Vehicular Ad hoc Networks and its Applications in Diversified Fields

Raju Barskar
Department of Computer Science and Engineering
Maulana Azad National Institute of Technology
Bhopal, M.P. 462051

Meenu Chawla
Department of Computer Science and Engineering
Maulana Azad National Institute of Technology
Bhopal, M.P.462051

ABSTRACT
Vehicular adhoc networks (VANETs) are the important subset of mobile ad-hoc network (MANET) application which uses set of smart vehicles on road in the form of mobile nodes. The VANET provides the benefits of road safety and travellers comfort while protecting driver's privacy from different types of attacks perpetrated by adversaries. In the forthcoming, it is usual that have vehicles which gradually increases become intelligent systems which will be equipped with radio communications interfaces. Therefore, vehicular networks be able to be formed and are usually called as VANETs (Vehicular Ad hoc NETworks). This paper presents a survey of an all aspects of modern review of VANET architecture, communication among vehicles, presenting outlet characteristics, security, challenges and addressing attackers are classified according to scope, nature, and behaviour of attacks and also discuss various categories of applications in VANETs, this paper also includes most appropriate security attacks in VANET.

General Terms
Performance, Reliability, Security confidentiality and Authentication

Keywords
Vehicular Ad hoc Network (VANET), On Road Unit (OBU), Application Unit (AU), Road Side Unit (RSU), Dedicated Short Range Communication (DSRC) and security attacks

1. INTRODUCTION
Vehicular Ad Hoc Networks (**VANETs**) are actually is the subset of mobile adhoc networks (MANETs).The communication between moving vehicles with each other and with the help of infrastructure a dedicated short range communication (DSRC) is used. The Dedicated Short Range Communication (DSRC), a band of 75 MHz in 5.9 GHz has been allocated by the Federal Communication Commission (FCC) [1, 2].

The Wireless Access in Vehicular Environments (WAVE) standard is expressed in IEEE 1609 Family. This standard contains standardized set of services, architecture, complementary and various interfaces are used for protecting vehicle communication (V2V) or communicate with fixed equipment next to the road, expressed to as road side unit (RSU) forming vehicle to infrastructure communication (V2I) [2].This category of communication are used to permit vehicles for distribute different types of information related to any instance, such as safety information is worn for accident prevention, post-accident investigation or traffic jams. The other category of information is expert to disseminate such as traveller related information that is measured by non-safety information [3]. The main cause for sharing and distributing these categories of information is warn drivers regarding unexpected accidents by using safety messages and save people's life or to furnish passengers with comfort journeys.

This is broad area of research attracts researchers for different fields to expand VANET applications, protocols and simulation tools. Communication and networking aspects of this technology and addressed the security and privacy issues have been introduced by Hartenstein and Laberteaux . In 2007, focus on the routing protocols of VANET and their requirements to complete better communication time with less consumption of network bandwidth and it also investigate the categories of routing protocols in VANET and the idea behind each of them is discussed by Li and Wang. In this paper, we present a key document which can make available detailed information to researchers accordingly as to appreciate the main aspects and challenges related to VANET. It covers various issues like network architecture, communication domains, challenges, applications and simulation tools in VANET[4].

2. ARCHITECTURE OF VANET
In the Vehicular communication systems the communication among vehicles and RSU is achieved by using a wireless medium is popularly known as WAVE. This scheme of communication provides a broad range of information to drivers and travellers and intelligent to safety applications to improve road safety and it also provide a secure driving [5].

The VANET architecture consist of the most indispensable system components i.e. application unit (AU), On Board Unit (OBU) and Road Side Unit(RSU). Usually, the RSU hosts an application that provides services and the OBU is a peer device. The application possibly will reside in the RSU or in the OBU. The device to facilitate hosts application is called as the provider and the device using the application is known as the user. Each vehicle is equipped with an OBU and a set of sensors to accumulate and process the information then send it on as a message to other vehicles or RSUs by the wireless medium, it also carries a single or multiple AU that use the applications provided by the provider using OBU connection capabilities. The RSU be capable of connect to the internet or to another server so as to allows AU's from multiple vehicles to join in the direction of the Internet [5, 6].

2.1 On Board Unit (OBU)
A wave device which is commonly known as On Board Unit(OBU), usually mounted on-board a vehicle used for exchanging information with RSUs or with other OBUs. The OBU are comprises of a resource command processor (RCP), and resources contain a read/write memory used to store up and recover information, a user interface, a specialized

interface to connect to other OBUs and a network device for short range wireless communication based on IEEE 802.11p radio technology. It also comprises of another network device for non-safety applications based on other radio technologies such as IEEE 802.11a/b/g/n. The OBU connects to the RSU or to other OBUs all the way through a wireless link based on the IEEE 802.11p radio frequency channel, and is responsible for the communications with other OBUs or with RSUs. It can also provides a communication services to the AU and forwards data on behalf of other OBUs on the network. The main functions of the OBU in VANET are wireless radio access, ad-hoc and geographical routing, network congestion control, reliable message transfer and data security [6].

2.2 Application Unit (AU)

The Application Unit (AU) is the device capable of within the vehicle which uses the applications provided by the provider using the communication capabilities of the OBU. The AU be able to a dedicated device for safety applications or a normal device such as personal digital assistant (PDA).The AU can be connected to the OBU through a wired or wireless connection and can reside with the OBU in a single physical unit. The dissimilarity between the AU and the OBU is logical. The AU communicates with the network only by the use of the OBU which takes task for all mobility and networking functions.

2.3 Road Side Unit (RSU)

The Road Side Unit(RSU) is a wave device normally fixed along the road side or in dedicated locations such as at the junctions or near parking spaces. The RSU is equipped with one network device for a DSRC based on IEEE 802.11p radio technology, and be able to be equipped with other network devices so as to be used for the purpose of communication within the infrastructural network (Figs. 2-4) [6,7].

The main functions and procedures associated with the RSU are given below:

1. To extend the communication range of the ad hoc network for redistributing the information to other OBUs and by transfer the information to other RSUs in order to forward it to other OBUs.

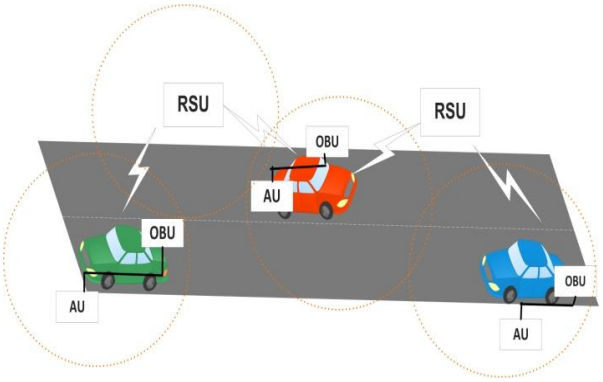

Fig.1: RSU extend the range of the ad hoc network by forward the data of OBUs

2. Running safety applications such as a low bridge warning, accident warning or work zone, by means of use of infrastructure to vehicle communication (I2V) and acting as an information source.

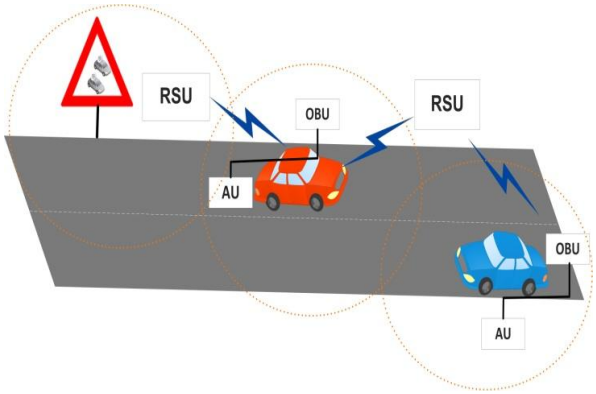

Fig.2: RSU work as information source (running safety applications)

3. Providing Internet connectivity to OBUs.

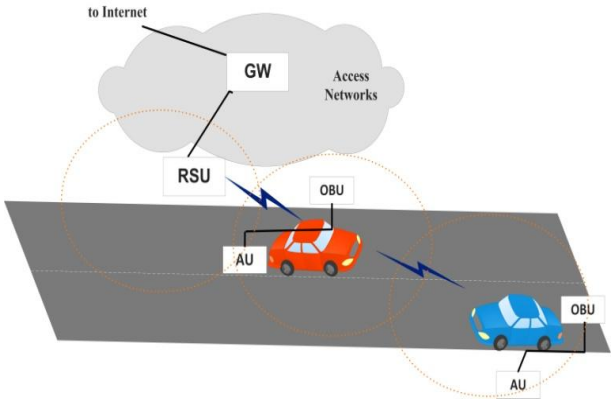

Fig.3. RSU provides internet connectivity to the OBUs

3. COMMUNICATION AMONG VEHICLES

The communication among vehicles and the RSU and the infrastructure are categorized into three types of domains:

3.1 Inter-vehicle Communication

In inter-vehicle communication configuration, it uses multi-hop, multicast or broadcast to transmit traffic associated information over multiple hops to a assembly of receivers. In intelligent transportation systems, vehicles must be disturbed with activity on the road ahead and not behind [8]. There are two types of message forwarding are exist in inter-vehicle communications: *naïve broadcasting* and *intelligent broadcasting*.

In *naïve broadcasting*, vehicles send broadcast messages periodically in regular intervals. Based on receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its personal broadcast message to vehicles behind it. It ensures so as to all enabled vehicles moving in the forward direction to get all broadcast messages. The boundaries of the naïve broadcasting method is to large numbers of broadcast messages are generated, as a outcome, increasing the risk of message collision resulting in lower message delivery rates and increased delivery times.

Intelligent broadcasting is used to understood acknowledgement addresses the problems inbuilt in naïve broadcasting by preventive the number of messages that broadcast for a well-known tragedy event. Event-detecting vehicle are receives same messages from behind it, then it

assume that at least one of the vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be dependable for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only [3].In-vehicle domain: Vehicle domain comprises of on Broad Unit(OBU) and one or multiple Application Unit(AUs). The connection type could be wired or wireless using WUSB or UWB. An On Board Unit and Application Unit are attached in a single device in vehicles. The OBU provides a communication link to the AU for execute one or more of a set of applications provided by the user with the use of the communication capabilities of the OBU [7]

The main applications of IVC, as summarized by [8], can be roughly categorized into three classes:

•Information and warning functions: Dissemination of road information (including incidents, congestion, surface condition, etc.) to vehicles distant from the subjected site.

•Communication-based longitudinal control: Exploiting the "look-through" capability of IVC to help avoiding accidents and platooning vehicles for improving road capacity.

•Co-operative Assistance Systems: Coordinating vehicles at critical points such as blind crossings (a crossing without light control) and highway entries.

3.2 Vehicle-to-roadside communication

The vehicle-to-roadside communication configuration is discussed in Fig.2.
In vehicular ad hoc networks, vehicular to road side communication in important part of communication. This communication consist single hop broadcast system, RSU sends broadcast message to all other participated vehicle in the surrounding area. In this communication used high bandwidth link for communication between RSUs and vehicles. The range of high bandwidth link is nearby road side unit an every kilometer or less. So that it is used to enabling high data rate for communication and maintain in every traffic scenarios.

For example, when a broadcast message is speed limits, then RSU will generate message for a suitable speed limit according to its internal timetable and traffic conditions. The roadside unit will regularly broadcast a message that containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the surrounding area. If a vehicle violates the required speed limit, a broadcast will be delivered to the vehicle in the outward appearance of an auditory or visual warning, requesting that the driver decrease his speed [8].

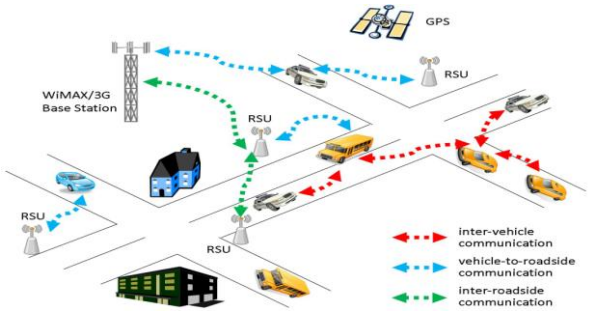

Fig. : - 4 Types of Vehicle Communication

3.3 Inter-Road Side Communication

The working of routing-based communication configuration as shown in Fig. 3, it is a multi-hop unicast that a message which is propagated in a multi-hop fashion until the vehicle carrying the desired data is attain. When the query is received throughout a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.

4. VANET CHARACTERISTICS

The main characteristics of VANET when it compared with other types of MANETs, the important characteristics of VANET are as follows [4]:

4.1 Predictable Mobility

VANET be different from other types of mobile ad hoc networks that nodes move in a random way, as vehicles are constrained by road topology and layout and with the requirement to obey road signs and traffic lights and to react to other moving vehicles principal to predictability in term of their mobility [4, 5].

4.2 Providing Road Safety, Enhancing Traffic Efficiency And Travellers Comfort

VANET provides the direct communications facility among moving vehicles, therefore it allows a set of applications and demanding direct communication between nodes towards applied over the network. These types of applications are capable to provide warning messages about accidents to drivers travelling in the same direction, or regarding the require for sudden hard breaking; leading the driver to construct a broader picture of the road ahead. Moreover, additional kinds of applications could be applied by the use of this type of network in order to recover passenger comfort and traffic efficiency by disseminating information about weather, traffic flow and point of interest information (gas station, shopping malls and fast food) [4].

4.3 No Requirement of Power Constraints

The power in VANET is not a significant challenge, because vehicles have the capability to provide continuous power to the OBU by the use of the long life battery.

4.4 Variable Network Density

The network density in VANET is varies according to the traffic density, that could be very high in the case of a traffic jam, or very low, as in suburban traffic.

4.5 Fast Changes In Network Topology

High speeds characterize moving vehicles, mostly at the highway leading to fast changes in network topology. In adding together, driver behaviour is exaggerated by the requirement for reacting to the data received from the network, which causes changes in the network topology. The life time of the link among vehicles is affected by the radio communication range and the direction of the vehicles, hence increasing the radio communication range leads to an increase in the life time of the link. The life time of the link between vehicles moving in opposite directions is very short lived compared with case in which vehicles move in the same direction. The fast changes in link connectivity cause the effective network diameter to be small, while many paths are disconnected before they can be utilized [4,6].

4.6 Large Scale Network

The network scale could be large in dense urban areas like the city centre, highways and at the entrance of the big cities [6].

4.7 High Computational Capability

In VANET the vehicles are represented by nodes, that they can be equipped with a adequate number of sensors and computational resources; like processors, a large memory capacity, advanced antenna technology and global position system (GPS). These resources raise the computational capacity of the node, which help obtaining reliable wireless communication and acquire accurate information regarding its current position, speed and direction [7].

5. SECURITY CHALLENGES IN VANET

VANET security is diverse from that of wireless and wired networks as of its unique characteristics of mobility constraints, infrastructure-less framework, and short duration of link between nodes. Therefore, it is necessary to develop security algorithms which help to guarantee the correct and safe operation of VANETs [10].

The main Cryptographic primitives to solve many security issues in VANETs are as follows:

- **Availability**

Availability guarantees that network be required to available at all times and useful information is shared in order to send and receive messages at any functional time. The another availability problem possibly will be caused by selfish nodes that are available in network and do not provide their services for the benefit of other nodes in order to save their own resources, battery power and CPU cycle [10]. This major security requirement for VANETs, that main purpose is to make sure the users' lives, is a significant target for most of the attackers. The most famous examples are the DoS and jamming attacks.

- **Confidentiality**

Confidentiality is a major security requirement challenges for VANETs communications; it provide to ensure data are only read/write and understand by authorized users. The entities (vehicle or infrastructure), outsiders are not capable to differentiate confidential information among the entities during communication, which pertains to each entity. It must be achieved by message encryption therefore; it can keep the confidential information of each driver like custom profiles and users' identity.

In VANET, message confidentiality based on the specific application scenario. For instance, sensitive information which is related to safety-related messages. The information collected in the absence of a confidentiality mechanism may manipulate the privacy of individuals, knowing that it is not easy to detect this kind of attack, while it is virtually passive and user currently is not aware of the collection. However, in the case where the exchanged messages do not contain any sensitive information [11].

- **Integrity**

Integrity ensures that a message was not transformed between the moment it was sent and received as the received message must match the message sent. The receiver will then be able to corroborate the sender's identity during the transaction. Integrity protects against the unauthorized creation, destruction or alteration of data. If a corrupted message is accepted, the integrity property is violated and the protocol would be deemed faulty. To achieve integrity, the system must prevent attackers from altering messages since the contents of messages must be trusted [12]. Thus, the attacker injects it again in the network packets previously received.

- **Authenticity**

Authenticity is a foremost challenge of VANETs security. All active stations in the network should authenticate prior to accessing available services. Any violation or attack involving the process of identification or authentication exposes the entire network to serious consequences. The main purpose of authenticity in a vehicular network is to protect the authentic nodes from outside or inside attackers infiltrating the network using a falsified identity. The significance of identification–authentication process comes from the fact which is frequently used whenever a vehicle needs to join the network or a service. There are numerous types of attacks in this category. This is one of the main requirements for any system. In VANETs, it is very important to have certain information concerning the transmitting node, such as its identification, and that of the message sender as well as its property and location. It is important to authenticate all users and messages which transit through the network. Authentication controls the authorization levels of vehicles. In VANETs, authentication prevents Sybil attacks by assigning a specific identity to each vehicle [13].

- **Non-Repudiation**

Non-repudiation is defined as one of the entities that involved in a communication deny for participate impracticality in all or part of a communication event. The main objective of non-repudiation consists of collecting, making available, maintaining, and validating undeniable evidence about a claimed event or an action in order to resolve disputes about the occurrence or non-occurrence of that event or action. Non-repudiation depends on authentication, but it generates solid proof as the system can identify the attackers who cannot deny their crimes. Violators or misbehaving users cannot deny their actions [13].

6. CONCLUSION

This paper is consist of a all aspects of state-of-the-art review of VANET architecture, communication among vehicles, presenting outlet characteristics, security, challenges and addressing attackers can be classified according to scope, nature, and behaviour of attacks. Then, threats, privacy and security solutions convergence of telecommunications, computing, and services that are enabling the deployment of different kinds of VANET technologies. In addition, we also discuss some security issues, VANETs characteristics and related applications, VANET architectures components, various types of attacks on VANET and certain architectures and solutions suggested in the literature have been pointed out. Through this extensive literature survey, concluded that effective and efficient communication between vehicles should be more secure, efficient, in which infrastructure networks should be considered further in designing VANET in future.

7. REFERENCES

[1] Uzcategui, R., and Guillermo Acosta-Marum. "WAVE: a tutorial." Communications Magazine, IEEE 47, no. 5 (2009): 126-133.

[2] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, 2011.

[3] Kiess, Wolfgang, Jedrzej Rybicki, and Martin Mauve. "On the nature of inter-vehicle communication." In Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference, pp. 1-10. VDE, 2007.

[4] Al-Sultan, Saif, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan. "A comprehensive survey on vehicular Ad Hoc network." Journal of network and computer applications 37, pp.380-392, 2014.

[5] Hartenstein, Hannes, and Kenneth Laberteaux, eds. VANET vehicular applications and inter-networking technologies. Vol. 1. John Wiley & Sons, 2009.

[6] Mohammad, Sajjad Akbar, Asim Rasheed, and Amir Qayyum. "VANET architectures and protocol stacks: a survey." In Communication technologies for vehicles, pp. 95-105. Springer Berlin Heidelberg, 2011.

[7] F. D. da Cunha, A. Boukerche, L. Villas, V. Aline, and A. A. F. Loureiro, "Data communication in VANETs: a survey, challenges and applications," Research Report RR-8498, Version 2, INRIA, 2014, https://hal.inria.fr/hal-00981126/PDF/RR-8498.pdf.

[8] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems 50, no. 4 (2012): 217-241.

[9] Olariu, Stephan, and Michele C. Weigle, eds. Vehicular networks: from theory to practice. Crc Press, 2009.

[10] Caballero-Gil, Pino, "Security Issues in Vehicular Ad Hoc Networks", INTECH Open Access Publisher, 2011.

[11] M. Raya, J.-P. Hubaux, "Securing vehicular ad hoc networks" Journal Comput. Security, 15 (1), pp. 39–68, 2007.

[12] Engoulou, Richard Gilles, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. "VANET security surveys." Computer Communications 44, pp. 1-13, 2014.

[13] Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions." Vehicular Communications 1, no. 2, pp.53-66, 2014.