MCAN IA2:

Vehicular Ad-Hoc Networks (VANETs)

By -

Meetali Neve (16014022058) & Ketaki Mahajan (16014022050)

SOMAIYA VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

Somaiya TRUST

Introduction

What is VANET?

- A wireless communication network formed between moving vehicles and infrastructure.

Why is it important?

- Enables real-time data exchange for safety, traffic management, and infotainment.

Key Applications:

- Collision warnings
- Traffic updates
- Emergency alerts
- Autonomous driving support

Focus of the Presentation:

- Architecture, routing, key challenges, and security solutions in VANETs

What are VANETs

- VANET = Mobile ad-hoc network formed by vehicles.
- Enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication.
- Designed for dynamic environments without fixed infrastructure.
- Crucial for safety-critical applications (e.g., medical emergencies).
- Each vehicle acts as a network node and manages its own communication.

Key Characteristics of VANETs

- **Dynamic Topology** – Vehicles constantly change position
- **High Mobility – Nodes** (vehicles) move fast
- Frequent Disconnections
- **Predictable Mobility Patterns** – Movement along roads/highways
- **Integration with GPS** and sensors
- **No Power Constraint** – Vehicles can support high-energy operations
- **Strict Delay Requirements** – Especially for safety/emergency alerts

VANET Architecture

Ad-Hoc Communication (V2V)

Vehicles communicate **directly** with each other, forming a **peer-to-peer network**.

Few features include:

- **Decentralized** and **infrastructure-less**
- **Self-configuring** communication

Few use cases include **collision warning systems**, **emergency braking alerts**, **lane-change assistance**.

Infrastructure-Based Communication (V2I)

Vehicles communicate with **infrastructure units** called **Road Side Units** (RSUs).

Few features include:

- **Centralized communication support**
- RSUs act as **gateways** to the internet or traffic management centers

Few use cases include **Traffic signal control**, **Toll collection** & **Real-time navigation assistance**.

Hybrid Architecture

Combines both **V2V** and **V2I** communication models.

Few features include:

- Enables **broader coverage** and **reliability**
- **Seamless data flow** even when RSUs are unavailable

Mobility and Signal Modelling

Mobility

Levels of Mobility Modelling:

- **Microscopic** which focuses on **individual vehicle** behavior.
  e.g. lane changes, braking, overtaking.
- **Macroscopic** which focuses on **overall traffic patterns**.
  e.g. traffic flow on highways, intersection.

Few of the mobility modelling techniques include:

- **Stochastic models** uses randomness to simulate movement.
- **Flow-Based Models** is based on fluid dynamics to simulate traffic as traffic flow.
- **Trace-Based Models** uses real GPS to reflect actual ehicle movement.

Realistic mobility modeling improves routing accuracy, reduces packet loss, and enhances simulation credibility.

Signal Modelling

Challenges:

- Signal undergoes **reflection**, **diffraction**, and **scattering**.
- Causes multi-path fading and signal degradation.

Common Channel Models:

Model	Description / Application
Free Space Model	Simplified line-of-sight (LOS) model used for basic transmission analysis in open areas.
Nakagami Model	Suitable for urban settings, accounting for **signal fading** due to obstacles and reflection.
Log-Normal Shadowing	Models the impact of **physical obstructions** such as buildings and trees on signal strength.

Simulation Tools:

- **NS-2**: Uses Nakagami model for urban scenarios.
- **OMNeT++**: Defaults to free space model, customizable.

Accurate signal modeling helps optimize transmission range, improve QoS, and enhance packet delivery reliability.

Challenges in Routing for VANETs

- **Highly dynamic topology makes routing difficult.**
- **Frequent disconnections and mobility require real-time adaptability.**
- **Traditional MANET protocols like AODV, DSR not always effective.**
- **Goals: Minimize delay, reduce control overhead, and ensure robust delivery in urban and highway scenarios.**

Classification of VANET Routing Protocols

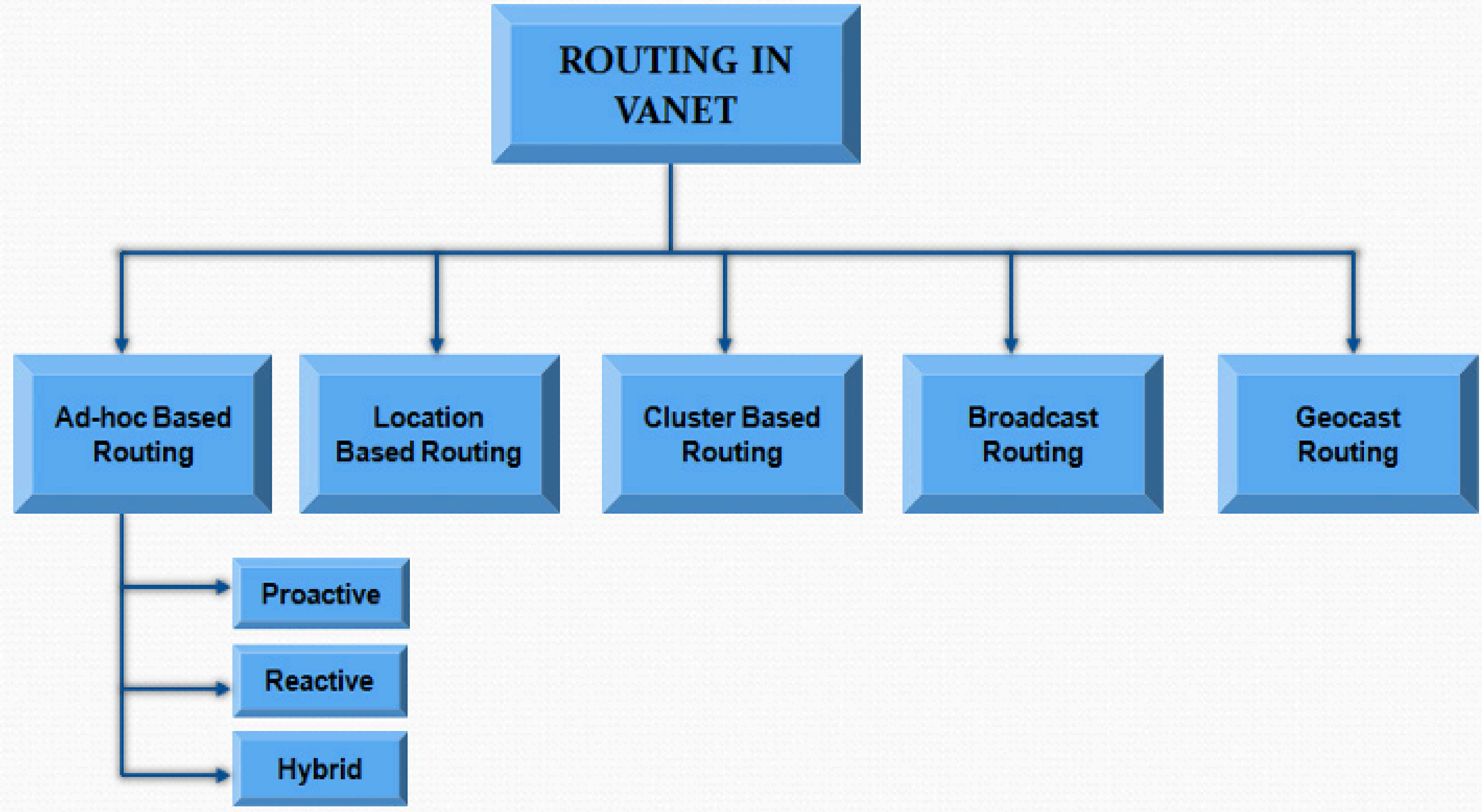

Figure 3. Routing Types in VANET

1. **Topology-Based:**
   - Proactive (e.g., OLSR): Frequent updates, higher overhead.
   - Reactive (e.g., AODV): Route discovery on demand.
   - Hybrid (e.g., TORA): Combines both.
2. **Location-Based (e.g., GPSR, GSR):**
   - Uses GPS/location info to forward packets efficiently.
3. **Cluster-Based (e.g., LORA-CBF):**
   - Vehicles grouped into clusters, cluster heads manage routing.
4. **Broadcast (e.g., BROADCOMM):**
   - Flooding based, used for emergency message dissemination.
5. **Geocast (e.g., ROVER, VADD):**
   - Sends messages to a Zone of Relevance (ZOR) only.

Security Threats and Approaches in VANETs

Security Threats in VANETs

Bogus Information

- Malicious nodes send false alerts (e.g., fake accidents or hazards), misleading other vehicles and disrupting safety systems.

ID Disclosure

- Attackers can track vehicles by analyzing broadcast messages, leading to privacy violations and location tracking.

Denial of Service (DoS)

- Attackers flood the network with excessive traffic, blocking legitimate communication and potentially causing safety issues.

Replay Attacks

- Valid messages are intercepted and resent later to mislead or confuse the system.

Sybil Attacks

- A single malicious vehicle assumes multiple identities to manipulate trust-based routing or traffic flow.

Security Solutions in VANETs

Public Key Infrastructure (PKI)

- Ensures messages are authenticated and sent by trusted vehicles using digital certificates.

Pseudonym IDs

- Vehicles use frequently changing temporary identifiers to protect driver identity and prevent tracking.

Authentication & Trust Models

- Nodes verify each other's legitimacy using behavior-based trust scores or certificate validation to filter out malicious actors.

Timestamps and Nonces

- Messages include unique timestamps or random values to confirm freshness and prevent replay attacks.

Trust-Based Filtering & Monitoring

- The system uses trust ratings or detection mechanisms to block fake identities and prevent Sybil attacks.

Key Research Areas

- **QoS (Quality of Service)**: Minimum delay, high connectivity, low retransmission.
- **Efficient Routing Design**: Delay-tolerant, adaptive, and low-overhead protocols.
- **Scalability & Robustness**: Performance in both sparse (highway) and dense (urban) environments.
- **Cooperative Communication**: How much data should be shared among nodes?
- **Advanced Security Mechanisms**: Lightweight cryptography and real-time trust management

Conclusion

- VANETs enable **smart**, **safe**, and **autonomous transportation**.
- **Unique characteristics** and **challenges** due to **mobility** and **environment**.
- **Routing** and **security** are key concerns.
- A **promising field** for future research in intelligent transport systems

THANK YOU!