Adaptive Network Segmentation Strategies for Cybersecurity in Autonomous Vehicle Networks

By Dr. Anna Wilson

Associate Professor of Information Technology, Mälardalen University, Sweden

1. Introduction

Vehicular systems are exposed regularly to new and sophisticated security attacks, aiming to violate users' privacy, steal drivers' sensitive data, and compromise vehicular Electronic Control Units. Thus, the improved defense systems for autonomous vehicles need to misuse and anomaly intrusion detectors combined with real-time user behavioral modeling and a robust and elastic network design, capable of adding or removing defensive segments according to the surrounding threat level. All the above-mentioned goals demand the implementation of an intelligent infrastructure that can self-adapt to the new network configuration depending on the similar network threat level, in order to the adaptively optimized network configuration can be obtained. The paper describes the devised methodology and preliminary findings in the design of a self-adaptive network segmentation strategy to protect the vehicular network [1].

Improvements in automotive technology and onboard systems' functionality are leading to the rise of vehicular networks and connected autonomous vehicles. This interconnectivity in CAVs has attracted great attention from both industry and academia to develop smart transportation systems, making them exposed to various adversaries and different types of attacks [2]. The paper's main goal is to design an adaptive network segmentation strategy to enhance the security protection within autonomous vehicles.

1.1. Background and Context

The expanding connected vehicle systems: intelligent transportation system, monetization data and attractive tax points that make the vehicle an important attack point. In-vehicle networks provide an attack surface characterized by the large difference between the security level and the security technology deployed by the different domains. For instance, in security management, according to the SAE J1939 standard, port 0 of each Vehicle Control Unit (VCU) node should be ISO 15765 (a Transport Control Protocol type) protocol for diagnostic communication, while port 1 through port 127 are a vendor reserved communication but in general terms, vendors have forgotten this basic separation. Sophisticated attacks exploiting this vulnerability have version code: zero transmission due to a fault in the OBD-2 tool and fake message threat injection. With flexibility, all major manufacturers have started using variable bus configuration, moving broadcast domains to each single bus, and hardware isolation between security-sensitive components and the rest of the world, typically using two controllers. This solution reduces the surface exposed to denial of service attacks by unauthenticated and non-Winner-Take-All extensions combining fault injection with man-in-the-middle attacks. From a middleware point of view, service interfaces such as interface implementation, distributed objects, fragments of RTOS, safe operating system duplicating security, partition domains in hypervisors and other isolation modules have been implemented and the adoption of zero-click concept is a reflection of this [3]

Cybersecurity is important to protect autonomous vehicles and connected cars from attacks. Cyber threats and popular attacks like remote hijacking, privacy invasions, and ransom demands could threaten passenger safety. Cybersecurity technology uses methods like intrusion detection to identify and defend against these attacks, which is crucial to protect passengers. Modern vehicles are similar to computers on wheels and represent a complex ecosystem of connected systems and architecture. The implementation of all this technology calls for additional security measures to be in place. In the meantime, the traditional security mechanisms are unable to adapt to evolving and dynamic attack surfaces [4]. In terms of weaknesses, vehicle autonomy increases vulnerability in different ways: unprecedented attacks will be a cause of confusion; human replacement is not susceptible to phishing attacks, engineering or social engineering; the size and velocity of the vehicle makes it a gun carrier for attacks while it is physically isolated from the driver. These features make attackers even more difficult to detect known vulnerabilities and to prevent computational attacks.

1.2. Research Problem and Objectives

[5] Autonomous vehicles (AVs) have been identified as a technology that will help with cities' mobility problems. Nevertheless, as many wireless ad-hoc networks, the distributed nature of AV networks is a weakness against cyber-attacks [6]. Since we cannot rely on humans for

driving and communication, we need to make these systems immune to cyber-attacks. This research question is important and timely because the number of AVs on the road is increasing. As the AV market grows, it will become more lucrative for cyber-attackers to attempt to bypass AV control systems or the physical infrastructure by deploying systems that deceive AV networks or users. Effective security reinforcement mechanisms are highly needed for AV networks, which can work based on either regular (accurate) or irregular (faulty) data.[7] More accurate or available data would improve the security of AV networks. Avoiding data loss, delay, and imperfect data will lead to better judgment of AV networks on the trustworthiness of the communication data. In this study, we plan to develop an adaptive trust-based machine learning security mechanism which would be scalable and can work with other systems without performance penalties. To provide the readers with the state-of-the-art on adaptive trust machine learning for AVs, we have catalogued and abstracted a set of significant challenges from three categories. A variety of aspects in data and network security were introduced and analyzed. Each of these challenges is aiming at evolving the research community.

1.3. Scope and Significance

Connected vehicle networks have emerged as an integral component of Intelligent Transportation Systems (ITS), thanks to the advances in Information and Communication Technology (ICT) and continuous research and standardisation efforts. The core of any ITS is guaranteed Smart Safety Services like collision warning, rear-end collision warning, emergency braking warning, lane departure warning, stop-sign violation prevention, etc., and by extension the dedicated short range communications (DSRC) service. DSRC operates in the 5.9 GHz frequency band and primarily serves vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications. The strict safety requirements on DSRC service have promulgated standardisation and developed dedicated educational programs and go to market commercial products [8]. Due to the continuously growing public interest, several advanced driver-assistance system (ADAS) technologies are already commercially available in modern vehicles.

Cybersecurity in the automotive sector covers a wide range of topics including advanced persistent threats, malware, ransomware, vehicle intrusions and discriminating attacks. Man-in-the-middle attacks and eavesdropping are the main focus of this paragraph. In a connected car, communication among a number of internal and external components, and between the vehicle and a remote/local infrastructure, is the base of services reliability, efficiency and smartness. Additionally, the connected vehicle on-board units (OBU) are internet-familiar devices and use protocols like WiFi and GSM/3/4g. By monitoring the traffic and possibly identify a target, a simple hacker capable of hacking into the communication subsystem. This type of attack is considered an elevation of privilege within the MAN-ATTACK-KILL combination of adversarial machine learning tactics according to [9].

2. Literature Review

Vehicular Adhoc Network (VANET) is a significant component of vehicular networks and intelligent transportation systems. Although VANETs further the future of vehicle-to-vehicle and vehicle-to-infrastructure communication, they face many challenges,such as security issues, high mobility, decentralized management, scalability and more. VANET standardization for data transmission and the like, have been shown to be unreliable, vulnerable and unsecure. Therefore, many incidents of potential security vulnerabilities have been reported for system infrastructures. For example, message wave increases emergency message propagation time delay due to more active parallel systems. They assume the message generated for any service provided by the infrastructure and increase the message flow for periodically frequently result in message clocking. However, in ad hoc networks active communication between vehicles and public infrastructure often operates under severe system or channel access restrictions (Ref. [4,5]), resulting in scenarios of highly distributed and decoupled wireless information exchange. VANET is designed with a focus on highly dynamic networking that allows increased amounts of added features such as safety, mobility and integration is the first awareness prototype (e.g., SwaP me profile) [10].

Vehicular Adhoc Network (VANET) is a significant component of vehicular networks and intelligent transportation systems. Although VANETs further the future of vehicle-to-vehicle and vehicle-to-infrastructure communication, they face many challenges,such as security issues, high mobility, decentralized management, scalability and more. VANET standardization for data transmission and the like, have been shown to be unreliable, vulnerable and unsecure. Therefore, many incidents of potential security vulnerabilities have been reported for system infrastructures. For example, message wave increases emergency message propagation time delay due to more active parallel systems. They assume the

message generated for any service provided by the infrastructure and increase the message flow for periodically frequently result in message clocking. However, in ad hoc networks active communication between vehicles and public infrastructure often operates under severe system or channel access restrictions (Ref. [4,5]), resulting in scenarios of highly distributed and decoupled wireless information exchange. VANET is designed with a focus on highly dynamic networking that allows increased amounts of added features such as safety, mobility and integration is the first awareness prototype (e.g., SwaP me profile). Furthermore, serious security breaches are not expected on underlying infrastructure, which is however not true for VANETs since adversaries can be vehicles themselves. [11]

2.1. Cybersecurity in Autonomous Vehicle Networks

User message is not understandable.

2.2. Network Segmentation Strategies

Network segments are created by devices like firewalls or switches. In the world of vehicular computing, the importance of segmentation is growing with increasing attention and research [9]. This is considering the new types of communication required to maintain safety and congestion control, as well as new types of attacks that can severely affect the functioning of the underlying networks. This means that we need network segmentation strategies which are secure, easily adaptable, and suitable to perform varied communication tasks. To this end, we classify the types of network segmentation in Section 2.2. We classify network segmentations as internal and external and we focus on a way to make these divisions secure and represented as hypervisors.

Vehicular Ad-hoc Networks (VANETs) are wireless communication networks that consist of vehicles and infrastructure which are connected temporarily. One of the most critical security issues related to VANETs are the distributed denial-of-service attacks (DDoS) [12]. The size of the VANET dynamically changes and a large number of vertices and edges play a major role in the occurrence of DDoS attacks. Nodes in the VANET are subjected to DDoS attacks because it does not have any infrastructure to keep safe. So the recent research focuses on how to protect the VANET networks from DDoS attacks. This makes the other intrusions to VANETs a soft target for the malicious attack. The main aim of underlying research is pointed on adaptation of network segmentation strategies in the VANETs [13]. Network segmentation divides the computer network into various sub-divisions such that these segmented networks can operate independently from the rest of the network.

2.3. Collaborative Incident Response

This paradigm results in not only vehicles' networking but also a massive communication paradigm among them. This redesign made these vehicular networks vulnerable to the intruders because there gain the opportunities to penetrate or jam the network with their malpractices, which would critically alter the network's regular operations and the traffic management systems, where these nanonodes are participating [12]. The work in this manuscript investigates the intrusion scenario in a standalone respective of open- parking vehicles' route-selection based security-critical application, providing a collaborative network segregation scheme based on enhanced support vector clustering-based unsupervised learning algorithm, i.e., SVM – Kmean with integrated seven families of Wheeler of PEDotnet testing.

Smart vehicles are vulnerable to cyber attacks as a result of their interconnected network and extensive use of software components [ref: df73a7d4- f777-4a5b-a221-a7d06ede1baf]. Since complete prevention is not feasible, collaborative incident response is crucial in addressing cybersecurity threats for intelligent vehicles [14]. This statement is equally applicable to vehicular ad-hoc networks (VANETs) where mobile software-defined network (SDN) enabled vehicles cooperate and offer services to the passengers and pedestrians in a neighborhood. In this work, we consider a hybrid network, which consists of intelligent connected vehicles (ICVs) and non-ICVs equipped with user equipment (UE) that facilitates direct or indirect communication via advanced mobile phones and mobile hotspots. In general, vehicular networks are meant to offer safer and comfortable travel facility, promoting a highly efficient road traffic system, and focusing on environmentally friendly and economically beneficial driving.

3. Theoretical Framework

The safety and security concerns needed to design robust systems with defensive capabilities. The future will bring several such technologies, in which supervision and management of resources will be done by smart devices (vehicles and UAVs). All these devices, vehicles, and UAVs, will communicate their status/mission-data to other vehicles or UAVs or to the roadside infrastructure [15]. Due to user anonymity or privacy reasons, the data sets, which are shared with the center cloud agent from all smart devices or vehicles, are non-identifiable. In other words, if all the data sets (status/mission) are not associated with any user's identity, called owner anonymization, then this data-set should not be related to any specific user before and after accessing the services of center cloud agents. There is no need to keep privacy-preserving data information for non-anonymous data sets. However, it is necessary to check whether the center cloud agents are able to protect privacy of all the data. For that purpose, protection mechanisms are deployable in Smart vehicles and UAVs to enhance the security of those mission-data; using trustful aerial and terrestrial communication nodes.

Privacy and security challenges in autonomous drone systems and autonomous driving applications are significant. Various researchers have proposed different solutions, including network-based artificial neural systems [16], mathematical models for trust-value assessment, and novel communication methods to prevent eavesdropping and message forgery. Road-side active, and road-side communication participate in vehicle communication and security within them is also one of the main concerns.

3.1. Human-Machine Collaboration in Cybersecurity Operations

Article References (280 words)[17] In traditional network security, static defense technologies such as firewalls and encryption are often utilized to provide network security [7, 8]. However, it is difficult to effectively defend against complex attacks, unknown vulnerabilities, and internal network threats using these technologies. In contrast to this, existing dynamic defense technologies such as Moving Target Defense, Cyberspace Mimic Defense, and Cyber Deception have gained considerable attention due to their ability to mitigate the aforementioned formidable challenges. Especially in the Internet of Vehicles (IoV) security, machine learning-based solutions and network dynamic defense technologies were introduced to provide real-time security [13, 15]. IOV is an intelligent system where all of the devices at home can behave as sensors and actuators simultaneously and standardly connect to the internet. With such technological advances, the driver-assistance system market is being rapidly expanded with the development of the concept of IoV. In parallel, with the rapid growth of data, known as big data, a number of researchers and automotive industries have made significant progress in recent years in the fields of telematics, data management, and analysis.[14] But the data-rich environment of IoV has brought a number of security and privacy-related challenges, with broadcast and unlicensed technologies being exposed to man-in-the-middle attacks that may significantly change the operation of the connected vehicles and culminate with catastrophic incidents. Among the many trends in the research, data security in IoV, anomaly detection [3, 24], smart automotive home security orchestration, electric vehicles charging service, and RTKN are particularly concerned with cryptographic operations as well as data processing and data privacy. The IoV security and privacy have very different application domains compared to the traditional computer and network security technologies. Since the overall future mobility is heading toward fully automated driving, any lack of reliability and trustworthiness may lead to a new paradigm of research and scientific discovery. With this ambition mind, we aim at filling in the gap and contributing to ensuring the overall opeational safety and advanced technological solutions for the present and future autonomous and connected vehicle networks and systems.

3.2. Adaptive Network Segmentation Models

After they move, them might be at the edge of specific neighboring clusters. According to their direction of movement and the network quality of service (QoS) selection of delay θ, five strategies of the SDVN's control and data planes are designed to adjust the optimal network segmentation in real time, namely the random, clock, round-trip-time (RTT), number of hops (HOP), and node sum (NS) strategies. In particular, when reasonable thresholds are adopted, the network delay can be controlled and effectively resolved to achieve vehicular network segmentation and improve the security of Internet-of-vehicles system in an adaptive manner. The results of the experiments in this paper all expressively demonstrated the merits of the proposed schemes. [10] [1] [18]

All vehicular networks, including VANETs, V2V, V2R, and Internet-based vehicular networks (Guo et al., 2018; Guo et al., 2019a; Pranjali & Sandeep, 2019), use software-defined vehicular networks (SDVN) (Raffetseder et al., 2013; Jiang et al., 2019) to perform encryption, data transmission, and key management security routing. As the vehicles move, they jump randomly between data plane levels by adjusting their positions in the vehicular network.

4. Methodology

[19] In the first step, we propose an innovative classification technique to detect the malicious nodes using clustering-based approaches like Kmeans, Kmedians, Agglomerative

(Hierarchical) Clustering, dbscan. (Density-Based Spatial Clustering of Applications with Noise (DBSCAN)) and two traditional classifiers SVM, Decision tree classifier. In order to classify the data into different clusters. The feature list (Table 5) has been extracted from the source code traceback, Accessing hardware which has a something, Reading the user agent from the host, prevented click jacking. For predicting the presence of malicious activity in each vehicle network. The table contains 9608 instances and 9 attributes. We have been extracted 4 attacks types from the dataset which is (Redio interference, Channel delay, collision attack, packet dropper) based on 15 simulation scenarios each scenario consists of 640 simulation round. The dataset file contains the dataset types (npy files, csv files).[20] As reported from the hardware point of view, we examine the ability of SDN to better manage nodes in the network and to achieve an efficient bandwidth allocation. This provides a lowering of the network's structure level in general. In other words, there is a level of resource isolating for every individual worker and there is a conflict between each sub-network that has its own master. Also, this research analyzes how a simple attack can affect the collaborative behavior of nodes in a Vehicular Network. In particular, an attacker can submit dummy nodes that should be discussed to submit attacks towards nodes of SDN. To shed away these kinds of behaviors, we propose an Algorithm to detect the legitimate vehicles considering the behavior of Opportunities Vehicles (OV). Our OPPORTUNITY VEHICLES DETECTION AND 168 F. ADAMO ET AL. REV. BRAS. ENG. AGRÍC. AMBIENTAL, V.22, N.3:166-170 will swap with the simulation results emphasized the effect of utilizing Opportunities vehicles performance (U-OPC-VIP) as a criterion for detecting legitimate vehicles in the network.

4.1. Research Design

As for resilience and security mechanisms selection we will apply adaptive methods to unravel security and privacy trade-offs. We are going to extract the factors necessary for each selection process from the context-aware environment model, the proposed metrics and the risk analysis [19]. The main goal is to learn the relationship between the available countermeasures and the attack scenarios in order to customise them to the vehicle and the environment. This cybersecurity module synthesizes optimised defence strategies based on internal vehicle and external perception information. The end result of this cognitive procedure is a dynamical discrimination of the available security and privacy solutions so that the vehicle will configure them seamlessly guaranteeing mission continuity [5].

Scalability is a key characteristic of the envisioned environment and is defined by the capacity of the platform to adapt its activities to the vehicular context, encompassing from short distance interactions to 5G connections. Each resilience strategy has different performance, cost and privacy overheads. However, most of them are common across different attack scenarios. Therefore, the proposed system will be able to adapt itself to the environmental and operational context, prioritizing particular resilience and charging the vehicle with an associated set of pre-conditions [7].

4.2. Data Collection and Analysis

For the sake of monitoring whether the connection, which is under scrutiny, is still experiencing any issues or weaknesses in terms of security and privacy, data segmentation strategies are a must. On top of it, identifying and understanding the different types of data within real-time network data can be useful in dealing with the network's cybersecurity systems. Moreover, people in charge must be aware of how to identify and distinguish different types of network traffic from intrusion-created data like Attack surface data, which might make identification challenging. As well as common and typically found in normal network traffic they do not contribute to the overall communication of IoT devices and AVs, e.g. microcontroller on the headlights, and a mobility management system's fifth interface. Similarly, by evaluating the attack surface's first two components, it can be implied that they are valid, while the legitimate hostname attacks can be easily seen and evaluated as U(1) and U(2) in the attack surface's first two principle components. Among all the network nodes in the pack-ets, 192.168.218 and 192.168.200 are at the very bottom of the plot and the others are on the upper side, and it is understood that other mentioned network nodes are the real potential attackers trying to make network nodes attack to each other.

In order to capture network traffic effectively, a dump of network packets is collected and the same is pre-processed. The data preprocessing process reduces inefficiencies, redundancy, and irrelevant data, which are common in network packets [19]. In order to be more specific, the preprocessing method uses large datasets in order to enable more generalized results, by keeping capability of presenting severely mutated traffic from various sources to the training process. The sole aim is to use a variety of network anomalies or attacks to execute an intrusion attempt in different ways, which is determined by specific network communication in the infotainment system of the vehicle; for example, starting or stopping an application is not necessarily always found in normal network traffic [21]. The developers created a net-intrusion detection system using datasets that they collected from their car. They noticed that the implemented anomaly detection algorithms gave better performance on the datasets they collected from their car in almost all situations, compared to the previously presented datasets. They believe that part of the performance gain stems from the similarities between the traffic in the datasets and the traffic seen in the infotainment system of their own vehicle [5].

5. Adaptive Network Segmentation Strategies

Using an adaptive job model for network segmentation algorithms together with an autonomous vehicle should be seen as being dependent on the specific vehicle and validated on multiple vehicle types. This prevents the over-fitting of particular traffic generating (sensor, control, infotainment, …) and repairing constellations of logical vehicle segments. This composite approach can achieve realistic and manageable solutions which can make unavoidable system specifications transparent. Securely network communication is in the field of safe real-time based motion control of driving processes from cruise control to automated vehicles. The wide spread perception that consecutively connected autonomous vehicle networks are of fault tolerance 0 or 1 may lead to dangerous conclusions in safety-critical applications. The communication systems for electric automated vehicles (AEVs) are if necessary or useful [16].

There are different architectures and different technologies used in an autonomous vehicle that contribute in the detailed segmentation of the vehicle network [7]. This problem will be tackled first and then the underlying specific technologies will be treated in detail. The mechanisms which are used for segmenting the network will then be implemented in a generic manner. Adaptive, vehicle-specific strategies are outlined and quantitatively characterized. Existing known workarounds will first be considered for alternative practical solutions which address these vulnerabilities [22]. The multi-network segmentation strategies will be treated in a complementary manner, giving rise to photon-based links and associated threats. This leads to the proposal of a generic segmentation concept for automotive architectures which is used to optimize two constructed communication patterns by the dynamic configuration of the diverse underlying network.

5.1. Definition and Conceptual Framework

Modern automation technologies have been used in vehicles already for many years, and autonomous cars are creating a fully novel sub-domain of the automotive manufacturing industry. They consist of classical mechanical parts also but are highly physically integrated construals with the spread of control and supporting systems for electromechanical, electrical, telemetric, and software functionalities. This critical inseparability of their conventional and electromechatronic systems with apparent cyber space presence and considerable external networks is crucial to consider its cybernetics aspects. Some attempts to build the networks of these artificial automates by introducing the cybersecurity solutions adequate for the current Human Internet are half-baked. [7] The article contributes to filling this lack by specifying and proving with appropriate protocol and safe routing execution examples optimal network segmentations of cyber domain for autonomous vehicles. We segregate the autonomous vehicle network domain into secure subdomains of different strategies of building hierarchical over the wireless communication physically layered local vehicular domain secure clusters stabilized by secure channels directly wired between their nodes.

Autonomous vehicles as newly occurring technology contribute a lot to global sustainable vehicle mobility. Nevertheless, they create many new challenges for its currently used cybersecurity solutions, especially for their network segmentation approach. The new segmentation strategy is needed as the main means to properly manage that network, furtherly providing a means of the division of the then occurring network domain into secure segments of various trustworthiness used for secure communication between the vehicle elements (which also include an electromagnetic topology which stabilisation is an additional security issue). The proposal of Network Segmentation Strategies for Cybersecurity in Autonomous Vehicle Networks addresses key cybersecurity challenges of real time functioning of this network. To effectively manage new arising cybersecurity issues in such new vehicle domain networks, adaptive methods are proposed to monitor the need for and to adapt the trustworthiness of domain network segments based on historical data about the functioning of autonomous vehicles and on the computational prediction of future cybersecurity incidents. The article summarises the presentation of the new and specific attributes of the method through their adaptation to real use scenarios.

[15]

5.2. Benefits and Challenges

In 5G systems, remote and local operators can monitor core and radio communication, manage and update the software, and dynamically allocate shared resources and services to identify and prioritize certain devices with specific service levels. However, this approach might introduce malicious and/or adversarial processes and actions at these layers. Moreover, network slicing mechanisms might result in an adversarial/ IoT device being assigned to any one of, preferably, a number of restricted, and/or segregated portions or subnetworks of the mobile operator internet-of-things network. This network has been scheduled into one of a list of distinct types of network service with a given expected or intended quality breadth of "trust domain". The network service prioritization strategy and the characteristics features of the relevant network subnetwork may allow reverse engineering of adaptive Autonomous Vehicle (AV) network sub-network with(possibly unrestricted) ways and ways by seeking to interact with the target(s).

At the downside it might be a dangerous shortcut to zoom in on endpoints reachable in less than 30 hops: Such a network may possibly be simply part of a poorly connected peer-to-peer network leading to an endpoint victim [1]. In these instances, when part of the knowledge any one node may have about the state of the network is constantly becoming outdated due to obfuscating (or even legally enforced) interaction modalities between its peers, the onus is primarily on how well-connected each end node knows its peers to be. Coordinated nodes are thereby able to share information about the layout of a network in a remarkably effective way as nodes deep inside a network are relatively easily reached due the cumulative knowledge about which way to share the finite total set of their neighbors. We find also we can safely rely upon trust propagation domination as well as trust-path prequalification even in networks of extreme depth provided no lies are believed [16]. In fact, this allows maximum information regarding connectivity, information about upcoming nodes, and even the knowledge under what passive continua-hostile circumstances their associates are communicating, to be extracted from any one or two endpoints and nodes they know are telling a dramatic or near approximation of the absolute network truth to and through the entire network, cross-domain.

Following the above discussion, it is apparent that ANSS brings together both the network and the transport layer control and adaptively defines subnetworks of different types(serial, shielded, and exposed). While the ideal network segmentation is often well-measured in network science and graph theory, we propose a new layer 3 connectivity model that lets us gain insight into (un)intended consequences of network policy decisions through modeling, to measure the relevance of (de)segmentation operations in a system of communicating nodes [23]. In general (though perhaps warranting further discussion here), feedback may change the usefulness of network policy decisions respectively. In other words, just because a switch or router notices a change in traffic type does not automatically mean it has to (re)segment the network – it might need to let the end node adapt its communication to more effectively learn how a longer connectivity path worked out.

5.3. Case Studies

In this architecture, a vehicle is expected to automatically interact with other nearby vehicles, road and traffic control systems, the environment around, central traffic control, and of course, this real interaction is made possible only by some communication means. Automotive Ethernet is the primary protocol to build the future in-vehicle networks. However, plug-and-play characteristics of Ethernet and integrated automotive technologies such as artificial intelligence, V2X, and IoT in automotive systems, pose both cyber and physical security threats. Machine learning-based algorithms that constitute the nervous system of autonomous driving and security technologies are introducing vulnerabilities in a short notice. These vulnerabilities should be mitigated executed to keep the autonomous vehicles safe [22].

Smart vehicles and transportation systems, otherwise known as Intelligent Transportation Systems (ITS), have gained significant attention from academia and industry as they are expected to revolutionize daily technology. The Advanced Driver Assistance Systems (ADAS) are digitally transforming traditional vehicles into smart cars. These smart cars are connected to the Internet, communication with other vehicles and nearby systems, and are equipped with a gamut of sensors and control units, turning these vehicles into powerful compute units that can decide and act in case of accidents. In a vehicle’s lifecycle, it goes through a set of services like manufacturing, sale, service, and then to be scrapped. Throughout its lifecycle, a vehicle requires safety, security, privacy, and traceability at different stages [16].

6. Collaborative Incident Response Mechanisms

In the real-world a group of collaborating persons can quickly understand when a member behaves in a compromising way. Similar conclusions can be extended to a set of brains cooperating for a common cause. A possible threat is ineffective when, as soon as it appears, it is rejected and a solution is found by the joint action of all the participants [8]. The same reasonments are employed when a group of autonomous systems constituted by ground vehicles, aerial vehicles, water vehicles, and other entities need to collaborate and counteract emerging threats. Furthermore, each contributing collaborator simultaneously acts as a wide set of advanced sensors that are able to inject on the network live and precise information about situational dynamics and emergent threats, when a threat is detected, immediately the infected sources share it with all the other vehicles that have been in recent communication.

As the cyber-threat landscape adapts to the self-organizing capabilities of autonomous systems, the design of collaborative incident response mechanisms has became critical in the cybersecurity domain. In fact, when a suspicious event is noticed at one system, rapid communication among collaborative members allows to quickly circumscribe the incident and to support preventive actions at the other interested systems [24]. From a theoretical point of view, a collaborative approach enables also more effective detection and prevention. Indeed, the knowledge of every single behavior of each device in a group can be employed to detect anomalies and deviations that consist in abuse attempt.

6.1. Human-in-the-Loop Approaches

At last, the implementation of network segmentation allows controlling the propagation of the attack by isolating different functionalities in the vehicle. Some studies have proposed the complete disconnection of the infotainment system. This approach has been implemented effectively by the automotive sector with the introduction of completely isolated E/E architectures for the infotainment of the vehicles. The human-in-the-loop approach is generic never-the-less it is not limited to automotive systems. Indeed, a new trend is on the horizon for UAS. The latter are now being used in a new domain of application: large aircrafts (commercial, military, cargo, etc...). The integration of UAS within large aircrafts requires methods and tools for ensuring the coexistence of the UAS with the aircraft's "traditionnal" avionic equipments. For this point, the human-in-the-loop approach also appears as being promising.

In the human-in-the-loop approaches, the driver is the single and unique safety controller of the entire vehicle. Consequently, the attack vectors are shut around the driver. To protect the driver from cyberattacks, several strategies have been proposed, based on human comfort and reduced response time to attacks. The most common approach is to trap cyberattacks until the driver has time to react, but with the immediate reaction of at least one system of the vehicle to cyberattacks through the connection of a firewall between the human interface and the gateway The major limitation on those approaches remains the required drive reaction time. Driving and human activity, especially in the case of adaptive algorithm attack strategies, are not compatible, and even if the necessary driving time is estimated, the driver's reaction to the cyberattacks is not guaranteed. Only 1 ms. Is required for cyberattacks on the vehicles and AEB systems that left the driver almost without reaction Read more on the restricted robot in the vehicle's main field. The implementation of autonomy also reopens the debate on the use of human beings as actuators in safety-critical systems.

In-vehicle network segmentation is the strict separation of vehicle safety, control, and infotainment systems, and the partitioning of vehicle systems to isolate them from each other. Figure below shows the segments typically proposed in the literature. In-vehicle network segmentation has been proposed by several researchers as one of the enablers for creating security zones in the vehicle. The advantage of this approach is that an attack only impacts the corresponding segment of the vehicle. This enables a way to control malware propagation through the vehicle, reducing the overall potential attack surface. The essential limitation of these approaches relates to a potential decrease in reactivity to security incidents and the reaction time due to disparities in the non-attack enabling communication capability.

6.2. Machine Learning and AI in Incident Response

These systems are heavily interconnected. Consequently, an incident response system needs mechanisms to share knowledge and resources and negotiation mechanisms to solve potential conflicts. We will specialize to apply machine learning, AI and big data technologies in the field of autonomous incident response such as incident detection, prediction, sense-making and response execution. In this field, exists an opportunity to consider new models of incident response: victim center, offensive and dependent model. The use of AI technologies results in mapping cybersecurity defense strategies and tactics for different management activities involved in the defense of information infrastructures. Using AI technologies enables mapping of different defense strategies and different tactics at a strategic, operational or tactical level. In general, certain defense strategies may have multiple tactics or actions according to how different organizations or their information systems are impacted.

[25]Although machine learning is being widely utilized for detecting malicious attacks, it could be employed for incident response as well. IoT-based ad-hoc emergency response teams [7] can be a good example of this trend. A central incident response system is not scalable for CVEs like autonomous vehicles, so we need an autonomous distributed incident response system, which can manage all interconnected entities and enable autonomous vehicles to deploy such distributed systems in order to take it into account within the safe operation.

7. Evaluation and Results

As visible in Figure 1E, starting both topologies using the Abilene animation available from the internet, the adaptive segmentation aligns its time scale with the packet reception time interval and adapts its distribution based on absolute delay. In this cycle, the Prism manycore re-anchors into every available segment, then counts consecutive annunciations as a connection to a new segment and adopts its segment-wise distribution based on the destination address. [26]Rapid FIB installation followed by chronic network segmenting towards optimal distribution was confirmed during the recovery period. The planned resegmentation strategy provides two types of physical distribution modification utilizing adaptive reconfiguration by intelligent devices for cluster-based packet transmission. The consequences were evaluated and the conclusion was made based on throughput and latency for the network recovery scenario.

In the first scenario, the validation phase is executed with the KDDTrain+ dataset, and it will validate the first-approach proposed, i.e., AIoT, that was developed following the same shape of the AdveNet, and is executed in a victim vehicle. The experiments will be executed online i.e., adding live attacks to the victim vehicle and analyzing the performance of the smart detection strategies. [5]A second scenario is more realistic since it introduces the overlay network and executes the AIoT-IPF during the validation phase, i.e., the scenario presents the association of the AIoT and the segmentation strategy IPF via a quality control network (AIoT-SEL).

The performance of the three network segmentation strategies – baseline, AIoT, AIoT-SEL, and AIoT-IPF – is evaluated in two different scenarios. [27]

7.1. Performance Metrics

We introduce as perimeter security metric the boundaries of the network are secured through SD-VEC with high efficiency. We are trying to rescue the whole topology and avoid attacks from the backbone (e.g., distributed denial of service, man in the middle, and so on) [28]. The security policies implemented are related to the set of features of the new protocol IEEE 802.1Qbv and IEEE 802.1Qci, which demonstrate a constant high level of QoS, low-jitter, and deadline satisfaction in mission-critical traffic. These two per-hops (SSDN) metrics were presented in, simpliciter as perimeter metrics and related to the first "P1.1" security strategy.

The different layers of security within the vehicular network provide different levels of robustness and strate- gies [11]. As part of the scope of this paper, we will only present a high level of description of the security metrics and methodologies in a vehicular network. We present the main differences in terms of security strategies in §5.2. This topic could be a complete research area and could include also different topics as Networking, SDN, or others.

7.2. Case Study Analysis

The body of evidence used in this paper confirms the authors' hypothesis that the current IVI reference architectures are not properly anchored in a security DSS. The results also highlight that our custom-developed DSS is a unique strategy and could logically extend and improve on existing strategies. The demonstrated individualization of security strategies and connections with a modern paradigm implementing, for example, domain-specific smart contracts, graph-chain management systems and device-to-device (D2D) V2X communications open new scientific and application perspectives. The DSS strategy enables multiple stakeholders to prioritize and chose a preferred version of an on-board security strategy. We suggest that this version of architecture meets the market and society needs. Our facts and circumstances are strong enough to recommend the direction of future research. The adaptation of a DSS strategy at the onset could reshape the conventional cybersecurity concept in Intelligent Transport Systems, reshaping the role of incumbent system providers. Our recommendations are scientifically proven and socially desired and we propose a prototyping phase.

To validate the proposed framework, we have functionally decomposed the latest National Institute of Standards and Technology (NIST) guidelines on security architecture in information systems [29]. Accordingly, we have performed an analysis based on a systematic literature review to inspect the current state of the art centered on the security standards of vehicular communications. A fuzzy analytic-hierarchy model in a group decision-making process was developed for the determination of potential courses of action. This paper constitutes a conceptual and empirical basis for the existence of an appropriate security architecture in vehicular ad hoc networks (VANETs) and Intelligent Vehicular Infrastructure (IVI) architectures. In order to prioritize the security in V2X, we have recommended the following: balancing the security virtual LAN and segmentation of data plane and control plane architecture elements of Dynamic Segmentation Strategies (DSS) to manage the implementation of (and balance between) isolation of services, subnetwork, aspect-oriented operating system (AOSO), network domain security, software-defined networking (SDN) and orchestration.

8. Discussion

The main challenge in promoting trust could be assumed as the fact that the malicious node is able to silently cooperate with the other legitimate vehicle nodes contributing in improving the local trust level sent by adjacent vehicles when the connected vehicle is tampered. In cases such as the 1.000, 0.070 and 1.000 from Table 7, it can be noticed that the trust levels of EVs may be influenced by the presence of malicious nodes. So it is important to face the problem of identifying and positively isolating malicious nodes only by means of data sensing and data processing. In this scenario the machine learning technique that we suggested at section 5 seems to be useful to distinguish the genuine messages from the malicious ones [1].

The key aspects we have discussed in the previous sections are cybersecurity strategies and methods capable of interacting with the vehicles on the other hand, managing the risk in Attack Impact and Vulnerability using Dempster-Shafer Theory. We observed that our proposed strategies in this paper covered aspects that were missed by the existing work. This can lead to advances in cybersecurity for product vehicle networks by initiating dialogue among the socially engineering aspect of autonomous vehicle network in human–machine interaction area [14]. Our study would be very relevant to those researchers who are developing new cybersecurity methodologies by considering the impacts of attacks and vehicles’ vulnerabilities in a complex manner. These are potentially beneficial for building the next generation of autonomous networks on the road.

8.1. Key Findings and Implications

We then investigated three main targeted criteria on the trajectory to this end: (1) connections, (2) network protocols and topologies, and (3) dynamic QoS in order to help improve the discussion on directions towards safer and more privacy-preserving AV networks both in the vehicular ad-hoc network and inside the car. Additionally, an insight into the configuration challenges of the field on the spy vs. spy problem is provided for good measure [15]. Together, these findings set up the network adaptation concepts we need to motivate a more robust autonomous defensive approach. As a practical application of this concept, we provide a generic six-stage process that can be adjusted for the complexity of the data sets of interest in scalable sophistication from the early prototype stages straight into production settings resembling the underlying power market of peer-to-peer communication. A single representative of filling the autonomy-related NLP activity space is inculcated with access to the full selection of datasets, networking activity, and system breaking capacities to traverse all mentioned states incrementally with various levels of autonomy in busy smart grid experiments [16].

In this chapter, we identified and analyzed several emerging trends on network segmentation in the context of cybersecurity in autonomous vehicle networks, investigated several segmentation strategies, and concluded on the implications of these findings for the design of network segmentation strategies in the future in the same context. We start by discussing the role of adaptability in achieving intrinsic defence in networks [5]. We found significant benefits for adaptive segmentation over static segmentation. In particular, the distribution of communications within intelligent real-world data sets adapted to network changes for increased action space coverage (disrupted segmentation) and created complex feedback opportunities, contributing to persistent chaos too complex to handle deterministically every time a new emergent data set is intended as opposed to adopted as a novel normalcy of variation. Beyond this, we observed that intrusion detection models in networks misclassifying (i.e., normal vs. compromised autonomy) failed to generalise to real-world systems listed in Section 2.2, thus needing to be optimised in the future with evolvable data.

8.2. Theoretical Contributions and Practical Applications

This article wants to propose and analyze a new network architecture and protocol stack to protect CAVE networks by detecting in a fast way potential attackers and making trap for them [23]. The AI's algorithm has the goal to learn the normal behavior of the vocal based on the network stack. It will learn to analyze all the packets types, transmitted protocol and pattern sequence that reach the device in a CAVE network, and will account that those packets are legitimate. Starting from the AI algorithm that works at network layer, it is possible to design two different filters that in the paper are exposed in details.

Cloud computing represents an innovative way to provide advanced services and tools to manage complex resources and systems. Considering this key aspect in a connected AV ecosystem (CAVE), cloud computing represents a suitable choice to store all the data and services vehicles, and other external nodes, could use and exchange [3]. The deployment of the cloud, and its set of services, may offer a fast, cheap and secure mechanism to store and manage the data generated by driverless car, the sensors data and AI algorithm. The greatest challenge of this approach is to guarantee the synchronization, integrity and confidentiality of the data transferred between the CAVE and the cloud infrastructure with end-to-end encrypted channels. Moreover, the AVs' connectivity to the network has to be managed very well to avoid that an attacker could launch a DoS attack against the driverless car, or that could suitable performance limitation limiting, for instance, the stability of AVs' algorithms, especially in a safety witze [20]. This structure is the starting point of a new concept of AI-driven Computational Network.

9. Conclusion and Future Directions

In this paper an optimal autonomic vehicular individual, vehicle, PKI-free pseudonym certificate, differentiate vehicular cell and software defined vehicular subnetwork, GPS, V2X communication, dangerous automotive collision case studies and congestion aware PKI-free pseudonymization schemes, can be used to prevent physical detriments to communication-relayed outperformed hardware-related engineering-side-arp vulnerability, stand ou. The new genetical approach is clear, of the IDPS concentrated on hardware building vehicle clusters and MD5 hash functions tested numerous interdependencies [2]. Although modern autonomic vehicular Vehicular Ad Hoc Networks (VANETs), i.e., vehicular-to-vehicular (V2V) and vehicular-to-everything then, defined networking. On the one hand protect the logic security/ data contamination, authenticating information supplied via the Cellular Vehicle-to- wonder message to component software and hardware and optimizing Quality of Service (QoS) conditions. On the other hand the proposed nes genetically engineered for securing the side-canal, shielding respectively transmitting the information in a Magic and

Snow scheme adaptation approaches are analyzed from both the engineering and the theoretical perspective.

Modern autonomic systems use the concept of software-defined networking for safe, resilient and efficient vehicular slices on the one hand and on the other, they utilize emerging vanet communication issues and security requirements in order to propose adaptive network segmentation strategies ([30]). The adaptive segmented network approach is a very powerful concept which perfectly fits to the modern connected autonomous vehicular systems. This approach is based on adaptive network approach re-evaluates and adapts the natively defined network requirements according to the runtime includes an overview of key network concepts used in autonomic vehicular networks and discuss issues and considerations for adaptive network segmentation strategies. The study also provides alternative people pods residing in separate segments. Finally, the study provides an optimized network slicing layer, together with an exemplary work on authentic antivirus, while a study on adaptable vehicle pods and adaptive software defined vehicular cell networks (SDVCNs) is underway.

Safety, efficiency, privacy, and cybersecurity constitute the main challenges of autonomic vehicular networks ([15]). In the literature, several cybersecurity methods have been designed for autonomic vehicular networks. Adversary models, packet losses, and security parameters are main factors taken into account in these methods. While losing packets make security parameters obsolete, adversaries impact security measures seriously. This study aims to investigate adaptive network segmentation strategies to be utilized in modern adaptive autonomic vehicular network applications for technical aspects. This study provides two main contributions.

9.1. Summary of Findings

This exposes all in-vehicle networks and especially main data aggregates, based on 10/100BASE-T1, 1000BASE-T1, or 100BASE-T1 protocols, to serious security risks. Hence, this paper proposes a comprehensive cybersecurity architecture for the Automotive Ethernet based system to safeguard vehicles against external and internal attacks. This security architecture is designed and developed in three sections, including the peripheral network, ECU network, and the payload networks. Each of these network segments is secured by erecting an access and security layer that assigns dedicated security parameters to secure and transmit data. Furthermore, the security parameters are monitored and updated dynamically by learning through the reinforcement of the neural network at runtime.

[2] [31]As automotive technology has evolved, so have in-vehicle networks and connected autonomous vehicles (CAVs). Creating new technologies like CAVs introduces unprecedented security risks. Researchers are focusing on making vehicular networks more secure by adopting network segmentation strategies and adaptive network security protocols. The primary protocol for future in-vehicle networks is Automotive Ethernet, particularly with respect to security [22]. It has been proved that external interfaces between aggregated networks on electronic control unit (ECU) side, as well as physical access to the vehicle networks, are more and more susceptible to hacking attempts.

9.2. Recommendations for Future Research

This research raised awareness and consequently multiple concepts toward inducing an innovative mechanism using reference architecture approach for network segmentation as enabler, obtaining the emerging adaptive active cyber defense. Protection mechanisms are much faster if they can adapt to unexpected events and emergent threats. Such considerations were not explicitly developed from VNCS cybersecurity research, and the blending of these concepts suggests specific future research challenges and directions that are identified here. The main findings and contributions of this research are summarized in a critical summary, together with the identification of future research directions. Many applied areas can improve the vehicle safety and performance thanks to the proactive detection and avoidance of generic problems and unseen threats. Additional works are needed towards the comprehensive exploration of this idea [32].

Attempts to protect data in a completely automated way, with the help of innovative approaches in cybersecurity for autonomous vehicle networks, is a growing research and development area. Research focusing and raising awareness on these measures is needed to be able to protect against a paradigm shift of cybersecurity vulnerabilities on autonomous vehicle networks. As a next step, a significant number of recommendations and practical guidelines for future research direction are delivered in this regard [16].

References:

1. Sadhu, Ashok Kumar Reddy, et al. "Enhancing Customer Service Automation and User Satisfaction: An Exploration of AI-powered Chatbot Implementation within Customer Relationship Management Systems." *Journal of Computational Intelligence and Robotics* 4.1 (2024): 103-123.
2. Tatineni, Sumanth. "Applying DevOps Practices for Quality and Reliability Improvement in Cloud-Based Systems." *Technix international journal for engineering research (TIJER)*10.11 (2023): 374-380.
3. Perumalsamy, Jegatheeswari, Muthukrishnan Muthusubramanian, and Selvakumar Venkatasubbu. "Actuarial Data Analytics for Life Insurance Product Development: Techniques, Models, and Real-World Applications." *Journal of Science & Technology* 4.3 (2023): 1-35.
4. Devan, Munivel, Lavanya Shanmugam, and Manish Tomar. "AI-Powered Data Migration Strategies for Cloud Environments: Techniques, Frameworks, and Real-World Applications." *Australian Journal of Machine Learning Research & Applications* 1.2 (2021): 79-111.
5. Selvaraj, Amsa, Chandrashekar Althati, and Jegatheeswari Perumalsamy. "Machine Learning Models for Intelligent Test Data Generation in Financial Technologies: Techniques, Tools, and Case Studies." *Journal of Artificial Intelligence Research and Applications* 4.1 (2024): 363-397.
6. Katari, Monish, Selvakumar Venkatasubbu, and Gowrisankar Krishnamoorthy. "Integration of Artificial Intelligence for Real-Time Fault Detection in Semiconductor Packaging." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023): 473-495.
7. Tatineni, Sumanth, and Naga Vikas Chakilam. "Integrating Artificial Intelligence with DevOps for Intelligent Infrastructure Management: Optimizing Resource Allocation and Performance in Cloud-Native Applications." *Journal of Bioinformatics and Artificial Intelligence* 4.1 (2024): 109-142.
8. Prakash, Sanjeev, et al. "Achieving regulatory compliance in cloud computing through ML." *AIJMR-Advanced International Journal of Multidisciplinary Research* 2.2 (2024).

9. Venkataramanan, Srinivasan, et al. "Leveraging Artificial Intelligence for Enhanced Sales Forecasting Accuracy: A Review of AI-Driven Techniques and Practical Applications in Customer Relationship Management Systems." *Australian Journal of Machine Learning Research & Applications* 4.1 (2024): 267-287.
10. Makka, Arpan Khoresh Amit. "Integrating SAP Basis and Security: Enhancing Data Privacy and Communications Network Security". Asian Journal of Multidisciplinary Research & Review, vol. 1, no. 2, Nov. 2020, pp. 131-69, https://ajmrr.org/journal/article/view/187.