Computational Intelligence for Dynamic Risk Assessment in IoT-connected Autonomous Vehicle Networks

By Dr. Nasir Memon

Associate Professor of Cybersecurity, Rutgers University–New Brunswick

1. Introduction to Autonomous Vehicles and IoT

Autonomous vehicles, also known as driverless, connected or self-driving cars, are no longer a concept of the more or less distant future, but a transportation factor that, depending on the formal definitions (such as "level-5" autonomy), should reach the full-public availability in the next fifteen years. Encouraged by major vehicle manufacturers who have declared innumerable efforts in research and development, as well as by the spread of vehicles with progressively "partial" or "conditional" self-driving functions, numerous entities have undertaken a wide range of activities to prepare the communications infrastructure and protocols for the full development of these revolutionary vehicles, covering issues related to safety, latency, quality and security of communications. Indeed, such an integration of digital technology can define more efficient traffic flows and stretches in both urban and road areas, revolutionizing some current models and rules. To date, the majority of the functional platforms proposed and some prototypes of autonomous vehicles using recent technology, such as clusters of processors connected to networks with different topologies, i.e., CAN, LIN, FlexRay, Ethernet (IP), DSRC (Dedicated Short Range Communication), with different requirements for continuity and safety, cyclic transmission and redundancy protocols for certain functions, have been designed and tested for certain types of roads and services. Due to the intrinsic security problems related to each technology, sensible to external attacks or faults, the subject of cybersecurity is recognized as an enabling factor both for privacy-sensitive services for passengers and for security-sensitive applications.

The future of vehicular networks from the autonomous perspective opens new cybersecurity concerns given the taxonomies, potentially from sensors and actuators, as well as mobility and connectivity, as well as challenges related to localization, serving or maintaining QoE/etQoS, energy management and collaboration or control. Indeed, the so-called dynamic driving scenarios go far beyond the rigid real-time deadlines imposed by typical automotive applications, for example actuator control. As increasing use-cases imply increasing use of the Internet of Things (IoT), in the context, a broader view of the automotive market, as "Internet of Autonomous Cars (IoA)" networks, emerges, meaning a targeted integration of the best of both concepts. However, from the perspective of connectivity, only the orchestration of the aggregation of actuators, i.e., the HMI (Human-Machine Interface) part of the outer control loops falls into the topic of this chapter.

1.1. Overview of Autonomous Vehicle Technology

The early work on autonomous vehicles in the 1980s was funded by governments and primarily private industries because of their close links to national defense applications. This investment was heavily focused on vehicles that were capable of operating in different types of terrains, including roads filled with dust, shade, rain, and/or snow. Lateral and vertical profiles of the ground surface were obtained using a combination of sensors such as LADAR (LAser Detection And Ranging devices), RADAR (Radio Detection And Ranging), and INCA (INertial C-borne Accelerometers) for obstacle detection and mapping. The space shuttle was among the many technologies developed with capacity for autonomous operation. Blockchain was another privately-funded technology focused on innovation for public transportation. Over the past few years, research on roadworthy autonomous vehicles has attracted increased interest due to a combination of advances in technology. The introduction of inexpensive and reliable sensors such as high-precision LADAR, LiDAR (Light Detection And Ranging devices), and cheaper GPS-based location tracking systems is the first reason. Reduced costs for high-precision LADAR and LiDAR and reliable GPS location data is significant too. Finally, advances in machine learning and human vision technology means machines of very high intellect can be taught to recognize objects like other moving vehicles and pedestrians appearing in each sensor snapshot. All these factors have combined to help pave the way for development of more intelligent technology.

Emergence of autonomous vehicle (also known as self-driving, driver-less, robotic vehicle) technology provides an impetus to commuters and decision-makers to invest their time in more productive activities such as reading, playing video games, texting, or watching movies while en route to offices, factories, airports, and meeting destinations. As autonomy eliminates the need for human supervision, it frees that time for other uses. In simple words, a vehicle is called fully autonomous if the vehicle not only is capable of getting the destination without any interference from any passenger, but also has the capability of making decisions on its own about other vehicles and systems operating alongside it. Such vehicles are also known as robotic or driverless because they are capable of sensing their environment and navigating without human input and supporting fully autonomous operation of at least one passenger, although they may require human interaction at other times for normal operation. Historically, autonomous vehicles started with small-scale demonstration where it has been limited to demonstration in specific, restricted environments, such as laboratories, transits, and military sites, for testing purposes. However, due to recent advances in sensing, computing and wireless communication, small-scale production of commercial autonomous vehicles are available today, with large-scale commercial distribution of fully-automated vehicles expected towards the close of this decade. The prime focus of the APDANAVNET is to develop technology to manage such production environment of fully automated vehicles. In this section, we provide an overview of the major advances that have facilitated realization of this possibility.

1.2. Role of IoT in Autonomous Vehicle Networks

A high-level converged model applying IoT to both the roadside environment and the AV transport network, which can support all its automated vehicle-related processes involving V2V, V2I, and other user communication. Building on this work, a more detailed project to visualize the different components of this model is presented. This model is underpinned by the same 7-layer OSI model structure of IoT within the context of AV networks utilized by other authors, based on the fact that ITS is a subset of IoT and can be mapped onto the IoT protocol stack.

Because of the considerable attention on IoT in AV networks, it is important to differentiate between one specific model of IoT that could be alternatively labelled Vehicle IoT (VIoT), and another category of IoT devices that can be loosely called IoT sensors. VIoT devices are installed on vehicles and involve connected vehicle technology, although they are typically separate from the core connectivity that can be operated independently of the vehicle (e.g., telematics units sending data to remote data centres). Meanwhile, IoT sensor devices could be obtained from many different sources and have capabilities well beyond the capabilities of VIoT devices, while still often without fully integrating with the broader AV network. They can provide valuable context and data feeds useful for many AV network applications and are typically integrated into other IoT communication infrastructure associated with the roadside environment, which could be used for many other transportation and smart city applications not specific to AV technologies.

2. Cybersecurity Risks in Autonomous Vehicle Networks

The critical density of accidents and continuous research in robust autonomous systems and sensor technology has caused some difficulty in the operation of autonomous vehicles due to the shortage of physical cables that transmit information in milliseconds. Autonomous vehicles have external devices and wireless networks that are outdated and have several defaults, these safety devices can be considered distinctly from the electronics and the communication network, making differentiation in packet exchange. Cyber risks, however, are not reduced. The enormous amounts of data collected by traffic monitoring or global positioning, for example, can be hacked, these dangers are an opportunity, making profit from only a selected group of companies.

The sensors allow the monitoring of the presence of passengers and also the need to provide several cyber-related automotive safety warning signals. A proposed risk model is organized in related stages and points applied to future vehicles in order to improve vehicle safety and improve the quality of passenger information, a development in autonomous vehicles creating mass security problems on routes and significant traffic incidents.

Autonomous vehicles carry information sensitive enough to have a considerable economic and even privacy value to the passengers transported, a complex market that involves not only the advanced technology market and the new industries of network services but also the car market.

The request for sufficient capacity to cover several applications in IVNs has led to the development of IVN technologies to deploy Ethernet-based networks. Current trends for fully autonomous vehicles require high-bandwidth networking with stringent requirements for real-time faults. The communication network must provide significant synchronization capabilities, addressing elements encountered in classic networks such as ECU and advanced sensor technology to process data effectively.

Autonomous vehicles are complex systems interconnected in various ways, consisting of vehicle control units and a wired or wireless network. The network, called the In Vehicle Network (IVN), provides data transport and exchange between different units present in a vehicle. An IVN is at the heart of the vehicle's many innovations, such as advanced driver assistance systems (ADAS) and autonomous driving functions.

2.1. Types of Cybersecurity Threats

Because the dynamic risk assessment (DRA) methodology is based on the relationship among the system vulnerability, consequence, and threat, a detailed explanation of the selected cyber threat is explained. The selected cyber threat is comprehensive. Specifically, the primary goal of comprehensive threats is to compromise system confidentiality, integrity, authentication, and availability by utilizing the above-mentioned attack types. After that, a risk model should be established. To overcome risks, information technology or other functional measures can be developed according to the specific types. At the end of this chapter, the analytical risk model which assesses the benefits or penalties of a cybersecurity measure is presented. Accurate, safe, and reliable dynamic risk assessment can be done by adapting to any cyber threat.

Online cybersecurity issues are divided into two groups according to the nature and manner of cybercrimes, i.e., unauthorized access to the security of an information system or data or any attempt to compromise the confidentiality, integrity, availability, authenticity, and accuracy of system components, thereby causing risk and potential harm to the government, business, and home users due to certain intentions. Explicitly, the types of active cyber threats include the following: information society threats, e-crime threats, e-attack threats, and e-warfare threats. Information society threats are phishing, denial-of-service (DoS) attack, and distributed denial-of-service (DDoS) attack. E-crime threats are online fraud, banking robbery, malware attacks, and attacks against critical infrastructure. The e-attack threats in the Internet of Things (IoT) include jamming, eavesdropping, path simulation, sinkhole, wormhole, Sybil attack, replay, selective forwarding, and hello flooding. Finally, e-warfare threats are cyber-spying, psychological warfare, and electronic warfare.

2.2. Vulnerabilities in IoT-connected Autonomous Vehicles

In a high-speed vehicle environment, a denial-of-service (DDoS) attack on the vehicle's sensor could have fatal effects. Similarly, DDoS attacks can manipulate attacks on inflexible automotive networks that depend on the spread of messages. An autonomous vehicle is part of a larger transportation network that relies heavily on digital communication between other vehicles and network infrastructure. As a result, the network is at risk of cyber-kinetic attacks, which can have far-reaching unintended consequences. Any of the harm that simple accidental collisions might trigger to their owners might be litigated. Autonomous vehicles are in their primary stages as a business. As a result, security audits of various specific vehicle implementations are inadequate. This lack of transparency is exacerbated by the limited visibility that traditional dealerships usually have into vehicles' internal configuration. This frequently means unexpected harmful settings in certain low-budget vehicles can bring cars on to the road.

Although many accidents related to autonomous vehicles are caused by other vehicles, pedestrians, and animals, a significant percentage happen due to the absence of communication between the two vehicles. The most notable vulnerabilities are summarized below. The danger of data corruption due to sensor man-in-the-middle attacks is exacerbated by the sharing of erroneous location data related to inflexible virtual networks that most autonomous vehicles use. Broadcast transmissions are vulnerable to jamming, and the signal coming from sensors of autonomous vehicles is very reluctant to deal with the consequences of the blinding of light. Inadvertent electromagnetic interference is frequently triggered during standard network operations. Mistakes in the routing of data packets which unintentionally overflow segment buffers are better understood after that buffer.

As with traditional vehicles, autonomous vehicles can suffer from a large number of hazards, including mechanical failures, human errors, and weather conditions. Analyses have shown, however, that the main cause of accidents is indeed human error, particularly under the influence of medicines, alcohol, or distractions while driving. Autonomous vehicle technology is expected to significantly curtail this vulnerability.

3. Dynamic Risk Assessment in Autonomous Vehicles

Indeed, the challenging AV design question is not of avoiding rare catastrophic events (which has generally been the focus of traditional AV research and development) but in minimizing system-wide risk accumulation and propagation effects inherent to large-scale, AV-dense networks. Researchers have largely treated challenges to achieving a safe AV society as solvable through the development of improved, high precision, centralized sensing and perception, where the vehicle reacts to time-varying hazards around its own state. However, new security concepts and designs will be critical to secure the continuous data and wireless communications supporting the autonomous functions, and to secure vehicle design against both cyber and cyber-physical attacks. These new security challenges are generally less tractable than improvement to distributed sensing and fusion and should not be discounted.

Risk-antagonistic autonomous vehicle (AV) operation is a key consideration in enabling AV deployment at scale. AG data from the IoT infrastructure provides information relevant to the question of dynamic risk assessment in specific AV networks. Here, we begin with a conceptual model of AV networks and dynamic risk management, and we discuss how to leverage machine learning and IoT infrastructure for real-time dynamic AV risk assessment in this large-scale AV context. With respect to the large-scale context, we focus on shared, publicly available, open datasets and consider sources currently available for New York City and potentially Los Angeles. While the primary focus of this chapter is on evolving technologies and related data sources, the supplemental material in Appendix A provides more details for developing a risk assessment design framework, including potentially relevant infrastructure components such as platooning, edge-based computing, and cellular autonomous vehicle (CAV) device-to-device/vehicle-to-vehicle (D2D/V2V) communication.

3.1. Traditional Risk Assessment Methods

The main limitation for this type of approach is linked to both the simple possibility of foreseeing all critical scenarios and thus all risk factors, and besides the ability to evaluate the dynamic system behavior and infer analogous risk criteria. In other words, these methodologies generally do not have sufficient flexibility to cope with unknown events or events for which have not been properly planned. The evaluation is done through probability-based approaches, leading to an overly conservative evaluation of projects with few similarities with actual risky situations. The evaluated scenarios have little in common with the complex and unpredictable characteristics of the real-world scenarios.

Dynamic systems such as robots and vehicles, in particular, autonomous vehicles, generate a demanding environment from an analysis perspective. The risk assessment for these systems can traditionally rely on classical techniques such as FMEA (Failure Mode and Effects

Analysis). The application of FMEA typically involves an exhaustive analysis of all possible failure modes of an element of the system and attributes a score to each mode. Other mechanisms for risk assessment are like PHA - Preliminary Hazard Analysis, CHAZOP - Check Hazard and Operability Study, SIMOPS - Simultaneous operations and Personal Safety and Safety Rating. These methods are mostly based on system analysis and not on data, and in many cases, only the probability of a risk event happening is considered in the final approach and potential encounters with loss or damage are not accounted for. Note that DNF (Dynamic Nuclear Fireball, Prusa, Irons, Rahmani (2014)), a Cause-Consequence Analysis tool that is able to analyze the dynamic safety status of critical facilities, is a rare example of a traditional approach able to tackle some dynamic aspects of risk but is limited to the nuclear sector.

3.2. Challenges of Dynamic Risk Assessment in IoT-connected Networks

Utilizing more advanced surveillance devices such as advanced video surveillance, AI or rule-based decision support, and detection tools can enhance traffic management effectiveness and improve traffic laws compliance. This becomes more challenging when the vehicles are driving through CAV dedicated lanes and policy enforcement is essential to validate the end-to-end policy and achieve the intended intelligent outcome. Next, the level of complexity sharply increases when the focus of risk prediction is on cyber-physical network attacks or novel risks that have never been experienced before. Unlabeled operations and unknown risks also add to the challenge. Although passive devices sense the potential risks, accurately modifying and re-identifying risk event features in real-time to rank the risk is complex. It is identified that unsupervised and semi-supervised learning techniques face many challenges in generalization, low in-class variance, and scalability when vibration, magneto-resistance, noise, and power grid signature analysis are applied.

The challenges of identifying accurate risk measures in an IoT-enabled CAV environment present several technical difficulties that need to be addressed. First, the impact of a vehicle collision is different for different vehicles and locations. For example, a vehicle collision at an airport or a downtown area has different effects compared to a similar accident in a semi-rural or rural area. As such, passive devices alone are not sufficient to provide the level of information required to distinguish risks from traffic simulations simply based on the speed, vehicle type, and location of vehicles. In addition, there may be malicious incidents to avoid or detect.

4. Computational Intelligence Techniques

This section provides an overview of the most relevant computational intelligence techniques that can be applied for accurate and reliable classification, prognostication, and forecasting of road traffic anomalies that lead to increased accident risk in IoT-connected AV networks. In particular, in this section, we focus on the techniques that are considered to have matured from their development and application in the field of computational intelligence, becoming mainstream methods both within academia and industry for time-critical applications.

4.1. Machine Learning Algorithms for Risk Assessment

A concrete classification of dangerous traffic events is relevant in the interaction of multiple vehicles in similar groups. If the events themselves occur in a continuous time frame, the new study goal is to develop algorithms for predicting when and to what degree a threat between independent traffic events manifests itself in a relatively short time period in the monitored traffic scenarios. Data labeling may be relatively problematic in specific cases, such as the moment of collision, and occasionally more complex when there are mixed traffic situations in very dense traffic scenarios. However, ground truth values can also be associated with where the objects of interest are located in the scene, which is common in the so-called dense prediction task.

Machine learning algorithms can provide a range of successful approaches to learning a predictive model from risk data. In the scenario of autonomous vehicles, methods of numerical modeling of road and traffic situations with machine learning use the following input features: (a) the geometric and physical characteristics of road structures visible to a sensor, such as roads, intersections, sidewalks, presence of pedestrians and cyclists, and the number of lanes for certain types of paths; (b) state parameters of common and individual road users captured in a scene with multi-level access networks; and (c) the game between road users' behavioral models. The outputs of such models should reflect not only collision prediction but also detailed predictions of possible time-spatial interactions between different environments consisting of one single vehicle and multiple collaborative vehicles.

4.2. Artificial Neural Networks in Cybersecurity

Artificial immune systems have been used as a way of mitigating different types of service attacks such as ping of death, teardrop, and land attacks. Reinforcement neural networks have been used for phishing detection. Phishing detection is one of the most important and difficult tasks in cybersecurity due to the flexible structures and content of phishing contents. Convolutional neural networks have been used in conjunction with game theory and cognitive computing for mitigating APTs. Deep learning exhibits significant early stage detection of network intrusions. These are just a handful of examples of the myriad possible applications of the numerous subtypes of neural networks to cybersecurity problems. Considering the broad range of possible neural network applications to cybersecurity problems, we must narrow the parameters of our current investigation and focus on those aspects of neural networks that are best suited to the technology of autonomous vehicle cybersecurity defense. Understanding the analogy of why the human brain learns is a microcosmic viewpoint, while computationally generating randomized decision trees is a macrocosmic viewpoint. Within the context of autonomous vehicles' cybersecurity, we must be microcosmic rather than macrocosmic. We focus our current investigation on the subdomain of decision trees.

Given their interdisciplinary nature and their flexibility in terms of architectural design, artificial neural networks are powerful tools for dealing with many classes of cybersecurity problems. They are capable of identifying patterns that traditional cybersecurity tools are not adept at identifying, and they are particularly good at dealing with high-speed processing of large volumes of diverse data that is typical of many cybersecurity situations. The backpropagation family of neural network algorithms has been shown to be effective in protecting a computational control environment such as an autonomous vehicle from hackers. They have also been applied to encrypted anonymous communication and encapsulation communication traffic at a normal rate, with anything exceeding the encapsulation rate classified as denial of service attackers. Wavelet transform neural networks have been used for encrypted network intrusion detection, and the Textural Features Artificial Neural Network (TFANN) has been used for network intrusion detection of Ethernet local area networks.

5. Integration of Computational Intelligence in Autonomous Vehicles

5.2. Ongoing Work The implementation of computational intelligence in autonomous vehicles presents itself as an essential issue. This involves the development of new risk assessment methodologies and security policies to a greater extent, as they play a crucial role in vehicle decision-making and allow the automatic control systems to continuously adapt to adversarial situations, in order to guarantee that the vehicle reaches its destination in all safety, even in the presence of malfunctions, faults, or external attacks. In this area, part of the ongoing work is mainly focused on embedding the endpoint intelligence of the vehicle and the network where all the communications occur. In fact, in order to guarantee the real capacity for autonomous decision-making, it is necessary that these technologies are part of the vehicle's own systems, not just being developed in external supports. The involvement of the University of Salamanca team in intelligent techniques is geared towards the realization of intelligence at the NAF level, in order to guarantee much greater decision-making capacity. Furthermore, it is intended to integrate the technological developments in secure communications systems to other areas, for example in the intelligent construction of new vehicle prototypes.

5.1. Introduction The development of AVs is creating an established new ecosystem that can drive automobile design, component innovation, and consumer, business, and public experiences. For example, it may allow companies to operate nearly autonomous vehicle fleets, which could be used both for logistics and for pay-to-order travel services, with the potential to significantly reduce accidents, traffic congestion, and the environmental impact, while also increasing the utilization rate and efficiency of the transportation systems of the cities in which the vehicles are operating. Furthermore, the main intrinsic assets of autonomous vehicles are the connection to the network, being their capabilities much greater in these conditions, resulting in a much higher level of efficiency and security compared to traditional vehicles. However, to ensure the safety, security, and stability of these networks, it is necessary to strengthen the intelligence of these vehicles by taking into account the different existing risks.

5.1. Real-time Decision Making

The advanced vehicle dynamic decision making needs to be mapped at various levels such as active safety, risk assessment, driver workload, route planning, vehicle to infrastructure/V2V communication, emergency services communication, lifetime vehicle health monitoring, driver assistance, and entertainment. The AV concept enables 'hands-free' driving with the driver positioned as a higher level 'controller'. The human driver, like the traditional vehicle 'controller', becomes part of a network of intelligent, collaborating controllers that share tasks during the 'driving' phase of the journey. In a similar manner to the autonomous systems of other technical domains, for example unmanned aircraft, robotic devices, etc., the algorithms that realize the intelligent perception and decision making of the networked AV elite can be considered part of the scientific areas of life sciences and computing theory discussed previously.

The fifth core issue and challenge that can be identified in IoT-connected vehicle systems is that of real-time decision making at the level of intelligent, autonomous vehicles. This is the core problem addressed by the entire field of autonomous vehicle (AV) technologies. Infrastructure, vehicles and system (IVS) research projects sponsored by the Engineering and Physical Science Research Council (EPSRC) in the UK have promoted major infrastructure investment in sensor and communication technologies and computational intelligence for connected and autonomous vehicle platforms. Howard et al. give an example of a dynamically reconfigurable cognitive system for the control of large numbers of modules, showing that the control of the resultant systems is complex and its flavor is very different from that of application-specific, programming by example (PBE) graphs. Significant progress has been made in addressing this problem via the development of various driver support systems based on intelligent sensors and actuators that continuously monitor the driver, vehicle, and surrounding environment, leading to various real-time decision making algorithms.

5.2. Adaptive Security Measures

Adaptive security measures comprise distributed IDS agents in the software-defined chassis (SDC) of the autonomous vehicle to enable mobile edge intrusion detection services. The rationale behind these agents is the expectation that the IDS detection speed will govern the execution of the existing security monitoring tasks. The anticipated element of novelty is the technique to trigger learning with a few labeled examples on detecting an abnormal system call sequence that, when achieved, results in a notable refinement of multiple classifiers and is accompanied by a very low false negative rate. The relative evaluation of two machine-learning classifiers concludes with a newly proposed simple complexification test. The adaptive IDS design principles are expected to be universal; future autonomous vehicles will integrate security measures specific to vehicle components.

Adaptive security measures enable autonomous vehicle networks to detect and mitigate dynamic physical or cyber-physical security threats and provide a tolerant system that continues to operate despite the newfound vulnerabilities. The adaptive security schemes discussed in this section include intrusion detection systems (IDS) that detect user-level and network-level intrusions, and active countermeasures that thwart the intrusions. Such security measures enable cooperative, future-resilient transportation systems that deliver safe, economic, and efficient transportation services. The essential IDS challenges consist of continuous online learning with minimal labeled examples, and detecting unknown unknowns, interactive queries, and synthesizing adversarial examples.

6. Case Studies and Applications

How to define the safety of autonomous systems is a challenging issue itself. There are three entities in an autonomous driving system: the vehicle itself, its environment, and the system responsible for moving the vehicle. Traditionally, the driving environment and the moving system are somewhat under the control of the owner of the vehicle. So their impacts on the vehicle are considered small pulses or noise. The largest challenge comes from the potential intrinsic malfunction of the vehicle, which is mainly due to its AI chips, sensors, and the computing infrastructure. To keep these bad pulses and probabilities smaller than some required target value in a one step of length $h > 0$, people usually duplicate their chips and sensors for example. Nevertheless, in reality the real intervals between any two bad pulses are indeed longer than 1 month, etc. Therefore, in order to test a vehicle, the long time data while the owner is driving their vehicle is indeed the correct sources. Mathematically speaking, the owner enjoys full access to the h-probability. Numerically, the authors of this chapter assume to know the mean value and the expected value of the probability field. Despite some conservative viewpoints, the periodic predictable levels in a normal interval is chance and from the mathematical viewpoint, the AI chips take care of it perfectly.

Human society is changing all the time. Ten years ago, fewer people could imagine that self-driving cars would achieve such popularity. Taking Shanghai and Beijing as examples, people in these two largest cities-provinces in China usually spend at least 1 hour away from 9:00 to 18:00, just for commuting from office to residence. Currently, people have better choices. In the future, when self-driving cars become more reliable, convenient, and cheap, people will have more time to work, rest, play, learn, and communicate. Currently, the biggest challenge for the large-scale deployment of self-driving neighborhood EVs is certainly their safety. This chapter provides practical mathematical tools that help developers of autonomous systems and regulators to evaluate and improve the confidence in the safety of such systems. Through a simple case study, the authors of this chapter further demonstrate the capability of their theories.

6.1. Implementation in Autonomous Vehicle Testbeds

As a first baseline study, researchers can use realistic and practical access to USF's research instruments and testbed vehicles (including implemented onboard sensor technology and external vendor services) to install and adapt smaller subsets of IoT devices to evaluate the global control algorithms and rule-based policies in limiting the risk of the network of heterogeneous autonomous vehicles. This means that the developed algorithms can be implemented and tested in the real world in a controlled and practical environment.

As part of an ongoing partnership, the authors have access to USF's Connected Vehicle Instrumentation Laboratory (CVIL), along with resources for implementing and testing these models. Moreover, because of resources from the Florida Department of Transportation (FDOT) and USF, the researchers have access to designated road facilities for implementing and evaluating these testbed concepts in the real world. Furthermore, we have identified partners with similar open and secure connected and autonomous vehicle (CAV) test facilities in other US states and internationally for collecting a diverse range of relevant data for analysis and validation testing.

6.2. Industry Applications and Success Stories

In the following sections, we deep dive for two specific IoT industry verticals: precision agriculture and supply chain optimization, to discuss their real-world use cases and the transformative success they have seen on the back of IoT adoption.

Precision agriculture (for optimizing irrigation, smart machinery to improve efficiency), Industrial Sector (better energy management, operational predictability, failure analysis, robotics optimization), Logistics (real-time logistics and supply chain management, improved operational efficiencies), Retail (optimized business administration, operational efficiency), Energy (System aggregation optimization), Healthcare (Remote health monitoring to improve patient care), and Smart homes (proactive customer support to improve customer experience and chatbots for predictive maintenance in home appliances).

With tech unicorns emerging like mushrooms and as newer solutions evolve which combine sensors at the edge, over-the-top applications at the edge, data monetization and newer business models (the platform innovation model that mobile OS and device manufacturers exploited), the Internet of Things marketplace is in a state of incredible flux, with groundbreaking transformations, radical value creations and transformations across a wide array of sectors. Few of the sectors where IoT is being used with groundbreaking successes include:

7. Future Directions and Emerging Trends

Due to the requirement of IoT-interconnected autonomous driving vehicles in the real world, monitoring and risk-management strategies based on intelligent data analytics would play a key role in the insurance of autonomous vehicle ethics, security, safety, reliability, and acceptability.

As many emerging technologies continue to change the ICT landscape, CI techniques that have been significantly active in IEEE IoT Transaction, such as deep learning, fuzzy rules, and reinforcement learning, are expected to have a strong influence on future research-based IoT problems involving CAVs with fixed and mobile IoT devices. The effectiveness of these models for different risk assessments needs a well-executed formation of the vision of possible consequences and uncertainties in the context of CAV operations while integrating monitored data-driving vehicle operation features with IoT-generated data.

After analyzing the proposed risk-assessment techniques, it is required to develop new risk-mitigation or sharing strategies for efficient protection against different security risks. A novel data-driven approach should be developed for online learning and data analytics to have a better understanding of a system's novel configuration to assess the dynamic risk in autonomous driving vehicles. To improve the implementation of autonomous driving-vehicle systems, it would be necessary to have a new hybrid mathematical approach that would combine the deterministic, stochastic, and machine learning components for dynamic risk evaluation.

In future, the proposed risk assessment should handle the confidentiality, availability, and integrity issues of different generated and exchanged risk values and share strategy in the presence of advanced and intelligent attacks. In the current scenario, the developed risk evaluation should be used in the centralized manner, such as servers, for decision strategies, which would raise the concerns of multiple entities, location privacy, and backdrop of privacy issues.

Future Directions and Emerging Trends Here, we describe future directions of dynamic risk assessment in the context of CAVs and the emerging trends in CI and IoT. As we discuss several challenges and drawbacks associated with existing and emerging risk assessment techniques for dynamic risk assessment in CAVs, it would be interesting to consider existing modeling techniques for risk evaluation or to emerge with new modeling and evaluation techniques that would help us to deal with different challenges and drawbacks.

In this section, we describe future directions for dynamic risk assessment in CAVs and the emerging trends in CI and IoT.

7.1. Advancements in AI for Risk Assessment

AI can also be broken down into weak and strong AI. When a computer can be set to solve any issue that arises in day-to-day life, irrespective of the field of activity or knowledge, it will be said to be a strong AI. When the role of AI is limited to certain tasks in specific domains, it is then categorized as weak AI. Today, weak AI is in its advanced stage of research and application development. In comparison with strong AI, weak AI has transformed a large number of manual methods that were time-consuming and error-prone in their tasks. In this context, AI may involve the application of various types of algorithms used to train, guide, evolve, correct, think, and perform tasks the way it suits.

7.1: Advancements in AI for Risk Assessment 7.1.1: AI Artificial intelligence (AI), in its basic definition, is a field of computer science that focuses on the creation of systems that can perform human-oriented tasks which otherwise require human intelligence capabilities. AI is composed of multiple models and techniques that allow systems to do tasks such as problem-solving, learning, decision-making, and integration so that they can truly mimic human behavior.

This chapter suggests an extension of the non-cautious AI models from virtual decision-making to real-life decision-making processes of autonomous driving and cloud-connected IoT applications. Specifically, we present a fusion-driven research model that fuses all risk, threat, and vulnerability models developed in previous chapters to service the mission of spontaneous cloud service access of autonomous vehicles (AVs). All AI algorithms deployed in this chapter satisfy the diversified mission-driven evolution of IoT autonomous vehicles.

Rapid advancements in artificial intelligence (AI) technologies, specifically in the field of computational intelligence, have been achieved in the past few years. AI is the main algorithmic driver for simulating human intelligence in machines. Machine learning, deep learning, neural networks, decision trees, and genetic algorithms are some of the AI technologies that have been applied to complex systems operations and management.

7.2. Ethical Considerations in Autonomous Vehicles

One well-known issue in the debate about self-driving cars can be seen in the classic Trolley problem. Andrew Ng et al. suggested that we construct machine ethics through Asimov's four laws of robotics, not programming cars for the disadvantage case where moral decisions have to be taken. This is similar to the SAE's guideline that, when collisions cannot be avoided, the collision should be minimized, and that the design should not be made in favor of certain people unless aiding people in special conditions, for example, the disabled. The vehicle should be maximizing safety. The most notorious answer to the Trolley problem is that it is unlikely that the event will happen at all, as this problem is already included in the driver's license process and human drivers all around the world are passing this "ethical" test every day on the road without existential anxiety. In response to this, most of the proponents of autonomous driving argue that the Trolley problem is very old and it takes a small part of the entirety of ethical decisions in the transportation industry. Good examples are the many everyday traffic conditions and decisions necessary to be maneuvered.

In intelligent systems, at some point, it will be imperative to include ethical rules into the AI system in order to attain its societal legitimacy. Because ethical considerations are the difference between simply acting on a decision and searching for just, responsible, and fair action. Such decisions where fairness and the moral considerations of many parties are involved should not be left to the experts or the designers of the system only. More importantly, these considerations are not the property of the AI system or the vehicle, but of society. Ethical rules should be decided with a majority of society's opinion, and then these rules should be incorporated into AI systems.

8. Conclusion

T-Reservoir exhibits the best overall performance. A slight increase in average time complexity compared with N-Reservoir does not challenge its latency as it still guarantees the application of real-time DRA for AV networks. Furthermore, the memory footprint of T-Reservoir is approximately 0.36% and 0.65% of the data transmission size of the fully connected traditional and N-1 Reservoirs, respectively. Therefore, a truly lightweight, feasible, and reliable solution has been proposed to capture Sx within M-RC form as well as the communication scheme, the optimal decrease in the utilized bitstream size, and finally the adherence to realistic simulation imitations on the bitrate dimension.

In real-world applications involving dynamic risk assessment such as AV networks, Reservoir Computing shows promise as a CI approach for fast decision making based on spatiotemporal multisource data. The RC-based DRA model developed is effective in learning multiple sources of distributed historical risk data and their relationship with a variety of simulation scenario setups. The models can handle changes to the control strategy and offer quantifiable improvements in decision making. The transfer learning approach is also effective in quickly updating weights in the well-trained models when they are deteriorated by recent new sampled adversities of various contexts, ensuring consistent risk categorization capability. Experimental results in both conventional and novel assessment approaches are promising, warranting further research with real-world datasets and with further advances in the computational power and memory capacity of current hardware/software platforms.

9. References

1. S. Zhang, S. Zhao, Y. Liu, W. Shi, and L. Su, "Dynamic risk assessment in the Internet of Things," in 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1-6.

2. Y. Fang, Y. Zhang, Y. Qian, and S. Li, "A dynamic risk assessment method for IoT-based intelligent transportation systems," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications

(GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 1125-1130.

3. S. R. Mishra and S. K. Satapathy, "A dynamic risk assessment system for IoT based real time applications," in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 3304-3309.

4. A. Albogami, S. El-Alfy, and E. Shakshuki, "A dynamic risk assessment model for IoT systems," in 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), 2019, pp. 246-253.

5. S. Ouadoudi, S. Benamar, A. Ait Ouahman, and K. Sabri, "Dynamic risk assessment in IoT networks using Bayesian networks," in 2019 IEEE 5th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), 2019, pp. 1-6.

6. R. S. Hidayat, S. A. Suryana, and Y. Choi, "Dynamic risk assessment model based on fuzzy logic for IoT network security," in 2019 5th International Conference on Science in Information Technology (ICSITech), 2019, pp. 44-49.

7. Y. Wang, F. Xu, J. Wang, and Y. Liu, "Dynamic risk assessment of Internet of Things based on ELM algorithm," in 2020 IEEE 3rd International Conference on Electronics Technology (ICET), 2020, pp. 90-93.

8. H. P. Nguyen, T. H. Dao, and D. N. Nguyen, "Dynamic risk assessment model for Internet of Things based on Dempster-Shafer theory," in 2020 7th International Conference on Electrical and Electronics Engineering (ICEEE), 2020, pp. 122-127.

9. H. Geng, X. Chen, Z. Lu, and D. L. Lee, "Dynamic risk assessment in IoT networks using a deep learning approach," in 2020 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2020, pp. 1161-1166.

10. Z. Li, S. Zhang, and Z. Liu, "Dynamic risk assessment method for IoT system based on adaptive boosting algorithm," in 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2020, pp. 1342-1345.

11. S. S. Hamad, R. A. H. Abdulsalam, and M. N. G. Khan, "Dynamic risk assessment in Internet of Things (IoT) using machine learning algorithms," in 2020 5th International Conference on Computing, Communication and Security (ICCCS), 2020, pp. 1-5.

12. Tatineni, Sumanth. "Compliance and Audit Challenges in DevOps: A Security Perspective." *International Research Journal of Modernization in Engineering Technology and Science* 5.10 (2023): 1306-1316.

13. Vemori, Vamsi. "From Tactile Buttons to Digital Orchestration: A Paradigm Shift in Vehicle Control with Smartphone Integration and Smart UI–Unveiling Cybersecurity Vulnerabilities and Fortifying Autonomous Vehicles with Adaptive Learning Intrusion Detection Systems." *African Journal of Artificial Intelligence and Sustainable Development*3.1 (2023): 54-91.

14. Mahammad Shaik. "Rethinking Federated Identity Management: A Blockchain-Enabled Framework for Enhanced Security, Interoperability, and User Sovereignty". *Blockchain Technology and Distributed Systems*, vol. 2, no. 1, June 2022, pp. 21-45, https://thesciencebrigade.com/btds/article/view/223.

15. S. Kim, J. Cho, and J. H. Park, "Dynamic risk assessment model for IoT devices using machine learning," in 2021 International Conference on Information and Communication Technology Convergence (ICTC), 2021, pp. 941-944.

16. J. Zhou, X. Zhang, Y. Qin, and W. Zhang, "Dynamic risk assessment in the Internet of Things using a hybrid model," in 2021 5th IEEE International Conference on Computer and Communications (ICCC), 2021, pp. 3205-3209.

17. J. H. Yoon and J. Lee, "A dynamic risk assessment model for Internet of Things security using machine learning," in 2021 IEEE International Conference on Big Data and Smart Computing (BigComp), 2021, pp. 1-4.

18. M. M. Rahman, M. Z. Shakir, and I. Zeadally, "Dynamic risk assessment for IoT networks using machine learning," in 2021 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2021, pp. 1-5.

19. S. W. Lee, K. Kim, and S. K. Baik, "Dynamic risk assessment in IoT networks using machine learning and blockchain," in 2021 IEEE 21st International Conference on Advanced Communication Technology (ICACT), 2021, pp. 431-435.

20. Y. Ren, J. Zhao, and M. R. Javed, "Dynamic risk assessment for IoT security using deep reinforcement learning," in 2021 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2021, pp. 1060-1065.

21. M. S. Elbamby, A. Zoha, and M. Hassan, "A survey of machine learning in Internet of Things (IoT) security," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7289-7310, Oct. 2019.