International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A STUDY ON APPLICATIONS AND CHALLENGES IN VEHICULAR AD-HOC NETWORKS (VANETs)

Ch. V. Raghavendran[1], G. Naga Satish[2], P. Suresh Varma[3]

[1]*Professor, Holy Mary Institute of Technology & Science, Bogaram, Telangana, (India)*

[2]*Associate Professor, BVRIT HYDERABAD College of Engineering for Women, Hyderabad, (India)*

[3]*Professor, College of Engineering, Adikavi Nannaya University, Rajamahendravaram, (India)*

ABSTRACT

Over the last few years advances in wireless networks have led to a new type of networks called Vehicular Ad-Hoc Networks (VANETs). These are distributed self organizing networks formed between moving vehicles equipped with wireless communication devices. These emerging networks have the potential to improve the efficiency of highways and improve traffic management. VANETs provide us with the infrastructure for developing new systems to enhance road safety. Along with the benefits, there arise a large number of challenges in VANET such as provisioning of QoS, high mobility, high connectivity, bandwidth, security to vehicle and individual privacy. A vehicular network consists of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V) communications supported by wireless access technologies such as IEEE 802.11p. This paper presents an overview on applications, challenges, advances and potentials of VANETs. Main envisions and findings of this study are that an efficient and robust VANET is one that has several new applications, which will improve traffic management and safety.

Keywords:Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), RFID, Wireless Access in Vehicular Environment (WAVE), Intelligent Transport System (ITS)

I. INTRODUCTION

In recent days, Vehicular Ad-Hoc Network (VANET) applications have an immense interest by the research community due to the important role that these networks can play. A VANET makes it possible to have communication between vehicles and between vehicles and infrastructure. VANET incorporates the capabilities of new generation wireless networks into vehicle [1]. These types of networks are highly dynamic in nature [2]. VANETS can autonomously organize networks without infrastructure and lack of guaranteed connectivity [3]. The study of VANETs has become an important research topic in the area of wireless networking and in the automotive industry. The goal of VANET research is to develop a vehicular communication system to enable quick and cost-efficient distribution of data for the benefit of passenger's security and comfort. Now VANETs have been established as reliable networks that vehicles use for communication purpose on highways or urban environments.

These types of networks are developed as part of the Intelligent Transportation Systems (ITS) to improve to the performance of transportation system. The integration of the embedded computers, sensing devices, navigation

systems (GPS), digital maps, and the wireless communication devices along with intelligent algorithms will help to develop applications to improve road safety for the ITS. The up to date information provided by the integration of all these systems helps passengers to get real-time information about road conditions allowing them to react on time.

Vehicular Ad-Hoc Networks (VANETs) are special type of Mobile ad Hoc Networks (MANETs), where wireless-equipped vehicles form a network spontaneously while traveling along the road. Direct wireless transmission from vehicle to vehicle makes it possible to communicate even where there is no telecommunication infrastructure such as the base stations of cellular phone systems or the access points of wireless dedicated access networks, needed in the previous Intelligent Transportation Systems (ITS) [4,5].

VANETs are defined as distributed, self organizing communication networks built up by moving vehicles, and are thus characterized by very high node mobility and limited degrees of freedom in the mobility patterns [6]. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. Vehicles equipped with wireless communication technologies and acting like computers will be on our roads and it will revolutionize the traveling. The concept of VANETs is: by incorporating the wireless communication and data sharing capabilities, the vehicles can be turned into a network, providing similar services to the ones we are used to in our office or home networks.

II. VANET ARCHITECTURE

VANET architecture mainly consists of (i) Vehicles (V) with an On Board Unit (OBU), (ii) Road Side Unit (RSU) and (iii) Infrastructure Domain (I). Communication is conducted mainly by using wireless standards (e.g. IEEE 802.11p). RSU acts like a router and its range is higher than that of vehicles range. The vehicles are installed with a Global Positioning System (GPS) for knowing its own position as well as for tracking other vehicles. The vehicles have an Electronic license plate (ELP) for its identification. In addition to these, Radio detection and ranging (RADAR)/light amplification by simulated amplification of radiation (LASER) technologies are also used to know the position of other vehicles. A Certification Authority (CA) exists in the architecture for providing services (e.g. security and TCP/IP) and applications. The following Fig. 1 shows the architecture of VANET.

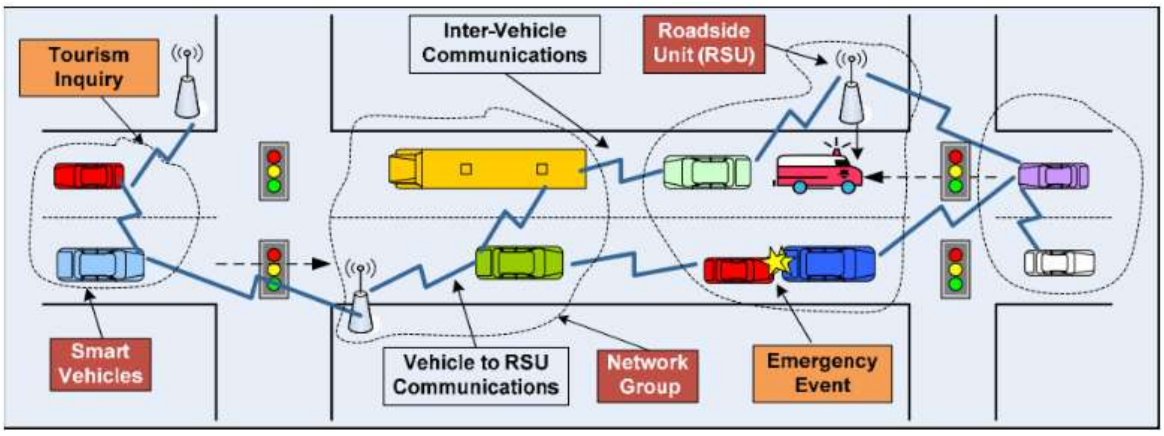

Fig.1. A basic architecture of VANETs [7]

In principal, there is no fixed architecture or topology that a VANET must follow. However, a general VANET consists of moving vehicles communicating with each other as well as with some nearby RSU. In VANET there are three types of possible communication scenarios for vehicles. First is vehicle to vehicle (V2V), second is vehicle to infrastructure/ infrastructure to vehicle (V2I/I2V) and third is hybrid.

In V2V communication, vehicles directly communicate with each other and there is no need of any RSU. This can be classified as Ad-hoc architecture. V2V communication uses multi-hop communication (multicasting/broadcasting) for transmission of data. In V2V, a vehicle can accept broadcast and exchange helpful traffic news i.e., traffic conditions and road accidents in particular area or with other vehicles. In V2I communication, vehicles communicate with each other through some RSU. This architecture may resemble wireless local area networks (WLAN). In this communication type, the information will be broadcasted between the nodes (i.e vehicle) and the infrastructure (said as ITS), to discuss about valuable information such as road conditions and safety events which have been taken into account. In this V2I, a vehicle (node) launches a connection between RSU and contact with external networks which is Internet. In third possibility, some of the vehicles can communicate with each other directly while others may need some RSU to communicate. This can be referred as hybrid scenario [8]. Fig. 2 shows these three possibilities.

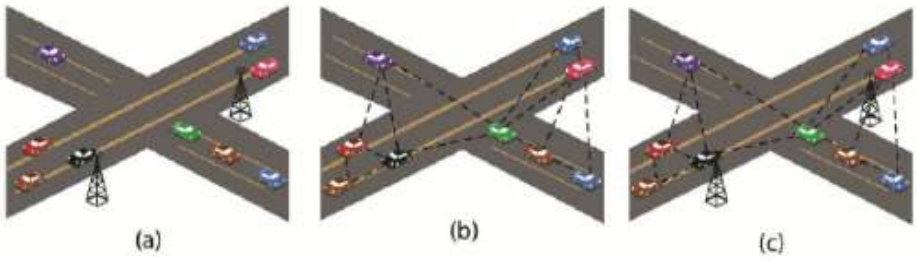

Fig. 2 Three possible communications in VANET

III. VANET STANDARDS

There are many standards used in VANET such as Dedicated Short Range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE). DSRC [9, 10] is a standard developed for a short to medium range communication service used for both V2V 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 [11]. DSRC, WAVE and IEEE 802.11p are the standards used to select the entire protocol stack to trade with VANETs.

3.1 DSRC (DEDICATED SHORT RANGE COMMUNICATION)

The DSRC band is regulated by European Telecommunications Standard Institute (ETSI) using only the channels 180 of Control Channel (CCH) and 172, 174, 176, 178 of Service Channel (SCH). The FCC (Frequency Communication Commission) characterizes the highest interoperability and the intention of standardization 0f frequencies in which the VANET works. The FCC attributed the band 5850 to 5925 GHz. This band will be said as Dedicated Short Range Communication (DSRC).

The band of 10MHz is separated into seven channels which is 178, 172,1 74, 176,180,182,184. The channel 178 is called as Control Channel (CCH).The other channel said to be Service Channels (SCH). For High Availability and Low latency (HALL) and high power and public safety, the service channels 172 and 184 are allocated.

3.2 WAVE (WIRELESS ACCESS IN VEHICULAR ENVIRONMENT)

To operate in a VANET situation and to set up a Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications [12], the WAVE station defines the architecture; services, interfaces and a set of standard protocols. It describes the security about exchangeable messages. In the transportation field, the deployment of a huge variety of application is all provided by this WAVE architecture. This architecture comprises improved navigation, automatic tolls, road and vehicle safety, traffic management and also many applications. The WAVE IEEE 1609 standards is organized as,

***IEEE P1609.0* –** This guides for necessary services to the multichannel DSRC machines for communicating in high mobile environment.

***IEEE P1609.1 (Resource Manager)* –** Defines command messages and storage data formats, data flows and resources. It specifies the device types which an On Board Unit has supported.

***IEEE Std 1609.2 (Security Services for Applications and Management Messages)* –** The secure message formats and the processing method used in WAVE and DSRC system are all defined by this standard. It specifies the method for secure the management messages, application messages, function necessary to hold message security and privacy of vehicle.

***IEEE Std 1609.3 (Networking Services)* –** Describes service for the transport and network layers, it includes routing and addressing with the support of secure WAVE data exchange.

***IEEE Std 1609.4 (Multi channel operations)* –** It defines the priority access parameters, interval timers, and service channel and control channels process. It describes the channel routing, management services and switching parameter.

***IEEE Std 1609.11 (Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS))* –** It describes secure messages and service needed by the usage of secure electronic payment formats.

***IEEE Std 1609.12 (Provider Service Identifier allocations (PSID))* –** Through the WAVE system, it provides the identifier values.

3.3 IEEE 802.11p

To hold vehicular networks, IEEE has enlarged its version from IEEE 802.11 protocols to IEEE 802.11p in agreement with DSRC band which describes the medium access and physical layers of VANETs.

IV. CHARACTERISTICS

VANET is an infrastructure less network in which the node is a Road Side Unit (RSU) or the moving vehicle. It provides a combination of wireless medium methods and the characteristics of ad hoc network which uses a different topology for communication and infrastructure dependent modes. Some of the distinct characteristics of VANET can be summarized as follows:

A. High Mobility – Nodes in VANETs usually move at high speed. This makes harder to predict a vehicle / node's position and providing protection of node privacy [5].

B. Wireless Communication – VANET is designed for the wireless environment. Nodes are connected and exchange information via wireless. Therefore some security measure must be considered in communication.

C. Unbounded Network Size – VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.

D. Rapidly Changing Network Topology – Due to high node mobility and random speed of vehicles, the node position will change frequently. So, network topology in VANETs is dynamic and unpredictable. It facilitates the entire network attacks and make hard to find of misbehavior in the network.

E. Frequent Exchange of Information – The ad hoc nature of VANET motivates the nodes to gather information from the neighbor vehicles and RSU's. Hence the information exchange among node becomes frequent.

F. Time Critical – The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and do action accordingly.

G. Sufficient Energy and Computing – The VANET nodes have no issue of energy, storage and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.

H. Better Physical Protection – In VANET, nodes/vehicles are physically better protected. So, VANET nodes are more difficult to compromise physically and difficult to reduce the result of infrastructure attack.

I. Limited transmission power – In the WAVE the transmission power should provide up to the data reached. The data reachability distance can be said to be 1000m. For crisis and any public safety such as accident problem or any traffic congestion problem, it is allowed to transmit with a high power.

J. Anonymity of the support – By using a wireless medium the data transmission will be generally mysterious. The limit and control of using network can leaved, everyone outfitted with a transmitter, which is operate in the same frequency band that can be transmitted and holed that band.

K. Limited bandwidth – In VANET, the standard DSRC band should be measured as limited, the width of the DSRC band was 27 MHZ. The throughput was 27 Mbps which is a theoretical value.

L. Attenuations – According to digital transmission, DSRC band has transmission problems with those frequencies, which is reflection, diffraction, and dispersion, different types of fading, and Doppler Effect, losses. The propagation delays occur because of multipath reflections.

V. APPLICATIONS OF VANETS

Critical applications for VANETs concern to safety features and should be offered on all vehicles. The success of VANETs depends on number of vehicles equipped with adhoc connectivity. VANET provides applications like e-Safety, traffic management, driver comfort support, maintenance, media services, gaming, e-shopping, crime investigation, defense and so on. VANET uses P2P (Peer-to-Peer) applications [13] for providing services to the customers. P2P applications are divided into four categories for handling the data [13] – Source, Customer, Source and Customer, Intermediate.

5.1 SAFETY RELATED APPLICATIONS

Using these applications the road safety can be increased. The following services can be offered under this category of applications.

Collision Avoidance – An alert can be provided in half a second before crash occurs which avoids 60% of accidents. Once the warning message sent to the driver, the crash can be avoided.

Cooperative Driving – Drivers will obtain signals for traffic associated warnings like Hazardous driving condition detection, detection of a rogue driver going the wrong way, lane change, curve speed etc.

Traffic Optimization – Traffic can be optimized by making use of sending signals like accidents, jam etc. to other vehicles.

5.2 USER BASED APPLICATIONS

These applications present the information about user. Several services can be offered for the user to utilize a VANET in this category.

Peer to Peer application – This type of applications include sharing music, movies, videos, etc among the network.

Internet Connectivity – VANET provides the constant connectivity of the Internet.

Other Services – Other user applications includes accessing the location of fuel station, restaurant, and payment service to collect the taxes etc.

5.3 VEHICULAR APPLICATIONS

VANETs have the responsibility of passenger comfort, road safety, and driver assistance.

Road safety – VANET offer some road work and collision avoidance, fixed obstacles, dissemination of weather information and detection of mobile.

Driver assistance – Vehicular networks has to help the driver in prevention of channels output, overtaking vehicles, detection and warning of traffic congestion, warning of potential traffic jams, etc.

Passengers comfort – The services like messaging, discussion between vehicles, mobile internet access, collaborative network games etc. make comfort to the passengers.

VI. VANET SECURITY CHALLENGES

VANET uses open medium and this makes it to face the security in adhoc protocols and is vulnerable against several attacks like unauthorized access, illegal use, eavesdropping, protocol tunneling, etc. Attackers by using these vulnerabilities can reduce performance of the network and cause serious problem for genuine users [14]. VANET security should satisfy four goals, it should ensure that the information received is correct (information authenticity), the source is who he claims to be (message integrity and source authentication), the node sending the message cannot be identified and tracked (privacy) and the system is robust. In [15] [16] author's have made a comprehensive investigation and discussion on VANET vulnerabilities and attacks. VANET attacks are classified into many categories like attacks based on insiders and outsiders or maliciousness and rational or

active and passive [17]. It is also possible that other types of attack may occur when VANETs are actually implemented in the real world [18].

When it comes to working of Adhoc Networks with co-operative transmission, security and privacy aspects must be taken into consideration to achieve the effective results. While considering the security and privacy the main requirements to fulfill by the system is to provide with following things [19] [20]:

- Availability
- Integrity
- Confidentiality
- Privacy
- Authentication
- Non-Repudiation
- Freshness

Secured possible solutions on some attacks have been proposed in [21–23]. But still the system requires many robust techniques to achieve secured and privacy preserved data movement. Some techniques provide hardware level security while others may provide just data related security. But, it depends on the application for which the system is designed.

VII. CONCLUSION

VANETs received potential attention in recent years due to their huge impact in enhancing traffic management systems and road safety. Researchers proposed number of aspects for VANETs such as protocols, coverage, security models and other related aspects. Security in VANETs is given more importance, but the nature of this kind of networks seems to stand against reaching adequate and effective security. This paper has briefly introduced applications and the security challenges related to the VANETs. Although much development has taken place, security still lags behind. Up to date, there are no security standards that sufficiently meet all security requirements with fewer overheads. Furthermore, seeking to preserve privacy would add much more complications to achieving an adequate security model. So, more research is required to focus on further developments of sufficient security standards. The current major challenge is how to attain a balance between security, privacy, and usability while ensuring a fewer overheads. As a future work, it is suggested that research would focus on developing a security framework that take into consideration all or most of the aforementioned observations in order to come up with a sufficient security solution that satisfies VANETs requirements.

REFERENCES

[1] Jabbarpour MR, Marefat A, Jalooli A, Noor RM, Khokhar RH, Lloret J. Performance analysis of V2V dynamic anchor position-based routing protocols. Wireless Networks. 2015; 21(3):911–29.

[2] Malik V, Bishnoi S. Security threats in VANETS: A review; 2014.

[3] Wu D, Cao J, Ling Y, Liu J, Sun L. Routing algorithm based on multi-community evolutionary game for VANET. Journal of Networks. 2012; 7(7):1106–15.

[4] H. Morimoto, M. Koizumi, H. Inoue, K. Nitadori, "AHS road-to-vehicle communication system", IEEE ITISC, Tokyo, 1999.

[5] O. Andrisano, M. Nakagawa, R. Verdone, "Intelligent transportation systems: the role of third generation mobile radio networks", IEEE Communication Magazine, pp. 144-151, Sept. 2000.

[6] Prabhakar Ranjan, Kamal Kant Ahirwar, "Comparative Study of VANET and MANET Routing Protocols", Proc. of the International Conference on Advanced Computing and Communication Technologies (ACCT 2011).

[7] Mahmoud Al-Qutayri, Chan Yeun and Faisal Al-Hawi, "Security and Privacy of Intelligent VANETs", in Computational Intelligence and Modern Heuristics, book edited by Al-Dahoud Ali, 2010.

[8] M. Watfa, Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, ser. Intelligent Transport Systems. IGI Global, 2010.

[9] 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.

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

[11] 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.

[12] Mauri JL, Ghafoor KZ, Rawat DB, Perez JMA. Cognitive networks: Applications and deployments. CRC Press; 2014.

[13] http://www.nrlweb.cs.ucla.edu/publication/download/521/09-Emerging_Vehicular_Applicati ons .pdf

[14] V.Kumar, Shalni, S.Rani, R.P.Singh, G. C. Banerjee, A Comprehensive Analysis on The Threats and Vulnerabilities in VANET Technology, International Journal of Computer Engineering in Research Trends, Volume 2, Issue 5, May 2015, PP 280-283.

[15] Tyagi P, Dembla D, editors. Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation. 2014 International Conference on Advances in Computing, Communications and Informatics ICACCI; 2014 Sep 24-27.

[16] de Fuentes JM, González-Tablas AI, Ribagorda A. Overview of security issues in Vehicular Ad-hoc Networks.2010.

[17] Singh A, Kad S. A review on the various security techniques for VANETs. Procedia Computer Science; 2016. p. 284–90.

[18] Engoulou R, BellaÃiche M, Pierre S, Quintero A. VANET security surveys. Elsevier. 2014:1–13.

[19] Kaur N, Kad S. A review on security related aspects in vehicular ad hoc network. Procedia Computer Science;2016. p. 387–94.

[20] Di Pietro R, Guarino S, Verde N, Domingo-Ferrer J. Security in wireless ad-hoc networks: A survey. Computer Communications; 2014. p. 1–20.

[21] Raw RS, Singh KM. Security challenges, issues and their solutions for Vanet. International Journal of Network Security and its Applications. 2013:95–105.

[22] Ertaul L, Mullapudi S. The security problems of Vehicular Ad hoc Networks(VANETs) and proposed solutions in securing their operation. DBLP Conference: Proceedings of the 2009 International Conference on Wireless Networks, ICWN 2009, Las Vegas Nevada, USA; 2009. p. 13–16.

[23] Dak A, Yahya S, Kassim M.A survey on security challenges in VANETs. International Journal of Computer Theory and Engineering; 2012. p. 1007–10.