Adaptive Network Defense Architectures for Autonomous Vehicle Networks

By Dr. Dimitrios Grammatopoulos

Professor of Electrical and Computer Engineering, National Technical University of Athens, Greece

1. Introduction

In this article, we built up and through simulations, assessed a novel architecture of Adaptive Network Defenses (AND) to achieve robust security in IoV. In our proposed architecture, the vehicles are functioned as sensors with processing and analysis capabilities and a SDN controller is directed and programmed to adapt to changes in traffic conditions and security attack measures. Moreover, the high-highway communication link is a shared-medium link. In which, the security commands of vehicle are saved and graphed as entries and that can be used to optimize the SFC decision. For analyzing the security of the proposed system, our comprehensive simulations for the different attacking scenarios and traffic conditions have been executed. The simulation results demonstrate that the proposed security architecture, after encountering the security changes, will detect the malicious nod in nearly one second, with recovering the link between the functions of an attacked nodes and the network. Also, in case of severe security changes, the proposed SFC system with iron correlation configuration, will detect 81% of the security attacking from a malicious node in 500 milliseconds.

It goes without saying that wireless vehicle communication technologies such as Vehicular Ad hoc NETworks (VANETs) are gaining attention. With the assistance of VANETs, a range of intelligent driving functions, such as autonomous vehicles and traffic-light cooperation systems, are developed to improve the road safety and traffic efficiency. In particular, it is expected that autonomous driving vehicles, a key model for the Internet of Vehicles (IoV), will be popular in smart-cities and co-transportation projects in which Intelligent Transportation Systems (ITS) are used. However, there are security attacks and accidents attributed to the potential malicious behavior of attackers in IoV. Therefore, moreover to compatibility,

security can be regarded while designing vehicle networks. Especially, when a vehicle is compromised or in the case of a wireless connection with it is arbitrary, it should be detected or isolated as soon as possible to prevent further serious security attacks and accidents. In related references, various security architectures and technologies were proposed and did not only attack it before entering into the IoV network but also isolate malfunction after detecting it.

1.1. Background and Motivation

Self-driving vehicles, known as autonomous vehicles (AVs), can be promising for the urban zones in the future, solving different traffic issues, for instance that of limited parking spaces. For autonomous driving, the application of mandatory cooperation between vehicles and infrastructure and vehicles and vehicles remains one of the crucial ways of increasing safety, economizing fuel costs and road capacities and preventing traffic accidents while driving [ref: 2336D6D9-3BD1-4200-84E7-2419FFF1DC89]. To implement cooperative driving from vehicle to vehicle (V2V) and vehicle to infrastructure (V2I), several prerequisites have to be guaranteed, for instance, accurate positioning techniques, an HD digital map which carries information for contacting roads and vehicles, a highly dynamic network which allows the allocation of large quantities of traffic data and computing tasks and a timely, high-quality transmission on all the communication and networking levels. These frequently mandatory requirements include network protection against cyber hazards and generating a dynamic process of assault defense and adaptative network defense.

Vehicle networks are bound to play a critical role and thus imaginative and innovative methods and architectures are inevitable for managing their resources to ensure good quality service delivery [ref: 3122758C-FDDE-4CCE-868D-4B2BF9A2AB1A]. The paper presents a novel hierarchical detection algorithm to build up the system of external communication security defense based on threat identification in each detection layer and the use of defensive resources adaptively [1]. WSN-based networks represent a feasible choice towards providing an effective security method in vehicular networks due to their advantageous characteristics such as low implementation cost, scalability, energy-efficiency and security. WSNs have been extensively exploited to construct stable, scalable and secure VANETs and they have been exploited in numerous research and experimental systems for vehicular network security testing and systems. These intrusion detection approaches are utilized to implement message

integrity check, data backup, order authentication, data encryption which are used to guarantee secure Vehicular Ad-hoc Networks (VANETs).

1.2. Scope and Objectives

There are undetected security vulnerabilities in AV, connected vehicle and smart mobility networks, services and plants, and there have been various recent large-scale network and vehicles failure, resilience and response incidents [2]. This calls for a high-level machine-to-tangible language heuristics for human guardianship, computer science and cybersecurity of a car network cybernetic operating environment. The current security and privacy provisions in place for connected vehicles, automated vehicle businesses and smart mobility are inadequate to meet the needs for a trust-based vehicle-to-everything (V2X) ecosystem. Security solutions and recommendations need to build on comprehensive attacker threat models and first principles and design 'secure by design' principles that are rigorously tested and can evolve situations over time yet avoid runtime cancellations and are apposite to legacy systems [3].

Autonomous vehicle (AV) networks are in a continuous state of creation, deconstruction and operation of software defined, optically defined and virtually defined dynamic identities and language- and machine-independent HVs self-awareness driven procedural functionality. The focus is on an adaptation and evolutionary approach of a dynamically evolving network architecture, artificial intelligence, cybersecurity and data privacy provisions environment, with minimal-to-advanced tamper-proof decision-making under time constraints and critical infrastructures.

2. Autonomous Vehicle Networks: Overview

Legacy autonomous agents (security mechanisms) cannot be used in AVN environment. The general security and privacy requirements of autonomous vehicles are need to provide spatial location security and privacy, physical person information privacy and user online behavior privacy. The privacy and security challenges in AVNs are intensively expanding or becoming significant mainly because of the aforementioned path break in sensations, dexterity, intelligence as well as personal rights, and freedom with the integral of the human factor. In terms of the systematic vulnerabilities, there are firstly physical-layer and cyber-layer passive attacks that can be observed on the sensor node during ride. The paper identity the network layer attack viz. eavesdropping, man-in the-middle (MitM), and denial of service (DoSer)

attacks threaten the centralized infrastructure, edge cloud, and entire network. The vehicle-to-network (V2N) and vehicle-to-vehicle (V2V) channels, vehicle-to-cloud computing (V2CC) channels, and Edge Computing had better be attacked, as a disruptive attack model on network chain communication in AVNs [3].

Vehicular technology evolves as day passes the premises of VANETs are transforming from simple vehicular ad hoc scenario to the more recent semi-autonomous level system and fully flow Autonomous Vehicle Networks (AVNs). Networked vehicles can share real-time information to one another in order to advise the self-riving module and effectively increase an automobile's abilities in sensing, dexterity, and intelligence. The infrastructure handled by Intelligent Infrastructure (II) from the perspectives of being self-sufficient, mobility, and the universal interconnected with associated IoT devices. The IoT devices identify as various smart objects are capable of communicating with each other allowing CAVs to communicate with them and they in turn can communicate with other devices as well [4].

2.1. Characteristics of Autonomous Vehicle Networks

[5] Collaborative driving enabled autonomous vehicles an ability to cooperate with each other and share traffic status and future plans to reduce the possibility of accident. The full autonomous vehicles make decisions following the execution of driving commands, including turning left or right, and checking vehicles in the neighboring lanes when shifting lanes and overtaking. Collaborative driving autonomous vehicle network can be designed with three layers: the Perception-Decision-Action (PDA) layer, the Intelligent Transportation Infrastructure (ITI) layer, and the Collaborative Vehicle Network (CVN) layer. The Autonomous Vehicle Network (AVN) layer in the traditional collaborative driving scheme does not exist in reality, in which the AVs could transmit their traffic status and plans to each other through vehicle-to-everything (V2X) communication using a model of car-to-car communication, adapting a centralized processing architecture, while all decision making and conflict resolution are implemented through the cloud platform in real-time mode.[4] Autonomous vehicle networks are designed using a combination of different technologies, creating various attack surfaces for internal and external attacks. To prevent application layer attacks, cryptographic approaches like digital signatures and timestamp-based random numbers can be used. Network layer attacks, such as distributed denial of service (DDoS) attacks, can be launched using vehicular botnets or by disrupting the communications network. Anomaly detection methods can help protect against security threats, including

compromised vehicles with valid certificates. Connection is sporadic in VANET, as vehicles are mobile and can transmit a message that could be concurrently received by different vehicles. Broadcasting messages is commonly used in VANETs, where RSUs broadcast road traffic condition messages, V2V broadcasts accident messages, and V2I broadcasts speed limit messages. An attack aims to disturb the VANET can delay the messages from vehicles RSUs, pollute the traffic and road condition information, or even stop the messages from vehicles and RSUs indefinitely.

2.2. Challenges in Securing Autonomous Vehicle Networks

The security requirements of autonomous vehicle networks are more challenging and complex than traditional network systems. The challenges include unique security requirements, dynamic characteristics, potential security attack targets, insider or physical threats among others, and demand the design of a more comprehensive and practical security architecture. In [3], the author forecast another concern referring to Blockchain network-based artificial neural network system. Cybersecurity of 6G is significantly predicated on a longer route of exposing data environments, evolved learning model systems, and greater data security. Hence within an epoch of emerging 6G applications and innovation, the demand for dealing with security hazards incrementally become complicated, ranging from security requiring more stringent connectivity, social, and surveillance infrastructure rotate. TRL Reserve Protocol entitles selective learning and optimizing network requirements when dynamic compromises explode.

Security threats are always present in vehicular communications, one of the fundamental requirements is to protect the valuable data from unauthorized access. Due to the data being valuable for commercial as well as safety reasons, privacy-preserving technologies need to be applied to prevent data leakage. In [6], the author foresaw all the concerns such as the Robust Security System to Ensure the Privacy Preservation and Communication Perfection. Professional Secure and Privacy-Preserving Data Sharing Transmission System for Efficient Real-time Communication. The extensive experiments have been carried out to evaluate the prominent attested technology from several aspects such as the inability of eavesdropping, the robustness of data shifting, the efficiency of real-time data sharing possible of low processing time, and the mining-based fine sorting. Encryption schemes should also be secure enough to support safety-critical applications using shared information, e.g., for highly accurate maps. Otherwise, these attacks, which do not require physical functionality of the

vehicles, can lead to dangerous situations on the road as malicious actions can be used to clearly divert the vehicles.

3. Network Defense Architectures

Next, the internal communication ANDs, Layer-1 and Layer-2 are located within each connected ECU and In-Vehicle Network. The Layer-1 corresponds to the state-based IDS which monitors the operation states of the ECUs and strictly abides by the defined safe operation states of all the ECUs [2]. If any ECU performs an abnormal operation that violates the defined safe operation state, the IDS immediately recognizes such acts as cyber-attacks. Primarily, the decision support systems and the tightened operation states of the ECUs will be referred to as countermeasures. In addition, the occurrence of any 'saturated' state in the relevant state models will be fed back to the AND Layer-2 (hierarchy controller) for further analysis and planning.

A robust security architecture must be in place to safeguard the autonomous vehicle networks from cyber-attacks. A three-tier Adaptive Network Defense (AND) architecture for the Autonomous Vehicle Network (AVN) is illustrated in Figure 1 [7]. The data sources are the feature signs of the normal and abnormal behaviors of the AVN. The proposed AND architecture predicts the behaviors of the systems by analyzing the current states of the systems, decision-making and applying countermeasures through information analysis, scenario prediction and planning, and countermeasure execution layers.

3.1. Traditional Network Defense Architectures

The hacker not only legislation measures which defense of problems but also the chance to launch cyber - attacks. The multi - identifier (ID) network security architecture based on the traditional DiD architecture, matched with a security strategy that combines static defense network architecture with dynamic technology, such as moving target system defense (MTD), cyber deception hopper (CDH), cyber deception technology (CDT). The attacker has to continuously modify the intrusion strategy to monitor the host network security system to retreat gracefully. The idea of using the multi - identifier network security architecture instead of the traditional DiD network security architecture is to reduce the frequency of programs of a systematic crash due to software vulnerabilities.

Generally speaking the protection only involves the information flow port, some defense technologies are based on the characteristics of the upper-layer application, so the protection inevitably has its limitations. In addition, the strategy that the DiD system defense mainly relies on the notification of historical threat intelligence, the proactive intrusion detection of it serves for only known attacks, without the detection capacity for those unknown vulnerability and new types of attacks. [8] At present, the static defense of network security in various organizations mainly depends on the defense capabilities of the DiD network security architecture. The attracted network connections are processed by current network devices and then transmitted to the local network. The physical network connection port means the permission of the attacker to enter is weak, and it based on the traditional thought that security lies in the heart of the city. In traditional security network architecture, all devices inside the enterprise network are implicitly trusted, Even if a malicious program attacks the host or server, the device may escape the defense by exploiting technical vulnerabilities through various paths. The DiD also has many other weaknesses. When an attacker learns the intrusion rules of a security device, the integrity of the security device and management rigidity become the targets of the attacker's attack.

[1] The classic defense-in-depth (DiD) security architecture. The DiD network security architecture layers defense capabilities such as the firewall, intrusion prevention system (IPS), and honeypot and is widely used in existing organizations. However, this traditional network defense system is vulnerable and difficult—likely im- possible—to quickly and accurately detect complex attacks and unknown vulnerabilities. Moreover, it is also challenged by the excessively high volume of maintenance work. The DiD security architecture does not consider any detection and protection against unknown vulnerabilities or zero-day unknown attacks. In DiD security architectures, as long as the route data packet is successfully transmitted to the end, this route data source terminal is generally accessible by the information source terminal. The defense system can only rely on the technology in the upper-layer application for protection, such as firewall, intrusion prevention system (IPS), emergency alert, etc. If the attack technology does not involve the upper-layer application, the attack can bypass the protection of the upper-layer application and cause harm.

3.2. Need for Adaptive Approaches

This challenge of achieving reliable and secure autonomous vehicle control over diverse sensor-fusion processes has driven another new approach, which reflects on Adaptive

Network Defense Architectures and illustartes attached contribution that forms the main motivation of this study [article: 68c81443-f395-4c7f-b8ed-864ceaa812cc].

Reduction of computing costs and increasing universe of adversaries have driven the latest cyber-attacks to be more sophisticated and that pose an increasing threat with tactical autonomy and related safety systems that are reliant on deep learning, among others [article: 49fe447b-1838-495e-b4d7-6c86a7a2cbe2]. Consequently, there is a growing interest in the exploration of the network security of autonomous vehicles. (3) In light of the inherent constraints and requirements, it has been investigated alongside several wireless automotive networking technologies. Until the present day, perceptions including the use of a distributed sensor-to-actuator communication model and associated security, integrity, modeling-related deficiencies and adversarial cyber-attack and environmental stress have taken the lead in research [article: 3068bfd4-c27d-49bb-91fb-dd63d3482d0c]. Nonetheless, the majority of vehicle network resiliency approaches only consider dynamic changes in network structures and algorithms so that malicious disruptions in communication can be observed. There are no widely referenced perspectives on addressing link-related adversarial impacts.

4. Adaptive Network Defense Strategies

Distributed security actuators, moving one step further, work 24/7 on the infrastructure behind our V2$, with Mobile_Assistant trust metering properly packaged [9]. Works are ongoing to develop the lateral jumps for searching attackers related to botnet infection and our verbal mobile assistant named amssiri has been already publicized. Targeting an autonomous vehicle network, for example V2X in Car2Car Communication, street side units (RSUs) and a common traffic dataset, it is fundamentally realized to adopt a combinatorial blockade and cross-infection interfering system composed of undependable honey pot and honey net strategies. Every time V2X, RSU, or other public place infrastructures pay inadvertently deadly attention or violently mushroomed attraction to specific questionable traffic, the system finds by individual traffic capture a convenient sleight scheme for mutual boobytrap we call innocent honey pot and hornet hive.

In the face of increasingly intelligent network layout, access road work enforcement and user-behavior inspection, upfront defense strategies on network and attack level should be taken seriously. Adaptive game-/Multi-armed bandit-based cyber security provisioning are a good start based on which, a closed-loop feedback-driven combined intrusion detection system

(IDS) and cross-infection forecasting system can be established [6]. The IDS reports any abnormal behavior of traffic packet and the malicious V2X device information to our game server, after preliminary network-level inspection. To validate these reported results, The game server will communicate with the challenger agent, fully exploiting possible vulnerabilities for optimal report-confirmed annoyance. More specifically, using the adversary vulnerabilities is a good way of attack generation without active adversarial planning and beta test. In response, the system aggregates new environment information exchanged from the infrastructure unit, and then updates our game solver deployed at the SC. Finally, based on real-time adversarial-level and network-level statistics, the IDS pattern library is updated correspondingly.

1. Automatic drive thru switching between V2V, V2I, V2P, V2C, V2G and uploading/downloading over WiFi, Bluetooth, LTE, LAN, device-to-device, or in-vehicle wired interlink. 2. Sharable V2I&C resource scheduling for vehicle-form organizations, and load balancing and backup failover in case of partial V2X network partition. 3. Good-to-best QoS selection, rate adaptive coding, multipath, multicast, and auto-emergency requirement tearing in a universal data offloading strategy to avoid any single-point-of-failure.

Autonomous vehicles communicate using extended integrated networks that encompass vehicle-to-everything (V2X) communication that includes vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), vehicle-to-network (V2N), vehicle-to-pedestrian (V2P), vehicle-to-grid (V2G) and vehicle-to-cloud (V2C) [10]. Such a unique network environment entails diversified and ultimately severe security Defcon levels, primarily including safety, privacy, and security provisions, not least needing to enshrine data integrity, geographic data consistency, microsecond-low E2E delay, authentic self-healing and efficient secure vehicular naming service and secure session initiation procedure. To tackle these combined challenges, programmable data plan technology, namely Software-Definition Networks (SDN), is a natural fit. Key attributes of the integrated data plan include:

4.1. Dynamic Threat Detection and Response

The inherent limitations and shortcomings of vehicular network-specific secure transmission and application layer security mechanisms highlight the need for integrated defense mechanisms embedded in the deeper layers of the communication stack Furthermore, [11] highlight the loss of performance of these measures when subjected to delay, packet drop and

jitter, which they rightly discuss. Moreover, their exclusive focus on developed transportation ecosystems means that they ignore transportation networks with already deployed E/E architecture based on less powerful hardware and relatively unrestricted software distribution. To the best of our knowledge, our work is the only resource in the published literature that focuses on addressing dynamic, malicious requests aimed specifically for automotive networks through multiple communication stacks and middleware, including the transmission, link and physical layer of vehicular communication whose protection goals also include safety-critical system flexibility and real-time performance.

As autonomous vehicle technology becomes more widely adopted, there are increasing concerns about the cyber-threat landscape that encompasses adversarial information and communication technology (ICT)-based attacks aimed at affecting the open- and closed-loop functionalities, including attack scenarios in which the interaction between physical and cyber domains can also be exploited to achieve sabotage [12]. When considering in-vehicle networks, so-called in-vehicle attacks may be launched with the introduction of malicious messages into the Controller Area Network (CAN). These can appear as messages that violate the standard protocols in the best case scenario, but they can aim to masquerade as legitimate messages in the presence of physical layer vulnerabilities. In the worst case, it is possible to overwhelm a vehicle network with a large number of messages (Denial of Service, DoS). Given the presence of diverse security requirements designed to protect privacy as well as safety features [13], highly dynamic vehicular networks capable of countering cyber On top of that, traditional security measures are becoming obsolete due to the high level of connectivity and the imminent arrival of 5G communication technologies. This likely ubiquitous connectivity makes the use of decentralized cryptographic solutions (only) ineffective.

4.2. Machine Learning and AI in Network Defense

Security issues are become increasingly serious as the amount of data processed in vehicular cloud networks continue to increase, traditional security solutions are increasingly losing their advantage in real time responding to unknown and complex attacks . Many automotive components have ignored network security or applied only traditional authentication (passive) functions . An effective and efficient network defense strategy is urgently needed. In some fields of networking, we have begun to use machine learning and artificial intelligence to provide security solutions dynamically and proactively .

Autonomous vehicle networks require a dynamic and comprehensive security solution [14]. Machine learning (ML) is becoming more popular in network defense, as recent studies have shown that there are significant vulnerabilities in the vehicular network, including vulnerable wireless communication elements and vehicle-to-network components [15]. Among the black-boxes, white-boxes, and gray-boxes testing methods , the white-box methodology is the most feasible one, which requires the least amount of resource usage while providing optimum security assessment.

5. Case Studies

In the V2V and V2R communications, prevention has been usually viewed as a less effective approach for security and safety. Instead, detecting attack and taking remedial actions are the main strategies. Another fundamental point for V2X system's safety and dependability is using machine learning technique to pre-observe the vehicle's abnormal behavior in real-time in order to bring to notice the malfunctioning of the mechanical parts of the vehicle. Various techniques are used to digitally prevent the dependent entry of attackers by reconfiguring the system. In parallel to the detection techniques, the architectures of the VANET network also need to be modified using different dynamic layers' arrangements [1].

Vehicular Ad hoc Networks or VANETs encompass a broad scope of intelligent transport systems (ITSs), where dynamic communication among vehicles and roadside infrastructures enables various types of vehicle-and-roadside or vehicle-to-everything (V2X) applications to cope with the traffic, environmental, and safety concerns. VANETs usually fall into a semi-enclosed system. The vehicular communication does not involve an access point that serves the vehicles alike laptop, smart devices and others connecting to a wireless local area network (WLAN). Instead, the vehicular data exchange is done through vehicle-to-vehicle (V2V) communication and vehicle to roadside intelligent traffic lights or road signs (V2R). In V2X, the vehicles are actually two types of devices. From a network perspective, both the vehicles and the road infrastructure, such as the traffic lights, are on the same network system, typically employing cellular networks, for their communication. The main adversary of VANET is cyber attackers to derive unprecedented rewards.

5.1. Real-world Implementations

Efficient communication system has been recognized as an important factor and a prerequisite for the overall success of AVs. The communication models in AVs are broadly classified into

vehicle-to-vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P) and vehicle-to-cloud (V2C). The summary of security goals proposed by patents as mandatory, integrity, authenticity, availability and confidentiality for self-driving test beds and real time deployments^{5} by closely examining the research literature and patents for sterility protection on self-driving communication systems exposes several repeatable challenges and opportunities [2]. After detecting misbehaviour which was found in communication systems of self-driving testbeds various objectives could be fulfilled if the security measures are enforced vigilantly.

Self-driving cars (also known as autonomous vehicles or AVs) have seen a surge of interest and investment in recent years. According to several research reports, the global market is expected to be worth $45.8 billion this year and could reach $467 billion by 2027 [16]. Companies such as Tesla, Uber, Volvo and Google are developing unmanned cars to make mode of transport safer by reducing human errors and improving mobility. Nonetheless, the crux of AVcrime is based on its communication systems which can be compromised, jeopardising network elements and other cars on the road (Swamy and Puttini in Telecommun Syst 62(1):5–25, 2016). A single act of mischief may result in life-threatening and significant financial losses. The major security challenges for AVs include but are not limited to misrouting, false data injection impersonation of legitimates nodes and node (s) traffic analysis. To overcome these challenges, this article briefly discussed the collaborative model in AVs, the security requirements, taxonomy of cyber-attacks, security strategies proposed by researchers, secure of communication protocols for self-driving networks (Supraja and Sathya in Wireless Pers Commun 9:1–1, 2020). Last but not least, the open challenges and research opportunities are elucidated.

5.2. Lessons Learned

The smart vehicle and the autonomous vehicle components are software, networks, and sensors, which are directly integrated with each other. Therefore, if any of these operational components fail to function properly, robustness and interoperability may be affected, resulting in damaging the road traces in terms of causing the user's death or threatening the autonomous vehicle environment directly within the vehicle's vicinity. Recent achievements in the survey of novel prediction models as a multi-model approach, hybrid-compatible self-defense operational frameworks by Virtual coaching and Digital Trust architecture, these results to improve the response and system robustness in terms of the optimal decision-

making models by selecting approaches of data used in the empirical multiple learning algorithms the physical modeling, cloud-based solution robustness, intrusion detection in the multi-layer approach. New intrusion detection algorithms, mutual authentication honey protocol new hybrid MAC protocols, new machine learning-based data mining hybrid machine learning techniques, the navigator scriptf is to use reinforcement learning and script data mining successfully employed in the infrastructure of a novel computational intelligence model that uses a directional approach for autonomous navigation operations. [17]

Various network simulator tools, such as Omnet++, Ns2, Ns3, and Opnet which are well-suited to simulate autonomous vehicle networks, and the properly explored challenges and opportunities regarding anomalous event identification have been misjudged [18] throughout this section. Anomaly detection is a security best-practice method that has been widely used to identify network attacks driven from the users' network communications, system-wide access mechanisms, and internal attacks based on decision-making accuracy of false-positive alerts in terms of network and system security. Anomaly refers to the ability-driven behavior of smart devices in determining the features of collected data that might differentially achieve sensor-based and actuator-based operability. For instance, a shift in sensors' and effectors' feature-level functions may introduce unexpected behavior, the network is largely non-linear, and the response instabilities produce structural changes on the data dynamics. Anomalous patterns of smart devices compared to normal operational patterns indicate that the normal classical vehicle activities such as driver preferences and users' transport services are seen as a normal realization of operating states.

6. Conclusion and Future Directions

We have outlined model designs which utilise the occurrence of individual vehicle-to-vehicle messages, as well as the sequence of events that results from such activities within the intelligent transportation systems ecosystem. These models, utilised in concert with machine learning to evaluate and predict the network state and potential associated vulnerabilities or characteristics can be used to make predictions about various communication based performance constraints in the network such as delivery dates, and eventually, exploit data to threat vector inference. These models as end game come with their own inherent advantages, as they allow predictions to be made on current and historical network state to be based exclusively on the message content that comprises the vehicle-to-vehicle communication over

a given period, addressed in Recurrent Neural Network (RNN) and Long-Short Term Memory (LTSM) models to address that the factors used to generate a sequence of messages can have an important bearing on their predictive capabilities [19]. Therefore, we are confident that given extra information about an attack within the vehicular network, our RNN model configurations can provide the best prediction to the rest of the models under investigation. This is not least because RNN models are specifically geared out to work well on sequence data and automatically take nested messages as input where other techniques do not. We also found that the use of other network state information as inputs in these models was always harmful to their overall predictive capability.

The goal of this paper was to explore new approaches to detecting and defending against a variety of threats to vehicular communications, namely the use of network events and adversarial learning to predict delays and attack vulnerabilities and exploit in the network and the use of a cascading model of machine learning to detect attacks leveraging these and other threat vectors [20]. The work herein involved applying established statistical models to data which has derived from real world vehicular communications [8].

6.1. Summary of Findings

Joint adversarial strategies against autonomous coordinated-driving have, for example, been discussed in, and a spoofed GPS strategy for attacks has been suggested in. Several defenses are proposed in, but could only be partially adapted to preclude adverse attacks on autonomous vehicle coordinated driving. A summary of the defenses in that have direct relevance to autonomous vehicle coordinated driving security are as follows: To protect Al components, such as the perception module, from adversarial attacks, additionally proposes a setup where the wireless sensor data from surrounding vehicles is directly streamed into the autonomous vehicle, without passing through the ego sensing module. This essentially adds a form of ground truth to the training data and makes the system more robust.

Vulnerable interfaces such as the CAN-bus and malicious messages pose serious threats to the safety of autonomous vehicles [16]. In [17] we found that sensitive information contained in transmitted sensor data (heat-maps, observed traffic patterns, etc.) could be used by an adversary to gain insight into a vehicle's sensor configuration and subsequently launch attacks. As low level DoS and query-reply based attacks would require significant energy and channel access, we inferred that adversarial pollutants sent on an infrequent basis, and

poisoned training data for V2V models (where the attacker has a software defined radio to transmit broadcast messages and can see the impacts of AI-adversarial pollution on sensor measurements) would pose significant threats to the vehicle's stability. According to [21], the error in perception caused by adversarial attacks could reduce the likelihood that a hop from the autonomous vehicle to the edge server would be carried out successfully. Consequently, the unreliable network hop would be skipped and coalition messages would not deviate from their current route.

6.2. Emerging Technologies in Network Defense

Emerging technologies have enabled various platforms and networks to maintain network security and improve the capacity to handle the dynamic attack model. Various virtualization techniques and reconfiguration strategies have been taken in last decade to tackle the zero–day attacks through anomaly detection mechanisms as well as policy–based defense mechanisms [18]. The anomaly detection techniques are implemented to mitigate zero–day attacks along with proper policy settings; however, the virtualization replica is fully reliable and secure or not is also the major concerns. Therefore, the network defense systems are not capable of capturing those attacks that are within the network and also policy settings could not ensure network security holistically. Therefore, it is important to detect and eliminate the insider and zero–day attacks along with virtualization and reconfiguration policies settings, also. In order to secure the advent of cyber-physical system (CPS), smart grid, VTS, and social networks, increased based on physical injury (s) in a timely manner and with neural network and soft coEIT as a secondary methods are useful in a 4Deferred Outage and cyber safety and security division.

Traditional network defense architecture is not sufficient to manage the security of emerging technologies and protect networks from various cyberattacks. Legacy network defense strategies are designed to monitor incoming and outgoing traffic and detect known threats through legacy signature–based techniques. However, these legacy defense architectures are not capable of capturing insider threat activities and are not able to detect zero–day attacks [1]. Therefore, the network defense systems should be capable of capturing insider threats and detect zero-day attacks. In case of a large-scale network, the traditional defense technique is not capable to examine every node thoroughly and minute-by-minute manner; therefore, advanced defense strategies should be capable to holistically ensure avoid insider threats in time and space, till the attacked node is quarantined and eliminated its bad attributes.

7. References

[1] Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

[2] Tatineni, Sumanth. "An Integrated Approach to Predictive Maintenance Using IoT and Machine Learning in Manufacturing." *International Journal of Electrical Engineering and Technology (IJEET)* 11.8 (2020).

[3] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov

[4] A. Talpur and M. Gurusamy, "Machine Learning for Security in Vehicular Networks: A Comprehensive Survey," 2021. [PDF]

[5] J. Xu, S. Hu, J. Yu, X. Liu et al., "Mixed Precision of Quantization of Transformer Language Models for Speech Recognition," 2021. [PDF]

[6] 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]

[7] M. J. Kang and J. W. Kang, "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security," 2016. ncbi.nlm.nih.gov

[8] 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]

[9] K. Halba, C. Mahmoudi, and E. Griffor, "Robust Safety for Autonomous Vehicles through Reconfigurable Networking," 2018. [PDF]

[10] M. Chowdhury, M. Islam, and Z. Khan, "Security of Connected and Automated Vehicles," 2020. [PDF]

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

[12] T. H. H. Aldhyani and H. Alkahtani, "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity," 2022. ncbi.nlm.nih.gov

[13] M. Dibaei, X. Zheng, K. Jiang, S. Maric et al., "An Overview of Attacks and Defences on Intelligent Connected Vehicles," 2019. [PDF]

[14] A. Molina-Markham, R. K. Winder, and A. Ridley, "Network Defense is Not a Game," 2021. [PDF]

[15] M. N. Injadat, A. Moubayed, A. Bou Nassif, and A. Shami, "Machine Learning Towards Intelligent Systems: Applications, Challenges, and Opportunities," 2021. [PDF]

[16] T. H. Luan, Y. Zhang, L. Cai, Y. Hui et al., "Autonomous Vehicular Networks: Perspective and Open Issues," 2021. [PDF]

[17] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]

[18] H. Peng, Q. Ye, and X. Shen, "SDN-Based Resource Management for Autonomous Vehicular Networks: A Multi-Access Edge Computing Approach," 2018. [PDF]

[19] A. Di Maio, M. Rita Palattella, R. Soua, L. Lamorte et al., "Enabling SDN in VANETs: What is the Impact on Security?," 2016. ncbi.nlm.nih.gov

[20] H. Baharlouei, A. Makanju, and N. Zincir-Heywood, "ADVENT: Attack/Anomaly Detection in VANETs," 2024. [PDF]

[21] Y. Deng, T. Zhang, G. Lou, X. Zheng et al., "Deep Learning-Based Autonomous Driving Systems: A Survey of Attacks and Defenses," 2021. [PDF]