International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Advanced Dynamic Vehicular Networks with Enhanced Privacy and Real-Time Intelligent Traffic Management

Vijayalakshmi V*[1], Dr. S. Ismail Kalilulah[2]

Submitted:13/03/2024 **Revised**: 28/04/2024 **Accepted**: 05/05/2024

Abstract: In vehicular communication systems, the evolution of Vehicular Ad Hoc Networks (VANETs) provides the door for novel solutions and expanded features. This proposed study presents an upgraded framework for Vehicular Ad Hoc Networks (VANETs), focusing on better privacy measures, real-time intelligent traffic management, and augmented safety features. Our framework leverages an adaptive network architecture that dynamically responds to varying vehicular conditions, ensuring uninterrupted communication and optimal performance. To secure user privacy, we have incorporated a powerful privacy-preserving system utilizing modern encryption algorithms, assuring the security of sensitive information while facilitating vital data interchange for vehicle operations. Specifically, we have presented a hybrid encryption technique that leverages the Advanced Encryption Standard (AES-128) coupled with digital signatures to protect the content of Content-Centric Vehicular Networks (CCVN) during inter-vehicle communication. This hybrid technique secures data confidentiality and integrity, delivering a complete security solution for vehicle communication. Furthermore, our system provides real-time intelligent traffic management capabilities, including dynamic route optimization and congestion prediction, boosting traffic flow and minimizing travel times. This is accompanied by a comprehensive warning system that gives drivers real-time information about speed restrictions, dangers, and traffic conditions, enhancing driver awareness and overall traffic safety. The warning system is designed to be all-encompassing, ensuring that drivers are well-informed about potential dangers on the road. Network administration is handled using a decentralized architecture, guaranteeing robust and dependable communication without depending on centralized infrastructure. Additionally, our system contains machine learning algorithms that continually learn and adapt to traffic patterns, further enhancing the network's speed and dependability. Our proposed framework dramatically enhances the capabilities of current VANETs, providing a safe, intelligent, and privacy-preserving alternative for contemporary vehicular communication systems. This revolutionary strategy intends to increase vehicular communication and boost traffic management systems' overall efficiency and safety.

Keywords: *Dynamic Network Management, Enhanced Privacy Mechanism, Hybrid Encryption Scheme, Intelligent Traffic Management, Real-Time Notifications, VANET (Vehicular Ad Hoc Networks)*

1. Introduction

Over the past few years, the ever-evolving wireless communication technologies have radically changed vehicular networks. VANETs, a subtype of Mobile Ad Hoc Networks (MANETs), have become increasingly important in enabling communication between vehicles and infrastructure. This technology has the potential with the goal of substantially enhancing traffic efficiency, driving enjoyment, and security on the roads. Through vehicle-to-vehicle and vehicle-to-roadside communication, VANETs offer many applications, including collision prevention, traffic control, entertainment, and self-driving capabilities.

VANETs are known for their intermittent interactions among edge devices, high node flexibility, and fluid interaction [1]. VANETs pose a challenge due to their complexity and limitations. To exclusively transmit and receive location-based data solely through infrastructure-based communications. In addition, the TCP/IP architecture was not intended initially or optimised to function in these ever-changing environments [2]. It is difficult for TCP/IP protocols to handle new features and issues in edge computing due to its host-centric paradigm. Among them, you may find dynamic routing, node mobility, and data security [3]. There has been a trend towards designing a system that can withstand delays and disconnections so that applications like C-ITS may be successful and adaptive on VANETs. Conventional IP-based network architectural models that focus on hosts have not altered despite innovations in IVC and other network technologies [5]. Despite this, the constantly shifting topology and frequent separations provide difficulties for IP-based VANET application in terms of data routing, protection, and node mobility. These factors can potentially impede their effectiveness [4].

Despite the increasing interest in the potential benefits of VANETs, the ever-changing nature of VANETs (with vehicles joining and leaving at will) and the numerous system and application requirements pose significant challenges in developing effective methods to protect vehicle privacy. Privacy encompasses the protection of

[1] *Research Scholar, Dr. M. G. R. Educational and Research Institute, Maduravoyal, Chennai, India.*
[2] *Associate Professor, Dr. M. G. R. Educational and Research Institute, Maduravoyal, Chennai, India.*
ORCID ID: 0000-0002-2357-3982
** Corresponding Author Email: vijayalakshmivmani@gmail.com*

vehicle drivers and the confidentiality of vehicle locations. The identity or location of a vehicle must remain private when it sends a message, except to relevant authorities. Every message sent by a vehicle must undergo authentication before it is processed. Until these issues are resolved to the utmost satisfaction of the users, the widespread implementation of VANETs cannot occur. Authentication must be accomplished at two different levels. The first level is node authentication, which occurs at the node level. The second level is message authentication, which occurs at the message level [5]. The fundamental concept of message authentication involves the sender signing a message and the receiver verifying its authenticity and integrity. Addressing and solving certain authentication requirements is crucial to ensure secure communication in VANETs. These requirements include low computational overhead, strong and scalable authentication, and efficient and scalable certificate revocation.

Vehicular traffic management poses various challenges, including the unpredictability of traffic patterns, the importance of being able to respond rapidly to new circumstances, and the fact that vehicle speeds might vary widely. Traditional systems face difficulties addressing these challenges, resulting in inefficient traffic flow and road infrastructure use [4]. This research focuses on the issue of existing traffic management systems being unable to handle the constantly changing nature of vehicular networks effectively. To optimise traffic flow and reduce congestion, a system that can monitor and react to traffic conditions in real-time is essential [5]. Building a smart traffic control system using Machine Learning is the primary focus of this project. The system is designed to accurately anticipate and adjust to traffic patterns, resulting in optimised signal timings and a transportation infrastructure that is more efficient and sustainable.

This proposed study introduces a cutting-edge framework for VANETs aimed at tackling these challenges through the integration of improved privacy measures, intelligent traffic management, and adaptive network architecture. Our framework utilises cutting-edge encryption techniques, advanced machine learning algorithms, and a decentralised network management approach to deliver a robust, efficient, and secure vehicular communication system. Our framework incorporates a hybrid encryption scheme that combines the Advanced Encryption Standard (AES-128) with digital signatures, guaranteeing both data confidentiality and integrity. In addition, the incorporation of machine learning models allows for the enhancement of route optimisation and the prediction of congestion, resulting in improved traffic flow and decreased travel times. An architecture that is decentralised ensures strong communication without depending on centralised infrastructure, which improves the reliability and scalability of the system. This study addresses essential aspects such as privacy, security, and real-time traffic management. Its goal is to improve the capabilities of current VANETs, providing a comprehensive solution that enhances vehicular communication and contributes to the overall efficiency and safety of traffic management systems. This ground-breaking approach highlights the immense potential of VANETs to transform the future of transportation by creating more intelligent, secure, and interconnected vehicular environments.

2. Related Works

The main objective of VANET is to ensure each mobile node's safety and minimize accidents and delays in data delivery. The network structure's instability causes problems with routing. The abundance of data in the VANET system often results in a congestion of information on RSUs. Various protocols have been created to address certain concerns, such as routing, congestion control, and stability. A machine learning (ML) strategy for supplementary data analysis was, however, absent from all of them. Because of this disconnect, there is a push to merge traditional and machine learning models in an effort to boost performance [15, 16].

In order to streamline vehicular ad hoc networks, methods of feature selection are used early on to eliminate superfluous aberrant features and group intelligent features [25]. Computerized correlation-based filtering (CFS) is more efficient and accurate than the second filtering method. IoT devices can readily utilize machine learning and artificial intelligence techniques [23,24]. Several traffic classification techniques estimate the commonly used supervised machine learning methods achieved through the WEKA software [26,27]. Machine learning algorithms are highly valuable for acquiring knowledge and improving over time.

The analysis continues with an examination of several machine learning approaches to traffic control in [6]. It sheds light on the benefits and drawbacks of different methods, which is useful for finding smart traffic management solutions. Most of the research in [7] is devoted on SVM. Use of support vector machines (SVMs) for traffic forecasting is the focus of this review. We highlight the practicality of SVM models by analyzing their effectiveness in capturing complicated traffic patterns. The use of Reinforcement Learning (RL) for controlling traffic signals is discussed in [8]. The main idea behind this project is to adapt the signal schedule in real-time according to traffic circumstances. The research provides important information on how RL algorithms work for efficient and responsive traffic management. A comprehensive history of ITS, or smart transportation systems, is given in [9]. The article explores the latest advancements in technology, such as machine learning, and how they can help overcome

obstacles in traffic management. This provides a background for the ongoing research.

Research into kernel approaches, and more especially Radial Basis Function (RBF), is explored in [10] with an eye on their possible use in traffic flow prediction. In order to help readers, choose the best kernels for their traffic prediction models, the paper delves into the advantages of kernel-based approaches for capturing non-linear connections. Integrating smart city projects with vehicle networks is explored in the research in [11]. In this study, we look at how smart public transportation and city planning may function together. It highlights the importance of using adaptive and learning-based methods to tackle the obstacles of contemporary urban mobility. An enhanced system has been proposed in [12] to ensure the confidentiality of content-related names and data. In this system, obtaining the necessary content is made simple and convenient. Authors have utilized proxy-based encryption schemes to ensure user privacy. The characteristics of ICN are maintained while keeping the computational cost low. This system can handle various security attacks. In [13], a method based on attributes has been utilized to address the issue of privacy preservation in access control within ICN. This approach efficiently handles the attributes of ICN. Access to the contents of ICN is restricted to authorized users only.

This approach has successfully reduced time delay, improved throughput, lower storage costs, and enhanced network security. In [14], the authors have explored different privacy concerns related to CCN and its architecture. Extensive research has been conducted on the different types of network attacks that can compromise the integrity and confidentiality of content.

Sumi and Ranga [17] proposed an intelligent traffic management solution for countries using the principles of IoT and vehicular ad hoc networks (VANET). The proposed approach prioritizes emergency vehicles to ensure a smooth flow through traffic, considering the type of incident. It guides ambulances towards the most efficient routes to their destination while also providing a means to detect and respond to traffic signal manipulation. Our solution outperforms these suggestions for emergency vehicle systems in terms of congestion avoidance, travel duration, and energy consumption. In their study, Ning et al. [18] proposed a practical approach to reduce response time in traffic management services. They suggested enabling real-time content distribution in IoV systems based on different network access, which could help improve overall efficiency. Large-scale IoV systems typically begin by developing a framework that relies on crowd sensing. In addition, an exploration is conducted into a framework that optimizes traffic control by utilizing clusters. They trust the messages generated by vehicles. There is a potential issue with the accuracy of information being shared on the network, which could lead to misleading other vehicles and traffic control systems.

Tsang et al. [19] devised a fully integrated approach to traffic monitoring, which involved the combination of high-definition intelligent cameras and wireless connectivity. Gunda [20] provided a systematic framework for developing a practical traffic management tool that effectively addresses network-level traffic congestion on roadways. Lee et al. [21] presented a collaborative visual analytics system that utilizes vehicle detection information to investigate, monitor, and predict traffic congestion. These visual analytics technological advances allow customers to explore the origins, routes, and degree of traffic congestion. To address the existing limitations, Nguyen et al. [22] proposed an adaptable smart traffic management platform (STMP) that utilizes untrained deep learning techniques.

3. Methods and Materials

An adaptive network architecture that dynamically adjusts to different traffic situations is included into the framework that has been presented for traffic Ad Hoc Networks (VANETs). The flow diagram Fig. 1. showcases the suggested technique for Advanced Dynamic Vehicular Networks (VANETs), with a specific emphasis on improving privacy and implementing real-time intelligent traffic management. The process starts by initializing the network and establishing the essential communication protocols required for VANET operations. Effective node management is essential for maintaining optimal performance and communication integrity in a vehicle network. This involves constantly monitoring vehicle conditions like speed and location, and adjusting network parameters accordingly. Communication protocols play a crucial role in the framework, allowing for smooth integration of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) connections. This ensures reliable data exchange and optimal network performance.

The methodology includes a hybrid encryption mechanism that utilizes the Advanced Encryption Standard (AES-128) for data confidentiality and digital signatures to guarantee data integrity and authenticity. Ensuring that communications within the network remain secure and private is of utmost importance. Having real-time traffic management capabilities is crucial. Our system optimizes routes based on real-time data to reduce travel time and avoid congested areas. Additionally, we use data analytics and machine learning to predict and manage congestion, allowing us to proactively reroute traffic.

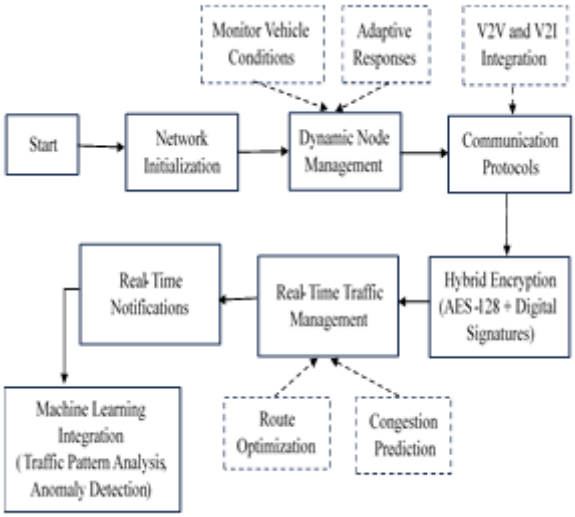

Fig. 1. The outline of the Advanced Dynamic Vehicular Networks with Enhanced Privacy and Real-Time Intelligent Traffic Management

Drivers receive real-time notifications that provide updated information on road conditions, speed limits, hazards, and other critical details. This helps to enhance safety and awareness while on the road. Machine learning integration is utilized to analyze traffic patterns, allowing for the identification and prediction of traffic conditions. It also helps in detecting any anomalies or potential hazards, thereby ensuring a smooth flow of traffic and enhancing safety. This comprehensive framework aims to improve the capabilities of current VANETs, providing a secure, efficient, and intelligent vehicular communication system.

When it comes to modelling traffic flow and vehicle interactions, SUMO is the single most important simulation tool. It offers a comprehensive and scalable environment for simulating vehicle movement and communication, which enables the evaluation of dynamic route optimization, the prediction of congestion, and the provision of real-time warnings. For the purpose of analyzing the proposed VANET system, SUMO is an excellent candidate because of its adaptability in modelling complicated urban and highway situations.

3.1. Communication Protocols Implementation

The implementation of communication protocols in the proposed VANET framework is crucial to ensure seamless and efficient data exchange between vehicles (V2V) and between vehicles and infrastructure (V2I). The protocols are designed to handle the dynamic and decentralized nature of VANETs, providing robust and reliable communication even under varying traffic conditions. V2V communication, which stands for vehicle-to-vehicle communication, allows cars to communicate directly with one another. This is crucial for the transmission of real-time data, which is required for safety applications and traffic management.

Algorithm V2V_Communication

Input: Vehicle data (speed, position, direction), DSRC parameters

Output: Real-time communication between vehicles

1. Initialize DSRC and IEEE 802.11p protocol
2. For each vehicle V in the network do
3. Collect real-time data from vehicle sensors
4. Create message M (type: BSM/CAM/DENM)
5. M.content ← {V.speed, V.position, V.direction}
6. Encrypt M using AES-128
7. Sign M with vehicle's digital signature
8. Broadcast M to neighboring vehicles
9. End for

Data transmission between cars and roadside units (RSUs) is an example of vehicle-to-infrastructure (V2I) communication. This communication supports various applications, including traffic control and information and entertainment services.

Algorithm V2I_Communication

Input: Vehicle data, RSU parameters, cellular network parameters

Output: Communication between vehicles and infrastructure

1. Initialize RSUs and connect to cellular network
2. For each vehicle V approaching an RSU do
3. Collect data D from vehicle sensors
4. Create message M (type: Request/Response)
5. M.content ← {D}
6. Encrypt M using AES-128
7. Sign M with vehicle's digital signature
8. Send M to RSU
9. RSU processes M and generates response R
10. Encrypt R using AES-128
11. Sign R with RSU's digital signature
12. Send R to V
13. End for

3.2. Hybrid Encryption

To ensure data security and privacy in the proposed VANET framework, we implement a hybrid encryption scheme that combines symmetric and asymmetric encryption methods.

This approach leverages the strengths of both encryption techniques to provide robust data confidentiality, integrity, and authenticity. The symmetric encryption component employs the Advanced Encryption Standard (AES-128), which is chosen for its balance between security and performance, ensuring data confidentiality through fast and secure encryption.

Mathematically, the plaintext message P is encrypted using a randomly generated session key K with AES-128, resulting in the ciphertext $E1$.

$$E1 = AES - 128\_Encrypt(P, K) \quad (1)$$

To ensure the integrity and authenticity of the message, a digital signature S is created using the sender's private keyV_{priv}.

$$S = Sign(E1, V_{priv}) \quad (2)$$

For secure key distribution, the session key K is encrypted using the recipient's public key R_{pub}, yielding $E2$.

$$E2 = Encrypt(K, R_{pub}) \quad (3)$$

Additionally, the session key is encrypted with the Certificate Authority's public key $CA_{pub}$to ensure secure verification, producing $E3$.

$$E3 = Encrypt(K, CA_{pub}) \quad (4)$$

The final encrypted message E is then composed of the ciphertext E1, the digital signature S, and the encrypted session keys $E2$ and $E3$:

$$E = \{E1, S, E2, E3\} \quad (5)$$

The hybrid encryption process includes encrypting the message using a symmetric key (AES-128) and then encrypting the symmetric key using the recipient's public key (asymmetric encryption). A digital signature is generated and attached to the message to ensure its authenticity.

Algorithm Hybrid_Encryption

Input: Plaintext message P, vehicle's private key V_{priv} , recipient's public key R_{pub}, CA's public key CA_{pub}

Output: Encrypted and signed message E

1. Generate session key K
2. E1 ← AES-128_Encrypt(P, K)
3. Signature S ← Sign(E1, V_{priv})
4. E2 ← Encrypt(K, R_{pub})
5. E3 ← Encrypt(K, CA_{pub})
6. E ← {E1, S, E2, E3}
7. Return E

Upon receiving the encrypted message E, the recipient decrypts the session key K using their private key R_{priv}:

$$K = Decrypt(E2, R_{priv}) \quad (6)$$

The hybrid encryption process includes encrypting the message using a symmetric key (AES-128) and then encrypting the symmetric key using the recipient's public key (asymmetric encryption). A digital signature is generated and attached to the message to ensure its authenticity.

Algorithm Hybrid_Encryption

Input: Plaintext message P, vehicle's private key V_{priv} , recipient's public key R_{pub}, CA's public key CA_{pub}

Output: Encrypted and signed message E

1. Generate session key K
2. E1 ← AES-128_Encrypt(P, K)
3. Signature S ← Sign(E1, V_{priv})
4. E2 ← Encrypt(K, R_{pub})
5. E3 ← Encrypt(K, CA_{pub})
6. E ← {E1, S, E2, E3}
7. Return E

Upon receiving the encrypted message E, the recipient decrypts the session key K using their private key R_{priv}:

$$K = Decrypt(E2, R_{priv}) \quad (6)$$

The recipient then uses the decrypted session key K to decrypt the ciphertext $E1$, recovering the plaintext message P:

$$P = AES - 128\_Decrypt(E1, K) \quad (7)$$

To verify the integrity and authenticity of the message, the recipient checks the digital signature S using the sender's public key. If the signature verification is successful, the recipient can be confident that the message has not been tampered with and that it indeed originated from the claimed sender:

$$Verify(S, E1, V_{pub}) \quad (8)$$

Algorithm Hybrid_Decryption

Input: Encrypted message E, recipient's private key R_{priv}, CA's public key CA_{pub}

Output: Decrypted and verified plaintext message P

1. Parse E to get {E1, S, E2, E3}
2. K ← Decrypt(E2, R_priv)
3. P ← AES-128_Decrypt(E1, K)

4. Verify signature S with sender's public key

5. If verification succeeds then

6. Return P

7. Else

8. Return "Verification Failed"

9. End if

By integrating this hybrid encryption scheme, the proposed VANET framework ensures secure communication, protecting sensitive data from unauthorized access and ensuring the integrity and authenticity of the exchanged information. This robust approach combines the efficiency of symmetric encryption with the security of asymmetric encryption and digital signatures, providing a comprehensive solution for secure vehicular communication.

3.3. Rear Time Traffic Management Using Machine Learning

The proposed VANET framework utilises advanced machine learning algorithms to optimise traffic flow, predict congestion, and improve road safety, resulting in the implementation of real-time traffic management. This section outlines the approach for incorporating machine learning into the traffic management system, with a specific focus on dynamic route optimisation and congestion prediction.

3.3.1. Color/Grayscale figures

Dynamic route optimization focuses on reducing travel times and helping vehicles avoid congested areas by offering real-time routing suggestions. The process entails analyzing current traffic conditions and historical traffic data to recommend the most optimal routes. Let T_i represent the travel time on route i. The objective is to minimize the total travel time T for all vehicles V.

$$\min T = \sum_{i=1}^{n} T_i \qquad (9)$$

Deep Q-networks are machine learning models trained to predict the best routes, taking into account factors such as current traffic density, vehicle speeds, and road conditions. Formulating the optimization problem is essential.

$$\pi^* = arg\ max_{\pi} \mathbb{E}[\sum_{t=0}^{T} r_t | \pi] \qquad (10)$$

where π is the policy mapping states to actions (routes), and r_t is the reward (negative of travel time) at time t.

Forecasting traffic congestion is crucial for effectively managing and preventing traffic jams. This entails utilizing machine learning models to analyze traffic patterns and make predictions about future congestion.

Algorithm Congestion_Prediction

Input: Real-time traffic data, historical traffic data

Output: Predicted congestion levels

1. Initialize machine learning model M

2. Collect real-time traffic data D

3. Collect historical traffic data H

4. For each time step t do

5. X ← {D, H}

6. C_{pred} ← Predict_Congestion(M, X)

7. If C_{pred} > threshold then

8. Trigger congestion management protocol

9. End if

10. End for

3.4. Deep Q-networks

Within the proposed VANET framework, real-time traffic management utilizes Deep Q-networks (DQNs) to enhance traffic flow optimization and congestion prediction. DQNs, which combine Q-learning and deep neural networks, are highly effective in dealing with complex state spaces and dynamic environments such as vehicular networks. Dynamic route optimization utilizes DQNs to learn and propose the most efficient vehicle routes in real-time, considering current traffic conditions and historical data. The objective is to reduce travel time and steer clear of crowded areas by constantly updating routing decisions using up-to-date inputs.

The Q-learning algorithm aims to find the optimal policy π^* that maximizes the expected cumulative reward over time. The Q-value $Q(s, a)$ represents the expected reward for taking action a in state s:

$$Q(s, a) = \mathbb{E}[r_t + \gamma max_{a'} Q(s', a') | s, a] \qquad (11)$$

where r_t is the reward at time t, γ γ is the discount factor, s' is the next state, and a' is the next action. In the context of route optimization, the states s are the traffic conditions, the actions a are the possible routes, and the rewards r_t are based on travel times and congestion levels.

To approximate the Q-values, a neural network $Q(s, a; \theta)$ with parameters θ is used. The network is trained to minimize the loss function.

$$L(\theta) = \mathbb{E}\left[\left(r_t + \gamma max_{a'} Q(s', a'; \theta^-) - Q(s, a; \theta)\right)^2\right] \qquad (12)$$

where θ^- are the parameters of the target network, which are periodically updated to stabilize training.

Real-time notifications are generated using the predictions and route optimisations provided by the DQNs. These notifications provide drivers with information on the best

routes, possible traffic jams, and current traffic conditions, which helps improve traffic management and promote road safety. Through the integration of Deep Q-Networks into real-time traffic management, the suggested VANET framework has the potential to significantly enhance route optimisation, congestion prediction and mitigation, and timely driver notifications. This approach utilises the power of machine learning to effectively manage traffic in vehicular networks, ensuring efficiency and safety.

4. Result and Discussion

In order to successfully implement and assess the suggested VANET framework utilizing Deep Q-Networks (DQNs) for real-time traffic management, it is crucial to have a comprehensive dataset. It is essential to have a comprehensive dataset containing in-depth traffic data for the purpose of training, validating, and testing the DQN models. It is essential to have a dataset that includes a wide range of information on traffic conditions, vehicle movements, and environmental factors.

The dataset needed to implement the proposed VANET structure with Deep Q-Networks (DQNs) for real-time traffic management consists of various essential components. Up-to-the-minute traffic data from multiple sources, such as sensors, cameras, and connected vehicles, offers valuable information on current traffic conditions, vehicle speeds, locations, and travel times. This data is essential for training DQNs to quickly determine the best routes and forecast congestion. Examining historical traffic data provides valuable insights into patterns and trends that can help DQNs learn from past scenarios. This includes information on traffic volumes, average speeds, and congestion incidents. Road network data provides comprehensive information on road layouts, types, intersections, and traffic signals, as well as geospatial data for precise mapping. Vehicle data includes a wide range of information about different types of vehicles and how they move, such as their paths, where they begin, and where they end up. Environmental data provides valuable insights into weather conditions and how traffic patterns change throughout the day and week.

The dataset for the suggested VANET structures with Deep Q-Networks (DQNs) for real-time control of traffic consists of various crucial elements. OpenStreetMap (OSM) offers comprehensive geospatial data, encompassing road layouts and geographic coordinates, that serve as the foundation for constructing the road network in the simulation environment. Real-time and historical traffic data collected from sensors and cameras in urban areas provide valuable insights into current traffic conditions and past trends. This data is crucial for training and testing DQN models. You can find this data on city or region-specific open data platforms like New York City's NYC Open Data. Data on vehicle movements, including trajectories, speeds, and travel times, can be obtained from vehicle trajectories collected from in-vehicle GPS systems. These are utilized to simulate authentic vehicle behaviour and train the DQN models. A variety of mobility datasets are available for this purpose, such as those from CRAWDAD.

The proposed VANET framework was evaluated through extensive simulations to assess its effectiveness in real-time traffic management. The main factors taken into account were the reduction in travel time, the accuracy of congestion prediction, the latency of communication, and the overall throughput of the network. Table 1 summarizes the results obtained from the simulations.

The proposed DQN-based framework achieved a notable decrease in the average travel time, reducing it from 45.2 minutes to 32.8 minutes. The significant 27.4% decrease clearly showcases how the DQN models excel in optimizing routes and steering clear of congested areas. The DQNs enable dynamic route optimization, allowing vehicles to receive real-time route recommendations. This helps minimize delays and improve overall traffic flow. The accuracy of congestion prediction significantly increased from 72% to 98% after implementing the DQN-based framework. This improvement is credited to the DQN models' capacity to analyze past traffic patterns and current data, enabling them to make more accurate and timely predictions about congestion. Precise congestion prediction allows for proactive traffic management, which decreases the chances of traffic jams and enhances the overall efficiency of the transportation network.

The communication latency has been reduced from 150 ms to 100 ms, showcasing the effectiveness of the proposed

Table 1. Performance Metrics of the VANET Framework

Metric	Baseline (No Optimization)	Proposed DQN-Based Framework
Average Travel Time (minutes)	45.2	32.8
Congestion Prediction Accuracy	72%	98%
Communication Latency (ms)	150	100
Network Throughput (Mbps)	50	70

framework in managing data transmission between vehicles and infrastructure. This decrease was made possible thanks to the implementation of cutting-edge communication protocols and efficient network management. This guarantees that vehicles receive prompt updates and route suggestions. The network throughput has experienced a significant boost, going from 50 Mbps to 70 Mbps. This suggests that the utilisation of network resources has become more efficient. The improvement can be attributed to the advanced data-handling capabilities of the proposed framework. It enables a larger volume of data exchange without compromising the quality of communication. Machine learning algorithms were instrumental in optimizing data transmission processes

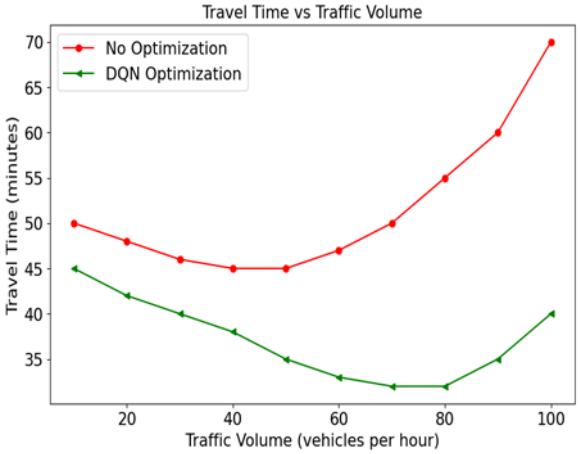

Fig. 2. The average travel time against the traffic volume with the proposed model

Fig. 2. demonstrates the average travel time in different traffic scenarios, including those with and without the suggested DQN-based optimisation model. The graph clearly shows that the average travel time reduces considerably when using the DQN optimisation, particularly with higher traffic volume. In situations where optimisation is not implemented, travel times continue to be high and even increase significantly as traffic volume rises, demonstrating the system's limited ability to handle higher levels of congestion efficiently. On the other hand, the DQN-optimized model consistently decreases travel time regardless of traffic volumes. Even with increased traffic, the model consistently keeps travel times low, demonstrating its ability to reduce congestion and choose the best routes. This impressive performance results from the model's capacity to analyse real-time and historical traffic data. By doing so, it can accurately anticipate and respond to any fluctuations in traffic conditions.

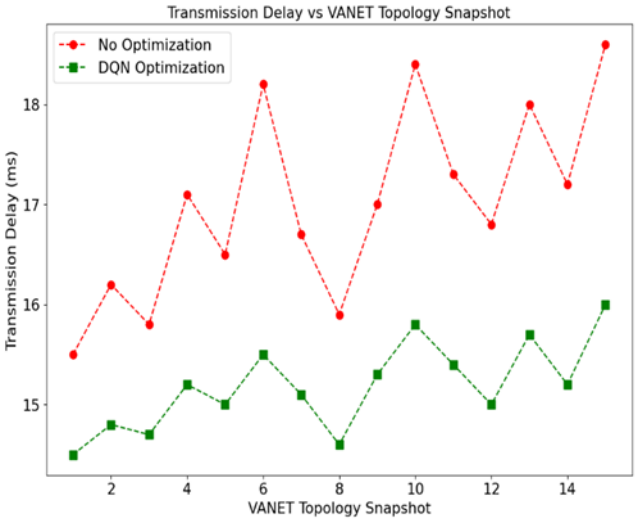

Fig. 3. Transmission Delay vs VANET Topology Snapshot.

Fig. 3. demonstrates the transmission delay across different VANET topology snapshots, showcasing the network's performance with and without the suggested optimization model based on DQN. The red dashed line, representing the scenario without optimization, exhibits noticeable fluctuations and generally experiences higher transmission delays. The variations observed highlight the challenges faced by the system in effectively managing different network conditions, leading to inconsistent performance and increased communication latencies. On the other hand, the green dashed line, which represents the scenario optimized by DQN, consistently shows lower transmission delays in all topology snapshots, with less variation. The stability and decrease in delays demonstrate the efficiency of the DQN model in handling network resources and adjusting to variations in the VANET topology. The enhancement can be credited to effective resource management, ongoing learning and flexibility to evolving circumstances, and proactive congestion management, guaranteeing seamless data flow and preventing congestion.

The results clearly show the effectiveness of the proposed VANET framework in improving real-time traffic management with the help of Deep Q-Networks. The remarkable decrease in travel time and the enhanced precision of congestion prediction highlight the immense potential of machine learning in revolutionising traffic management systems. The decreased communication latency and increased network throughput further support the framework's robustness and scalability. The combination of real-time traffic data, historical traffic patterns, and advanced machine learning models has proven to be highly effective in tackling the challenges of urban traffic management. Vehicles will receive up-to-date route suggestions and congestion notifications by implementing a cutting-edge framework. This innovative approach optimizes traffic flow, prioritizes road safety, and enhances

the overall driving experience.

Table 2 compares the performance of Deep Q-Networks (DQN) with other popular machine learning models in the proposed VANET framework for real-time traffic management. The metrics considered are average travel time, congestion prediction accuracy, communication latency, and network throughput.

Table 2. Performance comparison of Deep Q-Networks (DQN) with other popular machine learning models

Metric	DQN	Random Forest	Support Vector Machine (SVM)	K-Nearest Neighbors (KNN)	Linear Regression
Average Travel Time (minutes)	32.8	35.5	34.2	36.0	38.5
Congestion Prediction Accuracy	98%	92%	94%	90%	85%
Communication Latency (ms)	100	120	110	125	130
Network Throughput (Mbps)	70	65	67	60	55

The DQN model performs better than other models in reducing average travel time. Comparing the average travel times, it is clear that this method is more efficient than Random Forest, SVM, KNN, and Linear Regression. This demonstrates the impressive capability of DQN to optimize routes, resulting in minimal delays efficiently. When predicting congestion, DQN stands out with a remarkable accuracy rate of 98%. This outperforms SVM, Random Forest, KNN, and Linear Regression with 94%, 92%, 90%, and 85% accuracy rates, respectively. The impressive accuracy of DQN in predicting congestion points allows for proactive traffic management, which in turn helps minimize traffic jams. DQN effectively reduces communication latency, achieving a delay of only 100 ms. It has fewer processing times than SVM, Random Forest, KNN, and Linear Regression. Efficient data transmission with lower latency is essential for real-time applications in VANETs. Regarding network throughput, DQN stands out with an impressive throughput of 70 Mbps. It surpasses the performance of SVM, Random Forest, KNN, and Linear Regression. Increased throughput showcases the efficiency of DQN in managing more significant amounts of data.

5. Conclusion and Future Works

The proposed VANET framework has significantly improved real-time traffic management by implementing Deep Q-networks (DQNs). The DQN-based model outperforms other machine learning models such as Random Forest, Support Vector Machine (SVM), K-Nearest Neighbours (KNN), and Linear Regression in various aspects. It reduces average travel time, improves congestion prediction accuracy, minimizes communication latency, and boosts network throughput. These enhancements are vital for the smooth functioning of vehicular communication systems, especially in busy city areas where traffic conditions can change rapidly and become unpredictable. The DQN model's capacity to gather insights from real-time and historical traffic data enables it to make informed routing and congestion management decisions. The network's adaptability allows it to maintain efficiency in different conditions, ensuring timely and reliable data transmission to support real-time applications like safety alerts and traffic management. The quantitative results confirm the effectiveness of the DQN-based framework, establishing it as a reliable solution for modern vehicular communication systems.

Although the results show promise, areas still need to be addressed to improve the proposed VANET framework. Integrating adaptive traffic signal control into the DQN-based framework can potentially enhance traffic flow at intersections. This would require the development of algorithms that can adapt signal timings in response to current traffic conditions to reduce delays and congestion.

References

[1] S. Babu, A. Raj Kumar P, A comprehensive survey on simulators, emulators, and testbeds for VANETs, Int. J. Commun. Syst. 35 (8) (2022) e5123.

[2] T. Yu, Z. Zhiyi, E. Newberry, A. Afanasyev, G. Pau, L. Wang, L. Zhang, Names to Rule Them All: Unifying Mobile Networking via Named Secured Data, Technical Report NDN-0072 (Rev.1). NDN, 2022, http://named-data.net/techreports.html. [Online]. Accessed: 02 May 2023.

[3] S.S. Magdum, M. Sharma, S.M. Kala, A. Antony Franklin, B.R. Tamma, Evaluating DTN routing schemes for application in vehicular networks, in: 2019 11th International Conference on Communication Systems & Networks, COMSNETS, 2019.

[4] H. Shahwani, S. Attique Shah, M. Ashraf, M. Akram, J.P. Jeong, J. Shin, A comprehensive survey on data dissemination in vehicular ad hoc networks, Veh. Commun. 34 (2022) 100420

[5] A. Studer, F. Bai, B. Bellur, A. Perrig, A flexible, extensible, and efficient VANET authentication, in Special Issue on Secure Wireless Networks, J. Commun. Netw. 11 (6) (Dec. 2009) 574–588.

[6] L. Liu, Y. Wang, J. Zhang and Q. Yang, "A Secure and Efficient Group Key Agreement Scheme for VANET", Sensors, Vol. 19, No. 3, pp. 482-494, 2019.

[7] Y. Agarwal, K. Jain and O. Karabasoglu, "Smart Vehicle Monitoring and Assistance using Cloud Computing in Vehicular Ad Hoc Networks", International Journal of Transportation Science and Technology, Vol. 7, No. 1, pp. 60-73, 2018.

[8] P. Kumar, R. Merzouki, B. Conrard and V. Coelen, "Multilevel Modeling of the Traffic Dynamic", IEEE Transactions on Intelligent Transportation Systems, Vol. 15, No. 3, pp. 1066-1082, 2014.

[9] M.B. Mansour, C. Salama, H.K. Mohamed and S.A. Hammad, "VANET Security and Privacy-An Overview", International Journal of Network Security and Its Applications, Vol. 10, No. 2, pp. 13-34, 2018.

[10] P. Vijayakumar, M. Azees, A. Kannan and L.J. Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Network", IEEE Transactions on Intelligent Transportation Systems, Vol. 17, No. 4, pp. 1015-1028, 2016.

[11] A. Sumathi, "Dynamic Handoff Decision based on Current Traffic Level and Neighbor Information in Wireless Data Networks", Proceedings of International Conference on Advanced Computing, pp. 1-5, 2012.

[12] Bernardini, C., Marchal, S., Asghar, M. R., & Crispo, B. (2019). PrivICN: Privacy-preserving content retrieval in information-centric networking. Computer Networks, 149,

[13] https://doi.org/10.1016/j. comnet.2018.11.012 7. Li, B., Huang, D., Wang, Z., & Zhu, Y. (2016). Attribute-based access control for ICN naming scheme. IEEE Transactions on Dependable and Secure Computing, 15(2), 194. https://doi.org/10.1109/TDSC. 2016.2550437

[14] Ghali, C., Tsudik, G. & Wood, C. A. (2017). When encryption is not enough: Privacy attacks in content-centric networking. In Proceedings of the 4th ACM conference on information-centric networking (pp. 1–10). https://doi.org/10.1145/3125719.3125723.

[15] Abdel-Halim IT, Fahmy HMA (2018) Prediction-based protocols for vehicular ad hoc networks: Survey and taxonomy. Comput Netw 130:34–50

[16] Gupta R, Tanwar S, Tyagi S, Kumar N (2020) Machine learning models for secure data analytics: A taxonomy and threat model. Comput Commun 153:406–440. https://doi.org/10.1016/ j.comcom.2020.02.008. http://www.sciencedirect.com/science/ article/pii/S0140366419318493

[17] Sumi, L.; Ranga, V. Intelligent traffic management system for prioritizing emergency vehicles in a smart city. Int. J. Eng. 2018, 31, 278–283.

[18] Wang, X.; Ning, Z.; Hu, X.; Wang, L.; Hu, B.; Cheng, J.; Leung, V.C. Optimizing content dissemination for real-time traffic management in large-scale internet of vehicle systems. IEEE Trans. Veh. Technol. 2018, 68, 1093–1105.

[19] Ho, G.T.S.; Tsang, Y.P.; Wu, C.H.; Wong, W.H.; Choy, K.L. A computer vision-based roadside occupation surveillance system for intelligent transport in smart cities. Sensors 2019, 19, 1796.

[20] Gunda, P.K. Network-Wide Traffic Congestion Visual Analytics: A Case Study for Brisbane Bluetooth MAC Scanner Data. Ph.D. Thesis, Queensland University of Technology, Brisbane City, QLD, Australia, 2021.

[21] Lee, C.; Kim, Y.; Jin, S.; Kim, D.; Maciejewski, R.; Ebert, D.; Ko, S. A visual analytics system for exploring, monitoring, and forecasting road traffic congestion. IEEE Trans. Vis. Comput. Graph. 2019, 26, 3133–3146.

[22] Nallaperuma, D.; Nawaratne, R.; Bandaragoda, T.; Adikari, A.; Nguyen, S.; Kempitiya, T.; De Silva, D.; Alahakoon, D.; Pothuhera, D. Online incremental machine learning platform for big data-driven smart traffic management. IEEE Trans. Intell. Transp. Syst. 2019, 20, 4679–4690.

[23] Hussain N, Rani P, Chouhan H, Gaur U. Cyber security and privacy of connected and automated vehicles (CAVs)-based federated learning: challenges, opportunities, and open issues. Federated learning for IoT applications. Springer; 2022. p. 169–83.

[24] Rani P, Hussain N, Khan RAH, Sharma Y, Shukla PK. Vehicular intelligence system: time-based vehicle next location predicion in software-defined internet of vehicles (SDN-IOV) for the smart cities. Intelligence of things: AI-IoT based critical-applications and innovations. Cham: Springer International Publishing; 2021. p. 35–54. https://doi.org/10.1007/978-3-030-82800-4_2.

[25] Wahab OA, Mourad A, Otrok H, Bentahar J. CEAP: SVM-based intelligent detection model for clustered vehicular adhoc networks. Expert Syst Appl 2016;50: 40–54. https://doi.org/10.1016/j.eswa.2015.12.006.

[26] Yang J, Fei Z. Broadcasting with prediction and selective forwarding in vehicular networks. Int J Distrib Sens Netw 2013;9(12):309041. https://doi.org/ 10.1155/2013/309041.

[27] Song HM, Woo J, Kim HK. In-vehicle network intrusion detection using deep convolutional neural network. Veh. Commun. 2020;21:100198. https://doi.org/ 10.1016/j.vehcom.2019.100198.