A Survey on VANET Technologies

Tanuja K
Assistant Professor,
Acharya Institute of
Technology, Bangalore

Sushma T M
Assistant Professor,
Acharya Institute of
Technology, Bangalore

Bharathi M
Associate Professor,
SJCIT, Chikaballapur

Arun K H
PG Student
SJCIT, Chikaballapur

ABSTRACT

VANETS are considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. A VANET will be a major contribution toward the realization of Intelligent Transportation Systems. The main aim of VANET ranges from improved road safety, time critical safety applications, optimized traffic flow, delay tolerant, and infotainment and so on. High relative nodes pace and high active nodes mass has offered a typical challenges for connectivity within VANET. A lot of researches from the industry, academia, and standardized agencies to develop standards and prototypes for vehicular networks. In this paper, a complete survey on existing technologies in VANET is being presented.

Keywords
VANET (Vehicular Adhoc NETwork), OBU (On Board Unit), RSU (Road Side Unit), AU (Application Unit), DSRC (Dedicated Short Range Communication), WAVE (Wireless Access for Vehicular Environment).

1. INTRODUCTION

Vehicles are needed for transportation. People drive cars so that they can have the freedom they need to be able to get where they need to go when they need to get there. Due this reason number of vehicles is increased. The increase in vehicles leads to lot of mishaps on the road which can happen in highway or city areas. To overcome these catastrophes a good communication network need to be built between the vehicles. This leads to a new advance technology Vehicular Adhoc NETwork (VANET). VANET is one of the sub branches of MANET technology. In Mobile Adhoc NETwork (MANET) each mobile is considered as node whereas in VANET each vehicle is considered as a node. These days, an immense number of auto organizations are conveying vehicles with in-auto sensors, installed figuring and remote specialized gadgets, and navigation systems (e.g., GPS) in preparation for the use of large-scale vehicular networks. By using different sensors, cameras and communication competence, vehicles can gather and interpret information with the intention of helping the driver to make a judgment, particularly in driver support systems.

2. MANET vs VANET

Fig 1 gives the comparison between MANET and VANET. The nodes in MANET and VANET are self-composed, self-guided specially ad hoc network and decentralized in a distributed manner with a self observed authority or a server to direct the communication. Nodes themselves go about as servers and/or clients by exchanging and sharing data like peers. Even though VANET is a subpart of MANET, there are lot of difference in the characteristics of MANET and VANET. The MANET can contain many nodes that have uncontrolled moving prototypes. But since VANET is created generally by vehicles so node movement is limited by factors like road lane, traffic and traffic regulations.

2.1 MANET Characteristics and Applications
2.1.1 MANET Characteristics

Distributed operation: For the central control of the network operations, thusly there is no backgrounds arrange rather the control of the network is conveyed among the nodes. The nodes included in a MANET ought to coordinate with one another and convey among themselves
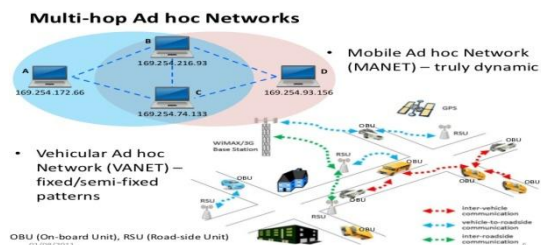
.

Fig 1: MANET vs VANET

Multihop routing: At the point when a nodes tries to send data to different nodes which is out of its communication go, the packet ought to be sent through lone or more intermediate nodes

Autonomous terminal: In MANET, every mobile node is a free node, which could work a host and in addition a switch

Challenges in MANET

MANET owns several challenges such as dynamic topology, limited physical security, limited bandwidth, energy and power constraints [1].

Dynamic topologies: Without reasonable explanation nodes can unconditionally move. In this way, the network topology which is typically multihop may adjust arbitrarily and rapidly at unpredictable times, and may incorporate both bidirectional and unidirectional connections

Bandwidth-constrained: Wireless links will go on with to have notably lesser capacity than their hardwired counterpart. Further, for the effects of multiple access, fading, noise, and interference conditions etc., the realized throughput of wireless communications after accounting is often much less than a radio's maximum transmission rate

Variable capacity links: Congestion is commonly ordinary instead of the special case is one of the impacts of the relatively low to direct link limits. Since the mobile network is frequently essentially an extension of the settled network infrastructure, mobile adhoc users will request comparative administrations. As there is a rise in multimedia computing and collaborative networking applications, these demands will continue to increase

Energy-constrained operation: Few or every node in a MANET may depend on batteries or other drainable means for their energy. For these nodes, energy conservation is the most vital system design reason for optimization

Limited physical security: Compare to fixed cable nets mobile wireless networks are usually more vulnerable to physical security threats. The attacks, for example, eavesdropping, spoofing, and denial-of-service ought to be mindfully considered. The present techniques on link security are regularly connected inside of remote systems to decrease security dangers. As favorable position, the network control in MANETs on account of decentralized nature offer additional robustness against the single purposes of breakdown contrast with incorporated methodologies

2.1.2 Applications of MANET

MANET has wide range of applications varying from tactical network, home appliances, etc., [2].

Tactical networks: Military communication and operations, automated battlefields.

Emergency services: Search and rescue operations, Disaster recovery, Replacement of fixed infrastructure in case of environmental disasters, Policing and fire fighting, Supporting doctors and nurses in hospitals

Commercial and civilian : E-commerce: electronic payments anytime and anywhere environments, Business: dynamic database access, mobile offices, Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks, Sports stadiums, trade fairs, shopping malls , Networks of visitors at airports

Home and enterprise: Home/office wireless networking, Conferences, meeting rooms Personal area networks (PAN), Personal networks (PN), Networks at construction sites

Education: Universities and campus settings, Virtual classrooms, Ad hoc communications during meetings or lectures

Entertainment: Multi-user games, Wireless P2P networking, Outdoor Internet access, Robotic pets, Theme parks

Home applications: smart sensors and actuators embedded in consumer electronics, Body area networks (BAN), Data tracking of environmental conditions, animal movements and chemical/biological detection.

2.2 VANET characteristics and Applications

2.2.1 VANET Characteristics

VANET poses following characteristics [3][7]

Extremely active topology: The super swiftness of the vehicles in VANET leads to constant change in the topology and the availability of multiple paths makes VANET an extremely active topology

Predictable Motion Patterns: Inspite of fast motion of vehicle it is difficult to predict the position and movement of vehicle, but in VANET environment most of the vehicles move on pre-defined roads and highways. This allows the use of predictable motion patterns in network design

Interaction with onboard sensors: Sensors are the means of communications in VANET. Sensors can communicate to the main data center by reading data associated to velocity and direction of the vehicle. Therefore for link formation and in routing protocols sensors can be used

No constraint on Battery Power and Storage: The nodes in VANETs have better battery power and storage compared to sensor networks

VANET Challenges

VANET possess several challenges such as frequent disconnected network, Delay constraints, security.

Frequent disconnected network: The speedy nature of the vehicles describes the dynamic topology which in turn requires an infrastructure (RSU) to be connected (V2V, V2I). The lack of such infrastructure results in frequent disconnections

Stringent Delay constraints: At some situation, delivery of emergency messages on time is very essential compare to only high data rates

Mobility modeling: As one of the characteristic of VANET is dynamic topology, to develop VANET environment effectively and efficiently , a perfect mobility model is required

Security and Authentication: The major issue is V2V communication is maintaining the security of message content. To utilize the information as early as possible, the content of a received message has to be verified within a short time. The authentication is assured with guarantee that the communication is authentic in its entities. Only when broadcast messages are generated by legal senders, vehicle should react to events

Integrity and Confidentiality: The integrity deals with the stability of the messages. It's a real challenge to assure the order of messages, i.e., the messages are received as sent, without any modification, insertion, reordering. Confidentiality is also one of the major challenge give the guarantee that the privacy of drivers against unauthorized observers is secured

Availability & Scalability: Indeed, even a powerful correspondence channel can in any case encounter a few attacks, (for example, deny of service) which can cut down the network. Subsequently, availability is likewise major deal in VANET. The term scalability implies that despite the fact that the activity volume gets expanded there ought to be no performance degradation or even network blackout, without changing the system components and protocols

2.2.2 VANET Applications

VANET has wide range of applications varying from traffic signal to entertainment [4].

Traffic Signal: With the help of technologies of VANETs, communication from the traffic light can be created. Safety applications is one in which a slow or motionless vehicle will broadcast alert message to its neighborhood. Notification about road congestions which can be used for route and journey planning. Vehicular networks have been shown to particularly useful for traffic management

Vision Enhancement: In vision enhancement, drivers get a reasonable sight of vehicles and checks in substantial mist environment and can pick up learning of the presence of vehicles covered up by blocks, structures, and by different vehicles

Other infotainment: Climate related data can be redesigned/ asked for by an application through Dedicated Short Range Communication (DSRC). In after accident a notice, would show alert messages about its circumstance to platooning vehicles to pass the data to the roadway watch for backing up. Parking spot serves to discover the availability of opening in parking lot in a certain land region according to the climate conditions. For the convenience of the vehicle, roadway and urban zone maps give the data which evade the congested driving conditions and mischance conditions furthermore give most limited way in discriminating circumstance which spares the time

Safety: Safety applications incorporate immediate impact cautioning, forward obstacle recognition and evasion, crisis message scattering, highway/rail crash shirking, left/right turn collaborator, path evolving cautioning, stop sign development aide and street condition cautioning, convergence choice bolster, helpful driving (e.g. impact cautioning, path blending, and so on)

Entertainment: Entertainment comes under non-safety applications. A number of applications aim to entertain passengers who spend a very long period in transit. Such as providing Internet access, radio FM, gaming mobile commerce, multimedia, streaming. Non-safety applications communication is on demand only request response bases

3. COMMUNICATION TYPES IN VANET

In VANET, Vehicle to Vehicle (V2V) communication, Vehicle to Infrastructure (V2I) communication, Infrastructure to Infrastructure (I2I) communication also called Hybrid communications are the main research goals of ITS(fig 2). In this section we are discussing each of these communications in detail.

3.1 Vehicle to Vehicle communication

V2V (Vehicle to Vehicle) [6] is designed to allow automobile to talk to each other. The system will use a region of 5.9GHz band using wireless protocol standard 802.11p for various public safety services. This technology is for safety and is dynamic wireless exchange of data between nearby vehicles that offers the opportunity for significant safety improvements. Data exchanged may include a vehicle's position, speed, steering angle, brake status, turn signal status, number of people in vehicle etc. V2V communications enables a vehicle to sense threats and hazards with an awareness of position of other vehicles and the threat or hazard they present. Message can be derived using non vehicle based technology such as GPS V2V communication technology uses Dedicated Short Range Communications (DSRC).
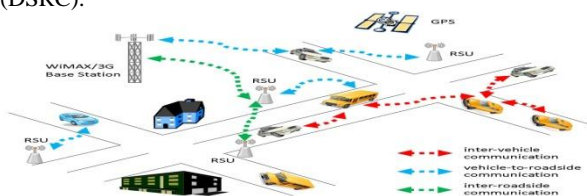

Fig. 2: Types of VANET Communications

Advantages of V2V communication

➢ Allows short and medium range communication

➢ It does not need any roadside infrastructure.

➢ Less cost

➢ It supports short message delivery

➢ It minimizes latency in communication link

➢ It is fast and reliable and provides real time safety

➢ Protect vehicles from potential road hazards and improve safety

Disadvantages of V2V communication

➢ Frequent topology partitioning due to high mobility

➢ Problems in long range communication

➢ Using traditional protocol is challenging

➢ Problem in broadcasting messages in high traffic & environmental forces

Applications of V2V

Applications are classified into 3 categories

a. Road safety applications

➢ Preventing collisions

➢ Preventing obstacles it can be fixed or mobile

➢ Distributing whether information

b. **Driver assistance applications**

➢ Helps in vehicle passing

➢ Prevention of straight or carved lane exists

c. Comfort applications

➢ Mobile access to the Internet

➢ Electronic messaging

➢ Inter-vehicle chat,

➢ Network games, etc.

3.2 Vehicle to Infrastructure Communication

In vehicle to infrastructure allows a vehicle to communicate with the roadside infrastructure mainly for information and data gathering applications. It is also called as Ad Hoc domain on VANET [14]. Fig 3 shows how one vehicle communicates with another vehicle directly if there is a direct wireless connection available between them, forming a single hop vehicle to vehicle communication (V2V). When there is no direct connection between them a dedicated routing protocol is used to forward data from one vehicle to another until it reaches the destination point, forming multi-hop vehicle to vehicle communication. Vehicle communicates with RSU in order to increase the range of communication by sending, receiving and forwarding data from one node to RSU to process special application forming vehicle to infrastructure. The information transferred between vehicle and RSU is more secure, because the RSU provides unique key for each and every user connected to it. V2I provides long range of communication.

V2I system should contain the following part

a. Vehicle On - Board Unit or Equipment (OBU/OBE)

b. Road Side Unit or Equipment (RSU/RSE)

c. Safe communication channel

OBUs are vehicle side of V2I system. OBUs are logically composed of radio transceiver (typically DSRC), a GPS system, an applications processor and interfaces to vehicle systems and vehicle's human machine interface (HMI) communications network. OBUs provide communications between both vehicles and RSUs and between the vehicles and other nearby vehicles. The OBUs transmits status messages regularly to other OBUs to support safety applications between vehicles. At intervals, the OBUs gather data to support public applications. The OBUs will accommodate storage of many snapshots of data, depending upon its memory and communications capacity. After some period of time, the oldest data is overwritten. The OBUs also assemble vehicle data together with GPS data as a series of snapshots for transmission to RSU.   RSUs located at intersections and other locations providing the interface to vehicles within their range.

A RSU is composed of radio transceiver (DSRC or WAVE), an application processor, and interface to V2I communications network. It also has a GPS unit attached. Through an additional interface, it may support local infrastructure safety applications. The RSU is connected to V2I communications network. Using its interface to V2I communications network, it can send private data to and from the OEMs. The RSU manage the prioritization of messages to and from the vehicle.OBU also has priorities set within its applications and prioritization must also be set within the RSU to ensure that available bandwidth is not exceeded. Local and vehicle to vehicle safety applications have highest priority, messages associated with various public and private network applications have lower priority. Entertainment messages have lowest priority.

Fig 3: Architecture of V2I (Source ITS joint Program office, USDOT)

3.3 Hybrid Communication

The RSU can connect to the infrastructural networks or to the Internet, allowing the OBU to access the infrastructure network. In this case it is possible that the AUs are registered with the OBU to connect to any internet based host. OBU can also communicate with other hosts for non-safety applications, using the communication of cellular radio networks (GSM, GPRS, UMTS, HSDPA, WiMax and 4G) [7]. It combines both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) (fig 4). In this scenario, a vehicle can communicate with the roadside infrastructure either in a single hop or multi-hop fashion, depending on the distance, i.e., if it can or not access directly the roadside unit. It enables the long distance connection to Internet or to vehicles that are so far.

Fig 4: Hybrid Communication

3.4 Infrastructure to Infrastructure (I2I/RSU to RSU) Communication:

RSU connects to the internet and produces needed information for user, when the vehicle is connected to nearby RSU [8]. The vehicle with VANET application contains the positioning system which identifies the nearby RSU. Once the vehicle identifies the nearby RSU, it sends the hello packet to get the conformation.   All information will be provided to user, when they are registered in RSU (for sending warning information between 2 vehicles there is no need of registration).

The authentication is done through digital signature algorithm. This provides the unique key for all the users who had registered in RSU. RSU is placed in each every end of corner of road. When the vehicle is moved out of particular range, handover scheme occurs. The bending information will be transferred from old RSU to new RSU. The service provided by RSU is called service oriented VANET [5].

4. VANET ARCHITECTURE

The basic main components of VANET are the AU, OBU and RSU [6]. The RSU's are communication units located on the roadsides where as OBU's are communication units mounted on vehicles. The RSU may act as host application that provides services and the OBU is a peer device that uses the services provided by the RSU through AU. The application may reside in the RSU or in the OBU; the device that hosts the application is called the service provider and the device using the application is described as the user. Each vehicle is equipped with an OBU and a set of sensors to collect the information and then send it as a message to other vehicles or RSUs through the wireless medium. The RSU can also connect to the Internet or to another server which allows OBU's of multiple vehicles to connect to the Internet.

The VANET architecture consists of central trusted authority (TA) at the root [9]. Under TA there are multiple RSUs and under RSUs there will number of vehicles moving on a road. Every vehicle is mounted with an OBU that has an ability to communicate. Since the transmission range of any vehicle is more than the total width of the road, position of a vehicle has no effect on communication. An OBU/RSU is equipped with private key / public key and a shared key which are provided by its immediate higher authority. TA distributes keys and certificate to short certificates to OBU/RSUs. Each vehicle has tamper proof device to store different keys. A vehicle will receive a short certificate at the time of authentication by TA via the corresponding RSU for inter-vehicle communication. The TA module which performs the encryption of the messages based on their need and sensitivity. If the communication is in between V2V & V2I, there is a need to perform encryption. Each vehicle must be connected to any of the nearest RSU through its OBU. The TA is very much required in the case of emergency vehicle, as the emergency vehicle needs to communicate with other vehicle in a quick manner, and the time and speed of communication play an
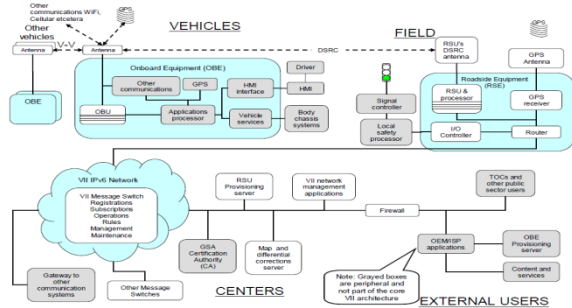
important role in emergency case. In such emergency cases V2I should not implement any encryption method for quick and faster communication. As RSU can be connected to any number of vehicles in its coverage area and hence the storage of the RSUs is also taken into consideration.

4.1 On Board Unit (OBU)

An OBU is a device usually mounted on a vehicle, which is used for exchanging information with RSUs or with other OBUs of different vehicles. It consists of resources which includes a memory used to store and retrieve information, a user interface, a specialized interface to connect to other OBUs and a network device for short range wireless communication based on IEEE 802.11p radio technology. These devices are connected through wireless link based on the IEEE 802.11p radio frequency channel. The main functions of the OBU are wireless radio access, adhoc and geographical routing, network congestion control, reliable message transfer, data security and IP mobility [9].

An OBE is logically composed of a 5.9 GHz DSRC transceiver (OBU), a GPS system, an applications processor and interfaces to vehicle systems and the vehicle's human machine interface (HMI). OBUs provide the communications both between the vehicles and the RSU's and between the vehicle and other nearby vehicles. The OBUs may regularly transmit status messages to other OBUs to support safety applications between vehicles. After some period of time, the oldest data is overwritten.

The set of system components required for OBU are:

Memory for storage: The OBU system must permit to provide a storage space to record the event processed, notified and communicated to the OBU. (Like a black box in airplane which keeps track of all the communication details with the flight)

GPS system: The vehicle must be able to communicate its own position to perform geo- located based position.

Wireless communication: The vehicle should be equipped with one or more communication transceivers to allow communication between V2I and V2V.

Easy Handoff: The OBU must manage handovers with network adapter.

Infotainment: The device should be equipped with different entertainment such as FM, Games etc

Sensors: Sensor networks can be deployed inside the vehicle. These can be used to monitor the driver's physical parameters (heart rate, temperature, etc) (Nakanishi, 2007). The data from these networks could be collected by the OBU for a later analysis. Users' gadgets as PDA or cellular can be used as an interface to generate information or to receive data from the vehicle or the external devices. The user can export data to his laptop at home and register all the information generated in a journey.

Human Interface: The main requirement is that the HI is interactive and non-intrusive, that is, it should be used by the driver while driving. Therefore the developed OBU should be implemented with a touch screen that restricts their use when the car is moving, it is also better that in future a voice system should be included to avoid distraction.

4.1.1 OBU Architecture

The LLC layer provides connectionless and connection-oriented data transfer. Connectionless data transfer is commonly referred to as LLC type 1, or LLC1. Connectionless service does not require establishing data links or link stations explicitly. After a Service Access Point (SAP) has been enabled, the SAP can send and receive information to and from a remote SAP that also uses connectionless service(fig 5). Connection-oriented data transfer is referred to as LLC type2, or LLC2.
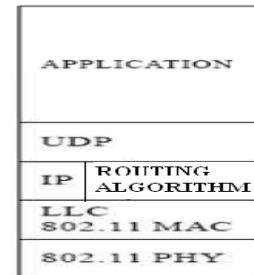

Fig 5: OBU Node on a Vehicle

Connection-oriented service requires the establishment of link stations. When the link station is established, a mode setting command is necessary. Thereafter, each link station is responsible to maintain link state information.

4.2 RSU

In MANET, the nodes will move randomly whereas, in VANET the nodes move in well-defined path. The routing used in VANET are proactive routing, reactive routing, hybrid routing. The vehicle with VANET application contains positioning system, communication facility, and human-machine interface in the vehicle. A vehicle with all these facilities will reduce the number of accidents and the data sharing will be more confidentiality, integrity, and availability. All this are done by using the fixed infrastructure called Roadside Unit (RSU). The Roadside unit is responsible to register the vehicle who wants to participate in VANET to form a group. It connects to internet and produces the needed information for the user, when the vehicle is connected to particular nearby RSU. The vehicle identifies the nearby RSU by using the digital positioning system which is attached in the vehicle. Once the vehicle identifies the nearby RSU, it sends the hello packet to get the confirmation. The responsibility of road side unit is to issue a secret token to each user during registration. Later, authentication process is performed based on the secret tokens issued by the roadside unit. Since tokens are used in authentication of vehicle identity which is protected. In order to prevent malicious vehicle to reveal their tokens to attackers, each token is a unique integer which is dynamically generated by the RSU. All information will be provided to user when they are registered in RSU. But for sending the warning information between two vehicles there is no need for registration. The RSU and vehicles are communicated using DSRC wireless protocol. Main functions of RSU are as under:

a. Extend the communication range.

b. Provide internet connectivity to OBUs.

c. Providing safety applications such as accident warning

4.3 AU

Application Unit (AU) executes the program making OBU's communicational capabilities. The AU is the device equipped within the vehicle that uses the applications provided by the provider using the communication capabilities of the OBU. The AU can be a dedicated device for safety applications or a normal device such as a personal digital assistant (PDA) to run the Internet, the AU can be connected to the OBU through a wired or wireless connection. The distinction between the AU and the OBU is logical. The AU communicates with the network solely via the OBU which takes responsibility for all mobility and networking functions [10] [11].

5. COMMUNICATION STANDARDS FOR VANET

There are numerous wireless access technologies available today, which can be used to provide the radio interface to the vehicles in order to communicate with each other, V2V communication, or to communicate with the RSUs i.e., V2I communication. These communication technologies intended to improve road safety, traffic efficiency and to provide driver and passenger comfort by enabling a set of safety and non-safety applications.

5.1 Long Range Communications

5.1.1 Cellular Technologies
The concept of the cellular system is to reuse the limited frequency available for the service. Global system for mobile (GSM) communication considered to be one of the cellular (fig 6) system standards that provides a data rate of a maximum of 9.6 Kbps and is characterized as a second generation (2G). GSM uses both frequency division multiple access (FDMA) and time division multiple access (TDMA) schemes. Two frequency bands are available for GSM 890–915 MHz for uplink and 935–960 MHz for downlink; these frequency bands are divided into channels and the capacity of each channel is 200 kHz. IEEE 802.11 standards can be applied to provide wireless connectivity; IEEE802.11a works at 5GHz and provides a data rate of 54Mbps with a communication range of at least 38m indoor and a 140m range for outdoor use. Another standard for IEEE 802.11 is IEEE 802.11g, which provides the same data rate and covers the same range as IEEE802.11a but working at 2.4GHz.

The strengths of cellular communication include wide coverage, small mobile units, low cost, high functionality, and the ability to integrate voice and data on the same network [28].

Fig 6: Cellular Technologies

5.1.2 WIMAX Technology
WiMAX is similar to the wireless standard known as Wi-Fi, but on a much larger scale and at faster speeds. A nomadic version would keep WiMAX-enabled devices connected over large areas, much like today's cell phones. WiMAX (fig 7)is based on IEEE 802.16, adopted by IEEE in the year 2004. A single WiMAX antenna is expected to have a range of up to 40 miles with speeds of 70 Mbps or more using multiple-input and multiple-output (MIMO), with an orthogonal frequency division multiplexing (OFDM). As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipment (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz. WiMAX works at 5 bps/Hz and can peak up to 100Mbps in a 20 MHz channel. WiMax will provide your several levels of QoS [15]. WiMAX is suitable for applications such as multimedia, video and voice over internet protocol (VoIP).
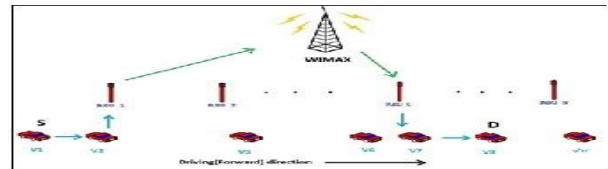
Fig 7: WIMAX TECHNOLOGY

5.2 Medium Range Communications

5.2.1 DSRC
DSRC is a 75 MHz licensed spectrum at a 5.9 GHz band allocated by the US Federal Communications Commission (US FCC) in 1999, to be used solely for vehicle to vehicle and vehicle to infrastructure communication in the United States.

There are two groups of standards supporting DSRC applications, each operating in a different frequency band: 915 MHz and 5.9 GHz. A set of 915 MHz DSRC standards was completed several years ago and is primarily used in commercial vehicle applications, electronic toll collection, and other applications. The set of 5.9 GHz DSRC standards, the majority of which were approved in 2006 or have been voted on and are undergoing revision for approval, are designed to support a larger variety of applications, including collision avoidance, advanced vehicle control, traveler information, increased freight/cargo transport support, transit, parking, and traffic management as well as supporting other private applications (this DSRC 5GHz Standards Group) [12].

Currently this is the only standard with support for direct vehicle-to-vehicle (V2V) communication [32]. DSRC/WAVE systems take out the disadvantages in wireless infrastructure by helping low latency, geographically local and high mobility communications. DSRC/WAVE supports vehicle-to-vehicle and vehicle-to-infrastructure communications for Intelligent Transportation Systems (ITS) which is a part of Federal Highway Authority's Vehicle Infrastructure Integration initiative. DSRC is meant to be a complement to cellular communications. DSRC provides very high data transfer rates and minimal latency. It has a range up to 1000m; data rage is of 6 to 27 Mbps and 7 Licensed Channels.

There are two types of channels in DSRC, all of them with a 10 MHz width: the control channel (CCH) and the service channel (SCH). The CCH is restricted to safety communications only, and the SCHs are available both for safety and non-safety use. Applications for vehicular communications can be placed in three main categories - traffic safety, traffic efficiency and value-added services (e.g. infotainment/business) [11]. In 1999, the U.S. Federal Communication Commission (FCC) allocated these 75 MHz of spectrum at 5,850-5,925GHz to be used exclusively for vehicle-to-vehicle and infrastructure-to-vehicle communications.

In fig 8, the main objective is to enable public safety applications in vehicular environments to prevent accidents (traffic safety) and improve traffic flow (traffic efficiency).

Currently we have at least three different organizations developing standards for safety communication in 5.9 GHz ITS band, each tailored to their specific focus, supporting 802.11p: North American IEEE 802.11p + IEEE P1609 (WAVE), European C2C-CC Communication System (ETSI TC ITS) standardized by European Telecommunications Standards Institute (ETSI), and Global ISO TC204 WG16 (CALM).
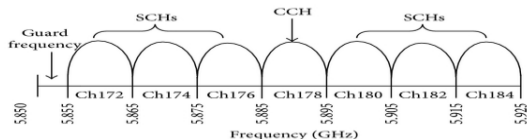

Fig 8: DSRC Spectrum Band and Channels

ARCHITECTURE OF DSRC

The standardization of application services and the corresponding communication architecture of vehicle-roadside communications (DSRC-Dedicated Short-Range Communications) (fig 9) were pursued in CEN TC 278 (Europe) and ISO TC 204 (International) and first draft standards have been issued during 1995. From 1996 to 1998 the validation of the DSRC standards was pursued in the European research project VASCO (Validation of Dedicated Short- Range Communications) [27].

The DSRC Physical Layer standard proposals provide specifications for two media: Micro waves at 5.8 GHz, in particular the bands 5.795-5.805 GHz according to CEPT recommendation for pan-European usage, and 5.805-5.815 GHz available for national usage. Infrared at 850 nm, the default downlink / uplink data rates are 500kbit/s and 250kbit/s respectively. Lower and higher data rates can be chosen after a negotiation phase between OBE and RSE. The DSRC Data Link Layer consists of the Logical Link Control (LLC) and Medium Access Control (MAC) sub-layers. The LLC sub-layer has been adapted from the IEEE 8088.2 specifications for connection-less and connection-oriented services. The MAC sub-layer caters for efficient contention mechanisms to avoid and resolve data collisions in multi-lane environments.
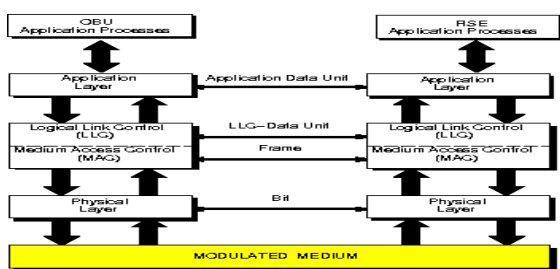

Fig 9: DSRC architecture

The DSRC Data Link Layer has been designed in a medium-independent way, i.e. the parameters can be adapted to both media available for the DSRC.

The DSRC Application Layer provides a service interface for the applications and specifies fragmentation, application multiplexing and a common initialization mechanism for each communication process between OBU and the roadside equipment (RSE).

Physical and MAC Layers: The physical and MAC layers of WAVE are based on IEEE 802.11p standard. The physical layer of IEEE 802.11P consists of seven channels in 5.9GHz

band which is similar to IEEE 802.11a design, but the main difference is that the IEEE 802.11p use 10MHZ bandwidth for each channel instead of 20MHZ bandwidth in IEEE 802.11a. The physical layer of 802.11p uses OFDM technology which is used for increasing data transmission rate and overcoming signal fading in wireless communication.
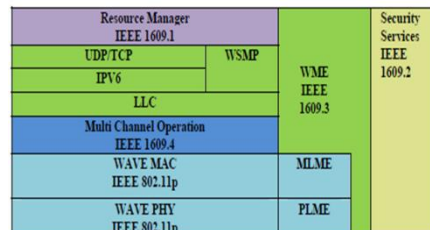
5.2.2 WAVE

Fig 10: WAVE Architecture

One of the specifications of IEEE 802.11p is that the management functions are connected with the physical and MAC layers which are called physical layer management entity (PLME) and MAC layer management entity (MLME), respectively [29]. The IEEE 802.11p uses CSMA/CA to reduce collisions and provide fair access to the channel. The figure 10 shows the architecture of WAVE.

Multichannel operation: IEEE 1609.4 is one of the standards of the IEEE 1609 protocol family, which manages channel coordination and supports MAC service data unit delivery. This standard describes seven different channels with different features and usage (six service channels (SCH) and one control channel (CCH)). In addition, these channels use different frequencies and transmit powers. Logical link control (LLC) is another element of WAVE structure which is similar to upper sub-layer of OSI layer two. LLC provides the communication between upper layers and the lower layer.

Network and Transport layers: The IEEE 1609.3 defines the operation of services at network and transport layers. Moreover, it provides wireless connectivity between vehicles, and vehicles to roadside devices. The functions of the WAVE network services can be separated to two sets:

• Data-plane services: they transmit network traffics and support IPV6 and WSMP protocols. WAVE short-message-Protocol (WSMP) provides this capability that applications can send short message to increase the probability of receiving the messages in time.

● Management-plane services: Their functions are to configure and maintain system, for instance: IPV6 configuration, channel usage monitoring, and application registration. This service is known as WAVE management entity (WME). The devices which use WAVE architecture should implement UDP as specified in RFC 768, and TCP as defined in RFC 793.

Resource Manager: There are two kinds of wireless access in VANETs Roadside unit (RSU) which are the static stations located along the road side, On-board unit (OBU) mounted on a vehicle and can operate while moving. IEEE 1609.1 standard defines a WAVE application known as resource manager (RM) which should allow communication between applications runs on RSUs and OBUs. The RM resides on either OBUs or RSUs.

Security Services: The IEEE 1609.2 standard defines security services for the WAVE architecture and the applications

which run through this architecture. This standard defines the format and the processing of secure messages; furthermore, it describes the core security functions.

There are numerous wireless access technologies available today, which can be used to provide the radio interface required by the vehicles in order to communicate with each other, V2V communication, or to communicate with the RSUs, V2I communication. These communication technologies intended to improve road safety, traffic efficiency and to provide driver and passenger comfort by enabling a set of safety and non-safety applications. Some of these technologies rely on a centralized infrastructure to coordinate the communications between nodes. In contrast, other technologies operate in adhoc mode (distributed coordination).

5.2.3 WiFi (Wireless Fidelity)

WiFi (fig 11) operates in the unlicensed ISM spectrum. It is trivial to deploy by anyone, anywhere and the required hardware is simple and cheap [30] [31]. It has become one of the most widely deployed and popular wireless standards. Wireless fidelity (Wi-Fi) can provide wireless access to enable V2V or V2I communication. IEEE 802.11 standards can be applied to provide wireless connectivity; IEEE 802.11a works at 5 GHz and provides a data rate of 54 Mbps with a communication range of at least 38 m indoor and a 140 m range for outdoor use. Another standard for IEEE 802.11 is IEEE 802.11g, which provides the same data rate and covers the same range as IEEE 802.11a but working at 2.4 GHz (Olariu and Weigle, 2009). IEEE 802.11b works at 2.4 GHz and provides a data rate of up to 11 Mbps (Moustafa and Zhang, 2009).
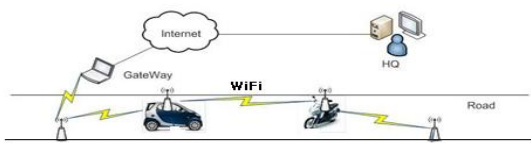

Fig 11: WiFi in VANET

5.3 Short Range Communication

5.3.1 BLUETOOTH

The ISM (industrial, Scientific and Medical) radio bands based Bluetooth (IEEE 802.15.1) protocol is used to transfer data at the rate of up to 1 Mbps to 4 Mbps over a distance of 10m. Bluetooth operates in the 2.4 GHz band and uses it uses Frequency Hopping Spread Spectrum technique to overcome signal interference [30]. Bluetooth Version 3 can work on 6 GHz to 9 GHz frequency band, it uses 2.4 GHz band to communicate with other devices. Bluetooth 4.0 uses low energy for transmission; it is not compatible with earlier versions [25]. It is predominantly used to create a Personal Area Network (PAN). Bluetooth technology can be used to support both V2V and V2I applications [26]. As compared to other Wi-Fi standards, it requires low power. However, it cannot be used to build safety applications because of slow transfer rate, short coverage area and vulnerability to air inferences. It is not suitable for bandwidth intensive infotainment applications such as VoIP and web browsing [13].

5.3.2 ZIGBEE

ZigBee (IEEE 802.15.4) uses the license-free 2.4 GHz band to transfer data at the rate of 250 Kbps up to 70 meters. It also uses lower frequency bands 915MHz (US) and 868 MHz

(Europe) to supports data transmission rates of 40 Kbps and 20Kbps respectively. This technology uses low powered radio signals to transfer data up to 100m using Offset Quadrature Phase Shift Keying (O- QPSK) modulation[16]. Since it uses low-power and low- latency, it is widely used in PANs, remote controls, transport monitoring, and sensor networks. It is simple and cheaper than Wi-Fi and Bluetooth standards. Moreover, it can support more mobile nodes simultaneously and has self-healing capability [17]. Like Bluetooth, it can be used to support V2V and V2I applications. However, it is not suitable for bandwidth intensive infotainment applications such as VoIP, web browsing [18].

5.3.3 INFRARED

It is another popular wireless access technique which uses invisible light to transfer data. It operates in the frequency band between 300 GHz and 400 THz. This broad spectrum is divided into three sub-bands: near- infrared, mid-infrared and far-infrared. Based on the type of sub-band, it can transfer data from 115kbps to 4Mbps. Since infrared signals are affected by obstacles, it is mainly used for short range communication [19]. Though it uses low power, it supports low data rate as compared to other standards such as Bluetooth. This technique is able to transmit voice, data, and video information more securely. It can be used to support safety application due to its ability to support high network traffic and large amount of bandwidth. Japan's most successful application Vehicle Information and Communication System (VICS) uses radio-wave beacons on the expressway and infrared beacons on the arterial routes [20].

5.3.4 Ultra Wideband (UWB)

Ultra wideband (UWB) communications systems are commonly defined as systems with large absolute and/or large relative bandwidth. Such a large bandwidth offers specific advantages with respect to signal robustness, information transfer speed, and/or implementation simplicity, but leads also to fundamental differences from conventional, narrowband, systems [21][22]. It support low power operation, low power dissipation, robustness for multi-path fading and higher throughput of up to 480 Mbps. Like Bluetooth, it has a transmission range of 10m. In VANET, it can be used for collision avoidance. This standard and differential GPS (DGPS) together were used to determine the relative position of a vehicle [23]. A paper by Asmaa El Gueraa shows the performance of the IR- UWB transceiver suitable for inter-vehicle communication system with analyzing the effect of the multi-user interference (MUI) [24].

6. CONCLUSION

This paper provides a broad survey on difference between MANET and VANET, VANET architectures components, VANET communication domains, wireless access technologies, VANET characteristics, challenges and VANET applications. This paper aims to provide the key concepts of VANET to the researchers.

7. REFERENCES

[1] Corson, M.: Information RFC 2501 MANET performance issues (january 1999)

[2] MANET Image: http://cwi.unik.no/images/manet_overview.pdf

[3] communications and network, 2013, 5, 12-15 doi:10.4236/cn.2013.51b004 published online february 2013 (http://www.scirp.org/journal/cn)

[4] VANET Parameters and Applications: A Review Kamini Rakesh Kumar Vol. 10 Issue 7 Ver. 1.0 September 2010 Global Journal of Computer Science and Technology

[5] "A novel approach for data acquisition and handover scheme in VANET"Shanmuga priya PG scholar and Erana veerappa dinesh S ,AP ,Dept. of CSE, VPMM Engineering college for women,KrishnanKoil, India

[6] A comprehensive survey on vehicular Ad Hoc network Saif Al-Sultann, Moath M. Al-Doori, Ali H. Al-Bayatti, Hussien Zedan Software Technology Research Laboratory, De Montfort University, Bede Island Building, Western Boulevard, Leicester LE2 7EW, UK

[7] Applications of VANETs: Present & Future Vishal Kumar1, Shailendra Mishra1, Narottam Chand2

[8] "A novel approach for data acquisition and handover scheme in VANET"Shanmuga priya PG scholar and Erana veerappa dinesh S ,AP ,Dept. of CSE, VPMM Engineering college for women,KrishnanKoil, India

[9] Infrastructure based Authentication in VANETs Brijesh Kumar Chaurasia1 and Shekhar Verma2 1,2Indian Institute of Information Technology, Allahabad, India bkchaurasia@iiita.ac.in , sverma@iiita.ac.in International Journal of Multimedia and Ubiquitous Engineering Vol. 6, No. 2, April, 2011 International Journal of Multimedia and Ubiquitous Engineering Vol. 6, No. 2, April, 2011

[10] C.C. Communication Consortium. Car 2 car communication consortium manifesto.〈 http://car-to-car.org/index.php?id=31〉

[11] Olariu S, Weigle MC.:Vehicular networks: from theory to practice. 1st ed. Chapman&Hall/CRC;(2009)

[12] DSRC 5GHz: Dedicated Short Range Communication at 5.9 GHz Standards Group (Standard* Activities Group) http://www.iteris.com/itsarch/html/standard/dsrc5ghz.htm

[13] M. Milton Joe, R.S. Shaji, K. Ashok Kumar, "Establishing Inter Vehicle Wireless Communication in Vanet a nd Preventing It from Hackers", I.J.Computer Network and Information Security, 2013,8,55-61

[14] Chapter 9. Vehicle to Infrastructure interaction (V2I) http://www.mogi.bme.hu/TAMOP/jarmurendszerek_iran yitasa_angol/math-ch09.html

[15] International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 2019 ISSN 2229-5518 An Efficient Routing Protocol for Minimizing Multi- hop in VANET using WiMAX Vaishak.P, T.Sivakumar

[16] C.M.Ramya, M. Shanmugaraj, R. Prabakaran, "Study on ZigBee technology" , 2011 3rd International Conference on Electronics Computer Technology (ICECT) , Vol.6, pp.297,301, 2011

[17] Bhargav, K.R.K.; Singhal, R., "Zigbee based VANETs for accident rescue missions in 3G WCDMA networks," Global Humanitarian Technology Conference: South Asia Satellite (GHTC-SAS), 2013 IEEE , pp.310-313, 2013

[18] K.Selvarajah, A.Tully, P.T.Blythe, "ZigBee for Intelligent Transport System applications," Road Transport Information and Control - RTIC 2008 and ITS United Kingdom Members' Conference, IET, pp.1-7, 2008

[19] JM Kahn, JR.Barry, "Wireless Infrared Communications," Proceedings of the IEEE, Vol.85, Issue.2, pp. 265 – 298, 1997.

[20] VICS- Vehicle Information and Communication System. www.vics.or.jp/english/vics

[21] M. G. diBenedetto, T. Kaiser,A. F. Molisch, I. Oppermann, C. Politano, and D. Porcino, Eds., UWB Communications Systems: A Comprehensive Overview. Darmstadt, Germany: EURASIP, 2005.

[22] Jin-Shyan Lee; Yu-Wei Su; Chung-Chou Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE , pp.46,51, 5-8 Nov. 2007

[23] D. Wang, K. O'Keefe, M.G. Petovello," Decentralized Cooperative Positioning for Vehicle-to-Vehicle (V2V) Application Using GPS Integrated with UWB Range", Proceedings of the ION 2013 Pacific PNT Meeting,pp. 793 – 803,2013

[24] Asmaa El Gueraa, Anouar Darif,Rachid Saadane,and Driss Aboutajdine"An efficient Transceiver for Vehicular Ad hoc Network Based on IR-UWB"

[25] R. Frank, W. Bronzi, G. Castignani and T. Engel, "Bluetooth Low Energy: An Alternative Technology for VANET Application," Proc. Of 11th IEEE/IFIP Annual Conference on Wireless On-demand Network Systems and Services, 2014

[26] H.Mamdouhi, S.Khatun, J. Zarrin," Bluetooth Wireless Monitoring, Managing and Control for Inter Vehicle in Vehicular Ad-Hoc Networks", Journal of Computer Science, Vol.5, Issue.12, pp.922-929, 2009.

[27] Dedicated Short-Range Communications (DSRC) communication architecture. http://www.wirelesscommunication.nl/reference/chaptr0 1/dtmmsyst/dsrc/dssr4.htm

[28] Emergency 9-1-1 Fleet Tracking. http://www.cypress.bc.ca/case_studies_emergency_fleet _monitoring.html

[29] Y. L. Morgan. IEEE Communications Surveys & Tutorials, vol. 12, no. 4, Fourth Quarter 2010 notes on DSRC & WAVE standards suite: its architecture, design, and characteristics

[30] International Journal of Scientific & Engineering Research Volume 3, Issue 12, December-2012 1 ISSN 2229-5518

[31] An Evaluation study of WiMAX and WiFi on Vehicular Ad-Hoc Networks (VANETs) Muhammad Rizwan Arshad, Shahid Mehmood, Salman Afsar, Muhammad Azam Zia,Umar Farooq\