Wireless Wheels: VANET

Syed 301318212

Deepak

Nirojan

ICET, Centennial College

CBER702_002: Communication Networks

Marjan Zandi

Due date

Abstract

The paper explores the transformative impact of Vehicular Ad-hoc Networks (VANETs) on the automotive industry over the past decade. Focusing on dynamic communication enabled by mobile technologies, the study delves into VANET's open network architecture, emphasizing its role in Intelligent Transport Systems. Key characteristics, including dynamic topology, intermittent connectivity, and onboard sensors, are discussed. The paper underscores the importance of VANET research in elevating road safety, optimizing traffic dynamics, enabling swift emergency response, promoting environmental sustainability, contributing to Intelligent Transportation Systems, shaping future mobility, and addressing unique security challenges. It comprehensively covers VANET communication architecture, transmission protocols, and imperative security considerations. Furthermore, it outlines diverse applications, categorizing them into safety and comfort domains. The challenges and future research directions in VANET adoption, including mobility, data administration, security, quality service delivery, and standardization, are highlighted.

Table of Contents

List of Figures

List of Tables

Summary

This paper provides a comprehensive overview of the profound impact of Vehicular Ad-hoc Networks (VANETs) on the automotive industry, specifically focusing on the last decade. Highlighting the evolution of mobile communication technologies, the study emphasizes VANET's role in creating dynamic networks where vehicles and connected devices exchange real-time information wirelessly. The paper explores VANET's key characteristics, including dynamic topology, intermittent connectivity, and the presence of onboard sensors, illustrating its crucial role in Intelligent Transport Systems.

Emphasizing the significance of VANET research, the paper discusses its contributions to elevated road safety, optimized traffic flow, swift emergency response, environmental sustainability, and the development of Intelligent Transportation Systems. It addresses the challenges of securing VANETs in dynamic and potentially adversarial environments, emphasizing the importance of robust security mechanisms. The communication architecture of VANET, transmission protocols, and various security considerations are thoroughly examined.

The study categorizes VANET applications into safety and comfort domains, outlining their contributions to road safety and passenger/driver comfort. Additionally, the paper identifies challenges in VANET adoption, such as mobility, data administration, security, quality service delivery, and the need for standardization. Overall, this paper provides a comprehensive understanding of VANET's transformative potential, its current state, challenges, and avenues for future research.

1. Introduction

Over the past decade, mobile communication technologies have significantly impacted the automotive industry, enabling communication between devices anytime and anywhere. This has led to the emergence of Vehicular Ad-hoc Networks (VANET), creating ad-hoc networks where moving vehicles and connecting devices exchange real-time information wirelessly. VANET operates as an open network, allowing nodes (vehicles and devices) to join and leave freely. Modern vehicles with onboard sensors can seamlessly integrate into the VANET, facilitating communication and leveraging its benefits.

Key characteristics of VANET include its dynamic topology, intermittent connectivity, observation of mobility patterns for routing protocols, assumption of unlimited power and storage in nodes, and the presence of onboard sensors. VANET plays a crucial role in Intelligent Transport Systems by generating insights from the exchanged information.

1.1 Background Context

Networks are broadly categorized as wired or wireless based on infrastructure. Wired networks rely on cables for stable connections, suitable for stationary setups. In contrast, wireless networks like WLANs use radio waves, providing mobility for homes and offices. A specific type, Wireless Ad-hoc Networks (WANETs), stands out for decentralization. In WANETs, devices communicate directly, ideal for scenarios without fixed infrastructure, like emergencies. This shift from wired to wireless ad-hoc networks signifies a move towards dynamic, adaptable communication, emphasizing mobility and decentralized connectivity, crucial in rapidly changing environments such as emergencies or military operations.

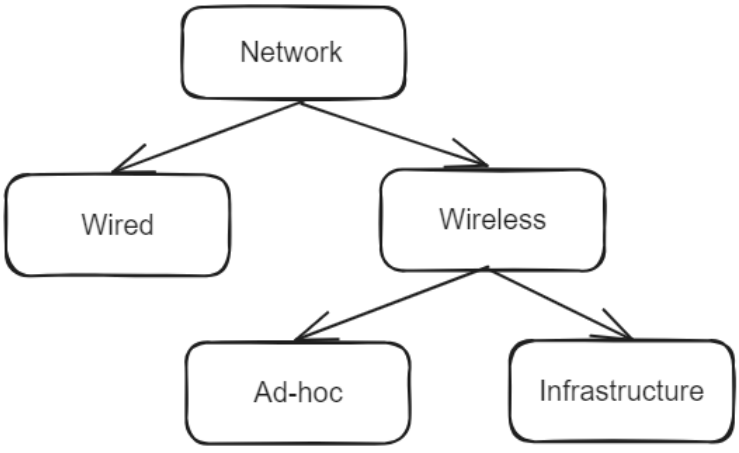

Figure 1 - Classification of Network

VANET, a variation of Mobile Ad-hoc Networks (MANET), is characterized by its dynamic topology, intermittent connectivity, mobility patterns, unlimited power and storage assumption, and the presence of onboard sensors. The communication in VANET contributes to increased

traffic efficiency, road condition detection, collision reduction, emergency awareness, and overall network efficiency through multi-hop transmissions.

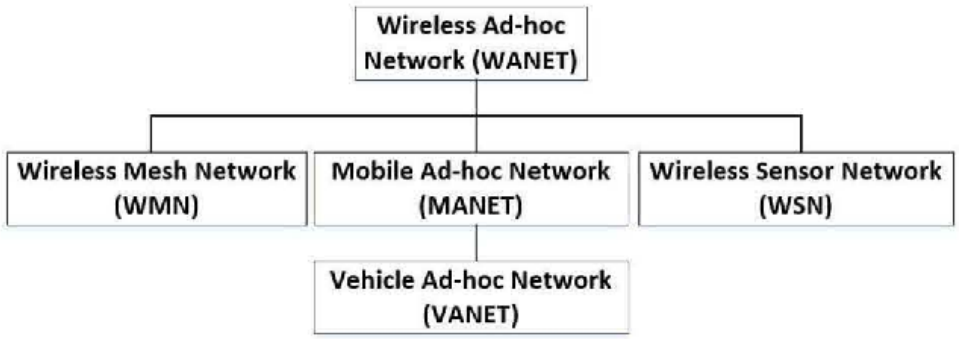

Figure 2 - Classification of WANET

2. Communication

2.1 Architecture

The architecture of VANET, designed to facilitate communication among neighboring vehicles, adheres to IEEE 1471-2000 and ISO/IEC 42010 guidelines, dividing entities into three domains:

1. Mobile Domain: Comprising vehicles in motion (e.g., cars, buses) and portable devices (PDAs, laptops, smartphones).

2. Infrastructure Domain: Split into roadside infrastructure (e.g., traffic lights) and central infrastructure (e.g., vehicle management center).

3. Generic Domain: Encompassing Internet and Private infrastructure, involving nodes, servers, and computing resources for VANET.

Data flow occurs from the mobile domain to the infrastructure domain, which processes and modulates data, then communicates with the generic domain. This interaction optimizes road utilization.

In the communication architecture, VANET involves four communication types:

1. In Vehicle Communication: Monitors vehicle system data for factors like driver exhaustion, crucial for public and driver safety.

2. Vehicle-to-Vehicle (V2V) Communication: Enables data exchange between vehicles, providing warnings and critical information, enhancing safety and security without relying on fixed infrastructure.

3. Vehicle-to-Road Infrastructure (V2I) Communication: Involves communication between mobile vehicles and roadside fixed infrastructure, offering updates on environmental sensing, traffic, and weather.

4. Vehicle-to-Broadband Cloud (V2B) Communication: Facilitates vehicle communication over broadband connections (e.g., 3G/4G), enhancing driver assistance and vehicle tracking.

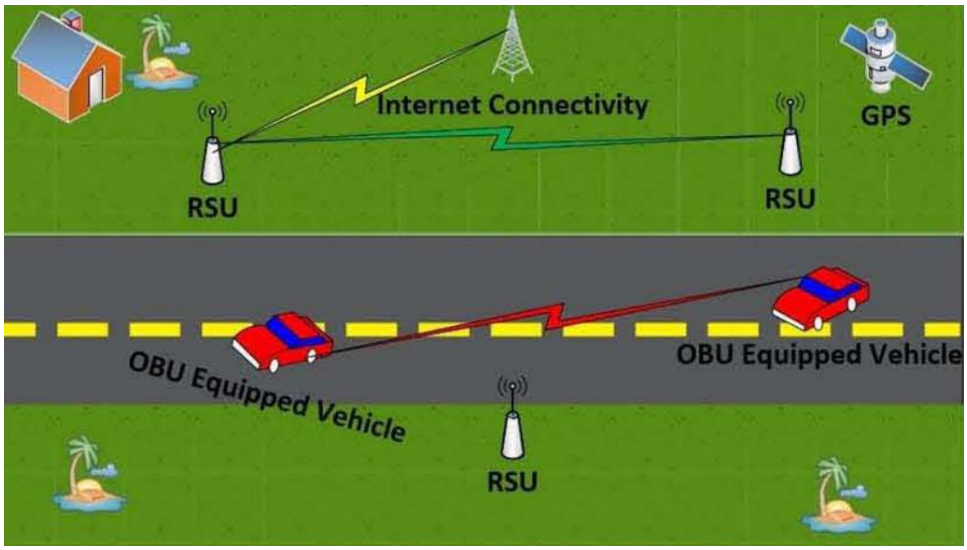

Figure 3 - VANET Architecture

2.2 Protocols for Transmission

The effectiveness of VANETs relies heavily on efficient communication among various vehicles. The exchange of data between these vehicles necessitates specific protocols or rules to ensure organized and systematic transmission. Routing protocols play a crucial role in facilitating the exchange of information between nodes in a VANET, determining how data packets are distributed among different vehicles. Three types of protocols are identified for VANET communication based on the senders and receivers involved:

1. *Unicast:* These protocols focus on transmitting data from a single source to a specific destination over a wireless medium. Two methods of packet transmission are employed: multi-hop transmission, where a packet is progressively transmitted through neighboring vehicles, and carry-and-forward technique, where a vehicle carries the packet for as long as possible before transmitting to minimize congestion or rebroadcasting. Trajectory-based protocols involve nodes calculating various paths for data transmission, ensuring minimal rebroadcast of packets.
2. *Broadcast:* Broadcasting protocols aim to communicate with as many nodes as possible. They are essential in scenarios such as roadblocks, traffic jams, high traffic density areas, or emergency situations, where data packets need to be transmitted to multiple nodes simultaneously. However, broadcasting protocols also increase the likelihood of packet rebroadcast or the storm problem. Figure 4 illustrates a list of broadcasting protocols.

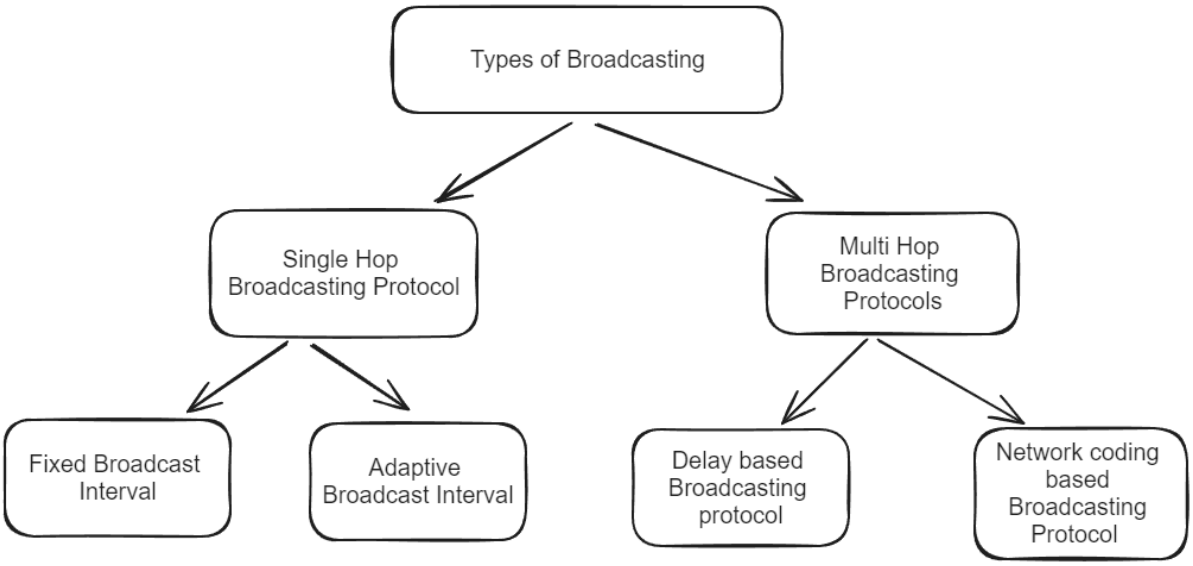

Figure 4 - Types of Broadcasting

3. Security

Ensuring security in Vehicular Ad-hoc Networks (VANETs) is paramount for the safety of drivers and passengers. It is essential to develop sophisticated algorithms to guarantee safety and protection. VANETs face various security challenges, including availability, authentication, integrity, confidentiality, non-repudiation, pseudonymity, privacy, mobility, data and location verification, access control, and key management issues.

3.1 Security Issues

Availability: Availability is a crucial aspect of VANET security, ensuring continuous accessibility of resources despite vulnerabilities and denial of service attacks. Cryptography, trust-based algorithms, and protocols play a role in safeguarding VANETs from such attacks.

Authentication: Authentication involves dual verification to allow the right participants to enter the network while preserving user privacy through pseudonyms, ensuring that the sender is not an intruder.

Integrity: Integrity ensures that the original data packets remain unchanged during transmission. Digital signatures, public key infrastructure, and cryptography revocation mechanisms are employed to guarantee data integrity between sender and receiver.

Confidentiality: Confidentiality involves hiding data from adversaries, ensuring that only authenticated users can access encrypted data, maintaining the confidentiality of information.

Nonrepudiation: Nonrepudiation ensures that the source of a message cannot deny generating it, binding the content with the originator and preventing denial of generating a specific message.

Pseudonymity: Pseudonymity involves using pseudonyms to hide original identities, allowing legitimate entities to communicate anonymously and protecting privacy.

Privacy: Privacy in VANETs involves concealing driver identity and location information from unauthorized users in the network.

Scalability: Scalability refers to the network's ability to respond to dynamically changing requirements, a challenge given the frequently changing topology of vehicular networks.

Mobility: Mobility is inherent in VANETs, with nodes changing locations rapidly. Secure and dynamic algorithms are needed to maintain quality of service requirements.

Data Verification: Data verification is crucial for eliminating malicious messages in the network, ensuring the accuracy of data and verifying the legitimacy of participating nodes.

Access Control: Access control monitors policy rights and roles for all participating nodes in the network.

Key Management: Key management involves the issuance and use of encryption or decryption keys during communication between nodes, resolved during the design of security protocols for the network.

Location Verification: Location verification is essential in VANETs to protect against attacks during communication and aid in the data validation process.

3.2 Security Attacks in VANETs

Eavesdropping Assault: Eavesdropping is a passive assault where an attacker secretly monitors the network traffic or the location and actions of a specific vehicle, collecting secret information. ID revelation assault, a subcategory, exposes the identity of a vehicle, aiding in tracking.

Denial of Service Assault: In DoS attacks, the assailant targets the service provider, rendering legitimate users unable to access services. This can be achieved by overwhelming resources with numerous requests, causing congestion in the communication channel.

Jamming Assault: Jamming involves generating a large number of messages to create congestion on the wireless channel, affecting network performance. The jammer disrupts communication by declining the signal-to-noise ratio.

Sybil Assault: In Sybil attacks, the assailant generates numerous identities of vehicles, broadcasting incorrect information on the network to create an illusion of heavy traffic.

Node Impersonation Assault: Node impersonation involves changing the original data packet's content and claiming it comes from a genuine user.

Black Hole Assault: A black hole attack occurs when a malicious node attracts victim nodes by presenting a fake shortest path, leading to misuse or dropping of messages.

Masquerading Assault: In masquerading attacks, the attacker sends packets on behalf of other vehicles, using their identities to deceive and manipulate the behavior of other nodes.

Global Positioning System Spoofing Assault: GPS spoofing involves an attacker faking their location information, forwarding false GPS data to deceive other nodes about their actual location.

Brute Force Assault: In brute force attacks, the intermediary node attempts to decrypt encrypted messages sent from one vehicle to another, compromising the security of the communication.

4. Applications

Throughout the years, numerous studies have been conducted to create applications and usage models for Vehicular Ad-hoc Network (VANET) communication. With an increasing number of individuals spending extended periods on the road, the demand for internet connectivity has risen, enabling communication, real-time access to news, traffic updates, and weather reports. Recent VANET applications include online file sharing, real-time video updates, and entertainment accessed through connections to the internet via Roadside Units (RSUs) or Vehicle-to-Vehicle (V2V) connections. These VANET applications are broadly classified into safety and comfort applications, catering to the diverse needs of users while on the road.

The primary goal of these applications is to preserve human lives on the road by delivering timely safety-related information to the intended recipients, thereby preventing accidents. The tables outline various safety applications, including the following examples:

1. *Information Messages:* These encompass messages pertaining to work zones, toll collection points, and speed limits, providing crucial information for highway driving.
2. *Assistance Messages:* Geared towards aiding drivers during their journey, AMs offer guidance on lane switching, cooperative collision avoidance (CCA), and navigation. CCA messages, in particular, are deemed critical for warning drivers to reduce speed in unpredictable conditions.
3. *Warning Messages:* Warnings such as upcoming traffic signals, toll points, or adverse road conditions fall under this category, aiming to alert drivers and enhance road safety.

In addition to safety applications, there are comfort applications that focus on enhancing passenger/driver comfort and traffic efficiency. These value-added services include automatic toll collection, site-based services like locating shopping malls and restaurants, and internet connectivity.

Applications	Description
Traffic Signal Violation	Alerts nearby vehicles to potential hazards from traffic signal violations.
Intersection Collision	Provides information on road intersections and warns about potential collision points
Turn Assistance	Assists drivers during vehicle turning maneuvers
Blind Spot Warning	Alerts about the presence of another vehicle in the blind spot, enhancing awareness
Pedestrian Crossing	Sends information about pedestrian crossings along the vehicle's path
Lane Change Warning	Ensures the intended lane is clear before initiating a lane change
Forward Collision Warning	Alerts the driver about a slower vehicle ahead, minimizing collision risks
Do Not Pass Warning	Warns the driver regarding safe overtaking practices

Post-Crash	Signals an alert in the aftermath of a collision
Emergency Service Vehicle	Facilitates a clear path for emergency vehicles, such as ambulances
Wrong-Way	Alerts a vehicle if it detects movement in the wrong direction
Work Zone	Provides advance warning about upcoming work zone areas

Table 1 - VANET Safety Applications

Applications	Description
Service Announcement	This application offers information about restaurants and rest areas during a journey, enhancing the overall travel experience by providing details on available services
Remote Diagnostic Connectivity	This application establishes a connection between the vehicle and the vehicle manufacturer or workshop, enabling remote diagnostics. This connectivity facilitates the assessment of vehicle health without physical presence.
Entertainment	Users can enjoy real-time audio and video entertainment within the vehicle, enhancing the passenger experience during the journey.
Remote Passenger Health Update	Designed for use in ambulances through a Wireless Body Sensor Network (WBSN), this application enables the transmission of patient health information directly from the ambulance to the hospital. This allows for swift and accurate diagnosis, improving emergency medical services.

Table 2 - Travelling Comfort Applications

Applications	Description
Map Download	Offers the capability to download maps for routing purposes
Navigation	Provides navigation services for efficient route planning and guidance during travel

Table 3 - Efficient Traveling Applications Points

Applications	Description
Electronic Toll Collection	Enables communication between the vehicle and the toll gate for seamless payment processing before reaching the gate.
Parking Availability	Provides real-time information about parking availability, particularly in major urban areas
Route Diversion	Assists in diverting the vehicle to alternative routes for optimized travel

Table 4 - Other Value-Added Services Points

5. Challenges and Future Research Directions

The adoption of Vehicular Ad-hoc Networks (VANET) introduces several challenges that require extensive research and solutions:

1. *Mobility:* VANET involves highly mobile vehicles, requiring advanced network topology models for efficient information exchange. Unique approaches are needed due to the rapid and dynamic nature of vehicle movement.

2. *Data Administration and Storage:* Managing and storing the vast amount of data generated by large-scale VANETs is challenging. While Big Data technologies offer potential solutions, their integration into VANETs remains a research topic.

3. *Security and Privacy:* The open nature of VANET allows any node to join, leading to concerns about trustworthiness. Robust security models are essential to ensure data integrity, and privacy threats from untrustworthy nodes observing user activities need to be addressed.

4. *Quality Service Delivery:* The dynamic environment of VANET introduces variations in factors such as node position, topology, and connectivity, challenging the effectiveness of routing strategies. Research is needed to design mechanisms ensuring consistent, high-quality service delivery.

5. *Heterogeneity and Standardization:* VANET involves diverse nodes, requiring communication protocols standardization for seamless communication. Collaboration between government, industry, academia, and other institutes is crucial for effective standardization.

6. *Routing Protocols:* Traditional routing protocols are inadequate for VANET due to high node mobility. Robust algorithms and routing protocols are essential to achieve higher throughput, better service, and an enhanced packet delivery ratio in VANETs.

6. Recommendations

Integration of Big Data Technologies: Investigate the integration of Big Data technologies to manage and analyze the vast amount of data generated by large-scale VANETs. Develop efficient methods for data administration, monitoring, and storage to address the challenges posed by the extensive data generated by millions of participating nodes.

Collaboration for Standardization: Advocate for collaboration between government entities, industry stakeholders, academia, and other institutes to establish standardized communication protocols for VANETs. Standardization is crucial for seamless communication between heterogeneous nodes, including various types of vehicles, roadside units, and computing resources.

User Privacy Preservation Techniques: Explore techniques to safeguard user privacy within VANETs. Given the open nature of the network, mechanisms to protect user activities, habits, and patterns from untrustworthy nodes should be a focal point of future research to ensure a secure and privacy-preserving environment.

Application of Artificial Intelligence: Explore the application of artificial intelligence (AI) techniques in VANETs to enhance decision-making processes, especially in the context of safety applications. AI can contribute to real-time analysis of data, enabling more intelligent and proactive responses to potential hazards on the road.

User Education and Awareness: Promote user education and awareness programs to enhance understanding of VANET technologies and their benefits. Increasing awareness among drivers, passengers, and other stakeholders can contribute to the successful adoption and utilization of VANET applications, ultimately improving road safety and traffic efficiency.

7. Conclusion

In conclusion, this paper provides a comprehensive exploration of the transformative role of Vehicular Ad-hoc Networks (VANETs) in the automotive industry over the past decade. The dynamic nature of mobile communication technologies has significantly impacted the development of VANETs, creating open networks where vehicles and devices exchange real-time information wirelessly. The study underscores the importance of VANET research in enhancing road safety, optimizing traffic dynamics, enabling swift emergency responses, and contributing to Intelligent Transportation Systems. It emphasizes the challenges posed by the unique characteristics of VANETs, including their dynamic topology, intermittent connectivity, and the need for robust security mechanisms.

The communication architecture, transmission protocols, and diverse applications of VANETs, spanning safety and comfort domains, are thoroughly examined. The paper identifies key security issues and recommends further research directions, including the development of advanced security protocols, integration of Big Data technologies, and the enhancement of routing strategies. Standardization, user privacy preservation, dynamic network topology modeling, and the application of artificial intelligence are also highlighted as critical areas for future exploration. The paper concludes by advocating for collaborative efforts in addressing these challenges and emphasizes the potential of VANETs in shaping the future of intelligent and sustainable mobility solutions within smart cities. Overall, this research lays the foundation for continued exploration and innovation in the field of Vehicular Ad-hoc Networks.

8. References

Afzal, Z., & Kumar, M. (2020, January 1). *IOPscience*. Journal of Physics: Conference Series. https://iopscience.iop.org/article/10.1088/1742-6596/1427/1/012015

Chaudhary Muhammad Asim Rasheed, Gilani, S., Ajmal, S., & Qayyum, A. (2017, March). (PDF) challenges in vehicle ad hoc network (VANET) - researchgate. https://www.researchgate.net/publication/326250676_Challenges_in_Vehicle_Ad_Hoc_Network_VANET

Ghori, M. R., Zamli, K. Z., Quosthoni, N., Hisyam, M., & Montaser, M. (2018, May 12). Vehicular ad-hoc network (VANET): Review - IEEE Xplore. https://ieeexplore.ieee.org/document/8376311

Kugali, S. N., & Kadadevar, S. (2020, June 29). *Vehicular Adhoc Network (VANET):-A brief knowledge*. International Journal of Engineering Research & Technology. https://www.ijert.org/vehicular-adhoc-network-vanet-a-brief-knowledge

Mahmood, J., Duan, Z., Yang, Y., Wang, Q., Nebhen, J., & Bhutta, M. N. M. (2021, June 30). *Security in vehicular ad hoc networks: Challenges and countermeasures*. Security and Communication Networks. https://www.hindawi.com/journals/scn/2021/9997771/

Vehicular Adhoc Network (VANET) - an introduction. (n.d.). https://hal.science/hal-01496806/document