed the growing concerns in the cybersecurity of infrastructure, communications, and data of vehicular networks against various types of cyber attacks. Vehicles in autonomous mode become more prone to such attacks, which can have serious consequences including human casualties. With the rapid development in automotive technology, the attack surfaces of cyber threats have also expanded. The 5G and 6G mobile networks, Internet-of-Things, infotainment and navigation systems, smart junctions and nodes, roadside units, and cloud computing platforms are a few examples of highly vulnerable context.

8. References

1. [1] M. B Jedh, J. Kai Lee, and L. ben Othmane, "Evaluation of the Architecture Alternatives for Real-time Intrusion Detection Systems for Connected Vehicles," 2022. [PDF]

2. [2] T. Wang, M. Tu, H. Lyu, Y. Li et al., "Impact Evaluation of Cyberattacks on Connected and Automated Vehicles in Mixed Traffic Flow and Its Resilient and Robust Control Strategy," 2022. ncbi.nlm.nih.gov
3. [3] 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
4. [4] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
5. [5] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
6. [6] K. M. Ali Alheeti, M. Shaban Al-ani, and K. McDonald-Maier, "A hierarchical detection method in external communication for self-driving vehicles based on TDMA," 2018. ncbi.nlm.nih.gov
7. [7] S. Park and J. Y. Choi, "Hierarchical Anomaly Detection Model for In-Vehicle Networks Using Machine Learning Algorithms," 2020. ncbi.nlm.nih.gov
8. 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.
9. 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.
10. Mahammad Shaik. "Rethinking Federated Identity Management: A Blockchain-Enabled Framework for Enhanced Security, Interoperability, and User Sovereignty". *Blockchain Technology and Distributed Systems*, vol. 2, no. 1, June 2022, pp. 21-45, https://thesciencebrigade.com/btds/article/view/223.
11. [11] 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
12. [12] S. Paiva, M. Abdul Ahad, G. Tripathi, N. Feroz et al., "Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges," 2021. ncbi.nlm.nih.gov

13. [13] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]
14. [14] R. Changalvala, B. Fedoruk, and H. Malik, "Radar Data Integrity Verification Using 2D QIM-Based Data Hiding," 2020. ncbi.nlm.nih.gov
15. [15] S. N. Saadatmand, "Finding the ground states of symmetric infinite-dimensional Hamiltonians: explicit constrained optimizations of tensor networks," 2019. [PDF]
16. [16] Y. Mei, "First-order coherent quantum Zeno dynamics and its appearance in tight-binding chains," 2023. [PDF]
17. [17] M. Hamad, A. Finkenzeller, M. Kühr, A. Roberts et al., "REACT: Autonomous Intrusion Response System for Intelligent Vehicles," 2024. [PDF]
18. [18] Y. Wang, A. Smahi, H. Zhang, and H. Li, "Towards Double Defense Network Security Based on Multi-Identifier Network Architecture," 2022. ncbi.nlm.nih.gov
19. [19] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]
20. [20] M. Hamad and S. Steinhorst, "Security Challenges in Autonomous Systems Design," 2023. [PDF]
21. [21] A. Jafar Md Muzahid, S. Fauzi Kamarulzaman, M. Arafatur Rahman, S. Akbar Murad et al., "Multiple vehicle cooperation and collision avoidance in automated vehicles: survey and an AI-enabled conceptual framework," 2023. ncbi.nlm.nih.gov
22. [22] D. H. Lee, C. M. Kim, H. S. Song, Y. H. Lee et al., "Simulation-Based Cybersecurity Testing and Evaluation Method for Connected Car V2X Application Using Virtual Machine," 2023. ncbi.nlm.nih.gov
23. [23] M. Dibaei, X. Zheng, K. Jiang, S. Maric et al., "An Overview of Attacks and Defences on Intelligent Connected Vehicles," 2019. [PDF]
24. [24] V. Zieglmeier, S. Kacianka, T. Hutzelmann, and A. Pretschner, "A Real-Time Remote IDS Testbed for Connected Vehicles," 2018. [PDF]
25. [25] P. Meyer, T. Häckel, T. Lübeck, F. Korf et al., "A Framework for the Systematic Assessment of Anomaly Detectors in Time-Sensitive Automotive Networks," 2024. [PDF]
26. [26] S. Boddupalli, A. Someshwar Rao, and S. Ray, "Resilient Cooperative Adaptive Cruise Control for Autonomous Vehicles Using Machine Learning," 2021. [PDF]

27. [27] N. Chinpattanakarn and C. Amornbunchornvej, "Framework for Variable-lag Motif Following Relation Inference In Time Series using Matrix Profile analysis," 2024. [PDF]
28. [28] S. Bagchi, V. Aggarwal, S. Chaterji, F. Douglis et al., "Grand Challenges in Resilience: Autonomous System Resilience through Design and Runtime Measures," 2019. [PDF]
29. [29] 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
30. [30] W. Payre, J. Perelló-March, and S. Birrell, "Under pressure: Effect of a ransomware and a screen failure on trust and driving performance in an automated car simulation," 2023. ncbi.nlm.nih.gov
31. [31] P. Marcillo, D. Tamayo-Urgilés, Ángel Leonardo Valdivieso Caraguay, and M. Hernández-Álvarez, "Security in V2I Communications: A Systematic Literature Review," 2022. ncbi.nlm.nih.gov