I. J. Computer Network and Information Security, **2016, 2, 49-55**
Published Online February 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.02.06

Enhanced Direction Based Hazard Routing Protocol for Smooth Movement of Vehicles

Needhi Lathar
Chandigarh Engineering College/Department of IT, Landran (Mohali), 140307, India
E-mail: nidhilather999@gmail.com

Shashi Bhushan and Manish Mahajan
Chandigarh Engineering College/Department of CSE, Landran (Mohali), 140307, India
E-mail: {shashibhushan6, cec.manish}@gmail.com

Abstract—Vehicular Ad hoc Network involves the movement of vehicles and the communication between them for their security. VANETs have many application areas. One of main applications of VANETs is to improve the driving safety. In various safety related applications, vehicular nodes constantly communicate with roadside equipments. Road Side Units (RSUs) can sense the real time information about road conditions, animals straying and road blocks and passes all this hazardous related information to the vehicles approaching in its range. These alert messages enable the driver to take timely decisions in preventing from accidents or delays in information delivery. In this paper, Enhanced Direction based Hazard Routing Protocol and Ad Hoc On-demand Distance Vector protocols are used to avoid prevent vehicles from collision and to increase the coverage range of VANETs. These issues are resolved by bypass routing and a synchronized clock maintained with the RSUs respectively. To solve the issues and make the system more reliable we propose the roadside wireless sensor nodes along with vehicular nodes in the network. The RSUs are fixed at some distances and communicate with wireless sensors attached at vehicular nodes.

Index Terms—VANET, Bypass Routing, Collision Detection, Hybrid connectivity, Flexible service.

I. Introduction

Vehicular Ad-hoc Network is a wide area being researched everywhere and a future technology of globe. It aims to revolutionize movement in massive scale through the implementation of road safety and management architectures. The underlying architecture is used to convert each vehicle into wireless human action entity, thence increasing driver's perception of horizon on the far side of the reach of human eyes. The targeted goal is to make sure that the travelling is a safer pass to generate early warnings and timely response to the things. However, to extend penetration, individual categories of applications like control and provision of motion picture are introduced. These goals need backend Infrastructure property to any or all nodes. The employment of infrastructure varies from design to design and service to service. Presently an outsized range of nation can be performed on VANET architectures and their implementations, either on individual basis or together with regional regulative authorities and automobile makers.

Vehicular Ad-hoc Networks are specific sort of mobile networks wherever nodes are area unit vehicles and no mounted infrastructure is required in managing the association and routing them. Vehicles in VANET area unit are self-organized and self-configured due to "ad hoc" routing protocols which manage message exchange. These characteristics build technology to make applications for safety functions or to just avoid traffic jam. Vehicles are designed to access internet once an entrance is encountered. Road side Unit or Access purpose may well be used as gateways in an exceedingly hybrid VANET to figure out intermediates between vehicles and different networks. Typically cars move at high speeds and this behavior reduces transmission capability, making conditions like:

1. Vehicular Ad-hoc Network permits the downloading of packets once vehicles cross access point (AP).
2. Highest nodes congestion in significant traffic conditions has an effect on protocol performance.
3. Highest level of packet losses Measurements of UDP and communications protocol transmissions of vehicles in exceedingly road passing ahead of AP moving at different speeds, report losses on order of 50-60% reckoning on nominal causing rate and vehicle speed.
4. Every node should be addressed unambiguously.
5. There are several Surrounding obstacles such as traffic jams, tunnels, lakes etc. It may interfere with transmission signal.
6. Ability with different networks has been achieved. Nodes are able to exchange information with individual sorts of networks which particularly support mounted science addresses.
7. Once traffic density is low, distance between vehicles will reach many kilometers on the far side vary of the wireless link.

In VANET systems, every vehicle takes the role of sender, receiver, and router to broadcast information to network or transportation agency that uses information to make safe and free-flow of traffic. For communication to occur between vehicles and edge Units, vehicles should be equipped with the form of radio interface or aboard Unit that allows short-range wireless ad-hoc networks to be fashioned. Vehicles should be fitted with hardware that allows position information like international Positioning System or a Differential international Positioning System receiver. Fixed RSUs can be connected to backbone network to facilitate communication. The amount and distribution of edge depends on communication protocol to be used. For instance, some protocols need edge units to be distributed equally throughout the road network; some need edge units at intersections, whereas others need edge units at region borders. However it is safe to assume that the infrastructure exists to an extent and vehicles have access to an impractical need that vehicles have wireless access to edge units forever. The unit potential communication configurations make the network as intelligent transportation systems.

A. Characteristics of VANET Networks

VANETs share characteristics with typical ad-hoc networks by sensing elements of network like self-organized and lack of the central management. VANET contains distinctive challenges for the effective look of communication system and its protocol security. These challenges include:

Probably high range of nodes: For the technical basis of visualized intelligent installations we have a tendency to expect that an outsized portion of vehicles are equipped with all the communication capabilities for conveyance communication. Taking in addition, the potential road-side units under consideration, VANETs must be scalable with awfully high range of nodes.

High quality and frequent topology changes: Nodes probably move with high speed. Hence in bound eventualities like once vehicle pass one another, the length of your time that continues to be for exchange of information packets is quite little. Also, intermediate nodes in an exceedingly wireless multi-hop chain of forwarding nodes will move quickly.

High demand on application of information delivery: Important VANET applications area unit for traffic safety is used to avoid road accidents; probably as well as safety of life. These applications have high necessities with real time relevancy and reliability. An end-to-end delay of even seconds will render safety information mindless.

No confidentiality of safety information: For safety application, the information contained in an exceedingly message is of interest for all road users and thence not confidential.

Privacy: Communication capabilities in vehicles may reveal information regarding the driver/user, like symbol, speed, position and mobility pattern. Despite the necessity of message authentication and non-repudiation of safety messages, privacy of user's and driver's ought to be revered above all location privacy and obscurity.

B. Threats to Accessibility

The following threats to the provision of vehicle-to-vehicle and vehicle-to-roadside communication are identified:

Denial of Service Attack: DoS attacks may be meted out by network insiders and outsiders and renders the network out of stock to authentic users by flooding and jam with probably harmful results. Flooding the management channel with high volumes of unnaturally generated messages, the network's nodes, aboard units and edge units cannot sufficiently method the excess information.

Broadcast Tampering: an internal wrongdoer could inject false safety messages into the network to cause harm, like inflicting an accident by suppressing traffic warnings or manipulating the flow of traffic around a selected route.

Malware: The introduction of malware, like viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks area unit a lot leading probably to be meted out by a rapscallion business executive instead of a outsider and will be introduced into the network once the aboard units and edge units receive code and computer code updates.

Spamming: The presence of spam messages on VANETs elevates the chance of magnified transmission latency. Spamming is formed tougher to regulate thanks to the absence of a basic infrastructure and administration.

Region Attack: A region is made once nodes refuse to participate within the network or once a longtime node drops out. Once the node drops out, all routes it participated in area unit will be broken resulting in a failure to propagate messages.

C. VANET Applications

VANET application may be categorized into following classes:

1. VANET provides present property on the road to mobile users.
2. It provides economical vehicle to vehicle communications that allows the Intelligent Transport System. ITS include style of applications like cooperative traffic watching, management of traffic flows, blind crossing and collision interference.
3. Comfort application is the application which permits the traveler to speak with different vehicles and with net hosts that improves passenger's comfort. For instance, VANET provides internet property to conveyance nodes whereas with the movement in order, the traveler will transfer music, send emails, watch on-line movies etc.

II. Related Work

Samara, G. et al. (2015) [2] described about Vehicular ad hoc Networks which have been induced in each business and domain. In necessary elements of transportation, Vehicular ad hoc Networks are used in rising road safety, control and business applications. Coverage issues are the number of necessary considerations in Vehicular ad hoc network. Road Side Units play vital role within the Vehicle-to-Infrastructure communications. Among all of coverage types, coverage is intended for driving-assistance and business promotion in Vehicular ad hoc Networks. This type of coverage focuses on covering important regions with high traffic flow or jammed vehicles.

Kumar, R. et al. (2015) [4] proposed that the Vehicular ad hoc Network is a sort of sophisticated task. AODV is utilized in topology based routing protocol for Vehicular ad hoc Network. Throughout the route of discovery process, AODV broadcast route message. It creates various unused routes between supply and destination nodes. To resolve this issue, this paper proposes genetic algorithm-based coverage with applied math analysis which aims at geometrical attributes of road networks, movement patterns of the vehicles and resource limitations. By taking scale of road segments into consideration, coverage rule gives buffering operation to different kinds of road topologies.

Mohammad, S.A. et al. (2015)[6] projected that the RSUs in Vehicular ad hoc Networks will enhance timeliness of assortment and the dissemination makes it attainable to perform coordinated path coming up for a gaggle of vehicles. To enhance standard of expertise, a point-to-point-based Vehicular network can be deployed for a better transmission delivery but it may expertise giant transmission delay. Hence, to scale back end-to-end transmission delay, taxis or buses relays to assist in delivering the information through the cellular network of public transportation.

Gajbhiye, V.A. et al. (2013)[10] planned about the Vehicular ad hoc Network that could be a style of ad hoc network during which the moving vehicles act as nodes. One application is the use of Vehicular ad hoc Networks to enhance driving safety. In any safety related application, the Vehicular nodes ought to perpetually communicate with one another and therefore with the margin equipment. For e.g., the margin units sense real time information concerning road conditions, road blocks or animals lost on the road and passes the message to the approaching vehicles. It plays a vital role in keeping the network connected and to guarantee message transmission.

Mejri, Nidhal, M. et al. (2014) [13] discussed that the Vehicular ad hoc Network could be a classification of MANET during which vehicles act as mobile nodes and provides a distinct approach to Intelligent transport System. Vehicular ad hoc Network is an associate rising space for transportation which might end in accumulated traffic safety, collision warning through exchange of messages via wireless media. Economical routing protocols are required for economical communication among vehicles.

Sultanet, S.A. al. (2014)[15] told about Vehicular cloud which have to be considered as sensible vehicles that offers numerous resources to neighboring vehicle's remote users via network of RSUs and outline a brand new thought STAR as vehicle that offers mobile cloud services on road. This paper explains the use of vehicles and square measure a thought as backbone of network on which a lot of wireless devices are mounted. However, generally RSUs don't seem to be out there in this case additionally there's no drawback as a result of ad hoc network.

Berlin, M.A. et al. (2014)[15] proposed a Direction based Hazard Routing Protocol (DHRP) for vehicles to transfer information about the road hazards like landslides, tree falls, snow pile ups, accidents etc. This work focused on transferring information in case of sparse traffic. It is also proposed that the RSUs are responsible for the fast and timely delivery of the messages.

III. Experimental Design

A. Protocol Description

To overcome the problem of coverage and connectivity, EDHRP and AODV protocols can be used to improve the VANETs. The hybrid connectivity based model will maximize to reach the desired coverage to offer the RSU-to-node and node-to-node architecture, where the not-in-coverage nodes can be connected to the nearest nodes, which are connected to nearest RSU. The not-in-range nodes do not have node-through connectivity to RSU which should be taken into account. Also transmission range is the major problem, where RSUs need to be optimized for smoother functioning and maximum coverage. The RSU architecture must be well connected, which can be solved by using the well-connected RSU architecture. Also the broadcast message can be stored in the unicast trigger, which will send a copy of the broadcast message to the newly registered nodes in the RSU architecture. This will solve the problem of transmission range as well as the coverage and inter-connectivity between the VANET nodes in the RSU architecture.

AODV Routing Protocol

AODV routing protocol is used for routing which establishes a route to a destination only on demand. AODV routing protocol uses a broadcast route discovery mechanism and dynamically establishes the route from source to destination for sending HM. Selective Forwarding can happen only if the highway has enough vehicles to forward the HM and this procedure minimizes network overhead and improves reliability of the transmission. If there are no other vehicles on the highway, it would not be possible for the Hazard Observer to locate a forwarder node. Then one of the following two things can happen: in the first instance,

Hazard Observer would take a U turn and proceed back in the direction from which it originally came. When it reaches the communication range of any RSU, it would receive the HM and reply with the hazard message. In the second instance, it could proceed further in the same direction in the opposite lane and send hazard message to the corresponding RSU. Some features of AODV are listed below:

1. An up-to-date path to the destination because of using destination sequence number.
2. It reduces excessive memory requirements and the route redundancy.
3. AODV responses to the link failure in the network.
4. It can be applied to large scale adhoc networks.

Enhanced Direction based Hazard Routing Protocol (EDHRP)

In this proposed methodology, Enhanced Direction based Hazard Routing Protocol (EDHRP) is used. In this, messages are sent into high zone with little increase of maintenance cost. EDHRP is enhanced protocol of DHRP for safely delivery of hazard messages. The biggest challenge for VANETs is when the traffic is sparse. In that case, EDHRP provides the hazard related information to all nodes via RSUs. Instead of flooding the entire data, only the valuable information is sent to the nodes and false information is rejected. RSUs broadcasts the hazards related message to all the nodes only once and if somehow any node disconnects and could not get the message; in that case, RSUs keeps an updated table which have entries for all the connected or disconnected nodes and thus if any node disconnects then RSU re-sends message to that particular node only after the connection is established again. Thus, network load is highly reduced and performance is greatly increased. It provides messages regarding collision, when a fix hazard is blocking the way, and Sybil attack, when fake hazard is created by some prankster. It intimates the node to change their route safely at an interspacing distance of 20 meters between the node and the hazard. It also helps to join the nodes which are out of any RSU's range by connecting them with the one of the nodes among the in-range nodes. Thus information is passed as RSU-to-node-to-node structure. RSU decides the edge node which is in its range and nearest to the out-of-range node. If somehow that edge node fails, RSU gives this connecting responsibility to another node which is nearest to the out-of-range node.

For the connectivity of out-of-range nodes, EDHRP uses the concept of relay nodes where a client node can be connected to server by making use of some intermediate nodes. Its concept can be easily understood by the concept of a computer making request for a web page to its server. Sever can be at a very large distance; so, server uses intermediate nodes to make a reply route for the client. Those intermediate nodes are called as relay nodes. EDHRP uses the same concept by making in-range nodes as the relay nodes and connects out-of-range nodes with RSU.

According to our protocol, three types of nodes can be used in network. Hence, every type of node's zone maintenance cost is different than each other. In case of EDHRP, route searching process of routing is same as ZRP with R=2 hops, therefore, maintenance overhead of network is lower than ZRP. In EDHRP, Node Identification Process includes the identification of nodes based on the signal power. Various protocols assume that each node knows about its neighbors. The advantage of NIP is to identify every node type, neighbors and ranges in time to discover its neighbors. Each node contains its own zone which depends on the signal power, so proposed protocol's network zone is dynamic. The EDHRP is proposed for large ad-hoc networks same as ZRP.

B. Research work

For identifying the neighbors, distance is the major issue which has to be known by nodes. All nodes use a distance calculation formula so that they can know all their surroundings well and that formula is:

$$\sqrt{(X1 - X2)^2 + (Y1 - Y2)^2} \quad (1)$$

where $(X1, Y1)$ are the coordinates of node 1 which is information seeker and $(X2, Y2)$ are the coordinates of node 2 which can be a hurdle.

The distance calculated between two different positions of a node is known as displacement which can be calculated by the following formula:

$$\sqrt{(X - X')^2 + (Y - Y')^2} \quad (2)$$

where (X, Y) is the position of node at time interval t1 and (X', Y') is the position of same node at time interval t2.

Point of hurdle is the collision situation whose vertices can be defined as (X, Y). And, a node is declared as collision or point of hurdle only if it does not share its location information with the requesting nodes. Algorithms which are used to detect any hurdle which can be the reason for collision are given in the paper [16] which makes routing of vehicles smoother.

Table 1. Simulation Parameters used in NS2

Name of parameters	Value
Number of RSUs used	6
Traffic Density	5-20 Vehicles
Protocol	AODV, EDHRP
Hello Interval	5ms
Road Scenario	Single Lane and Multilane
Transmission Range	250 m
Medium Access	MAC
Simulation Time	400 ms
Road Block	Single and Double Lane
Vehicle Speed, S	36 km/hr, 72 km/hr, 108 km/hr
Interspacing between Vehicles	20 m

IV. Results

The simulation has been attained in form of various performance parameters that includes End-to-end delay, Packet Loss, Throughput, Packet Delay Ratio and Network Load. Packet loss increases the retransmissions or rebroadcasting or flooding and hence, it leads to the increase in network load that ultimately provides a rise to end-to-end delay and makes all the nodes to wait for the information delivery. The proposed work has been entirely based upon detection and update of hurdles in vehicle paths that are responsible for flooding data and deliver wrong information within the VANET cluster. The aim of this research is to lower the data volume during detection and updating periods in comparison with existing schemes so that connected and disconnected nodes can be identified earlier and handled carefully at the starting stage and if necessary, can intimate all the other connected nodes about the disconnected one, and declaring that node as a hurdle, if necessary. The proposed model has been designed with the communication efficiency, which controls the data volumes during the proposed work simulation. All the parameters in graphical form are shown below:

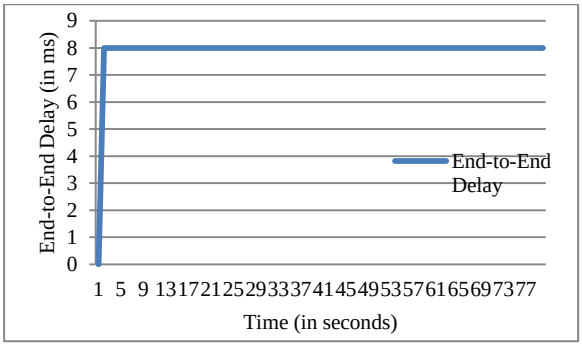

Fig.1. End-to-End Delay

The transmission delay is the parameter which indicates the total time taken by a packet to travel across the transmission link. The delay is added on the constant rate of 8 microseconds in the given simulation, which indicates the ideal data transfer across the given simulation. The transmission delay indicates the network latency caused due to the load across the path. The above graph indicates the consistency of the proposed model in delivering the data toward the sink node.

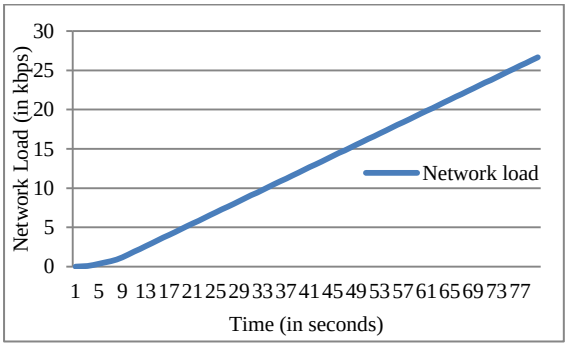

Fig.2. Network Load

The network load is the parameter which indicates the processing load over a node on a given time. The load is generated due to the data volume coming across the node in the form of the traffic flow which may contain rebroadcasted messages, flooding and wrong information to increase the load of the network. The main culprit which can effect this parameter is the person with wrong thoughts and can be termed as pranksters which intentionally increases the load. The proposed model is having the network load of 27 kbps at the peak traffic volumes. The network load is increased in the cluster as the data volume rises in the VANET cluster.

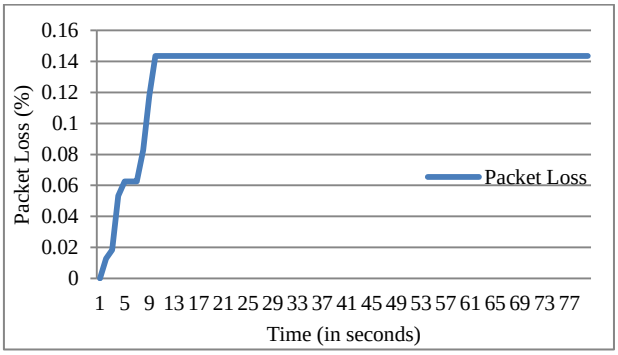

Fig.3. Packet Loss

Packet loss is the parameter which indicates the loss of data across the transmission link. Lower is the packet loss, the performance is considered stronger and stable. The packet rate in the proposed model is extremely low in the proposed model, which is recorded less than 0.14 percent data.

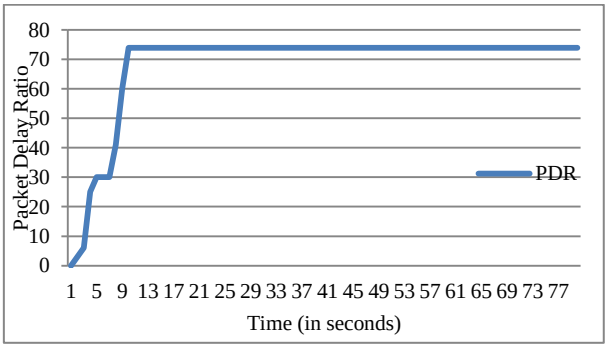

Fig.4. Packet Delay Ratio

The packet delivery ratio indicates the successful delivery of the data across the given path between the two nodes in the VANET cluster. The packet delivery ratio rises in the proposed model during the convergence mechanism and becomes consistent afterwards. The higher packet ratio indicates the healthy performance of the VANET cluster.

Throughput is the parameter used to calculate the data handling capacity of the network on a given interval. The high Throughput indicates the capacity to transfer large volumes of data between the two nodes on a given interval. The throughput in the proposed model is consistent at approximately 0.05 kbps, and accounts for the healthy performance of the proposed model in

delivering the data.

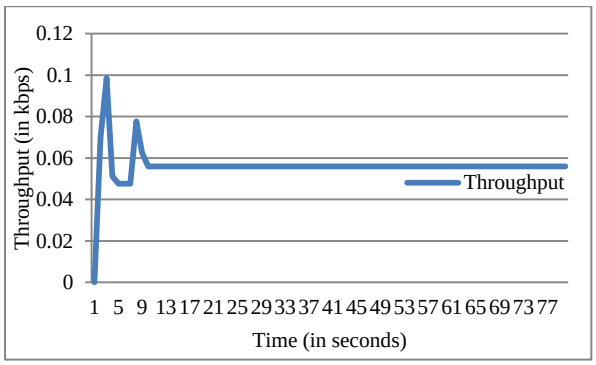

Fig.5. Throughput

V. Conclusion and Future Scope

According to the proposed model which has been designed for automatic driven vehicle based on VANETs which is capable in protecting the nodes against collision or hurdles produced by hazards like land sliding, tree falling, or other natural or un-natural obstacles reasons. The proposed model is capable to solve the distance connectivity problems through the Sybil attacks. The proposed model can be evaluated on the basis of several performance parameters. The proposed model performed better than previous existing models. The experimental results have proved its efficiency which obtained by EDHRP and AODV. With the help of EDHRP, network overhead is highly reduced and high reliability can be achieved. The protocol has been implemented and tested using NS2.35 simulator for transmission range of 250 meters and after connectivity of the out-of range nodes, the distance covered has increased up to 500 meters. The proposed model enhanced for the security of extended transmission range links through the one-hop nodes. Also the more bypass routing methods can be applied to the real time VANET application of the proposed model to create a highly robust and flexible security and movement management model.

Acknowledgement

We would like to thank all our professors in our respective departments to help and guide us in the ways we needed to get success in this field of research. Without their keen professional insight and critical suggestions, this research would not have been possible. We would like to thank all lab maintenance staff for providing assistance in various hardware and software problems encountered during the course of my thesis. We must make special mention of all the faculty members of information technology Department for their co-operation and assistance for providing such a great academic environment.

Finally, thanks to all our friends for their support and suggestions.

References

[1] A. Festag, P. Papadimitratos, T. Tielert, Design and performance of secure geocast for vehicular communication. IEEE Transactions on Vehicular Technology, Vol. 59, pp: 2456–2471, April 2015.

[2] G. Samara, W.A.H. Al-Salihy, R. Sures “Security issues and challenges of Vehicular Ad Hoc Networks”, Proceedings of The 4th International Conference on New Trends in Information Science and Service Science (NISS), pp: 393-398, June 2015.

[3] N. Lathar, S. Bhushan, M. Mahajan, Intelligent Hazard Routing for VANETs with Point of Interest Evaluation Technique. International Journal of Computer Science and Mobile Computing, Vol. 4, pp: 116-121, June 2015.

[4] R. Kumar, M. Dave, Department of IT, M. M. University, Mullana, Haryana, India ,”A Comparative Study of Various Routing Protocols in VANET”, February 2015.

[5] S.A. Mohammad, A. Rasheed and A. Qayyum, “VANET Architectures and Protocol Stacks: A Survey” Communication Technologies for Vehicles, Lecture Notes in Computer Science, 2015, Vol. 69, pp: 95-105, January 2015.

[6] P.K. Saini, K. Bhagchandani, Y.M. Sharma,” Modern Investigation of Issues and Ad-Hoc Routing Protocols Applied To VANET”, International Journal of Engineering and Advanced Technology (IJEAT) December 2014

[7] Z. Zheng, P. Sinha, and S. Kumar, “Sparse wifi deployment for vehicular internet access with bounded interconnection gap,” Networking, IEEE/ACM Transactions on, vol. 20, no. 3, pp: 956–969, September 2012.

[8] V.A. Gajbhiye, R.W. Jasutkar, “Study of Efficient Routing Protocols for VANET” International Journal of Scientific & Engineering Research Volume 4, Issue3, March 2015.

[9] Rasheed, Asim, et al. "Fleet & convoy management using VANET." *Journal of Computer Networks*, Vol. 1, pp: 1-9, March 2015.

[10] K. Mershad and H. Artail, "Finding a STAR in a Vehicular Network", IEEE Intelligent transportation systems magazine, pp: 55-68, August, 2015.

[11] Mejri, M. Nidhal, J. Ben-Othman, and M. Hamdi. "Survey on VANET security challenges and possible cryptographic solutions." *Vehicular Communications*, Vol. 2, pp: 53-66, July 2015.

[12] Cheng, Huang, et al. "A Genetic Algorithm-Based Sparse Coverage over Urban VANETs." *Parallel & Distributed Processing Symposium Workshops (IPDPSW), IEEE International*. IEEE, March 2015.

[13] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, “A comprehensive survey on vehicular Ad Hoc network ”, Journal of Network and Computer Applications, Vol. 37, pp: 380–392, April 2015.

[14] N. Lathar, S. Bhushan, M. Mahajan, “Enhanced Hazard Routing Mechanism with Collision-Avoidance for Smooth Vehicular Movement”, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) ISSN: 2394-2320, Volume 2, Issue 8, pp. 71-76, August-2015.

[15] M.A. Berlin, and S. Anand. "Direction based Hazard Routing Protocol (DHRP) for disseminating road hazard information using road side infrastructures in VANETs." *SpringerPlus* 3, August 2014.

Authors' Profiles

Needhi Lathar did her B.Tech. in Information Technology from kurukshetra University, India in 2012 and currently pursuing M.Tech. from Punjab Technical University, India. She was born on September 9, 1991 in India. She has published papers in reputes National/International Journals and conferences. Her areas of interest are Networking and Operating Systems.

Dr. Shashi Bhushan did his Ph.D from NIT, Kurukshetra, India in 2015. Dr. Bhushan is presently working as a professor in department of Computer Science and Engineering at CEC, Landran since April 2011. He is having more than 18 years of academic and administrative experience. Dr. Bhushan has published more than 20 research papers in various National/International Journals of repute. He had also filed two patents under Intellectual Property Right (IPR) entitled "System and Method of Self Destructive Program on Privacy" and "Advance Server Protection Framework (ASPF)". He had haired the technical sessions in Technical Seminars and in National/International Conferences. He had also delivered the expert lecture in various Workshops and Faculty development Program. His areas of interest are Peer to Peer Networks, Mobile Computing and Databases.

Manish Mahajan is an Associate Professor in Chandigah Engineering College, Landran, India. He is having more than 11 years of teaching experience and more than 5 years of experience in the field of research. He has done is B.Tech. (IT) from Kurukshetra University, India in 2004 and Completed his masters in CSE from Punjab Technical University (PTU), India in 2006. He is presently pursuing his Ph.D from PTU, India. He is having more than 15 publications in reputed conferences and journals like IEEE, Springer, Inderscience etc. He had guided 32 M.Tech. students and also, attended 10 International conferences. He is the reviewer/sub-reviewer of 6 International Conferences and Journals.

How to cite this paper: Needhi Lathar, Shashi Bhushan, Manish Mahajan,"Enhanced Direction Based Hazard Routing Protocol for Smooth Movement of Vehicles", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.2, pp.49-55, 2016.DOI: 10.5815/ijcnis.2016.02.06

