ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

A Review on Multipath Vehicular Ad Hoc Routing Protocol (VANET) Routing Protocol

Kavita[1] Prashant Gupta [2]
M-Tech Student[1], Assit. Prof.[2] & Department of CSE&Echelon Institute of Technology
Faridabad, Haryana, India

Abstract:
The basic factor for the VANET (Vehicular Ad hoc Networks) application success is routing however it must effectively deal with quick configuration changes and a distributed network. Latest MANET (Mobile Ad hoc Networks) routing protocols are not able to fully deal with these specific requirements particularly in a city environments (constrained but high mobility patterns, nodes distribution, signal transmissions blocked by obstructions, etc.). The aim of this review paper is to give an overview of the vehicular ad hoc networks, its standards, applications, security issues and the existing VANET routing protocols and this paper gives detail review on multipath AODV Routing Protocol.
***Keywords*: VANET, ITS, dynamic topology, mobility, routing protocols.**

I. VANET OVERVIEW

In present, many people throughout the world died each year in vehicle accidents, so in most countries some safety information i.e. traffic lights & speed limits are utilized, but however it is not a best solution. Also government and no. of automotive industries considered that vehicular safety is very challenging task. So as a result, to enhance people traffic safety of a novel advanced particular technology is developed i.e. VANET [3].

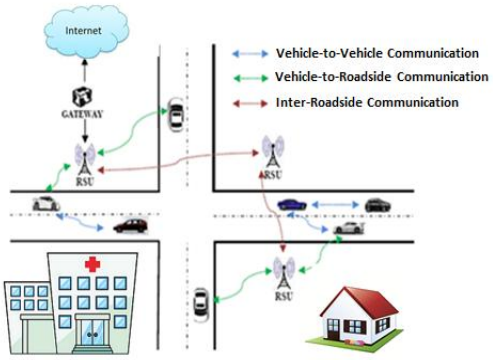

Figure1.Generalized VANET Architecture

It's an advance type of MANET (Mobile Ad-hoc Network). VANET manages a network in which vehicles are act nodes and utilized as mobile nodes to make a robust infrastructure-less ad-hoc network. Figure 1 illustrates the basic elements of VANET architecture. It Furthermore, apart from accidental-safety and security characters, there are also wide varieties of applications in VANET are available and possible that can offer passenger comfort like predictable mobility through GPS, web browsing and information updates and so on. Vehicular Ad-hoc Network (VANET) is a novel developed kind of Mobile Ad-hoc Network (MANET), where travelling nodes are vehicles like autos, cars, buses etc.

II. INTRODUCTION

In past few years, there is a fast improvement in the field of wireless and mobile communication. Mobile Communication Technologies have innovatively developed and developing "do it all" devices by leaps and bounds which has explosively triggered the growth of mobile data users: 1.5 billion users will use the new mobile data services by the end of 2017 according to the International Data Corporation [1]. This will led to a significant increase in wireless mobile traffic and demand for network resources in near future.

An important emerging wireless or mobile networking is an infrastructure-less "ad hoc" networking between mobile devices. Such networks are self configuring networks consisting of a set of mobile nodes that are connected by shared wireless channel forming an arbitrary topology without using any existing infrastructure or Central Management System[1]. In an Mobile Ad hoc network, each mobile node acts a host or router and forward the packets to other network in the node. These nodes are distributed randomly in the network and continuously participates or leave the network while moving. Vehicular Ad Hoc Network(VANET) is a special class of MANET in which entities that forms the network are vehicles and gives the concept of ubiquitous computing for future[2]. With VANET, vehicles can be turned into a network that will provide services similar like the ones used in offices and homes.

Every envisioned application of VANET requires that the nodes continuously broadcast vital information such as speed, location which will increase the awareness of vehicles about their whereabouts and warn drivers of

dangerous situations [3]. Traffic Management Applications require data dissemination in a multi-hop network to alert vehicles regarding traffic situation while Commercial Application require unicast routing. VANET has unique features like high mobility, dynamic topology limited transporting distance , distributed nature of operation which makes routing protocols developed for MANET show degraded performance in VANET scenarios[4].

A routing protocol decides the way of exchanging information between two communication entities. It utilizes the routing information to choose the next link whose maintenance is easy to realize according to performance criteria[5]. It establishes route, forward decision and maintain or recover from route failure. It's main aim is to provide an optimal path via minimum overhead[6].The performance of routing protocols depends on the characteristics of underlying network or environment. For example, at high node density, an on-demand protocol that diffuses requests on entire network at each route discovery may cause an important control traffic that prevents sending data packets. With table-driven protocol, the topology information kept at each node may become obsolete incase of high node mobility[7].

For a highly dynamic topology environment, Pro-active routing protocols need to update routing information more frequent. While Reactive routing protocols maintain routing information only when there is a data packet to send. So, Reactive protocols are best to adapt into VANET environment[8].

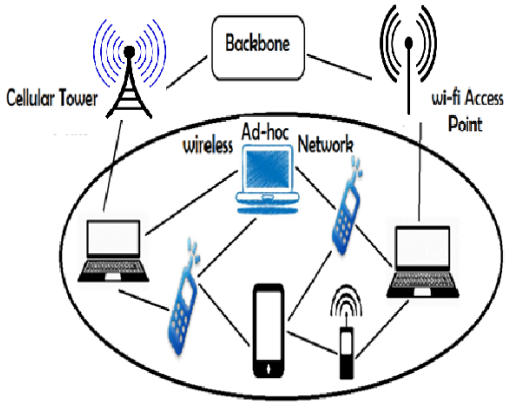

Fig2: Structure of Mobile Ad-Hoc Network

III. Route discovery in AODV

In an Ad hoc Network, if the source and destination mobile hosts are both inside the transmission range of each other, a simple query is all that is required to discover a "route" to the destination host. The returned MAC address may be utilized directly to transfer packets to that host. In this situation no periodic routing updates are required, offering substantial savings in bandwidth of network and battery power need for all included. A basic solution to route discovery in Ad hoc Networks is a mechanism for exploring this to the case in which source and destination may not be inside the range of each other. One possible solution is to forward a request packet but to send the request utilizing some form of broadcasting, for reaching other mobile hosts beyond the senders transmission range. As the request broadcasts, every host appends its own address to route being recorded in the packet, before forwarding the request on to its neighboring nodes. When achieving a request, if host detects its own address already stored in the route, since, it drops the copy of the request and does not forward that copy further. However some mobile hosts may be inside the transmission range of each other, although there may be some duplicate copies of every request forwarded. To highly eliminate these duplicates, every request should consist a unique request id from the real sender.

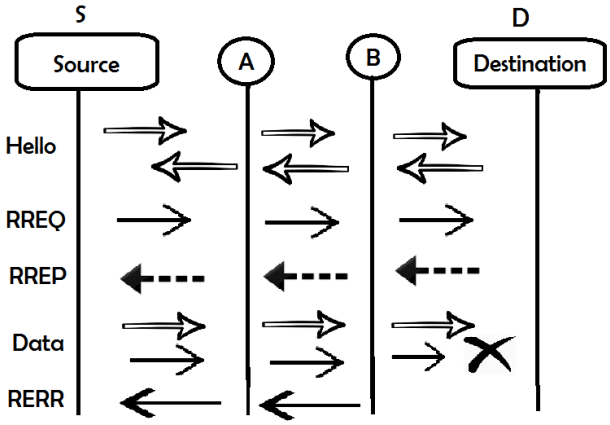

Fig3: Route discovery in AODV Protocol

A.ROUTE REQUEST MECHANISM

Every host keeps a cache providing the request id and sender address of recently sent requests, and drops a request instead of propagating it if it has already sent a current copy of the same request id. Hence every host will only forward the first copy of every request that it obtains. This will generally be the copy that came to it along the shortest route from the real sender, and this is most useful in discovering the shortest path to the final destination. This mechanism could easily be extended, though, to involve the path length in the request id cache and to forward a later copy of the same request if it some how reached over a shorter path as compared to early copy. Restricting the maximum no. of hops over which any route discovery packet can be forwarded, can hence further decrease the no. of duplicate requests sent. When processing a obtained route discovery request instead of sending it if it is not the request target and if the route stored in the packet has already arrived the maximum length. When the query packet ultimately arrive the

destination host, the entire route from the real sender to this host will have been stored in the packet. For using to the real sender, the destination host may try to reverse the stored route to arrive to the real sender, or may utilize the same route discovery mechanism to determine a route back to the real sender. The route from the real sender to this target should be returned to the sender in new query packet utilized for its own route discovery; this route discovery exchange between the two end mobile hosts could optimally be piggybacked on the first data packets forwarded between them.

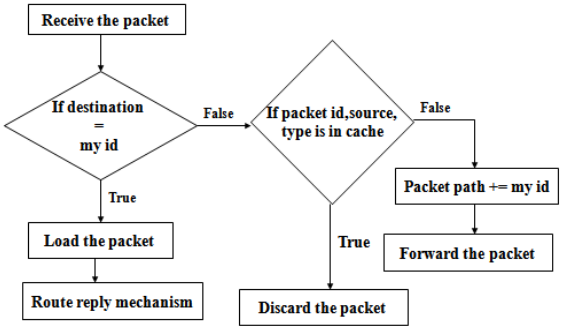

Fig 4: Route Request Mechanism

When host obtains the route request packet it processes the request with respect to the following steps:

• If the pair "initiator address, request id" for this route request is discovered in the hosts list of currently viewed requests, then drop the route request packet and do not process it further.

•Otherwise, if the address of host is already listed in the route record in the request then drop the route request packet and does not process it further.

• Otherwise if destination of the request matches machines own address, then the route record in the packet consist the route by which the request arrived this host from the route request initiator return a copy of this route in a route response packet to the initiator.

• Otherwise add this hosts own address to the route stored in the route request packet, and resend the request. The route request hence propagates Ad – hoc Network run until it arrive the destination host, which then give response to the initiator. The original route request packet is obtained by those hosts inside the wireless transmission range of initiating host, and every host sends the request if it is not the destination and if the request does not appear to this host to be duplicate. Dropping the request because the hosts address is already stored in the route record ensures that no single copy of the request can forward around the loop. Also dropping the request when the host has currently viewed one with the same "initiator address, request id" eliminates later copies of the request that reach at this host by a different route.

B. ROUTE REPLY MECHANISM

For returning route response packet to the route discovery initiator the destination host must have a route to the initiator. If the target has an entry for this destination node in its route cache, then it may forward the route response packet utilizing this route in the same manner as is utilized in forwarding any other packet which is depicted in Figure (5) Otherwise the destination may reverse the route stored from the route request packet, and utilize this route to forward the route response packet. This since, needs the wireless network communication between each of these pairs of hosts to work equally good in both directions, which may not be true in many environments or with many MAC level protocols.

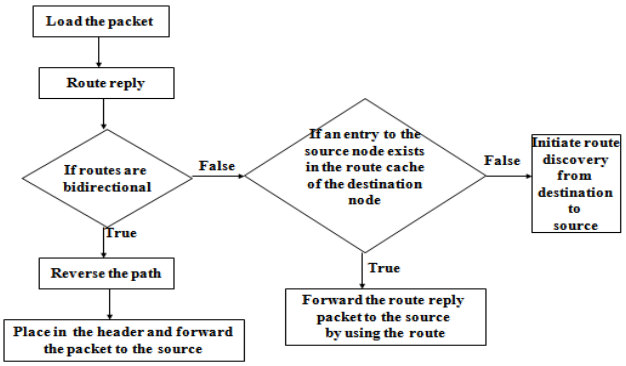

Fig 5: Route reply mechanism

C. ROUTE MAINTENANCE

Traditional routing protocols combine route discovery with route maintenance by continuously forwarding the general periodic routing updates. If status of a router or connection changes, the periodic updates will finally reflect the modifications to all other routers, presumably resulting in the computation of new paths. With the separate route discovery mechanism a connection or route going down would instead lead the route to mysteriously stop working with no feed back to the sender. The route maintenance protocol role is to offer this feedback, and to permit the route to be altered or a new route to be found in this situation. In an Ad hoc Network, a route may also stop working if one or more of the mobile host along the route simply propagates. In some wireless networks, route maintenance can be offered with very little overhead. However wireless networks are inherently less flexible as compared to the wired networks. Some wireless networks use hop by hop acknowledgement at the data link level for providing early detection and retransmission of discarded or damaged packets. In these networks, the issue of route maintenance is quite east, however at every hop, the sender can find if that route hop is still working. If the data link level reports a transmission issue for which it cannot recover, all that is required is to inform this error back to the real sender to cause the host re-invoke the route discovery mechanism to discover a new route. It

may also be possible for the intermediary host observing the error to instead utilize the route discovery mechanism itself to explore the available route on the correct packet.
If the wireless network does not support these lower level acknowledgements, an equivalent acknowledgement signal may be existed in some environments. After forwarding a packet to the adjacent hop mobile host, the sender may be capable to listen that host transmitting the packet again, on its way further along the route. As a last resort, a bit in the packet header could be involved to permit a host transferring a packet to request an explicit acknowledgement from the adjacent hop recipient. If no other acknowledgement signal has been obtained in some time from the adjacent hop on some route, The host could utilize this bit to cheaply probe this hop status on the route.
While route is in usage, the route maintenance mechanism monitors the route operation and reports the sender of any routing errors. Some wireless networks use hop by hop acknowledgement at the data link level for providing early detection and retransmission of dropped or damaged packets. In these networks, route maintenance can be easily offered, however at every hop the host transmitting the packet for that hop can detect if that hop of the route is still working. If the data link level reports a transmission issue for which it cannot recover, this host forwards a route error packet to the real sender of the packet finding the error. The route error packet consist the hosts address at both ends of the hop in error. The host that found the error and the host to which it was trying to transmit the packet on this hop. When a route error packet is obtained, the hop in error is eliminated from this hosts route cache, and all routes which consists this hop must be truncated at this point.
If the wireless network does not support such low level acknowledgements, an equivalent acknowledgement signal may be existed in some environments. A bit in the packet header could be involved to permit a host transmitting a packet to request an explicit acknowledgement from the adjacent hop recipient. If no other acknowledgement signal has been obtained in some time from the adjacent hop on some route. The host could utilize this bit to inexpensively probe this hop status on the route.

IV. WORKING OF AODV PROTOCOL

Ad-hoc On Demand Distance Vector (AODV) is the type of reactive routing protocol which creates the route only when a node wants to communicate with other node. In AODV protocol the route with high destination sequence number is preferred. In this protocol when a node wants to send the data packets to other node it sends directly to this destination node if it lies within its range, otherwise source node put out the RREQ packets to its neighboring nodes. The intermediate node receives the RREQ packet and takes the information about the route to destination node in its routing table. If there is no any fresh route present in the table it transfer the RREQ packets to the next neighboring node, and if there is a fresh route present then it checks the sequence number of destination node present in its table. The comparison of sequence number of destination node presents in the intermediate node and sequence number of destination node in RREQ packets takes place [4,5]. If the sequence number present in the intermediate node is higher or equal to the one present in the RREQ node then the route through this node is selected. Here this node sends the RREP packet to the source node in the same path
from where the RREQ packet comes. After receiving RREP packet source node send data packets to this node to reach the destination node [6]. The packet format of RREQ and RREP is shown in the Table I and II respectively.

Type	Flags	Reserved	Hop Count
RREQ ID(Broadcast)			
IP address(Destination)			
Sequence Number(Destination)			
IP address(Source)			
Sequence Number(Source)			

Table I: RREQ

Type	A	Reserved	Hop Count
IP address(Destination)			
Sequence Number(Destination)			
IP address(Source)			
Sequence Number(Source)			

Table II: RREP

A. OPNET: -OPNET's is normally specialized for network development and research. It is reliably utilized for communication networks study, about protocols, devices and the applications. As this is commercial service supplier it has a good graphical interface for subscriber and the graphical interface is utilized to make the network topology application and entities from the system application layer to the physical layer. Here, the object oriented programming language is utilized to generate a mapping from the graphical interface for the real implementation. The diagram below represents the graphical representation of every network nodes and the graphical output. As it has a graphical aspect, the parameter can be varied and seen the result repeatedly very easily without much hard work. This modeller is famous for network research and industry for the development. The provided programming tools and GUI interface are very useful to make the system according to subscriber need and to model the system. OPNET has

three important services as modelling, simulation and analysis. For modelling it offers good graphical interface to describe and generate all types of model protocol. For simulation it utilized different kind of advanced simulation technique to deal and address broad range of study aim. For analysis, the simulation results and data can be showed graphically in user friendly forms of graphs, charts and in statistics form for subscriber comfort.

B. Network Simulator 2 (NS2): - NS2 is the most famous network simulators. This is a discrete event modeller mainly designed for the network researchers. NS2 is the second version of NS (Network Simulator) and NS was formulated in 1989. The latest version of NS2 is broadly utilized for academic research. After that lots of packages are contributed by some non-profit groups to enhance and build it much better.

Network Simulator or in short NS2 is an object oriented discrete event driven network modeller. It was first formulated at the California-Berkely University. The programming language utilized is Tcl script and C++ language with object-oriented extension (OTcl). There is cause utilizing these two languages. C++ is very effective to design but complicated for visual and graphical implementation. OTcl is employed to fill the lap that the C++ lacks. So the integration of these two languages appears to be very efficient. Normally the C++ is employed to implement the detail simulation protocol and OTcl is employed for the subscriber to control the simulation and organize the events. The OTcl script is utilized to start the event scheduler, to establish the network configuration and to tell traffic source whether to forward or stop forwarding the packet from event scheduler. The view can easily change by the OTcl script. There is reliability that when a subscriber wish a new network object they can simply write the code utilizing the available object library and also plumb the data path from object.

C. OMNeT++: -OMNeT++ is a public source, a discrete event modeller with GUI support of component based network modeller. The primary application field of this simulator is the communication networks along with its reliable architecture it has other areas i.e. hardware architecture, IT systems, queuing network and also in business mechanism. Here the components are known as modules and programmed in C++ language. Its operating principal is same as that of Python in NS3 and OTcl in NS2. The smaller components are integrated into larger components and models utilizing high level language.

The OMNeT++ is intended particularly for the complex based architecture. Basically the reusable components are aggregated to build OMNeT++ module. The major characteristics of OMNeT++ are the modules are reusable and the modules are integrated in several ways. The key characteristic is the simulation kernel C++ class library which contains utility class and simulation kernel essential for simulation components. It has runtime subscriber environments and interface for simulation. OMNeT++ support multiple platform like it can operate on Unux, other Linux-like systems and on Windows systems.

V. VANET ARCHITECTURE

VANET architecture uses two kinds of communication devices: (1) On-board Units (OBUs) and (2) Road-side Units (RSUs). As name represents, OBU is equipped in a vehicle and RSUs are positioned on roadside. Every OBU contains a Global Positioning System (GPS) receiver, Event Data Recorder (EDR), a radar and computing platform. GPS recipient gives information about speed, geographic location, acceleration of a node and direction of movement at mentioned time intervals. EDR device stores the received and transmitted messages [3,5]. Information saved in EDR can help in recreation of an emergency/accident condition for later analysis after the happening of an event. The computing device is utilized to take suitable actions in reply to messages obtained from other nodes. Radar is employed for determining obstacles close to the vehicle. Every vehicle also has an omni-directional antenna that the OBU utilizes to use a wireless channel. An RSU is same as an OBU in that it has a computing device, antenna, sensors and transceiver. It is a static device positioned on roadside. An RSU may be equipped at road intersections or implanted in traffic-light for traffic control. It can be positioned for commercial usage also. For instance, a restaurant can utilize an RSU for advertisement of its existence. An RSU may utilize either omni-directional or directional antenna based on the kind of application. Fig 12.1 illustrates a general VANET architecture. VANET is not a pure *ad-hoc* network as an infrastructure in the form of RSUs may available in several parts of the network. Sometimes, there may not be any infrastructure on highway. VANETs provide support to two kinds of communications: (1) Vehicle-to-Vehicle and (2) Vehicle-to-RSU. A V2R communication enables vehicular safety applications, involving collision warning as well as other ITS applications i.e. high speed tolling and local traffic information for routing.

All the nodes are aware of their own motion and position details. They exchange this information with neighbouring nodes at periodic intervals. Every vehicle saves information about itself and neighbour vehicles in a local database. This database records are forwarded to neighbouring nodes and roadside resources periodically. These forwarded messages help in managing the information. Fig. 2 shows the structure of a normal forwarded message.

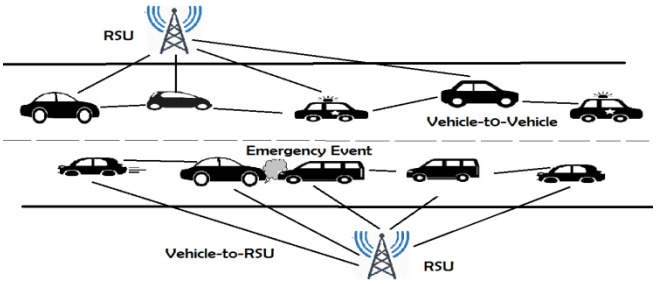

Fig 6: Example of VANET Architecture

VI. CLASSIFICATION OF APPLICATIONS

As proposed in [8], applications can be divided in the following three categories:

Safety-oriented applications (see Table A): they help the driver to avoid potential dangers via the exchange of information among vehicles. Collected information concern the status of nearby vehicles and road conditions. They are the most important applications because they serve to avoid accidents. They can take control of the vehicle in case of dangerous situations, as in the case of the automatic braking, or only send warning messages to drivers.

NAME	DESCRIPTION
On-coming traffic warning	It helps the driver during overtaking the maneuvers.
Vehicle stability warning	It alerts driver that they should activate the vehicle stability control system.
Post-crash notification	A vehicle involved in an accident sends warning message in broadcast to approaching vehicles.
Traffic signal violation warning	A road side unit sends message in broadcast to warn drivers of potential violation of traffic signals.
Lane changing warning	It helps drivers to perform a safe lane change.
Electronic break warning	It reports to the driver that a preceding vehicle has performed a sudden breaking.
Intersection violation warning	It warns drivers when they are going to pass over a red light.

Table A: Safety Applications

Commercial-oriented applications (see Table B): they serve to make the travel more comfortable and productive, for example, by means of the internet connection.

NAME	DESCRIPTION
Service Announcement	Restaurants and other businesses can use a roadside unit to send promotional messages to the drivers of the vehicle that they are in their communication range.
Remote diagnosis	The driver can start a wireless connection with the dealer in order to update the vehicle diagnostics information to detect possible problems
Media or map download	A vehicle can start a wireless connection with the home network or a hot-spot to downloads maps and multimedia contents.

Table B: Commercial Applications

Convenience-oriented applications (see Table C): they serve to improve the efficiency of the roads and to save drivers time and money.

NAME	DESCRIPTION
Electronic toll collect	A vehicle establishes unicast communication with a toll gate roadside unit and pays the toll without stopping.
Parking availability notification	A vehicle asks to a roadside unit for a list of available parking spaces and the roadside unit sends the list to the vehicle.
Intersection management	V2V and V2R communication allow a better intersection management.
Congested road notification	A vehicle in a congested road sends information in broadcast to other vehicle.

Table C: Convenience Applications

LITERATURE REVIEW

ZuhongFeng et al. : Here authors proposed on improved protocol Advanced-AODV algorithm based on energy model and load balancing. Authors used NS2 simulation

tool to simulate the network environment. Authors used quantitative indicators to judge the performance of the routing protocol: Packet delivery ratio, average end-to-end delay and routing load. In the simulation results, compared to AODV , Ad-AODV not only prologs the survival time of the network , but also improved the packet delivery ratio , lowers the average end-to-end delay and reduces the routing load.

WadhahAL-Mandhari et al. : In this the authors identified the effect of varying route states hold time parameters for Ad-Hoc On Demand Distance Vector and measured the degree at which the number of stations and their movement speeds affected the PDR.

Authors used OPNET modeler 11.0 for simulating the Ad-Hoc Mobile Network. The parameters used in the simulation were Active Route Timeout(ATR) , simulated time , packet size , bit raye , encoding type , packet interval arrival time. Authors simulation result indicated that at the default value of ART parameters , the PDR values were very low especially at high station movement speeds. Simulation results also showed that to use low ART values in a multi-hop wireless network to reduce the end-to-end delivery.

MeenakshiTripathi et al. : In this , authors analyzed the performance of AODV by varying the value of Active Route Timeout(ART) from one second to several seconds with the mobility of sensor nodes. Authors simulated the wireless sensor network using Qualnet 5.0 simulation. Parameters used for the simulation were number of sensor nodes , number of mobile nodes , channel frequency , data packet size , path loss model , speed. Parameters condidered for simulation were packet delivery ratio, average end-to-end delay , throughput , jitter. Simulation results showed that if the active route timeout is exactly 1 second then it provide maximum throughput result also indicated that if active route timeout from 1 second to 5 seconds, it gave almost some throughput.

Sangeeta Kurundkar et al. : Here authors presented an improved AODV(I-AODV) protocol. Authors used NS2 simulator to compare performances of AODV and I-AODV, Parameters used by authors were packet size , number of nodes , PDR , delay , node speed. According to authors simulation results , by using these techniques in routing protocol. We can reduce the energy and end-to-end delay about 7% to 24%. I-AODV is useful for applications in which nodes are mobile and packets of varying sizes are to be sent.

AshutoshLanjewar et al. : Here authors , concentrated on reducing the factors such as cost , end-to-end delay , network loads , packet loss in AODV routing protocol. Auhors used NS2 simulator for simulation purpose. Simulation parameters used by authors were number of nodes, routing protocol , traffic source , area , mac type. The simulation result indicated that as the number of nodes was increased, advanced AODV still performed well and yielded better throughput level with less delay and consumed less energy.

CONCLUSION AND FUTURE SCOPE

VANET is a promising technology and with the substantial advancement in wireless technology, vehicles are becoming a vital part of global network. VANET will not only provide life saving applications but will also become a powerful communication tool for users. Here, focus is paid on basic architecture of VANET, routing, simulation, attack and application. Fulfilling the requirements and facing challenges will result in an efficient communication tool which can also provide life saving tools to the users [6]. If improved it can give better results than other mobile ad hoc network. Vehicles can be designed in a way that they possess learning abilities so as to have perception of potential dangers and to modify vehicle's behaviour consequently. It can help vehicle to take decisions from it's past experience.

REFERENCES

[1] C. Sommer, Z. Yao, R. German, and F. Dressler, "On the need for bidirectional coupling of road traffic micro simulation and network simulation," in Mobility Models '08: Proceeding of the 1st ACM SIGMOBILE workshop on Mobility models. New York, NY, USA: ACM, 2008, pp. 41–48

[2] Zhao and G. Cao, "Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks," Vehicular
Technology, IEEE Transactions on, vol. 57, no. 3, pp. 1910 – 1922, may 2008.

[3] Q. Chen, D. Jiang, and L. Delgrossi, "Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications," in Vehicular Networking Conference (VNC), 2009 IEEE, oct. 2009, pp. 1 –8.

[4] Y. H. Choi, R. Rajkumar, P. Mudalige, and F. Bai, "Adaptive location division multiple access for reliable safety message dissemination in vanets," in Wireless Communication Systems, 2009. ISWCS 2009. 6th International Symposium on, sept. 2009, pp. 565 –569.

[5] Biswas, S., & Misic, J to Privacy-preser. (2013). "A Cross-layer Approach ving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192

[6] Pradweap, R. V., & Hansdah, R. C. (2013). A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET. In Information Systems Security (pp. 314-328). Springer Berlin Heidelberg.

[7] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen,Angela Irwin, Aamir Hassan," *Vehicular Ad hoc Networks(VANET):Status, Results, Challenges*". Springer Science, Business Media.2010

[8] Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan *Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.*

[9] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of

service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[10]Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.

[11] Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," *Vehicular Technology Conference, 2011 IEEE 73rd* , vol., no., pp.1,5, 15-18 May 2011

[12] Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," *Communications and Signal Processing (ICCSP), 2013 International Conference on* , vol., no., pp.1170,1174, 3-5 April 2013

[13] Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* , vol., no., pp.1,5, 26-28 July 2013

[14] Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[14] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," *Communications Letters, IEEE* , vol.18, no.1, pp.110,113, January 2014

[15] Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on* , vol., no., pp.26,27, 24-26 Sept. 2014

[16] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[17] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on* , vol.3, no., pp.261,265, 25-27 May 2012

[18] Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on* , vol., no., pp.152,157, 10-12 Feb. 2014

[19] Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," *ELEKTRO, 2014* , vol., no., pp.424,429, 19-20 May 2014

[20] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian* , vol., no., pp.135,140, 26-28 Nov. 2014

[21] Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on* , vol., no., pp.792,797, 5-7 March 2014

[22] Mehta, K.; Malik, L.G.; Bajaj, P., "VANET: Challenges, Issues and Solutions," *Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on* , vol., no., pp.78,79, 16-18 Dec. 2013

[23] Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," *Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian* , vol., no., pp.1,6, 7-9 Nov. 2012

[24] Shuai Yang; Rongxi He; Ying Wang; Sen Li; Bin Lin, "OPNET-based modeling and simulations on routing protocols in VANETs with IEEE 802.11p," *Systems and Informatics (ICSAI), 2014 2nd International Conference on* , vol., no., pp.536,541, 15-17 Nov. 2014

[25] Sadeghi, M.; Yahya, S., "Analysis of Wormhole attack on MANETs using different MANET routing protocols," *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on* , vol., no., pp.301,305, 4-6 July 2012

[26] Jhaveri, Rutvij H.; Patel, Ashish D.; Dangarwala, Kruti J., "Comprehensive Study of various DoS attacks and defense approaches in MANETs," *Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on* , vol., no., pp.25,31, 13-14 Dec. 2012

[27] Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, *Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a* , vol., no., pp.1,6, 25-28 June 2012

[28] Jie Li, Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" , IEEE Transactions on Parallel and Distributed Systems, 2012

[29] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," *Computers, IEEE* Transactions *on* , vol.63, no.2, pp.510,524, Feb. 2014

[30] Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on* , vol., no., pp.611,615, 8-10 Aug. 2012

[31] Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survay and taxonomy," *Communications Surveys & Tutorials, IEEE* , vol.11, no.4, pp.19,41, Fourth Quarter 2009

[32] Sun Xi; Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," *Wireless communication, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1,4, 12-14 Oct. 2008.