IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

"A Glance over the Working Methodology of VANET"

Apurva Kukade[1], Prof. Tilotma Sharma [2]

Student M. Tech (IT), Dept Computer Science & Information Technology, Mahakal Institute of Technology, Ujjain[1]

Reader (IT), Dept Computer Science & Information Technology, Mahakal Institute of Technology, Ujjain[2]

Abstract: Mobile ad-hoc network is a part of ad-hoc network which can change locations and synchronize itself. Because of their mobile nature they use wireless connections to connect different networks; it would be a Wi-Fi connection or some other medium. With growing technologies VANET (Vehicular ad-hoc network)are special category of dynamic wireless network. VANET allows vehicles to communicate with the roadside equipments. It works under ITS (Intelligent transportation system). In VANET nodes communicate wirelessly with their different mobility nodes. Mobile communication, traffic monitoring safety and public utility management are the key components of VANET. In VANET there are two modes of vehicle communication which are names as Vehicle to vehicle (V2V) and Vehicle to infrastructure (V2I). Infrastructure absence is the main characteristics of VANET such as access point or base station, existing in the Wi-Fi, WI-Max, GSM or UMTS. Vehicular communication explains the numerous initiatives of the research which enhance the security, efficiency of transportation systems, supplying, and traffic in the road conditions such as emergency, construction sites and congestion. The attributes of VANET works with a solution which takes routing protocols of MANET. IVCN (Inter Vehicle Communication Network) is the new approach of ad-hoc network.

Keywords: VANET (Vehicular ad-hoc network), WI-FI, WI-Max, GSM, UMTS, Vehicle to vehicle (V2V).

1. INTRODUCTION

Due to promising applications VANET have created emerging research and commercial interest. There are many applications of VANETs such as safety enhancement, traffic congestion and emergency notification, electronic tolling, and dissemination and media and the application layer. The below Fig. explains the architecture of VANET download. There are various forms of wireless communication technology which have been proposed to establish VANET, Wi-Fi (802.11 based) is one of them. Vehicles prepared with wireless network interface use either IEEE 802.11b or IEEE 802.11g standard to approach media. The interaction between the nodes which are out of the reach of transmission of the radio is made with multi hops through intermediate nodes. More the topology of the network move dynamics. Without wire media with the absence of infrastructures and multiple hops routing transmission, have network in strength of diverse types of attacks until active interferences creation, destruction and modification of messages. On the other hand node sensory mobile, vehicle supplies the sufficient high electric power in system of Inter Vehicle Communication, so energy consumption is second factor. Security and privacy are the key factors and challenges in Inter Vehicle Communication System. VANET features include a solution which integrates the routing protocols of MANET. ITS (Intelligent Transportation System), has necessarily exchange information between vehicles such as position and speeds. With IVCN each vehicle can change information with their neighbours.

2. VANET NETWORK ARCHITECHTURE

The three primary components of VANET are onboard unit (OBU), roadside unit(RSU), and backhaul network and mainly there are two categories of VANET, they are Vehicle to Vehicle(V2V) and Vehicle to Infrastructure(V2I). The network architecture of VANET consists of physical layer, the media access layer, the network layer, transport layer and the application layer. The communication between the inter vehicle and vehicle base station, for communication and interface each vehicle has its individual onboard units.[7]

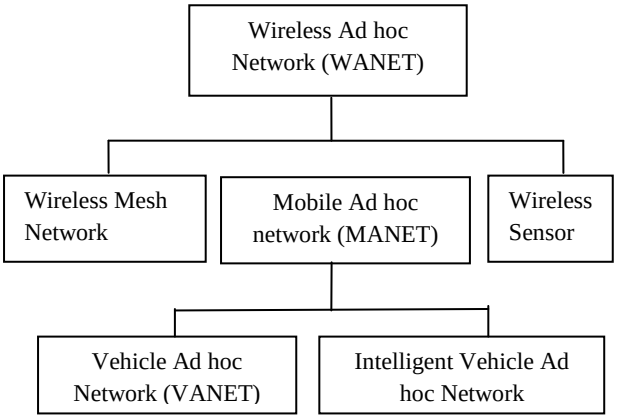

Fig.1 Architecture of vehicle ad-hoc network

The VANET architecture falls in three ways- pure cellular/WLAN, pure ad-hoc and hybrid. It may use fixed cellular gateways and WLAN/WiMax access point at traffic intersections connecting to the internet. Cellular network and WLAN together combine through VANET to form network so WLAN is used at the available access point.[2]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Table 1 Layered view of vehicular network

Network Architectures	Application Type	• Safety application • Intelligent transport application • Comfort application
	Quality of service	• Non-real time • Soft real time • Hard real time
	Scope	• Wide area • Local
	Network type	• Ad-hoc • Infrastructure based
	Communication type	• V2I • V2V

3. VANET OVERVIEW

3.1 Intelligent Transportation System

Each vehicle participates as a sender, receiver and router to transmit information to the vehicular network or the agency, than it uses the information for safety and free-flow of traffic. ITS explains technology relevant to transport and infrastructure, transferring information within systems to increase safety, productivity and environmental performance. Standalone application ex. traffic management system and information participate in it and they installed in vehicles. ITS encompasses large range of wire line and wireless communication depending information and electronic technologies.

3.2 Vehicle to Vehicle Communication

V2V communication composed a wireless network in which automobiles can transfer information with each one, such as safety warning and traffic information. The data or information about what they are doing contains of location, speed, travelling, direction, stability loss and braking. V2V uses a standard known as Dedicated short range communication (DSRC). For sometimes it can be explained as a Wi-Fi network, the reason is frequency is 5.9 GHz (used by Wi-Fi) band with bandwidth of 75 MHz, so we can say that it behaves more like Wi-Fi. Range is about 1000 feet (300 meters) which is on highway about 10 sec. In V2V every node can send, catch or transmit again the signals, we can say it become a mesh network. For vehicular network there are two standard division which include a class of IEEE called IEEE 802.11 which is Wireless Access in Vehicular Environments (WAVE). For 802.11 wireless LAN, MAC layer and PHY layer there is a enlargement known as 802.11p. The main role of 802.11p is to support specification for PHY and MAC layer for vehicular network.

3.3 Vehicle to Infrastructure Communication

The motivation of infrastructure in V2I is that by meeting global and local information of the traffic related to road state than create their protocol with the group of vehicles. V2I is the wireless exchange of critical safety and data between vehicles and infrastructure on highway. It represents a one way hop where on road unit send information to all vehicles. With the aim of elaboration of all the fuel consumption, emissions the acceleration and the velocities of the vehicles and the inter vehicle distance would suggests by the infrastructure which is based on the traffic conditions. Information to drivers are broadcast through the road display or wireless connections directly. The roadside units placing at every kilometre, taking high data rates which should be maintained for heavy traffic. For such an instance when broadcasting dynamic limits the infrastructure unit will examine the approximate speed according to its inner traffic conditions. The unit will broadcast a message at particular interval of time which can take the limit of speed and compare the directional limits with the vehicle.[1]

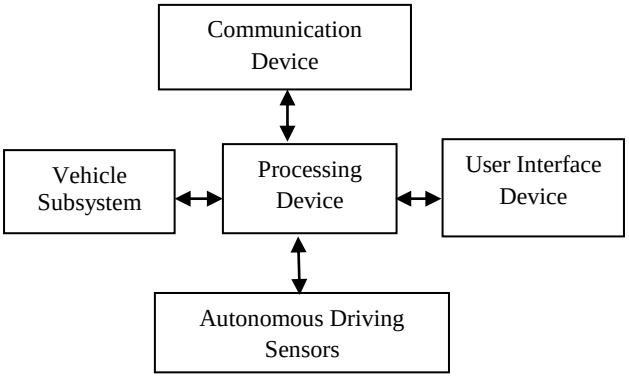

Fig.2 Vehicle to infrastructure

4. RULES FOR BROADCASTING IN VANET

The rules define for the operations in VANET which are as-

1) Dense traffic
2) Sparse traffic
3) Regular traffic

For the three rules one thing should take in mind that a good and efficient routing protocol dealt with it.

1) Dense traffic

When the density of the traffic is above the level than the most common problem is that there is a choking of the shared medium by controlled number of safety message which are broadcast by various cars following each other continuously. Therefore the result is confliction in the transmission of the data within the neighbouring nodes because of the negligent broadcast of the packets through the shared wireless channel. Normally this situation is known as broadcast storm problem.

2) Sparse traffic

Another traffic which is creating difficulty for the standard routing protocols is the sparse traffic in which there are least number of vehicles participating on the road. At some amount of time on day the traffic must become slow that multiple hoc coming from the source to the car may not be probable because they are not in the range of the transmission area of the source. On the opposite lane there might be no cars in the transmission range this situation make it more worse so this type of situation creates problems for routing and broadcasting, there are various

techniques available for this situation which address the sparsely joined behaviour of the mobile wireless network.

3) Regular traffic

The dense and the sparse traffics which we have talked about have one thing is likewise that the global connectivity is effected by the local connectivity in the networks of the vehicles such as take an examples of as in a busy network the vehicle notice the closely local topology and in sparse network vehicles observe very less or no neighbours or we can say that sparse topology. Therefore vehicles working in these two rules will observe the same local topology which should directly effect the global topology. As far this situation creates the vehicles will apply the algorithm which is known as broadcast suppression and to conserve network operability some vehicles will follow the save carry forward message.[5]

5. ROUTING IN VANET

Over the previous year's routing has been studied widely. The mainly used ad-hoc routing protocol on the initial level maintained for MANET has tested for the use in VANET. The protocols which are address based and topology based have main role that there is a unique address for the participating nodes. So there should be a mechanism which should used to assign that unique address but there is no guarantee of the avoidance of allocation of duplicate address. VANET related subjects as a network topology, mobility patterns, density of vehicles, rapid changes in vehicles all these can use the ordinary ad-hoc routing protocols. When the information is received by vehicle, than the features at the particular vehicle suddenly sends a uni-directional message that should contain the whole information of vehicle through which it receives the request than it forwards to the query source.

5.1 Proactive Routing Protocols

It enrols the standard named as Distance Vector routing or link state routing strategies ex. Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing Protocol (OLSR). The Distance Routing Effect Algorithm for Mobility explains a position based routing which is based on greedy forward mechanism which says nodes forward the packages. So the next hop position is every time will be nearer to the destination of current hop. The greedy perimeter which is placed on stateless routing known as perimeter routing which search for one after one results is not considered because the breadth of the highway is even smaller in comparison to the range of transmission.

5.2 Reactive Routing Protocols

Reactive routing protocols can demand and maintain the routes, so they can decrease the weight on the network. Vehicles under the communication use very limited number of routes.

5.3 Position based routing

The position based routing protocols enquire information for the physical position of the involving nodes for the availability of their direct neighbour than a request can be send by the sender for the position which consist in that packet. The packet which is send with no knowledge of map to one neighbour which is very close to the destination. These routing is profitable until the source to the destination path is properly maintained and created. These routing is widely separated into two parts which is position based greedy V2V protocols and Delay Tolerant protocols.[1]

6. VANET APPLICATIONS

To establish VANET there are some of the applications that can be profitable. These can be divided into two ways.[12]

6.1 Safety related applications

For increasing the safety on the road these applications are used which is further classified in following ways.

- Collision avoidance

60% accidents on road can be neglected if before the collision will happen the drivers were provided warning message just before half second and when they get warning message right on time than collision will be neglected.[10]

- Co-operative driving

The signals which are related by traffic warning can provide to the driver which are helpful for the driver for safe and uninterrupted driving such as changing the lane warning n about speed warning.

- Traffic optimization

To save time from traffic jam and accidents the signals can be used by the traffic optimisation according to which they can choose their different path and save their time.

6.2 User based applications

It supplies the user demonstration. VANET can be employed to avoid following services for the users.

- Peer to peer applications

The peer to peer applications are used to avail information related to sharing music, movies among the vehicles in the network.

- Internet connectivity

In today's world people need internet every time, so the VANET gives constant connectivity to the users.

Other services

VANET can be employed in other user based applications such as to locate the fuel station, restaurant, provide payment service to collect toll taxes.

7. CHARACTERISTICS OF VANET

- Basically VANET is the application of MANET but it too has its different characteristics which can be briefed as below.[11]
- VANET supports high mobility, the nodes in the network moving with high speed, it makes harder to find the position of the network and provide protection to the node.
- Because of the high mobility nature and the randomness in speed of vehicles the locality of the node changes rapidly through which network topology in VANET changes frequently.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

- There is no boundation of network in VANET, it can be execute for cities or for countries so VANET is geographically unbounded.
- The exchange and gathering of information to nodes through the vehicle and other road device becomes very rapid and frequent, this is because of the ad-hoc nature of VANET.
- VANET is mainly design for the wireless communication so the nodes in the network can exchange information wirelessly so the security also taken in mind for the communication.
- The one thing in VANET is explains that it is time critical according to which the exchange of information providing to the node can reach within time because of which there is a proper decision and action performed by the node.
- There is no such issue of energy and computation resources, VANET provides sufficient energy and unlimited transmission power for which they allow some demanding techniques such as RSA, ECDSA implementation.
- VANET provide better physical protection to the nodes, so it is difficult to attack the infrastructure and more difficult to physically compromise.

8. ATTACKS IN VANET

For better protection from attackers, we have some knowledge about attacks in VANET according to different security requirements. There are some attacks which are as follows.[12]

8.1 Impersonate

In this type of attack attacker supposed the uniqueness and rights of the authorised nodes, it can make the use of network resources that will be no longer available to it or it can interrupt the working of network, it is performed by the active attackers these are insider or outsider. These are multilayer attack which can perform in two ways, one is false attribute possession in which attacker steals property of the user and the other is sybil in which attacker use different character at same time.

8.2 Session Hijacking

It is easy to hijack the session after connection is established because authentication is done at the beginning of the session and the attackers can take control over the session between nodes.

8.3 Identity Revealing

For most of the cases driver itself is the owner of the vehicle therefore getting owner's identity put their privacy into the risk.

8.4 Location Tracking

To get the information of the driver attacker trace the vehicle on the base of the path which are followed along a time period and the location of the given moment.

8.5 Repudiation

The important threat in this type is the denial or attempting to denial by a node in the communication. In this type of attack two or more than two entity has its common identity so its easy to repudiation because they are in differentiate.

8.6 Eavesdropping

It is based on the confidentiality which is passive in nature and belongs to network layer attack. The main purpose of this type of attack is to get access of confidential attack.

8.7 Denial of Service

This type of attack are the most noticeable attack in which the attacker prevents the innocent user to so that they can use the service from the victim node. These type of attacks can bear in many ways such as jamming, SYN flooding and distributed DoS attack.

8.8 Routing Attacks

These attacks exploring the vulnerability of the network layer routing protocols in which attacker either disturbs the routing process or drops the packet of the network. There are most common attacks in the routing attacks which are as

8.8.1 Black hole attack

In this attacker attracts the node through which it can transmit the node itself after that when the packet is forwarded than it can be silently drops the packet.

8.8.2 Worm hole attack

In this type of attack an opponent receives the packet at some point in the network than it tunnels them to another point of the network and than it can replay it from that point. The tunnel made between these two opponents is known as wormhole.

8.8.3 Gray hole attack

It is the extended part of black hole attack. In this attack the malicious node behave just like the black node attack and drop the packet according to the selection. One is it can drop the UDP packet and forward the TCP packet and other selection is based on the probabilistic distribution.

9. SOLUTION OF THE ABOVE ATTACKS IN VANET

There are five solutions [12]
1) ARAN (Authenticated Routing for Ad Hoc Network)
2) SMT (Secure Message Transmission)
3) SEAD (Secure and Efficient Ad Hoc Distance Vector)
4) NDM (Non Disclosure Method)
5) ARIADNE

S. No.	Solution	Attacks Covered	Technology used	Security requirements
1.	ARAN	1. Replay Attack 2. Impersonation 3. False Warning	1. Cryptographic Certificate	1. Authentication 2. Message Integrity 3. Non-Repudiation
2.	SMT	1. Information Disclosure	1. MAC (Message Authentication Code)	1. Authentication
3.	SEAD	1. DoS 2. Routing Attack 3. Resource Consumption	1. One Way Hash Function	1. Availability 2. Authentication
4.	NDM	1. Information Disclosure 2. Location Tracking	1. Asymmetric Cryptography	1. Privacy
5.	ARIADNE	1. DoS 2. Routing Attack 3. Replay Attack	1. Symmetric Cryptography 2. MAC	1. Authentication

Table 2

DOI 10.17148/IJARCCE.2015.41274

10. CONCLUSION

In the last few years many VANET projects undertaken around the world and several standards have been found to improve V2V and V2I. This paper is a part of survey work, which aims to explain and elaborate VANET. There are various attacks which are explained above are the major issues in VANET, about the part of its safety and security, so the solutions also had been discovered. This involves various routing protocols and their performance depends on the mobility of the nodes. VANET will become an important factor for the automobiles that have the potential to achieve their safety of vehicles, it will make sure to correctly designed the technology before its implementation in vehicles, so the aim can be achieved. Finally there are some challenges still needed in order to lineup VANET infrastructure, security and reliability.

REFRENCES

[1] Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen ·Angela Irwin · Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges." Springer Science+Business Media, LLC 2010.

[2] Rakesh Kumar, Mayank Dave, Department of Computer Engineering, N.I.T. Kurukshetra, Haryana, India,"A Comparative Study of Various Routing Protocols in VANET." IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[3] James Bernsen, D. Mnivannan, "Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification", in journal of Pervasive and Mobile Computing 5 (2009) 1-18.

[4] Saleh Yousefi', MAhmoud Siadat MIousavi2 Mahmood Fathy'1. Iran University of Science and Technology," Vehicular Ad Hoc Networks (VANETs): challenges and perspectives." 2006 6th International Conference on ITS Telecommunication Proceedings.

[5] Yashpal Singh, Er .Anurag Sharma,"Study of Broadcasting and Its Performance Parameter in VANET." International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[6] Ghanishtha Narang, Yogesh Juneja," Review on classification of different VANET Protocols based on routing information." International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015.

[7]Patrick I. Offor Nova Southeastern Universitypo125@nova.edu," Vehicle Ad Hoc Network (VANET): Safety Benefits and Security Challenges."

[8] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng," Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges." Journal of Wireless Networking and Communications 2013, 3(3): 29-38 DOI: 10.5923/j.jwnc.20130303.02.

[9] Ram Shringar Raw1 , Manish Kumar1 , Nanhay Singh1 1Ambedkar Institute of Advanced communication Technologies & Research," Security Challenges, Issues and their Solutions for VANET." International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[10] Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21.

[11] Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).

[12] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, 2010.