RESEARCH ARTICLE WWW.PECEJOURNAL.COM

Vehicular Ad-Hoc Networks (VANETs) for Enhancing Road Safety and Efficiency

Rozman Zakaria[1], F. Mohd Zaki[2]

[1,2]*Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia*

KEYWORDS:
Vehicular Ad-Hoc Networks (VANETs),
Road safety;
Traffic efficiency;
Vehicle-to-Vehicle communication (V2V);
Vehicle-to-Infrastructure communication (V2I);
Intelligent Transportation Systems (ITS);
Real-time traffic data

ARTICLE HISTORY:
Received : 19.11.2024
Revised : 22.12.2024
Accepted : 15.03.2025

https://doi.org/10.31838/ECE/02.01.03

Abstract

Vehicular Ad-Hoc Networks (VANETs) represent an innovative technology poised to significantly enhance road safety and efficiency. VANETs, a specialized form of mobile ad-hoc networks (MANETs), enable direct communication between vehicles (Vehicle-to-Vehicle or V2V) and between vehicles and roadside infrastructure (Vehicle-to-Infrastructure or V2I). Utilizing wireless communication, VANETs facilitate the real-time exchange of critical information such as traffic conditions, road hazards, and emergency notifications.The primary objective of VANETs is to improve road safety. By enabling instant communication, vehicles can warn each other about potential hazards, sudden braking, or adverse weather conditions, thus preventing accidents. VANETs support cooperative systems for collision avoidance and emergency response, significantly enhancing drivers' situational awareness and reaction times. This communication framework also supports automated safety applications, crucial for the development and deployment of autonomous vehicles.In terms of efficiency, VANETs contribute to optimizing traffic flow by providing up-to-date information on traffic congestion, roadblocks, and optimal routing. This real-time data helps reduce travel times, fuel consumption, and emissions, promoting a more sustainable and efficient transportation system. Additionally, VANETs facilitate the development of Intelligent Transportation Systems (ITS), which integrate traffic management with advanced data analytics to improve overall transportation infrastructure.As technology continues to evolve, VANETs are expected to play a crucial role in the advancement of smart cities and autonomous driving, fostering a future of connected, intelligent, and safer roadways.

Author's email: rozman.zak@ukm.edu.my, zaki.f.m@ukm.edu.my

How to cite this article: Zakaria R, Zaki MF. Vehicular Ad-Hoc Networks (VANETs) for Enhancing Road Safety and Efficiency, Journal of Progress in Electronics and Communication Engineering Vol. 2, No. 1, 2025 (pp. 27-38).

Introduction:

With the rise in vehicular traffic and diverse requests for various services, ensuring optimal resource utilization and addressing growing needs remain a challenge for vehicular ad-hoc networks (VANETs).[1] Modern intelligent transportation systems leverage cutting-edge communication technologies to enhance transportation efficiency, accident prevention, and pedestrian comfort by enabling vehicles and road infrastructure to exchange entertainment and traffic information,[1-6] VANETs promise to revolutionize road safety and efficiency through advanced routing protocols like dynamic source routing, addressing key issues like bandwidth constraints, latency, quality of service, and network security.[1-6] This article explores the VANET architecture, components, connectivity challenges, mobility modeling, and security considerations, while delving into future research directions for seamless vehicular communication networks.[1-7]

Vehicular Ad-hoc Network (VANET) Overview

A Vehicular Ad-hoc Network (VANET) comprises a group of moving or stationary vehicles connected by a wireless network.[1] VANETs play a vital role in providing safety and comfort to drivers in vehicular environments by offering a range of services, including traffic control, entertainment, safety applications, driving assistance, collision avoidance, and safety services.[3] However, due to the potential for deadly traffic problems and significant delays for travelers, VANET developers prioritized the transmission of c rucial safety-related information.[3]

In recent years, economic and population growth have led to a rapid increase in the number of vehicles on the road, consequently increasing road accidents, driver exhaustion, and deterioration of roads and support infrastructure.[1] According to a healthcare report by the World Health Organization (WHO), road accidents are the leading cause of death for people aged 15–29 years, with 1.3 million people killed in accidents annually worldwide. [1] This rapid rise in traffic accidents can be mitigated by leveraging the latest technology to provide real-time information to drivers about vehicle health parameters, road conditions, traffic jams, and weather warnings.[1]

A. Key Characteristics

1. **Communication Models**: The two main communication models in VANETs are classified as Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I).[1] V2V communication enables the exchange of transmissions between different vehicles, while V2I facilitates communication between vehicles and the road-side infrastructure.[1] The main communication module consists of a Road-Side Unit (RSU), an on-board unit (OBU), and a trusted authority (TA), where the RSU unit is a fixed transceiver that sends and receives information from the OBU and TA.[1]
2. **Mobility and Network Fragmentation**: Due to the high mobility of VANET nodes, it is often necessary for them to leave the localized network and participate in new configurations, potentially causing intrinsic communication interruptions or reduced throughput in V2V and V2I communications.[1, 5] Additionally, the VANET network configuration continuously evolves as vehicles join and leave the network, creating opportunities for malicious nodes to compromise the network by hiding their routes.[6] Furthermore, VANET disconnections can occur due to other factors such as high-speed movement between vehicles, weather conditions, and a high density of vehicles on the road.[1, 8]
3. **Bandwidth and Processing Power**: The information exchange within VANETs depends on the users connected at a particular time, requiring adequate network bandwidth and processing power to store, process, and communicate important messages.[1]
4. **Real-Time Communication**: Regardless of the inherent delays between mobile platforms, some VANET applications, such as fault detection and collision prevention systems, require real-time information delivery, as drivers have minimal reaction time (several milliseconds) available to decode and react to received messages.[1]

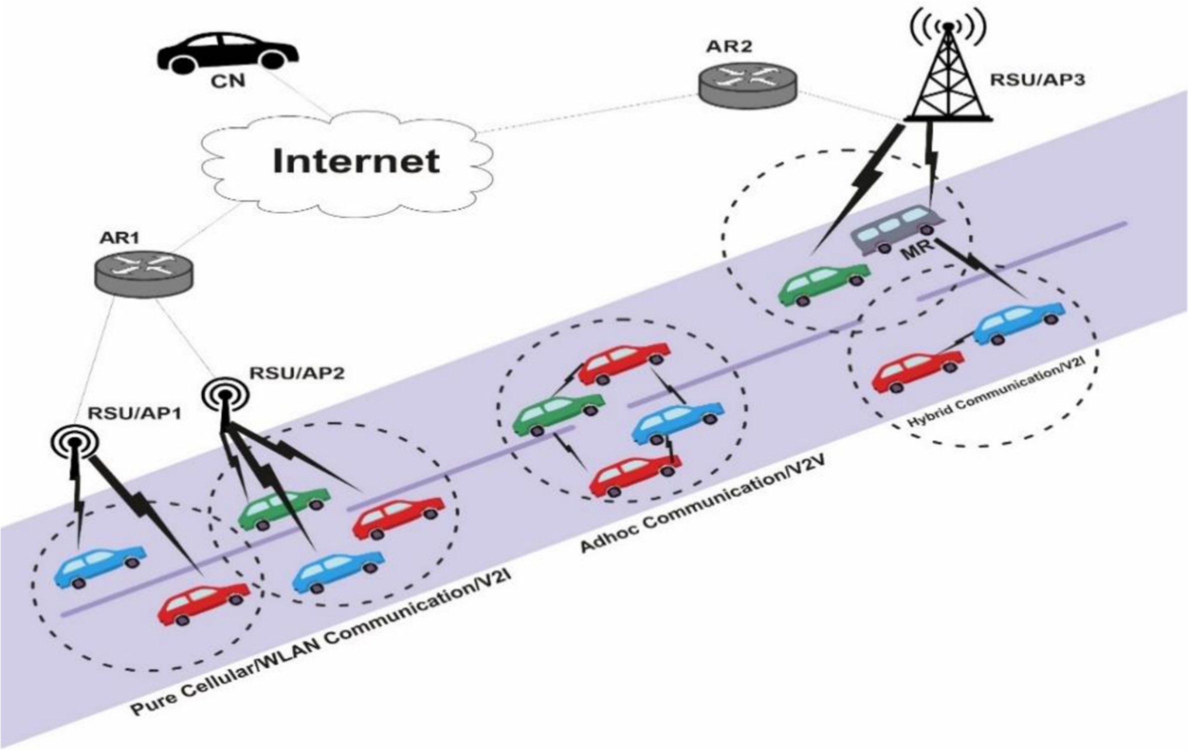


Fig. 1: Analysis of Intra-Domain Handoff

5. **Heterogeneity and Scalability**: A VANET comprises numerous nodes with varying properties and functions, including stationary RSUs and mobile vehicles, with some vehicles requiring the communication of entertainment information and others needing the exchange of safety-related information.[3] Additionally, VANET connections can span small cities, multiple towns, or large cities and countries, making scalability a significant challenge in automotive communications.[3]
6. **Unlimited Power and Computing Resources**: The communication between nodes in the VANET network is not restricted by power or storage limitations, as OBUs embedded in vehicles operate on continuous and unlimited energy sources from vehicle batteries.[3]
7. **Spectrum Scarcity:** Wireless technology standards for automotive networks, such as Wireless Access in Vehicular Environments (WAVE) and Dedicated Short-Range Communications (DSRC), have exhibited reliability and scalability issues in large-scale dense vehicular networks, according to recent research studies.[3]
8. **Environmental Effects**: In a VANET, all communication occurs outdoors, where the environment's impact on electromagnetic signals is relatively high.[3] Buildings, vehicles, trees, and other objects can interfere with these signals as they travel through the air, resulting in various signal disturbances, including multipath propagation, channel fading, and signal shadowing.[3]
9. **Accuracy of Information:** Several data delivery mechanisms in the VANET environment rely on positional information from navigation systems like GPS and GNSS, which are unable to provide precise location data.[3]
10. **Fault Tolerance and Data Security**: Real-time communication is a critical requirement for various safety-related services in VANETs, and any inaccuracies could result in further delays in data distribution, potentially causing traffic jams and accidents.[3] Additionally, data must be presented securely to ensure efficient and trustworthy communication management, with packets remaining unaltered during transmission and encrypted to prevent unauthorized access.[3]

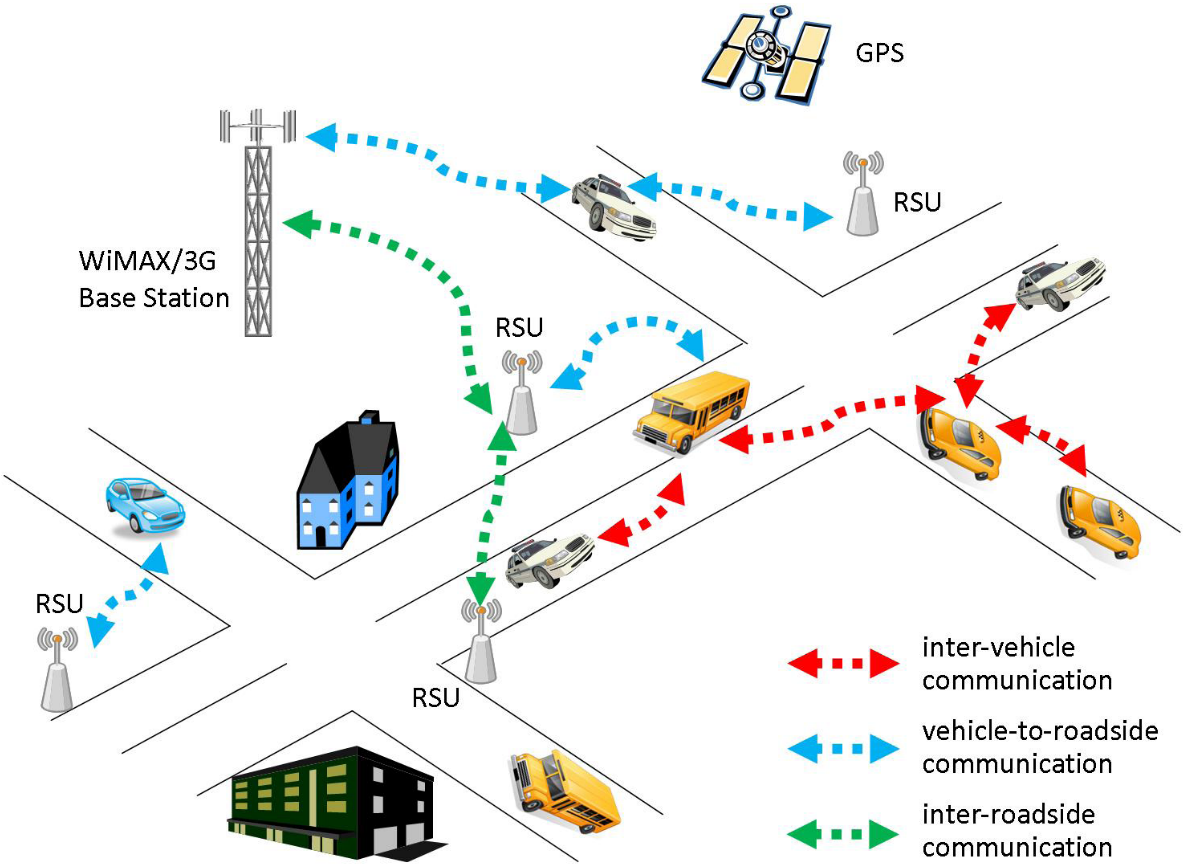

GPS
WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig. 2: **Vehicular Ad-Hoc Network**

11. **Data Privacy**: Many consumers are concerned about sharing their vehicle information or having it used to track their destinations, making data privacy one of the most crucial issues that must balance the public's desire for services with high levels of privacy.[3]

1. VANET Architecture and Components

A VANET comprises several components that facilitate communication among vehicles and with the roadside infrastructure. The main components are classified into three domains: the mobile domain, the infrastructure domain, and the generic domain.[11]

A. Mobile Domain

The mobile domain consists of two parts: the vehicle domain and the mobile device domain.[11]

1. **Vehicle Domain**: This domain includes all types of vehicles, such as cars, buses, and trains.[11]
2. **Mobile Device Domain**: This domain encompasses all kinds of portable devices, such as smartphones, personal navigation devices, laptops, and smartwatches.[11, 13]

B. Infrastructure Domain

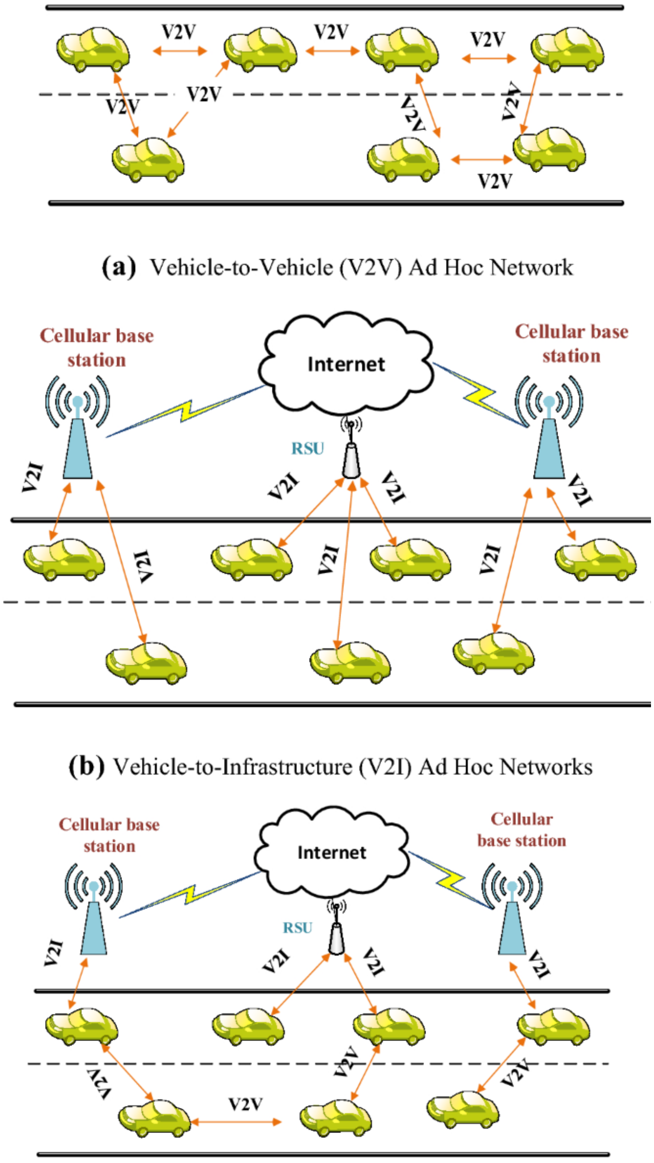
The infrastructure domain is divided into two parts: the roadside infrastructure domain and the central infrastructure domain.[11]

1. **Roadside Infrastructure Domain**: This domain includes roadside unit (RSU) entities like traffic lights, cameras, and other components equipped with communication capabilities. RSUs are wave devices typically fixed along the roadside or at dedicated locations like junctions or parking spaces. They are equipped with network devices for dedicated short-range communication based on IEEE 802.11p radio technology and can also have other network devices for communication within the infrastructural network.[11, 13]
2. **Central Infrastructure Domain**: This domain comprises infrastructure management centers, such as Traffic Management Centers (TMCs) and Vehicle Management Centers (VMCs).[11, 13]

C. Communication Types (V2V, V2I, etc.)

VANET communications are categorized into several types:[11]

1. **In-Vehicle Communication**: This refers to the communication between the On-Board Unit (OBU) of the vehicle and its Application Units (AUs).[11]
2. **Vehicle-to-Vehicle (V2V)**: This involves wireless communication between vehicles via their OBUs, either directly or through multi-hop communication.[9,11,13]
3. **Vehicle-to-Infrastructure (V2I)**: This refers to bidirectional wireless communication between vehicles and infrastructure-connected RSUs.[9, 11]
4. **Infrastructure-to-Infrastructure (I2I)**: This communication occurs between RSUs, enabling the extension of the network's coverage.[11]
5. 5. **Vehicle-to-Broadband Cloud (V2B)**: This



(a) Vehicle-to-Vehicle (V2V) Ad Hoc Network

(b) Vehicle-to-Infrastructure (V2I) Ad Hoc Networks

(c) Hybrid VANET architecture

Fig. 3: Hybrid opportunistic and position-based routing protocol

involves communication between vehicles and broadband cloud services via wireless broadband technologies like 3G, 4G, or 5G.[11, 14]

The OBU is a wave device mounted on each vehicle, used for exchanging information with RSUs and other OBUs. It comprises a Resource Command Processor (RCP) for storing and retrieving information, a user interface for linking with other OBUs, and network devices for short-range communication based on IEEE 802.11p radio technology.[14]

By leveraging these components and communication types, VANETs enable various applications, such as traffic management, safety services, and infotainment, ultimately enhancing road safety and efficiency.[1-14]

D. Routing Protocols in VANETs

Routing in Vehicular Ad-Hoc Networks (VANETs) is a challenging task due to the highly dynamic nature of the network topology, caused by the high mobility of vehicles.[25] The routing protocols in VANETs can be broadly classified into the following categories:

Topology-based Routing

Topology-based routing protocols rely on the knowledge of the network topology to forward data packets. They can be further classified into proactive, reactive, and hybrid protocols.[25]

- **Proactive Protocols**: These protocols maintain up-to-date routing information by periodically exchanging control messages among nodes, even when there is no data traffic. Examples include Optimized Link State Routing (OLSR) and Destination-Sequenced Distance-Vector (DSDV) protocols.[25]
- **Reactive Protocols**: These protocols establish routes on-demand when a node needs to transmit data. Route discovery is initiated only when necessary, reducing the control overhead. Examples include Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols.[25]
- • **Hybrid Protocols**: These protocols combine the advantages of both proactive and reactive protocols. They maintain routing information for nearby nodes proactively and discover routes reactively for distant nodes. Examples include Zone Routing Protocol (ZRP) and Hybrid Ad-hoc Routing Protocol (HARP).[25]

Position-based Routing

Position-based routing protocols use the geographic position of vehicles to make forwarding decisions. They do not require the maintenance of a routing table or the establishment of a complete end-to-end path.[25]

- **Greedy Forwarding**: In this approach, a node forwards the packet to the neighbor closest to the destination. Examples include Greedy Perimeter Stateless Routing (GPSR) and Geographic Source Routing (GSR).[25]
- **Non-Greedy Forwarding**: In this approach, a node selects the next hop based on additional criteria, such as link quality or vehicle mobility. Examples include Anchor-Based Street and Traffic Aware Routing (A-STAR) and Directional Greedy Routing (DGR).[25]

Cluster-based Routing

Cluster-based routing protocols group vehicles into clusters based on certain criteria, such as vehicle speed, direction, or position. Cluster heads are responsible for intra-cluster and inter-cluster communication.[25]

- **Mobility-Based Clustering**: Vehicles are clustered based on their mobility patterns, such as speed and direction. Examples include Clustering for Open IVC Network (COIN) and Robust Vehicular Routing (ROVER).[25]
- **Position-Based Clustering:** Vehicles are clustered based on their geographic positions. Examples include Location-Based Clustering Algorithm (LBCA) and Distributed Mobility-Adaptive Clustering (DMAC).[25]

Broadcast Routing

Broadcast routing protocols are used to disseminate information to all vehicles in the network. They are essential for safety applications, such as accident or traffic jam notifications.[25]

- **Simple Flooding**: In this approach, each node rebroadcasts the received message to all its neighbors. However, this can lead to the broadcast storm problem.[25]
- **Probability-Based Techniques**: These techniques use probabilistic methods to reduce the number of rebroadcasts. Examples include Weighted p-Persistent Broadcasting and Distributed Optimized Time Slot Assignment.[25]
- **Area-Based Techniques**: These techniques limit the rebroadcast area based on the message's

relevance. Examples include Multi-Hop Vehicular Broadcast (MHVB) and Urban Multi-Hop Broadcast (UMB).[25]

Geocast Routing

Geocast routing protocols are used to deliver messages to all vehicles within a specific geographic area. They are useful for location-based services and emergency applications.[25]

- **Flooding-Based Geocast**: In this approach, the message is flooded within the geocast region. Examples include Location-Based Multicast (LBM) and Robust Geocast (RG).[25]
- **Forwarding-Based Geocast**: In this approach, the message is forwarded to nodes within the geocast region using a forwarding strategy. Examples include Distributed Robust Geocast (DRG) and Intersections-Based Geographical Routing Protocol (IGRP).[25]

These routing protocols aim to address the unique challenges of VANETs, such as high mobility, dynamic topology, and intermittent connectivity, while ensuring efficient and reliable data dissemination for various applications.[25]

Signal Propagation and Channel Modeling

A. Basic Propagation Mechanisms

Recent empirical studies have shown that correctly modeling the vehicular channel is imperative for realistic evaluation of VANET applications.[25] This is particularly the case for safety applications, where the correct reception of a single message can help avoid an accident. [29] We start by describing the basic propagation mechanisms that enable wireless communication.[29] Wireless communication relies on the propagation of electromagnetic waves through various mediums, including air, buildings, and other obstacles. [29] The propagation mechanisms can be classified into three main categories: reflection, diffraction, and scattering. [29]

1. **Reflection**: When an electromagnetic wave encounters a smooth surface larger than its wavelength, it reflects off the surface, creating a reflected wave.[29] The angle of reflection is equal to the angle of incidence, following the laws of geometric optics.[29]
2. **Diffraction**: When an electromagnetic wave encounters an obstacle with sharp edges, it bends around the edges, creating a diffracted wave. [29] This phenomenon is described by the Huygens-Fresnel principle and is essential for understanding signal propagation in urban environments with buildings and other obstacles.[29]
3. **Scattering**: When an electromagnetic wave encounters a rough surface or an object with dimensions comparable to or smaller than its wavelength, it is scattered in multiple directions, creating scattered waves.[29] Scattering is particularly relevant in environments with foliage, buildings, and other irregularities.[29]

These basic propagation mechanisms, along with other factors such as path loss, fading, and shadowing, contribute to the overall behavior of the wireless channel in vehicular environments.[29]

B. Vehicular Channel Modeling Considerations

Modeling the vehicular channel accurately requires considering various factors specific to the VANET environment.[29] These factors include:

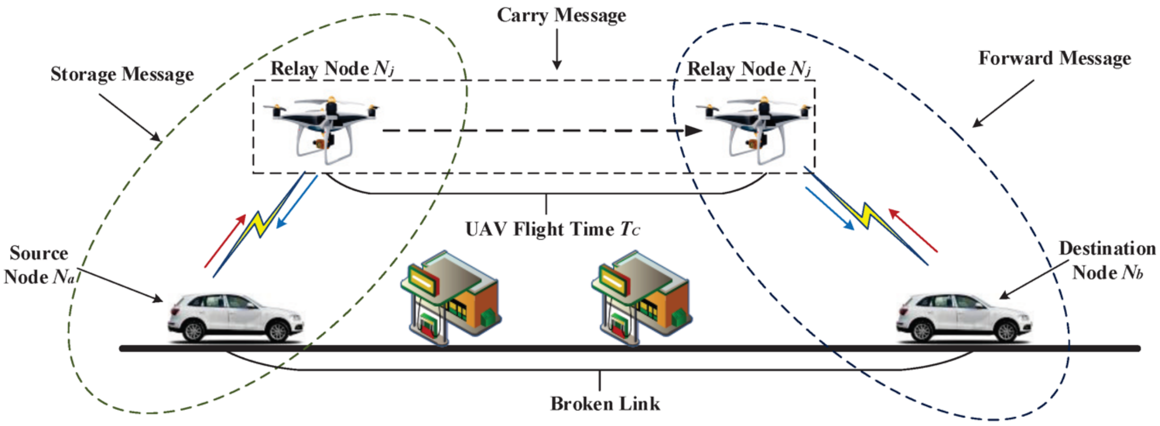


Fig. 4: A Relay Selection Protocol for UAV-Assisted VANETs

1. **Diverse Environments**: Vehicular communication takes place in various environments, such as urban areas, highways, rural areas, and tunnels.[29] Each environment has unique characteristics that impact signal propagation, such as the presence of buildings, foliage, and other obstacles.[29]
2. **Mobility and Dynamic Environments**: The high mobility of vehicles and the dynamic nature of the environment, with vehicles constantly entering and leaving the communication range, pose challenges for channel modeling.[29] Doppler shifts and time-varying channel conditions must be accounted for.[29]
3. **Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) Conditions:** In vehicular environments, the communication link can be either LOS or NLOS, depending on the presence of obstacles between the transmitter and receiver.[29] NLOS conditions can significantly impact signal propagation, leading to increased path loss and multipath effects.[29]
4. **Multipath Propagation**: In urban environments, the presence of buildings, vehicles, and other obstacles creates multiple propagation paths for the signal, leading to multipath fading and intersymbol interference.[29] Accurate modeling of multipath propagation is crucial for reliable communication.[29]
5. **Vehicular Obstructions**: Vehicles themselves can act as obstacles, blocking or attenuating the signal propagation between other vehicles or between vehicles and infrastructure nodes.[29] This effect is particularly relevant in dense traffic scenarios.[29]
5. 6. **Antenna Characteristics:** The antenna characteristics, such as radiation pattern, polarization, and placement on the vehicle, can significantly impact the signal propagation and channel characteristics.[29]

C. Channel Modeling Approaches

To address the unique challenges of vehicular channel modeling, various approaches have been proposed in the literature.[29] These approaches can be classified based on different criteria, such as the propagation mechanism scale, modeling approach, and suitability for a particular environment.[29]

1. **Large-Scale Propagation Models**: These models focus on characterizing the path loss and shadowing effects over large distances.[29] Examples include the Okumura-Hata model, the WINNER+ model, and the GEMV2 model.[29]
2. **Small-Scale Fading Models:** These models characterize the rapid fluctuations in the received signal strength over short distances or time intervals, caused by multipath propagation and Doppler shifts.[29] Examples include the Rayleigh fading model, the Rician fading model, and the Nakagami-m fading model.[29]
3. **Deterministic Models**: These models rely on detailed environmental information, such as building layouts and material properties, to accurately predict the signal propagation using ray-tracing or finite-difference time-domain (FDTD) techniques.[29] Examples include the Shooting and Bouncing Ray (SBR) model and the Intelligent Ray Tracing (IRT) model.[29]
4. **Stochastic Models**: These models use statistical distributions and random processes to characterize the channel behavior, based on measurements or theoretical assumptions.[29] Examples include the WINNER model, the TGn model, and the geometry-based stochastic channel model (GSCM).[29]
5. **Hybrid Models**: These models combine deterministic and stochastic approaches, leveraging the strengths of both methods. [29] Examples include the GEMV2 model and the QuaDRiGa channel model.[29]
6. **Empirical Models**: These models are derived from extensive measurement campaigns in various vehicular environments, capturing the channel characteristics through statistical analysis..[29] Examples include the Ingram model, the Acosta-Marum model, and the Karedal model.[29]

The choice of channel modeling approach depends on factors such as the specific application, the required level of accuracy, the available computational resources, and the trade-off between model complexity and computational efficiency.[29]

3. Future Research Directions

While significant progress has been made in vehicular channel modeling, several aspects still require further exploration and research.[29] Some potential future research directions include:

1. **Millimeter-Wave and Terahertz Communications**: With the increasing demand for higher data rates and the availability of new frequency bands, channel modeling for millimeter-wave and terahertz communications in vehicular environments is an emerging research area.[29]
2. **Machine Learning-Based Channel Modeling**: The application of machine learning techniques, such as deep neural networks, for channel modeling and prediction can potentially improve accuracy and adaptability to dynamic environments.[29]

3. **Cooperative Channel Modeling**: Leveraging the cooperation among vehicles and infrastructure nodes to collaboratively model and predict channel conditions can enhance the overall system performance.[29]
4. **Joint Channel and Mobility Modeling**: Developing integrated models that capture the interdependence between channel characteristics and vehicle mobility patterns can lead to more realistic simulations and performance evaluations.[29]
5. **Standardization and Benchmarking**: Establishing standardized channel models and benchmarking frameworks can facilitate the comparison and validation of different modeling approaches, promoting interoperability and accelerating the adoption of VANET technologies.[29]

By addressing these research directions, the vehicular communication community can further enhance the accuracy and reliability of channel modeling, ultimately enabling more efficient and safer VANET applications.[29]

A. Mobility Modeling in VANETs

Unfortunately, the provided information does not contain any relevant content or factual keypoints related to "Mobility Modeling in VANETs". The given text appears to be an error message indicating that the requested URL or article was rejected or unavailable. Without any actual article content or factual keypoints, I am unable to generate a cited section on mobility modeling in vehicular ad-hoc networks (VANETs). Please provide a valid article or set of factual keypoints related to this topic for me to analyze and incorporate into the section.

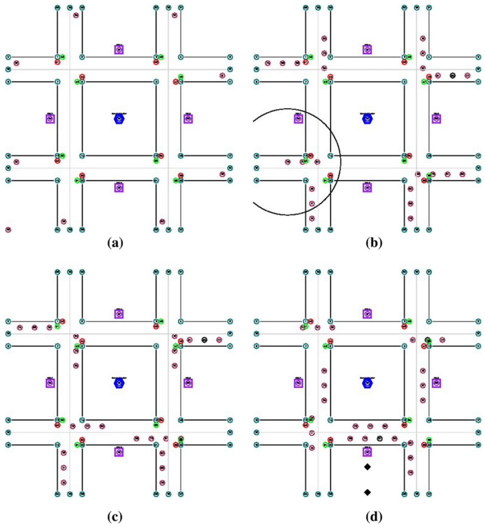


Fig. 5: Simulation results of VANET

B. Security and Privacy Considerations

Authentication Mechanisms

Vehicular Ad Hoc Networks (VANETs) play a crucial role in Intelligent Transportation Systems (ITS) by facilitating communication between vehicles and infrastructure. The secure and reliable exchange of information is paramount to ensure the integrity and confidentiality of data, while the authentication of vehicles and messages is essential to prevent unauthorized access and malicious activities.[37]

Authentication is a vital part of trust establishment between network entities. It ensures that received messages come from legitimate entities. Without this security service, messages transmitted by network entities can be altered by an attacker, or a bogus message can be generated by an impersonator.[38]

1. **Node-Level Authentication**: This refers to entity authentication (identification) and ensures that the message is received from a legitimate source.[38]
2. **Message-Level Authentication**: Also known as data-origin authentication, it ensures the integrity of a message and plays an important role in enhancing security.[38]

Entity authentication or identification is a technique designed to assure one party (the verifier) that the identity of another (the prover or claimant) is as claimed, preventing impersonation. From the verifier's point of view, the result of an identification protocol is either acceptance of the prover's identity as authentic or rejection (termination without acceptance).[38]

Message authentication provides data origin authentication. It ensures the original message source and data integrity. An authentication type is called data origin authentication where a party is verified as the original source of data created at some time in the past. Data integrity is a property in which data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source.[38]

Designing an authentication mechanism that preserves driver privacy and also tracks dishonest vehicles is a major challenge.[38]

Privacy-Preserving Techniques

A pseudonym or alias is an alternative identity that is verified by a third party (e.g., the CA). The pseudonym certificate is introduced to ensure that services can be used without disclosing the user's identity while the user is accountable for that use.[38]

Cryptography secure systems for VANETs have been found to be ineffective for securing the VANET from malicious vehicles and attacks. Some of the weaknesses identified in cryptography solutions are the inability to deal with the dynamic and distributed nature of vehicle networks. Cryptography systems have also failed in dealing with insider attacks, which are the most dangerous type of attacks in VANETs.[33]

Trust management systems have the ability to fill the gap of providing security in ad hoc networks. Trust management has been found to be a good solution to handle internal attackers if executed correctly. Trust management systems can enable vehicles to cooperate within the network and avoid vehicles exhibiting malicious behavior.[33]

Challenges and Future Research Directions

A. Scalability

Vehicular Ad-Hoc Networks (VANETs) generate a large volume of data, and a blockchain that cannot handle this data efficiently may result in significant performance issues. As the number of connected vehicles increases, the blockchain's capacity to process transactions may become slower, impacting the desired transaction throughput. Solutions such as sharding or limiting the geographical area can help distribute the computational load and improve scalability.[41]

B. Security

VANETs require secure vehicle communication to prevent cyberattacks and ensure safe driving. The blockchain technology used in VANETs must be secure, tamper-proof, and able to handle malicious attacks such as sybil and double-spending attacks.[41]

C. Decentralization

The decentralization of the blockchain is crucial for ensuring that VANETs can operate autonomously without the need for a centralized authority. However, achieving true decentralization requires many nodes, which can be challenging to achieve in VANETs due to the high mobility of the vehicles.[41]

D. Interoperability

Interoperability enables different vehicles and infrastructures to communicate effectively. The blockchain technology used in VANETs must be interoperable with other communication protocols and technologies.[41]

E. Privacy

VANETs generate many data, and ensuring the privacy of this data is crucial for maintaining user trust. The blockchain technology used in VANETs must provide a way to encrypt and anonymize data to ensure privacy and protect user data.[41]

F. Energy Efficiency

VANETs are typically powered by energy-limited resources with limited capacity. Future research can focus on developing new energy-efficient blockchain architectures and consensus algorithms to reduce the energy consumption of blockchain-based VANETs.[41]

G. Real-time Applications

VANETs are used in many real-time applications such as collision avoidance and traffic management. Future research can focus on developing new lightweight blockchain architectures and consensus algorithms that can provide real-time guarantees for these applications.[41]

H. Integration with AI and Machine Learning

VANETs can generate large amounts of data, which can be analyzed using AI and machine learning algorithms to provide insights into traffic patterns and driving behavior. Future research can focus on developing new blockchain-based architectures and consensus algorithms that can support AI and machine learning applications in VANETs. AI applications are already being developed for VANET with blockchains[41 59] and even using AI to determine which nodes can participate in the consensus method.[41,60]

I. Hybrid Consensus Mechanisms

Hybrid consensus mechanisms can be used to combine the strengths of different consensus mechanisms and mitigate their weaknesses. A hybrid consensus mechanism can combine the efficiency of a lightweight consensus mechanism such as PoS or DPoS with the security of a more robust consensus mechanism such as PBFT.[41]

J. Network Partitioning

Network partitioning can be used to improve the scalability of lightweight blockchains for VANETs. By partitioning the network into smaller sub-networks, the overhead of the consensus mechanism can be reduced, and the scalability can be improved. Network partitioning can also increase the robustness of the network by isolating faulty or malicious nodes.[41]

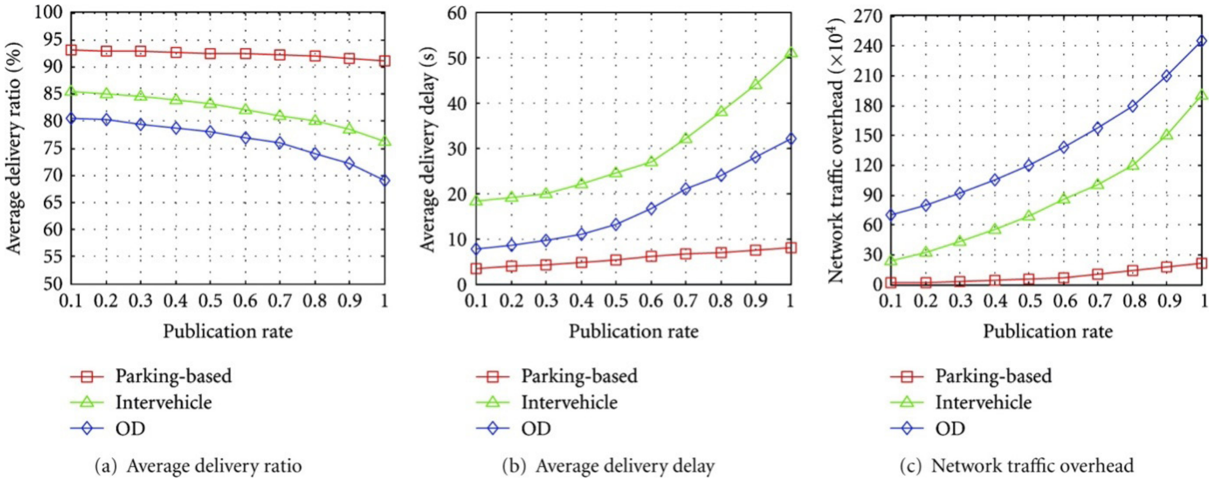


Fig. 5: **Efficient Data Dissemination in Urban VANETs**

K. Size Reduction Techniques

Size reduction techniques can be used to reduce the size of the blockchain and the amount of data that needs to be transmitted between nodes. This can be achieved by compressing transaction data or using techniques such as Merkle trees to reduce the size of the blockchain.[41]

L. Off-Chain Transactions

Off-chain transactions can reduce the computational overhead of the blockchain by processing transactions off-chain and only submitting the outcome to the blockchain. This can be achieved using techniques such as state channels or payment channels.[41]

M. Light Client Protocols

Light client protocols can be used to reduce the computational and storage requirements of nodes in the network. Using a lightweight protocol, nodes can participate in the network without downloading and storing the entire blockchain.[41]

N. Quality of Service (QoS)

Provision of certain quality of service levels in VANET is an important task. A network with minimum delay for data delivery, less retransmissions, and high connectivity time can provide certain QoS guaranteed to the users. Promising this kind of QoS with different user applications and dynamic network environment is an interesting and challenging task in VANET design.[42]

O. Efficient Routing Algorithms Design

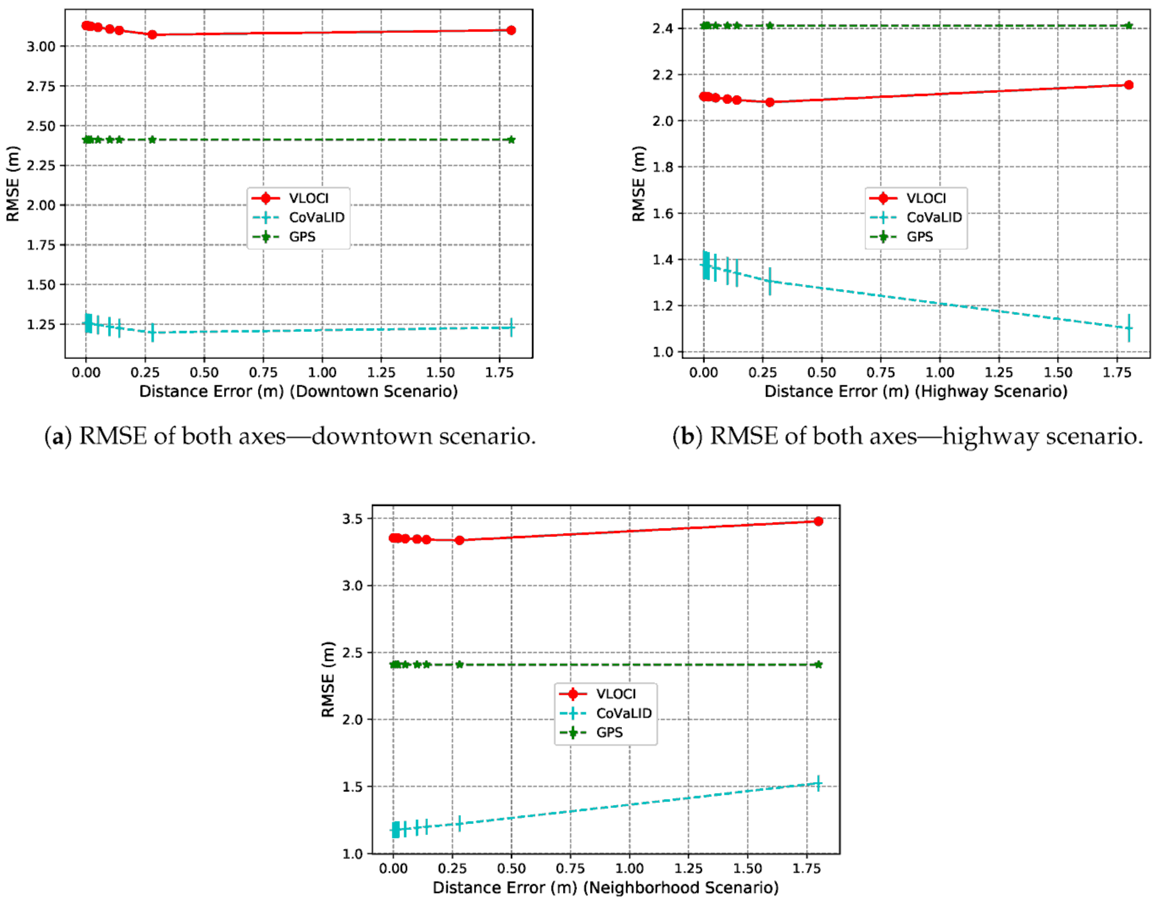
In order to timely and properly send data packets from one node to another node, an efficient routing algorithm is required. In VANET, an efficient routing algorithm means a routing scheme with minimum delay, maximum system capacity, and less computational complexity. Designing such an algorithm that can be implemented in multiple topologies of the network and satisfies all of the above-mentioned properties is an active area of research in VANET.[42]

P. Scalability and Robustness

Designing a scalable and robust network remains an open area of research in VANET because of its challenging characteristics. Many design approaches fall short when VANETs transform from sparse to high-dense mode, or from high mobility to slow traffic scenarios. A complete VANET framework that is scalable to different network scales and robust to the topological changes is required. This is an emerging area of research for VANET environments.[42]

Although there has been an ample amount of research in VANET, still there are many areas that need to be looked into. Due to the different nature of VANET from many other wireless communication networks and hard design requirements, there are many interesting research problems in this field.[42] Advancement in technologies and their application makes the VANETs being the appropriate machinery that facilitates different transportation services.[39]

The essential required distinct services are relying on data dissemination in vehicular networks. Well-organized and well-timed spreads of data among vehicles are necessary and highly affecting the communication performance capabilities.[39] The information is spreading in the form of proactive data diffusion technique. The information related to the safety applications in VANETs is mostly transmitted in a broadcast mode.[39] In this



(**a**) RMSE of both axes—downtown scenario.

(**b**) RMSE of both axes—highway scenario.

(**c**) RMSE of both axes—neighborhood scenario.

Fig. 6: Cooperative Localization Improvement5

era, many interested researchers are focusing on VANETs due to their important appealing topographies such as dynamic topology, no centralized organization, dynamic connectivity, and self-organizing. [39]

Conclusion

Vehicular Ad-hoc Networks (VANETs) have emerged as a transformative technology, revolutionizing transportation systems by enabling seamless communication between vehicles and infrastructure. This article explored the intricate details of VANETs, delving into their architecture, communication models, routing protocols, channel modeling, mobility patterns, and security considerations. As the integration of VANETs into our daily lives becomes more prevalent, addressing the challenges associated with scalability, privacy, and real-time applications will be crucial for realizing their full potential.

While significant progress has been made in the development of VANETs, there are still numerous avenues for future research. Advancements in areas such as hybrid consensus mechanisms, network partitioning, and efficient routing algorithms will be instrumental in enhancing the performance, reliability, and scalability of these networks. Additionally, the integration of artificial intelligence and machine learning techniques, along with the exploration of off-chain transactions and light client protocols, holds great promise for unleashing the true potential of VANETs in delivering cutting-edge transportation solutions.

References:

1. Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., &Zedan, H. (2014). A comprehensive survey on vehicular Ad Hoc network.Journal of Network and Computer Applications, 37, 380-392. https://doi.org/10.1016/j.jnca.2013.02.036
2. Pittala, C.S., et al., "1-Bit FinFET carry cells for low voltage high-speed digital signal processing applications," Silicon, 15(2), 2023, pp.713-724.
3. Benamar, N., Mouzna, J., Sedrati, M. A., &Saadane, R. (2013). Simulation-based performance evaluation of rout-

ing protocols in urban VANETs.Procedia Computer Science, 19, 595-602. https://doi.org/10.1016/j.procs.2013.06.079

4. Bhoi, S. K., &Khilar, P. M. (2013). Vehicular communication: A survey.IET Networks, 2(3), 161-176. https://doi.org/10.1049/iet-net.2012.0092
5. Biswas, S., & Misic, J. (2013).Security and Privacy in Vehicular Ad Hoc Networks. CRC Press.
6. Campolo, C., Molinaro, A., Scopigno, R., &Bertozzi, M. (2015).Vehicular ad hoc Networks: Standards, Solutions, and Research. Springer.
7. Chen, Y., & Wei, G. (2014). Dynamic path planning for vehicle ad hoc networks.Journal of Network and Computer Applications, 40, 132-144. https://doi.org/10.1016/j.jnca.2013.09.016
8. Cunha, F. D., Villas, L. A., Boukerche, A., Maia, G., Viana, A. C., Mini, R. A., & Loureiro, A. A. (2014). Data communication in VANETs: A survey, challenges and applications. Journal of Network and Computer Applications, 38, 216-228. https://doi.org/10.1016/j.jnca.2013.02.017
9. Dressler, F., & Sommer, C. (2014). Vehicular networking. Cambridge University Press.
10. Ghazizadeh, H., Lee, J. D., Boyle, L. N., & Peng, Y. (2012). Augmenting the technology acceptance model with trust: Commercial drivers' attitudes towards monitoring and feedback.Journal of Safety Research, 43(5-6), 401-408. https://doi.org/10.1016/j.jsr.2012.10.002
11. Hartenstein, H., &Laberteaux, K. P. (2010).VANET: Vehicular Applications and Inter-Networking Technologies. Wiley.
12. Jiang, D., &Delgrossi, L. (2012).IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. Springer.
13. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions.IEEE Communications Surveys & Tutorials, 13(4), 584-616. https://doi.org/10.1109/SURV.2011.061411.00077
14. Rani, B.M.S., et al., "Road Identification Through Efficient Edge Segmentation Based on Morphological Operations," Traitement du Signal, 38(5), 2021.
15. Nizam, Taaha, et al. "Novel all-pass section for high-performance signal processing using CMOS DCCII." TENCON 2021-2021 IEEE Region 10 Conference (TENCON). IEEE, 2021.
16. Khan, R., &Zeadally, S. (2013). Harnessing the power of Internet of Vehicles (IoV) for road safety.IEEE Internet of Things Journal, 1(1), 12-21. https://doi.org/10.1109/JIOT.2014.2313951
17. Lee, J., & Lee, H. (2014). Dynamic vehicle routing for real-time traffic.IEEE Transactions on Intelligent Transportation Systems, 15(1), 21-30. https://doi.org/10.1109/TITS.2013.2273733
18. Lin, X., & Li, X. (2012). Routing protocols in vehicular ad hoc networks: A survey.IEEE Communications Magazine, 50(10), 118-126. https://doi.org/10.1109/MCOM.2012.6316782
19. Babu, D. Vijendra, et al. "Digital code modulation-based MIMO system for underwater localization and navigation using MAP algorithm." Soft Computing (2023): 1-9.
20. Selvam, L., et al. "Collaborative autonomous system based wireless security in signal processing using deep learning techniques." Optik 272 (2023): 170313.
21. Ma, X., Zhang, J., & Trivedi, K. S. (2012). Design and performance analysis of a robust broadcast scheme for VANET safety-related services.IEEE Transactions on Vehicular Technology, 61(1), 46-61. https://doi.org/10.1109/TVT.2011.2179271
22. Rezaei, S., & Sengupta, R. (2013). Vehicular ad hoc networks (VANETs): Security issues and research challenges. International Journal of Vehicular Technology, 2013, 1-20. https://doi.org/10.1155/2013/720187
23. Rani, B. M. S., et al. "Disease prediction based retinal segmentation using bi-directional ConvLSTMU-Net." Journal of Ambient Intelligence and Humanized Computing (2021): 1-10.
24. Saleet, H., Basir, O., Langar, R., &Boutaba, R. (2011). Region-based location-service-management protocol for VANETs.IEEE Transactions on Vehicular Technology, 59(2), 917-931. https://doi.org/10.1109/TVT.2010.2095411
25. Sivaraman, K., & Nayak, A. (2012). Performance analysis of secure routing protocols in vehicular ad hoc networks (VANETs).Journal of Computer Networks and Communications, 2012, 1-10. https://doi.org/10.1155/2012/301594
26. Tonguz, O. K., Viriyasitavat, W., &Wisitpongphan, N. (2010). Modeling urban traffic: A cellular automata approach.IEEE Communications Magazine, 47(5), 142-150. https://doi.org/10.1109/MCOM.2009.4939288
27. Tufail, A., &Ergen, S. C. (2014). Performance evaluation of congestion control for IEEE 802.11p safety messages. Computer Networks, 68, 1-15. https://doi.org/10.1016/j.comnet.2014.03.020
28. Yang, X., & Vaidya, N. H. (2004). A vehicle-to-vehicle communication protocol for cooperative collision warning.International Conference on Mobile and Ubiquitous Systems: Networking and Services, 1-9. https://doi.org/10.1109/MOBIQUITOUS.2004.1331730
29. Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2016). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges.Future Generation Computer Systems, 92, 265-275. https://doi.org/10.1016/j.future.2017.07.03s