ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

# A Survey of Vehicular Communication

Vijay Kumar Tripathi[1], Fouziah M Hamza[2], Dr. Venkateswari .S[3]
Research Scholar[1, 2], HOD[3]
Department of Computer Science
Noorul Islam University, Kanyakumari Tamilnadu, India

**Abstract:**
VANET ( VehicularAdHoc Network) used in vehicular communication which is trending area of research in the field of Automobile technology. Many companies ( Google, Uber, Ford, Mercedes Benzes, Toyota , General Motors etc.) are advancing their cars with such technology. Google launched its self-driving car project in 2009 under the leadership of Sebastian Thrun, a Stanford University professor who is lauded as the founder of the autonomous car. While at Google, Thrun led several projects at Google's X research lab, including Google Glass and Street View. Thrun first began his research on driverless vehicles at Stanford, leading a student and faculty team that designed the Stanley robot car. The car won a $2 million prize at the 2005 DARPA Grand Challenge for driving 132 miles in the desert on its own Google began its project with six Toyota Priuses and an Audi TT that drove through the streets of Mountain View, California. It hired a handful of people with perfect driving records to sit behind the wheel, a position it still hires for seven years later Google's cars use GPS, sensors, cameras, radar, and lasers to "see" the world around them. The sensors on the car can detect objects up to two football fields away, including people, vehicles, construction zones, birds, cyclists, and more. Google self-driving car project, is an autonomous car developer and an independent company under Alphabet IncIn 2015 the project completed its first driverless ride on public roads, giving a ride to a sole blind man in Austin, Texas in December 2016, Google transitioned the project into a new company called Waymo, housed under Google’s parent company Alphabet. Alphabet describes Waymo as “a self-driving tech company with a mission to make it safe and easy for people and things to move around.” The new company, which will be headed by long-time automotive executive John Krafcik, plans to make self-driving cars available to the public in 2020. The development of software and hardware in communication systems leads to the generation of new networks. Many researches and projects have been conducted in this area. Lots of government projects have been implemented in the USA, Japan and the European Union. New architectures, protocols and implementations of vehicular ad-hoc network (VANET) have been made in recent years to provide Intelligent Transportation Services. In this study, we survey the current issues like development, deployment, security challenges and about the current projects running in different countries. We also survey the mobility models and simulators required to implement VANET. We have also reviewed the emerging applications of VANET which provides services to the end users. At last, we have presented future research problems in VANET. The main motive of this survey is to explore the current ideas in vehicular communication and their Challenges.

**Keywords:** VANET, V2V, V2I, DSRC, RSU

## 1. INTRODUCTION

Vehicular communication is defined as communication between the vehicles. The main objective of VANET is to reduce the level of accidents. It has a great effect on passenger’s safety and for drivers to drive smoothly in the urban area. As vehicles population increases day by day the rate of accidents also increases, therefore it is necessary for the vehicles to communicate. For example, suppose a vehicle A is moving in front of vehicle B and suddenly A meets with an accident by a thunderstorm and it applies its brakes, it does not want B to face the problem, then automatically, the brake sensors and rain sensors of A obtain activated and pass the signal to the main unit and then it broadcasts a message (Alert Message) to other vehicles. After obtaining the alert message, B slows down. By this example, we simply know the use of inter-vehicular communication and why it is needed. According to the World Health Organization (WHO) the Road-Traffic Injuries statistics of all countries show that after 2000, road accident is a major cause of death [1]. Hence, there must be a better traffic system to solve this problem. VANET is such an advanced network which mainly provides Intelligent Transportation System (ITS) services to the end users for providing fast data exchanges and safety. It uses different standards like DSRC and WAVE for fast data communication. Many routing protocols have been designed for implementation of routing in VANET. MANET routing protocols are used to implement VANET but it is difficult to implement VANET using these routing protocols (topology based) because of its high mobility. Nowadays, researchers are focusing on designing secure VANET systems to prevent them from different malicious drivers who disrupt the network performance VANET is affected by many active and passive attacks. For that, many secure routing protocols are developed to save the systems from these attacks. Many projects are implemented in the USA, Japan and the European Union to provide safety and security to the passengers as well as drivers. These projects provide many applications to the end users like safety alarm system, media downloading, safe communication, broadcasting advertisements, marketing and so on. To evaluate the performance of the VANET it is implemented using different network and traffic simulators. The main motivation behind this survey paper is that accidents and road fatalities are increasing day by day, people are facing problems and need safety. VANET systems are also not deployed all over the world and it is a big issue for the transportation organization and WHO. Hence, all people should be aware about these conditions and it is also becoming an emerging research area for the researchers to communicate between the vehicles and provide safety to the passengers. VANET provide many services to the end users like multimedia sharing, content delivery, security, e-health facilities **[2]** and so on. Recently, many developments and researches have been conducted under VANET and researchers are working on issues like routing, broadcasting, security, traffic management **[3, 4]** , information fusion **[4]** and so on. The organisation of the survey paper is presented as follows: Section 2 presents an overview of VANET. Section 3 presents the standards used for vehicular communication. Section 4 presents briefly about the routing techniques used in VANET for communication. Section 5 presents the security challenges and secure routing algorithms used in VANET. Section 6 presents the current projects deployed in some parts of the world. Section 7 presents the mobility model and simulation tools used for implementing VANET. Section 8presents the new emerging applications of VANET. Section 9 presents the future research problems in VANET. Finally, we conclude in Section 10.

## 2. VANET OVERVIEW

**2.1*VANET ARCHITECTURE***-VANET architecture mainly consists of vehicles (V), Road Side Unit (RSU) and Infrastructure Domain (I). Communication is conducted mainly by using wireless standards (e.g. IEEE 802.11p). RSU acts like a router and has high range (coverage) than vehicles range. Vehicles are installed with an On Board Unit (OBU) for communication. It is also installed with a Global Positioning System (GPS) for knowing its own position as well as for tracking other vehicles. Electronic license plate (ELP) is also set in the vehicle for identification. Radio detection and ranging (RADAR)/light amplification by simulated amplification of radiation (LASER) technologies are also used for knowing the position of other vehicles

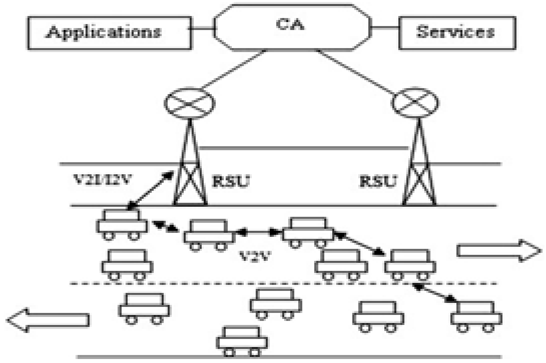

**Figure.1. VANET Architecture**

It is also supplied with high battery power. A Certification Authority (CA) exists **Fig1. VANET Architecture** (e.g. security and TCP/ IP) and applications. Fig. 1 shows the architecture of VANET

***2.2 INTELLIGENT TRANSPORT SYSTEM.*** Intelligent Transportation System [3] means that the vehicle itself acts as a sender, receiver and router for broadcasting information. As discussed earlier, the VANET consists of RSUs and the vehicles are installed with OBU, GPS, ELP and so on. ITS provides two types of communication in VANET: first is vehicle to vehicle (V2 V) and second is vehicle to infrastructure/infrastructure to vehicle (V2I/I2 V). Fig. 1 shows V2 V communication and V2I/I2 V communication. V2 V communication uses multi-hop communication (multicasting/broadcasting) for transmission of data. Inter-vehicle communication consists of two types of communication: first is naive broadcasting which produces beacons at regular intervals. The main demerit of using naive broadcasting is the collision of messages because of much more generation of messages. Second is Intelligent Broadcasting which generates messages on demand. The collision reduces in this method of data transmission. V2I communication uses single-hop communication (RSUbroadcasts message to the vehicles in Range). It has a high bandwidth link between the vehicles and the RSUs. The RSU determines the vehicles speed and if the vehicles speed is more than the limit then the RSU broadcasts a message in the form of a visual warning or alarm

## 3. VANET STANDARDS

Standards are used for development of the product and to assist users to verify and compare the products. Many standards are used according to the protocols used for example, security, routing, services and so on. There are many standards used in VANET such as dedicated short range communication (DSRC) and wireless access in vehicular environment (WAVE). Fig. 2 is adapted from [3] which shows the architecture of the WAVE, IEEE 802.11 p, IEEE 1609 and OSI models

### 3.1DSRC(Dedicated Short Range Communication)

DSRC **[3, 5]** is a standard developed by the USA. It is a short to medium range communication service used for both V2 V and V2I communication. The US Federal Communication Commission sets 75 MHz of spectrum at 5.9 MHz for the DSRC. The DSRC spectrum has seven channels. Each channel is 100 MHz wide. In 2003, the American Society for Testing and Materials (ASTM) prepared the ASTM-DSRC which was totally based on the 802.11 MAC layer and IEEE 802.11a physical layer **[6]**. Table 1 shows the DSRC standards used in the USA, Japan and Europe **[3, 7]**.

### 3.2 Wireless Communication in Vehicular Environment

The main problem with the IEEE 802.11a with a Data Rate of 54 Mbps is that it suffers from multiple overheads [8, 9]. Vehicular scenarios demand high speed data transfer and fast communication because of their high topological change and high mobility. For this, the DSRC is renamed to IEEE 802.11p WAVE by the ASTM 2313 working group. This works on the MAC layer and physical layers. Deng et al. [10] also proposed a collision alleviation scheme to reduce delays in the system. WAVE consists of a RSU and an OBU. WAVE uses the OFDM technique to split the signals. The WAVE stack presented in Fig. 2 consists of many standards and individually these standards perform their functions. *The IEEE 802.11a works on physical layer management, the IEEE 1609.1 works on the application field [11], the IEEE 1609.2 provides a security mechanisms, the IEEE 1609.3 works on WAVE management and the IEEE 1609.4 manages the logical link control layer*. However, according to [12], WAVE violates the TCP/IP layer design, hence, Li and Chao proposed a two layer design to access IPv6 in a quick manner. Table 2 shows the IEEE 1609/802 standards.

## 4. ROUTING

Routing is a vast concept used in the MANET and VANET environment. Many routing protocols have been designed for communication between the nodes in an ad hoc environment. In VANET, routing is a difficult task to achieve because of its high mobility. The main issues in VANET which require routing are network management, traffic management, broadcasting, mobility, topological change, quality of service, fast data transfer and so on. These are the challenging elements which require efficient routing techniques. The routing protocols [14] are divided into topology based, position based, cluster based, Geo Cast based and broadcast based. In this section, we survey briefly different routing protocols used in VANET implementations. Fig. 3 shows the taxonomy of the routing protocols in VANET. For More routing protocols we should refer to [15].

**4.1 Topology Based Routing-**Topology-based routing protocol [14, 15] is divided into proactive and reactive routing protocols. In proactive routing protocols, no route discovery takes place routes are predefined. Maintenance of unused routes leads to a high network load and high bandwidth consumption which degrades network performance. Destination Sequenced Distance-Vector Routing, OLSR: Optimized Link State Routing Protocol, Fisheye state routing, Cluster Head Gateway Switch Routing, The Wireless Routing Protocol, Topology Dissemination Based on Reverse-Path Forwarding and so on are some of the proactive routing protocols.

**Table.1. DSRC Standard Used in USA & Europe**

| Features | USA ASTM | Japan<br>(association of radio industries and business) | Europe<br>(European committee for standardization) |
|---|---|---|---|
| communication | half-duplex | half-duplex (OBU)/<br>full duplex (RSU) | half-duplex |
| radio frequency | 5.9 GHz | 5.8 GHz | 5.8 GHz |
| band | 75 MHz | 80 MHz | 20 MHz |
| channels | 7 | downlink: 7 uplink: 7 | 4 |
| channel separation | 10 MHz | 5 MHz | 5 MHz |
| data transmission rate | 3–27 MBps<br>downlink/ uplink | 1/4 MBps<br>downlink/ uplink | downlink: 500 KBps<br>uplink: 250 KBps |
| coverage | 1000 m | 30 m | 15 –20 m |

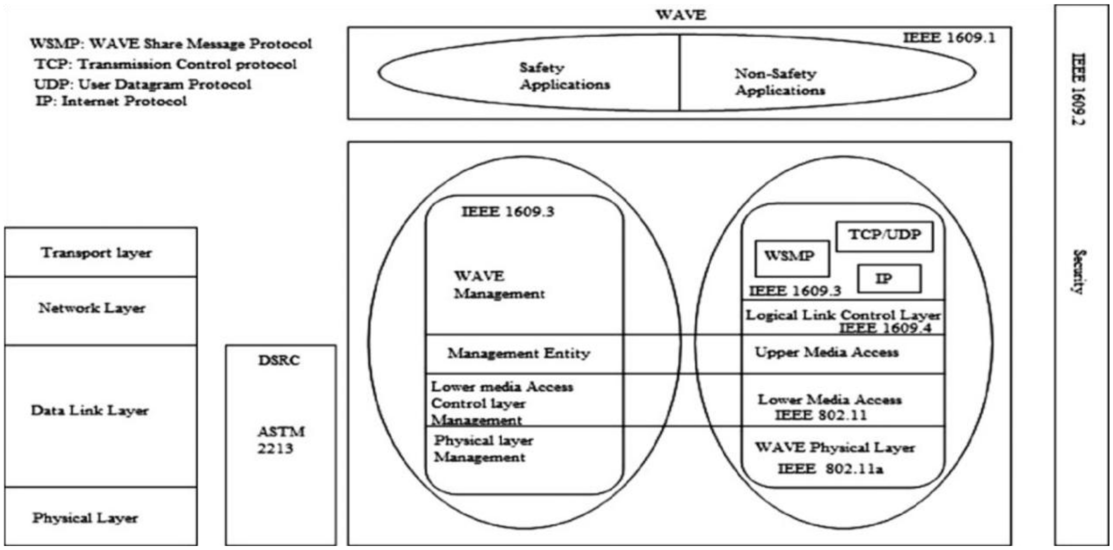

**FIGURE. 2. WAVE, IEEE 802.11P, IEEE 1609 AND OSI MODELS**

As the proactive routing protocol suffers from network load and high bandwidth consumption, reactive routing protocols are designed in which the route discovery takes place on demand. Hence, the network load reduces as only the route currently in use is maintained with a low packet overhead. Reactive routing protocol DSR: Dynamic Source Routing, **AODV**: Ad Hoc on Demand Distance Vector, Temporally Ordered Routing Algorithm, Junction-based Adaptive Reactive Routing, Preferred Group Broadcasting and so on are some of the reactive routing protocols. Hybrid routing protocols are then designed which gain both the properties of reactive and proactive routing protocol. It discovers the routes between the zones to reduce network load. Proactive protocols are used in intra-zone routing and reactive protocols are used in inter-zone routing. Zone routing protocol, Hybrid Ad Hoc Routing Protocol and so on are some of the zone routing protocols

**4.2 Position/Geography Based Routing-**Position-based routing [14, 15] uses geographical location information for the selection of next hop to forward the message. It uses beaconing to broadcast the messages. In this routing scheme, no routes and routing table are maintained. In this scheme, geographical location is used as information to route the packets to the nodes. This uses street maps, GPS service, OBU and so on for data transmission. As the mobility is more, the topology changes frequently and if topology-based routing is used, it may degrade the performance with high network load. Greedy Perimeter Stateless Routing, Distance Routing Effect Algorithm for Mobility, Connectivity Aware Routing Protocols, Geographic Source Routing, Anchor-Based Street and Traffic Aware, Greedy Traffic Aware Routing and so on are some of the position-based routing protocols.

**Table .2. IEEE 1609/802 e Standards [3,5,13]**

| IEEE standard | Features and services |
|---|---|
| 1609 [3, 5, 13] | describes architecture, communication model, management, security, WAVE interface, physical address for communication and so on |
| 1609.1-2006 [3, 5, 13] | describes applications, architecture, command and message formats |
| 1609.2-2006 [3, 5, 13] | provide security services |
| 1609.3-2007 [3, 5, 13] | addressing and routing services and describes WAVE short message protocol ( WSMP ) |
| 1609.4-2006 [3, 5, 13] | describes improvements to WAVE |
| 802.16e [3, 5, 13] | enables multi-vendor broadband access products |

**4.3- Cluster Based Routing**-Cluster-based routing scheme [14, 15] is designed because it has high scalability and it is better for larger networks. A group of nodes are identified as a cluster and in each cluster a cluster head exists which sends the message to other nodes. The main problem with cluster-based networks is that it increases the delay in formation of clusters. Cluster Based Routing, Cluster Based Location Routing, Clustering for Open IVC Network, Hierarchical Cluster-Based Routing and so on are some of the cluster-based routing protocols.

**4.4- Geo-cast Based Routing**- In this routing, message is delivered to a region by multicasting service [14, 15]. It uses flooding within an area or zone for message transmission. It can also use non-flooding techniques for data transmission. It reduces collisions as packet overhead is reduced. Inter-Vehicle Geo Cast, Direction-based Geo Cast Routing Protocol for query dissemination in VANET, Distributed Robust Geo Cast, Robust Vehicular Routing, Dynamic Time-Stable Geo Cast Routing and so on are some of the Geo Cast routing protocols

**4.5 Broadcast Based Routing**-This is a frequent routing technique in which the messages are broadcasted among the vehicles and between V2I/I2 V [14, 15]. However, when the network is large it creates many problems such as high bandwidth consumption, high collision and high packet overhead which reduces network performance. Hence, to recover from this, selective forwarding strategy is used. BROADCOMM, Urban Multi-hop Broadcast Protocol, Vector-Based Tracing Detection, Distributed vehicular broadcast protocol and so on are some of the broadcast-based routing protocols

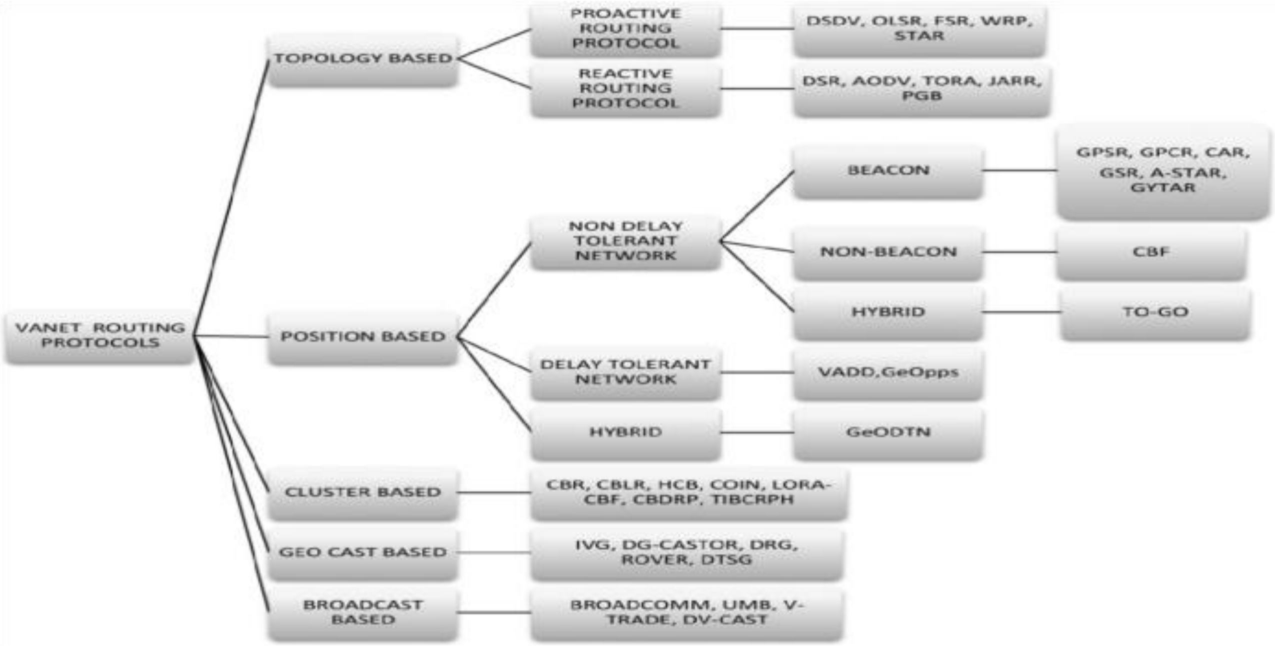
PROACTIVE ROUTING PROTOCOL
DSDV, OLSR, FSR, WRP, STAR
TOPOLOGY BASED
REACTIVE ROUTING PROTOCOL
DSR, AODV, TORA, JARR, PGB
BEACON
GPSR, GPCR, CAR, GSR, A-STAR, GYTAR
NON DELAY TOLERANT NETWORK
NON-BEACON
CBF
HYBRID
TO-GO
VANET ROUTING PROTOCOLS
POSITION BASED
DELAY TOLERANT NETWORK
VADD,GeOpps
HYBRID
GeODTN
CLUSTER BASED
CBR, CBLR, HCB, COIN, LORA-CBF, CBDRP, TIBCRPH
GEO CAST BASED
IVG, DG-CASTOR, DRG, ROVER, DTSG
BROADCAST BASED
BROADCOMM, UMB, V-TRADE, DV-CAST

**Figure. 3. Taxonomy of different VANET routing protocols [15]**

## 5. VANET SECURITY

Security in VANET [16–18] is a challenging problem for researchers in the era of cyber threats. The message passing from one vehicle to another vehicle may be trapped or hacked by an intruder or imposter who creates vulnerability in the systems performance. In VANET, many types of attack occur on the system like Position Cheating [19, 20], GPS Information Hacking, ID Cheating, Message Modification, and Spoofing and so on. Malicious drivers can create problems in the traffic which leads to accident and traffic jam. Hence, the vehicles should use security mechanisms to resist these threats. In this section, we present the threats to the VANET system and the security mechanisms to check the attacks.

### 5.1 Threat to Security

There are three types of security goals: first is Confidentiality, second is Integrity and third is Availability. However, these goals are strongly affected by malicious drivers. The attacks [3, 16–18] performed by malicious drivers are discussed as follows Snooping: In this attack, an attacker accesses the information without any authorization. When a vehicle in the network sends information to another vehicle then the attacker intercepts and accesses the contents of the information and uses it for its own work. Snooping is a passive attack in which the attacker only monitors or accesses the information without modifying the data. † Traffic analysis: In this attack, an attacker analyses the traffic (collection of information/ transactions). The attacker collects all the information by monitoring the vehicular network constantly. By collecting the information like email addresses, requests and responses of all the vehicles communicating, the attacker can attack by a guessing strategy. It is also a passive attack in which no data modification is performed by the attacker. † Data modification: In this attack, an attacker intercepts and modifies the data. When a vehicle in the network sends an important information say warning message (Thunderstorm Ahead) to another vehicle, then the attacker may modify the data, delete the data or delay the data. By doing this, the second vehicle suffers from thunderstorm problem and accident occurs. This is a very dangerous attack in which the attacker for its own benefit weakens the system. It is an active attack in which the data is modified.

† **Replay attack:** In this attack, an attacker intercepts and saves a copy of the message and later uses it for replaying. In the VANET systems, when a vehicle sends a warning message to another vehicle, the attacker keeps a copy of the message and later uses it to create delay in the system by unnecessarily stopping a vehicle by warning. It is also an active attack.

† **Masquerading:** In this attack, an attacker impersonates some other vehicle by providing false ID and advertises as a legal node. When two vehicles communicate in the system then the attacker acts as a man in the middle and spoofs as a second vehicle and gains information from the first vehicle. This is also an active attack where the data can be modified.

† **Repudiation:** In this attack, an attacker denies that he/she sends a message. In the VANET systems, a sender vehicle or a receiver vehicle can create this attack by denying that it sends a message or it receives a message, respectively. For example, if a vehicle A sends information to vehicle B and B refuses to receive the information, then the message is trapped and A may again send the information to B and it may increase the delay.

† **Sybil attack:** In this attack, an attacker generates multiple identities and cheats with false identities. A malicious vehicle in the network acts as multiple vehicle nodes and joins the network and after joining the network it behaves maliciously. This attack is an active attack which degrades the systems performance.

† **Tunneling:** In the tunneling attack, an attacker injects false data into the network which disrupts the network's consistency. In the VANET systems, when a vehicle in the network is going to receive the location information it suddenly injects faulty location information which creates a problem for the receiver vehicle.

† **Spamming:** In this attack, an attacker increases the flooding effect in the network by which traffic congestion occurs and it increases the latency in the system. It reduces the efficiency of the request/response scheme by creating a delay in the network.

† **GPS spoofing:** In the GPS spoofing attack, an attacker transmits robust signals which are powerful than the GPS signals. By performing this action, the attacker jams the network and the receiver obtains false position signals of itself. This creates a problem in obtaining a correct position and the receiver deviates from the right position and broadcasts its false position to other vehicles. Jamming: In this attack, an attacker jams the network by transmitting signals to interfere by which the network performance degrades [17]. The attacker captures an area by creating disturbances in that zone and divides the network.

### 5.2 Secure Routing Protocol in VANET

Many secure routing protocols have been designed and implemented in the real life scenario which uses the concepts of Authentication, Digital Signature, Public Key Infrastructure (PKI) and so on to secure the system from different active and passive attacks. The secure routing protocols are briefly described as follows.

**ARAN:** ARAN [21] stands for Authenticated Routing for Ad Hoc Networks and it is the same as the AODV protocol but with authentication scheme at the time of route discovery. It mainly provides message authentication and message integrity. In this scheme, there is a server which is fully trusted and it provides certificates to the nodes. In this scheme, every node validates the previous nodes signature. ARAN provides better performance than AODV in terms of security and discovery of routes. The main problem with this scheme is that it has a high packet overhead and high CPU processing.

† **ARIADNE:** ARIADNE [22] is another protocol which is an extension of DSR with the concepts of symmetric key cryptography. It uses the TESLA [3, 22] security scheme for routing which adds a HMAC key for authentication of nodes. ARIADNE protects DSR from malicious attacks like replay attack and looping condition. It increases the end-to-end delay as

security mechanism is included. It has a low packet overhead and average CPU processing.

† **CONFIDANT:** CONFIDANT [23] protocol stands for Cooperation of Nodes: Fairness in Dynamic Ad Hoc Networks and it is designed to support DSR. The main aim of CONFIDANT is to recognise malicious nodes in the network by excluding them from taking part in the route discovery phase. The main building blocks of this protocol are monitor, trust manager, reputation system and path manager. These four elements provide security to the system. It has low CPU processing with average packet overhead.

† **SAODV:** SAODV [24] is a secure AODV routing protocol used for providing authentication, integrity and non-repudiation. It uses a digital signature for authentication and hash chains for hop count information. It uses asymmetric key cryptography which increases the delay in the network but it provides a robust security. It has average packet overhead and high CPU processing.

† **SEAD:** SEAD [25] stands for Secure Efficient Ad Hoc Distance Vector Routing. It is used for removal of faulty routing state information in other nodes. It is based on the DSDV routing protocol and uses hash chains for providing authentication. The basic security mechanisms used in SEAD are hash chains and sequence numbers. It has a high packet overhead which creates congestion in the network. It uses less resources as it does not use asymmetric key cryptography.

† **SLSP:** SLSP [26] stands for Secure Link State Routing Protocol. It is a proactive routing protocol which protects the link state information and topology discovery of the network. It is used in the Zone Routing Protocol. The basic security mechanism used in the SLSP is certificate authority. It stops the attackers by controlling masquerading and flooding. It isbetter for larger networks because it has high scalability. It has an average packet overhead and high CPU processing.

† **SPAAR:** SPAAR [27] stands for Secure Position Aided Ad Hoc Routing, which uses position information for routing. It uses asymmetric key cryptography for message confidentiality and integrity. In this protocol, a certificate authority provides certificates to the nodes. The main objective of the SPAAR routing protocol is to detect and recogniSe malicious nodes. It has average packet overhead and high CPU processing.

† **SLOSR:** SLOSR [28] is an improved secure OLSR protocol used for providing authentication to the packets and prevents the network from replay attacks. It uses HMAC codes and time exchanges schemes in the nodes to protect the nodes from different attacks. It is better for smaller networks. It uses symmetric key cryptography which reduces computation. It has average packet overhead with less congestion.

### 5.3 Challenges in VANET Security

The main challenges while implementing security systems in VANET are discussed as follows:

Authentication: There should be an authentication of all the messages transmitted from one vehicle to another. Each vehicle in the network is to be authenticated by the central authority.

† High mobility: As the vehicle moves faster, there is a link disruption problem and handshaking is lost. By this, the vehicles are unable to interact and establish secure communication between them.

† Location-based services: By beaconing, we know the location of other vehicles. However, by implementing GPS, sensors, LASER, RADAR and so on we know the correct position of the vehicles.

† Real-time system: To develop a real-time system is a challenging task because in a high mobile area it is difficult to send a warning message in correct time before the deadline.

### 5.4 Features Supporting VANET Security

The features which support security in VANET are

† Government laws: If an attacker in the VANET network is caught by the officials then he/she should be punished under the rules and regulations of the government laws.

† Central authority: It controls the system by authenticating the message transmission, tracking vehicles location, providing internet services and safety related applications.

† High power status: Every vehicle in the network is supported with a high battery power. This means that the vehicle can perform many calculations and computations. † Electronic license plate: Each vehicle in the network is registered with an vehicle ID and every vehicle has a unique ELP.

† Time and position awareness: Every vehicle in the network knows the correct position of the other vehicle in the network by using beaconing. By beaconing, time and location information are broadcasted to other vehicles.

### 5.5 Future Research Scope

The future research scope of VANET Security is discussed as follows: Powerful secure routing protocol: Design of a robust secure routing protocol prevents the system from malicious attacks. It helps in secure transmission of information from the source to the destination. By the use of symmetric and asymmetric key cryptography techniques these protocols are implemented. Cost-effective systems: Design of a cost effective system is necessary nowadays for the development of VANET technology. By using less resources we can create a better cost effective system. Robust security architecture: Design of a powerful security architecture is a challenge in VANET as malicious drivers are entering the system repeatedly. By using security mechanisms like Central Authority, symmetric key cryptography, asymmetric key cryptography, PKI, authentication, digital signatures and so on a robust architecture is implemented.

## 6. VANET PROJECTS

VANET implementation in a real time system is a challenging task. Many such implementations have been deployed inrecent years and implementing such projects in a real time system requires complete simulation by measuring the performance of the system. Many new projects have been conducted by the government to develop ITS. The USA, Japan and the European nations are using the ITS systems by implementing VANET in the urban areas [29]. Early developments mainly focus on the protocol infrastructure (WAVE, IEEE 802.11p and DSRC). However, now it is acquiring the new concepts of messaging system and application architecture. Many car producing companies like BMW, Audi, Ford, General Motors, Daimler, Nissan and so on are using the ITS systems for passenger safety.

VSC (Vehicle Safety Communication) is a project in the USA, C2C-CC (Car-to-Car Communication Consortium) project in European nations and ASV (Advance Safety Vehicle Program) project and VII (Vehicle Infrastructure and Integration) in Japan are some of the government projects under these schemes. Fig. 4 shows the projects in the USA, European Union and Japan. Many such VANET projects are surveyed and referred from [29] and presented as follows.

### 6.1 VANET Projects in EUROPE

The C2C-CC project started in 2001 which uses the IEEE 802.11 WLAN in 100 m. This project is mainly designed for V2 V communication. The Fleetnet (2000–2003) [30, 31] project uses GPS information for V2 V and V2I communication. It is mainly deployed in urban areas and simulated by the Fleetnet Demonstrator. NoW (2004–2008) is a project mainly deployed in Germany and it is funded by Daimler, BMW and Volkswagen. This is mainly developed for providing security. It supports C2C-CCin communication. PreVent (2004–2008) project uses sensors, maps and communication systems. Its trial has 23 cars, trucks and different devices [3]. Its main applications are safety and collision control. CVIS (2006–2010) is a project mainly developed for providing V2 V communication. Its main applications are traffic control systems and network monitoring. CarTalk (2000–2003) [3] is a project used for Advance Driver Assistance (ADAS), Advance Cruise Control and Collision Avoidance Systems. The CARLINK project is used for generating intelligent wireless communication between vehicles. Its main applications are weather forecasting, city traffic management and information broadcasting. DIRICOM is a Spanish project financed by the Spanish Regional Ministry. SEISCINTOS is a project which mainly concentrates on providing intelligent communication in MANET, VANET and WSN. This project mainly aimed at providing ubiquitous services to the users. WiSafeCar stands for Wireless Traffic safety network between cars. It is a project mainly designed for traffic management and road safety. MARTA stands for Mobility and Automation through advanced Transport Networks. It is a Spanish project for providing safety and efficiency in ITS. ComeSafety provides safety in V2 V and V2I communication by supporting safety forum. Coopers stands for CO-Operative Systems for Intelligent Road Safety. This project provides traffic safety between vehicles and infrastructure by designing telematics applications. ESafetySupport is a project which aims to provide safety systems and supports the European Commission’s 2001 goal of reducing road fatalities by 2010. EVITA stands for E-Safety Vehicle Infrastructure Protected Applications. It provides secure communication. GST stands for Global System for Telematics. Its main aim is to deploy telematics services to the end users. GeoNet stands for Geographic Addressing and Routing for Vehicular Communications. The GeoNet project extends the work of C2C-CC by enhancing its specification and interfacing with IPv6. iTETRIS stands for An Integrated Wireless and Traffic platform for Real-Time Road Traffic Management Solutions. It works on emissions, travel time, traffic management and so on.

The Pre-DRIVE C2X project mainly focuses on driver assistance systems and safety communication. SAFESPOT is a project which mainly focuses on safety communication between the vehicles. SEVECOM stands for Secure Vehicles Communication. It is a European Union project which provides security to the system. SIM-TD stands for Safe Intelligent Mobility-Test Area Germany and it provides communication between V2 V and V2I for traffic safety

### 6.2 VANET Projects in the USA

WAVE (2004) [32] stands for Wireless Access in Vehicular Environments. It extends many projects in the USA such as IVI, VSC, VII and so on. IVI (1998–2004) [33] stands for Intelligent Vehicle Initiative which provides road safety. VSC (2006–2009) stands for Vehicular Safety Communication for providing safety. It works by coordination with Highway Traffic Safety Administration. VSC-2 includes protocols, messaging, systems and interface. VII (2004–2009) [3] stands for Vehicle Infrastructure Integration which started in Detroit. It integrates with Ford, General Motors, BMW, Honda, Toyota, Volkswagen, Daimler-Chrysler and Nissan for providing better communication.

### 6.3 VANET Projects in the JAPAN

ASV (1996–2000) [3] stands for Advanced Safety Vehicle. It was extended to ASV-3 in 2001 and ASV-4 in 2005 by providing automatic collision avoidance system and navigation system. It is supported by Honda, Mitsubishi, Suzuki and Toyota. DEMO [34] started in 2000 for providing a cooperative driver support system. It uses a band of 5.8 GHz and CSMA protocols for communication. JARI [3] stands for Japan Automobile Research Institute which conducts many trials for projects and it evaluated the USA projects and European Union Projects. It mainly focuses on security and safety.

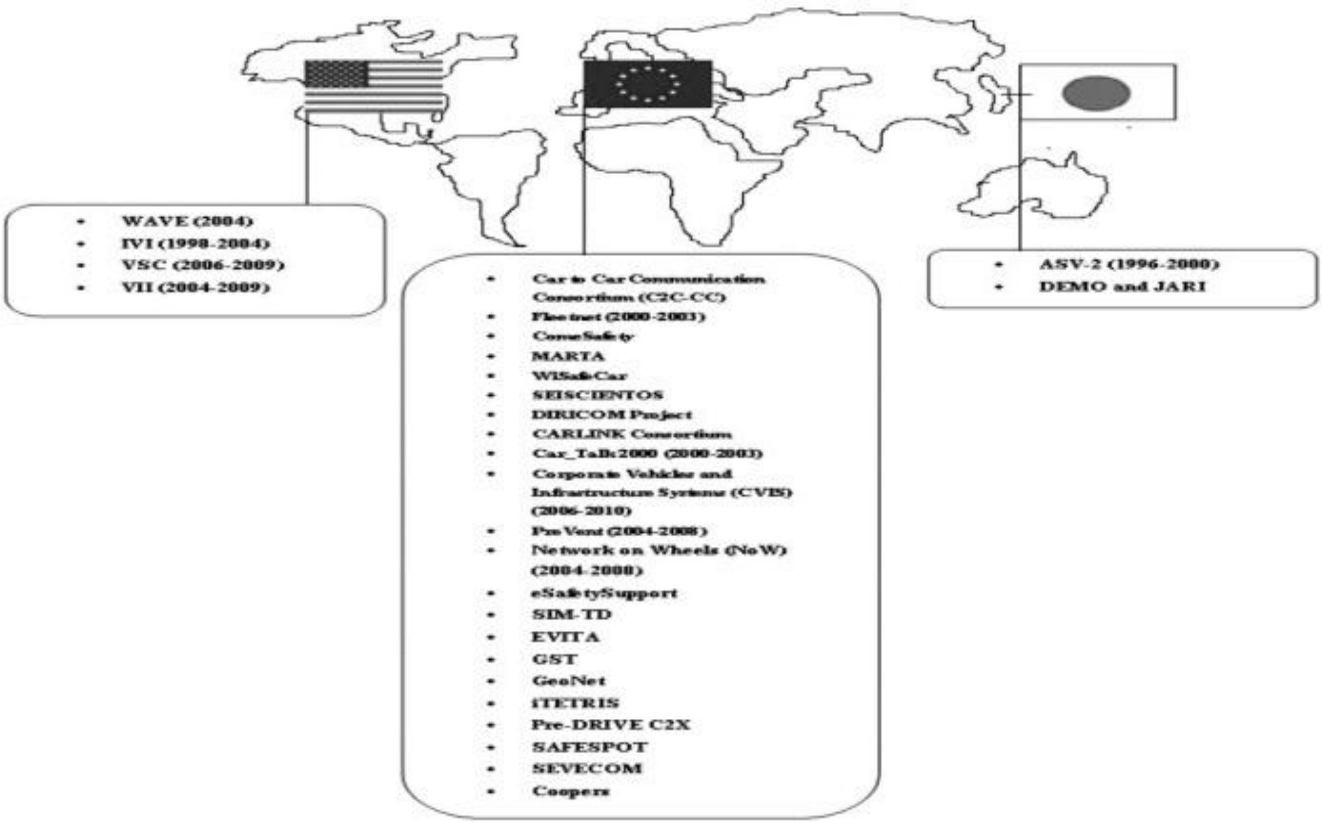

**Figure .4 .Projects in USA, Europe and Japan**

## 7. VANET Simulation

The mobility model [35] is a model or a set of rules for designing random network topologies by using simulators. It establishes connections between the nodes and performs some processes and activities between them. Role-based mobility model [36] is a mobility model which separates the nodes according to their roles. It provides different strategies according to micro and macromobility. The main limitation of this model ineffectiveness is that it creates difficulty in simulating complex traffic scenarios for example, it creates difficulty while simulating bridges, tunnels and so on. Liu et al. [37] designed a tool called VGSim which is an integrated and microscopic level simulation platform to model the road traffic accurately. VANET simulation required a complete, accurate and realistic mobility model which is gained by collecting patterns from mobility traces. We survey some models which generates traces which are used by the mobility model and shown in Tables 3–5. Fig. 5 presents the generation of a realistic mobility model. Tables 3 –5 are adapted from [35].

### 7.1 VANET Simulators

VANET is implemented using robust and effective simulators. The main element in VANET simulation is the generation of a realistic and robust mobility model. The main building blocks in designing a mobility model are: visualization tool, output, platform and a class which connects the mobility model and the network simulator [35]. In this section, we present different types of Traffic Simulators, Network Simulators, Isolated Vehicular Models, Embedded Vehicular Models and Advanced Vehicular mobility models. Tables 3–5 present some VANET simulators and their features

**7.1.1 Traffic simulators:** Traffic simulators [35] are mainly designed to simulate the urban intersections and highways. This is an important tool for traffic engineering. TRANSIM [40] or VISSIM [41], CORSIM [42], PARAMICS [43], CARISMA [44], SHIFT [45] and so on are some of the traffic simulators for simulation of the microscopic and macroscopic levels. These simulators are validated and used for providing accurate mobility models. The main disadvantages of traffic simulators are that they take more time in planning and transportation which increases the time complexity. To use these simulators end users requires a license. Many open source traffic simulators are available nowadays to handle large traffic like SUMO (Simulation of Urban Mobility) [46]. SUMO generates traces which are used by the network simulators. For traffic generation it takes the route assignments and for motion constraints it contains parsers for TIGER [47]. MOVE (Mobility Model Generator for Vehicular Networks) [48] tool is used to simplify the SUMO configuration and adds a GUI environment to it

**7.1.2 Network simulators**: Network simulators [35] play an important role in managing and controlling the network parts. These are available in the market as commercial as well as open source. Commercial tools include Opnet [49] and Qualnet [50] with high network protocols and wireless suite. Omnet + + [49] is a free tool for academic purposes but for commercial purposes it requires a license. Open source simulators are like ns-2 [51] and Glomosim [52]which are mostly used for MANET simulation. Swans [53], GTNets (Georgia Tech Network Simulator) [35] and so on are some of the network simulators used for MANET simulation

**Table.3.Features of mobility models**

| | GUI | Output | Platform | Model class | Requirement | Obstacles |
|---|---|---|---|---|---|---|
| SHIFT | Y | N | C++/SHIFT | I | highway | N |
| STRAW | Y | Swans | JiST-Swans | I | urban, highway | N |
| Groovesim | Y | N | C++ | I | N | N |
| Voronoi | N | ns-2 | C++ | I | N | N |
| CanuMobisim | Y | ns-2, Qualnet | java | I | highway | Y |
| city | Y | ns-2 | C++ | I | urban, highway | N |
| Udel Models | Y | ns-2, Qualnet | C++ | I | urban, highway | Y |
| VanetMobisim | Y | ns-2, Qualnet | java | I | urban, highway | Y |
| MoVeS | Y | × | C++ | E | urban, highway | N |
| NCTUns 5.0 | Y | ns-2 | C++ | E | urban, highway | N |
| SUMO | Y | ns-2, Glomosim, Qualnet | C++ | F | urban, highway | N |
| MOVE | Y | ns-2, Glomosim, Qualnet | C++ | F | urban, highway | N |
| TraNS | Y | ns-2, Glomosim, Qualnet | C++ | F | urban, highway | N |
| MobiREAL | Y | GTNets | C++ | F | urban | Y |
| CARISMA | Y | ns-2, qualnet | C++ | F | urban, highway | Y |

**Table.4. Motion Constraints In Mobility Models**

| | Graph | | | Multilane | Speed control | S–D points | Intersection |
|---|---|---|---|---|---|---|---|
| SHIFT | Y | N | N | Y | Y | AP | N |
| STRAW | N | N | TIGER | N | N | R | signs and traffic light |
| Groovesim | N | N | TIGER | N | Y | R | N |
| Voronoi | N | Voronoi | N | N | N | R | N |
| CanuMobisim | Y | N | GDF | N | N | R, AP | N |
| City | N | Grid | N | N | N | R | signs and traffic light |
| Udel Models | Y | N | ESRI [38] | Y Y | Y | R | signs signs and |
| VanetMobisim | Y | Voronoi | TIGER, GDF | N | Y | R, AP | traffic light signs and |
| MoVeS | N | N | GPSTrack | Y | Y | R | traffic light signs and |
| NCTUns 5.0 | Y | N | N | Y | Y YY | R | traffic light signs |
| SUMO | Y | grid, spider | TIGER | Y | Y | R, AP | signssigns |
| MOVE | Y | grid, spider | TIGER | Y | N | R, AP | N |
| TraNS | Y | grid, spider | TIGER | N | Y | R, AP | signs |
| MobiREAL | Y | N | N | Y | | R | |
| CARISMA | N | N | ESRI [38] | | | R | |

**Y: yes, N: no, GDF: geographical data files, AP: access points and R: randoms**

**Table .5.Traffic generators in mobility Models**

| | Path | Velocity | Lane changing | Human patterns | Trip |
|---|---|---|---|---|---|
| SHIFT | N | S | Y | CFM | N |
| STRAW | RWALK and dijkstra | S | Y | CFM | random |
| Groovesim | RWALK and dijkstra | S, Markov, Density | N | N | random |
| Voronoi | RWALK | U | N | N | random |
| CanuMobisim | dijkstra | U | N | IDM | random, activity |
| City | RWM | S | N | IDM | random |
| Udel Models | RWALK | S | Y | CFM | random |
| VanetMobisim | RWP, speed, density and dijkstra | S, Density | MOBIL | IDM, IDMIM and IDMLC | random, activity, user-defined |
| MoVeS | RWALK | U | N | CFM | random |
| NCTUns 5.0 | RWALK and user defined | S | Y | CFM | random, user-defined |
| SUMO | RWALK and dijkstra | S | Y | CFM | random S–D, activity |
| MOVE | RWALK and dijkstra | S | Y | CFM | random S–D, activity |
| TraNS | RWALK and dijkstra | S | Y | CFM | random S–D, activity |
| MobiREAL | RWALK | N | N | CPE | random |
| CARISMA | speed, density and dijkstra | N | N | CFM | random S–D |

### 7.1.3 Isolated vehicular model:

Isolated vehicular models [35] are the mobility models with lack of interaction with the network simulators. It is divided into four parts: legacy mobility model, improved motion constraints, improved traffic generator and improved motion constraints and traffic generator. Legacy Mobility Model includes RandomWaypoint model, Gauss-Markov model, Reference Point Group model, Random Walk model and Node Following model. These models are mainly meant for MANET study. For VANET, Freeway model and Manhattan model are designed. Improved Motion Constraints include BonnMotion tool [54], Obstacle Mobility model [55], Voronoi model [39] and so on. Improved Traffic Generator includes GEMM tool [56] ,CanuMobisim tool [57] and so on. Improved Motion Constraints and Traffic Generator create interaction between the traffic generator and motion constraint. It includes tools like STRAW (Street Random Waypoint) tool [58], SSM/ TSM (Stop Sign Model/Traffic Sign Model) [59], GMSF (Generic Mobility Simulation Framework), VanetMobisim, Udel Model and so on.

### 7.1.4 Embedded models:

The embedded model [35] mainly signifies the union of mobility and networking modules. Groovenet/Groovesim [60] is the first tool to provide embedded vehicular mobility model. Groovesim is the model and Groovenet is the project for modelling. City Model tool [61] is designed for embedding, implementing and testing routing protocols. Then, Bononi et al. designed MoVes [62] which provides driving patterns and a better mobility model. Gorgorin et al. [63] also found a simulator embedded withmobility and networking capabilities. Vuyyuru and Oguchi [64] also designed a tool called Automesh which consists of a radio propagation block, network simulator and driving simulator. Then, NCTUns [65] is developed for providing better mobility and networking capabilities. It can simulate the 802.11 a, 802.11b and 802.11p MAC.

### 7.1.5 Advance mobility models:

These models provide better networking features and motion features. It is also divided into open source and commercial based models. Open source models are the TraNS [66] tool with SUMO and ns-2. One project named VGrid [67] is also launched for study on traffic accidents after using the alert messages. Then, MobiReal [68] is developed which is mainly based on GTNets. These models are also called Federated Mobility Models.

## 8. VANET Applications

At last, we survey the emerging applications of VANET technology. As we know, V2 V and V2I communication provide high mobile applications by which the producer (car manufacturers) as well as consumers (End users) gains better facilities and services. VANET provides applications like e-Safety, traffic management, driver comfort support, maintenance, media services, gaming, e-shopping, crime investigation, defence and so on. VANET uses P2P (Peer-to-Peer) applications [69] for providing services to the customers. P2P applications are divided into four categories for handling the data [69] and are shown in Fig. 5

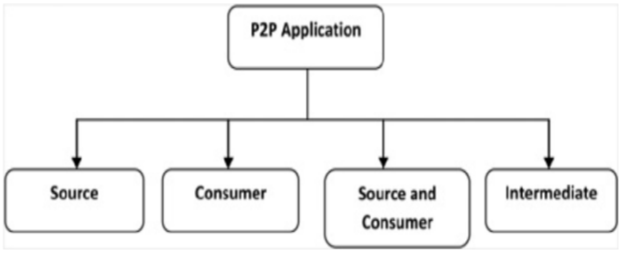

**Figure. 5. Taxonomy of P2P application**

**Source**: Vehicular Sensor Applications use sensors for monitoring and sharing the data. Vehicles use GPS, video cameras, detectors, sensors, RADAR, LASER, vibration and so on to sense the data. MobEyes [69] is a middleware which provides urban monitoring and services. Cartel [70], Pothol Patrol (P2) [71], Zebranet [72], SWIM [73], Metrosense [74], DFT-MSN (Delay/Fault-Tolerant Mobile Sensor Network) [75], CENS [76], Irisnet [77], Sense Web [78], Urbanet [79] and so on are some of the data monitoring projects which sense the data and share the information. † Consumer: Data is downloaded from the AP (Access Points) [69] and it is communicated between the APs and vehicles or vehicles to vehicle. SPAWN [80], CarTorrent [81], CodeTorrent [82] and MOVi (Mobile Opportunistic Video-on-Demand) [83] are some of the protocols for data distribution. Advertisements are mainly produced by the business companies to spread the message in the form of audio, video and images. The main applications include car parking information and location awareness information [69].

**Source and consumer:** Producer and Consumer Application includes V3 (V2 V live Video) [84] streaming. Tavarau [85] is a communication system used for video streaming by using 3G services. Fleanet [86] is a marketplace which creates a virtual environment of market. By this, one can easily find the routes and the product in the market and streets. Roadspeak [87] is an architecture designed for drivers to chat smoothly and exchange information. The main objective of Roadspeak is to provide safety

### 8.1 Advance Applications

Nowadays, many new VANET applications are developing which provides safety and security and establishes strong relations between the producer and the consumer. Applications in VANET are mainly categorised into four parts: e-Safety, traffic management,  e-Safety applications: Traffic Signal Warning System, Stop Sign Warning System, Left Turn Assistance, Emergency Vehicle Approaching Warning System, Intersection Collision Warning system, Pedestrian Crossing Information Enhanced Driving Support and Maintenance. Fig. 6 shows the advanced VANET applications

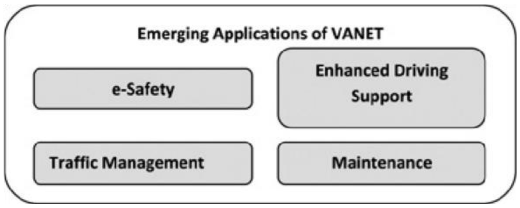

**Figure.6. Emerging applications of VANET**

System, Emergency Vehicle Signal Preemption, Vehicle Safety Inspection System, Electronic License Plate, Electronic Driver

License Plate, Stolen Vehicle Tracking, Crime Investigation, Breakdown warning system, Pre-crash Sensing system, Curve Speed warning System, Accident warning system, Speed Breaker Warning, Rail Collision Warning, Work Zone Warning and so on are some of the e-Safety applications.

† Traffic management applications: Area Access Control, Crash Data Collection, Weather Data Collection, Intelligent Traffic Flow Control, Cooperative Planning, Adaptive Cruise Control, traffic management and so on are some of the traffic management applications.

† Maintenance applications: Software Updating, Wireless Diagnosis, Safety Recall Notice, Hardware, Maintenance, Repair Notification and so on are some of the maintenance applications.

† Enhanced driver support applications: Internet Service Provision, Fuel Information. Media services, Region of Interest Notification, GPS Information, Location Awareness, Parking Spot Information, Route Information Downloading, Map Updating and Downloading and so on are some of the driver support applications.

## 9. Future Research Scope

Vehicular technology is gaining momentum as vehicles are increasing in a rapid manner. Deployment of this advance network is a necessity for many safety applications. The future of VANET is very bright as new ideas and scopes are coming up in recent times. Researchers are working in these upcoming areas to provide safety and security to mankind. There are many research scopes which are to be mined to obtain new ideas and to provide services to the people. Fig. 8 shows the future research areas in VANET. The areas are briefly described as follows:

† Vehicular cloud: Implementation of cloud computing concepts can provide services in software, hardware and platform level. The main use of cloud computing is to provide on-demand resources to the users using virtualisation. By using cloud, many applications are projected like multimedia services, content delivery, location sharing, e-applications, P2P services ( Peer-to-Peer ) and so on. The vehicles with internet access can form a network cloud to provide content delivery and information sharing. The storage can also be used as a service because cars have terabytes of memory. This technology can be used for many applications and it will be an emerging area of research.

† Fault tolerance: VANET is a network and it consists of vehicles which act as nodes. The nodes can fail at any time because of hardware tampering or software fault and this leads to the generation of faulty nodes in the system. At the time of routing, if a vehicle sends data to a faulty vehicle then the data may be dropped and delay increases. Hence, there should be a recovery mechanism which recovers or protects the network from these faults. The generation of new fault tolerance techniques nowadays is also an emerging area of research.

† Mobility model: To enhance the performance of the network there should be a realistic mobility model which implements the traffic scenario. A mobility model can be designed by considering vehicles, buildings, roads, maps, driving patterns, vehicular density, driver's behaviour and so on. This mainly supports in solving the routing problem where the vehicles are moving at a high speed. † MAC layer protocol: The main objective of designing the MAC protocol is to provide fast data exchanges. In the WAVE standard, the IEEE 802.11p protocol is used for wireless communication. The WAVE stack consists of IEEE 1609.1, IEEE 1609.2, IEEE 1609.3 and IEEE 1609.4 to provide services like security, resource allocation, safety applications, LLC management, network services and so on. Hence, there should be a robust and efficient MAC layer protocol.

† Image processing: Image processing is a wide area of research with a huge scope. By using advanced image processing algorithms, the vehicles can track a person by using cameras on the vehicles. This application is used for tracking terrorists on the roads. If a terrorist's image matches with the database image then the vehicle suddenly broadcasts the information to the nearby police station. The videos of the street can also be recorded for criminal investigation.

## 10. CONCLUSION

In this paper, we mainly surveyed the fundamentals of VANET, its architecture, standards, routing issues, security challenges, current projects, simulations, emerging applications and future research problems. Researchers all over the world are mainly working on the current issues of VANET like broadcasting, routing, security, implementation and so on to expand the area of vehicular technology. In this review, we have discussed some secure routing protocols like ARAN, ARIADNE, CONFIDANT, SAODV, SEAD, SPAAR, SLSP and so on which provide security to the routing. In the future, security is a main issue to implement in VANET because many new types of attacks are being generated. This survey helps future researchers to obtain ideas about VANET security. We have also discussed the current VANET projects running in some parts of the world such as the USA, Europe and Japan. Car companies are collaborating with the WHO to design new architectures which provide safety to the passengers and the drivers. We have also reviewed some simulators which help the researchers to select the best one for the implementation of VANET. We have briefly described the mobility model, traffic simulators, network simulators, isolated models, embedded models and federated models. We have presented the current andemerging applications of VANET which provides better services to the end users. We have also surveyed the current applications like driver assistance systems, traffic management systems, e-safety applications and maintenance. At last, we have briefly described some of the future research areas in VANET like Vehicular Cloud, Fault Tolerance, Mobility Model, Image Processing and MAC layer protocol. These research topics play an important role in spreading VANET systems all over the world. We hope this VANET review will help researchers to explore the knowledge about vehicular communication.

## 11. REFERENCES

[1]. http://www.en.wikipedia.org/wiki/List of countries by traffic-related death rate, accessed on January 2013

[2]. Yan, G., Wang, Y., Weigle, M., Olariu, S., Ibrahim, K.: 'Wehealth: a secure and privacy preserving ehealth using notice'.

Proc. Int. Conf. Wireless Access in Vehicular Environments (WAVE), 2008

[3]. Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., Hassan, A.: 'Vehicular ad hoc networks (VANETS): status, results, and challenge', Telecommun. Syst., 2010, 50, (4), pp. 217–241

[4]. Zhang, L., Gao, D., Zhao, W., Chao, H.-C.: 'A multilevel information fusion approach for road congestion detection in VANETs', Math. Comput. Model., 2013, 58, pp. 1206–1221

[5].Kenney, J.B.: 'Dedicated short-range communications ( DSRC ) standards in the United States'. Proc. IEEE, July 2011, vol. 99, no 7 , pp. 1162–1182

[6]. Festag, A.: 'Global standardization of network and transport protocols for ITS with 5 GHz radio technologies'. Proc. ETSI TC ITS workshop, Sophia Antipolis, France, February 2009

[7]. Kudoh, Y.: 'DSRC standards for multiple applications'. Proc. 11 thWorld Congress on ITS, Nagoya, Japan, 2004

[8]. Ho, K.-Y., Kang, P.-C., Hsu, C.-H., Lin, C.-H.: 'Implementation of WAVE/DSRC Devices for vehicular communications'. Int. Symp. Computer Communication Control and Automation, May 2010, vol. 2

[9]. Morgan, Y.L.: 'Notes on DSRC & WAVE standards suite: its architecture, design, and characteristics', Commun. Surv. Tutor., 2010 , 12 , (4), pp. 504–518

[10]. Deng, D.-J., Chen, H.-C., Chao, H.-C., Huang, Y.M.: 'A collision alleviation scheme for IEEE 802.11p VANETS', Wirel. Personal Commun., 2011, 56, (3), pp. 371–383

[11]. Yin, J., Elbatt, T., Habermas, S.: 'Performance evaluation of safety applications over DSRC vehicular ad hoc networks'. Proc. VANET'04, Philadelphia, PA, USA, October 2004

[12]. Li, C.-S., Chao, H.-C.: 'IPv6 auto-configuration VANET cross layer design based on IEEE 1609', IET Netw., 2012, 1, (4), pp. 199–206

[13]. http://www.standards.its.dot.gov/factsheet.asp?f=80, accessed January 2013

[14]. Li, F., Wang, Y.: 'Routing in vehicular ad hoc networks: a survey', IEEE Veh. Technol. Mag., 2007, 2, (2), pp. 12–22

[15]. Nagaraj, U., Kharat, M.U., Dhamal, P.: 'Study of various routing protocols in VANET', IJCST, 2011, 2, (4), pp. 45–52

[16]. Fuentes, J., González-Tablas, A., Ribagorda, A.: 'Overview of security issues in vehicular ad-hoc networks'. Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, 2010, pp. 894–911

[17]. aya, M., Hubaux, J.-P.: 'Securing vehicular ad hoc networks', J. Comput. Sec., 2007, 15, pp. 39–68

[18]. Isaac, J.T., Zeadally, S., Cámara, J.S.: 'Security attacks and solutions for vehicular ad hoc networks', IET Commun., 2010, 4, (7), pp. 894–903

[19]. Leinmuller, T., Schoch, E., Kargl, F.: 'Position verification approaches for vehicular ad hoc networks', IEEE Wirel. Commun., 2006, 13, (5) , pp. 16–21

[20]. Gongjun, Y., Olariu, S., Weigle, M.: 'Providing location security in vehicular ad hoc networks', IEEE Wirel. Commun., 2009, 16, (6) , pp. 48–55

[21]. Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., Belding-Royer, E.-M.: 'A secure routing protocol for ad hoc networks'. Proc. Int. Conf. Network Protocols (ICNP), Paris, France, November 2002 , pp. 78–87

[22]. Hu, Y.-C., Perrig, A., Johnson, D.B.: 'ARIADNE: a secure on-demand routing protocol for ad hoc networks'. Proc. ACM Int. Conf. Mobile Computing and Networking (MOBICOM'02), Atlanta, GA, USA,
September 2002, pp. 12–23

[23]. Buchegger, S., LeBoudec, J.-Y.: 'Performance analysis of the CONFIDANT protocol (cooperation of nodes: fairness in dynamic ad-hoc NeTworks)'. Proc. Third ACM Int. Symp. Mobile and Ad Hoc Networking and Computing (MobiHoc 2002), Lausanne, Switzerland, June 2002, pp. 226–236

[24]. Zapata, G.M.: 'Secure ad hoc on-demand distance vector routing'. ACM Mobile Computing and Communications Review (MC2R), July 2002

[25]. Hu, Y.-C., Johnson, D.B., Perrig, A.: 'SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks'. Proc. Fourth IEEE Workshop on Mobile Computing Systems and Applications, Calicoon, NY, USA, 2002, pp. 3–13

[26]. Papadimitratos, P., Haas, Z.J.: 'Secure link state routing for mobile ad hoc networks'. Proc. 2003 Symp. Applications and the Internet Workshops, Washington, DC, USA, January 2003, pp. 379–383 27 Carter, S., Yasinsac, A.: 'Secure position aided ad hoc routing protocol'. Proc. IASTED Int. Conf. Communications and Computer Networks, November 2002

[28]. Clausen, T., Adjih, C., Jacquet, P., Laouiti, A., Muhlethaler, A., Raffo, D.: 'Securing the OLSR protocol'. Proc. IFIP Med-Hoc-Net, June 2003

[29]. http://www.neo.lcc.uma.es/staff/jamal/vanet/?q=content/vanet-its-projects, accessed on January 2013

[30]. Festag, A., Fubler, H., Hartenstein, H., Sarma, A., Schmitz, R.: 'FleetNet: bringing car-to-car communication into real world'. Proc. 11th World Congress on Intelligent Transportation Systems, Nagoya, Japan, October 2004

[31]. Hartenstein, H., Fubler, H., Mauve, M., Franz, W.: 'Simulation results and a proof of concept implementation of the FleetNet position-based router'. Proc. Eighth Int. Conf. Personal Wireless Communications, Venice, Italy, September 2003, pp. 192–197

[32]. IEEE Standard 1609.1-2006, IEEE trial-use standard for wireless access in vehicular environments (WAVE), 2006, pp. 1–63

[33].VI (Intelligent Vehicle Initiative): 'Technology-advanced controls and navigation systems'. Proc. Society of Automotive Engineers, SAE World Congress, Detroit, USA, 2005

[34]. Tsugawa, S., Kato, S., Tokuda, K., Matsui, T., Fujii, H.: 'A cooperative driving system with automated vehicles and intervehicle communications in Demo 2000'. Proc. IEEE Intelligent Transportation Systems, Dearborn, MI, 2000

[35]. Harri, J., Filali, F., Bonnet, C.: 'Mobility models for vehicular ad hoc networks: a survey and taxonomy', IEEE Commun. Surv. Tutor., 2009, 11, (4), pp. 19–41

[36]. Wang, J., Yan, W.: 'RBM: a role based mobility model for VANET'. Proc. Int. Conf. Communications and Mobile Computing, January 2009, 2, pp. 437–443

[37]. Liu, B., Khorashadi, B., Du, H., Ghosal, D., Chuah, C., Zhang, M.: 'VGSim: an integrated networking and microscopic vehicular mobility simulation platform', IEEE Commun. Mag., 2009, pp. 134–141

[38]. http://www.esri.com/library, accessed on January 2013

[39]. Zimmermann, H.M., Gruber, I.: 'A voronoi-based mobility model for urban environments'. Proc. European Wireless, April 2005

[40]. http://www.transims.tsasa.lanl.gov, accessed on January 2013

[41]. http://www.english.ptv.de/cgi-bin/traffic/trafvissim.pl, accessed January 2013

[42]. http://www-mctrans.ce.ufl.edu/featured/ SIS/V ersion5 /corsim.htm, accessed January 2013

[43]. http://www.paramics-online.com/, accessed January 2013 44 Schroth, C., Dotzer, F., Kosch, T., Ostermaier, B., Strassberger, M.: 'Simulating the traffic effects of vehicle-to-vehicle messaging systems'. Proc. Fifth Int. Conf. ITS Telecommunications, Brest, France, 2005

[45]. http://www.path.berkeley.edu, accessed on January 2013

[46]. http://www.sumo.sourceforge.net, accessed on January 2013

[47]. http://www.census.gov/geo/www/tiger, accessed on January 2013

[48]. Karnadi, F., Mo, Z., Lan, K.-C.: 'Rapid generation of realistic mobility models for VANET'. Proc. IEEE Wireless Communication and Networking Conf. (WCNC'07), March 2007

[49]. http://www.opnet.com/products/modeler/home.html, accessed on January 2013

[50]. http://www.scalable-networks.com, accessed on January 2013

[51]. http://www.isi.edu/nsnam/ns, accessed on January 2013

[52]. http://www.pcl.cs.ucla.edu/projects/glomosim, accessed on January 2013

[53]. http://www.jist.ece. cornell.edu/, accessed on January 2013

[54]. http://www.web.informatik.uni- onn.de/IV/ Bonn Motion, accessed on January 2013

[55]. http://www.moment.cs.ucsb.edu/mobility/, accessed on January 2013

[56]. Feeley, M.J., Hutchinson, N.C., Ray, S.: 'Realistic mobility for mobile ad hoc network simulation'. Lecture Notes in Computer Science, 2004, pp. 324–329

[57] http://www.canu.informatik.uni-stuttgart.de, accessed on January 2013 58 http://www.aqualab.c ms.northwestern. edu/projects/STRAW/index.php, accessed on January 2013

[59]. Sommer, P., Baumann, R., Legendre, F., Plattner, B.: 'Generic mobility simulation framework'. Proc. First ACM Sigmobile Workshop on Mobility Models, New York, USA, 2008, pp. 49–56

[60].http://www.andrew.cmu.edu/user/rahulm/Research/Groove Net, accessed on January 2013

[61]. Jaap, S., Bechler, M., Wolf, L.: 'Evaluation of routing protocols for vehicular ad hoc networks in city traffic scenarios'. Proc. Fifth Int. Conf. Intelligent Transportation Systems Telecommunications, Brest, France, June 2005

[62]. Bononi, L., Di Felice, M., Bertini, M., Croci, E.: 'Parallel and distributed simulation of wireless vehicular ad hoc networks'. Proc. ACM/IEEE Int. Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Torresmolinos, Spain, 2006

[63]. Gorgorin, C., Gradinescu, V., Diaconescu, R., Cristea, V., Ifode, L.: 'An integrated vehicular and network simulator for vehicular ad-hoc networks'. Proc. European Simulation and Modeling Conf. ( ESM), Bonn, Germany, May 2006

[64]. Vuyyuru, R., Oguchi, K.: 'Vehicle-to-vehicle ad hoc communication protocol evaluation using simulation framework'. Proc. 4th IEEE/IFIP Wireless On demand Networks and Services, Austria, 2007 , pp. 100–106

[65]. Wang, S.Y., Chou, C.L.: 'NCTUns simulator for wireless vehicular ad hoc network research'. Ad Hoc Networks: New Research, Nova Science Publishers, 2008

[66]. http://www.wiki.epfl.ch/trans/, accessed on January 2013

[67].http://www.csif.cs.ucdavis.edu/VGrid, accessed on January 2013

[68]. http://www.mobireal.net, accessed on January 2013

[69]. http://www.nrlweb.cs.ucla.edu/publication/download/ 521/ 09-Emerging_ Vehicular_Applications.pdf

[70]. Hull, B., Bychkovsky, V., Chen, K., et al.: 'CarTel: a distributed mobile sensor computing system'. ACM SenSys, Boulder, CO, USA, October– November 2006

[71]. Eriksson, J., Girod, L., Hull, B., Newton, R., Balakrishnan, H., Madden, S.: ‘The pothole patrol: using a mobile sensor network for road surface monitoring’. MobiSys’08, Breckenridge, Colorado, June 2008

[72]. Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L.-S., Rubenstein, D.: ‘Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with ZebraNet’. ACM ASPLOS, San Jose, CA, USA, October 2002

[73]. Small, T., Haas, Z.J.: ‘The shared wireless infostation model – a new ad hoc networking paradigm (or Where There is a Whale, There is a Way)’. ACMMOBIHOC, Annapolis, Maryland, USA, June 2003

[74]. Eisenman, S.B., Ahn, G.-S., Lane, N.D., Miluzzo, E., Peterson, R.A., Campbell, A.T.: ‘MetroSense project: people-centric sensing at scale’. ACM WSW, Boulder, CO, USA, October–November 2006

[75]. Wang, Y., Wu, H.: ‘DFT-MSN: the delay/fault-tolerant mobile sensor network for pervasive information gathering’. INFOCOM’06 , Barcelona, Spain, April 2006

[76]. Burke, J., Estrin, D., Hansen, M., et al.: ‘Participatory sensing’. ACM WSW, Boulder, CO, USA, October–November 2006

[77]. Gibbons, P.B., Karp, B., Ke, Y., Nath, S., Seshan, S.: ‘IrisNet: an architecture for a worldwide sensor web’, IEEE Pervasive Comput., 2003, 2, (4), pp. 22–33

[78]. Nath, S., Liu, J., Zhao, F.: ‘Challenges in building a portal for sensors world-wide’. CM WSW, Boulder, CO, USA, October–November 2006

[79]. Riva, O., Borcea, C.: ‘The urbanet revolution: sensor power to the people’, IEEE Pervasive Comput., 2007, 6, (2), pp. 41–49

[80]. Nandan, A., Das, S., Pau, G., Gerla, M., Sanadidi, M.Y.: ‘Co-operative downloading in vehicular ad-hoc wireless networks’. IEEE/IFIP WONS, Saint Moritz, Swiss, January 2005

[81]. Lee, K.C., Lee, S.-H., Cheung, R., Lee, U., Gerla, M.: ‘First experience with cartorrent in a real vehicular ad hoc network testbed’. MOVE’07 , Anchorage, Alaska, May 2007

[82]. Lee, U., Park, J.-S., Yeh, J., Pau, G., Gerla, M.: ‘CodeTorrent: content distribution using network coding in VANETs’. MobiShare’06, Los Angeles, CA, September 2006

[83]. Yoon, H., Kim, J., Tan, F., Hsieh, R.: ‘On-demand video streaming in Mobile Opportunistic networks’. IEEE Int. Conf. in Pervasive Computing and Communications, Hong Kong, China, March 2008

[84]. Guo, M., Ammar, M.H., Zegura, E.W.: ‘V3: a vehicle-to-vehicle live video streaming architecture’. IEEE Int. Conf. in Pervasive Computing and Communications, March 2005

[85]. Qureshi, A., Carlisle, J., Guttag, J.: ‘Tavarua: video streaming with WWAN striping’. ACM Multimedia 2006, Santa Barbara, CA, October 2006

[86]. Lee, U., Park, J.-S., Amir, E., Gerla, M.: ‘FleaNet: a virtual market place on vehicular networks’. V2VCOM’06, San Jose, CA, July 2006

[87]. Smaldone, S., Han, L., Shankar, P., Iftode, L.: ‘RoadSpeak: enabling voice chat on roadways using vehicular social networks’. SocialNets’08, Glasgow, Scotland, UK, April 2008

[88]. Golle, P., Greene, D., Staddon, J.: ‘Detecting and correcting malicious data in VANETs’. Proc. First ACM Workshop on Vehicular Ad Hoc Networks (VANET 2004), Philadelphia, PA, USA, October 2004, pp. 29–37

[89]. Marti, S., Giuli, T.J., Lai, K., Baker, M.: ‘Mitigating routing misbehavior in mobile ad hoc networks’. Proc. Sixth Annual ACM/ IEEE Int. Conf. Mobile Computing and Networking, Boston, MA, USA, August 2000, pp. 255–265iore, M., Harri, J., Filali, F., Bonnet, C.: ‘Vehicular mobility simulation for VANETs’. Proc. 40th Annual Simulation, Symp., March 2007 , pp. 301–309

[90]. Tuduce, C., Gross, T.: ‘A mobility model based on WLAN traces and its validation’. Proc. IEEE INFOCOM 2005, Miami, March 2005 92 http://www.udelmodels.eecis.udel.edu/, accessed January 2013

[91]. http://www.vanet.eurecom.fr, accessed on January 2013

[92]. http://www.omnetpp.org/, accessed on January 2013

[93]. Mahajan, A., Potnis, N., Gopalan, K., Wang, A.: ‘Evaluation of mobility models for vehicular ad-hoc network simulations’. Technical Report N.051220, Florida State University, 2005