A Survey on VANETs Applications and Its Challenges

Razia Begum[1]
Assistant Professor[1]
raziabegum2007@gmail.com[1]
Department of Computer Science and Engineering[1]
Deccan College of Engineering and Technology, Hyderabad, India.

Dr. Syed Raziuddin[2]
Professor & Head[2]
informraziuddin@gmail.com[2]
Department of Computer Science and Engineering[2]
Deccan College of Engineering and Technology, Hyderabad, India.

Dr. V. Kamakshi Prasad[3]
Professor& Head[3]
kamakshiprasad@yahoo.com[3]
Department of Computer Science and Engineering[3]
JNTUH College of Engineering and Technology, Hyderabad, India.

Abstract

Vehicular Ad hoc Network (VANET) is an ad hoc network in which vehicles acts as nodes. It is an application of MANET. VANET is becoming an active area of research because it has tremendous potential to improve safety of vehicles and traffic efficiency. We use the VANET instead of Mobile Ad hoc Network (MANET) due to high mobility of the vehicles as MANET does not support high mobility. Wireless Vehicular ad hoc network technology is designed for allowing wireless communication between vehicles on the road, enabling the transfer of information to ensure driving safety and traffic management with internet access to drivers and programmers. VANET applications include traffic optimization, payment services, location-based services and infotainment. Providing security in VANET is a challenging due to its characteristics like network topology changes, high mobility, scalability, limited bandwidth, frequent exchange of information, wireless communication, absence of infrastructure, battery power and storage capacity. Because of the road safety functions there is a strong demand for security in VANETs as human lives can be affected directly or indirectly by a single wrong message. In this paper, we are going to survey different applications and challenges of VANETs.

Key Words: ***Vanet, Manet, Mobile Ad Hoc Network, Network Topology.***

I. INTRODUCTION

Now days, the large road traffic affects the safety and efficiency of traffic environment. Approximately 1.2 million people are killed every year by the road accidents. Road traffic safety has been the challenging issue in traffic management. One possible way to make the vehicles analyze the traffic environment is by providing the traffic information to the vehicles. It can be done by exchanging the information of traffic environment among vehicles. A wireless mobile network is needed as all the vehicles are mobile in nature. It is possible to implement node and network device into a single unit called ad hoc network which has wireless inter connections. VANET is ad hoc application. In other words, VANET is an organized network that can be formed by connecting vehicles aiming to improve driving safety and traffic management with internet access by drivers and programmers. We use the VANET instead of Mobile Ad hoc Network (MANET) due vehicles high mobility and we know that MANET does not support high mobility. [1]. A Dedicated Short Range Communication (DSRC) is used for communication among vehicles and for vehicle to infrastructure communication. DSRC is a band of 75MHz in 5.9 GHz, allocated by Federal Communication Commission (FCC)[2]. As VANETs are implementation of MANETs, shown in figure 1 they inherit all vulnerabilities related to MANETs [3].

II. VANET ARCHITECTURE

The goal of VANET architecture, shown in figure 2 is to allow the communication among nearby vehicles and between

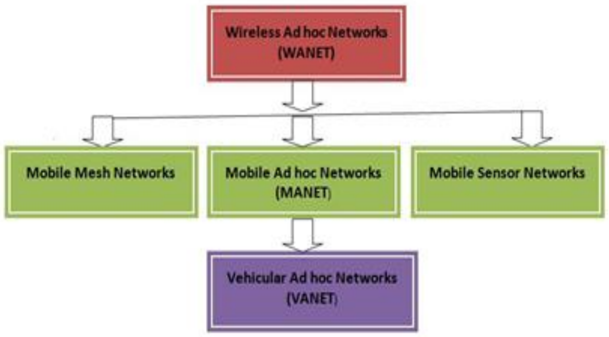
Wireless Ad hoc Networks (WANET)
Mobile Mesh Networks
Mobile Ad hoc Networks (MANET)
Mobile Sensor Networks
Vehicular Ad hoc Networks (VANET)

Fig. 1: Hierarchy of Wireless Ad hoc networks

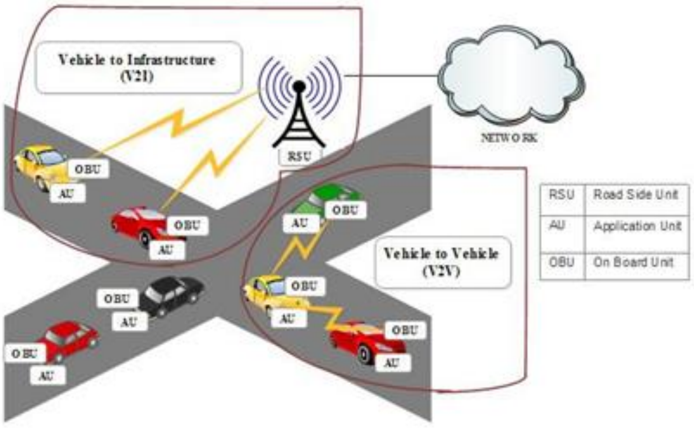

Fig. 2: VANET architecture

Vehicles and fixed roadside equipments in two possibilities:

A. Vehicle-to-Vehicle (V2V) ad hoc network:

Allows the direct vehicular communication without depending on a fixed infrastructure support and can be mainly used for safety, security applications.

B. Vehicle-to-Infrastructure (V2I) ad hoc network:

This network allows a vehicle to communicate with the road side infrastructure for information and data collection applications.

The main components of VANETs are the Application Unit (AU), On Board Unit (OBU) and Road Side Unit (RSU) [4]. Each node in VANET contains: On Board Unit (OBU) and Application Unit (AU). The OBU has the communicational capability whereas AU executes the program utilizing OBUs

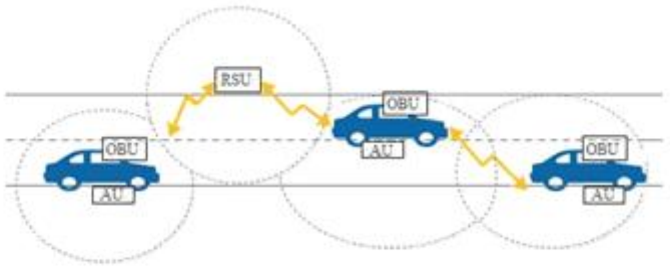

Fig. 3: RSU extending the range of networks

Communicational capabilities. RSU can be attached to the infrastructure network which is connected to the Internet.

1) Application Unit(AU): AU is an in-vehicle entity and runs applications which utilize the OBUs communication capabilities. Examples are:(i) A dedicated device for safety applications like hazard-warning and (ii)A navigation system.

AUs can be plugged in with a single OBU and share the OBUs processing and resources. AU communicates via OBU, which handles all mobility and networking functions on AUs behalf. The distinction between an AU and an OBU is only logical and an AU can be physically located with an OBU.

2) On-board Unit(OBU): An On-Board Unit (OBU) is responsible for both vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communication. It also provides communi-cation services to AUs (Application units) and forwards data in the ad hoc domain on behalf of other OBUs. An OBU is equipped with at least a single network device designed for short range wireless communications. This network device is used to send, receive and forward safety-related data in the ad hoc domain. OBU can also be equipped with more network devices, e.g. for non-safety communications. OBU functions and procedures include geographical ad hoc routing, wireless radio access, data security, network congestion control, IP mobility support, reliable message transfer, and other.

3) Road Side Unit(RSU): A Road-Side Unit (RSU) is a physical device which are located at fixed positions along roads or highways, and at dedicated locations such as parking places, gas station and restaurants. An RSU is equipped with at least a network device for wireless communication short in range. An RSU can also be equipped with other network devices in order to allow communications with an infrastructure network. The main functions of a RSU are :

i) Extending the communication range of an ad hoc network, by means of re-distribution of information to other OBUs and cooperating with other RSUs [5]. as shown in figure 3

ii) Running safety applications, shown in figure 4, such as for V2I warning (e.g. work-zone warning, low bridge warning), and act as information source and receiver.

iii) Providing internet connectivity to OBUs, shown in figure 5.

III. VANET CHARACTERISTICS

When compared to MANETs, VANETs has its unique characteristics. The characteristics of VANETs include:

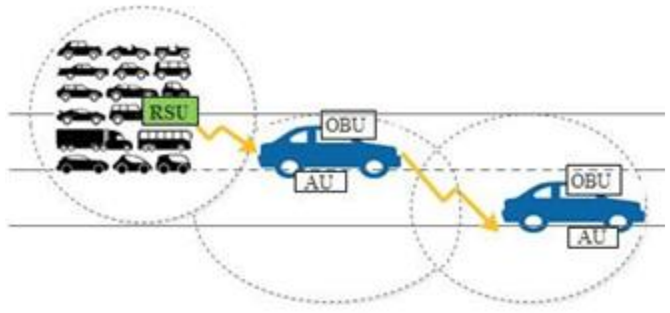

Fig. 4: Works as information source for vehicles

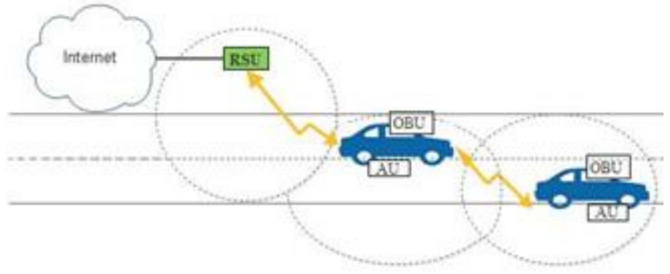

Fig. 5: RSU provides internet connectivity

A. High Mobility

The speed and location of every node in VANETs is high and different from each other which makes it difficult to find their locations and maintain privacy of nodes [6].Mobility pattern of vehicles depends on structure of road, environment of traffic, speed of vehicles, drivers driving behavior etc.,

B. Dynamic Topology

Due to high speed and mobility the directions of nodes changes frequently, hence the entire network gets prone to attack and detection of malfunctioning gets difficult [9]. Sup-pose two vehicles are with radio range of 160m and moving at the speed of 20m/sec. Then the link between the two vehicles will last 160/20 = 8 sec.

C. Interaction with onboard sensors

Onboard sensors like GPS device helps to find current position and movement of nodes. Communication and routing decisions can be made effectively by interacting with onboard sensors.

D. Limited Bandwidth

According to standardized band DSRC band is limited which is 75MHz, and also restricted to lower values in some countries. The lower bandwidth leads to frequent disconnections between two vehicles when exchanging information.

E. Frequent exchange of information

In VANETs the nodes exchange information with other vehicle and road side units. Hence, exchange of information is more frequent.

TABLE I: VANET Applications

Category	Sub-category
Safety Applications	Curve speed warning, Low bridge warning, Warning about violated traffic lights, Vehicle-based road condition warning, Visibility enhancer, Work zone warning, Blind spot warning, Intersection collision warning, Lane change warning, Highway/rail collision warning, Pre-crash sensing, Post-crash sensing, Approaching emergency vehicle warning, Emergency vehicle signal preemption, Left Turn Assistant, Traffic Optimization, In-vehicle signage.
Non-Safety Applications	Safety recall notification, Just-in time repair notification, Internet service provisioning, Instant Messaging, Electronic Toll Collection, Parking Availability, Fuel Saving

F. Energy Storage and Computing

VANET is different from other type of mobile computing techniques as it does not suffer from energy and capacity computing. Vehicles battery power and storage is unlimited. The VANETs nodes have no issue of energy and computation resources and also provide unlimited transmission power.

G. Wireless Communication

Nodes in VANET are connected and exchange their in-formation via wireless. VANETs are designed for wireless environment, therefore security measures must be considered.

H. Time Critical

Timely delivery of messages is very essential [7]. The process of transmission of information is bounded so that decisions are made by the receiver nodes and actions are performed accordingly. The information in VANETs must be delivered to the nodes within time limits so that a decision can be made by the node and actions should be performed.

I. Large Scale Network

The scale of network could be large in dense urban areas such as the city center highways and the entrance of the big cities.

IV. VANET APPLICATIONS

Based on the primary purposes, VANET applications are classified into two categories as shown in TABLE I

A. Safety Applications

These applications aim to improve road safety, to avoid accidents and to provide a clear environment. The safety applications are as follows:

1) Curve speed warning: In this application RSU
is to be fixed by the curve to distribute messages to approaching vehicles alerting them about the speed required to arrange the curve safely and alerting the location of the curve.

2) Low bridge warning: This system alerts the driver about the minimum height of the park they are trying to enter, by sending a warning message to the vehicle by an RSU installed close to the parking facility, and then the OBU can find whether it is safe to enter the structure.

3) Warning about violated traffic lights: When a vehicle violates the traffic rules by travelling in a wrong direction, then this system alerts the vehicle. By using V2V communication vehicles can also warn other vehicles travelling on the wrong way via warning messages to prevent occurring of accidents.

4) Vehicle-based road condition warning: This system is based on V2V communication, the vehicle collects

sufficient information about the road status by the vehicles sensors, after collecting road information, the in-vehicle units process this data to determine the road situation in order to start a warning to the driver or send a warning message to other vehicles.

5) Visibility enhancer: Bad weather conditions such as snow, rain and fog lead to poor visibility for the drivers. This system sense bad weather conditions and warn the drivers about these conditions and other vehicles on the road about them.

6) Work zone warning: This system depends on the RSU installed close to the work zone, and warns the coming vehicles about the work zone area by sending warning messages.

7) Blind spot warning: This application alerts the drivers if they decide to change the lane and there is a vehicle in the blind spot, it uses V2V communication for sending warning messages to other vehicles on the road.

8) Intersection collision warning: This application sends a warning message to all the vehicles if there is probability of an accident by collecting the information about road intersection via sensors.

9) Lane change warning: This application is designed to avoid crashes that might occur when the driver decides to change the lane. The system collects data about the vehicles such as vehicle position, speed and direction. When the driver changes his/her current lane the system examines the data collected and checks whether the decision will lead to an accident. Then the system issues a warning to alert the driver about this situation and uses V2V communication to alert other vehicles.

10) Highway/rail collision warning: This application prevents vehicles from train accidents by notifying vehicles about collision with trains or vehicles correct decisions by receiving warning messages directly from the train [12]. It uses RSUs placed at intersection for notifications.

11) Pre-crash sensing: The main goal of this system is predicting a situation where accidents are going to happen. This system uses V2V communication and increases the safety for drivers and passengers.

Post crash warnings: When a vehicle is disabling because of foggy weather or due to an accident then this Application is designed to send warning messages from the disabled vehicle to other vehicles coming in same or opposite direction by using both types of communications (V2V and V2I).

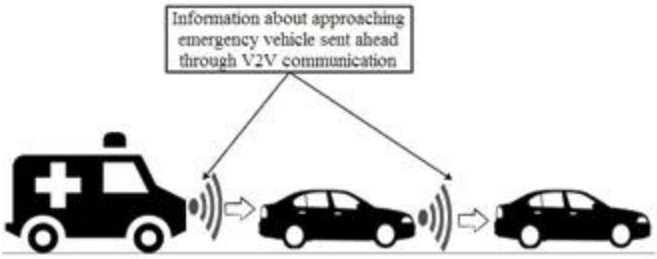
Information about approaching emergency vehicle sent ahead through V2V communication

Fig. 6: Approaching emergency vehicle warning

13) Approaching emergency vehicle warning: The aim of this application is to make arrangements to provide clear roads to allow emergency vehicles to reach their destinations as shown in figure 6.This system relies on one way V2V communication between vehicles traveling on the same route.

14) Emergency vehicle signal preemption: This system is designed to send messages to all traffic lights on the route to the destination using V2I communication to set all the lights to green when the emergency vehicle arrives at the traffic signals.

15) Left turn assistant: This application aims to help the driver to make a left turn at an intersection in a safe way by sending the information collected about the traffic status on the opposite side of the road to the vehicles desiring to make the left turn.

16) Traffic Optimization: Traffic can be optimized by send-ing jam, accident signals to other vehicles so that they save time by choosing an alternate path

17) In-vehicle signage: This application relies on RSU and is designed to send alert messages to vehicles approaching zones like schools, hospitals or animal passing area.

B. Non-safety Applications

These are also called as comfort applications. They provide drivers or passengers with weather and traffic information and provide the location of nearest restaurants, petrol station or hotel and their prices. The non-safety applications are as follows:

1) Safety recall notice: When a recall is issued, the driver is notified by a message sent to vehicle.

2) Just-in-time repair notification: If there is a fault within a vehicle then by using V2I communication the OBU sends a message to the infrastructure. Vehicles then receive reply message containing instructions to tackle the problem.

Internet service provisioning: The passengers in a vehicle can enjoy the facility of Internet connectivity where other wireless internet connectivity options (Wi-Fi, Wi-MAX etc.) are not available [11].Vehicles are allowed to connect to inter-net by using internet service providers for weather information, mp3 download as shown in figure 7 advertisements, parking payment, gas payment or for playing games.

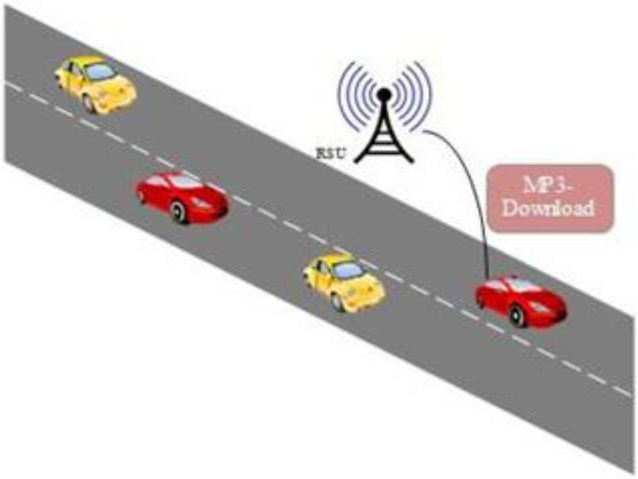

Fig. 7: Using Internet Service Provider for downloads

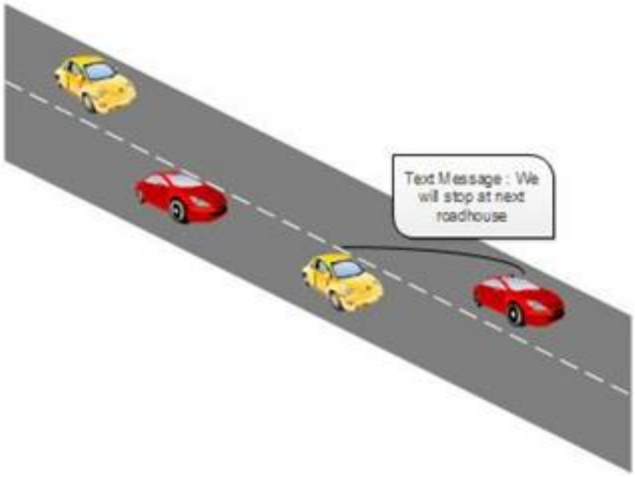

Fig. 8: Instant Messaging in VANETs

4) Instant messaging: Vehicles can communicate to other vehicles by using instant messaging as shown in figure 8

5) Electronic Toll collection: This application allows the vehicles to pay a fixed charge or tax for passage along a road. Toll payment can be done electronically. A Toll Collection Point is used for electronic toll payment as shown in figure 9. These points must be able to read vehicles OBU. Parking Availability: In parking lots, it is difficult to find availability of slots. Parking availability in metropolitan cities can be notified by using VANETs.

Fig. 9: Electronic Toll Collection in India

TABLE II: VANET Challenges

Category	Sub-category
Technical Challenges	Network Management Electromagnetic Communication Collision and Transmission errors Location Awareness MAC Design Congestion and Collision Control Network Fragmentation Signal Fading Data Management and Storage
Security Challenges	High Mobility Bandwidth Limitations Volatility Attacks on privacy Connectivity Scalability Key Distribution Low tolerance for errors Data Consistency Real time constraint
Socio-economic Challenges	Co-operation with other networks Convincing Manufacturers

7) Fuel Saving: Fuel around 3% is saved when vehicles are not stopped at toll booths. Vehicles TOLL system application collects toll at toll booths.

V. VANET CHALLENGES

Some characteristics of VANET impose challenges as shown in TABLE II for the deployment of VANETs. VANET challenges can be categorized as follows:

A. Technical Challenges

The technical obstacles that must be resolved before deployment of VANET are dealt by technical challenges. Some challenges are as follow:

1) Network Management: The network topology and channel condition changes rapidly, due toits high mobility so it gets difficult to manage network.

2) Electromagnetic Communication: In VANET the electromagnetic waves of communication are used and these are affected by environment.

3) Collision and Transmission errors: VANET topology can have 100s of vehicles in very small region; hence it is necessary to design protocols for medium access control to avoid collision and transmission errors.

4) Location Awareness: Awareness of location is necessary as any error in the location awareness can affect location based services.

5) MAC design: The shared medium is used by VANET to communicate. Hence, MAC design is the key issue. IEEE 802.11 adopted CSMA based MAC for VANETs [13].

6) Congestion and Collision Control: In rush hours, the network is congested and collision occurs due to the high traffic load.

7) Network Fragmentation: Network fragmentation occurs in places of light traffic or rural areas, it causes some of the nodes to become unreachable.

8) Signal Fading: Buildings or other vehicles in urban regions may contain obstacles for nodes communication. These objects may cause transmitted signal fading or prevent signals from reaching its destination

9) Data Management and Storage: Millions of vehicles Will generate huge amount of distributed data that must be stored and distributed across VANETs. Hence huge data storage is required.

B. Security Challenges

VANET architecture design, cryptographic algorithm, security protocols etc. requires the consideration of security challenges. Some of them are as follows:

1) High mobility: In VANET high topology changes occur due to high speed of vehicles. These changes cause frequent link failures.

2) Bandwidth Limitations: In VANETS there is no central coordinator to control and manage the bandwidth. Channel contention increases data transmission latency which is very negative impact for delivery of warning messages in safety applications. For entertainment applications, the non-optimal use of bandwidth and channel contention causes quality of service degradation.

3) Volatility: Vehicular networks lacks long life context. Long life password is required for personal contact of users device to a hot spot[8].

4) Attacks on Privacy: In VANETs vehicles exchange their sensed traffic environment changes to other vehicles. Such exchanges create privacy concerns since the vehicle generates reports containing much private information.

5) Connectivity: The nodes connectivity can be in short period of time. Communications between vehicles will be lost as each car has high mobility and may travel in opposite direction.

6) Scalability: As VANETS are experiencing growing interest both in industry and research and there is no global authority to govern the standards. Hence, scalability is a challenge to VANETs.

7) Key Distribution: Each message in VANET is encrypted by the sender and need to decrypt at receiver either with same or different key. Also the manufacturers can install keys in different ways. Therefore, for designing security protocols the right distribution of keys is needed.

8) Low tolerance of errors: A single small error in probabilistic algorithm may cause harm as VANET uses critical information and actions performed in a very short time

9) Data Consistency: Even the authentication node in VANET can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism is required to avoid this inconsistency.

10) Real time constraints: In VANETs, strict deadlines for message delivery is required as it is majorly used for collision avoidance, hazard warning and accident warning information. VANET is time critical where safety messages should be delivered with 100ms transmission delay.

C. Socio-economic Challenges

Social and economic challenges must also be considered apart from technical and security challenges. Some are as follow:

1) Co-operation with other networks: Drivers in a VANET must interact with people, applications and services in other networks. This co-operation is required to provide good ser-vice to user, like information about traffic conditions, weather and routes.

2) Convincing Manufacturers: To build a system which conveys traffic signal violation, monitoring is required which the consumers may reject. So, convincing manufacturers is a challenge in VANETs.

VI. FUTURE

VANETs have become the part of government projects. The National Highways Authority of India (NHAI) is planning to replace toll collections at plazas which are manually done with electronic toll collection (ETC) systems all over the country [13]. Various projects have been conducted in various countries to employ VANETs traffic efficiency and safety. Countries like USA, Japan and the European nations are using the ITS systems by implementing VANET in the urban areas [14]. Although there are many challenges left this will have strong influence on VANETs future.

VII. CONCLUSION

In this survey we have dealt with the issues facing VANET in particular, VANET architecture components, VANET communication, VANET characteristics. An emerging area of research in VANET is security enforcement in order to make the system more reliable for the users. In this survey, we have overviewed VANETs characteristics leading to security challenges. We also have discussed different types of communications possible in VANETs. Additionally we have discussed VANETs safety and non-safety applications. We want to clarify that the list of applications and challenges identified here is not exhaustive. This investigation may enable researchers to focus on issues surrounding VANET and its applications.

REFERENCES

[1] Vivek Chand Dubey and Vinod Kumar, ’Survey: Secure Routing in VANET’, International Journal of Advanced Research in Computer Science & Technology, Vol. 3, Issue 1 (Jan. - Mar. 2015).

[2] Raju Barskar, Meenu Chawla, Vehicular Ad hoc Networks and its Applica-tions in Diversified Fields,International Journal of Computer Applications (0975 8887) Volume 123 No.10, August 2015.

[3] Vinh Hoa LA , Ana CAVALLI,SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY, International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[4] Ramachandran. R, Saravanan. S,A Survey on Security Challenges and Threats of Vehicular Ad hoc Networks (VANETS), International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 2, February 2014, ISSN: 2278-0181.

[5] Mr. Bhagirath Patel,Ms. Khushbu Shah, A Survey on Vehicular Ad hoc Networks, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 4 (Nov. - Dec. 2013).

[6] Ram Shringar Raw, Manish Kumar, Nanhay Singh, Security Challenges Issues And Their Solutions for VANET, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[7] Divya Chadha, Reena, Vehicular Ad hoc Network (VANETs): A Review, International Journal of Innovative Research in Computer and Communi-cation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, March 2015.

[8] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, Security Analysis of Vehicular Ad Hoc Networks(VANET), 2010 Second International Conference on Network Applications, Protocols and Services.

[9] Gunjan, Dr. Dinesh Arora, Tulika Mehta, Detection of Malicious Nodes and Effective and Secured Communication in VANETs, IJECT Vol. 6, Issue 3, July.

[10] Vishal A. Polara, Chintan Mahant, Bijal Dalwadi, Study of Security Issues in Vehicular Ad-Hoc Network, International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 8616Volume 4, Issue 1 January 2015.

[11] Saira Gillani, Imran Khan, Shahid Qureshi, Amir Qayyum,Vehicular Ad Hoc Network (VANET): Enabling Secure and Efficient Transportation System.

[12] Saif Al-Sultan, Moath M Al-Doori, Ali H. Al-Bayatti, Hussien Zedan, A Comprehensive survey on Vehicular Ad hoc Network, Journal of Network and Computer Applications.

[13] Vishal Kumar, Shailendra Mishra, Narottam Chand, Applications of VANETs: Present & Future Communications and Network, 2013, 5, 12-15 Sourav Kumar Bhoi, Pabitra Mohan Khilar, Vehicular communication: a survey IET Networks, 2014, Vol. 3, Iss. 3, pp. 204217 , ISSN 2047-4954