Computational Intelligence for Energy-Efficient Routing in IoT-connected Autonomous Vehicle Networks

By Dr. Andrés Ortiz

Professor of Industrial Engineering, Universidad Industrial de Santander (UIS), Colombia

1. Introduction

AVs are, by definition, mobile platforms that can sense the environment. These can contribute to the IoT infrastructure by sensing and sharing with other AVs the location of crowded conditions, so that these areas are avoided. Such a benevolent action requires routing in an environment where not only the edge and cloud (wired) core nodes are capable of running the rich transport layer in conjunction with the wireless edge but also mobile nodes quickly switch between these layers and network segments. The ability to switch between these layers and network segments requires cooperation between transport layer users and network layer infrastructure. It is hypothesized that the ease of establishing the cooperation benefits from a cooperative approach, as opposed to the traditional hierarchical approach. A cooperative approach is characterized by the fact that not all functional tasks can be assigned to specialized entities. This feature requires all entities to have some competence in related functions pertinent to the task currently carried out by a different unit.

The widespread deployment of autonomous vehicles (AV) is expected to lead to significant societal benefits such as a reduction in the accident rate and enhanced traffic flow, both of which contribute to an increase in energy efficiency. These benefits are based on the assumption that vehicle components seamlessly communicate up to the point of being able to cooperate efficiently. The communication infrastructure, traditionally based on physical infrastructure, is expected to consist of crowd sensing Internet of Things (IoT) infrastructure, and connected AVs of varying manufacturer, sensor, and software sophistication. The social acceptance of such communication systems leading to the expected societal benefits may, in part, be driven by the range of applications, and in the context explored in this research, using the communication infrastructure for environmentally friendly solutions. Reducing the

environmental impact of AVs by making them electric is also expected to accelerate the acceptance of self-driving cars.

1.1. Background and Motivation

Therefore, we have a focus on developing that intelligent approach to support both autonomous vehicle operation as a peer of the Internet of Things in a road network in which there is a full support for the vehicle's transition from the vehicle support segment into the database access point supported by the Internet of Things but at a higher cost. Consequently, determining the vehicle segment-of-the-edge support structure in the road link is important. Simulations of the node capability when using a monitoring and data collection approach to understand how the IoT functionality supports the operation of the AV by exchanging data with the operating vehicle. However, they do not look at the routing algorithms to determine the importance of the sensing data exchange that also can be used by the vehicle to determine the best path that will have the least cost due to consuming less fuel while transiting the VSB. In this document, this situation is our core interest and is therefore discussed towards the development of an approximate solution to this model.

Autonomous vehicles represent an important research area involving various features such as maximum ad hoc system operation, data exchange round delay requirements, and energy consumption during connection and operation. Support on using the intelligence of the vehicle to address the demand and management of the applications and sensors in support of its operation shows the result of information exchanges with the Internet of Things. The exchange between the autonomous vehicle and the Internet of Things means that such network enables autonomous vehicle operation without losing access to the Internet of Things connection point and the improvement provided by data stored in the associated database because those pools do not necessarily change attributes. An insight on how to prioritize the exchange of information with the vehicle and of the types of information that are weighted within the decision-making process when preserving the vehicle's Internet of Things connection point due to the availability of finite energy provides some guidelines to design the traffic engineering employed for the exchange.

1.2. Research Objectives

The primary objective of this research is to propose the use of computational intelligence (CI) paradigms, specifically nature-inspired algorithms that include genetic algorithms (GAs), convolutional neural networks (CNNs), and particle swarm optimization (PSO), for energy-efficient routing mechanisms in IoT-based autonomous vehicle communication environments. The learning and optimization capabilities of these CI methods are capable of making resource allocation decisions by predicting and evaluating the consequences of our proposed problem solutions with minimum dependencies on propagation models and architectural assumptions. This evolvement proposes generic solutions which can potentially work with different vehicle operating conditions and enabling computational scalability to allow real-time application of the IoT domain. Other benefits include adaptive decision rules to account for the intrinsic uncertainties in channel states, ad-hoc joint optimization of transmit powers, selection of network parameters, and enhancing overall system performance in terms of improved energy utilization, quality of service, minimum packet drops, and seamless service provisioning even under high levels of varying velocities and low rate of available channel state and side information. Our research problems include performance evaluation in terms of average packet delivery ratio, energy efficiency, average end-to-end delay, and information density under a variety of traffic possibilities, traffic classes or marking schemes, link and flow properties, and different vehicle configurations with varying number of antennas and transmit power levels for different types of communication channels in a vehicular environment. Additionally, our secondary objective is to identify any potential misuses or misinterpretations in existing learning paradigms and proposing alternative improved learning and networking paradigms for various autonomous vehicle-specific applications.

2. Autonomous Vehicle Networks

The agents in the AV network consist of the AV and the IoT devices which support the functions/services required by the AV. The IoT devices can be divided into two categories, including infrastructure devices and non-infrastructure devices. The infrastructure devices are fixed devices, such as access points (APs), which are mainly used to forward the data between the AV and the core network. The AI technique is used to route the AV energy efficiently to the destination while ensuring the service quality of the IoT devices on the route, so as to avoid the occurrence of AV energy deficiency and route malfunction caused by the limitation of the AV battery. In the environment, a large number of the non-infrastructure

devices which are either stationary devices that provide the information, like the road information in front of the vehicle, or mobile devices that help the AV perform specific tasks can be connected via their capabilities.

Smart cities, increasingly powered by services based on the Internet of Things (IoT), are considered an innovative and green networked community, composed of many IoT-enriched building blocks, including millions of autonomous vehicles (AVs) that can move towards their energy efficiency and intelligent ideal. Nevertheless, due to the inefficient use of energy, the ever-increasing intelligence of the vehicles, and the continuous connection with the surrounding IoT devices, autonomous vehicles may face insurmountable barriers that hinder their ideal transformation. By employing the devices on the AV's route as the agents in an artificial society, the potential of Artificial Intelligence (AI) can be exploited with an aspiration to improve its performance and realize its ideal.

2.1. IoT Connectivity

There are essentially three important components for the design and construction of IoT-connected car and networking systems. Namely, the vehicle components, the communications technology components, and the information technology components. With these interconnected components, vehicles are expected to communicate with other vehicles (V2V), roadway infrastructure (V2I), and even pedestrians' devices (V2P) to follow its trajectory into the hyper-connected autonomous world. Internet application services, which include Internet radio, weather warnings, and road and traffic conditions, are increasingly available in the connected car network. As a result, vehicle-to-everything communication technology, which is a derivative of the IoT concept, has now emerged as one of the most vibrant research areas for automotive and communications.

The future of automotive technology is shifting away from the vehicle as a stand-alone driver of agility and road-wise wisdom. It is entering an era in which the driver remains in control safely but increasingly cedes authority over vehicle and driver-domain decision-making to the vehicle itself. This new driving domain, often referred to as the "connected car," is developing through an array of advanced wireless communication technologies and functions. Such a landscape of converging automotive and connectivity capability includes advanced driver assistance, safety, and road weather notification, location-aware

infotainment, and connectivity to sensors and devices with cloud and web services outside the car.

In this section, we briefly review the emerging connected car technology that represents a major step in autonomous driving. We highlight the prominent role of IoT in the foundation of the emerging vehicle networks and the connectivity establishment by exploiting the cut-the-cord IoT capabilities, including V2V, V2I, and V2P.

2.2. Challenges and Opportunities

Firstly, new routing protocols should be developed to enable the CVIS networks to cope with the basic networking requirements of low-latency communication, error-resilience, bandwidth, and fault tolerance. Indeed, for V2I and V2V protocols to enable multi-path communication, the construction of multiple communication paths from an origin to a destination should consider the available bandwidth, signal quality, residual battery energy, and the vehicular traffic in the roads intersected by these paths. These design issues pave the way to green routing in CVIS-based IoV networks. The major goal of green networking protocols is to minimize the energy consumption and the greenhouse gas emissions of CHV networks without degrading the network performance.

The combination of IoVs and autonomous vehicles is promising for enabling unprecedented levels of road traffic efficiency in an urban environment. In particular, the incorporation of CVIS communication technology enables cooperative collision avoidance and traffic management strategies to mitigate the impact of induced traffic congestion. As the relevance of such technologies becomes critical in minimizing traffic accidents and improving the traffic flow, a few major challenges of these technologies are listed below.

3. Energy-Efficient Routing

Several recent works have proposed the use of edge and fog computing in solving instrumental problems in some well-known applications such as video processing, autonomous driving, and Vehicular Ad Hoc Networks (VANETs). Although all the above with fog and edge sounds straightforward and provide lots of advantages, the energy consumption in these applications is a vital problem. We believe that the computation part plays a vital role in energy consumption because the transmitted and received part of wireless communication devours approximately 3% of total energy spending with continuous sensing

and processing that ask for more energy provisioning from the power sources of the nodes. A real-time and low-earth-delays problem such as the autonomous vehicles' problem that communicate as well as make decisions while driving simultaneously is crucial for fog and edge computing. In this study, we propose a simple but effective method based on the Bayesian Network, RPL (Routing Protocol for Low-Power and Lossy Networks) and Fog Computing. The model of this study provides intelligence to vehicle devices and uses the Fog Computing resources only if it is necessary. With a smart decision provided by vehicle routing protocol, the simulation results in some scenarios show that the proposal model provides a significant decrement in energy consumption compared with WirelessFog.

The energy-efficient routing is vital for extending the life of devices in any IoT (Internet of Things) applications. As in the case of autonomous vehicles where energy-consuming devices are connected and communicate via a wireless medium, a properly designed protocol is paramount. The number of IoT devices is overly increasing with the enhancements in wireless communications, handling of vehicles, the ability of edge computing, and the deployment of fog computing resources. In the proposed artificial intelligence-based routing, vehicles are considered as intelligent IoT devices. The current work takes into account the communication between the cooperative vehicles via the use of fog nodes. In this scenario, the vehicles communicate with successful transmissions by assigning the messages to the appropriate vehicles without utilizing Signal-to-Interference-Noise Ratio (SINR) for the physical layer.

3.1. Importance and Benefits

No matter whether it is safety-related services or advanced IoT services that require higher data transmission rates, the focus on these services is on finding efficient ways of transmitting massive amounts of data while attempting to minimize the broader communication constraints, such as communication delay, network connectivity, bandwidth efficiency, and synchronization. For instance, vehicle speeds can be high, which implies rapid changes in network topology. The energy consumption and vehicle lifetime are relevant in IoT as well as in VANET communications, especially when that is real-time, decentralized, and efficient data dissemination, data collection, or monitoring. Devices in an IoT-connected VANET use batteries with delayed or well or hard limited recharging cycle or mechanisms. Consequently, prolonging the reliability of the energy-constrained VANETBI is essential to network sustainability cost considerations for government and vehicle owners.

While traditional VANETs have attracted increasing attention in the literature, to the best of our knowledge, little attention has been given to the integration of IoT and VANET services within an IoT-connected VANETBI. The future resource-rich IoT-connected VANET corresponding to an IoT-connected autonomous vehicle network consists of not only safety-related traffic information but also high-level predictive monitoring on the surrounding environment, together with the advanced high level of vehicle machine intelligence. The adopted advanced V2X IoT services for autonomous vehicles, either at technical or economical levels, could be satisfying various VANETBI requirements individually depending on promising latency, throughput, reliability, power, and the coverage. As latency reduction, energy consumption, and moderate probability of error are important issues in such high-velocity VANETs, energy-awareness routing protocols built with advanced hardware could achieve more efficient communication. This chapter puts forward a routing method for the autonomous vehicle-specific IoT-connectivity to enhance the reliability of VANETBI simultaneously considering multiple QoS factors and use of a cooperative communication paradigm on the connection of certain vehicles.

3.2. Existing Techniques

The WAVE standardization can instruct the installation standard and safety protocol implementation for vehicular safety communications based on DSRC technologies. It significantly promotes the development of VANET with numerous functions and advantages, such as reduced traffic accidents, concrete and vivid entertainment, completely new infrastructure for smart cities, and so on. The most favorable feature of VANET is direct communications between surrounding vehicles, functioning as a real intelligent traffic mechanism and cooperative road safety insurance for each individual vehicle. The DSRC-enabled wireless environment does not only prevent the development of traditional broadcast and multi-hop technologies for WMN, but requires the integrated network management cooperation, vehicle trustworthy infrastructure, large-scale network situational awareness, and vehicle efficient synergy. Most of these merits are actually challenges in VANET operation, such as plug-and-play functionality, available bandwidth discovery, routing latency and broadcast storm occurrence, trust and privacy issues, etc.

This section provides an overview of the existing primary techniques for energy-efficient routing in WMN. The typical routing algorithm is a minimum-latency and minimum-hop

distance strategy. Our primary concern in this paper is the QoS support for the running AVs in IoT-enabled VANET, so that our algorithm has the following extra features: more dynamics during the vehicles' operation and better service rendering ability in heterogeneous wireless communication environment. For most WMN routing algorithms, however, energy saving has not been considered as an essential criterion. In the scenario that WMN interconnected AVs are used to offer various safety warning and infotainment applications, the energy congestion issue gradually becomes a challenge of energy-efficient routing in WMN.

4. Computational Intelligence

The main focus of this research problem in this paper is to model the problem of the V2E IoT design and integration with an Urban Mobility Management (UMM) network. In this context, we took advantage of the CI system and its swarm intelligence, combining ANFIS models and RBF prediction with reactive PSO, and exploiting the expert knowledge.

If autonomous vehicles need too large an energy reserve to be marketable in some business, the charging cabinets are at stake. In extreme cases, when the autonomy requirements are addressed in some form of transport system, routing algorithms that have been designed for selfish IoT vehicle clients may no longer be reliable. It is imperative to count on self-adaptive performance objectives that align their actions with their environment or allocate decision power to a coordination entity commonly in charge of the infrastructure. Enhancing the vehicle electronic brain with computational intelligence could provide a real innovative advantage or at least a critical minimum level of safety under the traditional operational system that IoT will provide.

The classical approach to designing the mobile network is to keep energy efficiency into account since the beginning of the process, shaping the network for sustainable and resilient performance. Energy-efficient routing algorithms are designed taking future battery recharges of the mobile IoT clients into account and to self-adapt the performance objectives on an energy-efficient speed. However, a reactive model assumes that the energy budget is still acceptable. In more critical energy constraints model, the new problem of the optimization of the Vehicle-to-Energy (V2E) IoT network and its briefcase of chargers arises.

Computational intelligence (CI) is the ability of a computer-based system to reason about data and use prior experiences to learn from it. CI represents a significant potential for IoT and

autonomous vehicles. This leads to the focus of this paper: autonomous vehicles represent a new source of user traffic in IoT networks, and their emerging businesses are mostly subject to their moving power supply. Energy efficiency is crucial for service continuity, i.e., reaching the vehicle with replacement power in unknown areas before its battery runs out.

4.1. Definition and Scope

We consider a scenario where the autonomous vehicles are equipped with the Doppler radar (sensing the distance and speed of surrounding vehicles), GPS (determines the destination), and vehicle-to-everything (V2X) communications (sends and receives information about the surroundings and the driving situation, and the messages are categorized as Global, Local, Personal, or Management). The messages are transmitted to the IoT gateways (which can be located at intersections, buildings, etc.), through 802.11p direct communications, and from there, to the cloud, through the infrastructure IoT gateways, using more reliable technology, such as LTE. The IoT cloud will provide different services and resources to the connected vehicles, based on their location, speed, traffic conditions, emissions level, number of passengers, destination, and some other car-related functions, such as weather sensors, temperature, etc. Then, messages originating from people and devices not integrated in the V2X ecosystem will reach the autonomous vehicles through the same infrastructure IoT gateways. In this context, the most critical challenge comes from the need for reliable and efficient connections between location-aware vehicles and geographically distributed IoT cloud services and resources.

Recent research suggests that the integration of autonomous vehicles, traffic control systems, and the Internet of Things (IoT) can provide several benefits, such as enhanced traffic flow, reduced accident rates, reduced energy consumption, improved safety, etc. Although the technologies and infrastructure exist to realize such benefits, several issues need to be addressed, particularly cost, security, trust, privacy, performance, and energy efficiency. In this paper, we focus on network performance and energy efficiency.

Computational Intelligence for Energy-Efficient Routing in IoT-Connected Autonomous Vehicle Networks

4.2. Applications in Autonomous Vehicles

Security, trust, privacy, and reliability issues in vehicle-to-everything communications are being properly standardized like 3GPP C-V2X, IEEE 1609.3 DSRC, and 3GPP Xn/X2. As with other applications, including Industry 4.0 and other critical mission scenarios, computational intelligence algorithms can be designed to use appropriate levels of integration and given priority over different services and traffic flows to communicate faster and in a more reliable way. Despite datas will be generally shorter than those that can be handled by other kinds of applications, it is still fundamental to use a proactive network access control approach, instead of detecting and mitigating incidents only as a posterior measure, to promptly address potential data pilferages or system hijacks.

Considering the huge potential of autonomous vehicles in the coming years, many researchers in the field of intelligent transport are aiming at managing the autonomous vehicle networks properly. This can play a key factor in controlling the non-negligible percentages of energy usage by vehicles. Computational intelligence, primarily nature-inspired algorithms, are widely employed in several types of applications for these connected vehicles, ranging from cooperative driving safety, eco-friendly behavior, new-business models with additional car manufacturers or electronic components suppliers, to decision-support systems for collecting, processing, and sharing real-traffic data, allowing the autonomous cars to effectively communicate each other and external traffic managers through wireless technologies. Plenty of vehicles will be also, at least partially, supervised by implantable medical devices to assist people with specific kinds of disabilities, serving as an automated means of transportation.

5. Cybersecurity in Autonomous Vehicles

The decision-making of steering control of the autonomous car based on the incoming environment information, such as the forecasting of other dynamic and static obstacles such as vehicles or pedestrians, determines the driving safety. The attacker launches a time-dependent adversarial controlled input attack on the accelerator or brake signal to perform target deviation of the autonomous vehicle and inherent safety by manipulating the road border. Moreover, many suggestions show that the exact and simple capacity matrix for the eavesdrop construction operation is dangerous and accurate, allowing to extract critical information from the visual road through the non-original pixel-level entrance.

The advanced V2I VANET enables the control center to orchestrate the dynamic traffic light decisions based on the current state of vehicle route requests, which can help reduce emissions

and increase autonomous driving comfort on suburban and urban roads. V2X connectivity can influence factors such as traffic flow reduction, orbital engine combustion, vehicle desegregation, fuel consumption, and pollution formation. However, given the mass reality of these vehicles, significant communication and trust challenges must be considered. Information exchanges in the carrier of the vehicle are also intrinsically unsafe for potential intruders.

To perform increasingly challenging self-adaptive driving, self-driving vehicles must be able to communicate V2V to access and share routes, positions, speeds, and preferences with other vehicles on the road. Such opportunity awareness helps prevent collisions and relieves traffic congestion at the intersection. Effective V2V communication using VANET allows information sharing across the relevant geography to improve the mobility mode, comfort, and safety of autonomous vehicles and can cooperatively maintain the stability of routing through the dynamically capable metric of such V2V links.

However, existing cybersecurity problems can be divided into these two different levels: wired and wireless environment analysis. For example, in the wired level, digital signatures are untraceable, and multi-signatures requiring manageability are recommended. In the wireless level, the secure route is designed to shock spraying and riposte echo routing. Other tools can also sensitize the origin and obstacle enforcement algorithms, resist multiple interference sources, and malware prevention solutions.

Thus, in order to ensure privacy, safety, and security in autonomous vehicles, it is imperative to understand the nature of the cybersecurity threats and then develop multiple levels of intelligent security layers based on computational intelligence. In this chapter, many research works have proposed adaptations of deep learning, anomaly intrusion detection systems, vulnerability assessment tools, and computing intelligence techniques including assembly code, malware code, file-based, and network-based detection methods for autonomous vehicular cybersecurity.

The most representative active attacks on V2X communications are jamming, spamming (using an anti-collision scheme of false danger messages), and eavesdropping. On the other hand, the most representative passive threats aim at gaining unauthorized access to vehicle and infrastructure data, privacy, and data theft, and require stored and transmitted data manipulation and/or modification in the protocols.

The development and deployment of connected and autonomous vehicles introduce new security and privacy threats against all layers of communication, from vehicle to vehicle (V2V), vehicle to infrastructure (V2I), and vehicle to cloud (V2C). Both active and passive threats exist at these three levels, together with vulnerabilities in the system's technologies. These technologies are mainly short-to-medium wireless communications and V2X gateways which can initiate messages to and from the vehicle and the roadside infrastructure and cloud services.

5.1. Threat Landscape

In the vehicle environment, we highlight multiple important attack surfaces. These range from both known and new threats, based on specific Intelligent Transportation System (ITS). We describe the nature of these attack surfaces and how they can be used as an entry to the other (unprotected) networks currently in vehicular and V2X communication. These network attacks, vehicle applications, and general ITS applications using V2V and V2I are well known. The SAE J2735 (2016) standard defines messaging exchanges for traffic and situational awareness. Vehicles can communicate with ISP backhaul systems through cellular communication, such as vehicle cellular units. Adequate assurance and privacy are required to prevent data from being compromised.

When individual vehicles exchange data, the potential for attacks against the vehicle network rises dramatically. For vehicles to transport growing data payloads securely, there is a need for a secure-by-design vehicular communication infrastructure and secure framework when considering new data services and applications. However, to accommodate the concept of enhanced in-vehicle media, streaming content, and infotainment services, autonomous vehicle networks are likely to emerge as a vehicular sensing and communication platform. A prerequisite for autonomous vehicles is communication between cars or between cars and infrastructure. Autonomous vehicle networks generate enormous amounts of data and directly affect the outside world. This data affects the actions of multiple vehicles on the road. These data may be used by entities such as commercial advertising companies to display advertisements. With access to data, it is likely that undesirable behavior may take place, which is incongruent with a portfolio of safe, socially beneficial services and functions to be developed over time for society.

5.2. Best Practices

At this point, they increasingly rely on their own sensing and established historical traffic conditions. IoT data for the transportation networks of the near future might provide vital benefits to society if processed and disseminated in a timely fashion. These benefits include congestion alleviation, pollution reduction, societal safety nets in terms of mobility assistance and crime prevention, emergency response (to both the origins of and the consequences of), sustainable energy use, and a personalized drive or use of mass transit in terms of reduced trip times, reduced costs, and improved safety. The advancement of actions based on time- and space-based traffic data in manageable data dissemination is in our sights. Treating self-driving cars as intelligent agents, we employ computational intelligence to design a communication network (Aurora) for sending and acquiring the right automated vehicle data at the right time to and from the right destination. Crucially, we consider the needs of multiple stakeholders, as well as IoT for measuring pollution levels around the city, providing similar temporal constraints in combination with Q-learning alongside several heuristic algorithms performing relative comparisons from which to base decisions.

Applying computational intelligence in the form of the proposed Q-Learning and metaheuristic algorithms, using diverse datasets in routing and sensing for as many traffic scenarios as possible, would be extremely beneficial. The autonomous vehicles, many of which will soon be connected during driving, represent unique agents in the form of mobile network nodes. Collaboration and cooperation between vehicles will soon be possible and is the focus of this work, to effectively and efficiently route large quantities of time and location-critical data for both private and public needs. The AI will allow these routing networks to respond to new, less predictable travel patterns as they emerge, given new vehicle availability and ownership models. Our proposed routing solutions simultaneously consider traffic data acquisition, actuation, communication, citizen service needs, and urban policy imperatives.

Best practices: These are the recommendations that can help ease the replication or use of this work. These may include general patterns and best practices employed in the mechanism, but also task-specific suggestions and hints on how to optimize different tasks.

6. Human-Centered Training Approaches

The evolution of task-specialized training items employed in artificial intelligence is expected to be constantly made increasingly more user-adapted and human-centered. To aid the development of such artificial intelligence-driven IoT optimization infrastructures that can be

both flexible and user-friendly, in this section we focus on the discussion of non-typical use cases of chatbot technology as a popular online personal assistance tool: we report activities carried out for generating and cultivating human expertise on a relevant case study via a chatbot. In particular, the present article is expected to open in better detail the hidden layers of the engineering of chatbot-based online knowledge-based technology inference systems and to contribute to the improvement of any existing agent technology by discussing knowledge engineering challenges and issues of the particular approach deployed.

The realization of an efficient communication between vehicles and devices in the evolving connected and autonomous vehicle world does have some immediate technological, scientific, and practical commercial and social value, with various sectors proposing IoT networks of different scale deployments with various task profiles in very near timeframes. Therefore, the problem of designing and understanding the leading principles that could be used to engineer the future IoT-assisted autonomous vehicle architectures are not only exciting but also of immense practical relevance, and continue to stimulate intense research activities for the last decade, across experts of multiple disciplines. Due to conflicting design challenges, the development of such architectures requires a flexible approach in favor of the designing for and appealing directly to human expertise and knowledge. That is, a new urban driver needs to be trained in a novel way for those autonomous vehicles which will become her or his physical reality.

6.1. Importance in Cybersecurity Education

For example, remote code triggers, previously prepared code updates, wireless injections, interruptions, denial of service (DoS), and software errors can cause accidents, whereas unauthorized exchange losses and wiretapping for cars or motorbikes or their team can lead to stolen credentials, credential theft, identity theft, eavesdropping, monitoring, espionage, traffic theft, ransom data and privilege escalation. Fortunately, several simulation tools tailored to cybersecurity challenges cover many of the known cybersecurity risks to the proposed vehicle network and the underlying network infrastructure. These teaching tools include attacks inspired by hacking into ZigBee networks to extend the XML Web Services security model, using XML as an attack vector combination, developing an SDL and RBC-based security assessment methodology, and implementing systems that prevent cyber attacks.

Compromising IoT devices connected to autonomous vehicles can be dangerous, particularly when real-time gigabit data speeds that inform sensor data mapping or classify and refine detected objects are exchanged over air prior to decision-making. Such wireless data exchange presents opportunities for bad actors who can cause accidents, steal credentials, or ransom the vehicle. Once compromised, autonomous vehicles can be weaponized, used to spy on others or conduct espionage, used in large-scale distributed attacks for a nation-state, sell the vehicle and occupants for embarrassment reasons, threat-related vehicle behavioral modification and crash execution, or be misused for piracy. The potential negative impact is wide-ranging and affects various entities of an IoT-connected autonomous vehicle network. Autonomous vehicles connected to the network are associated with students and administrators, who are responsible for the safe development, use, and maintenance of the vehicle. They are directly or indirectly affected if data are sensitive, semi-sensitive, or confidential and include the following types: personal, proprietary, compliance, safety, government, military, and other national security. Data exchanges are also sensitive external factors of the attacks.

6.2. Design Principles

In exemplification of specific design efforts, this paper provides sensor aggregation and sensor resource allocation to meet the very high energy-efficiency targets linked to solutions for selected EDRVN sensor network challenges considered and draw on as-is available, studies from related scientific literature. For simulating an external communications device that can be turned off during vehicle function as detailed above, sensor data is forwarded from the independence sensor models for the different vehicle's computer-based control functions to the sensor and self-sensor ECU for a comprehensive model of such an ECU.

Energy efficiency impact via sensor hardware

To achieve sustainable energy efficiency, computations need to employ forward-looking resource management. Predictable vehicle navigation tasks are handed to special hardware accelerators if feasible at all, which may interact with and influence system-wide scheduling decisions. The use of surge computing mode directly impacts the rate of rising energy consumption while dealing with hot traffic situations, in particular in high energy-consuming computation scenarios involving specialized hardware, which may require additional cooling mechanisms.

The inherently distributed nature of the use case of IVN suggests implementation of many if not all sensing, processing, and actuating tasks must happen on the actual device. However, in particular significantly reducing processed data volume via preprocessing helps limiting energy requirements. Accurate function specifications allow for much more precise decisions about what processing indeed is required. Since energy availability heavily depends on runtime system state, any scheduling, allocation and configuration parameter must relate energy implications and influence in a fashion measurable at runtime.

The domain-specific challenges in autonomous vehicle networks imply both device hardware and software must cope with specific constraints like strict real-time requirements, and in particular, challenging ambient conditions. Hence, designers need to implement measures for energy-efficient processing at runtime based on comprehensive domain knowledge and not general maturity of design parameters.

7. Case Studies and Experiments

In this section, we list three important use cases that call for the proposed optimization by the joint design of two critical layers of a V2V IVC-enabled cellular network for the crucial benefit of EVs interconnected to the cloud layer. It is important to point out that all EVs could transform into a cloud layer; thus, the benefits of this considered issue are not restricted to EVs. Indeed, any profile uploading process would benefit. In practice, we may simply have homes, parking spots, public places, and so on. We would like to analyze the potential benefits of the proposed mathematical contributions to experimentally demonstrate and quantify the potential gains. This important question is not only novel, but also critical and challenging.

In the following, we list four case studies and their experimental setups, respectively. On the basis of these experiments, we provide detailed numerical analysis in order to demonstrate the advantages offered by the proposed bio-inspired intelligence. Furthermore, we provide the main observations accompanied by detailed numerical results, which confirm the claim that, in IoT-connected AV networks, V2V IVC deployments can greatly benefit from the proposed contributions. The use cases and the numerical results presented are important because the issue of cross-layer optimization algorithm in the context of IoT-connected AV networks has never been systematically and thoroughly studied before.

7.1. Simulation Setup

A routing algorithm's main task is to determine the optimal path for data to reach from the source to the destination. By considering the vehicular communication network operating in the highway scenario, the aim here is to propose a novel energy-efficient routing algorithm to prolong active lifetime by considering three important attributes, such as rectilinear (easier to implement), distance with minimal hops, and energy consumption. In this, using vehicles as relay agents is adopted over fixed infrastructures to transfer data among them. An ad hoc on-demand distance vector routing protocol is suggested in the IoT network context for intelligent communication among the moving vehicles. Here, the main challenge is the limited movement range for an autonomous vehicle. Moreover, the engine ignition and moving periods bring sporadic network scenarios. Because of these attributes, automobiles quickly deplete their stored electric energy (batteries).

7.2. Results and Analysis

From the graphic depicted in Figure 8a, it can be observed that the CI-RE-RT outperforms the RE-RT solutions by 4.9 times in terms of the average convergence time. Over the 50 instances, the average convergence time for CI-RT was 7237s while the worst-case convergence took place after 20480s. On the other hand, the RE-RT solutions' average convergence time was 35564s while the worst case occurred only after 20480s. The initial solution of the RE-RT technique, on the other hand, was numerically better once the global error might be better decreased due to the combined solving of the proposed energy-expensive objective with the energy-conservative ones.

The comparison was made for the adopted CI-based cloud, fog, and mobile energy-expensive workflow solutions, with similar counterpart energy-conservative techniques that did not consider the IoT-connected autonomous vehicles networks, except in the M-DeNB case. Given that MEC may be combined with all other solutions, especially with cloud-based ones once the cloud processing capabilities could be limited when compared with the MEC. The RE best EE cloud-based solution was labeled as CI-RE-RT, the bio-inspired COA-ACK. Regressed-based solution was named BR.

8. Conclusion and Future Directions

Next, we present an integrative reference architecture, which characterizes the integration of conventional vehicular networks and the future Internet of vehicles through the realization of

in-vehicle IoT connectivity. The introduced concepts are based on multimodal sensors, multi-interface capabilities, reinstated drive-thru Wi-Fi, and high-performance IoT-capable computational engines within the vehicle. Afterward, we present typically considered IoT use cases in the context of modern connected autonomous vehicle scenarios and emphasize various technical considerations and societal expectations adopted therein. Then, we discuss a machine-learning-based IoT computational offloading opportunity leveraging-based prototype in a connected autonomous vehicle context and demonstrate efficacy in terms of power conservation. It reveals that highly intelligent interdependence among involved entities maximizes connectivity, thus allowing vehicular network infostations and surrounding IoT infrastructure to improve connected vehicle-related services.

In this chapter, we first gave an overview of emerging trends in IoT and energy-efficient computational intelligence paradigms for autonomous vehicular networks. Both the vehicular network and the IoT have become integral parts of modern IoT-era applications. With the integration of vehicular networks with the IoT, a plethora of applications becomes enabled, such as road traffic analysis, smart intersections, in-car infotainment, onboard healthcare, fuel-efficient routes, hit-and-run alerts, stolen car recovery, and so on. Although full-fledged usage clusters witness the immediate benefits of such a combination, the realization of its potential also needs extensive placement of it on board of the IoT-connected autonomous vehicle networks. In response, it leads to computation offloading selection issues, the remote server selection problems, as well as the identification of potential proximity clusters that are likely to have IoT service offload opportunities.

8.1. Summary of Findings

In this respect, this chapter utilizes BSN/WSN-connected IoT for the discovery of supervised and unsupervised algorithms creating Energy-Efficient Routing (EER) matrix modules. It is demonstrated that the EER obtained leads to efficient real-time communication systems with long life of AV networks for different driving scenarios. A connected vehicle scenario is utilized using six different vehicular densities. Results confer that Hopfield Neural Network-based Energy-Efficient Routing improves energy savings of the wireless network with a small increase in latency, so as to allow efficient real-time communication for a variety of driving scenarios while enhancing the life of the vehicle. Furthermore, the enhanced ability of HNN-based routing is sustained with increasing density of vehicles being able to communicate with

one another. Minimal energy consumption network module routing improves with time, which also decreases the latency on the routes.

This chapter is motivated by the objective of achieving energy and time-efficient routing for autonomous vehicle (AV) networks connected via the Internet of Things (IoT). AVs are playing an increasingly important role in passenger safety and mobility. A significant constraint on the increasing capabilities of AV is the level of available energy in an AV. As a result, the ability of the AV to exchange useful information with other AVs and fixed road infrastructure while on its journey is highly attractive. However, the problem of communicating such information when connectivity is available due to energy constraints has not been extensively researched. The major contributions of this chapter, supported by simulation results and comparison, are that Hopfield Neural Networks (HNNs) can be efficiently trained such that their form is suitable for the smart routing of autonomous vehicles, and that such connectivity in AV networks can be self-adapting.

8.2. Potential Research Directions

Still, autonomous vehicle technology itself provides more potential research opportunities stemming from the complex and growing field of AI. Autonomous vehicles have exceptional challenges that can only be adequately addressed at the level of the autonomous decision, which must be carried out in a fraction of a second, and that must manage decision-making under environmental constraints, regulation constraints, and safety requirements, estimating possible interactions that might happen and planning for several futures. They also have limitations, especially related to their limited field of vision, the multithreading of different tasks and different levels of information (both spatial and temporal), and their scarce compute resources. The merging of different AI techniques at different abstraction levels, such as functional modules and inference levels, is a context that offers excellent opportunities for research on suitable hybrid AI, capable of providing the autonomous decision with tools for performance monitoring (error detection and possible recovery from errors) and runtime evaluation of AI execution and decision-making.

Another potential area is the investigation of energy-efficient routing in autonomous vehicle networks. In this context, vehicles play multiple roles—namely, data consumers (driving the vehicle), data producers (smart sensing solutions), and data carriers for the data generated by IoT peripheral devices in the vehicle's environment. The vehicle's environment is populated

with IoT devices that derive from the future of complex urban transportation. The research problem involves dynamics because vehicles perform duties for different connected applications such as traffic safety communication, traffic efficiency, social networking, infotainment, and commerce. These vehicles provide services using efficient computation, data handling, and communication. The service deployment to support many IoT applications should be adaptive, efficient, and secure at all times. Another research challenge is the autonomic control of IoT devices and the decision support to allocate tasks to vehicles on the road.

9. References

1. Z. Li, Q. Sun, H. Zhang, and L. Zhao, "Energy-efficient routing in vehicular ad hoc networks using multi-objective particle swarm optimization," *IEEE Access*, vol. 7, pp. 102681-102694, 2019.

2. S. K. Gupta, P. S. Karthik, and M. S. Obaidat, "A novel energy-efficient approach for routing in IoT based autonomous vehicular networks using particle swarm optimization," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 8, pp. 3006-3015, Aug. 2019.

3. Tatineni, Sumanth. "Exploring the Challenges and Prospects in Data Science and Information Professions." *International Journal of Management (IJM)* 12.2 (2021): 1009-1014.

4. Vemori, Vamsi. "Human-in-the-Loop Moral Decision-Making Frameworks for Situationally Aware Multi-Modal Autonomous Vehicle Networks: An Accessibility-Focused Approach." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 54-87.

5. Shaik, Mahammad, Srinivasan Venkataramanan, and Ashok Kumar Reddy Sadhu. "Fortifying the Expanding Internet of Things Landscape: A Zero Trust Network Architecture Approach for Enhanced Security and Mitigating Resource Constraints." *Journal of Science & Technology* 1.1 (2020): 170-192.

6. Tatineni, Sumanth. "Climate Change Modeling and Analysis: Leveraging Big Data for Environmental Sustainability." *International Journal of Computer Engineering and Technology* 11.1 (2020).

7. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.

8. H. Zhu, L. Zhang, and Y. Li, "Energy-efficient routing in IoT-enabled vehicular networks using deep reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 6518-6529, July 2021.

9. X. Zhang, W. Li, and Q. Tang, "Energy-efficient routing protocol based on ant colony optimization in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 6, pp. 2353-2364, June 2020.

10. J. Tang, G. Li, and C. Chen, "A deep Q-learning approach for energy-efficient routing in IoT networks," *IEEE Access*, vol. 8, pp. 195854-195864, 2020.

11. F. Yang, T. Zhang, and W. Zhao, "Energy-efficient routing based on swarm intelligence in IoT networks," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3331-3341, Mar. 2021.

12. S. K. Shah, A. A. Khan, and F. Akhtar, "Optimization-based energy-efficient routing in vehicular networks using particle swarm optimization," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 4, pp. 1556-1565, Apr. 2020.

13. L. He, Y. Guo, and M. Wang, "Energy-efficient routing in IoT-enabled vehicular networks using deep learning," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2332-2343, Mar. 2021.

14. Y. Liu, X. Liu, and H. Zhu, "Energy-efficient routing protocol for IoT-based vehicular ad hoc networks using fuzzy logic," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 3, pp. 982-992, Sep. 2020.

15. S. Singh, P. Gupta, and M. K. Ghose, "Energy-efficient routing in IoT-enabled vehicular networks using machine learning," *IEEE Transactions on Intelligent Vehicles*, vol. 6, no. 2, pp. 233-244, June 2021.

16. T. Zhao, J. Cao, and S. Liu, "A novel energy-efficient routing protocol for IoT networks using artificial neural networks," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2156-2167, Mar. 2020.

17. Q. Xu, Y. Zhu, and H. Wang, "Energy-efficient routing in vehicular networks using deep reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4364-4374, Apr. 2020.

18. K. Wang, J. Zhao, and L. Wang, "A bio-inspired energy-efficient routing protocol for IoT-enabled vehicular networks," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 1, pp. 123-133, Mar. 2021.

19. X. Liu, Y. Wang, and Z. Zhou, "Energy-efficient routing in IoT networks using genetic algorithms," *IEEE Access*, vol. 7, pp. 135778-135790, 2019.

20. W. Chen, M. Li, and Y. Liu, "Energy-efficient routing protocol for vehicular ad hoc networks using swarm intelligence," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 2, pp. 872-882, Feb. 2021.

21. Z. Wang, H. Wang, and W. Liu, "Energy-efficient data collection and routing protocol for IoT-based vehicular networks," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4786-4797, June 2021.