Secured Geocast Routing in VANET (Vehicular Ad-Hoc Network) with Two Stage Efficient Communication Protocol

Bhaskar Das
Department of Compute and System Sciences,Siksha-Bhavana, Visva-Bharati, Santiniketan-731235

Utpal Roy
Department of Compute and System Sciences,Siksha-Bhavana, Visva-Bharati, Santiniketan-731235

ABSTRACT
In the present study we have proposed a secured geocaste routing in VANET with two stage efficient communication protocol. The communication protocol operates on two stages. In the first stage vehicles transmit messages within its transmission range of its radar and to the VANET Server. In the second stage VANET Server receives messages from vehicles and sends those messages to all other vehicles belonging to the same geographical region as of sender. Geographical regions are predetermined by VANET Server. One of the interesting features of this protocol is that we use the MANET infrastructure instead of roadside equipments to communicate with VANET server. Added feature of the protocol is that unlike other geocast routing protocol [8] it incorporates security issues too. So the messages are secured and trustworthy messages are broadcasted among the vehicles. The protocol has been simulated with the NS2 simulator. For this two stage communication protocol it has been found from the simulation results that the bandwidth usage is less and thus enhance the throughput and decreases the packet loss.

General Terms
Geocast routing protocol, NS2 simulator.

Keywords
VANET server, MANET, Two stage communication protocol.

1. INTRODUCTION
Vehicular Ad-hoc Network (VANET) is emerging as a new type of ad hoc networks in which vehicles play the role of wireless network nodes. A Vehicular Ad-Hoc Network, or VANET, is a form of, rather a subset of, Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. The main goal of VANET is to provide safety and comfort journey for passengers. To this end some special electronic devices will be placed inside each vehicle which will provide Ad-Hoc Network connectivity for the vehicles. This network tends to operate without any infra-structure. Each vehicle equipped with VANET devices will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way. Detail discussion about the VANET and its routing protocols are available in the references [1-14].

2. Improved Distributed Robust Geocasting Techniue Applied in VANET with Two Stage efficient communication protocol
Harshvardhan P. Joshi et al 2007 proposed a geocast algorithm for forwarding message in VANET [8]. This algorithm uses forwarding the message through zone of forwarding towards zone of relevance. But it has some security issues. The present study proposed a more effective geocast routing protocol which is simpler, easy to implement and cost effective. In brief it functions in following manner.

1. Forwarding the message through zone of forwarding towards zone of relevance, and through zone of relevance such that the message travels towards the edges of zone of relevance, i.e., spreading the message in right directions.

2. Delivering the message reliably to all the nodes within the zone of relevance.

These functions must be performed with the least amount of redundancy, by restricting flooding. By the by, the zone of relevance (ZOR) is defined as the set of geographic criteria that a node must satisfy in order for the geocast message to be relevant to that node [8]. The information contained in geocast packet header regarding the sender location and the zone of relevance or zone of forwarding is used in conjunction with the node's current position to restrict flooding and reduce redundancy. A forwarding algorithm to restrict flooding with back-off based on a node's distance from the last transmitter. All of these algorithms are developed so that a node does not need to know its one-hop neighbors or to build multi-hop routes. Each vehicle sends messages to other vehicles those are behind of it but within its transmission range and to the VANET server. Messages are sent with the information provided by a vehicle or when the other vehicles asked for it to authenticate the information provided by a vehicle. Messages will also be sent to the main server. This message will use MANET infrastructure to travel from vehicle to the server.

The VANET server segregates the area based on geographical location. It generates a table based on geographical locations and vehicles belong to a particular geographical location. The VANET server will make an analysis based on those information received by vehicles traveling a particular area and feed them into table. This table will contain geographical *location id, identification numbers of vehicles in that location, speed, the information* provided by that vehicle, analysis made by the server, and vehicles trustworthiness. Other vehicles can access this information from the table and can also check trustworthiness of a particular vehicle. The server also creates

another table which contains *geographical location id, location description, average speed, time*. From this report server can analyses about the average condition of a particular area. From these report vehicles can map their journey beforehand. This will help the smooth traffic flow. Depending upon the geographical location a *vehicle id* to each vehicle will be issued from the VANET server. The vehicle id is the identification of vehicle within a certain geographical location as soon as it changes the geographical location the vehicle id will be changed automatically from the VANET server.

2.1 Message Categorization

Considering the nature of the present algorithm here we have categorized the messages into four main categories. This categorization specially helps to incorporate security within the routing protocol and to reduce important packet loss and efficiently utilize communication channel. Four types of messages are described below according to their priority.

- **Short messages:** These types of messages are most important. It provide information which is used for safety driving, like turning indicator, immediate braking signal, overtaking information, lane change etc. It travels only within the transmission range of a particular vehicle; have highest priority and **not intended** for VANET server.
- **Warning messages**: It identifies the false messages. It is fed into the VANET server and warns other vehicles of a particular geographical region about the wrong messages and which vehicles are generating those messages.
- **Traffic messages:** It provides traffic related information and fed into VANET server. It provides information such as congestion, road condition, accidents etc.
- **Check messages:** It is used to check the authenticity of a message provided by a vehicle. It travels in the direction car moves; can be replied back with Boolean value (i.e. yes/no i.e. 1/0).

2.2 Communication Technique

A message transmitted by a vehicle is received by all other vehicles residing in the transmitting range of the sender vehicle and the MANET infrastructure present in that area (mobile phone tower). If the message is a "short message" type then it will not be accepted by MANET infrastructure, hence not received by VANET Server. Other types of messages will be received by VANET Server. When a vehicle sends message it will travel to all other vehicles traveling through a particular geographical area. As traffic increases, the numbers of messages will also increases. This leads to network congestion and packet loss. To overcome this problem we propose a dual stage efficient communication method to improve channel utilization and to reduce packet loss. In the first stage, a vehicle sends messages to other vehicles within its transmission range and to the VANET server thru mobile communication network. The database of VANET server is updated with these messages. In the second stage, VANET server sends messages to other vehicles within that particular geographical location. Other vehicles, from other geographical region, would not get the messages unless they explicitly ask for that information from the VANET server. Therefore the message passing around the vehicles is performed in two steps, one is through vehicle to vehicle communication and other one is with the intervention of MANET.

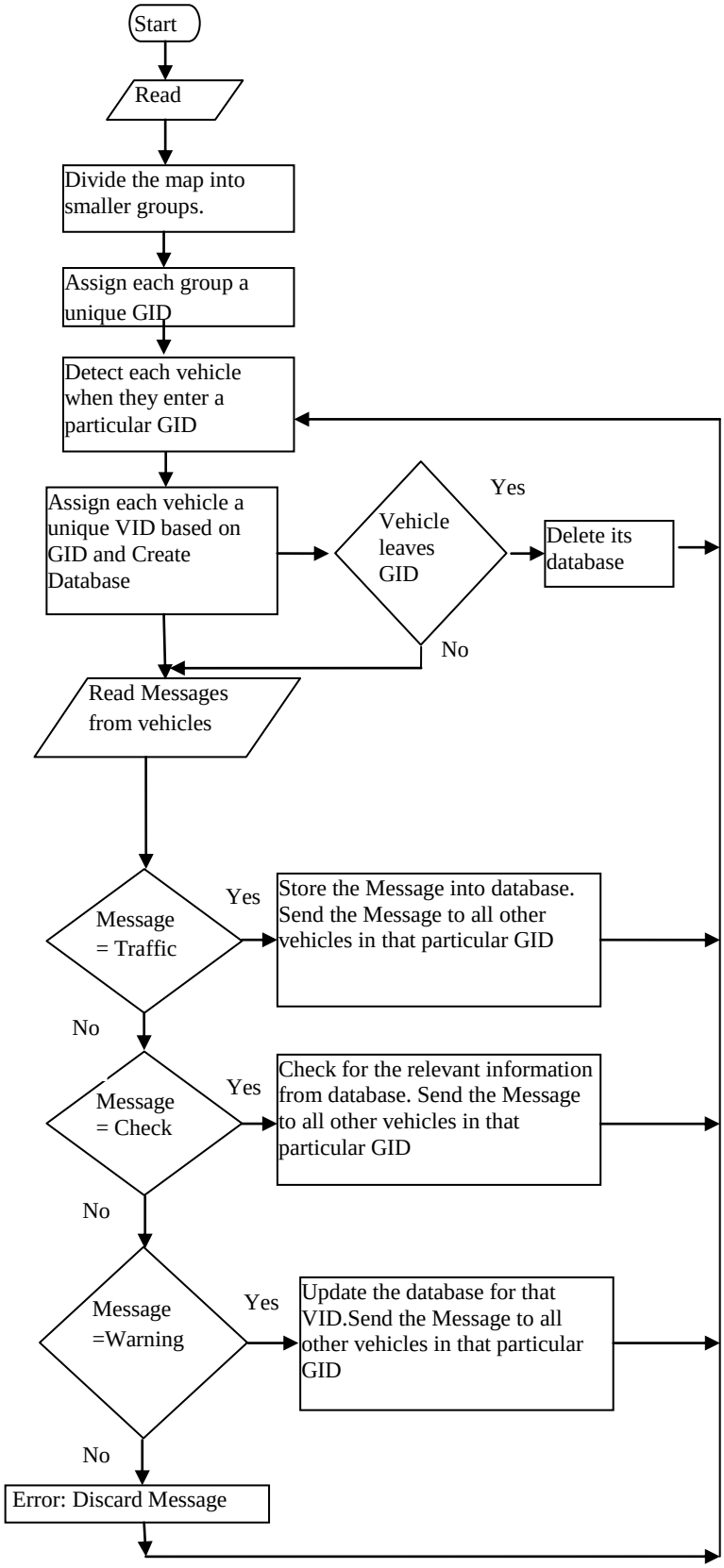

Figure1. VANET Server working – Flow Chart

2.3 VANET server

The VANET server segregates the area based on geographical location. It generates a table based on geographical locations and vehicles belong to a particular geographical location. The VANET server will make an analysis based on those information received by vehicles traveling a particular area and feed them into table. This table will contain *geographical location id, identification numbers of vehicles in that location, speed, the information* provided by that vehicle, analysis made by the server, and vehicles trustworthiness. Other vehicles can access this information from the table and can also check trustworthiness of a particular vehicle. The server also creates another table which contains geographical location id, location description, average speed, time. From this report server can analyses about the average condition of a particular area. From these report vehicles can map their journey beforehand. This will help the smooth traffic flow. For example, if there is a road block in a particular area, then all the cars moving through that area will generate road block message and there speed will also be 0 (zero). So other cars moving towards that direction can check with all the cars present in that geographical area and take the decision about moving toward that direction. In case a car is generating a false message other cars in that geographical area can contradict it.

2.4 ATTACKS

It is important to secure the communication in VANETs; otherwise everything will be in vain. Protocol without proper measure can easily damage the communication. Attackers could send falsified messages, or can identify and block the other nodes to receive and send priority messages. Most of the works related to VANET are mainly devoted to design principle and issues related to VANET [15-19], attacks and security issues have been considered there with less attention, though the articles [17] and [18] deals with attacks and security issues as a general case of wireless communication. Importantly Charles et. al [20] in their article have considered the security of the network layer operation for wireless multi-hop communication in VANETs. In the proposed geocast routing four possible threats and their solutions have been discussed. These are discussed briefly below.

Attack 1: Bogus traffic information: In that case the database of the VANET Server will be checked. The VANET server now already has the latest updated information in the database from other vehicles (in case of accident/traffic jam the vehicles taking part in the accident/traffic jam will give the information to VANET Server). According the query from the database table of the server the information will be nullified.

Attack 2: Generate "Intelligent Collisions": In this type of attack the vehicles should not trust on the information they are getting from other vehicles. Information should always be cross-checked with the VANET Server (if available).The VANET Server will store the data in "read only" fashion. The VANET Server will update the database periodically as vehicles upload data. Say, if one or few vehicles inform that there is an accident and from the database of the server it is recorded that the rear vehicles passing that location safely then according to the database record the accident warning message will be discarded. The VANET Servers will be able to provide warning messages on particular location.

Attack 3: Cheating with identity, speed, or position: Anonymity of all the vehicles should be maintained by using our geographical addressing scheme which changes with the geographical location.

Attack 4: Tracking: This problem can be solved by using our geographical addressing, where each node is characterized by its geographical position. As the nodes moves from one geographical location to another its address changes.

2.5 Simulation and Results

The above two stage message passing secured routing algorithm has been simulated with the NS2 network simulator. The vehicle to vehicle communication has been simulated with suitable simulation parameters as given below. The simulation results have been compared with that of algorithm proposed in [8]. The obtained results are quite logical and sometimes out-perform the results obtained in [8].

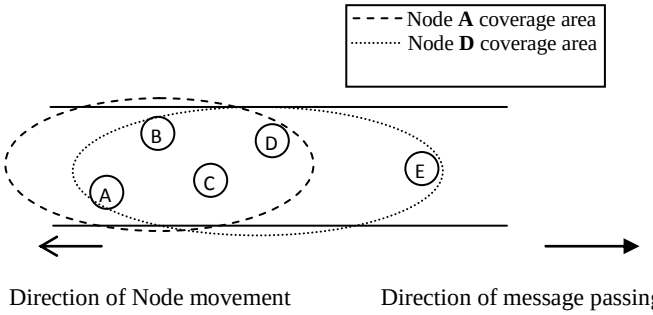

Figure 5: Node movement with message passing

Let us assume a scenario with 5 nodes (vehicles). Node A can send message to Node B, Node C and Node D. Node D cover Node A, Node B, Node C and Node E. Nodes are moving from right to left direction. Node B, Node C, Node D and Node E follows Node A. According to Geocast protocol proposed by [8] message transmitted by Node A received by Node B, Node C and Node D. Node D as having the most forward advance retransmits the message to Node E. Message retransmitted by Node D is also received by Node C and Node B but they both ignored it as they are ahead of Node D. According to the protocol proposed by the authors in this paper, message sent by Node A would be received by Node B, Node C and Node D. Node A will also sent the message to VANET server through MANET infrastructure. Node E will receive the message from VANET server. This two stage communication technique provides better use of bandwidth. The message is also categorized to give better channel utilization. "Short Messages", when generated by Node A only circulated to Node B, Node C and Node D. This type of messages would not go to the server; hence Node E would not receive it. "Traffic Messages", when generated by Node A would be received by all other nodes including server and Node E. In this simulation "Traffic Messages" of the proposed protocol have been used to compare with the Geocast protocol [8]. Proposed message categorization methods restricts the flooding of message hence better utilizes the scarce wireless channel. For example, in our protocol "Short Messages" will only be circulated within the range of sender node's, whereas in Geocast protocol [8] all the messages will be circulated to all other nodes those are out of range also. This mechanism of our protocol yields better channel utilization. Although we are using centralized VANET server, but when links breaks with the server that time also our protocol works as "Short Messages" still can pass within sender's transmission range.

Table 1: Simulation Parameters

Simulation Parameters	**Value**
Simulation Area	1000m * 1000m
Number of Vehicles	5
Average speed of Vehicles	16 metre/second
Transmission Range	250m
MAC Protocol	802.11 DCF

Simulation results for both (Geocast protocol [8] and present one) the algorithms have been presented in Figure 2 and Figure 3 respectively. It is evident from Figure 2 and Figure 3 that channel utilization in present protocol is better than the protocol proposed in Ref. [8].

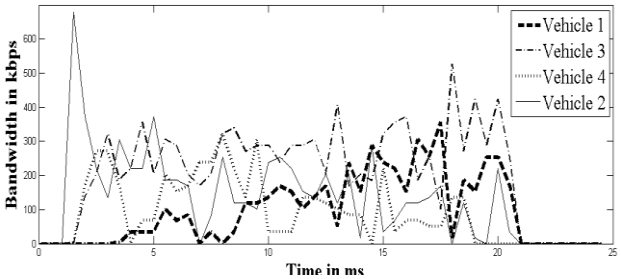

Figure2: Gives the channel utilization with protocol in [8]

Figure 4 depicts the bandwidth while nodes are communicating among the groups, means the nodes within the transmission range of each other. The figure represents the node failure state after 9 ms., which is expected from the protocol presented in Ref.[8]. Whereas Figure 5 represents the bandwidth while the nodes are communication through present protocol. In this protocol when the node does not belong within range of communication they communicate through VANET Server. The node failure case rarely occurs. Even in the case of node failure "Short Message" still can propagate.

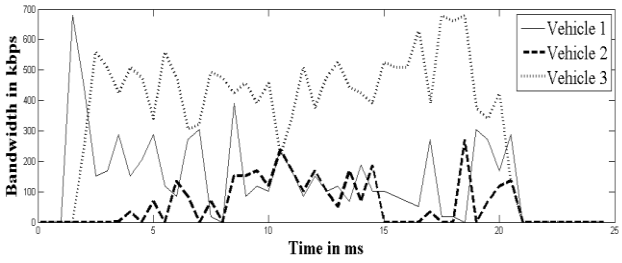

Figure 3: Channel utilization with present protocol

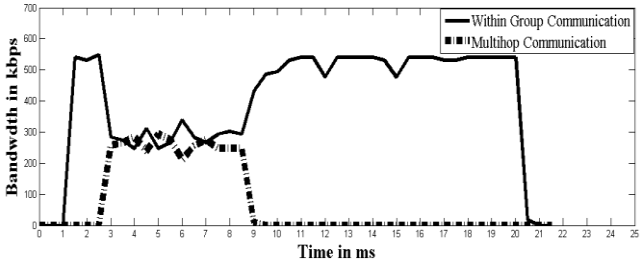

Figure 4: Bandwidth within group communication with node failure in Geocast protocol [8]

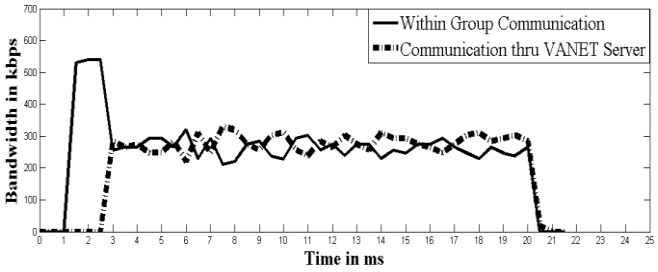

Figure 5: Bandwidth within group communication with presented protocol

Table 2: Difference Between Geocast Protocol[8] and Two Stage Communication Protocol in VANET

Protocol	Bandwidth within Group Communication (in kbps)	Bandwidth Inter Group Communication (in kbps)	Bandwidth within Group with Node failure (in kbps)	Bandwidth within Group without Node failure (in kbps)
Geocast Proto-col[8]	562.5	150.0	650.0	475
Two Stage Communication Protocol "Traffic Message"	325	275	Does not arises in the case	300

Table 2 represents the bandwidth utilization in all possible sates that may occur in the present proposed protocol and the geocast protocol that is used in Ref.[8]. It is observed from the table that bandwidth used by the geocast protocol [8] is always remain in higher range where as the bandwidth used in present protocol is a less. The power of the present protocol is that the node failure case is hard to occur as the role of VANET server comes into play. It is worth to mention here that in case of only message type of "Short Message", bandwidth obtained by presented protocol is equivalent with the Bandwidth within Group with Node failure of Geocast protocol [8] shown in Table 2 which is 650kbps. From the result it can be concluded that our protocol always produce better average results with stable connection.

3. Conclusion and future scope

The present protocol "Secured Geocast Routing in VANET (Vehicular Ad-Hoc Network) with two stage efficient communication protocol" provide better security and efficient channel utilization in comparison to the well known available routing algorithm in VANET [8]. Over and above the present protocol is simple minded, easy to implement and cost effective. Cost effective in the sense that it does not require much extra equipment, on the contrary it used the MANET infrastructure.

But the proposed protocol is not free from some minor limitations. In the rural areas where the wireless connections

are very feeble the connection between the VANET server and the vehicles breaks down, so in remote and rural areas in absence of MANET equipments the algorithm is not expected to perform. It is wise to apply the present VANET algorithm in hilly areas where, the accident-prone zones and the turning of roads occurs in ample. If due to any reasons the wireless connection between vehicle to vehicle and vehicle to server breaks down, it may invite devastation.

As mentioned in [21] and the references therein, multihop broadcasting in traffic jam is familiar in VANETs , however serious redundancy, connection and collisions are caused by frequent communication in this condition. All methods devote to reducing rebroadcasts to get relief from the above problem. Our method is much useful in this situation as multihop rebroadcasting is not a virtue of it.

The simulation of VANET performance is much more complicated, it needs so many decision making and database accessing and updating algorithms..

In Near future, the vehicles will be equipped with wireless communication devices, allowing for vehicle to vehicle and vehicle to infrastructure communication based on short range wireless technology (IEEE 802.11 like). These VANET enable a new set of application to improve safety, traffic efficiency and driving comfort. Such as traffic group can warn other traffic group regarding accident, road condition, entertainment etc.

4. REFERENCES

[1] William C. Y. Lee, *Wireless and Cellular Communications*, 3rd Edition, McGraw Hill Publishers, 2008.

[2] T. S. Rappaport, *Wireless Communication: Principles and Practice*, Prentice Hall Pub Ltd, 2nd Ed, 2006.

[3] H. Alshear and E. Horlait, "An optimized Adaptive Broadcast Scheme for Inter-Vehicle Communications", *IEEE Vehicular Technology Conference*, Stockholm, Sweden, May 2005.

[4] M. Torrent-Moreno, D. Jiang and H. Hartenstein, "Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks", *Proceedings of the 1st International Workshop on Vehicular Ad Hoc Networks, ACM*, pp 10-18, Philadelphia, PA, USA, October 2004.

[5] J. Blun, A. Eskandarian and L. Hoffman, "Challenges of Intervehicle Ad Hoc Networks", *IEEE Transactions of Intelligent Transportation Systems*, Vol. 5, No. 4, December 2004.

[6] Q. Xu, T. Mak and R. Sengupta, "Vehicle-to-Vehicle Safety Messaging in DSRC", *in Proc ACM VANET*, Philadelphia, October 2004.

[7] C. Koner, P. K. Bhattacharjee, C. T. Bhunia, U Maulik, "A Novel Approach for Authentication Technique in Mobile Communications", *International Journal of Computer Theory and Engineering*, Singapore, vol. 1, no. 3, pp. 225-229, August, 2009.

[8] Harshvardhan P. Joshi, Mihail L. Sichitiu, and Maria Kihl, "Distributed Robust Geocast Multicast Routing for Inter-Vehicle Communication", in Proc. of the First Workshop on WiMAX, Wireless and Mobility, (Coimbra, Portugal), May 2007.

[9] H.Alshearand, E.Horlait, An Optimized Adaptive Broadcast Scheme for Inter. Vehicle Communication, in Proc. IEEE Vehicular Technology Conference (IEEE VTC 2005. Spring), Stockholm,Sweden,May2005.

[10] J.Blum, A.Eskandarian ,and L.Hoffman: Challenges of Intervehicle AdHocNetworks, IEEE Transactions of Intelligent Transportation Systems,Vol.5,No,4,December2004.

[11] S. Y.Ni, Y. C.Tseng,Y.S.Chen,and J.P.Sheu. TheBroadcast Storm Problem in a MobileAdHoc Network, in Proc. ACM/IEEEMobiComm,1999.

[12] Young-Bae Ko, Nitin H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," Volume 6, Issue 4 (July 2000) Pages: 307 - 321 Year of Publication: 2000 ISSN: 1022-0038 in Proc. of MobiCom, 1998;

[13] Abdelmalik Bachir and Ahderrahim Benslimane, "A multicast protocol in ad hoc networks: Inter-vehicles geocast," in Proc. of the 57th IEEE Vehicular Technology Conference, vol.4, (Korea), pp. 2456-2460, April 2003.

[14] Utpal Roy, Bhaskar Das, Pijush Kanti Bhattacharjee and Achintya K. Mandal, "Secured Geocast Routing Protocol in VANET (Vehicular Ad-Hoc Network)," Proceedings of the International Conference on Computing and Systems-2010, pp 64-68, November 2010.

[15] Papadimitratos, P., Gligor, V. and J-P. Hubaux. Securing Vehicular Communications –Assumptions, Requirements and Principles. In Proc. ESCAR, 2006.

[16] Fonseca E. and Festag A., A Survey on Existing Approaches for Secure Ad-hoc Routing and Their Applicability to VANETs. Technical Report NLE-PR-2006-19, NEC Network Laboratory 2006.

[17] Raya. M. and Hubaux, The security of Vehicular Ad Hoc Networks, In Proc. SASN, 2005.

[18] Aijaz. A. , Bochow, B. Dotzer F.,Festag. A. Gerlach, M. Kroh. R. and Leinmuller. T. , Attacks on Inter Vehicle Communication Systems – An Analysis , In Proc. WIT 2006.

[19] Raya. M Papadimitratos, P, J-P. Hubaux. Securing Vehicular Communications. In IEEE Wireless communicaton Magazine, 2006.

[20] Harsch, C., Festag, A. and Papadimitratos, P.,"Secure Position-Based Routing for VANETs". In Proceedings of the 66th IEEE Vehicular Technology Conference, 2007.PP-26-30.

[21] Zhou. L. , Cui G. Liu, H. Wu Z and Luo D " NPPB : A broadcast Scheme in Dense VANETs", Information Technology Journal 9(2) : 247-256, 2010.