Computational Intelligence for Predictive Analytics in IoT-connected Autonomous Vehicle Networks

By Dr. François Garnier

Professor of Geomatics Engineering, Université de Montréal, Canada

1. Introduction to Computational Intelligence and Predictive Analytics

The fleet of vehicles on our roads is expected to incorporate more and more smart and emphasized capabilities. Road accidents are a significant societal problem leading to the loss of human lives, pain, wealth loss, harm, and financial liabilities. Their vehicles should be independent, open-curious, tolerant, and successful and respect traffic regulations. They can recognize their driving capabilities and quickly suspend and restart them. In traffic, the vehicles must have 'social abilities' and collaborate together and with traffic challenges. Smart energies and energy-effective vehicles are demanded by regulations. Consumers gain added benefits with new automotive user interfaces, multimedia, and infotainment activities like business models, documentation of legitimate evidence, etc. To satisfy these demands, sensors together with dynamic processing on board are sharp, including the real sense by artificial perception, forecast, and normal action control loop, the Architectural Perception instance. The current situation is a prototype. The predictive study within the automotive environment on the future event is most of them. It applies interdisciplinary techniques from data mining, data science, complexity theory, control systems, engineering, software engineering, quality risk management, verification and validation, human-computer interaction, safety, dependability, security, and ethics. Pedestrian-vehicle incident and external road system environmental understanding events are difficult. For instance, while driving at a fast pace in very close proximity to different users, they pose unique challenges in terms of, e.g., dynamic vehicle control. Medical networking and smartness will analyze essential vehicle data, search for suitable behavioral action, and apply the methods. Large datasets derived from automotive AI operate together to predict the events. To take alternatives, the car interface has to properly communicate that they are able to execute efficiently. Frameworks can plan good control oxidations. Diving and accelerative actions and can also accomplish reasons and constraints. To determine essential data to the Vehicle System Control, create this issue. Auto engineers also profit from the quality of analysis and reporting to achieve the assessment of the latest prototype movements enforcing specialized use for these special instances with safety standards.

Computational intelligence involves studying and developing the ability of machines, artificial agents, and robots to act in a way that is flexible, autonomous, and adaptive. Computational intelligence can be examined by studying learning, adaptation, perception, action, and cognition, as well as by examining neurological processes and the development of intelligent organisms. It can be considered as a broad discipline that includes neural networks, fuzzy logic, and evolutionary methods. Since the inception of computational intelligence, its theoretical and practical benefits and applications with real-world problems have become increasingly popular. Among the real-world problems is the nature of predictive analytics in massive IoT-connected autonomous vehicle data due to an explosive growth in the automotive-infotainment system and multimedia service market.

2. IoT-connected Autonomous Vehicle Networks: Overview and Challenges

The objective of improving vehicular road safety for connected and automated driving has been the impetus for significant advances in the development of cooperative Intelligent Transport Systems (C-ITS) applications empowered with machine learning and advanced communication systems. There is a proliferation of published papers describing C-ITS over both LTE-V2X and DSRC technologies, which illustrate the current difficulties relating to C-ITS deployment. In a review of the interconnection scenario in C-ITS applications, it was found that LTE, DSRC, ad-hoc WiFi, and Ethernet technologies are the most successful options currently being used.

The IoT was envisioned by connecting objects embedded with sensors to Internet Protocol (IP) networks in order to ubiquitously monitor and manage objects in real-time, thereby providing new business opportunities and enhanced quality of life. The approaching era of intelligent autonomous vehicle networks empowered by revolutionary IIoT technologies is characterized by autonomous driving on cloud roadway infrastructure (IoCT), vehicle-to-anything (V2X) communications protocols, self-detecting sensor nodes, data-fog-cloud-big-data analytics lifecycle, and distributed edge and cloud computing infrastructure. Future AVNs will support intelligent driving, advanced healthcare information systems through in-vehicle biometric monitoring, and new business models providing mobility services to autonomous vehicles, drones, and mobile robots.

3. Ethical Considerations in IoT Sensor Deployment for Autonomous Vehicle Monitoring

We model different non-technical adverse effects of sensor deployments as impacted interests. Once these adverse effects of sensor deployments are identified, there is a need to predict which of these adverse effects may result when a cluster of different sensors with different characteristics are combined in the same network. Such predictive analytics involves different types of probabilistic models and other advanced methodologies, none of which is sufficiently accurate to be selected at the time of writing of this paper. In the absence of a method that can reliably calculate the benefits versus the harm, sensor combinations need to be predominantly regulated by the precautionary principle. Such exclusive use of the precautionary principle becomes infeasible, manageable only if the sensor networks are at different trust levels. If architectural and other technical countermeasures would keep the harm within threshold levels, the trust models that classify networks in different trust levels would have legal consequences such as the appropriate level of insurance and necessity of informed consent for data collection purposes.

Recent research on the ethical aspects of sensor deployment for connected autonomous vehicles becomes even more acute due to the associated consequences of threat-related scenarios that involve life-sustaining interests. The autonomous vehicle networking community has an opportunity to innovate in the definition of best practices. It also needs to be aligned with privacy and data protection principles at a technological level, which become complex due to a large number of connected devices that their IoT platforms are designed to support. Our focus is on the ethical aspects related to predictive analytics in IoT-connected fleets of autonomous vehicles. We consider more elementary unethical issues in order to provide better insight that can guide future human rights advocacy as well as support effective whistleblower protection in the industry. These insights are important because unethical behavior can often be foreseeable in predictive analytics due to severe technological limitations that interfere through statistical bias, limited accountabilities in AI usage, and the low interpretability of the phenomena that the technology is constructed to understand.

4. Computational Intelligence Techniques for Predictive Analytics in IoT-connected Networks

In computational intelligence and predictive analytics research areas, some advanced captures by different Bus Rapid Transit (BRT) systems, taxis, and the video-cameras could provide traffic data of different quality with different spatial and time resolutions. Many computational intelligence techniques, including classical regression, time series, probability theory, as well as neural networks, fuzzy logic, rough sets, evolutionary algorithms, swarm intelligence, artificial life, artificial immune system and soft computing, statistics, and time series must be explored and proposed with sophisticated hierarchies and deep-learning models with complex architectures in both computer science and transportation domain. With the rapid development of spatiotemporal data science and related applications, various computation and communication tasks in the intelligent transportation systems can be effectively executed in the integrated IoT cyber-physical network, and a broad range of data mining activities are developed to support various types of transportation prediction and early actions.

The prediction algorithm for transportation reliability in IoT-connected vehicle networks must employ advanced computational intelligence techniques that can accurately handle the complex spatial and temporal data as well as tackle significant traffic variations. In the big data era, large volumes of dynamic transportation and traffic flows are continuously produced, captured, and managed. Assisted with the embedded computational intelligence algorithms, the prediction model must have the capacity for massive big transportation data processing which could be more convenient, efficient and real-time for the IoT-connected vehicle application. The real-time transportation prediction via smart IoT system can provide accurate and timely information for intelligent transportation services (ITS) and make great profit in lowering transportation operation cost, reducing travel time and improving route selection of users, and enhancing transportation system efficiency and environmental sustainability of each trip in the connected transportation systems, especially in the spatiotemporal, on-demand and real-time transportation access network for autonomous vehicles.

4. Computational intelligence techniques for predictive analytics in IoT-connected vehicle networks

5. Case Studies and Applications in Autonomous Vehicle Monitoring

This chapter presents how autonomous vehicles can benefit artificially intelligent algorithms to scale different dimensions with several metric contexts to perform completely or partially perceptual, cognitive, or physical V2X series-communications in our new urban context. Protecting the user's privacy, tire health monitoring, and updating behavioral rules for autonomous driving algorithms are a salient prerequisite to simulate intelligent decision-making. AVs self-driving prototypes have clocked millions of miles on our roads, experiencing various and new types of complex traffic, threatening to further speed complex when operating in a realistic urban driving environment. With these advanced capabilities, there is a threat to the user's privacy. As intelligent vehicles get equipped with more and more sensors, which continuously record information, we can easily forecast possible solutions only if we properly map the various traffic events.

This section looks at the various case studies related to the running of autonomous vehicles and how they have helped improve autonomous vehicle technologies. It innovatively presents various strategies adopted to monitor the manifold autonomous vehicle operations. In order to address the major challenges in the autonomous operations, diverse methods, proposed by researchers, are discussed thoroughly in different scenarios. For safety reasons, the case studies discuss the use of vehicle-to-infrastructure and vehicle-to-vehicle communications, monitoring vehicle health and safety status, fatigue detection, emotion detection, intrusion detection, systems for smart cities. The development of many systems in real-time along with V2I and V2V communication networks has led to considerable extraction of information from smart city infrastructures.

6. Future Trends and Research Directions in Computational Intelligence for IoT-connected Autonomous Vehicles

With regard to connected vehicles being IoT-enabled, there are 3 V's characteristics of big data: high volume, velocity, and variety. Large amounts of high-frequency and high-dimension data need to be processed within strict time limits for prolonged durations under a range of real-world conditions. With such data and system characteristics, one possible direction for future research is with regard to novel prediction and decision-making methods that aim to ensure that with frequent data extractions over time, there is no performance degradation with an inherent throw and re-calibrate attitude within autonomous vehicle ecosystems in re-training prediction or decision-making tools.

First and foremost, one might be related to data protection standards and frameworks. In every computation-intensive scenario, especially the ones involving data-driven models and prediction algorithms, raw data is the most precious input. This might be considered of obscene value in the realm of autonomous vehicles as it can be necessary for creating digital twins and testing autonomous vehicles. This kind of digital twins is crucial not only in real-life connected vehicle scenarios but also in predictive analytics utilizing artificial takes of the future.

This special issue aims to address a number of conceptual and technical challenges that are delaying the full realization of this new computational intelligence paradigm in big connected vehicle data. However, there are eight main research directions where the wider community may consider devoting their attention in the future.

The exponential increase in the number of IoT-connected autonomous vehicles is likely to result in an unprecedented volume of vehicular big data. Big Data Analytics, especially Predictive Analytics, when coupled with modeling, simulation, and emulation in a sophisticated Cyber-Physical Framework, becomes essential to extract important patterns and insights from these connected vehicle data. Before realizing the full potential of Predictive Analytics in this emerging ecosystem, a number of intrinsic and extrinsic challenges need to be addressed.

7. Conclusion and Recommendations

These insights are quite useful in formulating the standards, making policy, and regulations given that such insights are quite decisive when fault detection, optimization, and preventive actions are to be initiated at electronic, mechanical sensor actuator levels. The IoT-AVN systems generate data, forecast, detect, and provide preventive insights using CI models. The data sources in IoT-AVN systems are complex and ingest both streaming and non-streaming type of data and are exogenous. In this regard, the exponential growth in data must be reduced as it produces noise and makes insight discoveries difficult. In this chapter, we reviewed and shed light on why we should continue working on these insights to predict failures and optimize IoT-AVN.

This chapter comprehensively reviewed the state of computational intelligence (CI) for predictive analytics, big data, and machine learning with potential applications in IoT-connected Autonomous Vehicle Networks (IoT-AVN). The primary objective and novelty were to propose a data-driven intelligent predictive and preventive system using data mining and big data for CI's fault detection and predictive insights using machine learning and deep learning in IoT-AVN.

8. References

1. C. Liu, F. Wu, and H. Hu, "A survey of data mining techniques for malware detection using static features," in Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 1817-1824.

2. 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.

3. 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.

4. K. J. M. Moran, R. Byres, and E. Von Solms, "The three faces of IoT security," in Computers & Security, vol. 69, pp. 35-51, 2017.

5. Tatineni, Sumanth. "Federated Learning for Privacy-Preserving Data Analysis: Applications and Challenges." *International Journal of Computer Engineering and Technology* 9.6 (2018).

6. M. M. Hassan, E. Hossain, M. M. A. Hashem, M. A. Almogren, and A. G. Yaqoob, "Network traffic classification in Internet of Things (IoT) based on deep learning approach," in Future Generation Computer Systems, vol. 82, pp. 315-323, 2018.

7. Tatineni, Sumanth. "Ethical Considerations in AI and Data Science: Bias, Fairness, and Accountability." *International Journal of Information Technology and Management Information Systems (IJITMIS)* 10.1 (2019): 11-21.

8. Vemori, Vamsi. "Towards a Driverless Future: A Multi-Pronged Approach to Enabling Widespread Adoption of Autonomous Vehicles-Infrastructure Development, Regulatory Frameworks, and Public Acceptance Strategies." *Blockchain Technology and Distributed Systems* 2.2 (2022): 35-59.

9. Tatineni, Sumanth. "Blockchain and Data Science Integration for Secure and Transparent Data Sharing." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.3 (2019): 470-480.

10. R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," in Future Generation Computer Systems, vol. 78, pp. 680-698, 2018.

11. S. Chauhan and B. Choudhury, "Security issues in cloud computing: A comprehensive study," in International Journal of Computer Applications, vol. 47, no. 10, pp. 1-6, 2012.

12. Tatineni, Sumanth. "Recommendation Systems for Personalized Learning: A Data-Driven Approach in Education." *Journal of Computer Engineering and Technology (JCET)* 4.2 (2020).

13. J. P. Anderson, "Computer security threat monitoring and surveillance," in Technical Report, James P Anderson Co., Fort Washington, PA, USA, 1980.

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

15. K. D. Bowers, "The need for a strategic approach to cloud computing," in Computer, vol. 44, no. 3, pp. 22-24, 2011.

16. S. E. I. Group, "Security in the Internet of Things," in Technical Report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, 2016.

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

18. T. Duc, P. Jun, and P. Hoon, "Secure data communication in IoT applications using software-defined networking," in Wireless Communications and Mobile Computing, vol. 2018, Article ID 8713834, 12 pages, 2018.

19. Tatineni, Sumanth. "INTEGRATING AI, BLOCKCHAIN AND CLOUD TECHNOLOGIES FOR DATA MANAGEMENT IN HEALTHCARE." *Journal of Computer Engineering and Technology (JCET)* 5.01 (2022).

20. K. M. Dantu, S. K. Garg, and M. K. Gupta, "Security issues in healthcare applications using wireless medical sensor networks: A survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 55-67, 2014.