

CS8601 –MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.8. VANET: VEHICULAR AD - HOC NETWORK

The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network.

Vehicular Ad Hoc Networks (VANETs) are created by applying the principles of Mobile ad hoc networks (MANETs) - the spontaneous creation of a wireless network for data exchange - to the domain of vehicles. They are a key component of Intelligent Transportation Systems (ITS).

The term VANET became mostly synonymous with the more generic term inter-vehicle communication (IVC).

VANET is an application of mobile ad hoc network. More precisely a VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers.

WORKING OF VANET

VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range.

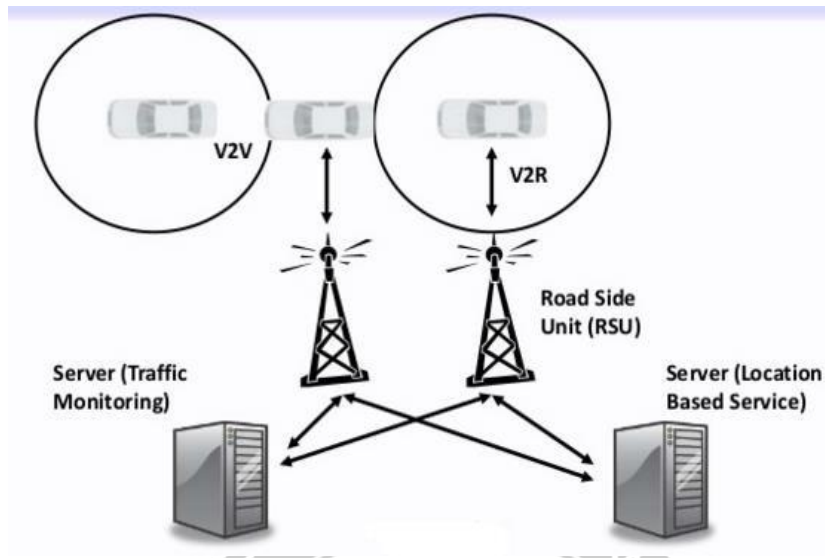
As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created.

It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

COMMUNICATION IN VANET

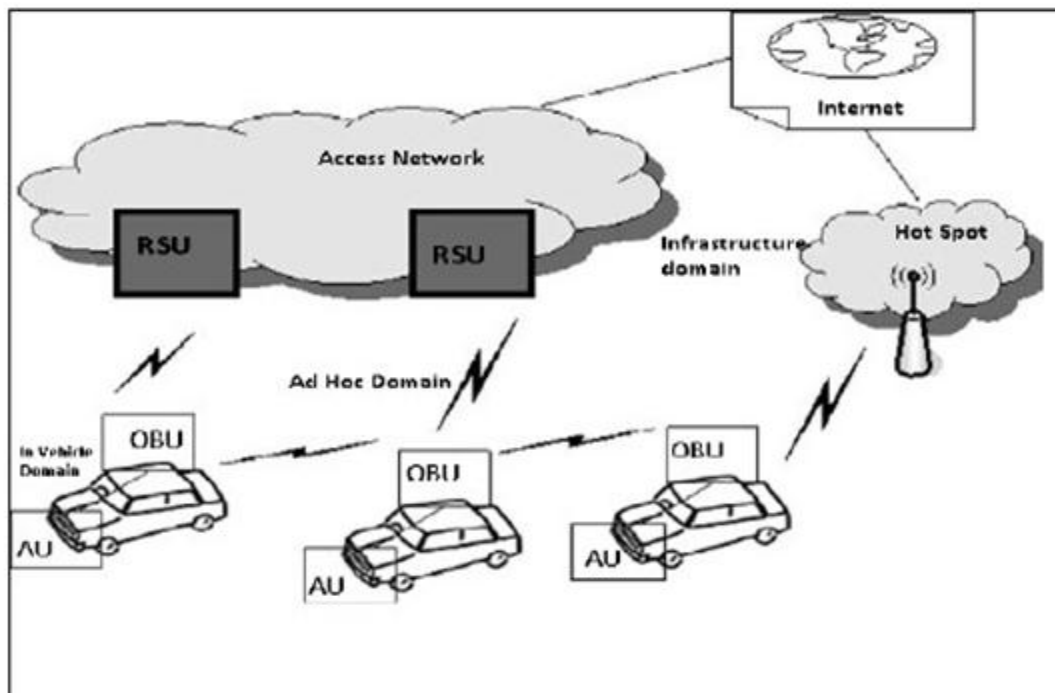
Two types of communication are provided in the VANET.

- First a pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure.
- Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle.



ARCHITECTURE OF VANET

Each node in VANET is equipped with two types of unit i.e. **On Board Unit (OBU)** and **Application Unit (AU)**. OBU has the communicational capability whereas AU executes the program making OBU's communicational capabilities. An RSU can be attached to the infrastructure network which is connected to the Internet.



TECHNOLOGY USED IN VANET

To establish a VANET, IEEE has defined the standard 802.11p or 802.16 (WiMax). A Dedicated Short Range Communication (DSRC) is proposed which is operating on 5.9GHz band and uses 802.11 access methods. It is standardized as 802.11p which provides short range communication with low latency.

CHARACTERISTICS OF VANET

High Mobility: The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy

Rapidly changing network topology: Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.

Unbounded network size: VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.

Frequent exchange of information: The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.

Wireless Communication: VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication.

Time Critical: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

APPLICATIONS OF VANET

i) Safety Related Application:

These applications are used to increase the safety on the roads. These applications can be further categorised in following way.

Collision Avoidance: If a driver gets a warning message on time then the collision can be avoided.

Cooperative Driving: Drivers can get traffic related warning signals & these signals can co-operate the driver for an uninterrupted and safe driving.

Traffic optimization: Traffic can optimized by the use of sending signals like jam, accidents etc. to the vehicles so that they can choose their alternate path and can save time.

ii)User Based Application:

These applications provide the user infotainment. A VANET can be utilised to provide following services for the user apart from safety:

Peer to peer application: These application are useful to provide services like sharing music, movies etc. among the vehicles in the network.

Internet Connectivity: People always want to connect with the Internet all the time. Hence VANET provides the constant connectivity of the Internet to the users.

Other services: VANET can be utilised in other user based application such as payment service to collect the toll taxes, to locate the fuel station, restaurant etc.

CHALLENGING ISSUES IN VANET

Network Management: Due to high mobility, the network topology and channel condition change rapidly.

Congestion and Collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. In rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment.

MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue.

Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied

SECURITY ISSUES IN VANET

Lack of physical boundary: Each mobile node functions as a router & forwards packets from other nodes. AS a result, network boundaries become blurred. So it is difficult to deploy firewalls or monitor the incoming traffic.

Low power RF transmission: It is possible for a malicious node having high power RF transmission capability to continuously transmit & monopolise the medium & cause its neighbouring nodes or the entire targeted MANET to wait endlessly for transmitting their messages. Also signal jamming can lead to denial-of-service(DOS) attack.

Limited computational capabilities: Nodes in an ad hoc network usually have limited computational capabilities. It therefore becomes difficult to deploy compute-intensive security solutions such as setting up a public-key cryptosystem. Inability to encrypt messages invites a host of security attacks such as spoofing as well as several other forms of routing attacks.

Limited power supply: Since nodes normally rely on battery power, an attacker might attempt to exhaust batteries by causing unnecessary transmissions to take place at the targeted node or might cause excessive computations to be carried out by the targeted nodes.

Real time Constraint: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

Low tolerance for error: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.

MANET Vs VANET

MANET	VANET
Collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.	Nodes(vehicles) can communicate with certain roadside infrastructures or base stations.
The node movement is more random in nature	The node mobility is constrained to the road topologies.
Power is a major constrained	The battery power available in a vehicle is quite adequate.
Cost of production is cheap	Expensive
Change in network topology is slow	Frequent & very fast
Node lifetime depends on power resource	Depends on lifetime of vehicles
Multi-hop routing is available.	Weakly available.
Attribute based addressing scheme	Location-based