Adaptive Intrusion Response Systems for Autonomous Vehicle Networks

By Dr. Agata Grabowska

Associate Professor of Computer Science, Wrocław University of Science and Technology, Poland

1. Introduction

The Internet of Vehicles (IoV) and ITS work as a backbone for the integration of numerous services in data-centric applications associated with future communication paradigms. IoV is expected to offer a wide range of novel ITS driving services and different categories of informative data. That being said, securing the interactions within IoV remains a challenging problem, particularly with regard to effective security measures for various emerging communication paradigms [1]. Generally, to guarantee the authenticity, integrity, and confidentiality of emerging services within the IoV, many communication-centric communication protocols are secure. Usually, this approach of network-centric security paradigms does not offer a comprehensive security solution spanning to the entire forward signaling process of services. Nonetheless, a more diverse security strategy in the security ecosystem is needed.

Autonomous vehicles have proven their potential worldwide by overcoming a variety of challenges such as urban traffic congestion, pollution, traffic crashes, increased transportation, and on-demand mobility requirements [2]. A surge in demand for AVs has entwined these vehicles into the Internet of Things (IoT), Intelligent Transportation Systems (ITS), and Vehicle-to-Everything (V2X) eco-systems. This significant integration of AVs with other interrelated technologies has further led to cyber-security vulnerabilities, which in turn poses a serious threat to transportation technologies [3]. The in-vehicle electronic architecture and multi-level architecture make AVs an attractive target for cyber-attack activities. Due to their high complexity and a large number of Electronic Control Units (ECUs), an adversary can bypass multiple protective layers to achieve pre-set objectives. Thus, the absence of an effective cyber-security mechanism can threaten the swift adoption of AVs and V2X communication networks.

1.1. Background and Motivation

Autonomous intrusion response in a vehicle network supports a V2X-based vehicle protection system to a certain extent in addition to its interconnected characteristics as it can overpower other adversary vehicles. In this system, our goal is to develop a system level technology that operates fast enough with distributed architecture even if hardware is resource-constraint and that operates at each secure node such as an autonomous vehicle or a centralized security operation center. Machine learning methods which are based on the infraction such as Deep learning, 1-D/2-D CNN, and Convolutional-LSTM, which have learned parameters among the vehicle network attacks in the all-electric field, are utilized [4]. The introduced hierarchical model for characteristic features can manage and protect another autonomous control or driver by raising the additional integrity level. The accuracy of the presented model is comprehensively evaluated by the receiver operating characteristic curve and other metrics and is compared with the existing work.

In safety-critical autonomous systems like autonomous vehicles, the response to an attack is as crucial as detecting the attack itself [5]. Therefore, it is essential to devise a method to drive anomaly detection with other relevant hardware resources in vehicular in-vehicle networks. The failure of an electric controller can affect the brake system [6] and cause unintentional motions. To address this threat, a more fundamental solution is needed because the usage of a controller with the internet service only does not provide assurance for all-remote attacks, and the dedicated networks for the internet service are costly. Therefore, as a solution, it is proposed to realize and protect a flexible plot by integrating the machine learning in the in-vehicle system. In the present study, we developed a secure intrusion response system that is implemented by extending intrusion detection systems and provides real-time mitigation and visualization techniques for surveillance measurements for autonomous connected vehicles.

1.2. Research Objectives

[7] According to the articles, one of the major challenges organizations face in establishing the secureness of autonomous vehicles is to effectively prevent, detect, and respond to attacks aimed at disrupting the proper operation of the network and, consequently, increasing the potential hazards for passengers or other road users. Therefore, the overarching objective of this research is to design a set of security controls effective in counteracting a variety of intrusions—both known and unknown—in autonomous vehicle networks. More specifically,

I propose the design and test of the following system which will provide essential features such as anomaly-based intrusion detection, context-aware alert correlation, probabilistic risk assessment, intruder response, and autonomous intrusion adaptation.[8] To the best of my knowledge, this is the first attempt to realize a full adaptive infrastructure intrusion response system for autonomous vehicles which includes cybersecurity lifecycle management through a fully autonomous incident response system. This project is informed by cutting-edge advances in adaptive security systems and our noble need for autonomous vehicle cybersecurity, initiated by access to the relevant literature. However, my findings should be advanced and tested across multiple prototypical vehicle networks to confirm their effectiveness and their robustness to the potential dynamism of the operating environment. This research is targeted to both practical and scientific audiences. First, the impacts it has on two fervently thematic research communities— automotive networks and adaptive, autonomous incident response—will be transformative, contributing to advances in both fields. Second, by addressing any omissions made in prior research, contributing to the science of adaptive security and autonomy, and by becoming the only system in designed experiments to self-adapt during attack sequences, this research will serve as a source for important insights to re-invigorate the research question it asks and will potentially spawn future investigation.

1.3. Scope and Organization of the Work

Under this assumption, even though the intricate languages among autonomous vehicles are fenced within the wireless intra-vehicle sensor networks of an individual vehicle, these closed systems are supposedly invulnerable to outside attacks. This is an impractical assumption because the infrastructure will in reality involve numerous services that the vehicles will communicate with, such as the vehicle security operation center (VSOC), municipal control centers, other vehicles, traffic lights, and surveillance cameras. It is anticipated that vehicles and their infrastructure will be heterogeneous transparency sources involving mobile ad hoc networks and the wireless Internet communication. This innovation will provide a motive and opportunities for a multifarious array of potential cyberattacks against the control systems of each vehicle. These security threats will originate in diverse ways, such as the provision of forged information, cyberattacks against emerging application protocols that participate in communication, or the compromise of a few vehicles that then mount a distributed denial-of-service (DDoS) attack.

Autonomous vehicles are currently in their development phase, gradually progressing toward their ultimate goal of guaranteeing safe, efficient, convenient, and comfortable traveling experiences [4]. There is little doubt that autonomous vehicles will combine artificial intelligence, big data, and communication technologies in ways that promise to revolutionize transportation options. The crucial underlying assumption for the successful establishment and operation of a safe, efficient, and comfortable autonomous vehicle ecosystem involves the continuous real-time exchange of information among the vehicles using wireless communication technology [9]. This information exchange, coupled with the set of rules of the road that the vehicles must follow, will allow myriad vehicles to navigate both predetermined routes and spontaneous detours without colliding while traveling at speeds requiring relatively rapid decision making. For the majority of research on autonomous vehicles, vehicular control assumes the absence of external cybersecurity attacks [10].

2. Fundamentals of Autonomous Vehicle Networks

The paper organized as follows, In Section 2. Basics of the operations of autonomous vehicle networks and introduces the attack types could face these networks. In Section3, I presented the VIDS, in Section4, I presented the implementation and evaluation of an instance of VIDS called VIDS-A1, in Section5, In Section6, I concluded my work. Before concluding, I represented future work for enhancing the detection performance and proposing some applicable countermeasures against the attacks that happens in the AutV. [11].

Viewport-Based Intrusion Detection System to Protect the Autonomous Vehicle Networks FaridHadiji and Hassan T. Mourad [12], ViktorBalogh and AttilaBátky [9], I present a viewport-based intrusion detection system that monitors and analyzes data from a forward-facing camera of autonomous vehicles.Autonomous vehicles are resource limited and work in the real-time environment. These characteristics impose challenges on developing robust and high-performance cyber security techniques in managing network security. One Intrusion Detection System (IDS) for a network of autonomous vehicles is made up of monitoring the forward-facing view of vehicles called Viewport-based Intrusion Detection System (VIDS). I analyze different attack scenarios occurring in autonomous vehicle networks and suggest the types of virtual attacks that can be fought with VIDS.

2.1. Key Components and Technologies

Moreover, engine control units (ECU), steering/braking/acceleration system might operate in higher criticality levels in autonomous, connected or electric vehicles, especially remotely controllable and programmable ones. VANET communications are also vulnerable to DoS and resources consumption attacks. DDoS mitigation plannings that outperform classical defenses like firewalls are needed for secure V2X transmissions [13]. Anomaly attacks like replay attacks may compromise the road safety since digital evidence of vehicular communications and physical evidence in vehicles is essentia in case of collisions. False data injection and source authenticity attacks have devastating consequences. For example, location-spoong for a vehicle will let an attacker lead other vehicles into a trap. An attacker can also insert artificial traffic jams in order to disturb the equilibrium of the network and dare adversary vehicles to switch lanes into a possibly disrupted environment.

The connected and autonomous vehicles rely on different key technologies to perform a fully concrete and efficient ad hoc wireless communications that require mechanics of authentication, encryption, and data confidentiality and integrity. Undeniable authentication is the foundation for a secure data exchange agreement between the ego vehicle and its surrounding entities [14]. Adaptive and dynamic consensus-based authentication onledgers are suggested to prevent data-undermining attacks such as Sybil attacks on vehicular blockchain [15]. QoS-aware paradigm is proposed to optimize data delay and energy consumption for data exchange among entities in VANETs. Blockchain provides the overt potential of resisting stakeholders and outsider threats. Furthermore, safety applications in VANETs, where vehicles disseminate emergent dangers, require high trustworthiness and the European Telecommunications Standards Institute (ETSI) Cooperative Awareness Message (CAM) is the underlyinglomatic scheme.

2.2. Communication Protocols and Standards

A platoon network, like autonomous vehicle networks, mainly rely on wireless communication protocols and corresponding standards. There is an urgent need to transform the message communication layer(CAL) in the platoon network into a reliable and secure mayoral medium or system. The common international standard under the IEEE 802.11 registration group in vehicle local area network is the 802.11 p standard. Connection with cellular communication services provide long-distance communication. The most promising

upcoming mobile communication connection is the fifth-generation mobile connection (5G) [16].

A platoon network, like autonomous vehicle networks, mainly rely on wireless communication protocols and corresponding standards. There are specific communication standards available from society of automative engineers (SAE) and IEEE groups which are specifically designed to cater the requirements of the autonomous vehicles to work effectively [17]. The primary vehicular communication standards, which are relevant for vehicle to vehicle (V2V) and vehicle to infrastracture (V2I) communications, are dedicated short range communications (DSRC) and innocent wave. The use of any of these either standards is based on the content, location and technology used. The DSRC communication standards are based on the dedicated short range communications (DSRC) frequency which are unlicensed spectrum. The technical working of the DSRC standard is regulated by IEEE 802.11p and is specifically designed to cater the requirements of V2V and V2I communications.

3. Security Challenges in Autonomous Vehicle Networks

The crucial role of the physical security layer has been described [2]. Attacks like Digital Power Amplifier Impersonation and Voltage Glitching are indeed difficult to launch, however attackers have demonstrated their effectiveness against other chip design. Since these circuits are actually on each chip made by each vendor, they need to be robust against threats from adversary unlike traditional technique as part of TAMPER resistance in hardware penetration tests. Software security layer, represent the protocols implemented for Intrusion Detection System (IDS) over ECUs [18] inside CVs. A comprehensive literature review has been done. The limitations have been briefly mentioned without any Source presenting the solutions. Most software attack detection techniques are statistical anomaly detection methods and until peer reviewing, no efficient method has been proposed to detect this type of attack. The network layer has been discussed with a slight emphasis on distributed DDos attacks, vehicular botnet and jamming attacks. Next, a short analysis of application layer attacks has been analysed. This analysis contains SymakeA, gatekeeper, john the ripper, stegcracker, OpenSSL etc. These tools that have been recently updated to work directly with network data capture files. Vehicle network layer security where vehicles are communicating with neighbors using the ITS G5 DSRC protocol. For all these sections, the details of potential vulnerabilities of protocols in different layers and attacks that can exploit these vulnerabilities

are presented. A novel idea of leading phishing attack has also been explained orally in the thesis. Moreover, Rightclick and seccure algorithms have been explained. Introducing seccure algorithm for secure broadcast of the failed session key shows proposed a refined detection scheme with CDF shorter than earlier.

Vehicular networks differ from general mobile ad-hoc networks as vehicles exhibit highly dynamic movement patterns, vehicles stop frequently and the drivers speed up as the traffic signals turn orange. Nowadays, vehicular networks are also being considered in the domain of autonomous vehicles. Connected Autonomous Vehicles (CAV) technology brings complex security issues at various levels, i.e., vehicle level security, sensor data collection and processing, secure supply chain, etc. It is a necessary requirement in vehicular networks to rely on the technology based on security components including authentication and confidentiality in communication both inside and outside a vehicle network. Authentication has to be performed potentially at all layers starting with physical, data link and network.

3.1. Threat Landscape

A limitation of the landscape analysis and the intrusion report calculation (steps 1 and 2) is that we consider attacks one by one [5]. In practice, this could be incorrect as a sequence of attacks may be more harmful. Detriments suffered during an attack may influence future combinatorial attacks and sequential attacks may be needed to single out a vulnerable system from an adaptive attacker. Also, one might speculate if an intruder could use multiple tactical attacks at the same time. To fix these limitations, the temporal model in a general setting with many adversaries will be the subject of further work.

Since environments with a high density of vehicles hinder distributed coordination of the system, a natural idea for handling that network topology is to bridge careless nodes with more urgent vehicles [18]. Once a vehicle is attacked, in addition to its response, the revenant network dynamics are important because they will determine the success of the offending node. To further increase the resilience of the system, the last line of defense can be based on a firewall of selfish colonies. These colonies interfere with an attacker and they may become selfish when late or behaving badly in the first place. The fact that colonies, as well as brain-stem commands, are similarly manipulable opens up for future research in artificial intelligence which is devoted to the security of networked autonomous vehicles through dynamical-systems design.

3.2. Vulnerabilities and Attack Vectors

The main focus of attack vectors at the communication level is adversarial attacks such as jamming attacks and man-in-the-mi attacks. Many researchers in this field have proposed reliable and secure communication solutions to mitigate these types of attacks. For example, Balakrishna et al. propose a jamming attack detection and mitigation approach for connected and autonomous vehicles in. Kabil et al. propose a trust and energy aware routing metric for V2I in an urban VANET scenario. The main focus of attack vectors at the data-link layer is attacks on the Time-Division Multiple Access system and the Binary Phase-Shift Keying modulation system. A none of the above cross-layer security approach for the physical and MAC layers of connected vehicular content requests is proposed by Sangaiah et al. by Chen et al. present the design and evaluation of a smart attack defense strategy for VANET.

Attack vectors for connected and autonomous vehicular systems mainly include field area network (FAN) protocol level vulnerabilities, communication-level vulnerabilities, and data-link layer vulnerabilities [19]. Our usage of the term 'vulnerabilities' remains consistent throughout this paper. The main focus of attack vectors at the FAN protocol level is the 5G-V2X (Vehicle-to-Everything) communication system, with typical attack vectors including eavesdropping, false data injection, and replay attacks. Many researchers have studied these security problems. For example, Sivanathan et al. propose a secure FAN protocol for connected and autonomous vehicular systems in [20]. Yang et al. propose a secure in network cache for connected and autonomous vehicular systems in [21].

4. Intrusion Detection Systems for Autonomous Vehicles

Depending on the localization, security risks vary in these two networks. In external networks, nodes contain to be found in the environment surrounding our vehicle and can be fixed nodes (roadside units) or mobile nodes (vehicles). Moreover, based on the attacking intention, nodes can be benign, malicious, or selfish. Malicious nodes are those nodes that try to inflict harm by affecting the functioning or threatening security. These could include masquerading nodes, or trying to distort packets (from the receiver node's point of view) [14]. On the other hand, selfish nodes have no direct intent to inflict on the network, but detour messages do not reach their destination in accordance with the normal traffic paths and time. Nevertheless, benign nodes act on their purpose and are considered mean. An intelligent, hierarchical, and optimized intrusion detection system using machine learning algorithms has

been suggested to identify the security intrusions depended on individual or even enumerating the famous route request generation time.

The purpose of intrusion detection systems (IDSs) is to assure vehicles' safety and functionality [15]. A real-time and efficient intrusion detection system can be developed by monitoring the communication between vehicles devices and infrastructures. Research has shown that many studies have proposed solutions where the security of the system is separated into two stages of internal and external security, as depicted in the literature. The intra-vehicular network, namely the Controller Area Network bus is within the vehicle, whereas the external network consists of vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-device communications [22].

4.1. Types of IDSs

Anomaly-based IDSs compare observed data with a statistical model of normal operation. This model is established under an understanding of the operational principles of the system [23]. If the discrepancy exceeds a predefined threshold, the IDS triggers a response for corrective action. The unsupervised approach compares the statistical description of the data generated by the system in different conditions and triggers responses if the similarity between the detected and the missing data patterns increases. The 2 key features of anomaly-based detection are its data training scheme and detection model description. Therefore, the main challenges for the anomaly-based IDS are how to create an optimal model using automatic training data from the vehicle network, assigning an appropriate threshold to decide whether the model has detected an anomaly, and minimizing false alarms while having high intrusion detection rate.

Intrusion detection systems (IDSs) can be classified into two main types [24]: signature-based detection and anomaly-based detection. The principle of signature-based detection is to compare incoming data with the signatures of known attacks. If the two match, the IDS alarms. Another way to classify IDSs is by how they maintain their knowledge of the environment. Some IDSs rely on signatures; this is known as signature-based detection. However, signature-based detection is ineffective when familiar attack signatures are insufficient. These features make signature-based detection a poor fit for in-vehicle network intrusion detection systems.

4.2. Machine Learning Approaches

For detecting the vehicle networks' intrusion and threats, many different approaches have been proposed in the literature so far. The vehicle networks' intrusion detection methods are categorized into traditional and machine learning-based methods. Traditional IDS methods are dependent on man-made rules and signatures and when a new abnormal behavior happens in a network, these are not able to detect them. Their behaviors are totally inflexible. To increase more flexibility and discover unknown malicious behavior usage of learning construct enables designing learning-based IDS. This type of designing systems is called machine learning-based intrusion detection systems [25]. The disadvantages and advantages of traditional and machine learning based methods are briefly given in the following.

Information in a systematic and intelligent manner [26]. The growing concern about network security threats has led to extensive research on network security measures. Intrusion detection techniques are broadly divided into two categories: anomaly intrusion detection and misuse intrusion detection. In misuse intrusion detection systems, malicious activities are detected based on already known patterns of attacks. Previous studies on network security focused on misuse detection techniques, but the increased number of modern malicious patterns in recent years has caused intrusion detection researchers to shift their attentions towards anomaly detection techniques. In modern vehicles, due to the increase of electronics and technologies equipped, the possibility of communication equipment being hacked has increased [15]. The impacts of these attacks may be so complex that they increase the possibility of physical accidents, while the average vehicle speed is increasing. One of the components that have a critical role in detecting these vulnerabilities is the Design of intrusion detection systems.

5. Adaptive Intrusion Response Systems

In the last few years, there have been numerous threats identified to the V2X communication systems, and as time goes, more and more will be added to the list. One of the emerging threats might cause significant havoc to the trust of the other peer devices and pose significant negative impact to the network and the ecosystem of cooperation. This emerging security threat could be in termed as a Sybil-based vehicle positioning attack. Although many online and offline tests have been performed, but all of the test scenarios either assumed perfect or near perfect driving conditions or intentional attacks which were only designed to deceive

independentes know the exact location of the vehicles. In this study we discuss a type of attack where vehicle positioning is seriously affected after the successful security and privacy identity formation of the V2X clients.

Cybersecurity gained significant momentum in the last few years due to the widespread utilization of autonomous and semi-autonomous systems [12]. In the network terminology, the vehicles with their associated systems and the external entities like roadside units, pedestrians, and other vehicles together can be considered as a vehicular network. While, on a wider perspective, these vehicles together with other nodes can form an ad-hoc network or a mobile ad-hoc network (MANET) whenever needed [16]. Vehicle-to-everything (V2X) communications are fundamentally important in these networks to realize the concept of smart driving, as it enables communication of vehicles with nearby vehicles, infrastructure, and other non-vehicular elements like pedestrians, etc. Along with the numerous advantages of V2X, it has some serious security threats that are needed to be acknowledged and neutralized effectively. For this, Adaptive Intrusion Response Systems (AIRSs) are needed to be deployed as part of the overall security framework for V2X systems to detect and mitigate/mitigate the impacts of a wide range of known and unknown cyberattacks [13].

5.1. Definition and Components

The services are offered from the infrastructure following a V2I solution supporting cooperative, connected and automated mobility (CCAM). The V2x (Vehicular to Everything) communication architecture integrates the communication links among vehicles (V2V), RSUs and vehicles (V2I), vehicles and pedestrians (V2P), vehicles and road markings (V2M), and vehicles with everything else, like homes, buildings, shopping centers, clinics etc. (V2X). V2x supports the Sentient/Aware vehicle concept. The AV components and their environment require to be secure to offer a secure transfer of passengers and goods. In this chapter we propose an ADAPTIVE INTRUSION RESPONSE SYSTEMS (A-IRS) that supports a security framework where the cooperative AV network offers the services promised to road users and other stakeholders. A-IRS is part of the Intrusion Response Systems (IRS) challenging the next generation of Vehicular Intrusion Resilience Systems (IRS) for EVs networks.

An Autonomous Vehicle (AV) network aims to transport road users from one location to another comfortably, efficiently, and safely [14]. The AV network consists of three components: vehicles, communication infrastructure, and human users [27]. The technology

of autonomous vehicle networks has gained momentum in the last decade as it offers the potential of efficient road transport through a reduction of collisions, human errors, and traffic congestion, and through an efficient use of energy and road resources. The vehicles are equipped with communication facilities among them and with the infrastructure, shared sensors, actuators, and communication links to access information on the communication network, and with an onboard computing unit to support the navigation and driving tasks. They share the communication network with road side units (RSUs) and, apart from the compliance with V2X services, RSUs also offer services as edge servers for the AV network [12].

5.2. Adaptive Decision-Making Algorithms

To overcome these barriers, properly designed decision support systems must be designed to facilitate quick and reliable decision-making in unique and current scenarios. Cause-and-effect prediction algorithms can be used to predict the most likely outcomes of a given decision, and this approach is useful for intrusion response systems. It is also important to consider user bias, which is often present in autonomous decision-making processes. It is crucial to use algorithms that can adapt to multiple optimization objectives. The traffic-aware response order emerges as distinct from strategies that rely exclusively on optimization. The multi-agent nature of the problem and, in the context of traffic systems, the complex relationship between road users has been crucial. It was noted that several pertinent factors influencing autonomous vehicle deployment and the development of novel algorithms.

The smart, autonomous vehicular networks allow for a wide variety of attack surfaces. The development of resilience-enhancing mechanisms necessitates a new way of thinking in terms of intrusion detection, as the teams behind the research [12]. Anomalies and known attacks must be identified in real time and remedial action quickly implemented to ensure the continuous operation of real-time decision-making systems. Because autonomous vehicles typically operate on the edge, separate from mainline networks, it is crucial to detect adversarial activities and attempt to mitigate them in real time with an immediate response [4]. A response to an attack, often more important than merely detecting it, is extremely crucial in the case of safety-critical autonomous systems like autonomous vehicles and controls systems [7].

6. Case Studies and Experiments

In our first tool, a programmable intrusion detection system is proposed for a swarm of drones. It has three Modules of decisions. Occasionally, the intrusion response decisions can be irrelevant, inflexible, and inaccurate due to these hardcoded rules. Such negative responses in a dynamically changing environment can increase the overhead. Intelligent Anti-Anti-Spoof Scenario Detection switcher, InSRT, module is designed. It envisions that malicious intentions of individuals will employ unacknowledged automatic safety cases like manipulating LIDAR (Laser Illuminated Detection and Ranging) sensors to execute an offline spoofing attack. In fact InSRT predicts the enormous miscellaneous vehicle-vehicle communications consisting of swapping lighthouses and motors to conceal the elements of the real time capture so it could intend to analyze a spoofing utilizing different switching combinations.

[12] [4]Intrusion response systems can mitigate stochastic cyberattacks to autonomously detect, classify and manage possible threats against the vehicle or its components. In our second tool, designed for selfdriving automobiles, a Resilient Adaptive Multi-Threat Auto-response System, REACT, is integrated into the car. This tool has a suitable evaluators' combinations and machine learning based capabilities to find the best response set, with associated costs and is able to estimate their outcomes. Therefore, it is able to autonomously deal with them or it can be used to suggest advises for the Security Operation Center. A chain of cyberattacks on the vehicle can result in tampering with all automated driving functions, e.g., loss of control mechanics, energy management, collision detection germane this will impact the planning phase of the car as well. The vulnerability of these Automated Vehicles due to the enmeshing of infotainment systems with other systems has been identified. Attackers may make these vehicles a part of distributed botnets that could disrupt Intelligent Transportation Systems and inter-auto and infra-auto transmissions, as an example one can challenge increment in Capital Costs, disruption of e-Health, social life, cyber-attacks accelerating criminal or terroristic operations, and deteriorating dependence on automotive services.

6.1. Real-world Implementations

Identify specific target augmentations for confidentiality and security-aware testing of currently-used firewalls to identify, whether intruded attacks implicit data leakage opportunities. A system where the augmenting packages are sent by the firewall to the Victim

ECU and then transferred to a secure hidden channel generated by the data-leaking operation. These assets are gathered into comprehensive, realistic and high-fidelity vehicle intrusion scenario models, and validated by automotive cyber security system developers and testers including for the in-vehicle and vehicle-2-vehicle communication channel. This scenario model will allow to establish a systematic methodology of formal, quantitative calculation and assessment of the vehicle security asset leakages under realistic package contents in a model based, logical reasoning analysis. Consequently, the compliance of the OtS firewalls for providing the desired level of coverage against BDI attacks. [28]

To achieve real-world implementation of the proposed Adaptive Intrusion Response System, the following steps should be executed: Compile the comprehensive, real-world dataset, referred continuously, with the traffic patterns unique to different vehicle models and manufacturers, thereby representing the target NADS environment. The records are created by mixing simulated vehicle traffic, as modeled by aggressor and victim vehicle roles, with injected attack attempts. The metrics obtained from the traffic and attacks in the logs are tagged correlates those convolutionally available in SimuTrcks CMVCP aggregation. Real-world attacks apply flexibly consequential the attack generation, reflection real environments, and represent attack variants and modi operandi not necessarily directly captured by CMVCP aggregation. Replicatory attack metrics and traffic evolution in the logs is evaluated and logic relevant to the surrounding environment, as droids, cyclist and pedestrians, can be included as features, including under senders receivers role, in the communication logs.

6.2. Simulation Environments

In this thesis, we respond to the need for a more rigorous approach to vehicle security incident response, proposing a dynamic and autonomous system for vehicular networks: REACT (Rapid Edge Assistance Counteraction Tool). REACT employs policy abstraction, resource-light packet parsing, and domain-specific heuristics, enabling swift evaluation of a problem instance's capability response, enabling the vehicle to act autonomously without need for interaction with the vehicle security operation center (VSOC). This study establishes a firm base of theoretical and practical research for REACT, providing the first comprehensive evaluation, and addressing gaps with future research marked for future work. The proof of concept implementation presented here demonstrates its suitability, especially for single round packet interference problems or DoS attacks with little computational and memory

overhead achievable in a high-speed, low-latency network with the system's ability to dynamically adjust between different strategies without predetermination.

Field studies are expensive and time-consuming; as a result, valuable as they are for measuring the effectiveness of security systems employing real-world deployments, they are rare in the literature. Analytical models and simulations are an invaluable asset for researchers, as they can offer insights and observations at a fraction of the cost and time. However, in practice they, too, are subject to limitations, not least in requiring a diligent approach to calibration [29]. Simulation itself can be costly, particularly for more complex models, or where fine-grained packet-level interaction is required. In such cases, simulation studies can be greatly accelerated by the use of tools able to run simulations en masse. However, even when using simulators, directly analyzing the collection of simulation results is non-trivial. Due to constraints on storage, tracking and subsequent calculation of at-scale data can prove to be an intimidating task. One of the overarching goals for the simulation framework for the system presented in this thesis, then, is to facilitate the highly scalable production, calculation and analysis of large quantities of empirical evaluation data [4].

7. Evaluation Metrics and Performance Analysis

In this way, a study of different vehicular communication and security protocols is also presented using this work. The ISSS system can be used to improve the learning result and provide a secure communication scenario for vehicular applications. In addition, the knowledge of the IDS enhances overall bandwidth and accuracy while conserving energy for near vehicles. For providing system services with accuracy and minimum disturbances, all data is considered using decision aggregation mechanisms. The external protocol of TDMA gives the least chance of collision in wireless communication and uses either application or direct MAC addressing for the identification of the target node. Finally, the external detection of the intrusion approach based on machine learning (MLN-ETD) and time-division multiple accessing external communication (TDMA-ETD) is characterized by a high capture probability, certain packet forward probability, and an expeditious suppression effect of the wrong node [14].

The efficacy of an adaptive intrusion response system can be assessed based on the ability to keep all the vehicles in the network safe from several types of attack models [30]. In practice, several performance metrics are indicative of the time, number of vehicles, or both that it takes

for the system to resume normal operation after an attack. All these attack models are both combined to construct a realistic attack model manifesting three layers, stealth, operation, and impact. Clearly, the attack models pose a tradeoff between true and false positive vehicle ids involved in attack and intrusion response interaction. Additionally, the average times of intervention required and the number of optimal resets for each type of virtual method present a clear trade-off behind real-time performance and the system's average reaction time [5]. As we can see, in all the evaluation measures we can observe a tradeoff between accuracy and computation, which means that for some applications, we can prefer a fast but simplified version of our methodology, while, for the application required for higher accuracy, less ambiguous decision can be made.

8. Future Directions and Emerging Trends

The security attacks on autonomous vehicle networks (AVNs) posses a big threat to intelligent transportation systems (ITS) [2]. Robust AI models can enhance the security and safety of AVNs by utilizing adaptive response systems. We identify that the waste of computational resource and computation time, adversarial training, robust container random replacement, robust multiple models deployment and frequent retraining can be considered for future extensions. We also discuss the potential challenges in adopted 11ad-MGWS technology and the blockchain in relation to AIAI algorithms.

The system block of FIG. 2 in [26] discusses the implementation of AI models for anomaly detection in an automotive controller area network (CAN) bus. We trained three different types of anomaly detection models using three datasets based on different adversarial driving strategies with the motivation to evaluate the robustness of the models against diverse adversarial attacks. The experiment results in this section have shown our proposed adaptive response system based on the AI models has much better robustness than the state-of-the-art static anomaly detection models.

9. Conclusion and Key Findings

Prevention and protection techniques ensure the perimeter of the network and physical security of the devices in the network. While these approaches are sufficient in the current context, these are insufficient in 5G environment. The reason to sustain operations of the vehicle networks securely under the security incidents, adaptive intrusion response systems

will be become vital. AD measurements will increase the advancing detection method self-protection abilities. Though significant research works are carried out in the informatics security domain with respect to adaptation of security mechanisms and the response, significance of the strategic adaptable response methods were emphasized by Alexandra et al. The concept of the ADR to be established with respect to nature of the attack and the desired objectives is defined in the scope of the U-GOV [4].

Autonomous vehicle networks use advanced control strategies, can provide a better safety level compared to traditional vehicles, and are expected to be a major part of future transportation systems due to the numerous advantages that they have. However, as these networks allow information flow within the autonomous network itself and between relevant entities outside the autonomous network such as the road-side infrastructure and other vehicles or entities, and compromise can lead to unexpected behaviors in these vehicles, they are also potential targets of new security attacks or virus spreading, denial of service, fake signal injection, routing attacks or privacy attacks if they are not designed or operated carefully [1]. In the recent past, there have been a number of works that have proposed solutions for the prevention of these threats; to name a few of the related closely related previous works, in [1–4], they consider methods to prevent an attacker attempting to inject fake position or fake message in the vehicle network. In contrast to these, in [5–6], the authors consider methods to prevent an attacker that is attempting to intrude into the network and reading and controlling the internal dynamics. It should be noted that while these solutions are themselves valuable in enhancing the autonomy and awareness level of the autonomous vehicle system and are valuable by themselves up to a certain point, the present work focuses more on the recovery manner from these intrusions. It defines response methodologies using the controller dynamics of the affected vehicle, with limited influences over the behavior of the rest of the network.

References:

1. [1] R. Singh Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," 2022. ncbi.nlm.nih.gov

2. [2] A. Ferdowsi, U. Challita, W. Saad, and N. B. Mandayam, "Robust Deep Reinforcement Learning for Security and Safety in Autonomous Vehicle Systems," 2018. [PDF]
3. [3] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
4. [4] M. Hamad, A. Finkenzeller, M. Kühr, A. Roberts et al., "REACT: Autonomous Intrusion Response System for Intelligent Vehicles," 2024. [PDF]
5. Tatineni, Sumanth. "Customer Authentication in Mobile Banking-MLOps Practices and AI-Driven Biometric Authentication Systems." *Journal of Economics & Management Research. SRC/JESMR-266. DOI: doi. org/10.47363/JESMR/2022 (3)* 201 (2022): 2-5.
6. Vemori, Vamsi. "Evolutionary Landscape of Battery Technology and its Impact on Smart Traffic Management Systems for Electric Vehicles in Urban Environments: A Critical Analysis." *Advances in Deep Learning Techniques* 1.1 (2021): 23-57.
7. Shaik, Mahammad, Srinivasan Venkataramanan, and Ashok Kumar Reddy Sadhu. "Fortifying the Expanding Internet of Things Landscape: A Zero Trust Network Architecture Approach for Enhanced Security and Mitigating Resource Constraints." *Journal of Science & Technology* 1.1 (2020): 170-192.
8. [8] S. Ullah, M. A. Khan, J. Ahmad, S. Shaukat Jamal et al., "HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles," 2022. ncbi.nlm.nih.gov
9. [9] T. H. H. Aldhyani and H. Alkahtani, "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity," 2022. ncbi.nlm.nih.gov
10. [10] M. J. Kang and J. W. Kang, "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security," 2016. ncbi.nlm.nih.gov
11. [11] T. H. Luan, Y. Zhang, L. Cai, Y. Hui et al., "Autonomous Vehicular Networks: Perspective and Open Issues," 2021. [PDF]
12. [12] 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
13. [13] E. Seo, H. Min Song, and H. Kang Kim, "GIDS: GAN based Intrusion Detection System for In-Vehicle Network," 2019. [PDF]

14. [14] 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
15. [15] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles," 2021. [PDF]
16. [16] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]
17. [17] I. Koley, S. Adhikary, R. Rohit, and S. Dey, "A CAD Framework for Simulation of Network Level Attack on Platoons," 2022. [PDF]
18. [18] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and The Way Forward," 2019. [PDF]
19. [19] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
20. [20] A. Olivares-Del Campo, S. Palomares-Ruiz, and S. Pascoli, "Implications of a Dark Matter-Neutrino Coupling at Hyper-Kamiokande," 2018. [PDF]
21. [21] 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
22. [22] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based Intelligent Intrusion Detection System in Internet of Vehicles," 2019. [PDF]
23. [23] A. Haydari and Y. Yilmaz, "RSU-Based Online Intrusion Detection and Mitigation for VANET," 2022. ncbi.nlm.nih.gov
24. [24] M. Dibaei, X. Zheng, K. Jiang, S. Maric et al., "An Overview of Attacks and Defences on Intelligent Connected Vehicles," 2019. [PDF]
25. [25] Y. Dong, K. Chen, Y. Peng, and Z. Ma, "Comparative Study on Supervised versus Semi-supervised Machine Learning for Anomaly Detection of In-vehicle CAN Network," 2022. [PDF]
26. [26] M. N. Injadat, A. Moubayed, A. Bou Nassif, and A. Shami, "Machine Learning Towards Intelligent Systems: Applications, Challenges, and Opportunities," 2021. [PDF]
27. [27] A. Shoker, V. Rahli, J. Decouchant, and P. Esteves-Verissimo, "Intrusion Resilience Systems for Modern Vehicles," 2023. [PDF]

28. [28] 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]
29. [29] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," 2018. [PDF]
30. [30] S. Boddupalli, A. Someshwar Rao, and S. Ray, "Resilient Cooperative Adaptive Cruise Control for Autonomous Vehicles Using Machine Learning," 2021. [PDF]