Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 5, April-2019, ISSN 2230-7540

Review Paper on VANET and the Challenges

Jyoti Kushwaha[1]* Dr. Kanojia Sindhuben Babulal[2]

[1] M. Tech Scholar, United College of Engineering and Research, Naini, Allahabad, India

[2] Assistant Professor, United College of Engineering and Research, Naini, Allahabad, India

Abstract – In the past few years, Vehicular Adhoc Networks (VANETs), known as Vehicle-to-Vehicle and Vehicle-to-Roadside wireless communications, have received a huge amount of well-deserved attention in the literature. Indeed, because of their unmistakable societal impact that promises to revolutionize the way we drive, various car manufacturers, government agencies and standardization bodies have spawned national and international consortia devoted exclusively to VANET. Examples include the Car-2-Car Communication Consortium, the Vehicle Safety Communications Consortium, and Honda's Advanced Safety Vehicle Program among others. The impetus of VANET is that in the not-so-distant future vehicles equipped with computing, communication and sensing capabilities will be organized into a ubiquitous and pervasive network that can provide numerous services to travelers, ranging from improved driving safety and comfort, to delivering multimedia content on demand, and to other similar value-added service. Indeed, the fact of being networked together promotes car-to-car communications, even between cars that are tens of miles apart.

Keywords – VANET architecture, Attacks, Challenges, DSRC, On- Board Unit, Inter vehicular Communication.

----------X----------

1. INTRODUCTION

The field of VANETs started gaining attention after 1980s and has, now-a-days, been an active field of research and development. Various types of challenges in vehicular communications have been identified and addressed. A large number of routing protocols have been proposed for VANET. (Royer and Toh, 1999) (Park and Corson, 1999)

A routing protocol governs the way that two communication entities exchange information; it includes the procedure in establishing a route, decision in forwarding, and action in maintaining the route or recovering from routing failure.

VANET routing protocols can be classified as topology- based and geographic (position-based). Topology-based routing protocols can further be divided into proactive (table- driven) and reactive (on-demand) routing.

Enough research has already been carried out which includes the comparison of various routing protocols and their performance evaluation based on different mobility models. It will be interesting to evaluate the performance of one of the routing protocol by varying the number of mobile nodes.

For this purpose, Ad Hoc on Demand Distance Vector (AODV) routing protocol is simulated because it has been observed that A0DV is a better approach as compared to both Destination-Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR).

2. VANET

The networks that interconnect vehicles on road are called Vehicular Ad hoc Networks (VANETs). "A mobile ad hoc network (MANET) consists of mobile nodes that connect themselves in as decentralized, self-organizing manner and may also establish multi-hop routes. If mobile nodes are cars, this is called vehicular ad hoc network".

A Vehicular Ad Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters from each other to connect and, in turn, create a network with a wide range. (Eklund, et. al., 2002) As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile network is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

VANETs come under the category of wireless ad-hoc network. In vehicular ad-hoc network, the node may be a vehicle or the road side units. They can communicate with each other by allowing the wireless connection up to a particular range. Inter-Vehicular Communications (IVC) also known as vehicular ad hoc networks (VANETs) have become very popular in recent years.

A main goal of VANETs is to increase road safety by the use of wireless communications. To achieve these goals, vehicles act as sensors and inform each other about abnormal and potentially hazardous conditions like accident, traffic jams and glazes. Vehicular networks closely resemble ad hoc networks because of their rapidly changing topology. Therefore, VANETs require secure routing protocols.

The constraints and optimizations are remarkably different. From the network perspective, security and scalability are two significant challenges. A formidable set of abuses and attacks become possible. Hence, the security of vehicular networks is indispensable. The growing importance of inter vehicular communications (IVC) has been recognized by the government, corporations, and the academic community. (Das, et. al., 2000)

2.1 VANET Model Overview

There are many entities involved in a VANET settlement and deployment. Although the vast majority of VANET nodes are vehicles, there are other entities that perform basic operations in these networks. Moreover, they can communicate with each other in many different ways. (Manchanda and Bangar, 2014) Fig. 1 shows the typical VANET scheme.

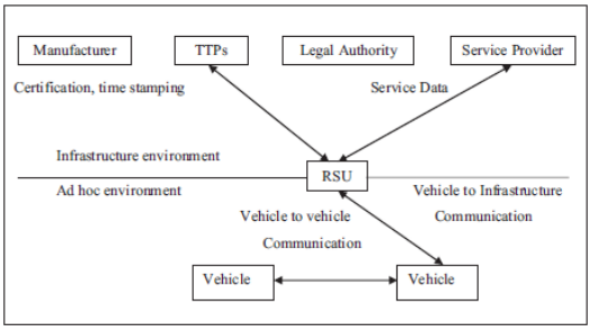

Figure 1: VANET Model

Three categories of network architecture of VANET are Pure cellular/ WLAN, Pure Ad hoc and hybrid as shown in Fig. 2.

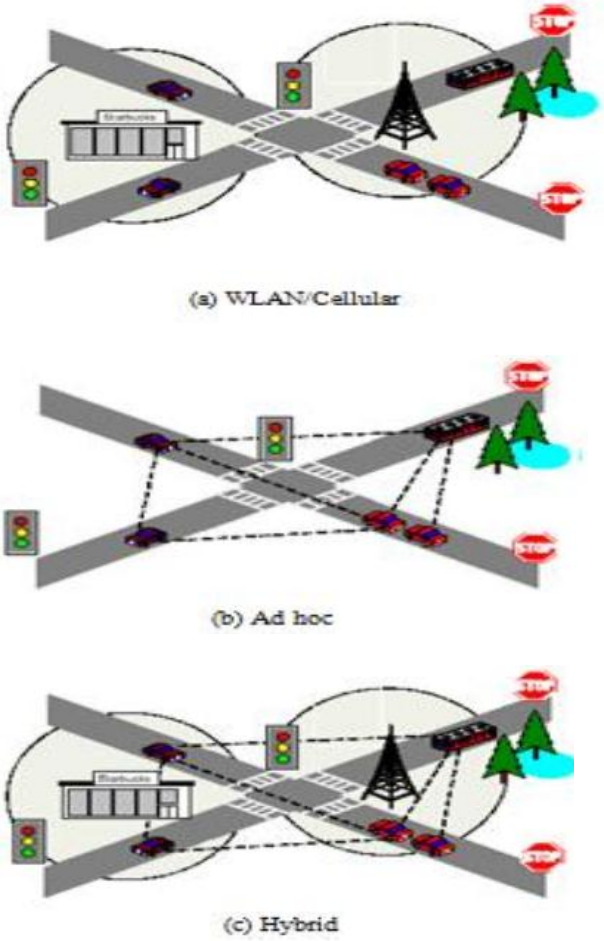

Figure 2: Three Categories of VANET Network Architecture

Entities in infrastructure environment can be permanently interconnected. It is mainly composed by those entities that manage the traffic or offer an external service. (Royer and Toh, 1999)

From the VANET point of view, they are equipped with three different devices. Firstly, they are equipped with a communication unit (OBU, On-Board Unit) that enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. On the other hand, they have a set of sensors to measure their own status (e.g. fuel consumption) and its environment (e.g. slippery road, safety distance).

2.2 System Architecture and Working of VANETs

Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today, these vehicles will require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), (Elias, et. al., 2010) for range can reach 1 KM, this communication is an Ad Hoc communication that means each connected node can move freely, no wires required, the routers used called Road Side

Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. (Moreira, et. al., 2009)

Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets, all the information about the vehicle like keys, driver's identity, trip details, speed, route etc. (Yan-tao, 2010)

The **architecture** of VANET implies that the communicating nodes in a VANET are either vehicles or base stations. Vehicles can be private or public. Base stations can belong to the government or to private service providers. As shown in Fig. 3 the vehicles can communicate with each other and communicate with Road Side Units (RSU) interchangeably. [8] (Hasan, et. al., 2011)

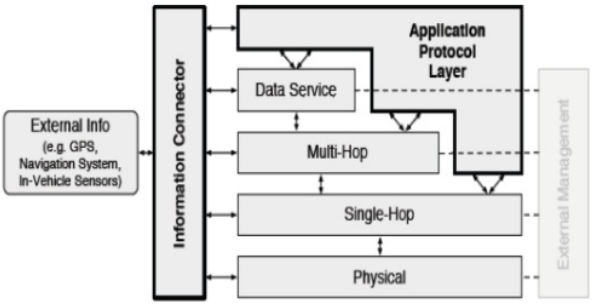

Figure 3: Architecture of VANET

2.3 Challenges and Issues

The security challenges which are faced in Pervasive Network are because of the weak connecting link between different nodes. As the nodes are distributed in the wireless medium, they can communicate by making proper utilization of signal propagation through air medium. So, it is easy to faucet. The resources are very much limited for the nodes present in the pervasive environment.

Therefore, proficient schemes with less overhead are required and preferred. Due to its dynamic nature, there is a requirement of the self-organizing, self-healing algorithm for tolerance of the security attacks. (Perkins and Royer, 1999)

The attacks generally observed and often occurs in Pervasive Network may be broadly categorized into two categories: Passive and Active attacks. Eaves dropping falls into the category of passive attack. In this, the intruder captures the data while it is transmitted.

On the other hand, in the active attack, the malicious node misleads other nodes to affect the communication. All types of ad-Hoc networks come under Pervasive Networks. In this research work, the Vehicular Ad hoc Network is taken to provide the security from location based attack. (Tee & Lee, 2008)

2.4 Possibility of Attacks in VANET

Besides having advantages of the proxy reencryption method for authentication, there are still some attacks that can be possible that are explained as in following section. (Moreira, et. al., 2009), (Manchanda and Bangar, 2014)

2.4.1 Denial of Service (DoS) attack

Attackers may seek to initiate excessive authentication requests in order to exhaust the resources of the Access Point (AP). A general solution would be to limit the number of authentication requests which can be processed in a unit of time period. This method can guarantee that the server is not overwhelmed by DoS.

2.4.2 Eavesdropping

Since the session key is calculated based on the nonce's contributed by the car and the AP respectively. Both of the car's nonce and the AP's nonce are encrypted by the public key of the SP during transmission. The attacker can reveal the session key, if he/she got the SP's private key, or an appropriate re- encryption key/private key pair.

2.4.3 Masquerade Attack

An unauthorized car which did not subscribe service from the SP may overhear the authentication messages on the air and try to have it authenticated to the AP by replaying them. The attacker can get the car's public key and certificate and replay the car's authentication request.

2.4.4 Key Bootstrapping and Rekeying

Anonymous keys are preloaded by the transportation authority or the manufacturer, but with different consequences. (Bianzino, et. al., 2012) Moreover, while ELPs are fixed and should accompany the vehicle for a long duration, anonymous key sets have to be periodically renewed after all the keys have been used or their lifetimes have expired.

3. VEHICULAR COMMUNICATION

Rapid advances in wireless technologies provide opportunities to utilize these technologies in support of advanced vehicle safety applications. The VANET aims to provide a high data rate and at the same time minimize latency within a relatively small communication zone. A number of novel problems are associated with a VANET because of the unique characteristics of the network.

4. DEDICATED SHORT-RANGE COMMUNICATION

Dedicated Short-Range Communication (DSRC) is a standard that aims to bring vehicular networks to North America. Traffic fatalities have been a long standing problem in the United States, as in the rest of the world.

5. BACKGROUND AND LITERATURE SURVEY

Y. Zhang and W. lee Zhang 2000 discussed about the statistical anomaly detection approach for mobile ad hoc networks (Intrusion detection in Wireless ad-hoc Networks). So far, the authors concentrate on simulations at the routing protocol level, but in they have not mentioned about multi-layer integrated intrusion detection would be helpful to increase detection rate.

Shengming Jiang (2001) proposed and investigated a prediction-based link availability estimation, (Tp) , for MANET in this search. This algorithm tries to predict the probability that an active link between two nodes will be continuously available for a predicted period, which is obtained based on the current node's movement.

Jeremy J. Blum et al. (2004) said that the IVC network exhibits very different characteristics from other MANETs. Specifically, the constraints on vehicle movements, varying driver behavior, and high mobility cause rapid topology changes, frequent fragmentation of the network, a small effective network diameter, and limited utility from network redundancy.

Daniel Jiang et al. (2006) presented the operational concept of 5.9GHz DSRC-based vehicular safety communication. The overall DSRC communication architecture in the draft IEEE 1609 standard contains two parallel stacks.

Kun Yang et al. (2007) - A cross-layer protocol called coordinated external peer communication (CEPEC) was proposed for Internet-access services and peer communications for vehicular networks. They assumed that IEEE 802.16 base stations (BS) were installed along highways and that the same air interface is equipped in vehicles.

Gongjun Yan et al. (2010) proposed the classification of existing VANET routing protocols into five categories: connectivity based, mobility-based, infrastructure-based, geographic location based, and probability-model-based, according to their employed routing metrics. For each category, we present the general design ideas and state of the art. Their objective was to attract more attention to the VANET routing problem and encourage more research efforts on developing reliable solutions.

Alexey Vinel et al. (2012) said that vehicular adhoc networks enabled the design of emergent automotive safety applications, which were based on the awareness among vehicles. Recently, a suite of 802.11p/WAVE protocols aimed at supporting car-to-car communications was approved by IEEE.

Mahmoud Hashem Eiza et al. (2012) proposed a new reliability-based routing scheme for VANETs in order to facilitate Quality of Service (QoS) support in the routing process. The link reliability was defined as the probability that an active link remains available for a certain time interval.

Mahmoud Hashem Eiza et al. (2013) proposed a new vehicular reliability model to facilitate the reliable routing in VANETs. The link reliability was defined as the probability that a direct communication link between two vehicles will stay continuously available over a specified time period.

Manchanda, P. and Bangar, P (2014) said that Vehicular ad-hoc networks (VANETs) offer a vast number of applications without any support from fixed infrastructure. These applications forward messages in a multi-hop fashion. Routing is an important component in vehicle-to-vehicle (V2V) and infrastructure-to-vehicle (I2V) communication. Designing an efficient routing protocol for all VANET applications is very hard.

Tasneem Darwish, Kamalrulnizam Abu Bakar (2014) - Vehicular ad hoc networks (VANETs) are gaining tremendous interest among researchers and industries.

Puneet Manchanda, Parvinder Bangar (2014) discussed the route discovery process for AODV protocol in a VANET. When the source vehicle Shas data to send, it first looks at its routing table. If there is a valid route to the destination de, then it will use it, else a new route discovery process starts.

Mohammad Fathian, Ahmad Reza Jafarian Moghaddam (2015)- A vehicular ad Hoc network (VANET) is a network in which vehicles acting as dynamic nodes communicate with each other.

Yuzhong Chen, Mingyue Fang, Song Shi, Wenzhong Guo and Xianghan Zheng (2015) - Vehicular ad hoc networks (VANETs) have become important components of metropolitan area networks, and clustering for VANETS provides many advantages.

Preeti Rawat, Shikha Sharma (2016) – The VANET security has become an important and active area within the research community. Despite the various attacks aimed at particular nodes in

VANET that have been revealed, many attacks including multiple nodes still achieve little care.

Ramesh C. Poonia, Deepshikha Bhargava (2016) - In recent years, continuous progress in wireless communication has opened a new research field in computer networks. Now- a –days wireless ad-hoc networking is an emerging research technology that needs attention of the industry people and the academicians.

Samiksha, Anit Kaur (2016) - A novel kind of ad hoc network is defeating the roads: Vehicular Ad Hoc Networks. In these networks, vehicles communicate with each other and perhaps with a roadside infrastructure to provide a long list of requests varying from transit safety to driver support and Internet access.

6. CONCLUSION

Ad Hoc on Demand Distance Vector (AODV) is a topology-based reactive routing protocol, which operates on hop-by-hop pattern. AODV maintains the established routing path in the given period and copes well with fast- changing network topologies and high relative vehicle speeds.

To propose and implement a novel protocol with novel approach based on distance vector, greedy forwarding strategy with perimeter forwarding strategy, GPS system and vehicle's environment which has lower packet loss rate, high throughput, less network load and less time delay.

Simulation of vehicular movement should be done by using road traffic simulation and network simulation. Here we will be able to observe the directionally coupled simulation have advantage over the uncoupled simulation and simple traffic simulation will not be appropriate for VANET simulation.

REFERENCES

1. Tee, C.A.T.H.; Lee, A.C.R. (2008). "Survey of position based routing for Inter Vehicle Communication system", Distributed Framework and Applications, DFmA 2008. First International Conference on, pp.174-182, pp. 21-22.

2. Samir R. Das, Charles E. Perkins, and Elizabeth M. Royer (2000). "Performance Comparison of Two On demand Routing Protocols for Ad Hoc Networks." Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Tel Aviv, Israel, p. 3–12.

3. Carl Eklund, Roger B. Marks, Kennethl. Stanwood, Stanley Wang (2002). "IEEE standard 802.16: Atechnical overview of the wireless MANTM air interface for broadband wireless access", IEEE Communications Magazine, Vol. 40, no. 6, pp. 98–107.

4. E.M. Royer and C-K Toh (1999). "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Personal Communications, vo1. 6, no. 2, pp. 46–55.

5. E. M. Royer and C.K. Toh (1999). "A Review of Current Routing Protocols for Ad-Hoc Mobile Ad hoc Networks," IEEE Personal Communications.

6. Yan-tao Liu (2010). "Stationary of Random Direction Direction models", 2010 Second International conference on network security, wireless communications and trusted computing.

7. G. Elias, M. Novaes, G. Cavalcanti, and D. Porto (2010). Simulation-based performance evaluation of the SNDP protocol for infrastructure WMNs. In Proc. 24th IEEE Int Advanced Information Networking and Applications (AINA) Conf, pages 90-97.

8. The Working Group for WLAN Standards of the IEEE. HWMP protocol specification. 2006.

9. Puneet Manchanda and Parvinder Bangar (2014). "A SURVEY ON ROUTING IN VANET", International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume:5, Issue:4, Pages:1-6.

10. V. D. Park and M. S. Corson (1999). A highly adaptive distributed routing algorithm for mobile wireless networks. In Proc. IEEE Sixteenth Annual Joint Conf. of the IEEE Computer and Communications Societies INFOCOM '97, volume 3, pages 1405-1413.

11. C. E. Perkins and E. M. Royer (1999). Ad-hoc on-demand distance vector routing. In Proc. Second IEEE Workshop Mobile Computing Systems and Applications WMCSA '99, pages 90-100.

12. Z. Hasan, H. Boostanemehr and V. K. Bhargava (2011). "Green Cellular Networks: A Survey, SomeResearch Issues and Challenges," Communications Surveys & Tutorials, IEEE, Vol. 13, No.4, pp. 524-540, Fourth Quarter.

13. A. P. Bianzino, C. Chaudet, D. Rossi and J. I. Rougier (2012). "A Survey of Green Networking Research," Communications

Surveys & Tutorials, IEEE, vol.14, no.1, pp. 3-20, First Quarter.

14. W. A. Moreira, R. Lopes Gomes, and A. J. Gomes Ableem (2009). A multiple metric approach for routing in wireless mesh networks. In Proc. IEEE Int. Symp. a World of Wireless, Mobile and Multimedia Networks & Workshops WoWMoM, pages 1-6.

15. Puneet Manchanda and Parvinder Bangar (2014). "Modified AODV-R Routing Protocol", International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 16, Issue 01, pp. 96-101.

Corresponding Author

Jyoti Kushwaha*

M. Tech Scholar, United College of Engineering and Research, Naini, Allahabad, India

jyotikush1993@gmail.com