# SUBGRAPH COMPLEX MATRIX BLACK HOLE PREVENTED DISSEMINATION PROTOCOL FOR VANET

R.Mounika, ME Student, Department of CSE, PSRR Rengasamy College of Engineering for Women, Tamilnadu, INDIA. mounikar0497@gmail.com.

J.Veneeswari BE.,ME., Asst. Professor in Department of CSE, PSRR Rengasamy College of Engineering for Women, Tamilnadu, INDIA. Veneeswari26@gmail.com

***Abstract - Vehicular Ad-hoc NETworks (VANETs) are composed of moving vehicles with the ability to process, store, and communicate via wireless medium. VANETs promise a wide scope of services, such as, safety and security, traffic efficiency, and others. For instance, a VANET application can detect, control and reduce traffic congestion based on data that describes traffic patterns. However, disseminating data in VANET is a challenging task, due to its particular characteristics, i.e., heterogeneous density, short-range communication, and node mobility. Since, existing protocols for data dissemination do not effectively address the high overhead. But dissemination routing are vulnerable to many security threats. One severe attack is blockhole attack, in which a malicious node forges large number of fake identities in order to disrupt the proper functioning of VANET applications. In this work, we introduce a new block hole detected dissemination protocol based on chaotic map for urban VANET scenarios. In addition, the BP-AODV is able to protect against a cooperative blackhole attack launched during the routing process and guards against the blackhole attack that might take place during the forwarding process. The BP-AODV is developed by extending the functionality of the AODV protocol along with utilizing the chaotic map features. The results also reveal that the BP-AODV can strongly guard against the blackhole attack that occurs during the forwarding process.***

**Keywords: Data dissemination, Relay Selection, TMS, Vehicular communication, Subgraph Operation.**

## 1. INTRODUCTION

The vehicular ad hoc networks (VANETs) are actually the mobile ad hoc networks (MANETs) having very high mobility in which every vehicle node is acting as a host as well as router and forwarding packets to other mobile nodes [1, 2, 3] and changing their topology very fast. Therefore, the protocols used for MANETs are not necessarily be suits to VANETs and can be optimized for providing better results. VANETs forms decentralized networks. VANETs perform the communication between the vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R), which not only enhances traffic safety but can also enable infotainment applications via multihop communication, between vehicles [4, 5]. The mobile node can send their current location information to the nodes existing at some particular location using location management protocol and can reply of their request [6, 7]. The multihop data delivery is a challenging job due to large, highly mobile and sparsely connected vehicular networks. There are some techniques based on the density of the vehicles on the particular road. It is supposed that the delay is tolerable up to some limit and [1, 8] provides the model of effective route of destination and reply from that vehicle in tolerable delay. The road side unit (RSU) is typically the buffering point or they act as a router to provide communication between vehicles. At every intersection the data packets can be transferred to the RSU and the packet will be delivered to the vehicles that can transfer this packet to the destination with minimum delay.

In vehicular ad hoc network the delivery is not only single hop but multihop delivery of data could be done and even the vehicle which is miles away from the destination can also query there request like – traffic condition in the city can be obtained by the vehicles when they are out of city. In these situation vehicle can forward their request to the other vehicles and can receive the response in some seconds or in fraction of minutes. Many data dissemination protocols [9] have been proposed to disseminate information about obstacles information, traffic conditions and mishap on the roads.

There are two type of the communication in VANETs, first in which the delay could be tolerated and in others it could not be. The data like commercial advertisements, parking condition at the parking place, remaining stock status at the commercial stores, estimated arrival time of bus at stop, schedule of the meeting etc are some of the examples where slight delay is tolerable. The prediction of available parking space information sharing model has been proposed in [10]. By using inter vehicle communication vehicles can collect traffic jam information by calculating the approximate arrival time of vehicles at any location proposed in [11]. However, these types of services are already available in 3rd generation mobile systems but these services are very costly and are not available in the infrastructure less environment or infrastructure damaged environment. The cost of vehicular ad hoc networks is very high but the facilities obtained on traffic safety, commercial applications given in [12, 13, 14] can show the requirement of VANETs. On the other hand, there are many places where slight delay may be responsible for the loss of life. Ex- During the war period vehicle may find some poisonous gases or detects some mines or any other dangerous substance or activity then it needs to forward this message to other members of the mission and save many lives. This has been expressed that with the help of the relay, carry and forward the message can be send to destination without establishing end to end connectivity. There was the problem of the efficient delivery of data. Vehicle assisted data delivery (VADD) has been proposed [1] for those vehicles whose requests can tolerate some delay on their request. As a result packet delivery ratio, data packet delay, protocol overhead was found outstanding

## 2. RELATED WORK

Existing evaluates an Efficient Multi – directional Data Dissemination Protocol (EDDP), which considers the requirements of an urban vehicular environment without requiring the extra communication overhead. We rely only on simple local data to indicate the road condition for better dissemination performance. In this paper, the design considerations of urban layout include message format, broadcast suppression mechanism, and delay control. The EDDP utilizes the properties of the received messages along with positioning information to make decisions on suppressing broadcasts, with the objective of improving coverage indifferent directions without unnecessary transmissions.

Drawbacks: Leads to the allocation of waiting times similar to several vehicles, increasing the collision probability. Each vehicle also has to transmit packets in each contact with neighboring vehicles that have not yet received this packet, increasing the overhead

## 3. PROPOSED WORK

Proposes a secure dissemination protocol called BP-AODV to overcome the security breaches related to the SAODV protocol along with the original AODV protocol. In general, the proposed protocol protects VANET routing node against black hole attack and cooperative black hole attack and specially, it remedies the black hole vulnerability of the protocols. In addition, the protocol detects malicious nodes that behave abnormally during the routing process.

### i) BLOCK HOLE DETECTION IN FLOODING FORWARD ROUTE

Like the AODV and SAODV, the proposed has a route discovery phase and a route maintenance phase. The route discovery phase of the BP-AODV protocol extends the functionality of the route discovery phase of AODV protocol to implement the challenge-response confirm pattern along with establishing up to three routes instead of one route by the AODV protocol. The route discovery phase of the BP-AODV protocol is achieved by completing three rounds or processes: Request, Reply, and Confirm.

During this round, reverse routes with the *src* are established and a challenge value *cs* generated by the *src* is conveyed to the network nodes. Specially, the *src* creates a MRREQ message together with putting parameter values (e.g., *cs*, hop count *hc*, and broadcast id bid) into corresponding fields of the message the Reply process shown in the bottom part of node is started by the *dst* immediately after receiving the *_rst* MRREQ message. During this round, a response value v calculated by the *dst* is propagated to nodes on the route paths and reverse routes with the *dst* are established.

Also, the protocol allows the receiving of only one MRREP message from the same node along with a maximum of three from different nodes. Specially, when receiving a MRREQ message, the *dst* executes a maximum of four main steps. Firstly, if the same message is previously received, the *dst* skips this step and starts the execution from the second step. Otherwise, the *dst* calculates a response value v based on Equation where the symbol b c is the Math _oor function that rounds its argument while x(n) is the Logistic chaotic map.

The Logistic map is widely employed in several applications for securing multimedia contents. The BP-AODV incorporates the Logistic map in its design to inherit its brilliant features such as ergodicity, randomness, and sensitivity to initial conditions and control parameters. Accordingly, the parameters used in calculating the response value and confirmation of the route are not fire and totally related to the src and dst nodes in each route request. In fact, the utilization of the chaotic map grants the proposed protocol more security. The chaotic value x(n) can be computed by Equation

$$v = \lfloor x(\eta) * 10^{14} \rfloor$$

Where n is a secret value randomly generated by the dst to represent the number of chaotic map iterations. x(0) _ (0; 1) and µ is (0, 4] are the initial value and the control parameter of the Logistic map, respectively. To assure the good chaotic behavior of the map, the parameter µ

Attack detection forwarding process as a second layer of defense to protect network against the blackhole attack achieved by a malicious node that behaves normally (i.e., the malicious node follows the protocol steps) during the routing process but it behaves abnormally during the forwarding process. The forwarding process starts immediately by the src after approving its routes with the dst during the routing process. During the forwarding process, when the src or any forwarding node on route paths to the dst wants to should be maintained in the range [3.5699456, 4]

Introduces a new forwarding process as a second layer of defense to protect VANET against the blackhole attack achieved by a malicious node that behaves normally (i.e., the malicious node follows the protocol steps) during the routing process but it behaves abnormally during the forwarding process. The forwarding process starts immediately by the src after approving its routes with the dst during the routing process. During the forwarding process, when the src or any forwarding node on route paths to the dst wants to forward a data packet to the dst, it selects next hop ni toward the dst based on the developed by Equation

$$n_i = \begin{cases} f(x, r) & \textit{if } y_1 \text{ to } y_r \text{ are equal} \\ 1 & 0 < x \leq \frac{y_1}{\sum_{j=1}^{r} y_j} \\ 2 & \frac{y_1}{\sum_{i=1}^{r} y_i} < x \leq \frac{y_1 + y_2}{\sum_{j=1}^{r} y_j} \\ 3 & x > \frac{y_1 + y_2}{\sum_{j=1}^{r} y_j} \end{cases}$$

where x _ (0; 1) is a random number generated by the forwarding node. r is an integer representing the number of routes toward the dst at the forwarding node and its value is 1, 2, or 3. yj is the number of received data packets from the next hop

nj associated with the jth route at the forwarding node. The function f () is evaluated by Equation

$$f(x, r) = 1 + \lfloor x * 10^3 \rfloor \bmod r$$

The function f () is used to randomly select a next hop when all next hops have the same degree of trust at the forwarding node (i.e., all values of yj are equal for 1 _ j _ r). The value of yj associated with the next hop nj provides a degree of trust for the jth route.

if the value of x ∈0:7, the 1st route is selected. Otherwise, the 2nd route is chosen. This means that the higher the trust degree of a route, the higher the chance of the route to be selected. Note that the protocol does not directly select the route of the highest degree of trust for two reasons: 1) the forwarding node increases its trust at the next hop and 2) it makes load balance between different routes.

This comes from the fact that a malicious node that performs the blackhole attack does not forward data packets (i.e., the number of received data packets from the malicious node is zero). Therefore, the degree of trust of the route through the malicious node is zero.

**ii) RELAY SELECTION**

In the relay node selection step, SCMC considers two complex networks' metrics: *i)* degree centrality, and *ii)* betweenness centrality. The degree centrality reflects the popularity of a given vertex in the graph in terms of the number of neighbors computed based on Eq. Where, *i* means the vehicle that wants to find its degree centrality, *j* represents all other vehicles, *n* is the total number of vehicles, and *a* denotes the adjacency matrix, in which the cell *aij* is set to 1 if there is connection to the node *j* and 0 otherwise.

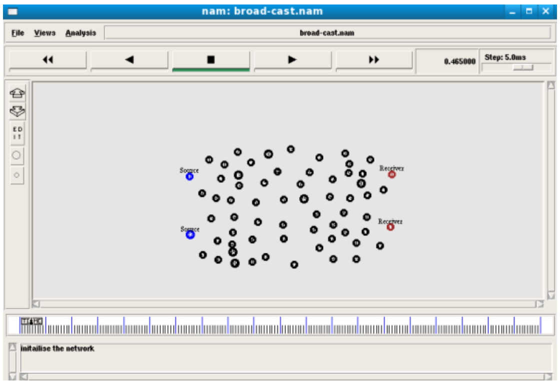
$$G(i) = \sum_{j=1}^{n} a_{ij}$$

### iii) SCMC'S OPERATION

Introduces the processing of a data message required for SCMC operation, where SCMC selects only the vehicles that are inside the AoI to relay the message *MSG*. Besides, a vehicle only performs the retransmission as soon as it is the first time it is receiving *MSG* and has been indicated as a relay node in the field *relays* contained in *MSG* which decreases the number of redundant messages and packet collisions considerably. Hence, the list of neighbors is used to create the subgraph $G\_E\_u\_$ to select the best neighbors used to continue the retransmission process., The selected relay node identifiers *ids* are included in the field *MSG*. *relays*, and then a relay scheduling time *st* that follows a uniform distribution ($st$ ∈[ 0.0, 0.05]) is established

## 4. SIMULATION RESULTS

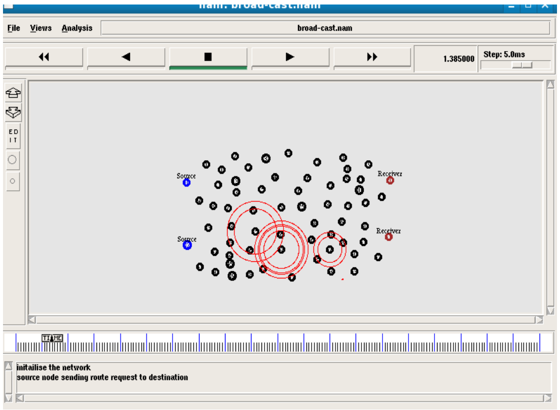
The proposed work is simulated in network simulator2 (ns2) platform



```
initailise the network
```

**Figure1.1 Node Creation & Deployment**

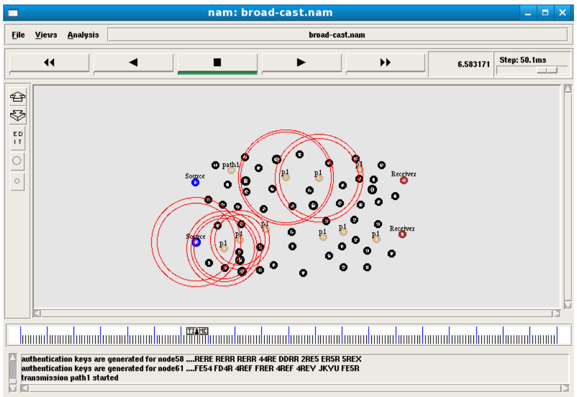
The above figure 1.1 represents node creation & deployment and corresponding protocol fetching. The following figure 1.2 shows route request initiation by identifying one hop neighbor.



```
initailise the network
source node sending route request to destination
```

**Figure 1.2 Route Request Initiation**

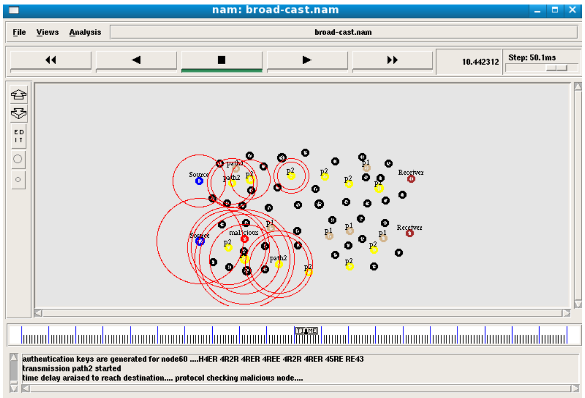
From the figure 1.2, sender to receiver node discovery and beacon signal transfer among nodes.



```
authentication keys are generated for node58 ....RERE RERR RERR 44RE DDRR 2RE5 ER5R 5REX
authentication keys are generated for node61 ....FE54 FD4R 4REF FRER 4REF 4REY JKYU FE5R
transmission path1 started
```

**Figure 1.3 Chaotic Map Operation**

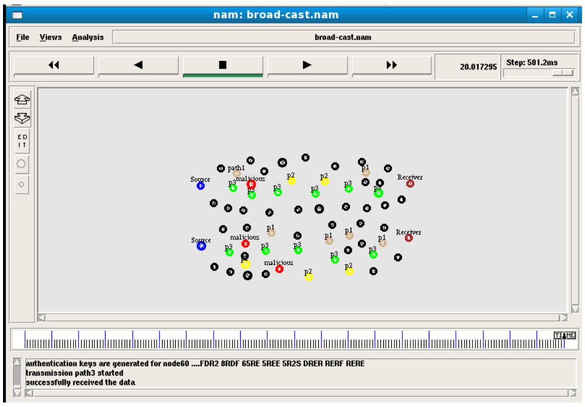
Figure 1.3 shows chaotic map operation from source to destination. Two hop neighbor identified for secure connection



```
authentication keys are generated for node60 ....H4ER 4R2R 4RER 4REE 4R2R 4RER 45RE RE43
transmission path2 started
time delay araised to reach destination.... protocol checking malicious node....
```

**Figure 1.4 Route Formation**

Figure 1.4 shows secure path identification without any malicious node



```
authentication keys are generated for node60 ....FDR2 8RDF 65RE 5REE 5R2S DRER RERF RERE
transmission path3 started
successfully received the data
```

**Figure 1.5 Attacker Node Detection**

Figure 1.5 shows secure path identification without any malicious node .The node with red colour indicates attacker nodes

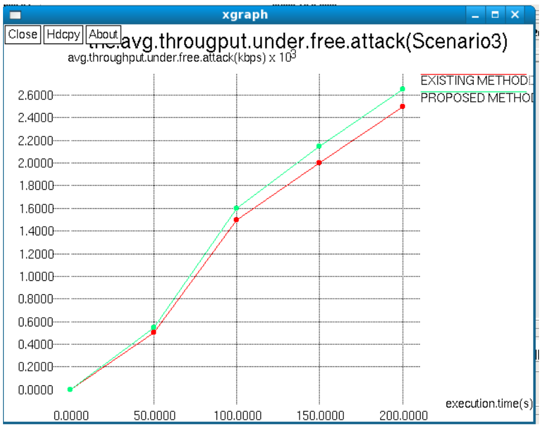


**Figure 1.6 Throughput analysis**

Figure 1.6 shows compariosn of exisiting and proposed methods.The proposed method shows higer thriughput than exisitng method

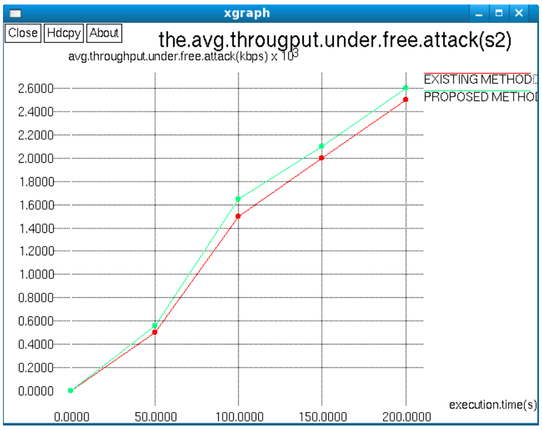


**Figure 1.7 throughput analysis**

Figure1.7 shows compariosn of exisiting and proposed methods.The proposed method shows higer accuracy than exisitng method

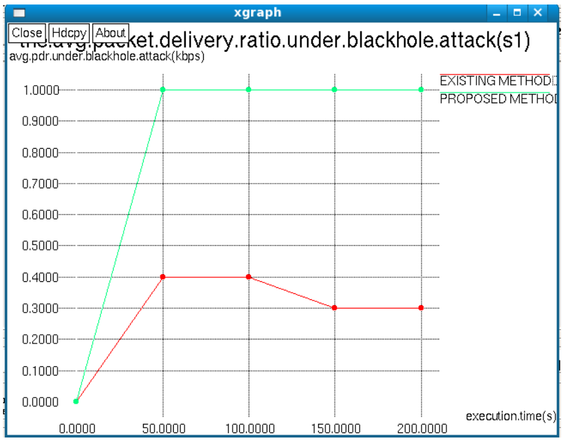


**Figure 1.8 PDR analysis 1**

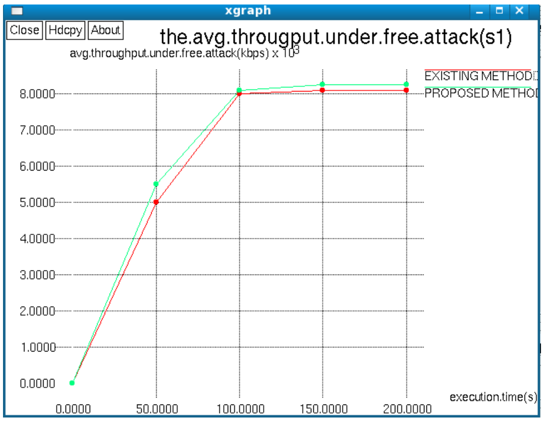


**Figure 1.9 PDR analysis 2**

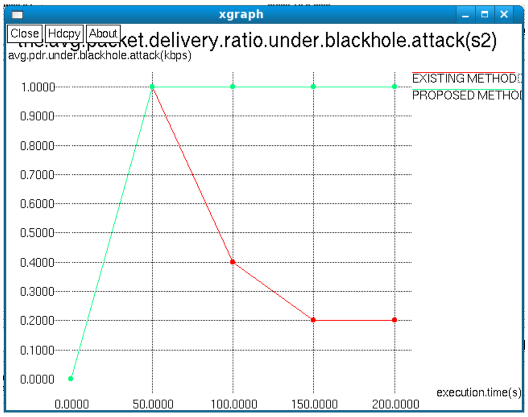


**Figure 1.10 PDR analysis 3**

Figure 1.8, 1.9 and 1.10 shows PDR compariosn of exisiting and proposed methods.The proposed method shows higer delivery rate than exisitng method

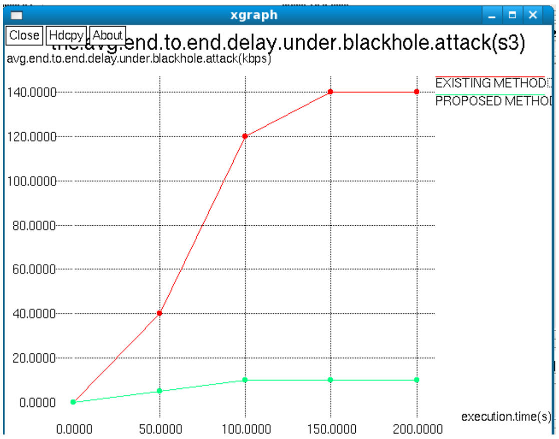


**Figure 1.11 Delay analysis**

Figure 1.11 shows compariosn of exisiting and proposed methods.The proposed method shows lower delay than exisitng method

## 5. CONCLUSION

Data dissemination over VANET is a challenging task due to the specific characteristics of VANETs, such as highly dynamic mobility, short time of contact between vehicles, and short-range communication. The paper introduced a blackhole protected ad-hoc on demand distance vector (BP-AODV) routing protocol for MANETs. The BP-AODV addressed the blackhole vulnerability associated with each of the AODV and SAODV protocols. In addition, it utilized the chaotic map features to protect against cooperative blackhole attack that is performed by two malicious nodeS. The experimental results showed that the BP-AODV protocol is effective in thwarting blackhole attack that might be occurred in different scenarios in VANET dissemination.

## REFERENCES

[1] J. Zhao and G. Cao, “VADD: Vehicle-assisted data delivery in vehicular ad hoc networks,” IEEE Transaction Vehicular Technology, Vol. 57, No. 3, pp. 1910–1922, May 2008.

[2] T. Arnold, W. Lloyd, J. Zhao, and G. Cao, “IP address passing for VANETs,” in Proceedings IEEE International Conference PerCom, pp. 70–79, March 2008.

[3] A. Skordylis and N. Trigoni, “Delay-bounded routing in vehicular ad-hoc networks,” in Proc. ACM MOBIHOC, pp. 341–350, 2008.

[4] Y. Toor, P. Muhlethaler, A. Laouiti, and A. Fortelle, “Vehicular ad hoc networks: Applications and related technical issues,” Commun. Surveys Tuts., Vol. 10, No. 3, pp. 74–88, 2008.

[5] B. Ducourthial, Y. Khaled, and M. Shawky, “Conditional transmissions: Performance study of a new communication strategy in VANET,” IEEE Transaction Vehicular Technology, Vol. 56, No. 6, pp. 3348–3357, November 2007.

[6] S. Das, H. Pucha, and Y. Hu, “Performance Comparison of Scalable Location Services for Geographic Ad Hoc Routing,” in Proceedings IEEE INFOCOM, Miami, FL, pp. 1228–1239, 2005.

[7] B. Ducourthial, Y. Khaled, and M. Shawky, “Conditional transmissions: Performance study of a new communication strategy in VANET,” Transaction Vehicular Technology, Vol. 56, Number 6, pp. 3348–3357, November 2007.

[8] J. Zhao, Y. Zhang, and G. Cao, "Data Pouring and Buffering on the Road: A New Data Dissemination Paradigm for Vehicular Ad Hoc Networks," in IEEE Transaction on Vehicular Technology, Vol. 56, No. 6, pp. 3266-3276, 2007.

[9] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner, “Urban multi-hop broadcast protocol for inter-vehicle communication systems,” in Proceedings of VANET, October 2004.

[10] Murat Caliskan, Andreas Barthels, Bjrn Scheuermann, and Martin Mauve, “Predicting Parking Lot Occupancy in Vehicular Ad Hoc Networks”,65th IEEE Vehicular Technology Conference, (VTC2007), pp. 277-281, April 2007.

[11] Q. Xu, T. Mark, J. Ko, and R. Sengupta, “Vehicle-toVehicle Safety Messaging in DSRC,” in Proceedings of VANET, October 2004.

[12] X. Yang, J. Liu, F. Zhao and N. Vaidya, “A Vehicle-toVehicle Communication Protocol for Cooperative Collision Warning,” International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004), Aug. 2004.

[13] J. Yin, T. Eibatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, “Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks,” in Proceedings of VANET, October 2004.

[14] Giovanni Resta, Paolo Santi, Janos Simon, “Analysis of Multi-Hop Emergency Message Propagation in Vehicular Ad Hoc Networks”, Proceedings 8th ACM international symposium on Mobile ad hoc networking and computing pp. 140-149, 2007.

[15] S. S. Manvi, M. S. Kakkasageri, Issues in mobile ad hoc networks for vehicular communication , IETE Technical Review, Vol. 25, No. 2, pp. 59-72, March-April, 2008.