A Detailed Survey on VANET Environment

B. Iswarya, Dr. B. Radha,
Research Scholar, Associate Professor
Department of Computer Science
Sree Saraswathi Thyagaraja College, Pollachi, India.

ABSTRACT: Vehicular Ad-Hoc Network (VANETs) is a technology which considers vehicles as a node to form a network. VANET is an emerging technology in research, academic and application area. VANETs area specific type of moving network in which nodes are cars with processing, storage and wireless communication capacity. VANET can be considered as a prominent technology to provide safety applications for travellers. Traveller's safety has been the challenging issue in traffic control management and infotainment applications. The main goal of VANET is to provide safety information among the nodes (i.e. Vehicles).

Keywords:

VANET, Protocols, Vehicles, Communication, Traffic, Technology, Application.

I. INTRODUCTION

Vehicular Ad-hoc network (VANETs) is a core application of Mobile Ad-hoc Network (MANETs). VANET is a self-configuring network like MANET. A VANET is a technology that considers moving vehicles as nodes in a network. Vehicles in VANET moves at higher speed from 0 to 40 m/s. VANET can improves the safety and provides comfort of driving for the passengers while travelling. In VANET vehicle leaves the network and other vehicles can join the network to create a mobile network.

VANETs are considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation system. Connectivity in Vehicular Ad-hoc networks is continuously changing due to high mobility of vehicles, causing rapid changes in the network topology [1]. Vehicular Ad-hoc network includes different classes of vehicles such as trucks, cars, buses, motorcycles and bicycles. The problem of VANET applications is mobility because the vehicles travel at different speed according to the traffic condition [Sparse & Dense Traffic], Road conditions [Rural & Urban areas].

VANET improves secure transportation and provides information to the drivers about the condition of road, traffic jams and weather conditions. In recent trends the car manufactures are supplying vehicles with Onboard Unit (OBU), GPS (for navigation), wireless communication devices and sensors (RADAR, LADAR).

The main purpose of VANETs applications is to collect and transform information to the drivers to make a decision. VANETs can connect to vehicles within the range of 100 to 900 mtrs if 802.11p technology is used.

Vehicular Communications is considered as an enabler for driverless cars of the future transportation system. The Privacy issues are concerned with protecting and disclosing driver's personal information such as name, location, plate number and so on [2]. Security issues in VANETs are Confidentiality, Authenticity, Integrity, Availability and Non-Repudiation aimed to secure communication between V2V and V2I is shown in figure [1].

How Communications work?

VANETs communication technology accumulate all data associated with Road conditions including traffic density, speed, direction of vehicles and weather conditions to prevent accidents and to provide comfort for driving and travelling.

1. **Vehicle to Vehicle Communication** – The messages are transformed between the vehicles without any support of infrastructure.
2. **Vehicle to Infrastructure/Road Side Unit Communication** – the communication is between the vehicle, nearby fixed equipment and the Road Side Unit (RSU).
3. **Hybrid Communication** – It combines both the V2V and V2I/V2R communications.

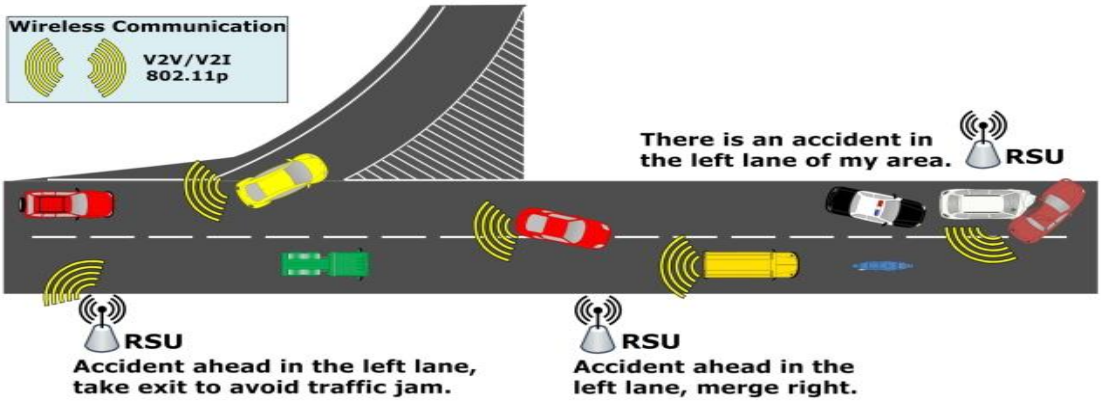

Figure [1]

How Communications work?

VANETs communication technology accumulate all data associated with Road conditions including traffic density, speed, direction of vehicles and weather conditions to prevent accidents and to provide comfort for driving and travelling.

4. **Vehicle to Vehicle Communication** – The messages are transformed between the vehicles without any support of infrastructure.
5. **Vehicle to Infrastructure/Road Side Unit Communication** – the communication is between the vehicle, nearby fixed equipment and the Road Side Unit (RSU).
6. **Hybrid Communication** – It combines both the V2V and V2I/V2R communications.

II.VANETCHALLENGES & CHARACTERISTICS

There are some challenges and issues in VANETs that need to be overcome. In VANETs network connections are not constant, some of the key challenges are

1. **Lack of centralized infrastructure –** There is no centralized infrastructure.
2. **Network Management –** The topology of network can change rapidly due to high mobility.
3. **Security –** VANETs provide safety applications to transform the life critical emergency messages.
4. **Frequent Disconnections –** In VANETs vehicles travel at random speed especially on Sparse / Dense Traffic conditions.
5. **Congestion and Collision Control –** Unbounded network size creates a challenge. The traffic condition is sparse in rural areas and night time in urban areas.
6. **MAC Design –** VANETs are generally use the shared medium to communicate.
7. **Environmental Impact –** VANETs use the electromagnetic wave for communication.

The characteristics of VANETs can be summarized as

1. **Mobility –** The vehicles in VANET usually moves at high speed. This is challenging to predict the position of vehicle.
2. **Rapidly Changing network topology –** The vehicles in the VANETs moves at random speed and at different direction. Due to mobility, the vehicles position will change frequently. The nodes can leave/join the network within the short period.
3. **Unlimited battery power –** The vehicles travel with their own battery, there's no limited power supply for the components to function properly.
4. **Unbounded Network size -** Network size is not limited to a particular range [Rural/Urban].
5. **Frequent Exchange of Information –** Information can be transformed between vehicles and RSU.
6. **Wireless communication –** Vehicles are connected each other and transforms their information via wireless.
7. **Time Critical –** The information must be delivered to the vehicles within time limit to avoid unwanted delays.
8. **Better physical protection –** In VANETs vehicles are considered as nodes, nodes are special physically, it's more difficult to compromise physically and also reduce physical attack on the Infrastructure.

III. VANET APPLICATIONS AND TECHNOLOGIES

VANETs Applications are classified into

1. Safety Applications.
2. Non-Safety or Infotainment applications.

Safety Applications are such as Lane Changing, Intersection Warning, Emergency Approaching Vehicle, Rollover Warning, Cooperative Collision Warning are improved to minimize road accidents and to provide safe to passengers by applying traffic control monitoring applications.

Non-Safety or Infotainment Applications enable the travellers to surf on the Internet/Web browser, online games, hotel booking, payment services and updating of information while travelling.

VANET is a technology which uses moving vehicles as a node in a network. In Intelligent Transportation System [ITS] moving vehicles are connected and communicated via wireless communications. Some of the wireless technologies are considered as **refer fig.2.**

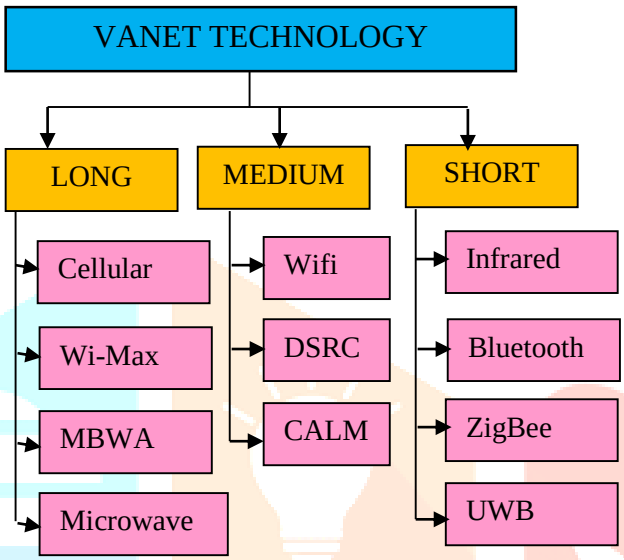

Figure 2 – Wireless technologies

IV. POSSIBLE ATTACKS IN VANET

There are number of possible attacks in VANETs. The main purpose of attackers is to create problem for users.

1. **Sybil Attacks –** creation of multiple fake nodes to broadcast the false information.
2. **Node Impersonation –** It is an attempt by a node to send modified message & claims the message passed from originator for the unknown reason.
3. **Sending False Information –** It can be described as transforming the Incorrect and fake information purposely by one vehicle to another to create misinterpretation scenarios.
4. **ID Disclosure –** The node is able to disclose the identity in the network and track the location of the target nodes and sends a virus to the nearby nodes of the target nodes. When the neighbour nodes are attacked by virus, then they can easily take the location and Id of the target node.
5. **DoS and DDoS Attack –** They attack the network's nodes to cause the channel or some problem to network nodes.

V. VANET ROUTING PROTOCOLS

The main goal of routing protocol is to select the best routing path in less time with less expensive. The routing involves finding the best route from source to destination. The routing protocols are classified into different categories they are

1. **Topology based routing protocol –** This type of protocol uses the existing link information in network to forward the packet. It is further classified into i) Proactive Based Routing Protocol – It is also known as table driven routing protocol. They do not have any initiated route discovery. ii) Reactive based routing protocol – It is also known as on-demand routing protocol. It opens the route only when it is necessary for a vehicle to communicate each other. iii) Hybrid Routing Protocol – It is used to reduce the control overhead of proactive and decreases the initial route discovery delay in reactive routing protocol. Some of the Topology based routing protocols are FSR, OLSR, TBRF, AODV, DSR, TORA, ZRP AND HARP.
2. **Position Based Routing Protocol –** These protocols use geographic positioning information to select the next forwarding nodes. So there is no global route between source and Destination needs to be created and maintained. Position based routing protocols are classified into GPSR, VGPR, MIBR, GYTAR.

3. **Geocast Based Routing Protocol –** These type of protocols are used to send a message to all vehicles in a pre-defined geographical region. Geocast based routing protocols are further classified into ROVER and DTSG.
4. **Cluster Based Routing Protocol –** The network is divided into sub-networks or substructures are called as clusters. Cluster based routing protocol is a virtual grouping formed among the vehicles. Some of the cluster based routing protocols are CBLR, CBR, and CBDRP.
5. **Broadcast Based Routing Protocol –**The packets are not forwarded and routed by the routers in any network. Some of the Broadcast Based routing protocol includes EAEP, DVCAST, SRB, and PBSM.

CONCLUSION

In this paper we have discussed about various aspects of VANETs like it's Characteristics, Challenges, VANET Technologies and it's Applications, VANET attacks and security issues involved in VANET Routing Protocols. Travellers need a safe and secured environment while travelling on the road.

The VANETs Safety Applications overcome the problems to reach a secure VANET environment in the future. In future the research work will be considered in the area of safety Applications.

REFERENCES

[1]. Marina Wadea, Ahamed Mostafa, Dharma P.Agarwal and Ahmed Hamad "Enhancing VANET Connectivity through Utilizing Autonomous Vehicles" The 4th International Workshop on Cooperative Wireless Networks – 2017, page No. 2004-2011.

[2]. Ahmad Yusri Dak, Saadiah Yahya, Murizah Kassim, "A Literature Survey on Security Challenges in VANETs" International Journal of Computer Theory & Engineering, Vol.4, No.6, dec 2012, Page No. 1007-1010.

[3]. Ram Shringa Raw, Manish Kumar, Nanhay Singh "Security Challenges, Issues and Their solutions for VANET" International Journal of Network Security and It's Apllications, Vol.5, No.5 Sep-2013, Page No. 95-106.

[4]. Chan-ki Park, Kuk – Hyun Cho, Min-Woo Ryu, Si-Ho Cha, "Measuring the Performance of Packet size and Data rate for Vehicular Ad-Hoc Networks".

[5]. E.A. Donato, G. Maia, E.R.M. Madeira and L.A. Villas "Impact of 802.11p Channel Hopping on VANET Communication Protocols", IEEE Latin America Transactions Vol-13 No.1, Jan-2015, Page No. 315-320.

[6].Bhuvaneswari.s,Divya.G, Kirthika.K.B and Nithya.S "A Survey on Vehicular Ad-hoc Network" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering vol-2, Issuse 10, oct – 2013, Page No. 4993-5000.

[7]. M. Shahid Anwer, Professor Chris Guy, "A Survey of VANET Technologies" Journal of Emerging Trends in Computing & Information Sciences Vol-5, No. 9, Sep – 2014, Page No. 661-671.

[8]. Felipe Domingos de Cunha, Leendro Villas, Azzedine Boukerche, Guilherme Maia, Aline Carneivo Viana, Raquel A.F. Mini, Antonio A.F. Loureivo "Data Communication in VANETs: Survey, Applications and Challenges" HAL sep-2016.

[9]. Jagadeesh Kakarla, S. SivaSathya, B. Govindha Laxmi, Ramesh Babu B, "A Survey on Routing Protocols and its Issues in VANET", International Journal of Computer Applications, vol-28, No.4, Aug-2011, Page No.38-44.