# Hybrid Threat Detection Models for Cybersecurity in Autonomous Vehicle Networks

*By Dr. Luisa Mastroianni*

*Associate Professor of Information Engineering, University of Florence, Italy*

## 1. Introduction

For the first time in the academic literature, the contributions made in this paper were designed and implemented for our proposed hierarchical anomaly detection model for EVs "ABLE" and "NADINE" [1]. These two algorithmic models have been integrated to perform as feature aware supervised anomaly detection models predicting vehicle type, wireless network performance and attack impact cluster under the hierarchical abnormal behaviour classification. The results demonstrated an increased detection accuracy and specificity compared to a single shot model. The performance improvement of both the models is supported by being able to handle data in a more insightful manner when making feature-aware decisions in detections.

Cyber-attacks targeting the in-vehicle network (IVN) can be particularly dangerous for autonomous vehicles (AVs). This is because AVs rely on sensory and environmental data from the "outside world" (e.g. lidar, radar, camera data, etc.) to make decisions about their trajectories, while also being able to interconnect with the rest of the world in some way [2]. Therefore, the impact of an adversarial attack can be far-reaching. With this thought in mind, the potential risk of conditionally undetectable stealth attacks on security-critical features within an AV has prompted us to propose and develop novel machine learning solutions for constructing the anomaly detection models.

### 1.1. Background and Motivation

Security threats in the area of vehicular system control and automation have attracted a lot of attention in recent years. Autonomous vehicles (AVs) make highly dynamic use of information, adding to the complexity of the system. The need for security in autonomous driving results from the ability of intruders to manipulate the state of automated components

such as electronic control units (ECUs), sensors, actuators, engine control unit (ECU), radar, camera, etc. This will have serious consequences for automated driving, the safety of passengers and other road users, increasing the probability of vehicle accidents. These threats pose a high risk for the vehicle. These have inspired designs based on multi-sensor fusion to provide control systems with high autonomy against cyber-attacks [3]. Multisensor data filtering, providing a high degree of system awareness, derives from an area of computational intelligence where different input data of the same object or phenomena are utilized in decision-making processes. It allows to obtain signals more realistic than the sum of information from separate sensors. The state recognition of a machine can be shown to be one of the key uses of MFCI. Corruption and manipulation of real connection data are paramount to cyber-attack scenarios. These can cause a widespread destruction environment. This calls attention to the situation, i.e. them being exploited in a separate thread until the cyber attack becomes aware of the security risks related. To be aware of the attack situation and to estimate and identify different types of cyber attack, it is important to concentrate on the situation recognition from single and numerous source of information [4].

### 1.2. Research Objectives

Additionally, it is observed from literature of autonomous vehicles that, the ratio of developing solutions for preventing attacks in the future, the ratio of providing solutions to identify and secure the existing deficiencies of vehicles is significantly low [5]. As it is the industry's status quo in the past; new products are developed without paying attention to security, and then safety measures are created in the place. However, the potential threats, attack scenarios, and related security choices must be known before creating secure products in the area of autonomous vehicles and especially AVs. The main insights from this article are as follows: An overview about the possible attacks, exploits, and vulnerabilities for autonomous connected vehicles are provided. The study highlights the need for a survey for determining possible scenarios and their possible security precautions in CAVs. Attack taxonomy and details are provided: six main groups of potential attackers, twelve given examples of possible attacks on AVs by Greenberg in (IoTv, GPS and Internet attacks, Hardware attacks, Spoofed signals, Physical changes in perception, Overload and saturation and Remote control).

A significant amount of research is being carried out to develop well-founded security solutions for connected and autonomous vehicles (CAVs). In this subspace of security research, anomaly detection based security models and intrusion detection models are gaining popularity. Machine learning-based security models for in-vehicle network behaviour observation have attracted a lot of attention in literature [6]. However, to the best of our knowledge, no previous work in the literature has been focused on building a hierarchical in-vehicle network anomaly detection model, like the one developed in our previous research where our research focused on Hierarchical Anomaly Detection Model for In-Vehicle Networks Using Machine Learning Algorithms [1]. The main insights from this article are as follows: An anomaly detection model for understanding attacks on in-vehicle networks is developed. The model provides capabilities for detection of the presence or absence of attacks, if present, determines type of the attack. A two phase model is developed, the first phase details whether an attack (s) present or not, if they are present the model in the second phase determines their type and impacts on vehicles' safety.

**2. Cybersecurity in Autonomous Vehicle Networks**

One of the key challenges in ensuring availability and security of new communications technologies in adversarial environments—the focuses on which this chapter is based—has been the increasing sophistication of cyber attackers and their tools in finding the vulnerabilities in these networks. As the vehicle fleet becomes more autonomous and newly developed embedded systems and communications equipment for these systems become more reliant on complex software designed by a variety of sources, the surface area for attack is correspondingly increasing. These attacks encompass threats through various vectors, including the over-the-air firmware update processes, electronic control modules in vehicles, digitized architectures, on-vehicle wireless communication interfaces, external auxiliary devices through USB connections, and so on [6]. With millions of connected vehicles on the roads today, we are seeing that a single existing misconfigured system could more easily cause denial of service in these communication environments. This is a fatal consequence in the environment of safety-critical systems—such as those of the automotive industry. In the present scenario, the CSP is the primary point of the intervention by regulating the defaulted nodes that infringe security policy. Random walker tracker model is effective for detecting selfish, compromised, or data forwarding malicious nodes.

Modern advancements in the transportation sector are driving the increasing of connectivity and ultimately paving the way for fully autonomous vehicles [7]. For autonomous vehicles to be truly autonomous, they must have continuous connectivity to each other and to centralized infrastructure. In the connected autonomous vehicle (CAV) ecosystem, it is essential to have reliable and secure in-vehicle and inter-vehicle communication systems to ensure the safety of the passengers, the vehicle, and other vehicles on the road. The Department of Transportation issued a guideline for the security of vehicle control systems to address these risks; however, these guidelines are not mandated and are not legally binding because there is concern with backlash from car manufacturers that believe meeting these guidelines would raise the cost and time to bring their product to market.

### 2.1. Challenges and Threats

[line:0]==Challenges and Threats== The potential cyber threats and vulnerable entities that exist in connected vehicle networks are numerous. A broad range of cyber-attacks and related network issues can affect any of the interconnected soft or hard entities within the connected vehicle environment leading to various types of problems. These issues may include node-to-node transmissions, node-to-infrastructure element communications, and inter-infrastructure communication among Base-Stations (BSs) or Road Side Units (RSUs), as well as coordination and interoperation problems among different manufacturers' hardware and software components in the vehicle networks [2]. DoS attacks, routing attacks and identity faking are detected at the network layer and application layer (CoAP) attacks such as false messages flood and incorrect reporting of state. Reliability and security of data must be taken into account for the exchange of vehicular data, in particular for safety related messages. Accordingly, how the quality of data and legitimacy of data producers can be checked and ensured deserves particular attention among researchers [8]. During their funneling of data to the connected vehicle network, connected vehicle networks safety applications must be adequately protected to prevent potential security breaches. Wrong information in the warning message might cause the crash to happen, some code injection attacks such as denial of service, or false data injections or be initiated and transmitted into the network. Intrusion Detection Systems (IDS) are a security component that monitors and controls data and messages that pass through the vehicle networks and in this way help to assure that only the authenticated information, messages, and data are allowed to circulate through the vehicle networks. The new hybrid model works fine on the traffic of the combined car-hacking based

on the dataset of usenixandbotnet dDoS in the network of vehicular networks with F1-score as 96.3% and 94.3% respectively. In the case of model-based attacks represented by neural typical attacks and fuzzing, the detection performance of the hybrid Intrusion Detection System is highly efficient [9].

### 2.2. Existing Security Measures

ID-based cryptography and a novel multi-layered and privacy-preserving sensor cryptosystem for secure V2X communication ensures that the identities of legitimate vehicles are protected-while ensuring the funniness of the V2X environment with time-stamp and local encoding mechanisms and Charlie values The optimal controller chosen plays a crucial role in ensuring the security of AVNA. Both the state observer structure and the controller have been optimized to cooperate in real-world algorithms to design detection systems capable of accurately and efficiently detecting cyber threats and intrusions [10]. Two detection frameworks for V2I communication have been designed: A time-series change point model that detects when smart nodes are hacked and A Long-Short Term Memory neural network that determines if enemies are nearby. On the basis of these strategies, this paper establishes a detection strategy for AVNA.

Various defense strategies exist that can help in identifying and eliminating cybersecurity threats. Currently employed cybersecurity techniques rely on cryptographic and blockchain-based systems, vehicle security architecture strategies, security-focused vehicle-to-everything (V2X) communication, machine learning-based security system approaches, and security-focused hardware-based designs . Vehicle security architecture strategies provide specific layered countermeasures to provide protection at individual layers, including case detection, intrusion detection systems (IDS), intrusion prevention systems (IPS), and firewalls ; security-focused V2X communication employs encryption and authentication for secure V2X communication, including ID-centric security system, revocation mechanism, periodic rekeying procedure, and new hybrid anonymous and non-anonymous authentication mechanisms ; and machine learning-based security system approaches can be either standalone anomaly detection approaches or hybrid anomaly and signature-based detection with an early-disconnection system exploration strategy that explores models to identify threat patterns, in order to ensure the effectiveness of detection and the detection of potential model backdooring.

## 3. Hybrid Threat Detection Models

module is very significant in order to identify and recognize the threat revealed on the network. Therefore, it is continuously open for attacks, 24*7, in the ideal scenario. Hence, profile based network monitoring along with imperfections of the profile, always remains very demanding task. Therefore, trained-to-trust sensor has been developed to recognize the intended and unintended attacks in association with the network protocol specification [11]. In our findings, trained-to-trust sensor is proposed in the physical layer of the intelligent vehicle in forms of secure virtual vehicle countermeasure to provide physical network protocol profile to recognize the anomalies in the network sensed information. This is then propagated to the intelligent vehicle domain. For this purpose, responders' nodes are aware of the vehicle bus physical specification. Responders' module also learns the network behavior without manual annotation. The batch of data provided by the vehicle physical protocol provider is fed to the network physical protocol profile builder tool.

modern vehicles are composed of electronic control units (ECUs) that are linked through an in-vehicle network [12]. This mechanism has substantially developed in recent years due to technological growth and demanding safety and comfort features. Various in-vehicle network protocols are used for this purpose such as: Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, Ethernet, etc. Modern automobiles have the capability to connect with the external networks as well. This brings features such as Remote Diagnostics, Uninterrupted Internet, Satellite Navigation, Intelligent Socio-Parking, etc. Modern Cars also use various sensors, Global Positioning System (GPS) receiver, cameras, LiDAR, and other hardware that are known as the peripherals connected with the advanced vehicles [6]. Based on their data and information, various new features have been planned for driver safety such as Intelligent Parking Assistance System, Autonomous Driving, and Environment Data such as Carbon Dioxide, Air Ratio, etc. These features, on the other hand, have opened the doors for the attackers' domain. Attackers remain interested as they can pose threat to the road safety and passengers. This provides an open challenge to the network security community in terms of maintaining continuous monitoring, detection, recognition and counteraction on the transported network.

### 3.1. Definition and Overview

Automotive networks record many driving vehicle states and infotainment data. The physical distance of vehicle buses is short, but it is exposed when this data is trafficked outside the vehicle. It was confirmed that attacks on external networks caused operations on the inside of the vehicle. When a threat occurs on any internal and external network, it can cause a cyber-physical system that cannot be used. In addition, some vulnerabilities in automotive systems have been tested and proven by car hackers. Therefore, in order to provide safe autonomous vehicle services, secure and robust protection measures must be secured.

[1]When autonomous vehicles are running in the external environment, they are connected to various networks. When a threat occurs in an external system, or when the operation of the entire network is destroyed through DoS attacks, etc., the vehicle network can be damaged, which is fatal for people's lives and the vehicle [11]. It is required to have a high level of experience in detecting attack activities for the autonomous vehicle control system under such environments with various network technologies. An anomaly-based approach can help to identify new attacks and improve the ability to detect never-encountered attacks, in contrast to using pre-defined rules [13].

### 3.2. Types of Hybrid Threat Detection Models

Multi-Tiered Intrusion Detection System (MT-IDS) primarily processes data on the edge. This redundancy ensures faster processing when compared to more complex methods that require multiple systems to work together. In introducing Anomaly based Detection, an anomaly is defined as data that significantly differs from known data. This data can be related to the size of attack data, missing values, new values and out-of-norm values. This subsystem is described in more detail in section 8. The scheme of this is such that each of the automotive units will calculate multiple times. Then a decision can be made by a majority vote. The source data is not obtained from a real-world network. After a normal behaviour based acceptable output, the improved method is introduced with added attacks and with expanded test scenarios. The Multi-Tiered Intrusion Detection System is defined in Section 2. Its working model and advantages are mentioned in Section 3. Section 4 analyses the dataset used while the output of the system is discussed in Section 5. The results are believed to support novice researchers and prospective new vehicle manufacturers by providing essential information regarding the expected detection rates from both the individual systems and the combined system.

CAn and its higher-layer protocols lack the ability to protect against modern cyber-security threats, and vulnerabilities remain widespread across Vehicular Networks. Intrusion detection systems can be used to monitor traffic and report when anomalous activity is detected in order to prevent data injection attacks on these communication links. Machine learning methods have been identified as one of three types of vehicular environment detection mechanisms in prior literature, with one-class classification methods such as one-class Support Vector Machine (OCSVM) and Support Vector Data Description (SVDD) found to be particularly promising for supervised classification tasks. In this work, we investigate the use of a one-class classification model for detection of data injection attacks on a CAn bus in a vehicular environment. Using record level labels to simulate an anomaly detection scenario, both OCSVMand SVDD are tested for the same task, exploring and evaluating the performance of each method under minor and major user-to-injector vehicle distances. We demonstrate the potential of one-class classification methods in the detection of modern cyber-security threats on a Vehicular Network by demonstrating reliable attack detection and discussing its usability for future applications.

**4. Data Sharing Mechanisms**

Autonomous vehicles (AVs) are the new generation of vehicles equipped with sensors and global positioning systems. AVs' sensors enable them to gather information about surrounding environment, vehicles, and traffic whereas Global positioning systems help AVs to maintain knowledge of their own position. In autonomous vehicles, intrusion detection systems (IDSs) are necessary to monitor communication data, information and provide possible solutions in the presence of cyber-attacks, and protect information being transferred, maintained, and transferred between vehicles. Hybrid IDS models have been proven to be more accurate than traditional ones. Thus, in this paper, we design an end-to-end hybrid IDS to achieve three key functions—prediction of vehicle locations, time to collision (TTC) estimation, and security threat detection. Typically, data sharing among AV can be done in two ways – direct data sharing and proxy based data sharing. However, both of these techniques have some disadvantages like unreliable direct data sharing in short range communications, high usage of bandwidth and higher response time via proxy.

Vehicular Ad Hoc Networks (VANETs) constitute a special type of wireless Mobile Ad hoc NETwork (MANETs) [14]. A VANET is a sub-class of Mobile Ad Hoc Network (MANET) that

contains vehicles with Mobile On Board Units (MOBUs) such as GPS and small computing devices in roads [15]. VANETs fall into two categories, namely vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) in which vehicles communicate with nearby vehicles and receive beacon messages and Roadside Units (RSUs), respectively. Keeping in view that security threats are increasing in both vehicular communications, and with each passing day, several kinds of attacks are introduced. As the existing solutions of dealing with security threats in VANETs are not adequate [6], hence it is necessary to have a solution based on a new data sharing mechanism among several vehicles within the network. This will enhance the security in VANETs.

### 4.1. Importance of Data Sharing

While protecting computerized vehicles on the intrusion detection system (IDS), the sensor feeds and the car two X network IU. The IDS supervises and protects internal car connections (CAN bus, .). This method guarantees that an attacker is unable to send or change secure data in an automated vehicle, although the focus was limited on security issues by hacking vehicles and vehicle-to-vehicle (V2V) communication. This objective is one of protecting V2X interconnections from the perspective of overall security as well as ensuring that the vehicle does not take any insecure drives.

The speedy deployment of hardware technologies in automatic vehicles makes driving easier, more comfortable, safer, and faster [16]. Any sensor using automatic vehicle to assess the environment and decisions taken by the neural network also engage in the process. This could have an impact if attackers target the automatic vehicle, leading to hijacked cars crashing in targeted zones to determine the threatened information of the vehicle [15]. Other aggressive assailants are also easy to imagine using that any form of V2X bypasses such as vehicular attacks to Road Side Units (RSU), customer to customer, user to infrastructure, etc.

### 4.2. Privacy-Preserving Techniques

Another option is to use Homomorphic encryption techniques to train a model in the encrypted representation of the data set of each vendor. Then, the models of each vendor in the encrypted space are together to form an encrypted model, and the information in this encrypted model can be transferred to the other vendors' private keys in a parallel way. The final global model can be received in local encrypted models, allowing each vendor to decrypt

their global models with their private keys. The final decryption step returns the prediction model and ensures data privacy [15]. This feature could be a solution for a collective training of simultaneous models of each vendor in a joint way, affected by anomaly reduced rate.

This section describes a privacy-preserving technique based on federated learning to train effectively a global model without requiring the exchange of the individual vendors' customers [2]. The specific technique, federated learning, was proposed by Google in 2017. Instead of transferring data to the cloud, the learning algorithm is transferred to the data source (i.e., the vehicle), and a part of the model is trained locally, in each connected vehicle, based on the local data of each one. Then, all the partial models are merged, and a new global model is trained. This model can be used for the detection of anomalies or for any other application that can be useful to increase the security in connected car networks [1].

**5. User Privacy and Data Integrity**

[ref: 49fe447b-1838-495e-b4d7-6c86a7a2cbe2;3bc39819-0b49-4002-b9bf-4fa73facfd9c] There is significant potential for cyberattacks to have a substantial impact on the safety and physical integrity of the occupants of connected vehicles. Thus, it is imperative that cyberattacks launched against any of the aforementioned internal and external connected vehicle layers be detected and identified in a proactive manner. There are two major schools of thought in this cybersecurity domain: signature-based detectors and anomaly-based detectors. The former approach observes network packets and application performance in real time in order to detect specific patterns, and is capable of detecting only attacks for which there are associated patterns (signatures). This contrasts with the latter – or signature-free – approach which, rather than observing signature patterns, compiles a baseline behaviour profile via an agent installation, and subsequently evaluates nuances to identify and isolate malicious behaviour.

[6] One approach for maintaining user privacy and data integrity in connected vehicles is to avoid broadcasting unnecessary information. Another alternative solution is to encrypt the broadcast information so that the information stored in the D2B computer does not reveal any sensitive details regarding the vehicle and the occupant(s). Combined with these approaches, in-vehicle communication cybersecurity could be sustained via the implementation of vehicle-specific keys, for vehicle identification and authentication. This solution would discourage unauthorized persons/users from accessing any proprietary or private information about the occupants and the vehicle.

### 5.1. Key Principles

In this context, we must consider two prominent challenges. It is currently assumed that the controllers in vehicles permissible for cyberattacks are solely local networks. Nonetheless, the entire vehicle software stack can be reached by extra-vehicle target computers for network externalities and predictable side effects. Autonomous vehicles must be indistinguishable from human-driven cars, so external target computers cannot distinguish between normal vehicle operation and flaws. This has direct access to the vehicle's ECUs in analysis mode, allowing manipulation through virtually every physical signal and privileged access to the OBD-II port. This permits packet reconstruction of every controller in the vehicle (often the most sensitive one opening a direct gateway into the vehicle's network). Results reported in the literature have indicated the possibility of successful cyberattacks on the vehicle's local network from research on real vehicles have included locked doors, engine key cycles, and emergency brake interventions. Such attacks bear close similarity to electronic control units (ECUs) interferences encountered during the normal operation of the car. In short, academic results support the realistic nature of our considered threat scenarios. An in-depth and operational awareness of hybrid threats (cyber-physical attacks) to a car is critical for safety-aware designs and comprehensive risk assessments [1].

In the previous section, I summarized several successful models for detecting cyberattacks within a vehicle's local networks, or for recognizing different states of cars. In this section, I argue that robust models for detecting a vehicle's states/diagnosing potential risks of vehicle controllers require a fundamental paradigm shift. To protect a vehicle from potential dangers, such as anti-autonomy technologies [10], researchers must construct vehicles' libraries of normal behavior (car's "physics") and provide models for recognizing anomalous events and determining their causes [17].

### 5.2. Technologies for Ensuring Privacy and Integrity

In the in-vehicle network, the Controller Area Network (CAN) operates in a honeypot network, thereby preventing interference in controllers, as privacy and integrity are necessary to prevent attacks on the network. Privacy issues can arise due to sharing of IVN data for legitimate IPSS and also affect passengers' safety. IVN attackers can disturb the systems of an original vehicle, preventing any communication in the CAN network and causing big losses. The proposed anomaly detection method enables monitoring of ISPs in vehicles from real-

time zero-day attacks to unknown and known attacks, as well as exceptions. The training of command, request, response, and event datasets was carried out using the generated data which are distributed to the input layers of convolution operators using deep models [1]. The validation of the model, which creates the same architecture with the training environment and uses the same model and the same environment data, was good with an accuracy ratio of 100%. The proposed model is compared with various algorithms in the light of real-time anomaly detection and resource requirements with excellent results. All the experimental comparisons revealed that the proposed model achieved higher true positive and lower false positive rates than the other detection algorithms. The main goal is to protect against attacks, ensuring privacy and integrity in real vehicles through a study that can detect ISS anomalies with maximum efficiency.

Security and privacy are major issues regarding vehicular network communication, and researchers have proposed several techniques for analyzing attacks on connected vehicles. The communication systems also have challenges such as heterogeneity, mobility of nodes, energy constraints, and time-sensitivity. Current security mechanisms are inefficient due to susceptibility to adversarial attacks, limited detection capabilities, high latency, and significant computational resources [18]. This report proposes hybrid threat detection that shows optimum values while considering the real-world conditions and analyzing outputs of multiple attack detection models in a much more effective way rather than state-of-the-art MATLAB simulations. Key difference to the related works is that this study implies lower level physical data layer anomaly detection algorithms' output into upper layer communication based suspicious behavior analysis instead of utilizing only one model. Combining the best performing attack detection models for cyber-physical hybrid threats results in a more robust security in vehicle networks. It is also crucial to ensure data integrity, on which this study focuses by considering intrusion detection literature and discussing signature based, anomaly based, hybrid anomaly and signature based, and machine learning based methods. Given the complexity of vehicular networks, the relatively high number and most importantly the black-box nature of the underlying physical layer Channel State Measurements, the effectiveness of hybrid anomaly detection in validating or disregarding the information manifestation in the upper MAC and Application layer protocols is also investigated.

**6. Experimental Evaluation**

6.3. Drumming Down Attacks (DOW) and Jamming Attacks in Sensor Nodes and LD in AECS: Simulations consider car leading and car following scenarios in which the data propagation for Denial of Service (DOS) and jamming attacks are observed and verified. For the lead car scenario to the follow car, a DOW attack from the LD can halt the functions of the lamps and the LD will not be able to perceive the rear surroundings. For the LMS, a LD can disengage the normal working pattern of High Beam and Auto headlamp systems. As a result, any resultant accidents and mishaps with other cars or any pedestrians can occur. For simulating jamming attacks, if an LD of a vehicle/car is sending false warnings or false data for controlling a FLC or lamp functionalities, then jamming occurs and it ultimately postpones the commands for controlling the low beam, high beam, and foreshadowing headlamp control systems [6].

The presented methodology has been employed to manage cyber-attacks in an in-vehicular communication network leading to a heterogeneous connected network. The provided mechanisms are highly beneficial for the protection of autonomous vehicles from cyber-attacks. The hierarchical fuzzy generative network (FGN) serves the purpose of an optimal anomaly detector with its adaptive tuning mechanism. Robust mechanisms to monitor the new threat of physical security, i.e., collisions and accidents, are also being handled by the FGN. RCNN image processing is conducted to develop countermeasures for adversarial attacks on the camera sensor in autonomous vehicles. Finally, the interoperability of homogeneous and heterogeneous connected networks in autonomous vehicles has been established for the aforementioned threat and attack models. The findings of the experiments highlight that the proposed methodologies perform exceptionally well in anomaly detection and also reject adversarial attacks presented to adversarial learning models. All experiments were carried out in a real environment, and toxic and adversarial attacks were also introduced in multiple experiment iterations. However, instances of the tests are different, with specific dedicated probabilities for the occurrence of cyber-attacks. The analysis is obtained and performed across various networking scenarios trying to generate different traffic loads.

We presents an experimental study to evaluate the proposed tuning methods and mechanisms of a hierarchical fuzzy generative network (FGN) and adversarial learning-assisted generative network (AGR) designed for detecting cyber-attacks in the communication network of autonomous vehicles in real time [13]. The proposed methodology involves hierarchical data analysis, machine learning algorithms, data-mining techniques, and RCNN

image processing. DDoS, Man-in-The-Middle (MITM), replay, impersonation, and jamming attacks, and various cyber-physical threats have been addressed [19]. The vehicle's CAN, such as different ECUs and their sensors-related data, followed by the in-vehicular network, such that the images of the vehicles on a scene are further utilized to generate optimal tuning mechanisms handling cyber-attacks on sensors. As a thorough part of the experiments, significant attention is given to carry out empirical analysis on the fundamental robustness, tuning behavior, and preservation of quality of service (QoS) offered to legitimate applications while handling cyber-attacks and new cyber-physical threats.

### 6.1. Methodology

In the present article, 'Detecting stealthy cyberattacks on adaptive cruise control vehicles: A machine learning approach' [20] is concerned with the detection of compromised automated vehicles within a dynamic traffic flow context. Specifically, a machine learning approach is proposed to develop a detection model for a smart vehicle equipped with an adaptive cruise control (ACC) system. The model utilizes the raw sequence of longitudinal velocities \((v_i)\), confirmed by both car-following models and real-world data. A promising Generative Adversarial Network (GAN) is developed in three different scenarios that pose a variety of potential attacks that can be witnessed in the real world, recently, and in the near future.

Transportation networks encompass many privacy-critical and safety-critical systems, such as connected vehicles, connected transportation systems, and vehicular ad hoc networks (VANETs). For these emerging systems, mitigating the risk of cyber threats is not an afterthought but intended as a paramount design requirement. In this article, we focus especially on one representative real-world design scenario: connected vehicles. Following this requirement, many cyber-security and ANTISECURITY (resilience to cyber threats) techniques have been devised for all emerging and connected transportation ecosystems, amongst which increasingly critical are driver-less, connected, autonomous vehicles (CAVs). Above article, 'Hierarchical Anomaly Detection Model for In-Vehicle Networks Using Machine Learning Algorithms' [1], presents a hierarchical learning mechanism which is capable of real-time, open-set, and self-supervised learning. The hierarchical learning model has been considered semi-supervised in which the learning objectives at the three hierarchical level are associated with different objectives and methods. The hierarchical learning model

allows the information fusion in hierarchical representation models which promotes the discrimination capacity of the neural networks, and hence increases their interpretability. In the source code we designed the number of sub-clusters as n3 and n4 for classification and novelty detection, respectively.

### 6.2. Results and Analysis

To improve the behavior of the first types of models, they need to consider how the system will react to the attack when estimating the final judgment. Models of that type include in particular fault diagnostics, control and monitoring models encountered together and separately during HMI studies, as discussed in. Moreover, these strategies offer the possibility of widening their scope to computer or perception level attacks. On another scale, they can also be used to combine different feature spaces from the car subsystems to increase the robustness of the model.

The most conventional detection model receives communication and event information. Their behavior is then anybody's guess and you must hope that the attack does not look dissimilar from ordinary mistakes and crashes, especially since the other vehicles will hardly ever be able to see the error produced by the attacked unit. Another solution is to use detailed information from the vehicle's dynamics, such as the neural network approach used in [21]. This method is a convenient way to use highly heterogeneous information by exploiting simulators to generate large datasets. Nevertheless, the dimensionality of the inputs and the presence of outliers make it more difficult than a classical approach to filter the candidate threats in a timely and reliable manner.

This Section provides an evaluation of the main strategies to detect cyber threats in a mixed network of autonomous vehicles and a human driver [4]. We suggest that cybersecurity should also be considered within the testing of driverless vehicles, whether simulated or real, and that we contribute to a literature review. The starting points of this survey were the categories of attacks described by Poovendran et al.. We then conducted a review on hybrid threat detection models, and also consider two articles dealing with the detection of physical threats on the driver module, i.e., model (ii) in.

## 7. Case Studies

Certainly, intrusion detection in AV-network and safety critical embedded systems is a hard problem with multi-faceted challenges both from the cyber security as well as the anomaly detection perspective. Although potential solutions to these problems have been studied by academia, standards bodies, and businesses extensively during the last decade. Effect of Injections of DoS and EoA signals on Vehicular Flow Dynamics In our studies the analysis is performed on previously developed models meeting good explanations of traffic flow dynamics such as micro- and macroscopic flow dynamics models. At the micro-level, the rush inside the traffic flow are considered as single can in a sequence of automobiles. They follow one another at a distance which decays and alike two pendulums they swing around each other. Equations describing the conditions of distances between vehicles in particular time instants ripe the Traffic Flow Kagawa model [12]. Periodic formation of such platoon-like assemblies instead of homogenous flow in the system can be understood as a malfunction of vehicles – stable operation of the ACC system consisting of the vehicle affected by DoS attack is realized. Behavior controlled by ACC system corresponds to numerical solution of a system of two nonlin- ear ordinary differential equations.

Several instances of impact assessment of DoS and EoA cyber- attacks are presented in [21]. However most of these studies are focused on effect of malicious activities within the vehicular network. In this section threats which are realized in the vehicular network and may compromise the proper behavior of the system and lead to undesirable consequences in the physical world outside the consider network are also treated. The malicious activities are realized in the vehicular network, and their consequences extend to the behavior of the vehicle outside this network. We call this first category of deliberate attacks attack inside the vehicular network and attacks affecting not only the vehicle communication systems are called cross-layer attacks. High-Level Models for Attack Impact Assessment This type of malicious activities over attacker intended actions on the cyber, network and application layers severely compromise the vehicular network as the means of transportation. This class of attacks, cross-layer attacks raises also significant concerns since one network transaction in the form of parking or warning message can lead to failure of high level functions so if the threats of such nature succeed they can form scenarios to unexpected consequences which may lead to cascade effects in traffic congestion and others [20].

### 7.1. Real-World Examples

The second approach leverages the specific capabilities of the ISM mechanisms to fight and evade overfitting, avoid the performance collapse during the real-world application, and to enable the proper communication interface with the other actors, Welsh. For detecting the cyberattacks, such ISM core is provided by diverse target discriminators of the hit-and-run type each localized across a proper submanifold of the multi- and heterogeneous-space. The decision of alert or no alert is then based on the consensus of the majority of the whole committee composed by these independent sub-decision makers.

A variety of real-life application areas, including prototype systems, examples during the development of the Throttle Valve Control Unit (TVCU) of Ford F1,500 [22] and the experimental testing of a driving simulator [4] were presented. It is important to note that we designed a modular and versatile architecture, collecting real-time networking data at each of the four OSI layers, such as physical signals (PHY) and data link layer. The heterogeneous ISM-DNN we propose is experimentally compared with a DNN implemented over uniform common recurrent units The first was trained in a traditional manner, while we modified the standard training and inference procedure of the latter.

**8. Future Directions**

One of the weaknesses of the reviewed methods is their reliance on "the true condition of content" and "external condition of usage capabilities" for security calculation, which makes serious security weaknesses. Furthermore, the current approaches attempt to resolve the problem with the lack of data in training sets by using causality-based AI and machine learning methods. Additionally, they have been working to address the lack of synergy between detection, defense, response, and contradiction of AVs and the security protection diamond model against denial of knowledge-based security protection. Finally, one major challenge in defending the attacks against AVs in the future could also be the responsible authority's cooperation, which is essential to assess the full impact of successful attack strategies, understand the routes of risk acceptance, and block the occurrence of critical failures.

The principles and trends in the study of cyber-attacks against autonomous vehicles have been discussed in this book. Cyber-security threats have recently become one of the most critical concerns for autonomous vehicle (AV) technologies. In this chapter, we reviewed and discussed a few of the most important techniques and vulnerabilities of future AV

technologies with adversarial settings. We further outlined future research directions and discussed the challenges to solve for security threats of autonomous vehicles [2]. Incoming intelligence and learning-based methods, including intelligent intrusion detection, prevention systems, and adaptive security alert technologies, are the main solution for secure AV networks.

### 8.1. Emerging Technologies

In the era of intelligent autonomous vehicles, various vehicular data, such as trajectory data, sensory data, and communication data, provide the capability of detecting and diagnosing hidden behavior patterns from the view of cybersecurity, safety, and energy efficiency, which is defined as the in-vehicle network (IVN). To obtain the functional requirement of the vehicle control systems, the vehicles are integrated with different controllers and sensors [1]. All devices can respond to and send commands to each other through the electric signal when required. There is a vast amount of in-vehicle communication and coordination performed between various controllers for the automation of the vehicle. Autonomous controller engineering is critical in the present day for simplified car assembly. The complexity and interferences between the controllers in an automobile can pose systemic threats to cybersecurity and passenger safety. The unprotected restful connection between the vehicle and outside world can result in a multitude of attacks, including remote attacks, man-in-the-middle attacks, and intrusion attacks, which can lead to platform deformation and personal control loss\nstatus. The complexity and interferences between the controllers in an automobile can pose cybersecurity threats and affect passenger safety. To address this, we advocate the use of dedicated networks to run different operations. However, due to the usage of self-Managing techniques in in-vehicle networks such as the MQTT protocol, RESTful APIs, network sniffing can be used to access system inside information leading to more devastating attacks [8]. In this setting, we work on cybersecurity within the vehicle, performing the anomaly detection task detecting and diagnosing unknown behaviors in the present dataset.

Today, the automotive industry is investing heavily in cybersecurity because of a growing number of attacks, and it aims to develop policies for data security, protection of infrastructures, and inspection of user identity. Therefore, mechanisms for detecting malware and intrusion are required [10]. New mobile networks technologies are able to provide the idea of any service anywhere, anytime, and for any device, which has developed the internet

of vehicles (IoVs) from the Internet of Things (IoT). The incorporation of the 5G network with the IoV architecture allows the exchange of traffic information, road condition information, and accident warning information among different platforms distantly. Recent technology innovation in wireless communications, such as 5G and 6G cellular network systems, Wi-Fi 6 and 6E, V2X (vehicle to everything), V2V (vehicle to vehicle), V2I (to infrastructure), V2P (to pedestrian), and V2N (to network), has also increased the risk of cyberattacks, which can have severe consequences.

### 8.2. Potential Research Areas

The above-mentioned knowledge can create a flexible and highly efficient hierarchical anomaly detection model, which contains two main stages, to achieve the purpose of our study. The first stage, applied in the leader node, includes the regulation of periodic communications and the detection of internal violations and/or to measure the global state of the networks where also belongs to almost all existing detection models and controllers such as vehicle-related controllers. The second stage is separated as the detection stage of the leader node (i.e. globally existing detection) which involves not only the local detection for all members but also the detection of the threats via the study of the interferences between leader followers. This stage, which is more complex, so involves working data for many local events and thus realizes the core of our technical results. In the following part, we will analyze the application and practical advantages of the detection model by associating it with some threats which happen during CAN intrusions.

Interferences between controllers in autonomous vehicles can pose threats to cybersecurity and passenger safety. In this study, we analyze the potential of a hierarchical anomaly detection model that can detect threats early [19]. The interferences that can occur are complex and are not isolated. For instance, in the case of hierarchical controllers, it would not suffice to only consider the out-of-bounds or anomalous behavior of controllers as the existence of this status, in itself, does not necessarily mean that an anomaly or threat has occurred. By focusing on early detection, it becomes evens essential to evaluate the numerical behaviors continuously and in real time because of the severe potential impacts of the violations of controllers on the safety of the vehicles. Finally, to prevent false alarms, the level of the warnings for only certain types of violations with respect to the fixed thresholds must not be immediately labeled as the threats; but an activity, which would enable determining how

threatening this situation is, is required [1]. Therefore, we need more fundamental solutions in order to protect devices from the potential impacts of the interferences between controllers in autonomous vehicles effectively without being related to the traditional network security of communication systems of vehicles. In our study, we aim to present a more effective hierarchical detection model instead of several detection techniques in order to detect and finally cope threats without any need to produce results continuously in real time [23].

## 9. Conclusion

Theses security threats presented for CAN bus driving environment necessitate implementing effective intrusion detection system (IDS) models with high accuracy. In this work, a novel Ensemble-Long Short-Term Evolution (LSTET- IDS) method for zero to light level automation level vehicle environments is proposed in the context of deep-learning-based invasion detection problem. Stochastic threats such as false data injection (FDI) and sniffing attack are included as EV can be compromised by security threats, just like viruses and worms in traditional computer environments. In this paper, we developed a Generative Adversarial Network (GAN), more specifically a Wasserstein GAN (WGAN) that minimizes the earth mover distance, and trained it on sequential data with non-iid properties to learn underlying distributions of particular normal and malicious traffic using Wassersteindistance [20].

Threats often presented to intelligent connected vehicles (ICV) necessitates implementing effective intrusion detection models for the detection of malicious activities while achieving high detection accuracy. Department of Transport reports that there was a high number of vehicle collisions involving fatalities, or serious injuries in 2018 with many of these accidents attributed to human error. The emergence of ICV(C) technology can reduce these issues introducing relative new engineering challenges. Malicious vehicle hijacking, spoof attacks and wireless channel jamming funnels such incidents to proneness. Detecting and mitigating those attacks related to intelligent connected vehicles (ICV) is pivotal and crucial because it may lead to the catastrophic consequences in real-world driving environment due to the inherent complex messaging interaction that those vehicles augment into the transportation system. In this paper, a novel Can (controller area network) intrusion detection method named Ensemble-IogLoaroShTE (IogLSTET-IDS) for ICV scenarios with low-level automation levels is proposed [21].

### 9.1. Summary of Findings

Besides traditional IT security threats, connected and autonomous vehicles are exposed to several security infrastructure threats. In connected vehicles, where the communication is mainly between vehicles and infrastructure, the vehicle has to respond within a very short time frame (in a time lag from some milliseconds to several tens of milliseconds). Consequently, various cyber-physical infrastructure attacks (CPIAs) such as sensor flooding, remote control abuse, and data inconsistency may result in fatal crashes in real-world applications. The integrity protection of the infrastructure infrastructure is an inevitable need for supporting certifiable real-world autonomous vehicle platforms. The (possibly existing) vulnerabilities in the infrastructure may be exploited during the remote programming operations. The software upgrade vulnerability may result in undesired firmware mismatch and brick-up the firmware upgrade process. Similarly, the other software-related deliberate misconfigurations and setting-up issues may heavily impact the cybersecurity maturity of the concerned system [2].

Connected and/or self-driving autonomous vehicle (AV) systems afford significant security threats in a real-world environment [24]. It is important hardening those systems in a way to make them resilient to these threats. The first step in achieving this goal is to secure the communication among the sensors, decision making components, and controllers. Signal jamming and modification (usually through a man-in-the-middle setup) are the standard cyber threats against the communication network in traditional IT systems [25]. However, the autonomous vehicle communication networks are exposed to several additional threats as depicted in Figure 1. According to the research on 11.5 million connected vehicles in Europe by Connecthings, it is reported that around 583 thousand vehicles (5.5%) are adopting Android Wi-Fi, 11,749 (0.1%) are running MySQL, and 5158 (0.04%) are connected with MongoDB. These Android and MySQL driven systems open the door for specific security threats such as security loopholes, firmware modification, and data corruption.

### 9.2. Implications and Recommendations

The research community has been utilizing artificial intelligence and machine learning techniques for vehicle network safety monitoring and control. Specifically, most of the studies related to this field have focused on developing defense mechanisms and security models for detecting security breaches and mitigation of cyberattacks. In addition, most of the AI-based security management frameworks for vehicular networks are based on passive defense

mechanisms. Attackers are able to successfully bypass existing security solutions by evading detection through clever manipulation of entrada data, as observed in Google's Adversarial example [26].

In a related study [10], the authors developed an ensemble based methodology, constructed to monitor and detect malware and denial of service (DoS) attacks within vehicular ad hoc networks to prevent against data losses and obtain safe, and secure driving experience. Moreover, Mahjoub [6] identified various intrusion detection models, and employed a convolutional neural network (CNN) based network traffic for intrusion detection systems for vehicular networks. Several examples of both individual and ensemble based intrusion detection systems have been proposed in literaeure. However, real time activities for intrusion detection systems in vehicular networks are still in the preliminary stages.

**Reference:**

1. Pulimamidi, Rahul. "Emerging Technological Trends for Enhancing Healthcare Access in Remote Areas." *Journal of Science & Technology* 2.4 (2021): 53-62.
2. Tatineni, Sumanth, and Anirudh Mustyala. "Advanced AI Techniques for Real-Time Anomaly Detection and Incident Response in DevOps Environments: Ensuring Robust Security and Compliance." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 88-121.
3. Biswas, A., and W. Talukdar. "Robustness of Structured Data Extraction from In-Plane Rotated Documents Using Multi-Modal Large Language Models (LLM)". *Journal of Artificial Intelligence Research*, vol. 4, no. 1, Mar. 2024, pp. 176-95, https://thesciencebrigade.com/JAIR/article/view/219.
4. Sontakke, Dipti, and Mr Pankaj Zanke. "Quality Analytics and Customer Satisfaction: Insights from Retail Industry." *Available at SSRN 4847927* (2024).
5. Ponnusamy, Sivakumar, and Pankaj Gupta. "Connecting the Dots: How Data Lineage Helps in Effective Data Governance."
6. Bojja, Giridhar Reddy, and Jun Liu. "Impact of it investment on hospital performance: a longitudinal data analysis." (2020).

7. Singh, Amarjeet, and Alok Aggarwal. "Microservices Security Secret Rotation and Management Framework for Applications within Cloud Environments: A Pragmatic Approach." *Journal of AI-Assisted Scientific Discovery* 3.2 (2023): 1-16.
8. Shahane, Vishal. "Optimizing Cloud Resource Allocation: A Comparative Analysis of AI-Driven Techniques." *Advances in Deep Learning Techniques* 3.2 (2023): 23-49.
9. Vemoori, Vamsi. "Harnessing Natural Language Processing for Context-Aware, Emotionally Intelligent Human-Vehicle Interaction: Towards Personalized User Experiences in Autonomous Vehicles." *Journal of Artificial Intelligence Research and Applications* 3.2 (2023): 53-86.
10. Tillu, Ravish, Muthukrishnan Muthusubramanian, and Vathsala Periyasamy. "Transforming regulatory reporting with AI/ML: strategies for compliance and efficiency." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.1 (2023): 145-157.
11. Bayani, Samir Vinayak, Ravish Tillu, and Jawaharbabu Jeyaraman. "Streamlining Compliance: Orchestrating Automated Checks for Cloud-based AI/ML Workflows." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023): 413-435.
12. Tomar, Manish, and Vathsala Periyasamy. "Leveraging advanced analytics for reference data analysis in finance." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.1 (2023): 128-136.
13. Abouelyazid, Mahmoud. "Advanced Artificial Intelligence Techniques for Real-Time Predictive Maintenance in Industrial IoT Systems: A Comprehensive Analysis and Framework." *Journal of AI-Assisted Scientific Discovery* 3.1 (2023): 271-313.
14. Prabhod, Kummaragunta Joel. "AI-Driven Insights from Large Language Models: Implementing Retrieval-Augmented Generation for Enhanced Data Analytics and Decision Support in Business Intelligence Systems." *Journal of Artificial Intelligence Research* 3.2 (2023): 1-58.
15. 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.
16. Gupta, Pankaj, and Sivakumar Ponnusamy. "Beyond Banking: The Trailblazing Impact of Data Lakes on Financial Landscape." International Journal of Computer Applications 975: 8887.

17. Zanke, Mr Pankaj, and Dipti Sontakke. "The Impact of Business Intelligence on Organizational Performance." *Available at SSRN 4847945* (2024).
18. Shahane, Vishal. "Evolving Data Durability in Cloud Storage: A Historical Analysis and Future Directions." *Journal of Science & Technology* 1.1 (2020): 108-130.