International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 9 Sep 2021, pp: 1504-1511 www.ijaem.net ISSN: 2395-5252

Vehicular Ad hoc Network (VANETs): A Review

Virendra kumar, Dr.Akash Sanghi

M.Tech (CSE), Invertis UniversityAssistant Professor, Invertis University

Submitted: 15-09-2021 Revised: 25-09-2021 Accepted: 28-09-2021

ABSTRACT- In the near future we know that vehicles will communicate with each other to make Vehicular ad hoc network and gives the concept of intelligent transportation system Vehicular ad hoc networks (VANETs) have great potential to improve road safety and increase passenger convenience in vehicles. On the other hand, since they use an open medium for communication, they are exposed to several threats that influence the reliability of these features. Our aim is to provide a privacy- aware trust-based lightweight security model that works in the VANET environments. The messages sent in the network require trusted software components to ensure that a particular safety message is based on real events and not injected from a malicious vehicle.

Keywords :- RSU,OBU, MANET,GNSS, Inter Vehicular communication.

I. INTRODUCTION

At the present time, road transportation and traffic activities are involved in our important daily life. So new improvements in this area are going on day by day for improving the safety and driving conditions. The number of vehicles on the roads has been rising significantly, leading to increase in traffic-based issues such as accidents and congestion.[1]Vehicular ad hoc network are wireless networks where every one of the vehicles from the nodes of the network. It is for the driver comfort and road safety, the inter-vehicle communication give them. Vehicular specially appointed network is subclass of mobile impromptu networks which gives a distinguished approach to canny transport system.[2]VANET is a subsystem of Mobile Ad Hoc Network (MANET), VANET communicates with the MANET- like technology with the equipment nearby along the road side, and also to communicate between vehicles. Their characteristics are different from that of other networks. Unavailability of road information can create a possibility of accurately stating the position of the vehicle at that time. The vehicle is the node in VANET and the nodes are limited to a particular type of topology while in motion which is the road topology. The nodes can provide power for data processing and information transmission to sustain the functioning of the node.[3][4]

Vehicular Ad Hoc Network (VANET) utilizes cars as a mobile node to create a mobile network. Vehicles act as a mobile node with the corresponding network. The basic aim of VANET is to improve and increase the safety on our roads and road users, comfort of passengers, and also aid the communication between vehicles and roadside equipment. The VANET communication medium is installed on each node (vehicle).VANET is mainly aimed at providing safety related information and traffic management. Safety and traffic management entails real time information and directly affect lives of people travelling on the road.[5] [7]

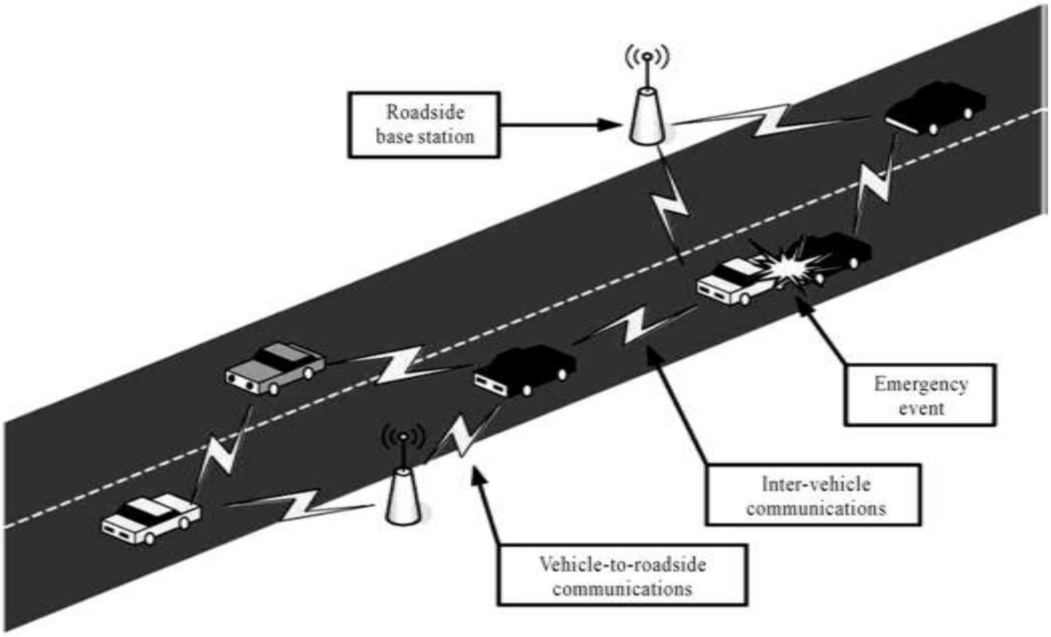
Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Figure1. A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give the drivers the time to react to life-endangering events.[6]

Smart Vehicle

Vehicles which are equipped with multi interface cards and sensors, on board unit and externally. The number of vehicles equipped with on-board wireless devices (e.g., UMTS, IEEE 802.11p, Bluetooth, etc.) and sensors (e.g., radar, ladar, etc.), is increasing for efficient transport and management applications are focused on optimizing flows of vehicles by reducing the time taken to travel and avoiding any traffic congestions. As an instance, the radar present on on-board could be used to sense traffic congestions and automatically slow the vehicle. In another accident warning systems, sensors can be used to determine that a crash may be occurred if air bags were deployed; this kind of information is then relayed via V2I or V2V within the vehicular network.[21]

Different levels of functionality is provided by using number of systems and sensors. The major systems and sensors exploited for intra-vehicle communications we cite: crash sensors, the data recorder, the braking system, the engine control unit, the electronic stability control, the infotainment system, the integrated starter generator, the electronic steering, the tire pressure monitoring system ,the power distribution and connectivity, the lighting system, seat belt sensors , etc. For the brake systems, there are also the antilock brake system and the parking brake system. The parking brake is also referred to as an emergency brake; it controls the rear brakes using a series of steel cables. It allows the vehicle to be stopped when the event of a total brake failure occur. Vehicle-mounted cameras are mainly used to display images on the vehicle console of smart vehicle.[21]

Commonly, a smart vehicle is equipped with the following technologies and devices:

(i) A wireless transceiver for data transmissions among vehicles (V2V) and from vehicles to RSUs (V2I); (ii) A Central Processing Unit (CPU) which implements the applications and communication protocols; (iii) A Global Positioning Service (GPS) receiver for navigation and positioning services;

(iv) An input/output interface for the interaction of human with the system;

(v) Different sensors laying outside and inside the vehicle is used to measure various types of parameters (i.e., acceleration, speed, distance between the neighbouring vehicles, etc.[21]

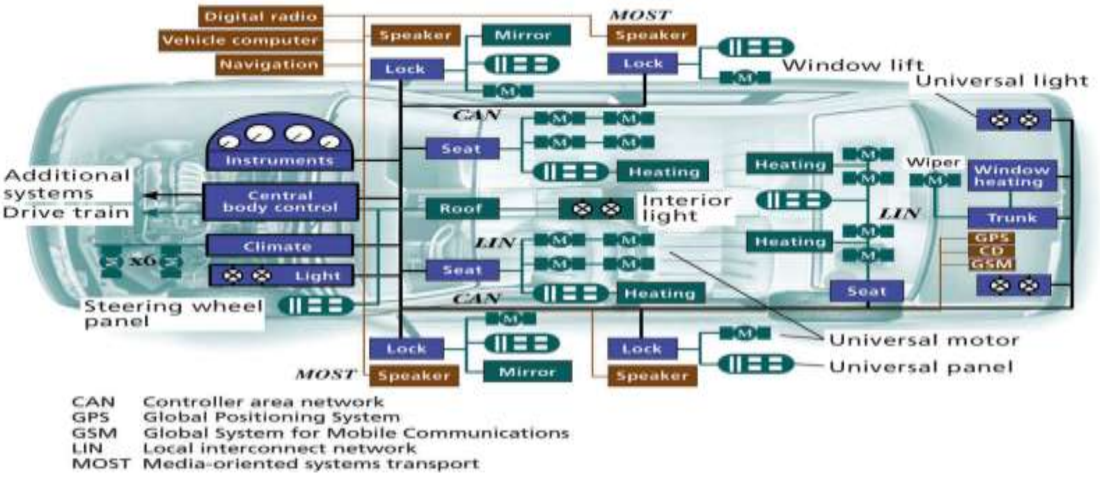

Figure2. Smart Vehicles[21]

The basic idea behind smart vehicles is addressed to safety issues of vehicles, and then by with a proper combination of functionalities like communications, control and computing technologies, it will become possible to assist the driver decisions, and also helps to prevent driver's wrong behaviours' .The control functionality is directly added into smart vehicles for connecting it with the vehicle's electronic equipment.

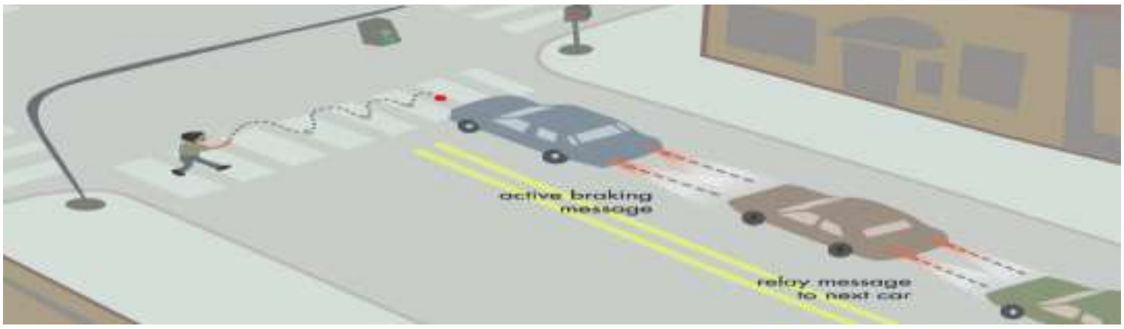

Figure3.Safety application (i.e., brake messaging) by the use of Visible Lighting Communications (VLC)s[21]

Architecture of VANET

According to the IEEE1471-2000 and ISO/IEC42010 [6] architecture standard guidelines, wearable to achieve the VANET system by entities which can be divided into three domains: the mobile domain, the infrastructure domain, and the generic domain As is shown in Figure2, the mobile domain consists of two parts :the vehicle domain and the mobile device domain.[7] The vehicle domain comprises all kinds of vehicles such as cars and buses. The mobile device domain comprises all kinds of portable devices like personal navigation devices and smart phones.Within the infrastructure domain, there are two domains: the roadside infrastructure domain and the central infrastructure domain. The roadside infrastructure domain contains roadside unit entities like traffic lights. The central infrastructure domain contains infrastructure management centers such as traffic management centers (TMCs) and vehicle management centers.[7]

However, the development of VANETs architecture varies from region to region. In the CAR-2-X communication system which is pursued by the CAR-2-CAR communication consortium, the reference architecture is a little different.CAR-2-CAR communication consortium (C2C-CC) is the major driving force for vehicular communication in Europe and published its "manifesto" in 2007. This system architecture comprises three domains: in-vehicle, ad hoc, and infrastructure domain. [3]

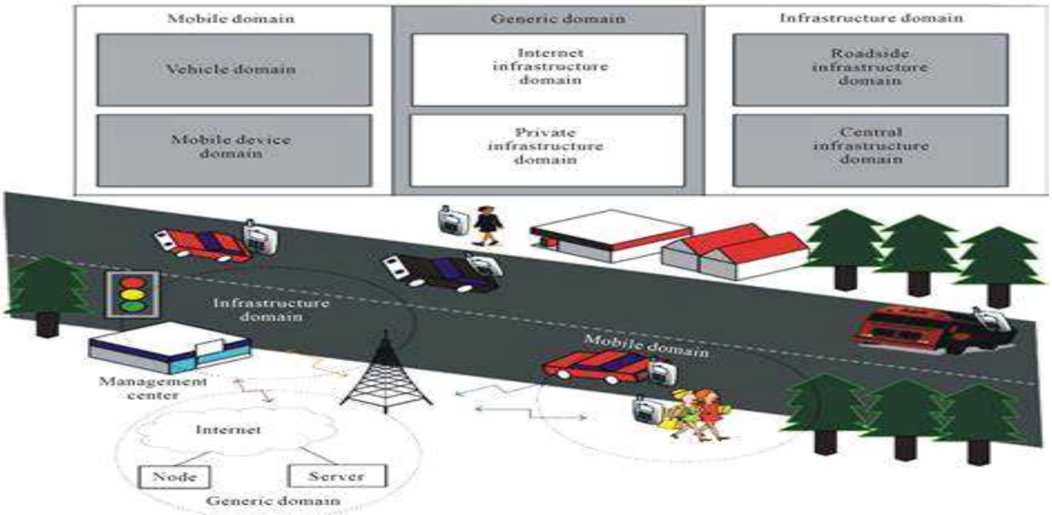

Figure4: VANETs system domains[3]

As shown in Figure3,the in-vehicle domain is composed of an on-board unit (OBU) and one or multiple application units(AUs).The connections between the mare usually wired and sometimes wireless. However, the ad hoc domain is composed of vehicles equipped with OBUs and road side units (RSUs). An OBU can be seen as a mobile node of an ad hoc network and RSU is a static node likewise. An RSU can be connected to the Internet via the gateway; RSUs can communicate with each other directly or via multihop as well. There are two types of infrastructure domain access, RSUs and hotspots (HSs).OBUs may communicate with Internet via RSUs or HSs. In the absence of RSUs and HSs, OBUs can also communicate with each other by using cellular radio networks (GSM ,GPRS, UMTS, WiMAX , and4G).[8]

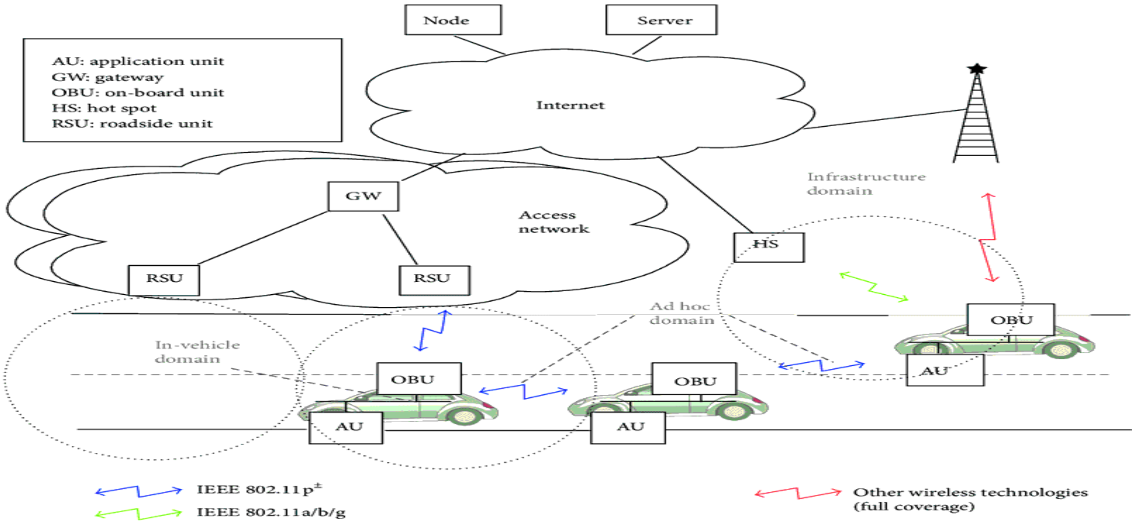

Figure5:C2C-CC reference architecture[9]

Communication in VANETs

The Vehicular Ad hoc network is a subclass of Mobile Ad-Hoc Networks (MANETs) in which communication nodes are above all vehicles and this means that all nodes can move easily within the network coverage and stay connected. Individual node can communicate with each other in single hop or a multi hop. In Vehicular Ad Hoc Networks, communication is divided in to two different categories. [1]

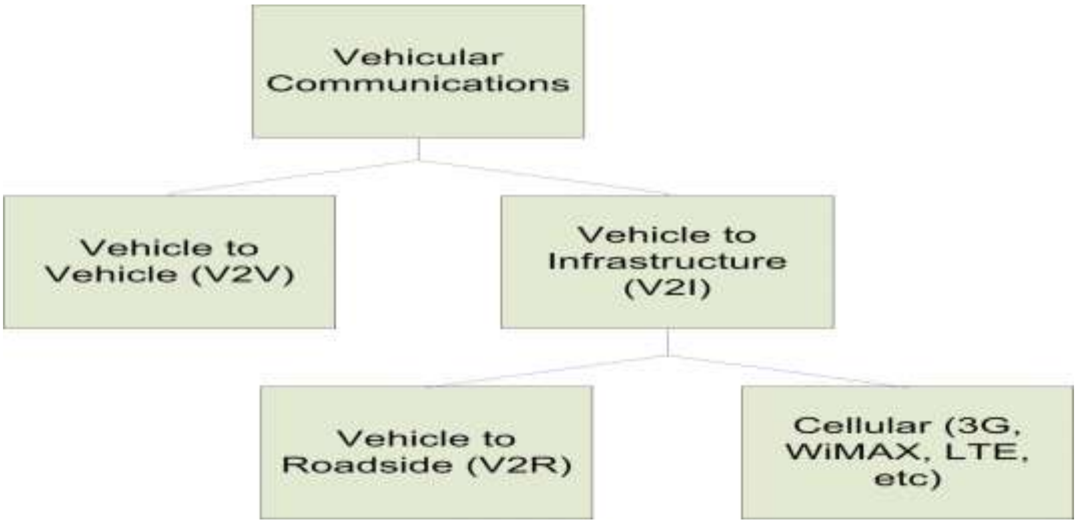
Vehicular Communications
Vehicle to Vehicle (V2V)
Vehicle to Infrastructure (V2I)
Vehicle to Roadside (V2R)
Cellular (3G, WiMAX, LTE, etc)

Figure6. Categories of VANETs Communication [google]

Vehicle-to-vehicle (V2V) communication can provide a data exchange platform for the drivers to share information and warning messages , so as to expand driver assistance. Vehicle-to-road infrastructure (V2I) communication is anotherusefulresearchfieldinVANETs.V2Icommunication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.[10][11]

1.Vehicle To Vehicle Communication: It refers to inter vehicle communication. Vehicles or a group of vehicles connect with one another and communicate like point to point architecture. It proves to be very helpful for cooperative driving.[12],[13]

2.VEHICLE TO INFRASTRUCTURE COMMUNICATION: Number of base stations positioned in close proximity with a fixed infrastructure to the highways is necessary to provide the facility of uploading/downloading of data from/to the vehicles. Each infrastructure access point covers a cluster.[14]

Characteristics of Vehicular Ad Hoc Networks

The characteristics of Vehicular Ad hoc Networks are mainly a combination of wireless medium characteristics. A VANET can be utilized to offer following characteristics in the communication. [15] VANETs has its own separate characteristics given below.

- **High Mobility: -** In VANETs, nodes are frequently moving at high speed. A node positions predict and creating security of node privacy.
- **Unbounded networks size: -** Vehicular network can be built for small city, numerous cities, countries, and for worldwide. So network size in Vehicular ad hoc network is geologically unbounded network size.
- **Anonymity of the support: -** Wireless medium is generally used in data transmission. Transmitter operating on the same frequency band can transmit and hold the band for data transmission.
- **Rapidly changing network of dynamic topology: -**The position of node changes regularly due to high node mobility, dynamic topology in rapidly changing vehicular network changes frequently.
- **Enough Energy: -**The nodes do not have issue of energy and computation power resources. Because we can provide power from battery also.
- **Wireless Communication: -** VANETs is intended for wireless surroundings. All nodes are connected and conversation their information through the wireless communication. Hence, some security can be implemented over it.
- **Availability of the transmission medium: -** The transmission medium of Vehicular Ad hoc Network is air. We can transmit the data wirelessly but in wireless transmission the major concern is security advantages in Inter Vehicular. Communication (IVC), becomes the starting point of some security matters.
- **Time Critical: -** The information in vehicular ad hoc network should be delivered to the node

with in real limit so a choice will be created by the nodes and perform action consequently.

- **Frequent disconnections:** -The rapidly changed network topology and high mobility of nodes along with another different conditions such as weather, climate mass of traffic perform disconnections of vehicles.

Vehicular Ad Hoc Network Applications
VANETs will play important role will be applications classified into two general types.

- **Safety Related Applications**

There are some applications used to increase for safety. There applications will be categorized in subsequent manner.
1.**Collision Avoidance:** If drivers were provided a warning a second before collisions so that seventy percentage accidents will be avoided [17]. If driver come to be warning messages on time, collisions will be avoided.
2.**Cooperative Driving:** Driver will send signal for traffic related warnings like lane amendment warnings, curve speed warnings, etc. There signal will cooperate the motive force for associate interrupts and safe driving.
3.**Traffic optimization:** Traffics will optimize by way of utilization causation signal like accidents, traffic jams etc. towards the vehicles so that they will be opted for their alternative paths and may save the time also.

- **User Based Applications**

- **Peer to peer applications:** These applications are helpful to produce facilities like sharing movies, music, etc. amongst the vehicle within the networks.
- **Internets Connectivity:** Individual users always need to connects with the net every time. Therefore, Vehicular ad hoc network offers the constant connect to the internet.
- **Other type of services:** VANETs may be used in alternative users primarily based on applications like all payments facilities to gather the toll taxes, to find the nearest fuel stations, eating place such as restaurant etc.
- **Driver-oriented applications:** To assist the drivers on the road if it receives data concerning the risks ahead, traffic, etc[16]
- **Vehicle-oriented applications:** In this application, permitting to provide data to their vehicles to extend automation and improve road safety.
- **Applications for road safety:** It's mainly enhance travel safety and scale back road accidents, VANET applications offer collisions shunning and road work, detection of mobile and stuck obstacles and dissemination of weather data. During this class of applications, we find e.g.: Slow/Stop Vehicle Advisor, Emergency Electronic stoplight. Post-Crash Notification, "Road Hazard Management Notification" collaborate Collision Warning.
- **Applications for driver assistance:** They aim to facilitate driving and assist the motive force in specific things like passing vehicles, bar of channel outputs, detection and warning of holdup, warning of potential traffic jams, etc. During this class we discover e.g.: engorged road notification, parking available notification, toll plaza collections.
- **Applications of passenger's comfort:** These applications area unit for the comfort of the motive force and passengers, they basically give services like mobile web access, messaging, discussion between vehicles, cooperative network games, etc. within the remainder of this section we have a tendency to limit ourselves to the outline of some services and samples of applications of vehicle-to- vehicle communication systems.

Various Challenges and Issues in VANETs
VANET differentiates a unique network although the characteristics. However, deployment of the VANETs to some characteristics executes to some challenges. These are may be categorized into subsequent classes.[15]

- **Technical Challenges**

The technical challenges cope up with the technical obstacles that ought to be resolved before the preparation of VANET. Some challenges areas are given below.

- **Network Management:** In VANETs channel condition modification and topology changes frequently due to high mobility. we can't use tree like structures due to freely change in topology.
- **Congestion and collision control:** In rush hour, the traffic is more in urban area as compared to the urban area.[10]
- **Environmental Impact:** The electromagnetic (EM) waves are used for vehicular ad hoc network communication. EM waves are highly effected due to atmosphere. Hence, to deploy the VANET the environmental effect needs to be measured.
- **MAC Design:** Shared medium is used to speak in VANET therefore the medium access control is that the key issue. Various approaches used in VANET are TDMA, SDMA, and CSMA etc.

- **Security:** The purpose of VANET is to provide the road safety application. Hence messages should be secure.

B. Social and Economic Challenges

Social and economy also create challenges in VANET. It's hard to design such a system which tells about traffic rule violation because this kind of system are rejected by user but the warning message of police trap is appreciated by them. Therefore, to encourage the manufacturers to deploy Vehicular ad hoc network can get very little incentives.

- **Security Challenge of VANETs**
- Security issues in VANETs

Security got less attention to this point. The packets contain life critical information in VANET hence it is necessary to made send packets so it is not changed by the attacker. In VANETs security [19] is major concern as compare to general communication. The difficult to implementation to makes size of network, high mobility, geographically relevancy etc.

- **Security Challenges in VANETs**

The various security challenges are planning of VANET design, security protocols, scientific discipline formula, cryptographic algorithm solution etc. The subsequent list presents some security challenges.

- **Real time Constraint:** Vehicular ad hoc network is time critical wherever safety connected message ought to be delivered with 100ms transmission delay. Therefore, to realize real time constraint, fastest cryptographic algorithmic rule ought to be used. Message and entity authentication should be tired time.
- **Data Consistency Liability:** In VANETs even verification of node will perform malicious activities which will cause accidents or disturb the network. Therefore, a mechanism ought to be designed to avoid this inconsistency. Correlation among the received information from totally different node on explicit data might avoid this sort of inconsistency.
- **Low tolerance for error:** The basis of probability is design some protocols in VANET. In VANETs, life critical information is used and action performed for very short time. In probabilistic formula occurrence of small error might cause problem.
- **Key Distribution:** VANETs is a key dependent safety mechanism. Every encrypted message is decrypted at receiver side either with same key or completely different key. [20] Every manufacturer uses different security mechanism for installation of keys and in case of public key infrastructure trust on CA become a big issue. Therefore, distribution of keys among vehicles may be a major challenge in planning a security protocols.
- **High Mobility:** The mobility is a major issue because the speed of the vehicles is unpredictable.

II. CONCLUSIONS

VANET is an area of research that holds promising future and for vehicular users. However, it has its own challenges in the security prospect. VANET aims at reducing the accidents on our roads and increasing the flow of information among vehicle and the road users. The unique nature of VANET springs up issues like illegal tracking and jamming of the network. In this paper, we introduced VANET, its architecture, components, communication pattern and issues in its security.

REFERENCES

[1]. J. M. de Fuentes, A. I. G. Tablas and A. Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, (2010).

[2]. Kuldeep Kumar and Sandeep Kumar Arora, “Review of Vehicular Ad Hoc Network Security”.

[3]. Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. International Journal of Communications, Network and System Sciences, 8, 19-28.

[4]. Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. Transactions on Networks & Communications, Society for Science and Education, United Kingdom, 2, 1-6.

[5]. Stampoulis, Antonios, and Zheng Chai, ‘A Survey of Security in Vehicular Networks’, Project CPSC, 2007.

[6]. D. Emery and R. Hilliard, “Every architecture description needs a framework: expressing architecture frameworks using ISO/IEC 42010,” in Proceedings of the Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture (WICSA/ECSA ’09), pp. 31–40, Cambridge,UK,September2009.

[7]. T.Kosch,C.Schroth,M.Strassberger,andM.Bechler,AutomotiveInternetworking,Wiey,New York,NY,USA,2012.

[8]. H. Moustafa and Y. Zhang, Vehicular Networks: Techniques, Standards,andApplications,CRCPress,Boca Raton,Fla,USA, 2009.

[9]. CAR 2 CAR Communication Consortium Manifesto, 2007, http://elib.dlr.de/48380/1/C2C-CC manifesto v1.1.pdf.

[10]. R. S. Raw, M. Kumar and N. Singh, "Security Challenges, Issues and their Solutions for VANET", vol. 5, no. 2, (2013), pp. 1-6

[11]. AL-Hashimi, Haider Noori, Kamalrulnizam Abu Bakar, and Kayhan Zrar Ghafoor, 'Inter-domain proxy mobile ipv6 based vehicular network', Network Protocols and Algorithms, vol. 2, issue 4, pp. 1-15, 2011.

[12]. Lupi, Francesco, Veronica Palma, and Anna Maria Vegni, 'Performance Evaluation of Broadcast Data Dissemination over VANETs,' A Case Study in the City of Rome, pp. 1-4, 2012.

[13]. Benslimane, Abderrahim, Tarik Taleb, and Rajarajan Sivaraj,'Dynamic clustering-based adaptive mobile gateway management in integrated VANET—3G Heterogeneous Wireless Networks', Selected Areas in Communications, vol. 29, Issue 3, pp. 559-570, 2011.

[14]. Majeed, Muhammad Nadeem,' Vehicular Ad-hoc networks history and future development arenas', nternational Journal of Information Technology and Electrical Engineering, vol. 2, Issue 2, pp. 25-29, 2013.

[15]. A. Hamieh, J. Ben-Othman and L. Mokdad, "Detection of radio interference attacks in VANET", Global Telecommunications Conference, (2009), pp. 1–5.

[16]. X. Lin, "Security in Vehicular Ad Hoc Network", IEEE communications magazine, (2008), pp. 88-95

[17]. R. S. Raw, M. Kumar and N. Singh, "Security Challenges, Issues and their Solutions for VANET", vol. 5, no. 2, (2013), pp. 1-6.

[18]. M. Raya, "The Security of Vehicular Ad Hoc Networks", SASN'05, Alexandria, Verginia, USA, (2005), pp. 11-21.

[19]. A. Burg, "Ad hoc network pecific attacks", Seminar Ad hoc Networking: Concepts, Applications, and Security, 2003, Technische Universitat Munchen, (2003)

[20]. M. N. Mejri, J. B. Othman, M. Hamdib, "Survey on VANET security challenges and possible cryptographic solutions", (2014).

[21]. "Location Identification and Vehicle Tracking using VANET (VETRAC)" given by Arunkumar Thangavelu, K. Bhuvaneswari, K. Kumar, K. SenthilKumarl and S.N. Sivanandamof MIT Campus, Anna University, Chennai.