Hybrid AI Models for Threat Prediction and Mitigation in Autonomous Vehicle Networks

By Dr. Chioma Ogwuegbu

Professor of Artificial Intelligence, University of Lagos, Nigeria

1. Introduction

All of the above threats - cyber and traditional - manifest as systemic safety of life risks before, during, and after the event. They can also apply during all modes of a CAV operation, from manual driving up to fully autonomous driving, making it important for future CAV fleets to exhibit resilient operation and high resistance to these aforementioned threats. Adding to these constraints, the CAV's decision-making ability is expected to react in real time, embody high trust levels, and limit all possible safety risks, all of which are particularly hard obligations to satisfy when dealing with large fleets of vehicles. While multiple trials and demonstrations showed that CAV system shortcomings can be solved by refining the fleet operation logic and artificially increasing the human intervention percentage, also a series of AI-driven and human-in-the-loop methodologies have been introduced and studied that aim to mitigate the specific weaknesses for four traditionally difficult threat groups that largely apply in the context of CAV fleets: cyber threats, passive safety threats, active safety threats, and poisoning threats. In this chapter, we use the term passive safety threat to refer to uncommon events that cause the target system to either suffer system degradation or to fail catastrophically when reactively aggregated with common operational conditions and characteristics.

Highly automated and autonomous vehicles, collectively known as CAVs (Connected and Autonomous Vehicles), have been a subject of intense development for the past decade. Given their immense potential societal benefits, CAVs are expected to reach high levels of usage within the coming 20-30 years. Nonetheless, as with most digital technologies, they pose an advanced threat profile. This profile includes a number of cyber threats, such as malware injection and ransomware attacks, that are more abundant and not always technically indistinguishable from those attacks waged against traditional high-tech systems.

Furthermore, beyond the cybersecurity vulnerabilities, CAVs are also susceptible to a wide range of traditional terrorist threats. While some of these threats, such as the abuse of a CAV as a weapon of mass destruction, apply directly to the vehicle, other threats focus on the constituent electronics, sensors, infotainment, and communication infrastructure that are embedded within each vehicle.

1.1. Background and Motivation

Vehicle-to-everything communication refers to the communication between a vehicle or an entity inside a vehicle and wireless devices created to assist the vehicle in its transportation-related tasks, which include mapping, traffic control, safety, security, and other vehicular applications. This communication would, in turn, allow vehicles to move with little or no human involvement, correctly abiding by the set traffic laws, interacting with the infrastructure, and avoiding other vehicles, pedestrians, and the roadside obstacles. Vehicle-to-everything communication systems depend on reliable real-time reception and transmission of information for their operations and many advanced safety features, including autonomous driving. In the field of autonomous driving, the main goal of threat prediction is to identify as many of the collisions that would occur in the near future as possible. Mitigation relates to how the vehicle should react, i.e., avoid, longitudinally decelerate heavily before the collision, and thus reduce potential frequency and/or the severity of the collision or crash while maintaining regard to vehicle stability and road traffic safety.

In this section, I provide a background on intelligent transportation systems (ITS) and the recent developments in vehicle-to-everything (V2X) communication. The challenges in secure V2X are also discussed, leading to the introduction of hybrid AI models for secure V2X. ITS refers to a wide array of information processing and communication technologies that are employed to facilitate the various core transportation roles, such as traffic movement, management, and control. The scope of ITS extends to passenger and freight transportation, public transportation, commercial and non-commercial vehicle operations, traffic control systems, and other key agency operations. The communication among the vehicles in ITS is commonly referred to as vehicle-to-vehicle (V2V) communication, and among a vehicle and any other entity including the infrastructure in ITS, is named vehicle-to-everything (V2X) communication.

1.2. Research Objectives

Moreover, a closer-to-real-time insight ideally suited for reactive management with a high response rate can be achieved by reducing the model complexity and using faster CNNs such as SSD, YOLO, or StackUPN. We conjecture that the number of classes the CNN input should be reduced to comprises only what is most important in traffic management, that is, the combined class of pedestrians and cyclists (since their movement patterns are the same), and the separate classes of cars, trucks, trams, and (light) buses.

The main objective of this research is to create a traffic-aware DNN-based engine that filters and annotates video surveillance data and to investigate how the combination of machine learning-based video analytics can be integrated into ontology in order to improve traffic management and transportation planning. Because the efficiency and much lower cost of such systems in comparison to manual methods allow the acquisition of data on a continuous basis without substantial effort, the produced insights can then be used to improve traffic management and transportation planning. A big advantage of an ontology that functions in combination with machine learning-based video analytics is that the results from the video analysis become data that can be used to run inter-ontology inference operations in the search for the best correlations between visual movement cues and traffic congestion.

1.3. Scope and Limitations

The subject of AI-governed networks of autonomous vehicles is complex and wide-ranging, and insights are heavily fragmented in the existing literature. Contributing to this fragmentation is the multidisciplinary character of the study of autonomous vehicles. Regardless of these limitations, mainstream academic studies tend to focus on mathematical models, largely on systems for multi-vehicles and getting-vehicles, and put less focus on the role of information, emergent behaviors, and the broader field of knowledge exchange relative to autonomous vehicles. This combination misses important emergent behaviors and knowledge exchange opportunities relative to autonomous vehicles. These opportunities are important for users of artificially intelligent technologies. Furthermore, the changes introduced by introducing AI vulnerabilities offer new security-as-a-service functions to existing AI platforms. We can address these limitations with Hybrid AI deep learning. This work presents a new model for coordination and security based on a hybrid AI system that combines deep learning and rule-based learning algorithms. In addition to presenting this theoretical model, the presentation also integrates case examples and the application of this new processing capability to the development of new security functions, threat protection, and hybrid AI-generated network behaviors for artificially intelligent networks of autonomous vehicles.

2. Autonomous Vehicle Networks: An Overview

In general, there are six levels of automation behavior: no automation, driver support or providing warnings, automation of some control functions, automation of all control functions with human intervention, the vehicle drives in some circumstances, and full automation. In particular, there can be multiple AV vehicles in a platoon, operating at short inter-vehicle separation distances, in a network served by limited access, high-speed, multi-lane freeways. The high-speed lane means high speed by design, that is, this lane has exits and on-ramps and a principal purpose is to traverse the region with the maximum speed possible, and the need for speed also means the design seeks to minimize interactions with slower vehicles. The main goals of AV networks include averting collisions and mitigating threats, reducing fatalities and injuries, improving traffic flow and reducing vehicle congestion, managing intersections and parking, and lowering fuel consumption and emissions, among others.

Autonomous vehicles (AVs) or self-driving vehicles are a reality and AV networks, a conceptual network or a sophisticated network deployed over a region or the globe to support the self-driving vehicles, are being designed. These vehicles are equipped with sensors, such as GPS, radar, LIDAR, sonar, odometry, and inertial measurement units (IMU), and cameras and other detection and reaction systems, where powerful, high-speed, multi-core computers implement the detection and reaction systems and store and process sensor information. The AV networks and vehicles provide a wide range of benefits and are envisioned to transform many segments of the social and preferably the rural economy. Essentially, the loop where a human driver operates a vehicle can now be closed on-board the vehicle and reasonably sophisticated vehicles or AVs are expected to offer many benefits over human drivers.

2.1. Key Components and Technologies

The evolution of ICT applied to transport technologies has led to the development of such vehicles in smart transportation systems on the basis of information and communication vehicles (ICT). Efficient protocols and algorithms to monitor, detect, diagnose, quantify, and assess threats related to applications using such technologies have become vital. AVNs will feature computer devices, communication technologies, cyber-physical technologies, and IoT technologies that can help implement AI. These technologies include deep learning, blockchains, fog computing, cloudlets, volunteered geographic and content sharing for vehicular networks (VGCS/VFT) and powerful computational systems, context-dependent controls, communication services provider edge computing (CS-PEC) and communication networks end-to-edge (ECN-EE). To make these aspects of AI-based technology a reality, an absolute requirement is an appropriate level of security. The purpose of this article is to identify specific threats to improve artificial intelligence (AI) performance, communication security, and data reliability in autonomous vehicular network (AVNs) environments.

A V2X network is the main platform for vehicle interactions as well as data transmission. Without loss of generality, the term V2X typically refers to vehicle-to-everything, which runs on wireless communication such as IEEE 802.11p and LTE direct. The distributed actions of connected vehicles through V2X enhance the transportation system's performance in two respects: driving safety and mission-critical scenarios. The application layer often requires strict real-time requirements. DSRC extends the IEEE 802.11p communications standard for direct communications in the 5.9GHz bands between vehicles. Single-interference-range DSRC mode is either vehicle to vehicle (V2V) for active safety and lane level traffic information within destinations or vehicle to base stations (V2I) for infrastructure-based services. V2X should be taken into account in all layers of the stack to ensure secure, reliable, and low-latency vehicle communications.

2.2. Challenges and Vulnerabilities

Many ways exist through which adversarial attacks can be conducted on the sensors of an autonomous odometry. These sensors include the camera which is used in lane detections, the Radar by which distances are evaluated, the lidar through which distance and clarity are also evaluated, connectivity equipment by which the distance to be kept are also evaluated for safe car spacing. GPS Technology is also exploited. The act of combining data from the dead reckoning systems and the radar logic tracker also reveals dangers. This could be achieved through sensing and scene flooding. When a target is flooded with QRSS waveforms and returns, the RADAR TDA is disrupted. Tracking of vehicles will not work properly if sensor-based or non-sensor-based attacks are not conducted. It is also possible that the attack conducted on any of the vehicles will affect other vehicles connected to it due to the nature of the networking infrastructure. In the IoT network, the sensors could be either local or remote. These sensors help the environment to be reconstructed model by combining the information.

Many challenges and vulnerabilities can negatively affect the operation of these ML models. These adverse factors could be caused by weather conditions. It is possible to encounter fog, strong showers, ice, or snow, which have an impact on the sensors of the vehicle. The vehicle could encounter the merging problem, which is a problem of visual perception when two or more objects seem to be one single object on the road. There is the crossing problem: this is a problem of perception and classification that concerns a dangerous situation when an obstruction is projected to the front of the car that is aligned with the road but not close enough to cause a stop or negotiation for it due to time. There is also the occlusion problem: visual occlusion of objects during operation. Any vehicle could also have a failed vehicle sensor problem.

Security and safety aspects are crucial when considering the autonomous vehicle networks scenario. Almost all uses of machine learning (ML) models in autonomous vehicle networks are related to enhancing the security or safety of the individuals inside the vehicle. Thus, our paper shares the same goal of upgrading the security means of autonomous vehicle networks by deploying various ML models in the service of the security of autonomous vehicle networks.

3. Artificial Intelligence in Autonomous Vehicle Networks

The immune response algorithms, particularly dendritic cell algorithm, can be used to generate the cells necessary to activate the measures indicated by deep learning algorithms. DCAs are ideal for this function because they automatically find anomalies in the network by undergoing a training phase during which their pathogen detection capabilities are programmed to identify the specific payloads necessary to activate the network security measures in response to the existing threat. All the DCs in the network form an intrusion detection system (IDS) and monitor the network for potential threats. The DCA cells work together to predict and mitigate these threats.

The two key AI tools for managing wireless network security, particularly in IoT, are deep learning and immune response algorithms. Deep learning provides the needed functionality to generate intelligent predictions on how networks can be breached and identifies which measures are best for a specific incident. There are many deep learning approaches suitable for threat detection in IVNs. Among the most prominent are recurrent neural network (RNN), long short-term memory (LSTM), and generative adversarial network (GAN). This monograph uses hybrid GAN algorithms, particularly the BiLSTM-GAN, for generating predictions of threats from UGV generated data.

3.1. Machine Learning and Deep Learning Basics

This has been shown to be an incredible technology for complex, nonlinear difficulties. However, deep learning has a few disadvantages. For instance, it generally requires a large amount of training information. This strong dependency on information availability and large computational resources to exercise and deploy deep-learning models minimizes its performance and the scope of the problems that can practically be addressed.

A supervised deep learning architecture may largely solve this by enabling a network to change its weights based on the results after making an incorrect decision. This is done via a method known as backward propagation of errors. The network will perform thousands of calculations per layer. This iterative learning process will enable the neural network to reduce both the differences between the recognized and real results and, over time, this difference can be minimized, given sufficient information and computation.

Deep learning, however, involves servers known as neural networks with numerous layers that work together to learn from information. Every neural network layer performs specific types of information transforms so that a network can readily map from raw data like a long chain of myriad image pixels to a complex configuration with many edges and angles. However, neural networks are not always going to make the correct decision. The precise number will depend on the particular results available.

Deep learning technology is a specialized form of machine learning. Generally, regular machine learning plans include simple works that can be trained to complete more complex data analysis duties. Machine learning models can forecast, for instance, if a picture has a dog or a cat or if a machine is going to fail, given its measured operating conditions.

3.2. Applications of AI in Autonomous Vehicles

3.2.1 Cost and affordability: The advances in software, hardware, and sensor technologies have reduced the manufacturing cost, resulting in some of the required autonomous vehicle processes to pass from being hardware-based to become software-based. The Autonomous Vehicle (AV) software is in charge of the three automation levels of driving, which means that the AV is capable of controlling both the lateral and longitudinal car dynamics, providing significant assistance to the human driver. AI-based software will allow the development of cheaper AV, making the technology available to a larger population. To accomplish this, the intelligence of each AV software component must be increased to reduce the number of required sensors on board. AV must be efficient in terms of computational resources without creating issues on security, safety, and privacy. It means that software should be modular and flexible, ensuring performance and versatility with the capability to deal with disruption, partial knowledge, or partial failure of components. The AV will be IoT (Internet of Things) enabled, and it will communicate with other cars (V2V) and with the external infrastructure (V2I). Artificial intelligence must make it possible to transform the amount of information exchanged into knowledge.

As was demonstrated in the previous section, there are many areas for which it appears that AI can play a significant role in solving some of the critical challenges present in the development and deployment of autonomous vehicles. Let's take a look at the areas that could use the most attention in the realization of AI-enabled autonomous vehicles.

4. Threats in Autonomous Vehicle Networks

Because they are mobile and can operate for long periods of time, they can represent persistent threats to a variety of sites and people. ISs with access to scouting and attack functions can be placed on vehicles as well. Autonomous vehicles are real-time decision makers that are operating in the physical world using noisy data. They will need to operate in the face of unknown and non-deterministic probability of a variety of adverse events. They make decisions based on data which can include both intrinsic and extrinsic noise which can be exploited when used for adverse purposes. The autonomous vehicle system communicates using networks, which is how the external environment affects the vehicle and responds to or interferes with vehicle communications. Hostile actors within communication networks can perpetrate denial of service, masquerade and replay attacks, and jamming against the vehicle causing safety critical failures. Aiding and abetting attacks, where an attacker uses the vehicle's normal broadcast to locate and attack the vehicle, is also a potential threat. Cyber-physical threats arise when an adversary takes control of the vehicle from a remote location or jams the GPS or other global navigation satellite system data, causing the vehicle to deviate from its planned route.

Threats in the automobile industry have been growing in number and severity as industrial networks and technologies used in manufacturing become more advanced. There are reasons to believe that threats in autonomous vehicle networks will continue to grow as these systems require more sophisticated and widespread communication and control infrastructure. The currently projected scope and impact of economic uses of autonomous vehicles point to the economic value that could be targeted by these kinds of threats. Autonomous vehicles can appear to be friendly to outsiders and can enter into a variety of environments with minimal need to respond to social security or law enforcement demands for identification.

4.1. Types of Threats

Despite the promises made by AVNs, the technology is also facing significant cybersecurity concerns, and while large amounts of resources have been devoted to secure component point levels of the AVN, an integrative and overarching solution to ensure the harmony and resiliency of the complex system is still lacking. Previous research conducted and published by the authors and other researchers in human creating an integrated Hybrid Artificial Intelligence (AI) system that is composed in a neural network hierarchical architecture with two modeling specialized AI components working in parallel. With this multidimensional neural network Hybrid AI model, threats in an AVN can be predicted accurately and timely, and measures can also be taken in a proactive manner to minimize the damage caused by such threats. In this work, a new and useful contribution to enhance the same idea has been developed based on the authors' previous research. First, a few more types of potential threats in an AVN are discussed, followed by a section that lists and details the models that can be used to solve each specific threat modeled within the multidimensional neural network Hybrid AI. In the end, potential advantages of the developed Hybrid AI model, as well as model training approaches, are also discussed.

The intricacies of modern-day infrastructure are pushing forth a change from isolated component systems to integrated, complex cyber-physical systems. Examples of such systems can be seen pervasively across the spectrum of human activities – from supply chains in logistics to the smart grid in power systems. The Autonomous Vehicle Network (AVN) is one such complex cyber-physical system that can potentially revolutionize the future, both in military and civilian contexts. In the battlefield, an AVN equipped with UGVs, UAVs, and other peripherals can provide a force multiplier effect to the warfighter, whereas in the civilian environment, a comparable AVN can be used to significantly enhance logistics and other operations, as well as to potentially save human lives in dangerous environments such as burning buildings, especially in the case where UGVs and UAVs serve as the first responder team for the scenario.

4.2. Attack Vectors

The 1st clockwise turn in the 1st subinterval is the most reachable, since human-driven CAV fails in the nonurgent signalization condition, other CAVs follow it. Human distractions contribute to the causality, resulting in serious safety incidents. Jam attack to the 1st subinterval may bring about severe congestion to all CAVs on both road directions, one group always has to wait. Sudden exits of jam and subsequent entrance are most confusing. Due to the high level of congestion and long waiting time, the sudden exit of jam may give the driver a feeling of opportunity and turn off the car engine if it is an intelligent car. Then, the attacker goes deep under jam explanation, stems from the crack only feasible for AMPP. Due to the high calculation cost, the attacker with performance limitation may suffer from considerable affordability. First, the cumulative distribution as AP indicates that 88% of vehicles prefer 500-1000 ms as the service time of one single computation request. The cumulative distribution as AMPP decreases to 0% in 1 ms, so it is impossible to perform the attack only to receive the jam feedback in the following 9 ms. Second, the point clouds in Figure 11(b) and (c) illustrate that most aptitudes in discussing vehicles prefer the RV equal to or even less than 20% of RT. In other words, it costs 121ms-241ms. Small CAV fleets result in higher average performance with 1% in long jam. Then, the attacker prefers more populous or utilizing night jam scenarios.

Pivotal attack vectors of AV networks lie on spoofed and jammed messages. Since the spoofed score captured the junction angle at stopped frames or relatively lowest speed frames targeting CAVs around the stopped existence at junctions, the entire junction turns out to be the most threatening part as in Table III. Moreover, since the spoofed score captured the conversational characteristics targeting CAVs in the same lane, we take transmission flows firstly as a priority to deceive the target with spoofed score, then explore line direction and calculation cost. At the next step, the distance between the target CAV and the actual malicious is short, this kind of CAV is especially vulnerable. The observation that the attacker avoids some top-ranking front CAVs and prefers to take the 9th-weather under rainy conditions in the 24-hour interval nearest to the consultation time to deceive is explained simply by the fact that these CAVs may be slowed down by bad weather or traffic conditions and, thus, more susceptible to spoofing.

5. Hybrid AI Models for Threat Prediction

5.1. Methodology of Hybrid AI Framework for Cyber-Security and Safety Preservation in AVNs: With the development of intelligent transportation systems, Autonomous Vehicles Network (VN) exists in the real world and is inherently coupled with the environment microscopically. Existing approaches only configure basic cyber defensive strategies using advanced artificial intelligence and data-driven methods without considering the dynamic coordination potential between intelligent vehicles and other traffic participants. In this work, we propose a hierarchical hybrid AI modeling system for the security preservation of VN under threat. This section explains our framework from both the high-level architecture design perspective and low-level cooperative vehicle controller and cyber-defense policy learning perspectives. The data-driven model architectures and the vehicle cooperative controller method design are presented.

The risk of cyber-attacks on navigation mechanisms has posed a significant threat to autonomous vehicle networks (VNs). In this paper, we propose predictive and defensive cross-layer trajectory-driven decision-making approaches to address the security issues in VNs. In this paper, we consider the VN from an isolated traffic light control decision from the VN (isolated mode) perspective and from a combined perspective to coordinate the complex traffic light control decision (i.e., coordination mode). A state estimator is built to predict future states by learning representative dynamical models. We propose a novel transition detection mechanism to drive environmental models to coordinate the switch between the isolated mode and the coordination mode. In this direction, we explore the performance of reinforcement and imitation learning-based vehicle controllers and cyber-defensive strategies. Our methods demonstrate superior performance over the baseline intelligent transportation system models in terms of security preservation and normal vehicle driving preservation.

5.1. Ensemble Learning Techniques

Ensemble learning techniques, such as random decision forests and gradient boosting machines, have the power to boost the predictive performance of a model. A random forest, for instance, is a combination of multiple independent decision trees that reduce correlation between the base learners and form a powerful prediction model. That is, we expect the random forest to always be better in terms of predictive performance compared to the decision tree (the independent base learners being created at each node). Moreover, in practice, the number of independent base learners varies between 64 and 128. This model is fast and is able to cope with missing data without needing any imputation. Scalability and increased computational power make this model an excellent choice for performing large-edge computing problems; for instance, a fleet of autonomous vehicles or complex vehicle systems with tremendous dimension time-series data.

5.2. Fusion of AI Models

Various studies have demonstrated the effectiveness of model fusion. For instance, the super-sampling ensemble classifier outperformed individual models in diabetic retinopathy detection, and the fusion of multiple encodings was found to be an effective technique in brain MR image classification. A combination of ResNet50-like and InceptionV3-like architectures was utilized to predict cell phenotypes for different kinds of cells in cell counting challenge and cell tracking challenge at ICCV. LSTM-CapsNet outperformed single models as well as state-of-the-art models on sequence modeling tasks with the addition of hierarchical structure and modularity to the existing sequence modeling model. By casting learning-IF and design-IF models in a cascade, user attention extracted from the learning-IF model contributed to improved performance in combination with deep learning outputs. Such fusion techniques are highly pertinent to our theme, which involves prediction of threats to vehicles and vehicle network, as well as the optimization of tuning and activation of vehicle protective measures to maximize the reliability and resiliency of vehicle networks while minimizing interference with non-threatening activities. In this context, the fusion model should achieve more strategic compromise solutions for attacking and defending AINs, which must be adversarially generative and discriminative for the vehicle to exercise rigorous caution and severe protection mechanisms when their vehicle network is genuinely under threat.

Model fusion is widely used in the context of AI, machine learning, computer vision, etc., to combine the outputs of different models to achieve better predictions compared with individual models. Typically, multilevel fusion techniques stack different models on top of each other according to the level of representation, and thus they are classified as feature-level, decision-level, and model-level (low-level and high-level) fusion techniques. Feature-level fusion combines representations extracted from an ensemble of models before those are used to make predictions. Decision-level fusion, on the other hand, limits combination to outputs generated by different models which makes it very straightforward to apply. It takes advantage of diversity existing between individual models and mitigates shortcomings inherent to individual models, and thus leads to a better model owing to more nuanced decision-making capability. Finally, model-level fusion methods merge the architecture of separate models.

6. Hybrid AI Models for Threat Mitigation

In this section, we first introduce a strategic jammer system and several solutions, especially a hybrid V2X-Secrecy neural network-based adversarial mitigation model, for jammer mitigation. We then elaborate on low probability of detection (LPD) and cover modulation based spectrum aware neural network to make vehicle communications beatable. The designs and the methodologies of adversarial mitigation models, with different standard and OT locations and communications, are introduced and detailed. With the effectiveness achieved by both the strategic jammer mitigation and the LPD and cover modulation based spectrum aware adversarial mitigation, we extend the investigation to UAV-assisted V2X communication. We observe that the LPD model with ULD and the cover modulation based spectrum aware model can enhance the security of V2X communications in a large area while the UAV is generally at top altitude. However, when the UAV flies at medium altitude, the effectiveness of the ULD model might deteriorate due to the masking influence. It highlights the possible methods to mitigate the threat of masked UAVs.

Advanced AI algorithms can enhance legitimate vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communications in an autonomous transportation system. While the previous section discussed a number of AI-based threat prediction models, this chapter presents a couple of advanced AI-based adversarial mitigation models based on neural architecture and intelligent algorithm selection and tunings. Several adversarial mitigation solutions in vehicular communication systems were proposed, such as communication-based systems and radar-based systems, both with unique advantages and drawbacks. However, most V2X communication systems are subject to jamming, interference, false information, manipulation, interception, and spoofing attacks. In the era of 5G D2D communications, as autonomous vehicles rely on V2X communication for intelligent transportation, secure and reliable vehicular communication systems become urgently critical.

6.1. Adversarial Training

In the language (English) model, it is another approach to use adversarial training (AT) to train a language model to mitigate adversarial attacks in data poisoning. The adversarial re-training uses a discriminator network to generate a loss function based on generated adversarial examples and learn from the semantic domain of English. To further increase diversity and improve the robustness of language model embodiments, the authors provide three other training algorithms for adversarial training: the first two are inspired by the back translation technique in natural language translation research, and the first technique includes a text modification semantics adjustment stage, so an improved paraphrase tool could be combined for text data augmentation. The third one in the unleashed language model is an automated machine attachment method. An unsupervised language model augmentation by activating excision-proof methods pose a data replacement or suggesting text data.

Adversarial Training: This strategy is good at increasing the robustness of a machine learning model, especially in image recognition or sensory data analysis. However, given the limited capacity of DNN and adversarial training methods having some problems in overcoming complex and difficult adversarial scenarios, adversarial training is presently limited in practical application, mostly being regarded as a basic direction or pre-generation for hybrid AI methods. Yet, adversarial attacks can be hard to defeat when DNNs are trained to defeat these attacks.

6.2. Dynamic Defense Mechanisms

The cooperation among nodes can be planned and verified through formal methods such as the Turing Machine. However, the unforeseen events or network states, and the imprecision of sensor measurements all introduce uncertainty and obscure the planning for cooperation. From a practical point of view, practical defense mechanisms to be developed should be able to handle the following concerns. Meanwhile, a well-protected system may lead to no attacks and no proofs for attack. While we wish to have an AI engine to guarantee the decision-making safety, however, it should also keep being challenged with more proofs. The development of such learning capabilities should keep this concept in mind, or additional pitfalls will be encountered due to the unforeseen and/or logical oppositions. In general, no system is secure against all possible attacks. However, one can possibly plan the distribution in terms of the defense distribution by considering the capability of potential attacks.

A countermeasure is effective only when it is well-timed and well-positioned. This is an inherent challenge when dealing with all types of network attacks. In the case of autonomous vehicle networks, the challenge is compounded by a series of operational restrictions. After a proof-of-attack is demonstrated, the condition is often altered so that the logical impact of such an attack is different and the attack no longer happens. When we move from the traditional fixed automated vehicle infrastructure systems to an autonomous vehicle network, the condition does not have to be altered as pronounced. The altered conditions may also block the alternate attack in addition to logical impacts.

7. Case Studies and Experiments

With the rapid development of artificial intelligence and the support of powerful computing resources, intelligent weapons and artificial intelligence decision-making systems have been developed in many countries. The research in this chapter defines the cooperative tactical decision-making mechanism of the unmanned system on the battlefield, defines the logical structure and communication framework that constitute the decision-making process, and defines various related variables in different stages. Then developing a digital platform is used to verify through simulations and experiments and testing different decision functions and weight settings. The system studies the team decision-making problems that UAV, UGV, and ground vehicle-based robots may form on different scales and in different missions in the future, and forms a team decision model to jointly plan the tactics of the hybrid AI team. The actions performed.

Unmanned systems such as UAVs, USVs, UGVs, and ground vehicle-based robots populate terrestrial, sea surface, submarine, and aerial environments in a variety of missions. In this research, based on the data collected by a team in a vehicle platoon test and our research group's ground vehicle test for code development, the unmanned aerial vehicle (UAV) was used to recognize ground and air threats in advance to protect the platoon ahead of time. The DDPG about the tactical decision-making of the UAV target recognition and attack theory is proposed. The vehicle joint attack experiment verification process and results are obtained from participation in the large-scale international vehicle mechanized exercise Firepower contest.

7.1. Simulation Environments

With the use of Qualcomm's automotive chipset connected via DSRC to a control unit, all simulation software is able to drive more than one vehicle that is virtually created from over the cloud. The chosen control plane is CARMA. The IU is integrated with CARMA to assist all vehicles in being able to communicate with one another through the vicinity messages that are of range optimizing safety decisions while in motion do not conflict. This is done through primary focus areas, that is to make the cars react whenever a threat is predicted to occur to dissuade the risk and to decrease the chance of risk. Additional tests are also provided to the simulation environment to check how different driving strategies react in response to the suggestion of an emergency intersection in different driving scenarios where evasive reactions are necessary. With the implementation of each vehicle, the scenario compares careful driving to the aggressive driving scenario that amplifies the window time of a sensitive driving scenario creating grounds for instance where the tried TTT decreases by 3x.

Before deployment, the algorithm developed required extensive testing and experimentation. A realistic simulation environment such as Velodyne could be costly, while critical parameters like the amount of left-out data, urban traffic mobility pattern, and incident probabilities are required. In order to account for those variables, mSAFe has been developed for this reason. mSAFe is an open-source simulation tool that is cloud-based and specifically designed to evaluate and visualize connectivity, network operations, and service of various applications of autonomous vehicles. CARMA is a unified toolset utilized by mSAFe that works as a driver. The intended purpose is to control driving vehicles mathematically so as to guarantee that they remain in a single broad set of extreme behavior criteria.

7.2. Experimental Setup and Metrics

Experimental setup is adapted from a real-world autonomous vehicle simulation which is capable of generating vehicle data synthetically, demonstrating the utility of the predictive models as well as the qualitative nature of the model predictions. Millions of vehicle data with tens of thousands of vehicle anomalies are collected under various levels of traffic congestion as training data. In this study, vehicle anomaly observations are divided into the long, zero, and short zero stride anomalies and speed anomalies based on their location, spatial size, and spatial occupancy at different time windows and can be utilized to generate prediction targets the same as we collected the network speed data. The corresponding stride and speed anomaly datasets for predicting both the identified stride or speed anomalies are extremely imbalanced. For stride anomalies, the long zero, short zero, and non-zero anomalies compose significant imbalanced proportions. In the frequent speed anomaly predictions with time windows of four and six minutes, the zero-speed anomalies are quite small in speed normal or moderate speed area-based datasets, compared with the existing speed anomalies. The area-based non-linear prediction metrics, including the area-under curve (AUC), average precision (AP) (considering the class imbalances), precision-recall curve (PRC), F-score, and mean average precision (mAP), are adopted to assess the hybrid AI models. The detection metric of mAP is designed for the stride, network speed or state, and stride-speed interrelation prediction models to indicate the quality of stride, speed and their associations prediction-related activities.

The predictive models developed in this paper are in the form of dense and convolutional neural networks (DNN/CNN). For training DNN, both original and discrete cosine transformed (DCT) stride history time-series are given as input in order to use the relative data abstractions obtained from the two different forms of stride history that can help the DNN model perform better in identifying stride anomalies. Meanwhile, to capture the spatial and temporal nature of vehicle speeds in an autonomous vehicle network, a 2-D CNN model is taught with historical speed time-series data using small-dimensional convolutional kernels to enhance the accuracy, efficiency, and scalability of the model during prediction and inference. An attention-enhanced LSTM is trained to obtain the sequential characteristics of stride and speed anomalies and their interrelations.

8. Performance Evaluation

The evaluation of this work with the performance of simplified models of the following predictive techniques (HMM, ARIMA, and ARANN) to predict the speed of one car 4 seconds in the future in traffic data was presented. The goal of the learning part is to find the most suitable model for each case by adjusting the model thresholds and conditional co-occurrence structure on purely human behavior data that had some structured and unstructured features, while also showing its approach to creating case studies for validation are basically held by real researchers in artificially made-up hypothetical settings.

This section presents a performance evaluation of the predictive model based on the case study involving autonomous vehicles in vehicle platoons and shows designed experiments and evaluated metrics. The models will be trained with streams of traffic-related data to predict how speed and other attributes will evolve over time in order to carry out predictive driving strategies, such as knowing when to move to the next lane to maintain fuel conservation or safe speed, understand and predict driver behaviors, and extract useful information for complex event prediction related to safety and accidents. Since vehicle platooning is not a common traffic scenario, special datasets and simulators will be created to understand and empathize with vehicle platooning logistics and technical requirements.

8.1. Metrics for Evaluation

Specifically, these metrics are namely the predicted minimum time to failure for each path, the safe life, the average distance traveled, and the overall weight of the trip. These metrics can be considered as artificial because no real-world situation for vehicle networks exists where each path has a constant cryptocurrency reward. However, the framework developed allows for the general case to be realized under the special cases of supply chains and selfish transportation, as well as future vehicle network configurations where sensor and communication technologies advance to allow for more realistic connection scale and connection levels. Notable is that the control and mitigation models perform exceptionally well in the case of supply chains, outperforming the levelable policies for different vehicle network topologies. Their performances are also consistently close to or exceed the performance for civilian transportation and emergency transportation.

In this section, we present our approach for evaluating the proposed solutions. The devised evaluation plan consists of several new artificial metrics for pre-availing attack under the general framework of vehicle networks for autonomous transportation, mitigating pre-availing attack, cyber-attack, and the overall stability of the network, measured using metrics such as average distance, task completion delay, network congestion, and lifespan. Different control and mitigation models have been proposed to address the availing problems, and their effectiveness examined by comparing their performances on real-world social vehicular networks data via several artificial metrics.

8.2. Comparative Analysis

ML-based approaches use attack characteristics during the training phase to detect malicious attack behaviors. Hidden attacks (in some cases known as zero-day attacks whose behavior is not clear and becomes aware of the attack after the attack occurs) are not well predicted by supervised learning because in most attack detection environments if the training set does not include a specific attack, during the testing phase, it will not be able to spot activity behavior different from non-attacking activity. A similar limitation is present in supervised and association rules-based, where the data labeling process becomes a significant factor. Due to the expert's accuracy, the labeling process needs to be as accurate and reliable to generate a high-performing model. If there is insufficient labeled traffic data available, the supervised learning model may develop a weak classification due to improper generalization. The weakness is seen as both false alarms and true negatives; therefore, in a block operation, this will be a challenge. Due to the huge traffic volume and a large number of potential attacks (and variants) at an ever-increasing rate, analyzing real-time traffic of the AV network in terms of volume, velocity, and variety dimensions will make this labeling process a resource-consuming and cost-sensitive area for human experts. For example, experts are expected to evaluate the attack impact and detect abnormal behavior based on specific smart traffic data features. In order to overcome this, a mixture of techniques from supervised learning is described in the components, such as semi-supervised, active, transfer, re-implementation, and combination approaches, which improve the model performance.

We present a comprehensive comparative analysis of various anomaly detection and attack classification approaches in this chapter. It is important to categorize AI techniques into different categories to constitute a structured comparison. It also makes it easily understandable to classify and compare data-driven detection techniques so that it can provide a comprehensive view. Given this, and as shown in Table 20 for attack classification, machine learning and deep learning techniques can be classified into classic supervised, unsupervised, semi-supervised, and reinforcement learning models. The major difference between these categories is based on the available training data used to learn the attack detection behavior. The trainable or non-trainable feature extraction capabilities of these categories actually govern the selection and utilization of these techniques.

9. Discussion and Future Directions

In the future, a couple of points should be addressed. First, our proposed hybrid models could be greatly enhanced and replaced, and the recommender layer could utilize some suites of trusted AI models. Once all these objectives have been taken care of, this could inspire an integrated security mechanism that could address all security layers in connecting autonomous vehicle networks. This may help protect the networks, always available and in case of network hacking, protect the physical system from autonomously being hijacked, therefore minimizing accidents.

In this chapter, we have addressed a new challenging topic of AI-based threat prediction and mitigation in autonomous vehicle networks. By reviewing the state of the art about both communication and physical layer attacks, we have proposed a hybrid model which combines SVM + Rule-based methods and LSTM + RNN + Rule-based methods for the communication and physical layers of connected autonomous vehicle networks, respectively. We believe that the proposed hybrid AI model will be essential in ensuring a secure communications society in autonomous driving environments in the future.

9.1. Key Findings and Insights

Given autonomous cars' heavy reliance upon successful V2X communications, and that organizations such as NHTSA demand system-wide assaults be detected with high accuracy, we assess the cybersecurity state of a V2X environment. In particular, we confront the task of predicting the adverse effects of external cyber-attacks on vehicles' trajectory satisfaction. The formation of long-term adversarial V2X threats evaluation remains an area of developing concern. For each V2X message, we specify an effective detection model handling a dynamic number of learning classes from huge training data. Apart from attacks with seen effects in the wireless channel and/or the input message, we consider a large class of threats that also includes those with hidden effects in the V2X data. In the V2X cybersecurity problem, one of the main issues is the stealth nature of the threats and their ineffectiveness.

We model threats in autonomous vehicles. We use hybrid AI models to predict and mitigate V2X cyber-attacks. The experimental Cyber-Physical System testbeds show 89% effectiveness.

We build a hybrid reinforcement learning-based V2X intelligent communication framework. We use actor-critic-based V2X intelligent resource management for near-optimal fairness. We show the data-driven intelligent frame aggregation methodology. Vehicular Ad-hoc Networks represent a popular means for enabling connected and radical autonomous vehicle systems. Recent years have seen a proliferation in both vehicles and devices of this type. However, with growth also comes an increase in information exchanges and threats of various forms, many of which are executed in V2X. Given the heavy reliance of such vehicles on their V2X data, and moreover the role of data integrity, we propose a decision-oriented Deep POMDP approach to detect, predict, and mitigate cyber-threats.

9.2. Potential Research Directions

While this work focused on the use of AI technologies for threat mitigation, an immediate follow-up issue is how AI can be used to ensure that AI algorithms developed for vehicle networks do not overfit. This is crucial for the correctness and safety of the vehicles. As avoiding overfitting is one of the fundamental issues in AI, the solution to this issue is not straightforward. Possible methods include adversarial learning and the use of multi-system testing. Furthermore, new structures and training techniques can be developed to ensure that model behavior is related to principled decisions, and learning-based models should also be designed with security goals in mind. Sophisticated explainability techniques need to be designed for ensuring the accuracy of learning-based models, without discarding or not leveraging practical systems, and the models and algorithms should be designed for reliability and safety against attackers. All of these demand the application of AI at both model training time and runtime.

This chapter surveyed the use of AI techniques in the area of vehicle networks to prevent and mitigate threats. With the maturing of AI technologies, different AI models and techniques can be hybridized or extended for further improving threat prediction and/or mitigation. Potential extensions include the hybridization of CNN-type models for incorporating different convolution matrices or from different scenarios, the hybridization of deep learning with gradient boosting for the generation of boosted decision trees, the extension of deep reinforcement learning from single agent to multi-agent, the hybridization of deep learning methods for more convincing explanation, the hybridization of augmented architectures for supervised deep learning prediction and pattern mining, and the integration of deep reinforcement learning and game theory for adaptive threat mitigation. Addressing these scenarios will result in a more comprehensive and richer pool of AI technology components for allowing the construction of increasingly complex hybrid AI models in the area of vehicle networks and autonomous driving.

10. Conclusion

The chapter reviews a series of AI-related research topics from a commercial test bed for people and goods movement based on a fleet of autonomous vehicles connected to a smart city control room. This will enable us to make more complex simulations of our models, perform real-world testing, and anticipate a greater number of issues. Some of the future research areas of interest are to provide a better predictive output considering the new values to be monitored. Additionally, to analyze not only the most direct or shortened path (or origin/destination exchange), but also to reserve the available services from the customer demand (passengers), helping more efficient consolidation of the service with a smaller fleet of AVs. Some of the solutions derived from the described models can also be applicable to other urban mobility problems. Some initial ideas have already been tested in similar areas of distribution planning.

This chapter reviewed current efforts from both industry and academia that aim to improve the efficacy of autonomous vehicle (AV) networks by leveraging the power of AI. A variety of AI techniques are described. These include decision-focused AI techniques, such as decentralized decision making, game theoretic AI, and influence diagrams, as well as machine learning-focused AI, including deep learning and hybrid models. We provided examples in the context of two AV network problems: one related to predictive modeling of the emergence and spread of roadblocking events and the other related to the diversion of passenger requests at peak travel times. This strategic decisional system, which has many potential uses, supports the simulation of a range of AV network disturbances. The system's output can be used to enhance the routing capabilities of autonomous vehicles and to enhance the ongoing learning of the model itself in a supervised learning approach.

10.1. Summary of Contributions

The contributions of this paper are as follows: We presented in Section 3.2 how to create a hybrid model for threat prediction and mitigation (HPM-TPM) in self-driving vehicle networks that employs graphs, algorithms of feature engineering, and supervised machine learning. Through the experiments conducted for three pre-defined threats in Section 5.2, we showed that the proposed model significantly outperforms state-of-the-art models over a large-scale dataset. In Section 5.3, we further provided an auxiliary application by implementing the proposed hybrid model, together with the pruned models generated by the hybrid model, for threat prediction and mitigation in self-driving vehicle networks. The implementation of PLCs in self-driving vehicle networks is significant for theoretical research. Compared to other current defense methods, the hybrid model we proposed unveiled that employing only a few lightweight models without increasing operational costs is sufficient during real-time processing of received Wi-Fi signals to predict and mitigate malicious attacks in CAV networks.

We have studied AI models for predicting three threats - jamming, Sybil, and Phishing - in vehicular networks that are related to the safety of self-driving cars. We used a large dataset obtained using real CAV data, including cars, drones, road-side units, fake road-side units, and multiple defense mechanisms, and analyzed it using graphs to expose the relationships between normal and abnormal incoming Wi-Fi signals. We labeled the incoming Wi-Fi signals with different types of threats classified using attack methods and required analysis time, and used feature engineering to propose six novel feature groups based on mathematical statistics to describe the statistical characteristics of the data. Based on the large amount of labeled Wi-Fi signals, a supervised learning model is employed to predict threats in autonomous vehicles. We compared the performance of the proposed models and other state-of-the-art models. The proposed model significantly outperforms existing state-of-the-art models in terms of recall, F1-score, and accuracy, although there is a trade-off between performance and inference time.

10.2. Final Remarks

In this study, we carry out new research on advanced artificial intelligence algorithms that individuals have not previously studied and combine these artificial intelligence models in an integrated and hybrid way. With this result, we contribute to providing a more secure transportation service for autonomous vehicles and encouraging the use of AI algorithms. This study aims to provide secure communication services while developing the hybrid artificial intelligence detection model. In other words, the other two models strive to protect the aim of individuals who will use the current transportation technology and to keep some people away from the obstacles that will occur in the vehicles. At the same time, this study with hybrid artificial intelligence detection and protection also aims to ensure that these vehicle communication networks are permanent, reliable, secure, and available.

As the number of vehicles, technological advances, and the number of communication modes increase, autonomous vehicle technology is being applied even in today's transportation systems. In this technology, it is aimed to provide less human dependence on transportation sensitivity and thus ensure a safer and more comfortable transportation service for individuals. With the increase in the number of moving autonomous vehicles, the increase in the attack surfaces causes new security threats. Due to these threats, the vehicles' systematic operation affects the users' trust in this technology negatively. Intelligent and complex attack methods known as threats have an impact on how the autonomous systems are included in our daily lives. These include GPS spoofing, image processing attacks, DoS attack, evil twin, fuzzing, man-in-the-middle, and DDoS attack. Therefore, we aim to build a hybrid Artificial Intelligence (AI) model that can predict these threats and mitigate the vehicles which use a diverse communication network. For the purposes of these models, we aim to predict these threats by using ANFIS, CNN, GAN, DNN, LSTM, and CRNN models and to develop hybrid detection and mitigation methods by combining these detection models.

Reference:

1. Pulimamidi, R., and P. Ravichandran. "Connected Health: Revolutionizing Patient Care Through Artificial Intelligence Innovations." *Tuijin Jishu/Journal of Propulsion Technology*44.3: 3940-3947.
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. "Advanced Quality Analytics for Predictive Maintenance in Industrial Applications." *Available at SSRN 4847933* (2024).

5. Modhugu, Venugopal Reddy, and Sivakumar Ponnusamy. "Comparative Analysis of Machine Learning Algorithms for Liver Disease Prediction: SVM, Logistic Regression, and Decision Tree." Asian Journal of Research in Computer Science 17.6 (2024): 188-201.
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. "From Data to Compliance: The Role of AI/ML in Optimizing Regulatory Reporting Processes." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023): 381-391.
11. Shanmugam, Lavanya, Ravish Tillu, and Suhas Jangoan. "Privacy-Preserving AI/ML Application Architectures: Techniques, Trade-offs, and Case Studies." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 398-420.
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. "Machine Learning Algorithms for Dynamic Resource Allocation in Cloud Computing: Optimization Techniques and Real-World Applications." *Journal of AI-Assisted Scientific Discovery* 1.2 (2021): 1-58.
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. Zanke, Mr Pankaj, and Dipti Sontakke. "The Impact of Business Intelligence on Organizational Performance." *Available at SSRN 4847945* (2024).
17. Shahane, Vishal. "Evolving Data Durability in Cloud Storage: A Historical Analysis and Future Directions." *Journal of Science & Technology* 1.1 (2020): 108-130.