|  |  |  |  |
| --- | --- | --- | --- |
| **Course Name:** | **MCAN Laboratory** | **Semester:** | **VI** |
| **Date of Performance:** | **21 / 04 / 2025** | **Batch No.:** | **B – 2** |
| **Faculty Name:** | **Dr. Rajashree Daryapurkar** | **Roll No.:** | **16014022050** |
| **Faculty Sign & Date:** |  | **Grade / Marks:** | **\_\_\_ / 25** |

**Experiment No.: 10**

**Title: Report on Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges**

|  |
| --- |
| **Aim and Objective of the Experiment:** |
| Write a report on the research paper - Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges. |

**Introduction**

Vehicular Ad-Hoc Networks (VANETs) have emerged as a critical area of research, focusing on enabling communication among vehicles, enhancing road safety, and improving traffic efficiency. Unlike traditional mobile networks, VANETs do not rely on centralized infrastructure, allowing for ad-hoc communication between vehicles (Vehicle-to-Vehicle, V2V) and between vehicles and infrastructure (Vehicle-to-Infrastructure, V2I). The primary application of VANETs is in environments where infrastructure is scarce or unavailable, such as during critical medical emergencies.

Key Contributions and Objectives of VANETs:

* Enhancing road safety by providing real-time alerts about dangers.
* Improving traffic management by reducing congestion and travel time.
* Supporting comfort and convenience for travelers with advanced information systems and toll collection mechanisms.

**Architecture and Network Modeling**

VANETs can be classified based on the communication scenarios:

1. Infrastructure-Based: All vehicles communicate through Road Side Units (RSUs), resembling Wireless Local Area Networks (WLANs).
2. Ad-Hoc Communication: Vehicles communicate directly without any RSUs, which is typical of ad-hoc networks.
3. Hybrid Architecture: Some vehicles use RSUs, while others communicate directly with each other.

The high mobility of vehicles in VANETs requires dynamic network architectures. A mobility model is essential to understand vehicular behavior, including acceleration, deceleration, and lane changes. VANETs can use stochastic, traffic-based, and trace-based mobility models, depending on the level of detail and realism needed for simulations.

Challenges in Network Architecture:

* Dynamic topology due to rapid movement of vehicles.
* Frequent disconnections and short-lived connections, especially in high-speed environments like highways.

**Routing in VANET**

Routing is one of the major challenges in VANETs due to the constantly changing network topology. Several routing protocols have been explored, including Topology Driven, Location Based, and Cluster-Based Routing.

Routing Protocols:

* Topology-Driven Protocols (e.g., AODV, DSR): These protocols are reactive, meaning routes are only discovered when needed. However, they may result in flooding the network with control messages, causing bandwidth wastage.
* Location-Based Protocols (e.g., GPSR): These use the geographic location of vehicles to reduce routing overheads. The main advantage is the avoidance of constant route maintenance.
* Cluster-Based Routing: This method divides the network into small groups (clusters) of vehicles. Each cluster has a designated head, which controls communication within the cluster and with other clusters.

Challenges in Routing:

* Dynamic and unpredictable topology requires adaptive routing protocols.
* Ensuring minimal delay and high packet delivery ratio (PDR) while maintaining low overhead.

**Security in VANET**

Security is crucial for VANETs due to the sensitive nature of information being transmitted, especially for applications like medical emergencies. The main security concerns include:

1. Authenticity: Ensuring the message is from a trusted source (e.g., preventing the distribution of bogus information).
2. Confidentiality: Protecting vehicle location and personal information from being tracked or intercepted.
3. Availability: Preventing Denial of Service (DoS) attacks that could disrupt critical services.

VANET Security Solutions:

* Public Key Infrastructure (PKI) and Pseudonym Systems are used to maintain privacy while ensuring authenticity.
* Authentication Mechanisms: Each vehicle node can be authenticated, ensuring that only trusted nodes can transmit messages.

Threats:

* Bogus Information: Manipulation of safety messages, leading to potential accidents.
* ID Disclosure: Risk of vehicles being tracked based on their location.
* Denial of Service (DoS): Malicious entities flooding the network to disrupt communication.

**Key Research Areas and Challenges**

Several challenges remain for the widespread adoption of VANETs:

1. Quality of Service (QoS): Ensuring timely delivery of messages with minimal delay, especially in critical applications like emergency alerts.
2. Routing Algorithm Design: Developing efficient routing protocols that minimize delay and handle the dynamic nature of VANETs.
3. Scalability: Designing networks that are scalable to accommodate varying numbers of vehicles across different environments.
4. Cooperative Communication: How vehicles can efficiently share information with minimal resource consumption.
5. Network Security: Ensuring secure communication and privacy, particularly in the face of potential attacks.

Emerging Areas of Research:

* Adaptive and hybrid routing protocols.
* Improved security and privacy models.
* Efficient communication mechanisms for high-density traffic.

**Conclusion**

VANETs offer tremendous potential for improving road safety, traffic efficiency, and overall traveler experience. However, the high mobility and dynamic nature of vehicular networks present significant challenges in areas such as routing, security, and QoS. Ongoing research continues to explore ways to improve VANET performance, security, and scalability, aiming to create a reliable and secure vehicular communication network.

Future Research Directions:

* Investigating new routing protocols that better adapt to changing network conditions.
* Enhancing security protocols to protect user privacy without compromising network performance.
* Developing robust VANET systems that can operate effectively in different traffic environments, from highways to urban roads.

|  |
| --- |
| **Signature of faculty in-charge with Date:** |