Variable Delay Broadcasting Scheme for Fast Information Dissemination in Vehicular Ad hoc Networks (VANETs)

Jetendra Joshi, Sujoy Roy ,Rahul Siriponnala Raja, and Dr Debasis Das
Department of Electronics and Communications ,Department of CS&IS, BITS- Pilani,
NIIT University, Rajasthan, India K. K. Birla Goa Campus, Goa, India.

***Abstract*—A Vehicular Ad-Hoc Network, or VANET, is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. In vehicular ad-hoc networks (VANETs), network services and applications require an exchange of vehicle and event location information. Basically, the DTN protocol is used for message transmission which may result in some delay but it is more reliable in nature. To reduce delay in communication, we proposed a new algorithm called Variable Delay Broadcast Protocol (VDBP). We simulated and tested in Indian Road Scenario using NS2 and we got more efficient results. We also presented the algorithm for the application of protocol in Vehicular Networks.**

Keywords*—*Vehicular ad hoc networks, Intelligent transportation systems, Security Messages, SUMO, NS2, DTN.

I. Introduction

For past few years, the immense advances achieved in wireless communication technology, have yielded a great scope in networking research fields focusing at extending connectivity to different environments where wired solutions are not viable. As such, Vehicular Ad hoc Network (VANET) stand as one of the most promising and attracting research field for students, researchers and automotive companies. Vehicular Ad hoc networks (VANETs), are considered as a form of Mobile Ad hoc Networks (MANETs), and developed to provide wireless communication within a group of vehicles. Vehicles can communicate with other moving vehicles using Vehicle to Vehicle communications (V2V) and with stable network nodes placed next to the road called Road Side Units (RSU), using Vehicle to Infrastructure communications (V2I). RSU allows provision to moving vehicles with access to an infrastructure network, as well as infrastructure based services. Road side units can be placed alongside the road with uniform spacing between them, and can also be integrated in existing road infrastructures like bridges, road signs, toll gates, etc. However, the high speed of the network nodes in VANETs, and the presence of signal blocking obstacles like large buildings, produce a highly varying network topology, as well as more frequent segregations in the network. Therefore, typical MANET protocols do not adapt very well to VANET [1] since an absolute connected path between sender and receiver is usually missing. Under such conditions, Delay Tolerant Networks (DTN) is an alternative that can deal with VANET characteristics [2]. Many organizations have put great effort to elevate their vehicular networks using wireless access in vehicular environment (WAVE), which provides safety from many traffic related issues. Figure 1, represents a general view of WAVE architecture.

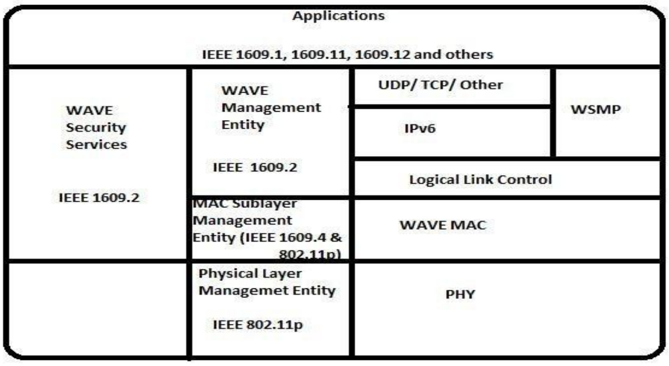

Figure 1. WAVE Architecture

Delay and Disruption Tolerant Network (DTN) can be distinguished by the lack of the possibility of creating a path between any numbers of pair of nodes at the same time. In the Delay and Disruption Tolerant Network, communication uses store, carry and forward pattern. This is done by using network nodes physically carrying messages called message mules or message ferries. DTN actually originated as a proposal for Inter Planetary Networks (IPNs) to provide communication between base stations, and satellites. In DTN, when a message fails to be routed to its destination, it is not dropped immediately. Instead it is stored and carried along until a new route becomes available for transmission. DTN allow for information to be shared between different nodes even in the presence of very high delays, which are typical in spatial communications. Messages are dropped from the buffer only when their lifetime expires or for memory management reasons. The researchers have been actively proposing new protocols and applications for Vehicular Delay Tolerant Networks (VDTN) over recent years.

Architecture and Standards:

The Delay and Disruption Tolerant Network architecture is designed to run as an overlay network over the network layer to support the heterogeneity of several networks. For that, two new layers are added: The bundle layer [3] and the convergence layer. The bundle layer encloses application data units into bundles, which are then forwarded by DTN nodes following the given bundle protocol. The convergence layer need not run over the Internet protocol stack, thus allowing for the implementation of DTN over any kind of network.

***1)* Bundle Protocol:** The Bundle Protocol actually stores bundles and forwards them between DTN nodes. The Bundle Protocol performs hop -by-hop forwarding, instead of end-to-end forwarding. The Bundle Protocol stores bundles in permanent storage devices until a new transmission possibility appears, to deal with network delay. The concept of reliable guided transfer ensures that a DTN node will not remove a bundle from its buffer until another DTN node has taken charge of it.

The Bundle Protocol operation depends on contacts. A contact will occur when a connection between two DTN nodes is established. The contact type depends on the type of operating network: it may be persistent, as in the Internet, opportunistic, as in VN or deterministic, as in interplanetary networks.

The Bundle Protocol performs fragmentation when the size of a bundle goes over the maximum transferred data of contacts. Fragmentation is supported in two different strategies: proactive, where a DTN node may break an application message into different bundles and forwards every bundle independently and reactive, where bundles are fragmented during transmission between network nodes.

2) **Convergence Layer:** The convergence layer outlines the characteristics of lower layers to the bundle protocol and is in charge of sending and receiving bundles on behalf of the bundle protocol. The convergence layer allows usage of any set of lower protocols to reliably transfer a bundle between two DTN nodes. For example, the TCP/IP convergence layer uses a TCP connection between two DTN nodes to transfer bundles. The TCP connection can be established via the Internet. To implement a DTN over other technologies, new convergence layers are needed. Convergence layers must provide the bundle protocol with a reception mechanism and reliable delivery scheme.

3) **Epidemic Protocol:** It is a protocol based on flooding and contains homogeneous nodes. This protocol is fast in nature and provides replication, without using any kind of mobility information. It works on “Store Carry Forward” approach.

Let’s suppose ‘A’ wants to send some information to B but they both are not in direct range with each other but suppose A is in direct range with its neighbor N1 and N2, and B is in direct range with its neighbor N3.

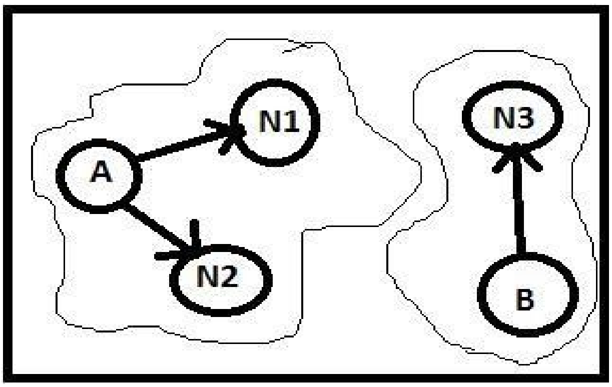

Figure 2. Data sending between Node A and B

So, A can transit its information to its any of the neighbor and if later if that neighbor comes under the direct access range of B then B can easily get the information supplied from A.

II. Related Work

The article [4] presented a decent survey of a number of proposed routing protocols for DTNs in VANETs. The major contributions of this survey are the classification of different DTN routing protocols into three types based on their neighbor selection techniques and their evaluation on the basis of their characteristics. Most of these routing protocols are appropriate for metropolitan vehicular networks. In [5], they have proposed deterministic and probabilistic approaches to determine the trust level which is used to filter out harmful information to provide VANET security. In this proposed schemes individual vehicles evaluate, decide and react locally based on the information received from other nearby vehicles. Proposed algorithms determine whether the received message is legitimate or not. Probabilistic approach uses the copies of received message to estimate trust level. Combined approach gives better results than the probabilistic and deterministic approaches individually, however combined approach needs more time to make a decision. They have validated their claims with the help of results obtained from extensive simulations. The paper [6] is a comprehensive review of VANET security, presenting challenges and addressing the attacker’s profiles for security. Then, threats, privacy and security solutions were discussed. Some security issues such as security requirements, adversary’s profiles and security attacks in VANET have been pointed out. Certain security solutions and architectures suggested in the literature were highlighted. [7] Proposed a geo-based opportunistic information dissemination model designed for Dynamic Routing. Instead of the assumption that vehicles participate in message exchanging unconditionally, they proposed that a considerable proportion of vehicles in real life belong to certain groups and take the willingness to make contributions to their own groups driving conditions as a rational cooperation bonus. They evaluated the performance of the model and its effect on saving trip-time in a realistic scenario on an integrated simulation platform. The experimental results show that the proposed dissemination model decreases forwarding overhead dramatically while still delivering as many useful messages into right vehicles. In the paper [8], they proposed a collaborative protocol to verify a declared position when direct communication between the questioned node and the verifier node is not possible. In addition to verification of a node location in a multi-hop cooperative approach, several security measures were added to improve the integrity of message. The simulation results showed that the proposed protocol highly increased the rate of neighborhood awareness in vehicles under the effect of simulated obstacles like buildings. In the work [9], they made a substantial analysis of several protocols proposed in the literature for message distribution in VANET under three study cases. In order to exhibit high reliability and less delay to transmit warning messages, they proposed a protocol that sets the waiting time for receiver candidates. The proposed protocol, Preset Delay Broadcast (PDB) protocol offers a high reliability and great reception rate when covering a specific area. In this paper, [10] have presented a cooperative mechanism for neighbor position verification based on the information interchanged among one-hop neighbors. Their Cooperative Neighbor Position Verification (CNPV) protocol is easily adaptable to different warning message distribution schemes that make use of the information of neighboring vehicles to decide the most appropriate forwarding scheme in VANET. CNPV allows verification of the neighbor’s position before deciding the next forwarding vehicle, favoring the distribution process and reducing the number of vehicles that do not receive the warning messages. To gain better understanding on the performance of Cooperative Neighbor Positioning in a VANET environment, [11] carried out a comprehensive characterization study through realistic experimental simulations. The results showed that the

Cooperative Positioning is an effective and feasible technique in improving the accuracy in vehicular positioning. In Geographic Delay-Tolerant Network (GeoDTN) Routing, [12] summarized and categorized geo-based routing algorithms in vehicular networks. The routing process is divided into three modes: greedy mode, perimeter mode and DTN mode. Vehicles are classified into 4 categories by the deterministic of their destinations and routes. Different distance metrics are defined for each category to switch between routing modes and next relay selection. To disseminate the road information in the network quickly and widely, [13] proposed a simple message dissemination algorithm, which broadcasts messages road by road firstly. Then, through measuring some road condition parameters such as average speed and car density, forwarders may adjust the broadcast interval to decrease communication overhead. In [14], they evaluated the effectiveness of Dynamic Routing and the feasibility of broadcast interval adjustment through simulation. They also found that relay candidates vehicle information can be very useful in selecting a good relay. Similar simulation results appeared in [15].

III. Proposed Algorithm

The proposed algorithm mainly focuses on the vehicles who rapidly broadcast the emergency warning packets .

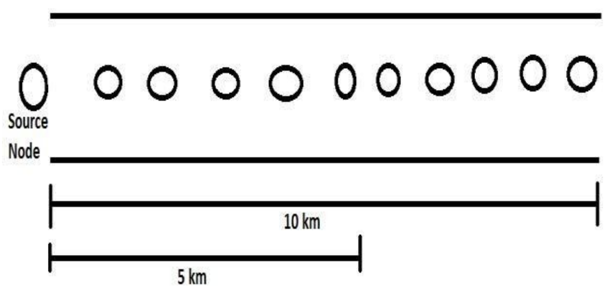

Figure 3. Node Diagram

Figure 3 shows that, the emergency packet is send to the ten farthest neighbours from the source node, which consists of bundle and their distances. Suppose if the congested area mentioned in the packet is 5 km from the source node and the vehicles which has passed the 5 km of distance from the source node can negotiate that emergency packet. The vehicles which are before 5 km checks whether the packet is received by them for the first time or not, if it has been received more than once then that vehicle can negotiate the packet. If the packet is receive for the first time then the vehicle receiving the packet would look for his own attribute in the list (mentioned in the packet). If the vehicle finds its attribute, then it will calculate the delay according to its position mentioned in the packet. In case, the attribute is not found then the vehicle measure its actual position from the source node and if it is found greater than the distance mentioned in the packet, then the delay will be considered as 0 and the rebroadcasting of the packet is done. The distance between Receiver and Source mentioned in the packet is greater than its actual distance, then the delay is calculated randomly between 7ms to 10ms.

The input in this algorithm will be the time taken by vehicle on a particular road segment, and finally rebroadcast the packet to the vehicles containing warning messages.

An emergency packet consists of a Bundle, and the Bundle has

Source node's ID, Congested Warning (C.W) message and hop-count of C.W {f, cw, hc}.The Congested Warning Message (C.W) has

Vehicle's ID, time, road which is congested and travel delay.

An emergency packet is send to the vehicle, when the time spend by the vehicle on the particular road segment is greater than the travel delay threshold (Segment Length/ Speed Limit), of that particular road segment. On receiving the emergency packet the receiver first of all updates its position and then uses the shortest path algorithm to find the new paths. The receiver checks whether he has covered the congested area mentioned in the list, if yes then the receiver will negotiate the emergency packet. Otherwise, the receiver will check whether he has received the emergency packet for the first time.

If the receiver has received the packet more than once that means the rebroadcasting procedure has been already tried before which was not successful, therefore we will eliminate the packet. But if the packet is received for the first time then the receiver carries the packet forward using the carry strategy and then the receiver looks for his own attribute in the packet, and further it will carry the packet forward according to algorithm mentioned above.

Finally when the vehicle receives the packet for the second time, then it cancels the retransmissions of the messages. This algorithm shows high reliability and low delay.

Given below is the following pseudo code for the VDBP algorithm:-

{
If vehicle time is greater than delay threshold then send WARNING PACKET
else
End the Algorithm
}
{
procedure GENERATE WARNING PACKET
ReceiverID← Get Farthest receiver ID Sorted
Distance← Get Max Distance of the vehicle receiving the Packet
f← Get Source Vehicle ID
C.W← Get Congested Warning Message
h.c← Get hop-count of Congested Warning Message Add (f) And (C.W) And (h.c) (f, C.W, h.c) Broadcast(P)
}
{
procedure RECEIVE(Packet)
update POSITION
if vehicle has not covered the danger area mentioned in the packet then
if packet is received for the 1st time then Carry Strategy for Carrying the Packet
ID← Get IDs from the Packet

```
      MaxDistance← Get Distance from the packet of the
receiving vehicle
      PositionFound← Search (ReceiverID)
      from (ID) RebroadcastFlag← Yes
   if PositionFound then
      Delay←
   MilliSeconds
   [(Position+1)/2] else
     if Dist.BetweenReceiverToSource > MaxDistance then
        Delay←MilliSeconds
     (0) else
        Delay←MilliSeconds(Random(7,
        10)) Schedule(Delay,
        Rebroadcast, P)
   else
        RebroadcastFlag←False
  else
     End the algorithm
}
{
 procedure REBROADCAST(Packet)
   if RebroadcastFlag = YES then
      ReceiverID← Get Farthest receiver ID Sorted
      Distance← Get Max Distance of the vehicle receiving the
Packet
      f ←Get Source Vehicle ID
      C.W← Get Congested Warning Message
      h.c← Get hop-count of Congested Warning Message
      ReplaceReceiverIDAndDistance(Receiver, Distance)
      Broadcast(P)
  else
      End the algorithm
}
```

IV. Simulation and Performance Analysis

Figure 5, shows the simulation structure, here we have used two simulators that are SUMO (TraCl-Server) as the traffic simulator and NS-2 (TraCl-Client) as the network simulator and to make them work simultaneously in an integrated manner we use TCP Connection.

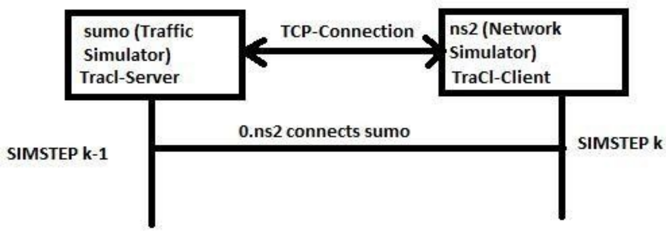

Figure 5. Simulation Structure

NS2 sends SIMSTEP commands to start the simulation process of sumo from the SIMSTEP k-1 to k and after that in response to that sumo sends the position of the vehicles to the ns2 which acts as TraCl-Client.

This figure basically shows the connection between the Traffic Simulator and the Network Simulator.

Figure 6, shows a variety of simulation parameters used in the comparison of VDBP with other protocols.

Parameters	Value
Simulator Used	NS-2
Time of simulaiton	50 sec
Servers	Single
Total number of Nodes	28
Traffic Model	CBR
Pause Time	20 second
Speed	40 mps
Transmit Power	15m W
Receiving Power	13m W
MAC Layer Protocol	802.S11s

Figure 6. Parameters used in Simulation

Performance Parameters:

1. **Average Delay:** On measuring the delay, the vehicles located at a distance of 1 km or greater, then shows the delay by calculating the time difference between the actual time of the receiver and the time stamp mentioned in the packet. If there is more than one delay registered still the first delay is only considered. The protocol has less delay time compared with other protocol which is shown in figure 7.

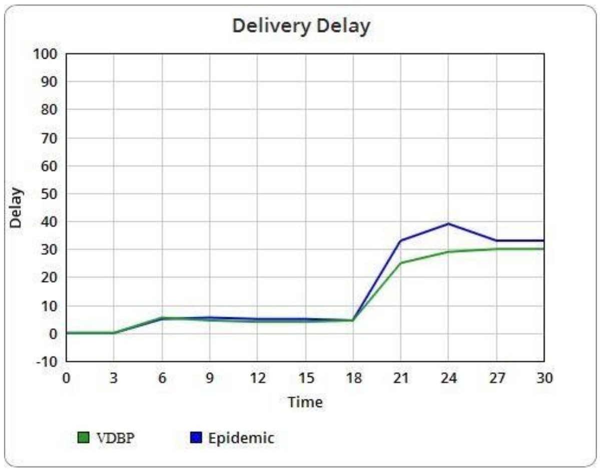

Figure 7. Analysis of Average Delay

2. **Throughput:** It is number of packets received successfully in unit time and is presented in bits per sec.

Formula:

*Throughput = Received data * 8 / Data Transmission Period.*

To trace the file and to produce output, commands to add a DTN agent are as follows:-

set dtn 0[new Agent/DTN]
$ns_attach-dtnagent $1(0)
$dtn0 $ns_connect-dtn $dtn0
$dtnSink $dtnBS set
nlsBSNode_1

$w(0) base-station [AddrParams addr2id [$BS(0) node-addr]] $w(0) base-station [AddrParams addr2id [$BS(1) node-addr]] $w(1) base-station [AddrParams addr2id

[$BS(0) node-addr]] $w(1) base-station [AddrParams addr2id [$BS(1) node-addr]] $ns_attach-dtnagent $w(0) $dtn1

$ns_attach-dtnagent $w(0)
$dtn2 $ns_connect-dtn
$dtnBS0 $dtn1

Figure 8, shows the comparison of Throughput of VDBP with epidemic protocol.

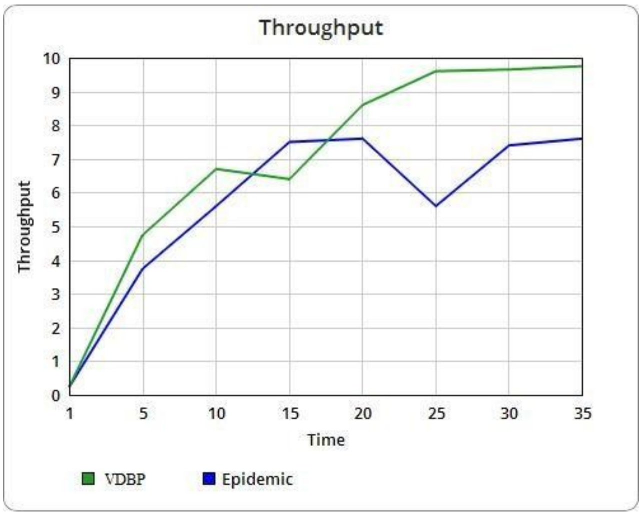

Figure 8. Analysis of Throughput

Figure 8. Clearly shows that as the time increases the throughput of the system also increases when we are comparing the two algorithms (VDBP and Epidemic).

V. Conclusion

In this paper, we made a considerable analysis of several protocols proposed in the literature work for message distribution in VANET. In order to exhibit highly reliable and less delayed protocol to broadcast warning messages, we proposed a protocol called Variable Delay Broadcast Protocol. We simulated and analyzed its performance; we can significantly reduce the delay needed to cover a given area. Furthermore, even if our VDBP protocol sustains to several retransmissions, they are significantly reduced by increasing vehicle density. Additionally, VDBP offers high reliability and also a great reception rate when it covers an interest area. But when it comes to security, messages from other groups may not be trusted completely in real life for security considerations. Trust management between different vehicles is still an unsolved problem in VANETs. Few models have been proposed for trust security in vehicular network, but they still need to be smartly fitted for specific applications and need to be evaluated for their effectiveness in realistic road scenarios.

VI. References

[1] G. V. Kumar, Y. V. Reddy, and M. Nagendra, “Current research work on routing protocols for MANET: A literature survey”, May 2010.

[2] V. Cerf et al., Delay Tolerant Networking Architecture, RFC 4838 (Informational), Internet Engineering Task Force, Apr. 2007.

[3] K. Scott and S. Burleigh, Bundle Protocol Specification, RFC 5050 (Experimental), Internet Engineering Task Force, Nov. 2007.

[4] Muhammad Amin, Ajmal Khan, Muhammad asif, Sana Ul Haq and Imtiaz Rasool, "A Survey of Routing Protocols for Delay Tolerant Networks in VANETS", Sci.Int.(Lahore),28(2),1137-1143,2016

[5] Danda B. Rawat, Gongjun Yan, Bhed B. Bista and Michele C. Weigle, "Trust On the Security of Wireless Vehicular Ad hoc Networking", Ad Hoc & Sensor Wireless Networks, Vol. 0, pp. 1–23, January 2015.

[6] Richard Gilles Engoulou, Martine Bellaiche, Samuel Pierre and Alejandro Quintero, "VANET security surveys", Computer Communications 44 (2014) 1–13.

[7] Zhang Yin Qian and Yue Wu, "An Opportunistic Dissemination Model for Traffic Congestion Management in Vehicular Networks", VEHICULAR 2013: The Second International Conference on Advances in Vehicular Systems, Technologies and Applications.

[8] Osama Abu Mansoor and Azzedine Boukerche, "A Secure Cooperative Approach for Non line of Sight Location Verification in VANET", IEEE Transactions on Vehicular Technology, Vol. 61, No. 1, January 2012.

[9] Salvador Gonzalez and Victor Ramos, "Preset delay broadcast, a protocol for fast information dissemination in vehicular ad hoc networks (VANETs)", EURASIP Journal on Wireless Communications and Networking (2016).

[10] Manuel Fogue, Francisco J. Martinez, Piedad Garrido, Marco Fiore, Carla-Fabiana Chiasserini, Claudio Casetti, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, "Securing Warning Message Dissemination in VANETs Using Cooperative Neighbor Position Verification", IEEE Transactions on Vehicular Technology, Vol. 64, No. 6, June 2015.

[11] Jun Yao, Asghar T. Balaei, Nima Alam, Mahmoud Efatmaneshnik, Andrew G. Dempster and Mahbub Hassan, "Characterizing Cooperative Positioning in VANET", 2011, .

[12] P. C. Cheng, K. C. Lee, M. Gerla, and J. Härri, "GeoDTN+Nav: Geographic DTN Routing with Navigator Prediction for Urban Vehicular Environments," Mobile Networks and Applications, Springer, Feb. 2010.

[13] L. Wischhof, A. Ebner and H. Rohling, "Information dissemination in self-organizing intervehicle networks", IEEE Transactions on Intelligent Transportation Systems, vol. 6, no. 1, Mar. 2005.

[14] Y. Yang and R. Bagrodia, "Evaluation of VANET based advanced intelligent transportation systems", Proc. of the 6th ACM international workshop on Vehicular InterNETworking (VANET ’09), ACM Press, Sep. 2009.

[15] I. Leontiadis and C. Mascolo, "Opportunistic spatio-temporal dissemination system for vehicular networks", Proc. of the 1st international Mobisys Workshop on Mobile Opportunistic Networking (MobiOpp ’07), ACMPress, Jun.2007.