THE EVOLUTION OF VANET NETWORKS: A REVIEW OF EMERGING TRENDS IN ARTIFICIAL INTELLIGENCE AND SOFTWARE-DEFINED NETWORKS

Lewys Correa Sánchezl[1], Octavio José Salcedo Parra[1] and Miguel J. Espitia R.[2]

[1]Falcutad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia
[2]Facultad de Ciencias Matemáticas y Naturales, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia

ABSTRACT

The use of vehicular ad hoc networks (Vanet) has become increasingly important in today's world due to their ability to enhance driving safety and vehicular traffic efficiency. This article will discuss artificial intelligence techniques used in Vanet, including machine learning, deep learning, and swarm intelligence techniques. Furthermore, we will examine the routing challenges within Vanet, including issues like communication link disruptions, obstacles, and varying vehicle speeds. Lastly, we will explore the implementation of software-defined networks (SDN) in Vanet, encompassing SDN protocols and architectures.

KEYWORDS

Vehicular communications, routing, artificial intelligence, software-defined networks & Vanet.

1. INTRODUCTION

Vehicular ad hoc networks (Vanet) have become an emerging and promising technology to improve safety and efficiency in road transport. Vanet networks are based on wireless communication between vehicles and/or between vehicles and road infrastructure, enabling a wide range of applications such as accident prevention, traffic management, and route optimization as shown in Figure 1. However, the use of Vanet also poses significant technical challenges, such as communication link disruption, selection of message forwarding nodes, and vehicle speed, among others.

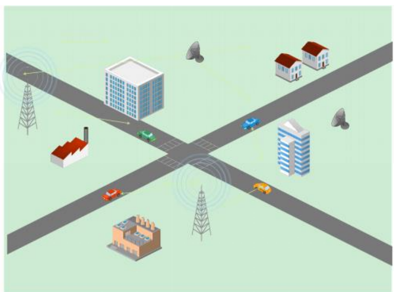

Figure 1. Vanet Network Source: Authors.

David C. Wyld et al. (Eds): IoTE, CNDC, ACITY, DPPR, AIAA, NLPTA, WEST, ICSS -2023
pp. 209-219, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.132216

This article aims to provide an overview of the artificial intelligence techniques used in Vanet, including machine learning, deep learning, and swarm intelligence techniques. In addition, the challenges of routing in Vanet will be discussed and software-defined networks (SDN) will be presented as a solution to address these challenges. SDN protocols, SDN controllers, and SDN architectures will be described, analyzing the advantages and disadvantages of their application in Vanet.

For the preparation of this article, a systematic review of literature was conducted on various databases, including IEEE Explore, Science Direct, and Scopus. The following search equations were used: (Vanet OR "vehicular ad-hoc network") AND ("intelligent transportation systems" OR ITS) AND routing, Vanet AND ("artificial intelligence techniques" OR "AI techniques"), Vanet AND ("machine learning techniques" OR "ML techniques"), Vanet AND ("deep learning techniques" OR "DL techniques"), Vanet AND ("swarm intelligence techniques" OR "SI techniques") and Vanet AND ("Software-defined networking" OR "SDN") to identify relevant articles. Studies that met inclusion criteria, such as relevance to the research topic and quality of content, were carefully selected. From the literature review, the main technical challenges and proposed solutions in the field of Vanet were identified, with a particular focus on the application of artificial intelligence techniques and software-defined networks.

2. ROUTING IN VEHICULAR AD HOC NETWORKS (VANET)

Routing is one of the challenges in Vanet, as vehicles move quickly and the network topology is constantly changing. The objective of routing is to send a message from the source to the destination through a suitable path in the network. However, in Vanet, messages can be interrupted due to lack of connectivity because of obstacles such as houses, buildings, or trees, or even due to the speed of vehicles. Furthermore, selecting the appropriate nodes to forward the messages is critical as some vehicles might have better connectivity than others.

Therefore, to address these routing challenges in Vanet, various routing techniques and protocols have been proposed. In [1], reliable routing protocols, like the improved genetic algorithm and lion optimization routing protocol, are suggested for selecting the best and optimal route. These routing protocols consider the movement and direction of vehicles, access points, and mobility, making them more efficient and reliable compared to traditional routing protocols. And in [2], traffic congestion is addressed and a cooperative and distributed information exchange mechanism is proposed to minimize communication redundancy and control the communication cost in Vanet. This method uses the travel time information measured by the vehicles and is sent through multi-hop communications to calculate the shortest routes. While in [3], the importance of security in the routing layer in IoT networks, including Vanet networks, is discussed. Different solutions for secure routing in IoT networks have been proposed, such as cryptography-based methods and trust-based mechanisms. Moreover, the reliability analysis of nodes is important to select reliable nodes for data transmission and deal with untrustworthy vehicles in Vanet.

Besides the aforementioned routing techniques and protocols, in [4], the challenges in disseminating warning messages in Vanet are specifically addressed. The authors propose a Traffic Warning Message Dissemination System (TWMDS) based on Vanet using a Reverse Routing Protocol (RRP). The RRP restricts the diffusion range of messages, specifies forwarding and receiving nodes, and reduces unnecessary communication overhead.

2.1. Communication Link Interruption

The communication link is a critical factor in Vanet, and its interruption can have a significant impact on the efficiency and safety of the network. The decentralized detection scheme proposed in [5] is an effective way to ensure the link quality, vehicle mobility, and behaviors, while the comprehensive resource in [6] thoroughly addresses security concerns in Vanet and offers practical solutions, such as authentication schemes and artificial intelligence techniques. In general, these studies are valuable resources to ensure the reliability and safety of Vanets.

The mentioned studies emphasize the importance of reliable communication in Vanet and propose solutions to address issues such as selfish nodes and malicious attacks.

2.2. Obstacles

The importance of reliable communication in vehicular networks and the potential problems arising from communication link interruption are addressed. Various studies presenting different solutions to improve network performance and minimize driving risks due to obstacles are included.

In [7], a collision prediction system for Vanet called QCP-SD is proposed, which uses a flexible Q-learning algorithm and aids in the dissemination of safety messages through the cloud. QCP-SD considers various factors to predict collision risk and is designed to predict vehicular accidents with high accuracy and disseminate safety messages timely to endangered drivers. On the other hand, in [8], the OPBRP routing protocol for Vanet is presented, which uses mobility prediction to avoid radio obstacles and enhance packet delivery reliability. The protocol employs predictive greedy forwarding and perimeter strategies to improve performance and reduce energy consumption. Simulation tests show that OPBRP outperforms other routing protocols in terms of PDR and E2E delay.

2.3. Message Forwarding Node Selection

In [9], a Q-learning and fuzzy logic-based hierarchical routing algorithm (QFHR) is presented that uses reinforcement learning techniques and fuzzy logic to find the most suitable route among different intersections in the network. This paper also presents a reinforcement learning-based routing protocol for clustered EV-Vanet. The results show that QFHR outperforms other approaches in terms of packet delivery rate, end-to-end delay, hop count, and routing overhead. While in [10], a multi-path route switching protocol for intelligent transportation systems is proposed that utilizes the Wiedemann car-following model. The protocol predicts future connectivity of multiple routes and dynamically switches between them based on the requested quality of service and the adopted switching criterion. The proposed LDD-based route switching protocol outperforms other criteria in ensuring packet delivery rate and average total end-to-end delay of packets. Moreover, this paper discusses the efficiency of position-based routing protocols for safety applications and the need for traffic prediction systems.

Both works present innovative solutions to improve the efficiency of vehicular ad hoc networks and intelligent transportation systems. They also provide a rigorous evaluation of their performance and discuss the strengths and weaknesses of related works in the field of fuzzy routing and multi-path route switching protocols.

2.4. Vehicle Speed

In [11], an overview of research on reliable routing protocols for Vanet is provided, evaluating the performance of topology-based routing protocols in high-density dynamic systems of vehicles. Researchers conclude that DSR and AODV are the most efficient routing protocols for Vanet and suggest further research to ensure location privacy and explore other routing protocols with more performance metrics.

On the other hand, in [12], the Internet of Vehicles (IoV) is discussed and its potential to reduce traffic congestion and improve traffic flow through real-time communication between vehicles and other devices. The paper also highlights the importance of security and privacy in the IoV network and the potential use of artificial intelligence and machine learning.
In summary, these two papers offer an overview of reliable routing protocols for Vanet and of the IoV and their potential applications in the field of Vanets.

3. Artificial Intelligence Techniques in Vanet: a Machine Learning, Deep Learning, and Swarm Intelligence Approach

Vanets have sparked great interest in recent years due to their potential to improve traffic safety and the performance of communications between vehicles and between vehicles and infrastructures. However, due to the dynamic nature of Vanets, effective congestion control protocols are essential to ensure reliable and efficient data transmission.

In this context, one of the most promising techniques to improve the performance of congestion control protocols in Vanet is artificial intelligence. In [13], the Adaptive Congestion-aware Routing Protocol (ACARP) was introduced, which uses artificial intelligence to detect congestion and establish safe routes for data transmission. The work also presents an evaluation of the performance of ACARP in comparison to other congestion control protocols in Vanet. The results show that ACARP outperforms other protocols in terms of performance, Packet Delivery Ratio (PDR), and CO_2 emissions reduction. Moreover, ACARP performs consistently under different mobility variations, making it an attractive option for implementation in Vanet. The evaluation results suggest that artificial intelligence could be a key ingredient in the future development of congestion control solutions in Vanet.

3.1. Machine Learning

In [14], the authors propose a cloud-oriented model that uses machine learning algorithms for cooperative routing, secure data sharing, and traffic pattern analysis. The model aims to improve the reliability and safety of Intelligent Transport Systems (ITS) for the development of smart cities. Whereas in [15], a reinforcement learning-based protocol for routing in Vanet networks is presented. The protocol uses multi-agent reinforcement learning (MARL) to enable agents to solve routing optimization problems in a distributed way. The proposed protocol adapts to dynamic changes by applying a dynamic model (fuzzy system) and learning new events. In [16], the challenges and opportunities of using big data in Vanet networks are discussed. The paper presents a machine learning-assisted approach to efficiently support and process big data in Vanet under a security protocol using 5G technology. The paper also reviews existing routing protocols and proposes new routing information systems that employ machine learning technology to predict vehicle movements and select appropriate routing paths.

In [17], they provide an overview of several misbehavior detection schemes for Vanet. The schemes are classified based on different criteria such as architecture, approach, node-centric, and data-centric. The paper describes various specific misbehavior detection schemes, including CAMDS, CA-DC-MDS, AECFV intrusion detection system, and MA-CIDS. On the other hand, in [18], they present ECRDP, an efficient clustering routing approach for Vanet that uses a new clustering algorithm based on Density Peaks Clustering (DPC) and Particle Swarm Optimization (PSO). The proposed scheme uses the advantages of both algorithms to group vehicles in an urban scenario. The paper also discusses the importance of group stability in Vanet and the use of machine learning for routing.

In [19], they discuss Vanet, their advantages and disadvantages, such as dynamic behavior, which requires an effective and efficient routing protocol to transmit data effectively. The paper proposes a hybrid detection method that uses machine learning and public safety techniques to enhance safety in transport systems. And in [20], they focus on using machine learning to predict the connection duration between two vehicles in a Vanet. Multiple features are proposed and different machine learning algorithms are examined to determine the best prediction method. The authors also discuss the implementation issues and challenges associated with implementing this type of system in Vanet.

In [21], they focus on the problem of detecting Sybil attacks in Vanet and examine various methods for doing so. A new method called SDTC is proposed that uses a movement matrix and an Extreme Learning Machine (ELM) to evaluate the mobility of actual vehicle nodes and detect Sybil nodes. The SDTC method aims to be fast, scalable, and low complexity while ensuring the security, integrity, and privacy of Vanet. And in [22], they cover various aspects of research in Intelligent Transportation Systems (ITS) and Vanet. It delves into Vanet applications, which can be categorized into road safety and traffic management. The paper emphasizes the importance of cellular Vehicle-to-Everything (C-V2X) technology and also proposes a new machine learning detector for RSU that can handle stealthy and brute-force DDoS attacks.

In [23], they focus on the use of machine learning in Vanet, particularly in its applicability to security and communication networks. A methodology for vehicular machine learning is presented, and various models and systematic techniques are reviewed. They also discuss a game theory-based approach for selecting the cluster leader and a stateless Vanet routing protocol called "geoSVR". In general, the paper explores the potential of machine learning and game theory to improve the social features, efficiency, and safety of transportation systems through Vanet. Whereas in [24], they focus on enhancing the efficiency and performance of Vanet through different approaches. One of these approaches is the use of a hybrid metaheuristic algorithm that incorporates machine learning techniques such as SVM, Naive Bayes, ANN, and Decision Tree to reduce latency. A comparative analysis between the HFSA-VANET and CRSM-VANET methods was carried out and it was found that the former achieved an 81% decrease in energy consumption, a 33% reduction in delay, and an 8% increase in throughput when using 80 nodes.

These papers present different techniques and machine learning approaches to enhance the performance, reliability, and safety of Vanet networks in the context of Intelligent Transportation Systems and smart cities.

3.2. Deep Learning

In [25], they propose a novel system for detecting and mitigating attacks in vehicular ad-hoc networks using a weight-optimized deep neural network and an improved particle swarm optimization algorithm. The system extracts features related to traffic flow and vehicle position, detects attacks, and uses a mitigation process based on BAIT. The proposed system outperforms existing techniques in terms of certain performance measures. The paper highlights the importance of road safety in Vanet communication and the decentralized nature of the network.

On the other hand, in [26], they describe a model for network traffic prediction that takes into account road traffic parameters. The proposed RF-GRU-NTP model combines machine learning and deep learning algorithms to predict network traffic flow considering road traffic parameters. The paper also provides an overview of recurrent neural networks (RNN) and their applications in deep learning. Additionally, the work compares different algorithms for predicting network and road traffic, and it was found that the RF algorithm was the best for both types of traffic prediction. As for [27], it proposes the use of a Q-learning deep learning approach and a centralized SDN control mechanism to address the negative influences of malicious nodes in Vanet. The proposed SD-TDQL framework improves data forwarding performance, link quality, and communication security of connected vehicles. A trust model is designed to assess neighbor behavior, and the expected transmission count (ETC) is used to characterize vehicle-to-vehicle communication link quality. Simulation results show that the proposed scheme significantly improves network performance. In [28], they discuss a hybrid relay selection technique that combines deep learning and reinforcement learning to improve diffusion in vehicular networks. The technique uses an artificial neural network to classify forwarding nodes and a Viterbi algorithm as a reinforcement tool to refine the classification. The proposed technique is tested using a grid map scenario with various traffic densities and compared with other parameter-based diffusion techniques. The results show that the proposed technique outperforms other techniques in terms of increasing success rate, saving retransmissions, and other parameters.

In [29], they present a deep learning technique based on convolutional neural networks (CNN) for the detection and recognition of pedestrians in urban environments using LiDAR sensors and RGB cameras. The proposed technique aims to detect and classify pedestrians in real-time in complex urban environments. The proposed neural network model uses a cascade structure to extract spatial and temporal features from the input data. The model is trained and evaluated using a dataset of pedestrians collected in a real urban environment. The results show that the proposed technique surpasses other deep learning methods in terms of detection accuracy and speed. And in [30], they present a deep learning technique based on convolutional neural networks (CNN) for traffic sign recognition using images from vehicle-mounted cameras. The proposed technique aims to detect and recognize traffic signs in real-time, which can be useful for driver assistance systems and autonomous vehicles. The proposed neural network model uses a cascade structure to extract spatial and temporal features from the input data. The model is trained and evaluated using a traffic sign dataset collected in a real urban environment. The results show that the proposed technique outperforms other deep learning methods in terms of traffic sign recognition accuracy and speed.

3.3. Swarm Intelligence

In [31], they present a collaborative communication scheme that uses drones to assist in vehicular ad-hoc networks. The problem is modeled as a multi-modal optimization problem, and a swarm-based optimization algorithm called Multimodal Nomad Algorithm is presented. The proposed scheme was compared with similar counterparts and demonstrated to outperform its competitors in terms of the number of hops, packet delivery ratio, and performance. The work highlights the importance of considering available UAVs when optimizing the location of drones. Whereas in [32], they propose an approach to maximize coverage in vehicular communication networks using Internet of Drones (IoD) nodes based on the locations of ground vehicles. An enhanced version of Particle Swarm Optimization (PSO) is used to optimize the deployment of IoD nodes. This approach is compared with two other schemes: one without IoD and another with a fixed IoD deployment. Simulation results show that the proposed approach achieves better coverage and signal quality, and is able to adapt to vehicle movements. This work concludes by highlighting the importance of considering available UAVs when optimizing the location of drones. And in [33], they discuss various routing protocols for vehicular ad-hoc networks and propose a routing protocol based on hybrid genetic and firefly algorithms (HGFA) to overcome the limitations of these protocols in different traffic scenarios for vehicular ad-hoc networks. The proposed system model integrates genetic features with the firefly algorithm to optimize routing in vehicle-to-vehicle communication networks.

On the other hand, in [34] they propose a protocol called PSOstreaming that addresses three challenging problems in video streaming in vehicular ad-hoc networks: load balancing, short-term mobility prediction, and efficient data caching. The protocol uses a particle swarm optimization algorithm to solve the load balancing problem, formulates short-term mobility predictions to react to vehicle mobility immediately, and performs efficient caching to store video data content on the calculated route until communication is completed. In [35], they describe a new clustering algorithm, called CAMONET, for vehicular ad-hoc networks. The algorithm uses the Moth and Flame Optimization (MFO) to generate optimized clusters for efficient transmission. The results of the experiments show that CAMONET provides results close to optimal, making it an efficient method for vehicular clustering. And in [36], it focuses on the challenge of ensuring safety in vehicular ad-hoc networks. Vehicular ad-hoc networks are used to improve safety and communication between vehicles, but they also face security threats due to the wireless and open nature of the network. The article discusses several common attacks in vehicular ad-hoc networks, such as denial of service (DoS), location spoofing, and message flooding attacks. Then, an overview of the proposed security schemes is presented and the limitations of each are highlighted.

4. Software-Defined Networking (SDN) in Vehicular Ad-Hoc Networks: Protocols And Architectures

Software-Defined Networking (SDN) technology has emerged as a promising solution to improve efficiency and security in vehicular ad-hoc networks. SDN separates the control plane from the data plane and allows a centralized controller to manage the network based on global information. In recent years, several SDN protocols and architectures have been proposed for vehicular ad-hoc networks that address issues such as security, reliability, and communication efficiency.

In [37], they propose a routing protocol based on MGM (Modified Gossiping Mesh) that applies network coding to entertainment and confidential messages to improve reliability and security. Additionally, a secure and reliable data broadcasting framework based on NC-enabled SDN is presented. In [38], they talk about how the use of blockchain and SDN in Intelligent Transportation Systems (ITS) can improve the vehicular ad-hoc network. A trust-based model is presented to limit malicious activities and ensure efficient network performance. In [39], they address the vulnerability of vehicular ad-hoc networks to cyber-attacks and propose a collaborative Intrusion Detection System (IDS) based on SDN and deep learning. Whereas in [40], they discuss an Adaptive Link State Perception (ALPS) scheme for software-defined vehicular ad-hoc networks. And in [41], they worked on the integration of blockchain and SDN in Intelligent Transportation Systems appears to be an interesting solution to ensure trust and improve the performance of vehicular networks. The simulation performed shows promising results in terms of efficiency and security in the network while in [42], they propose the safe routing protocol SURFER based on SDN and blockchain appears to be an innovative and effective solution for the Internet of Vehicles. The results of the simulations indicate that

SURFER outperformed other routing protocols in terms of latency, packet delivery, and network overhead, which is a great advancement for network management in this area.

4.1. Sdn Architectures

The presented papers address different aspects of SDN architectures for vehicular ad-hoc networks. In [43], they focus on detecting DDoS attacks in vehicular ad-hoc networks, proposing a detection model that uses SVM with an optimized RBF-SVM kernel. In [44], they propose a Q deep learning framework to improve the performance of data forwarding, link quality, and communication security of connected vehicles in vehicular ad-hoc networks. In [45], they address the concept of network "slicing" in the 5G architecture, which allows network operators to create multiple virtual networks for different types of services with different requirements. In [46], they propose a fog computing-enabled architecture for efficient data broadcasting in heterogeneous software-defined vehicular ad-hoc networks. While in [47], they present an adaptive data emission interval proposed for data broadcasting in Vehicle-to-Infrastructure (V2I) environments using Software-Defined Networking (SDN) architecture. And in [48], they propose an architecture called SEARCH for vehicle route planning in urban areas with high traffic congestion. The architecture uses technologies such as UAV, vehicular ad-hoc networks, 5G cellular systems, and SDN to collect real-time traffic information and plan faster routes. Simulations showed that the architecture is effective in saving driving time.

5. CONCLUSIONS

The systematic literature review conducted in this paper provides a deep understanding of recent advancements in Vanet and highlights the importance of ongoing research in this field to confront emerging challenges and harness the opportunities offered by new technologies. The application of artificial intelligence techniques in Vanet, such as machine learning, deep learning, and swarm intelligence, offer promising solutions to address the challenges of routing in Vanet networks, thus enhancing their efficiency and security. Whereas the use of SDN in Vanet also presents great potential to overcome technical obstacles, such as traffic management and communication link disruption, by implementing SDN protocols and SDN architectures.

Routing in Vanet is a challenge due to the dynamic nature of the network and the possibility of connectivity disruption due to obstacles and vehicle speed. To address these challenges, various routing techniques and protocols have been proposed, such as reliable routing protocols, the distributed and cooperative information exchange mechanism, and cryptography and trust-based methods. Moreover, artificial intelligence has shown to be a promising technique for improving the performance of congestion control protocols in Vanet. Together, these advancements suggest that continued research in this field can lead to even more effective solutions for routing and congestion control in Vanet.

REFERENCES

[1] S. A. Rashid et al., “A collaborated genetic with lion optimization algorithms for improving the quality of forwarding in a vehicular ad-hoc network,” IAES International Journal of Artificial Intelligence, vol. 12, no. 2, pp. 667–677, Jun. 2023, doi: 10.11591/ijai.v12.i2.pp667-677.

[2] Y. Regragui and N. Moussa, “A real-time path planning for reducing vehicles traveling time in cooperative-intelligent transportation systems,” Simul Model Pract Theory, vol. 123, Feb. 2023, doi: 10.1016/j.simpat.2022.102710. A Q-Learning and Fuzzy L

[3] J. R. Maranur and B. Mathapati, “ARPVP: Attack Resilient Position-Based VANET Protocol Using Ant Colony Optimization,” Wirel Pers Commun, vol. 128, no. 2, pp. 1235–1258, Jan. 2023, doi: 10.1007/s11277-022-09997-0.

[4] H. Ning et al., "Modeling and analysis of traffic warning message dissemination system in VANETs," Vehicular Communications, vol. 39, Feb. 2023, doi: 10.1016/j.vehcom.2022.100566.

[5] A. Shan, X. Fan, C. Wu, X. Zhang, and R. Men, "Dynamic Selfish Node Detection with Link Quality Consideration in Vehicular Networks," IEEE Trans Veh Technol, 2023, doi: 10.1109/TVT.2023.3244961.

[6] V. Krishna and G. Reddy, "VANET Vulnerabilities Classification and Countermeasures: A Review," Majlesi Journal of Electrical Engineering, vol. 16, no. 3, pp. 63–83, 2022, doi: 10.30486/mjee.2022.696508.

[7] N. Venkatamune and J. Prabhashankar, "A VANET Collision Warning System with Cloud Aided Pliable Q-Learning and Safety Message Dissemination," International Arab Journal of Information Technology, vol. 20, no. 1, pp. 113–124, Jan. 2023, doi: 10.34028/iajit/20/1/12.

[8] M. Khalid Diaa, I. Samer Mohamed, and M. Ayman Hassan, "OPBRP - obstacle prediction based routing protocol in VANETs," Ain Shams Engineering Journal, Jul. 2022, doi: 10.1016/j.asej.2022.101989.

[9] M. Rahmani et al., "A Q-Learning and Fuzzy Logic-Based Hierarchical Routing Scheme in the Intelligent Transportation System for Smart Cities," Mathematics, vol. 10, no. 22, Nov. 2022, doi: 10.3390/math10224192.

[10] M. Saleh, "Position-Based Multipath Route Switching Protocol for Intelligent VANETs Using Wiedemann Car-Following Model," International Journal of Electrical and Electronic Engineering and Telecommunications, vol. 12, no. 1, pp. 22–34, Jan. 2023, doi: 10.18178/ijeetc.12.1.22-34.

[11] P. Sehrawat and M. Chawla, "Interpretation and Investigations of Topology Based Routing Protocols Applied in Dynamic System of VANET," Wirel Pers Commun, Feb. 2022, doi: 10.1007/s11277-022-10042-3.

[12] S. Kumar and J. Singh, "Internet of vehicles (IOV) over vanets: Smart and secure communication using IOT," Scalable Computing, vol. 21, no. 3, pp. 425–440, 2020, doi: 10.12694:/scpe.v21i3.1741.

[13] L. M. Giripunje, A. Vidyarthi, and S. K. Shandilya, "Adaptive Congestion Prediction in Vehicular Ad-hoc Networks (VANET) Using Type-2 Fuzzy Model to Establish Reliable Routes," Wirel Pers Commun, vol. 125, no. 4, pp. 3527–3548, Aug. 2022, doi: 10.1007/s11277-022-09723-w.

[14] A. Rehman, K. Haseeb, T. Saba, J. Lloret, and Z. Ahmed, "Towards Resilient and Secure Cooperative Behavior of Intelligent Transportation System Using Sensor Technologies," IEEE Sens J, vol. 22, no. 7, pp. 7352–7360, Apr. 2022, doi: 10.1109/JSEN.2022.3152808.

[15] O. Jafarzadeh, M. Dehghan, H. Sargolzaey, and M. M. Esnaashari, "A Model-Based Reinforcement Learning Protocol for Routing in Vehicular Ad hoc Network," Wirel Pers Commun, vol. 123, no. 1, pp. 975–1001, Mar. 2022, doi: 10.1007/s11277-021-09166-9.

[16] S. Y. Zhang, M. Lagutkina, K. O. Akpinar, and M. Akpinar, "Improving performance and data transmission security in VANETs," Comput Commun, vol. 180, pp. 126–133, Dec. 2021, doi: 10.1016/j.comcom.2021.09.005.

[17] G. Husnain, S. Anwar, G. Sikander, A. Ali, and S. Lim, "A Bio-Inspired Cluster Optimization Schema for Efficient Routing in Vehicular Ad Hoc Networks (VANETs)," Energies (Basel), vol. 16, no. 3, Feb. 2023, doi: 10.3390/en16031456.

[18] K. Kandali, L. Bennis, O. El Bannay, and H. Bennis, "An Intelligent Machine Learning Based Routing Scheme for VANET," IEEE Access, vol. 10, pp. 74318–74333, 2022, doi: 10.1109/ACCESS.2022.3190964.

[19] G. P. K. Marwah et al., "An Improved Machine Learning Model with Hybrid Technique in VANET for Robust Communication," Mathematics, vol. 10, no. 21, Nov. 2022, doi: 10.3390/math10214030.

[20] P. Rocha et al., "Evaluating Link Lifetime Prediction to Support Computational Offloading Decision in VANETs," Sensors, vol. 22, no. 16, Aug. 2022, doi: 10.3390/s22166038.

[21] S. Kakulla and S. Malladi, "Sybil Attack Detection in VANET Using Machine Learning Approach," Ingenierie des Systemes d'Information, vol. 27, no. 4, pp. 605–611, Aug. 2022, doi: 10.18280/isi.270410.

[22] A. Haydari and Y. Yilmaz, "RSU-Based Online Intrusion Detection and Mitigation for VANET," Sensors, vol. 22, no. 19, Oct. 2022, doi: 10.3390/s22197612.

[23] N. Phull, P. Singh, M. Shabaz, and F. Sammy, "Enhancing Vehicular Ad Hoc Networks' Dynamic Behavior by Integrating Game Theory and Machine Learning Techniques for Reliable and Stable Routing," Security and Communication Networks, vol. 2022, 2022, doi: 10.1155/2022/4108231.

[24] G. P. K. Marwah and A. Jain, "A hybrid optimization with ensemble learning to ensure VANET network stability based on performance analysis," Sci Rep, vol. 12, no. 1, Dec. 2022, doi: 10.1038/s41598-022-14255-1.

[25] P. V. Sontakke and N. B. Chopade, "Optimized Deep Neural Model-Based Intrusion Detection and Mitigation System for Vehicular Ad-Hoc Network," Cybern Syst, 2022, doi: 10.1080/01969722.2022.2137643.

[26] S. S. Sepasgozar and S. Pierre, "Network Traffic Prediction Model Considering Road Traffic Parameters Using Artificial Intelligence Methods in VANET," IEEE Access, vol. 10, pp. 8227–8242, 2022, doi: 10.1109/ACCESS.2022.3144112.

[27] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, "Software-Defined Vehicular Networks with Trust Management: A Deep Reinforcement Learning Approach," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 2, pp. 1400–1414, Feb. 2022, doi: 10.1109/TITS.2020.3025684.

[28] McHergui and T. Moulahi, "A Novel Deep Reinforcement Learning Based Relay Selection for Broadcasting in Vehicular Ad Hoc Networks," IEEE Access, vol. 10, pp. 112–121, 2022, doi: 10.1109/ACCESS.2021.3138903.

[29] O. S. Oubbati, M. Atiquzzaman, A. Baz, H. Alhakami, and J. Ben-Othman, "Dispatch of UAVs for urban vehicular networks: A deep reinforcement learning approach," IEEE Trans Veh Technol, vol. 70, no. 12, pp. 13174–13189, Dec. 2021, doi: 10.1109/TVT.2021.3119070.

[30] T. Alladi, B. Gera, A. Agrawal, V. Chamola, and F. R. Yu, "Deepadv: A deep neural network framework for anomaly detection in vanets," IEEE Trans Veh Technol, vol. 70, no. 11, pp. 12013–12023, Nov. 2021, doi: 10.1109/TVT.2021.3113807.

[31] N. Lin, L. Fu, L. Zhao, G. Min, A. Al-Dubai, and H. Gacanin, "A Novel Multimodal Collaborative Drone-Assisted VANET Networking Model," IEEE Trans Wirel Commun, vol. 19, no. 7, pp. 4919–4933, Jul. 2020, doi: 10.1109/TWC.2020.2988363.

[32] G. A. Ahmed, T. R. Sheltami, A. S. Mahmoud, M. Imran, and M. Shoaib, "A Novel Collaborative IoD-Assisted VANET Approach for Coverage Area Maximization," IEEE Access, vol. 9, pp. 61211–61223, 2021, doi: 10.1109/ACCESS.2021.3072431.

[33] G. D. Singh, M. Prateek, S. Kumar, M. Verma, D. Singh, and H. N. Lee, "Hybrid Genetic Firefly Algorithm-Based Routing Protocol for VANETs," IEEE Access, vol. 10, pp. 9142–9151, 2022, doi: 10.1109/ACCESS.2022.3142811.

[34] Y. Shin, H. S. Choi, Y. Nam, H. Cho, and E. Lee, "Particle Swarm Optimization Video Streaming Service in Vehicular Ad-Hoc Networks," IEEE Access, vol. 10, pp. 102710–102723, 2022, doi: 10.1109/ACCESS.2022.3206786.

[35] Y. A. Shah, H. A. Habib, F. Aadil, M. F. Khan, M. Maqsood, and T. Nawaz, "CAMONET: Moth-Flame Optimization (MFO) Based Clustering Algorithm for VANETs," IEEE Access, vol. 6, pp. 48611–48624, Sep. 2018, doi: 10.1109/ACCESS.2018.2868118.

[36] P. Upadhyay, V. Marriboina, S. Kumar, S. Kumar, and M. A. Shah, "An Enhanced Hybrid Glowworm Swarm Optimization Algorithm for Traffic-Aware Vehicular Networks," IEEE Access, vol. 10, pp. 110136–110148, 2022, doi: 10.1109/ACCESS.2022.3211653.

[37] J. Bhatia, P. Kakadia, M. Bhavsar, and S. Tanwar, "SDN-Enabled Network Coding-Based Secure Data Dissemination in VANET Environment," IEEE Internet Things J, vol. 7, no. 7, pp. 6078–6087, Jul. 2020, doi: 10.1109/JIOT.2019.2956964.

[38] J. Gao et al., "A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks," IEEE Internet Things J, vol. 7, no. 5, pp. 4278–4291, May 2020, doi: 10.1109/JIOT.2019.2956241.

[39] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, "Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4519–4530, Jul. 2021, doi: 10.1109/TITS.2020.3027390.

[40] N. Lin, D. Zhao, L. Zhao, A. Hawbani, M. Guizani, and N. Kumar, "ALPS: An Adaptive Link-State Perception Scheme for Software-Defined Vehicular Networks," IEEE Trans Veh Technol, vol. 72, no. 2, pp. 2564–2575, Feb. 2023, doi: 10.1109/TVT.2022.3214660.

[41] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," IEEE Access, vol. 8, pp. 91028–91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[42] K. Mershad, "SURFER: A Secure SDN-Based Routing Protocol for Internet of Vehicles," IEEE Internet Things J, vol. 8, no. 9, pp. 7407–7422, May 2021, doi: 10.1109/JIOT.2020.3038465.

[43] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D. S. Kim, “Optimization of RBF-SVM Kernel using Grid Search Algorithm for DDoS Attack Detection in SDN-based VANET,” IEEE Internet Things J, 2022, doi: 10.1109/JIOT.2022.3199712.

[44] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, “Software-Defined Vehicular Networks with Trust Management: A Deep Reinforcement Learning Approach,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 2, pp. 1400–1414, Feb. 2022, doi: 10.1109/TITS.2020.3025684.

[45] A. A. Khan, M. Abolhasan, W. Ni, J. Lipman, and A. Jamalipour, “An End-to-End (E2E) Network Slicing Framework for 5G Vehicular Ad-Hoc Networks,” IEEE Trans Veh Technol, vol. 70, no. 7, pp. 7103–7112, Jul. 2021, doi: 10.1109/TVT.2021.3084735.

[46] K. Liu, K. Xiao, P. Dai, V. C. S. Lee, S. Guo, and J. Cao, “Fog Computing Empowered Data Dissemination in Software Defined Heterogeneous VANETs,” IEEE Trans Mob Comput, vol. 20, no. 11, pp. 3181–3193, Nov. 2021, doi: 10.1109/TMC.2020.2997460.

[47] J. Bhatia, J. Dave, M. Bhavsar, S. Tanwar, and N. Kumar, “SDN-Enabled Adaptive Broadcast Timer for Data Dissemination in Vehicular Ad Hoc Networks,” IEEE Trans Veh Technol, vol. 70, no. 8, pp. 8134–8147, Aug. 2021, doi: 10.1109/TVT.2021.3092065.

[48] O. S. Oubbati, M. Atiquzzaman, P. Lorenz, A. Baz, and H. Alhakami, “SEARCH: An SDN-Enabled Approach for Vehicle Path-Planning,” IEEE Trans Veh Technol, vol. 69, no. 12, pp. 14523–14536, Dec. 2020, doi: 10.1109/TVT.2020.3043306.

AUTHORS

Lewys Correa Sánchez. Systems Engineer from the Universidad de Córdoba (Colombia). He has a master in information and communications sciences from the Universidad Distrital Francisco José de Caldas. He is currently a doctoral student in engineering at the Universidad Distrital Francisco José de Caldas.

Octavio Salcedo Parra. He received his BS degree in System Engineering from the Universidad Autonoma de Colombia, Colombia, and his MS degree in Teleeinformatics from the Universidad Distrital Francisco José de Caldas, Colombia, in 1998, MS degree in Economy from the Universidad de los Andes, Colombia, in 2004. A diploma of advanced Studies (DEA) from the Pontificia Universidad de Salamanca, Campus of Madrid, Spain in 2010. A PhD in Informatics Engineering from the Pontificia Universidad de Salamanca, Campus of Madrid, Spain in 2013. A PhD in political studies from the Universidad Externado de Colombia, Colombia in 2013.

Miguel José Espitia Rico. In 1998, he received his BS degree in Licensed in Physics and Mathematics from the Universidad de Córdoba, Colombia. , and his MS degree in Physics from the Universidad Nacional de Colombia in 2007. A PhD in In Physical Sciences from the Universidad Nacional de Colombia in 2016. His current research interests are communications and physical materials. PhD Espitia is full Professor at the Universidad Distrital Francisco José de Caldas.