Information Table Based Decision Approach for Broadcast Storm Suppression in Vehicular Ad-hoc Networks

A Major Project Report submitted in partial fulfillment of the requirements for the Award of degree for

Bachelor of Technology

in

Electronics & Telecommunication Engineering

By

Aditya Om (12116005)

Krishna Narayan Mishra (12116031)

Rajat Chandrashekhar Shinde (12116057)

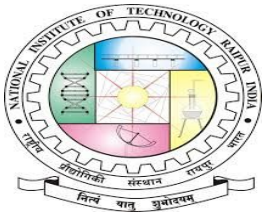
Sejal Agrawal (12116067)

Under the esteemed guidance of

Dr. A.S. Raghuvanshi

and

Mr. Shashank Gavel



NATIONAL INSTITUTE OF TECHNOLOGY, RAIPUR

Session: 2015-16

Information Table Based Decision Approach for Broadcast Storm Suppression in Vehicular Ad-hoc Networks

A Major Project Report submitted in partial fulfillment of the requirements for the Award of degree for

Bachelor of Technology

in

Electronics & Telecommunication Engineering

By

Aditya Om (12116005)

Krishna Narayan Mishra (12116031)

Rajat Chandrashekhar Shinde (12116057)

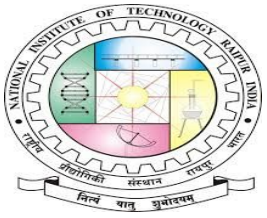
Sejal Agrawal (12116067)

Under the esteemed guidance of

Dr. A.S. Raghuvanshi

and

Mr. Shashank Gavel



NATIONAL INSTITUTE OF TECHNOLOGY, RAIPUR

Session: 2015-16

DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY RAIPUR

CERTIFICATE

This is to certify that the project entitled "Information table based decision approach for Broadcast Storm suppression in Vehicular Ad-hoc networks " submitted by **Aditya Om , Krishna Narayan Mishra, Rajat Chandrashekhar Shinde, Sejal Agrawal- Bachelor of Technology** in partial fulfillment of the requirements for the award of degree for **Electronics and Telecommunication Engineering** for the session 2015-16 at **National Institute of Technology**, **Raipur** is an authentic work carried out by them under my supervision and guidance. To the best of my knowledge, the matter embodied in this thesis has not been submitted to any other university/institute for the award of any degree.

Guided by:

Dr. Ajay Singh Raghuvanshi

Mr. Shashank Gavel

Dept. of ET&T Engineering

NIT RAIPUR, Chhattisgarh

Approved by:

Dr. Shrish Verma

Head of the Department

Dept. of ET&T Engineering

NIT RAIPUR, Chhattisgarh

DEPARTMENT OF ELECTRONICS & TELECOMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY RAIPUR

CERTIFICATE BY THE EXAMINER

This project work entitled **"Information table based decision approach for Broadcast Storm suppression in Vehicular Ad-hoc networks"** is successfully done **by Aditya Om(12116005), Krishna Narayan Mishra(12116031), Rajat Chandrashekhar Shinde(12116057), Sejal Agrawal (12116067)** under my supervision. This project report is submitted in the partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Electronics & Telecommunication Engineering**, offered by **National Institute of Technology Raipur** during the academic year **2015-16.**

Examiner 1

NAME :

DATE :

Examiner 2

NAME :

DATE :

ACKNOWLEDGEMENT

We, the students of 8th semester, Electronics and Telecommunication Branch, NIT Raipur, extend our heartfelt thanks to our project guide **Dr. Ajay Singh Raghuvanshi**, Assistant Professor, Electronics and Telecommunication Engineering, NIT Raipur, for providing us an interesting topic for our project work and guiding us at every juncture to complete it successfully. We also thank **Mr. Shashank Gavel**, Department of Electronics and Telecommunication Engineering, NIT Raipur for his support. Without their constant encouragement and guidance, this project would not have seen itself to this stage.

We also express our deepest gratitude to all staff members and friends for their encouraging support for the accomplishment of this project.

Aditya Om

8th Semester, ET&T

Krishna Narayan Mishra

8th Semester, ET&T

Rajat Chandrashekhar Shinde

8th Semester, ET&T

Sejal Agrawal

8th Semester, ET&T

DECLARATION

We hereby declare that the project entitled "**Information table based decision approach for Broadcast Storm suppression in Vehicular Ad-hoc networks"** being submitted in partial fulfillment for the degree of Bachelor of Technology in Electronics and Telecommunication engineering of NIT Raipur, is the authentic record of our own work done under guidance of Dr. A.S. Raghuvanshi, our project guide.

Project Members

1) Aditya Om

2) Krishna Narayan Mishra

3) Rajat Shinde

4) Sejal Agrawal

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

1.1 Ad-HOC NETWORKS

A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly" – anywhere, anytime. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts.

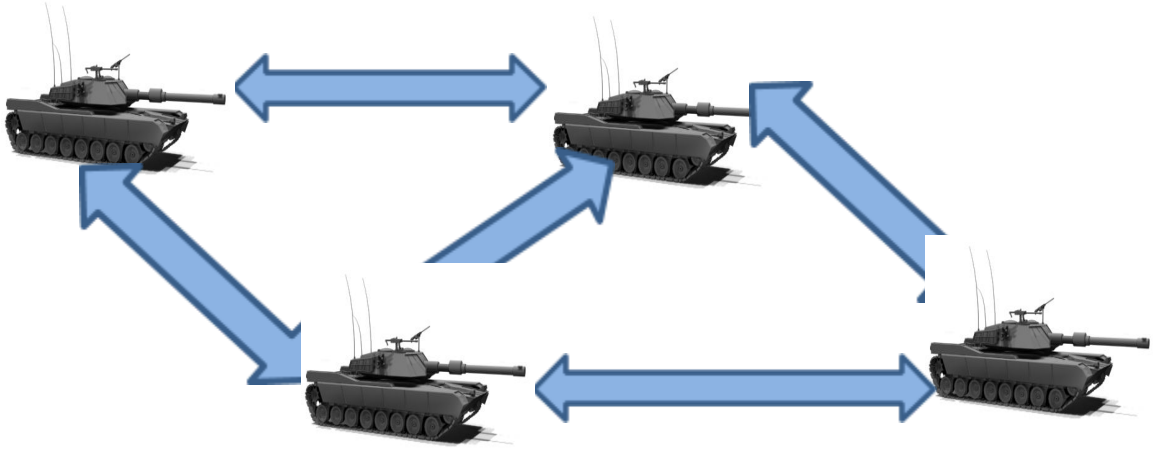
The earliest wireless ad-hoc networks were called "packet radio" networks, and were sponsored by Defense Advanced Research Projects Agency (DARPA) in the early 1970s. Bolt, Beranek and Newman Technologies (BBN) and SRI International designed, built, and experimented with these earliest systems. Experimenters included Robert Kahn, Jerry Burchfiel and Ray Tomlinson. Similar experiments took place in the Ham radio community. It is interesting to note that these early packet radio systems predated the Internet, and indeed were part of the motivation of the original Internet Protocol suite. Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. Another third wave of academic activity started in the mid-1990s with the advent of inexpensive 802.11 radio cards for personal computers. Current wireless ad-hoc networks are designed primarily for military utility.

A major limitation with mobile nodes is that they have high mobility, causing links to be frequently broken and need reestablishment. Moreover, the bandwidth of a wireless channel is also limited, and nodes operate on limited battery power, which will eventually be exhausted. Therefore, the design of a mobile ad hoc network is highly challenging, but this technology has high prospects to be able to manage communication protocols of the future.

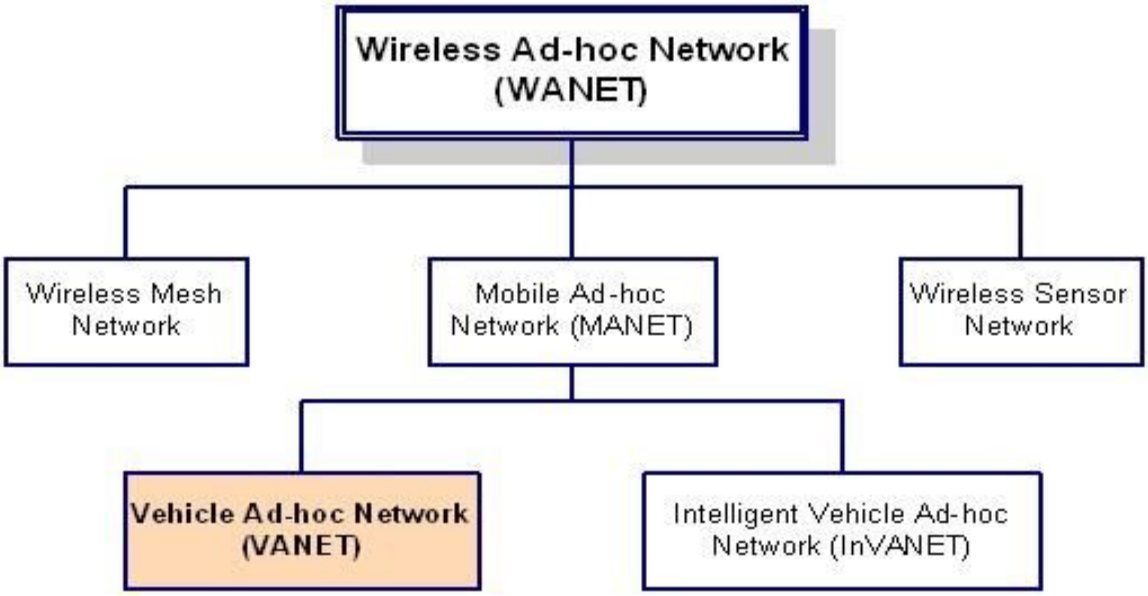
Applications of Ad-hoc Networks

Group of people with laptop with an aim to exchange files and data without having an access point.

It is suitable for military communications at battlefield where there is no network infrastructure.



Types of Ad-Hoc Networks



1.2 MANET

A **mobile ad hoc network** (**MANET**) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. *Ad hoc* is Latin and means "for this" (i.e., for this purpose).

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

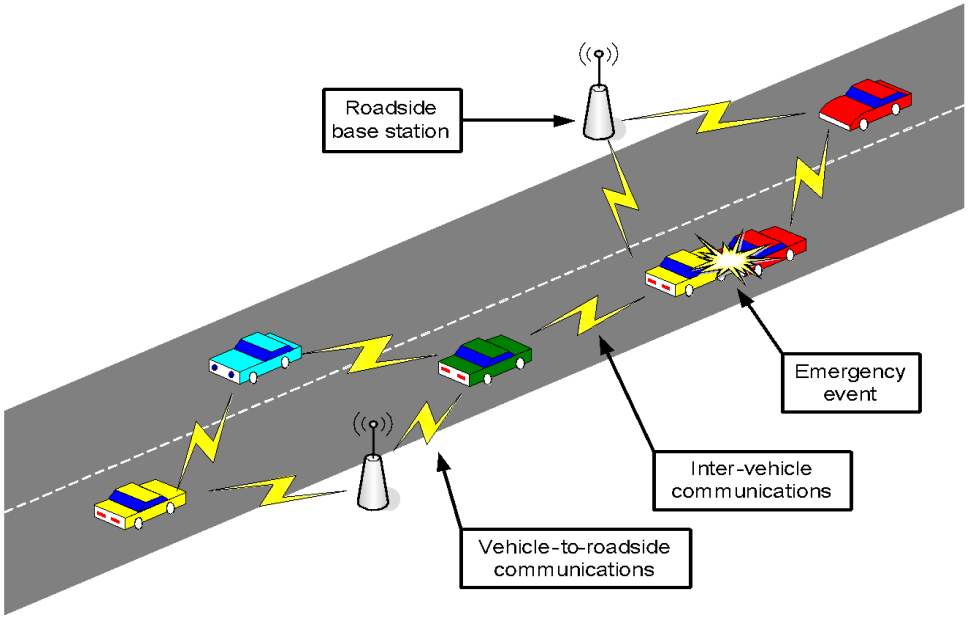
1.3 VANET

Vehicular Ad-Hoc Networks, (VANET), are a particular kind of Mobile Ad Hoc Network, (MANET), in which vehicles act as nodes and each vehicle is equipped with transmission capabilities which are interconnected to form a network. The topology created by vehicles is usually very dynamic and significantly non-uniformly distributed. In order to transfer information about these kinds of networks, standard MANET routing algorithms are not appropriate. The availability of navigation systems on each vehicle makes it aware of its geographic location as well as its neighbors. However, a particular kind of routing approach, called Geographic Routing, becomes possible where packets are forwarded to a destination simply by choosing a neighbor who is geographically closer to that destination. With the rapid growth of vehicles and roadside traffic monitors, the advancement of navigation systems, and the low cost of wireless network devices, promising peer-to-peer (P2P) applications and externally-driven services to vehicles became available. For this purpose, the Intelligent Transportation Systems (ITS) have proposed the Wireless Access in Vehicular Environments (WAVE) standards that define an architecture that collectively enables vehicle-to- vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. According to architectures of network, VANET can be divided into three categories, the first of which is the Wireless Wide Area Network (WWAN) in which the access points of the cellular gateways are fixed in order to allow direct communication between the vehicles and the access points. However, these access points require costly installation, which is not feasible. The second category is the Hybrid Wireless Architecture in which WWAN access points are used at certain points while an ad hoc communication provides access and communication in between those access points. The third and final category is the Ad Hoc V2V Communication which does not require any fixed access points in order for the vehicles to communicate. Vehicles are equipped with wireless network cards, and a spontaneous setting up of an ad hoc network can be done for each vehicle. This study will focus on studying ad hoc V2V communication networks, which are also known as VANETs. The purpose of VANET is to allow wireless communication between vehicles on the road including the roadside wireless sensors, enabling the transfer of information to ensure driving safety and planning for dynamic routing, allowing mobile sensing as well as providing

in-car entertainment. As VANETs have unique characteristics which include dynamic topology, frequent disconnection of the networks, and varying environments for communication, the routing protocols for traditional MANET such as Ad hoc On-demand Distance Vector (AODV) are not directly usable for VANETs. Researchers have developed a variety of efficient routing protocols for VANETs including Greedy Perimeter Stateless Routing (GPSR) ,Greedy Perimeter Coordinator Routing (GPCR); and GpsrJ+. The current issue, however, is that the range of the wireless 3 sensors on vehicles is limited to a few hundred meters at most and the traffic conditions in a vehicular urban environment often change dynamically. Other than that, VANET routing protocols also face other problems including the issue of unstructured roads, the difference in the sizes of the intersections in a certain area, the sharp curves of the roads, uneven slopes, and other obstacles such as large buildings, traffic lights, trees, and sign boards. As it is impractical to spend excessively on rebuilding or restructuring the existing roads in urban environments, a routing protocol for the purpose of a larger distance of data communication in one-to-one and one-to-many transfers specifically for VANETs need to be developed. This study will focus on the current challenges in the research of geographical routing protocols for real-time vehicular networks in urban environments.

Figure 1 :

A Typical VANET Scenario



Why VANETs ?

The following figures will answer this question. **Why VANETs?**

The first figure shows an accident occurred in the middle of the lane, thus, creating a chaos for the vehicles approaching the accident scene from different directions.

The Survey reveals some interesting facts related to our roads:-

- ✓ ***Safety***
  - ➢ On US highways (2004):
    - **42,800** Fatalities, **2.8 Million** Injuries
    - **$230.6 Billion** cost to society
  - ➢ Combat the awful side-effects of road traffic
    - In the EU, around **40,000** people die yearly on the roads; more than **1.5 million** are injured
- ✓ ***Traffic jams generate a tremendous waste of time and of fuel***

The next depiction shows a scenario of a highly congested road. Traffic jams waste time and fuel.

In 2003, US drivers lost a total of 3.5 billion hours and 5.7 billion gallons of fuel to traffic congestion.

All these problems can be mitigated to a significant extent by implementing VANETs. A sample automobile required to implement VANET is described below.

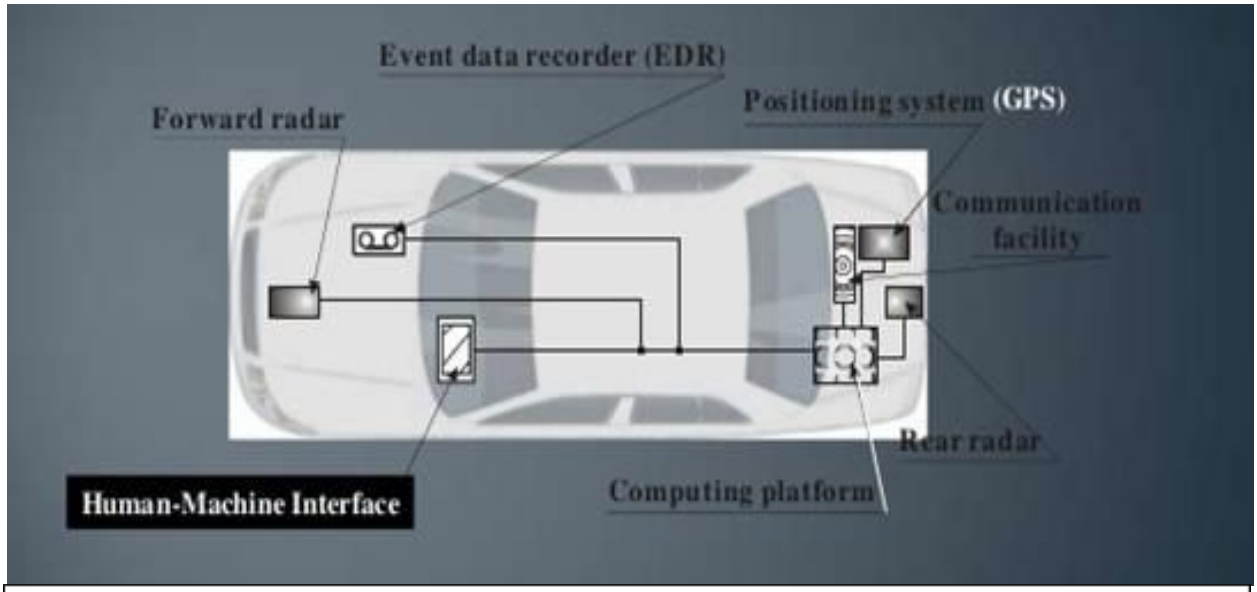


Figure: A Modern Vehicle. It is a network of Sensors/Actuators on wheels.

IEEE standard for Physical and MAC layers in VANET

As we have been discussing in this article unlike **MANETs, VANETs** have unique characteristics including high node mobility and a rapidly changing topology. VANETs should be designed to accommodate this characteristic. To do this, many researchers have proposed Media Access Control (MAC) protocols to improve the performance of VANETs. Most of these studies are quick message transmission to support the high mobility of nodes, multiple channels for multiple connections in urban areas, and channel coordination for these multiple channels and multiple connections. In order to improve VANET MAC protocols, **the IEEE 1609 Working Group (WG)** made up a standard VANET to support the data link layer of OSI layer 7 for Multi-channel Operations. To do this the **IEEE 1609 WG** adopted **IEEE 802.11p** as a subsystem. The IEEE 802.11p is designed to support multiple connections using Orthogonal Frequency Division Multiplexing (OFDM) in VANETs. Thus, it will support orthogonal channels between vehicles. However, even with these improvements, VANETs still have problems with traffic contention, hidden terminals, data transmission delays, decreasing throughput, and dynamic assigned channels for MAC protocols. Many researchers have proposed MAC protocols to improve the performance of VANETs.

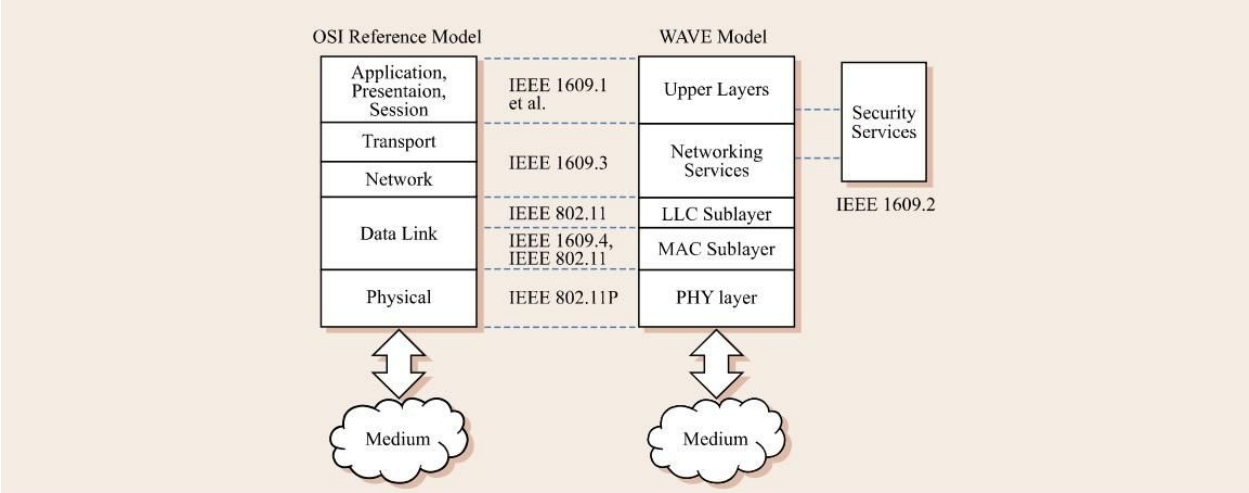


Figure: Relation of WAVE reference model and OSI reference model.

DSRC/ 802.11p

The **Dedicated Short Range Communication** was released in **2002** by the **American Society for Testing and Materials (ASTM)**.In **2003**, the standardization of this protocol was moved to IEEE forum and DSRC was changed to **WAVE (Wireless Ability in Vehicular**

Environments).The standard of **802.11p** is based on **IEEE 802.11a PHY layer** and **IEEE 802.11 MAC layer.**

1.4 Problem Statement

Vehicular ad hoc networks (VANETs) and Mobile ad hoc networks (MANETs) differ in many ways. First, VANETs consist of high mobility nodes moving in opposite or same directions. Vehicles moving along different, but nearby roads may or may not be able to communicate with one another due to small interaction time and obstacles. Second, the network shape description can be a more or less uniform one dimensional or strip in a non-chaotic scenario. Lastly, almost all applications for **VANETs** rely heavily on broadcast transmission for dissemination of traffic related information to all reachable nodes within a certain geographical area rather than a search request for route to an intended node.

Due to factors such as radio power limitation and channel utilization a mobile node may not be able to communicate directly with other nodes in a single-hop method. Particularly in this scenario, a multi-hop transmission occurs, where the packets sent by the source host are relayed by several intermediate hosts until the destination host is reached.

In our project, we try to identify and propose a solution to the problem of sending messages in a broadcast in a VANET.

Assuming that mobile nodes in the VANET share a single common channel with CSMA, but no collision detection capability. Synchronization in such a highly mobile network is difficult, and a general network topology information is not available to facilitate the broadcast scheduling. So the only solution is broadcasting by flooding. However it is observed that redundancy, contention, and collision could exist if flooding is done conventionally. Firstly, because the radio transmission is omnidirectional and a physical node position may be covered by the transmission ranges of neighboring nodes, similar repetitive rebroadcasts would be considered to be redundant. Second, heavy contention would exist because rebroadcasting nodes are close to each other. Third, collisions are more likely to occur because RTS/CTS dialogue is not applicable and timing of rebroadcasts is highly correlated.

All the above problems collectively have been considered as **BSP**. Various mitigation techniques have been introduced before for BSP in reference to **MANETS**. These methods generally involve reduction of possibility of redundant rebroadcasts by nodes in logical neighborhood and differentiating the rate at which selective rebroadcasting is done at each node. This gives arise to several schemes known as – counter based, cluster based, distance based, probability based and location based schemes. In our study we have considered **EIGRP** and **AODV's** distance based

routing algorithms as our basis for comparison with **MARS's** algorithm for performance metrics defined in the scenario created in **EXata** simulation environment.

Proposed Solution

To mitigate Broadcasting problem in VANETs we propose an **i-table (*information-table*)** based approach suggested as in **MARS algorithm** for packet forwarding in a non-chaotic scenario such as in Highway.

The rest of the report is organized as follows –Firstly, we provide the necessary research work related to the impact of the broadcast storm problem in VANETs. Then, we define the problem and assumptions. Thereafter, we propose our routing algorithm- **MARS** and analyze it in brief. Finally, the performance of the three broadcast techniques is presented along with the main findings and conclusions drawn from comparison.

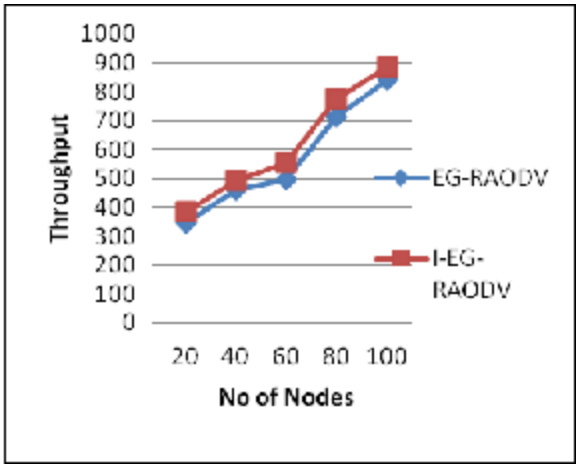
SECTION 2: Literature Review

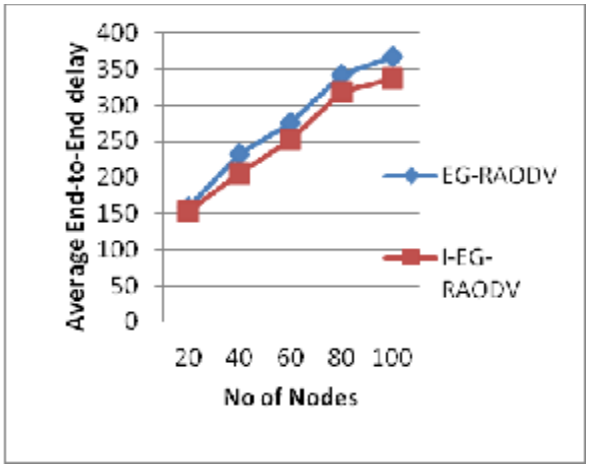
In the literature Review for each paper mentioned below the work of previous authors has been categorized under the following sections –

1. The main approaches
2. Methods of analysis
   a) Metrics
   b) Evaluation tools
   c) Analysis and interpretation of resulting simulation or measured data
3. Conclusions
4. Gaps/limitations that could be improved upon and ideas how this could be accomplished? Did all papers use a similar approach? Have they used the same criteria or method of analysis? If not what are the strengths/weakness of each method?

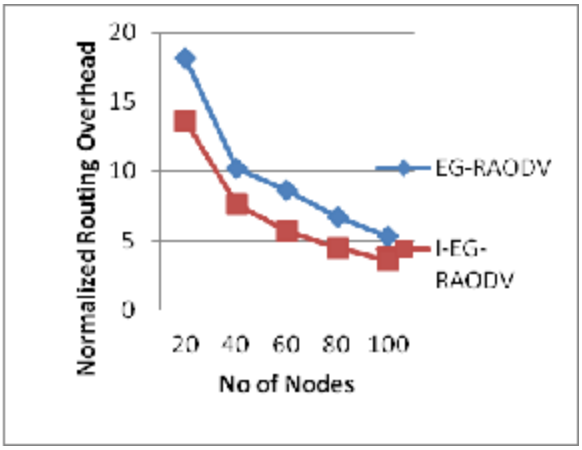
The Broadcast Storm Problem in Mobile Ad Hoc Network, by Mr. S-Y. Ni, Y-C Tseng, Y-S. Chen, and J-P Sheu

In a wireless ad hoc network to disseminate information to an area greater than that covered by the transmission range of a node, multi-hop relaying is used. The simplest way to perform multi-hop relaying is by flooding a packet. In this situation, when a node receives a broadcast message for the first time, the node then re-transmits the message. The node then ignores all subsequent broadcast messages it receives from other nodes, which are also rebroadcasting the message. There are three problems associated with flooding. First, there are a number of redundant rebroadcasts because of flooding. An instance of how serious this problem is when a message is to reach n hosts, the packet will be sent n times.





Second contention occurs, there is a high probability that a message will be received by many hosts in a close proximity and when these hosts try to rebroadcast the message. Each host will severely contend with each other for access to the medium. Third, a large number of collisions can occur because of the lack of RTS/CTS and because of the absence of collision detection. The authors of the paper term this problem the "broadcast storm problem". The authors evaluate the significance of the three problems related to the broadcast storm problem, and show how serious the problem truly is. To begin, a rebroadcast of a message will only provide 0 ~ 61% additional coverage.



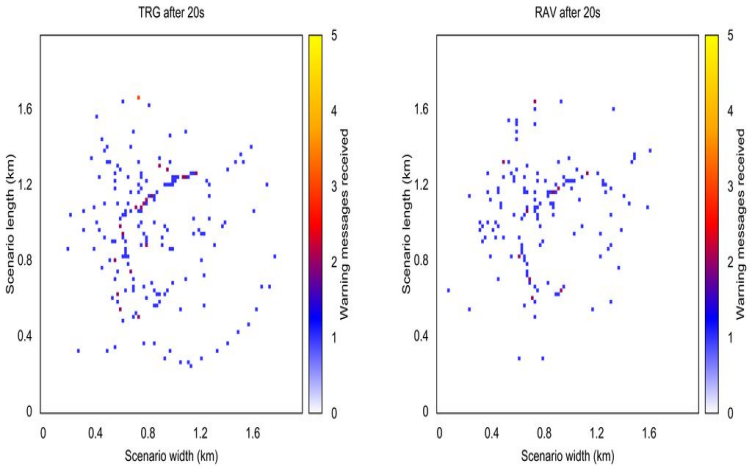
On the average, a rebroadcast will cover only an area of an additional 41%. The additional coverage dramatically decreases based on the number of times k that a message is heard being rebroadcast from other nodes. When k >= 4 the additional expect coverage is less than 0.05%. Also, the contention is expected to be higher as the number of nodes n increases. The authors show that probability of all n nodes experiencing contention increases rapidly to 0.8 when n >= 6. The results show that the denser a network is the less chance of a node being able to access the medium without experiencing contention. Last, the number of collisions that occur from broadcasting a message is high for a number of reasons, such as the PCF is not available, the RTS/CTS exchange can not be used, and collision detection is not used in wireless networks.

The Main Approaches

There are two possible solutions to reduce the effects of the "broadcast storm problem", which are to reduce the possibility of rebroadcasts or to differentiate the timing of rebroadcasts. **There are five possible schemes proposed by the author to alleviate the broadcast storm problem.**

First, a probabilistic scheme aims to limit the number of rebroadcasts. When a node receives a broadcast for the first time the message is rebroadcast with a probability P. otherwise, the node discards the packet. Moreover, when P = 1, this scheme tends to the flooding condition

Second, a counter is used to track the number of times a message is being heard before a node has a chance to rebroadcast the message. In this scheme, Tseng et al showed that when k is greater than or equal to 4 **(*k is number of times the message is heard after being rebroadcasted by other nodes*)** the additional coverage of a rebroadcast decreases rapidly. This scheme basically prohibits the rebroadcast when **c ≥ C**, where **c** is the number of times a broadcast has been heard and **C** the counter threshold



(a) (b)

Third, The **distance-based scheme** rebroadcasts a message depending on the distance between the sender and receiver. A parameter D_{min} is used to record the distance between the sender and receiver of the broadcast. If $D_{min} < D_{th}$ ($\mathbf{D_{th}}$ is the threshold value) , then the broadcast is prohibited from being forwarded.

Fourth, In **Location-based scheme** the coverage area is calculated with precision. A GPS device is used to locate the broadcasting nodes. If the additional coverage of a message is greater than a threshold the message is re-broadcasted .One possible solutions to calculate the additional coverage area is based on geometrical modeling using convex polygons. These three scenarios were discussed by *Ni et al* :

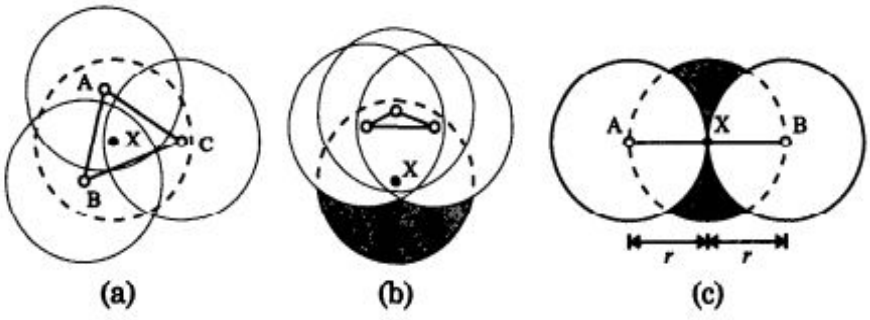


Fig. - Method of convex polygons to determine whether to rebroadcast or not :

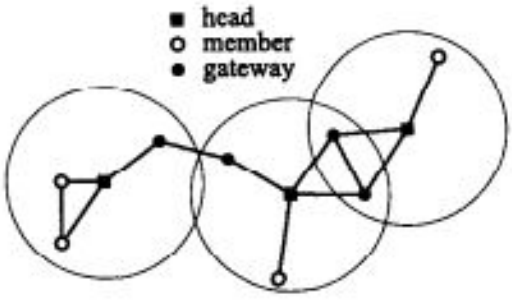
(a) X is inside the triangle formed by three senders nodes (A, B &C)

(b) X is outside of the polygon.

(c) Analysis of maximum loss of additional coverage

Lastly, In cluster based scheme network is partitioned into clusters. A host with *a local minimal ID* is self-elected as a *cluster head* and all neighboring hosts of a head are members of the cluster recognized by the *ID* of the head. A gateway member is also present within the cluster that can communicate with the head of other clusters and propagates the broadcast message through the head to its corresponding hosts. This method is more commonly followed in regular MANETs with fixed topology.

The following representation was shown by *Ni et al* to classify the various cluster members :



Methods of Analysis

A number of simulations are used to determine the effectiveness of the five proposed broadcast mechanisms.

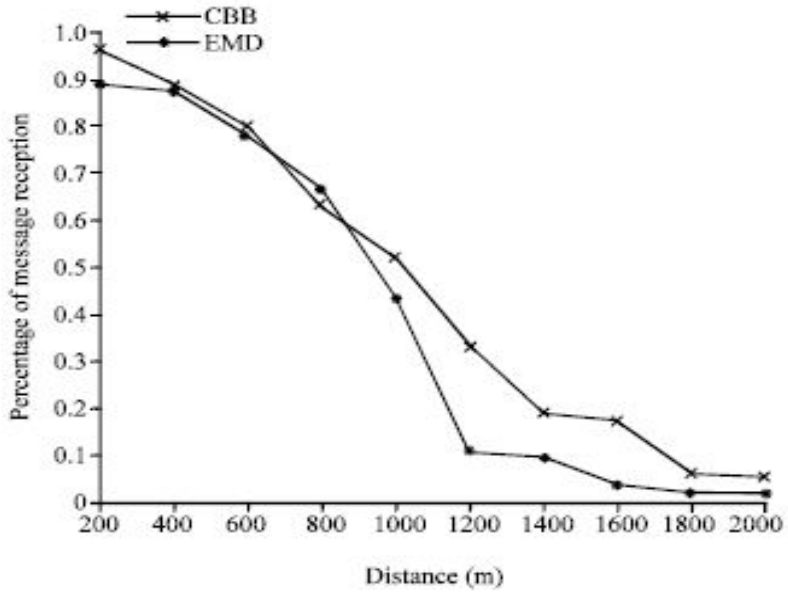
a) **Metrics:** Three metrics were used to evaluate the protocols: *reachability*, *saved rebroadcast* and *average latency*. ***Reachability*** is the number of host that received the broadcast divided by the total number of hosts. ***Saved rebroadcast*** equals (r-t)/t where r are the number of hosts that received the broadcast message and t are the hosts that actually transmitted the message. Last, **average latency** is the time from when the broadcast was initiated till the time the last host received the broadcast message.

b) **Evaluation Tools:** The authors developed a simulator written with C++. The parameters used for the simulation are 500m transmission radius, 280 byte packet size, and 1 Mbs transmission speed. The simulations uses 100 mobile hosts and which are randomly placed on a number of different maps. The maps range from a 1 x 1 to a 10 x10 unit map, where each unit is a 500 meters.

c) **Analysis:** The probability simulation shows that a small probability is sufficient to achieve a high reachability, when a map is densely populated. On the other hand, in the case of a sparse map a high probability value is needed to achieve a high level of reachability. Saved rebroadcasts also decrease as P increases, when P is set to one the protocol performs identical to flooding. Next, the counter-based scheme achieves the same level of reachability as the probability-based scheme when the threshold counter C is set greater or equal to 3. High density maps exhibited a 27~67% SRB when C is set to 3, while the spares maps achieve less savings.

```
Procedure receive_message
1  if x > R_target then                                   /* stopping condition */
2      return;
3  if new packet or (backwards SCF packet and I travel in the message direction) then
4      if x < r − Δt_max(v_last + v_new) then
5          start_timer(W);
6  else
7      if waiting W then
8          update closest relay position;
9      else if waiting t_w|t'_w|t''_w then
10         cancel retransmission;
11     else if SCF activated then
12         if TTL > my hop count then                     /* there is a new relay */
13             deactivate SCF;
14             if x < x_newrelay then
15                 repeat message;
16         else if TTL = my hop count and x + v_limit W < x_newrelay then   /* simultaneous
           retransmissions: selection of the furthest relay */
17             deactivate SCF;
```

The third simulation was the distance-based scheme which achieved better results for reachability, but did not save much in terms of the number of rebroadcasts. The distance simulation also had a higher broadcast latency than the counter-based scheme. Next, the location-based scheme performed the best out of all of the schemes that were simulated.



The benefit of using this scheme is it uses exact information to calculate the additional coverage area. Some of the other schemes did not perform well when simulated with sparse maps, but this was not the case with the distance-based scheme. Last, a cluster-based scheme that incorporates the distance-based scheme to send messages between clusters was evaluated. The cluster-based scheme performed better than the distance-based scheme in terms of rebroadcasts and latency. The problem with the cluster-based scheme is the reachability was poor when the maps were sparse. One possibility for why the reachability suffered is because of the hidden terminal problem, when two gateways in different clusters forward a broadcast at the same time to the same neighboring cluster a collision will occur. The simulation were also studied under a number of packet generation rates as the generation rate increased the reachability in the simulations degraded because of a greater number of collisions.

Conclusions

The paper addressed how serious the broadcast storm problem is. *The authors introduce five schemes that improve on simple flooding. Some of the schemes presented in the paper performance rely on the topology of the network, with some of the schemes performing poorly in sparse networks*. A simple counter-based scheme offers a tremendous improvement over flooding. The authors show that a location-based scheme performs the best under all situations. An area of possible future work is incorporating the schemes given in the paper into a reliable broadcast protocol.

Additional Questions

The paper was one of the first papers to address how serious the problem is with using flooding to broadcast messages in a mobile ad hoc network. One problem is each of the schemes

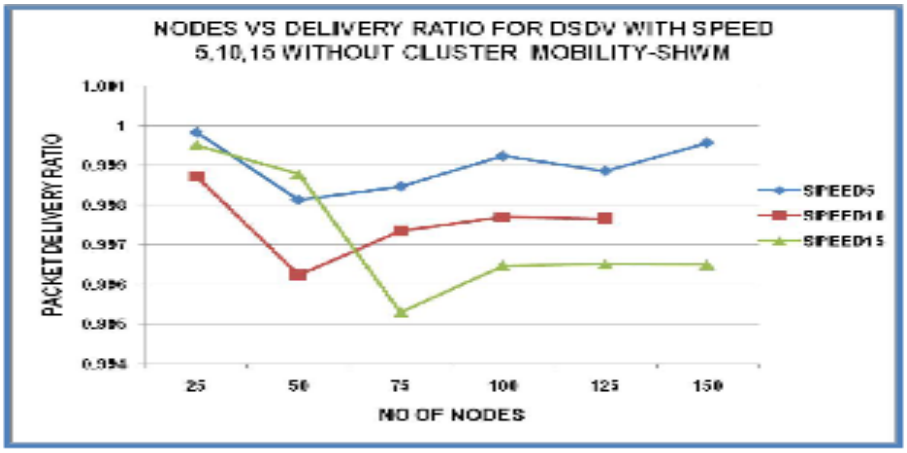
presented in the paper sets the parameters used by the protocols statically. One possible improvement to the presented schemes is changing the parameters dynamically based on the conditions of the network. One additional way that the algorithms may be improved is by dynamically changing the transmit power of the mobile host based on the density of the network. The paper showed that not all of the schemes performed well when the network was sparse. Based on the work done in this paper, many others have used variation of these algorithms for broadcasting in mobile ad hoc networks.

Vehicle-to-Vehicle Safety Messaging in DSRC, by Q. Xu, T. Mak, and R. Sengupta

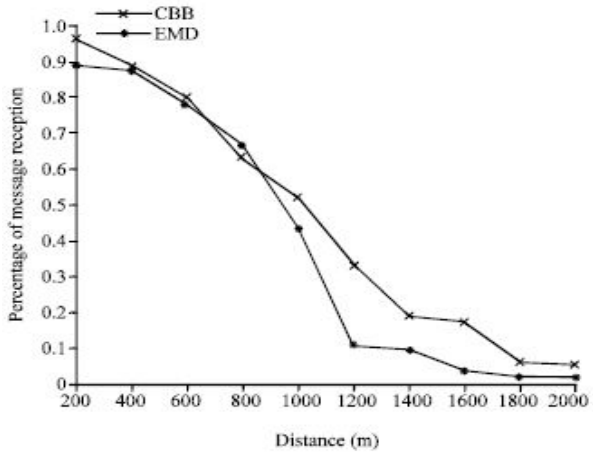
The paper addresses the feasibility of sending messages in DSRC. Broadcast messages are assumed to be used to for sending safety related information on the control channel of DSRC. The authors address sending broadcast messages in a single-hop scenario.

The Main Approach

To increase the chance of receiving a message a broadcast messages are repeated k times. Since it there are no guarantees that a message will be received when it is broadcasted, the message is repeated a number of times in the hope that the message will eventually be successfully received.



The authors explore the use of six different MAC protocols. The first four protocols use a MAC layer extension, which is placed between the 802.11 MAC and logical link layer. The final two protocols that are evaluated define a new MAC protocol. The first protocol is Asynchronous Fixed Repetition (AFR), k distinct slots are randomly selected among n total slots. Packets are always repeated a fixed number of times k and no carrier sensing is used. Second, Asynchronous p-persistent Repetition (APR) is similar to AFR except the number of repetitions of a message varies. The probability that a message will be transmitted p=k/n where k is a configuration parameter and n is the number of message slot available in the lifetime of the message.



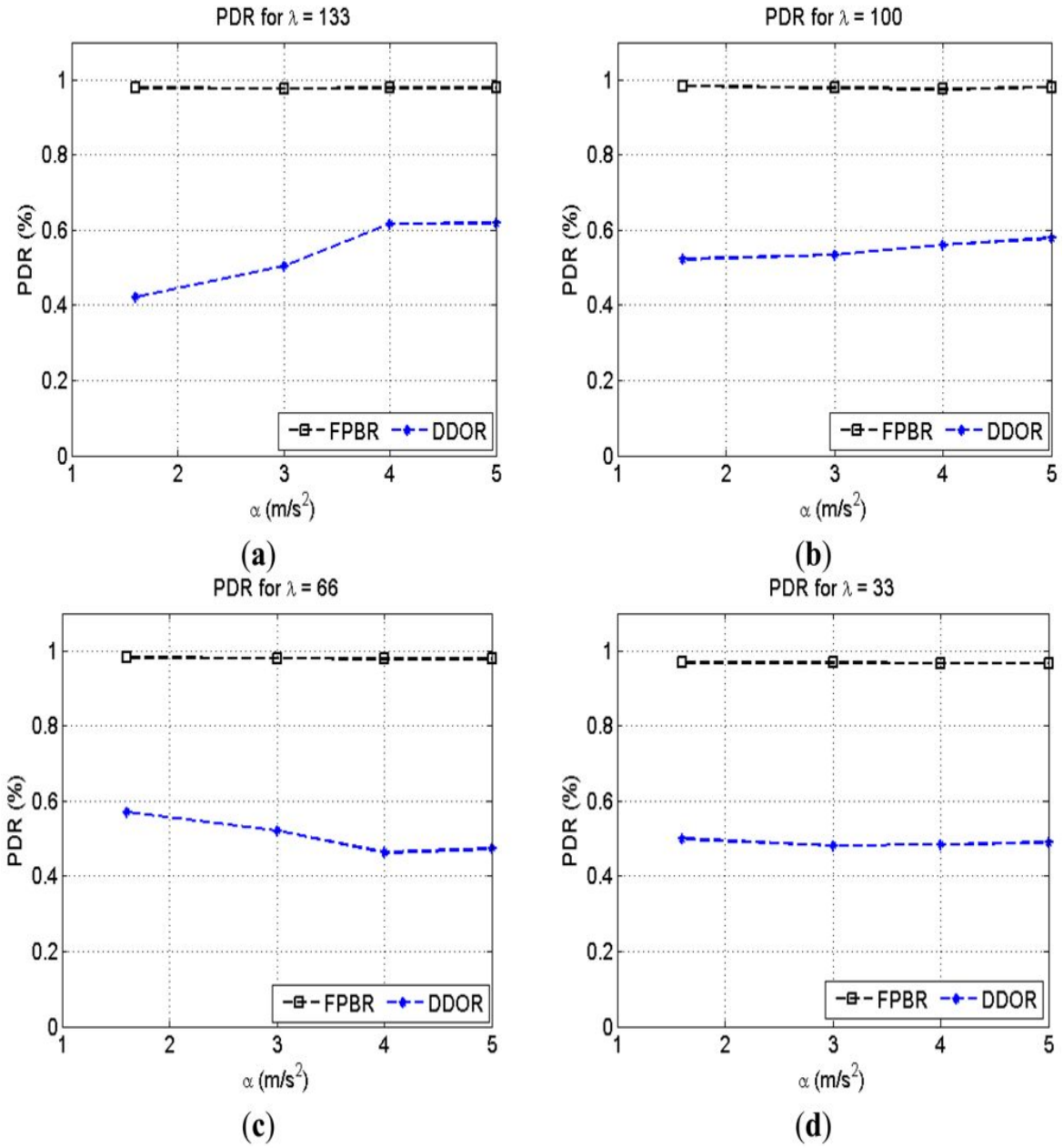
Third, Synchronous Fixed Repetition (SFR) is the same as AFR except that the slots used to transmit messages are synchronized to a global clock. Forth, Synchronous persistent Repetition (SPR) is the same as SFR, with the synchronization of transmissions to common slots, except it uses p-persistence. Fifth, Asynchronous Fixed Repetition with Carrier Sensing (AFRCS) generates repetitive packets the same as AFR the difference is this protocol uses carrier sensing. When a node has a packet to send it senses if the channel is busy. If another transmission is currently underway the packet is then dropped. On the other hand, if the medium is free the node broadcasts the packet. Sixth, Asynchronous p-persistent Repetition with Carrier Sensing (APR-CS) is the same as 3 AFR-CS except message slots are selected in a p-persistent manner.

Methods of analysis

The authors of the paper run a number of simulations to test the six MAC protocols they developed.

a) **Metrics**: The authors use two main metrics to evaluate the proposed protocols. First, ***Probability of Reception Failure (PRF)*** measures the probability of a message not be received at a certain distance within the lifetime of the message. Second metric that is evaluated is ***Channel Busy Time (CBT)*** which is the $\boldsymbol{CBT = T_{safety}/T}$, where $\boldsymbol{T_{safety}}$ is the total amount of time the channel is transmitting safety messages and T is the total time. CBT is measured because the channel will also be used by non-safety applications, so it is important the channel is not saturated with broadcast messages.

b) **Evaluation Tools**: The protocols are simulated using ***SHIFT*** and ***NS-2. SHIFT*** is used to simulate the traffic used in the simulation. The *Friis Free-space and two-ray models are used to determine receive power.*

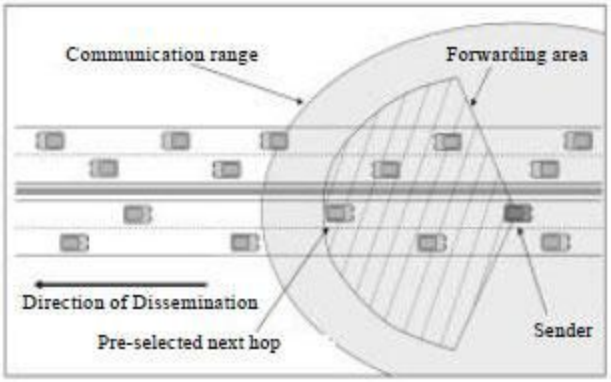


c) **Analysis**: The simulations show that there is an optimum number of repetitions, which depends on message range, traffic density, message size, etc. The simulations showed that the protocols that performed the best are the AFR-CS and SFR. *The best protocol was AFR-CS since it does not rely on the global synchronization of nodes.* The synchronous protocols out -perform the asynchronous equivalents, because the synchronous protocols eliminate the partial overlapping of packets. The fixed repetition protocols also outperformed the p-persistent protocols because there is less fluctuation in the number of packets sent. Finally, the protocols which used carrier sensing

outperformed those which did not carrier sensing. An inverse relationship between CBT and PRF was found until the optimum number of repetitions is reached.

Conclusions

The authors conclude it will be feasible to use 802.11a for DSRC, if the protocol designers and applications designers work together. The authors found it is possible to send broadcast messages every 200 ms to 140 points with 250 bytes of data.



GPS devices typically are updated at 5 Hz, so sending a message every 200 ms should be acceptable. A broadcast protocol does not need to have a 100% guaranteed rate of reception. An acceptable approximation of vehicular map can be created with a PRF of 1/100.

Additional Questions

One of the problems with this approach is that it is only a single-hop broadcast; it is unlikely that the protocol would support the multi-hop relaying of broadcast messages. If multi-hop relaying was used the CBT would likely rise to an unacceptable level. One weakness is the study doesn't measure the number of collisions that occur from broadcasting a message multiple times. One approach recommended by the authors to improve there protocol is to implement an adaptive control at the MAC layer. Protocols such as the one suggested by the authors could be used to passively construct the topology of the vehicles.

Mitigating Broadcast Storm Problems in Vanets by Mohd Umar Farooq and Khaleel Ur Rahman Khan

This paper proposes a strategy to overcome the broadcast storm problem in Vanets using the bounding algorithm. The analysis and simulation results illustrate better performance by a hybrid approach presented by combining the advantages of distance-based and counter-based schemes in terms of reachability and saving of rebroadcasting which performs efficiently.

Main Approach

The simple broadcasting without a rebroadcasting bounding mechanism at each node may result in an excess of redundancy, channel contention, and collisions. This phenomenon is called the *Broadcast Storm Problem* Redundancy indicates a situation where a node hears the same messages from more than one neighbors. Channel contention is due to the different nodes which are simultaneously trying to rebroadcast the received messages thus contending for the shared media, increasing the probability of collisions.

The counter-based and distance-based schemes canbe candidate solutions to efficiently address the well known broadcast storm problem. Moreover, location based approach, despite being a better option, is only meaningful when all nodes have GPS devices. In this paper, a re-broadcasting bounding algorithm has been presented which is based on both schemes to obtain an increase in reachability while highly reducing the amount of packets re-broadcasted.

According to the distance-based scheme, when a broadcast packet is sent, the receiving nodes re-send it only if the node is located farther than *DTH*. In this latter situation, a small counter threshold avoids the nodes passing the distance threshold test from rebroadcasting the message though the decreasing reachability. Therefore, a larger counter threshold is used when applying the counter-based scheme to the nodes located above the distance threshold. The bounding algorithm is the following :

S1*: Set dmin to the distance to the broadcasting host. If this is the first time message msg is received initialize counter c = 1, otherwise increment c by one.*

S2*: if dmin < DTH, proceed to S5. If c < CTH, proceed to S3. If c = CTH, proceed to S5*

S3*: Wait for a random number (0 ~ 31) of slots. If msg is heard again, interrupt the waiting and return to S2.Otherwise, submit msg for transmission, wait until the transmission actually starts and proceed to S4.*

S4*: The message is on the air. The procedure exits.*

S5*: Cancel the transmission of msg if it was submitted in S3. The host is prohibited from rebroadcasting the same message in the future. Then the procedure exits.*

Suppose two nodes A and B receiving a message broadcast by a sending node S. They are located farther than *DTH* from node S. If the expiration of node A waiting timer allows it to rebroadcast the message before node B timer expires, and they are respectively located within *DTH*, node B is also prohibited from rebroadcasting without being affected by the counter threshold. As shown in Figure below, node S initially broadcasts a message to the nodes within

its transmission range. Then, they decide whether or not to rebroadcast the message according to the distance between themselves and node S. While the nodes within *DTH* from node S are prohibited from rebroadcasting, the others (the nodes in the shaded area as shown in Figure) determine their random waiting timers.

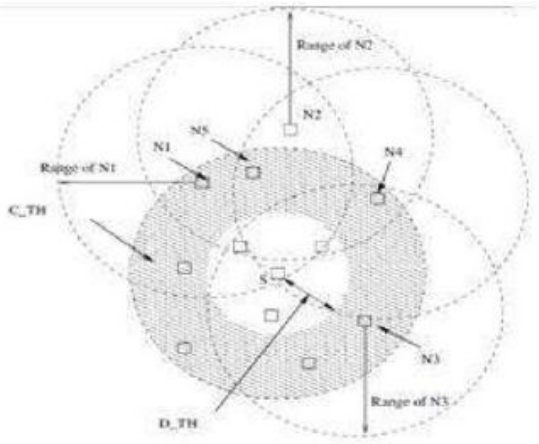


figure : Bounding Algorithm related scenario

Suppose that, the waiting timer of node N1 expires first. Then, node N5 is also refrained from rebroadcasting because it is located within *DTH* with respect to node N1. However, node N2 can be given a chance to rebroadcast the message because it is located above the distance threshold from node N1. If the waiting timers of nodes N2 and N3 expire earlier but not simultaneously than that of node N4, in addition to the message sent by node S, when node N4 hears the same message from nodes N2 and N3 before its waiting timer expires, it determines whether or not to rebroadcast according to its counter value. For example, if *CTH* is set to 3, the node N4 cannot rebroadcast the message.
Otherwise, if *CTH* is greater than 3, the node is allowed to re broadcast the message.

The Bounding Algorithm :-

```
procedure bounding(msg)
d_min = d_s
if (tcount(msg) == 1) then
   if (dmin < DTH) then
      inhibit msg rebroadcasting
   else
      wait for a random number (0 ~31) of slots
send msg
   endif
else
   if (tcount(msg) < CTH) and (dmin < DTH)
   then wait for a random number (0 ~ 31) of slots
    send msg
   else
    cancel waiting
    inhibit msg rebroadcasting
   endif
endif
```

Method of Analysis :

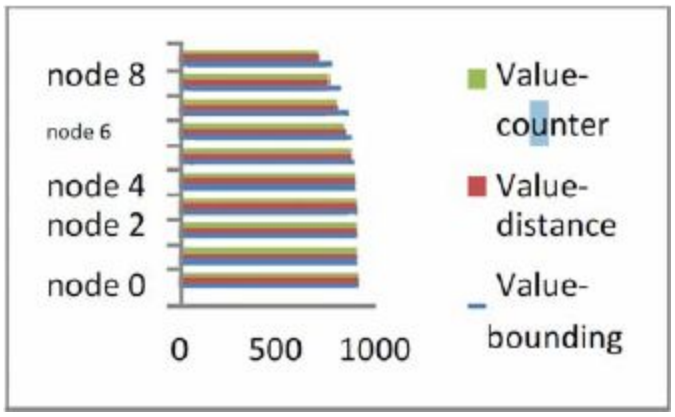
a) Performance Metrics

In this paper, authors have compared the proposed hybrid protocol with counter and distance based schemes on the basis of the following metrics :

1) Distance Covered
2) Reachability
3) Number of packets sent
4) Number of received broadcasts

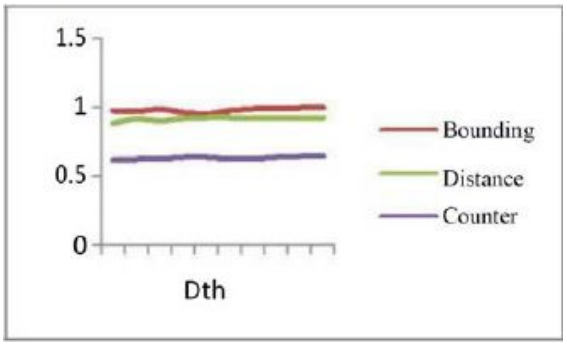
b) Analysis of measured data

Over the same given distance of about 1000 meters, the distance that is being covered by the 3 different schemes i.e. Counter-based flooding, Distance-based flooding and Bounding-based flooding. The below given graph (b (1)) shows the total **distance that is being covered** by the 10 nodes.



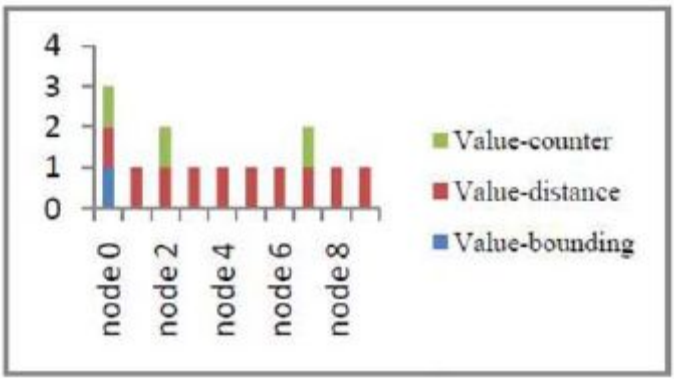
Graph : b(1) ; Comparison between three approaches on the basis of Distance covered

The main aim of bounding-based flooding is to increase the **reachability** of a single node. A close analysis of the graph b(2) shows that the single node that broadcasts the initial packet to all the other nodes when they are within its distance range thereby eliminating the rebroadcasting of the same packet by various other nodes present in its range. The task of preventing the same packet to be broadcasted by the other nodes is handled by the counter-scheme in the algorithm that is proposed.



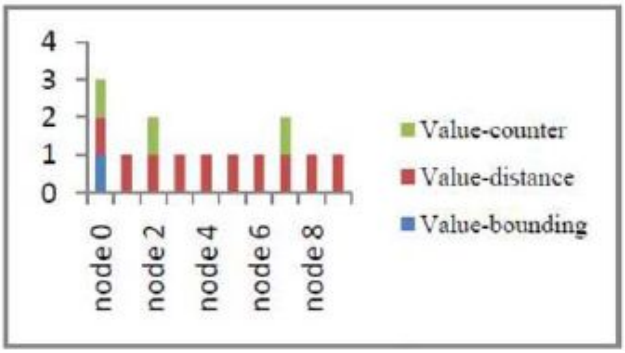
Graph: b(2)- Comparison between three approaches on the basis of reachability

To reduce the **number of the packets that are being sent** over a network, the bounding algorithm makes sure it uses the counter scheme which helps in decrease in the number.
It clearly has an upper hand over the distance-based scheme as well as the counter-based scheme. The graph b(3) justifies the reduction in channel contention by keeping the broadcast packets to as minimal as possible.



Graph: b(3)- Comparison between three approaches on the basis of number of packets being sent

The **number of broadcasts that are being received** have also been reduced as only the node that initializes the data dissemination sends the packet to all the other nodes present. This shows an improvement over both the schemes. See the graph b(4) for this performance metric :



Graph b(4)- Comparison between three approaches on the basis of broadcasts received

Conclusion :

The following hybrid approach combines the advantages of distance-based and counter-based schemes in terms of reachability and saving of rebroadcasting without the overhead of equipping all nodes with GPS devices as required by the location-based scheme. The counter-based constraint on the nodes located above the threshold is done to avoid excessive rebroadcasting. Simulations have asserted, that approach can be one of the acceptable solutions to satisfy two goals, high reachability and low redundancy.

Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks by N. WISITPONGPHAN and O.K. TONGUZ

In this paper, authors introduced three probabilistic and timer-based broadcast suppression techniques: *weighted p-persistence*, *slotted 1-persistence*, and *slotted p-persistence schemes*, to be used at the network layer. Their simulation results show that the proposed schemes can significantly reduce contention at the MAC layer by achieving up to 70 percent reduction in packet loss rate while keeping end-to-end delay at acceptable levels for most VANET applications.

Main Approach

Weighted p-Persistence Broadcasting **Rule** — *Upon receiving a packet from node* i*, node* j *checks the packet ID and rebroadcasts with probability* **pij** *if it receives the packet for the first time; otherwise, it discards the packet.*

Denoting the relative distance between nodes *i* and *j* by *Dij* and the average transmission range by *R*, the forwarding probability, *pij*, can be calculated on a per packet basis using the following simple expression:

$$p_{ij} = \frac{D_{ij}}{R}$$

Unlike the p-persistence or gossip-based scheme, weighted p-persistence assigns higher probability to nodes that are located farther away from the broadcaster given that GPS information is available and accessible from the packet header. This is shown in Figure 4(a)

Slotted 1-Persistence Broadcasting **Rule** — *Upon receiving a packet, a node checks the packet ID and rebroadcasts with probability* ***1*** *at the assigned time slot* TS_{ij} *if it receives the packet for the first time and has not received any duplicates before its assigned time slot; otherwise, it discards the packet.*

Given the relative distance between nodes i and *j*, *Dij*, the average transmission range, *R*, and the predetermined number of slots *Ns*, TS_{ij} can be calculated as :

$$T_{Sij} = S_{ij} \times \tau$$

where **τ** is the estimated one-hop delay, which includes the medium access delay and propagation delay, and ***Sij*** is the assigned slot number, which can be expressed as

$$S_{ij} = N_s \left(1 - \left\lceil \frac{\min(D_{ij}, R)}{R} \right\rceil \right).$$

For example, in Fig. 4 (b) the broadcast coverage is spatially divided into four regions, and a shorter waiting time will be assigned to the nodes located in the farthest region. Hence, when a node receives duplicate packets from more than one sender, it takes on the smallest *Dij* value .

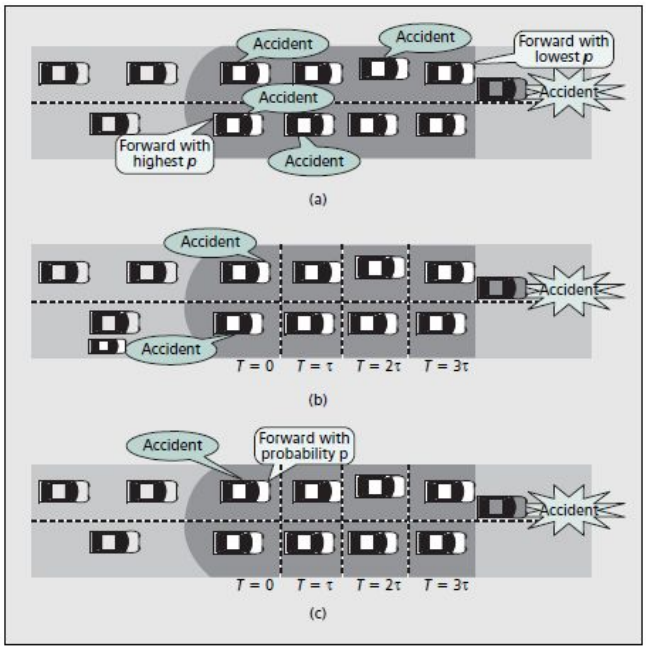


Fig 4 : -Proposed Broadcast Supression Techniques :- a) weighted p-persistence , b) slotted 1-persistence , c) slotted p-persistence.

***Slotted p-Persistence Broadcasting* Rule** — *Upon receiving a packet, a node checks the packet ID and rebroadcasts with the pre-determined probability* p *at the assigned time slot* TSij*,as expressed above in slotted l-persistence, if it receives the packet for the first time and has not received any duplicates before its assigned time slot; otherwise, it discards the packet.* Fig 4 (c) illustrates the concept of slotted p-persistence with four slots.
Similar to the p-persistence case, the performanceof this scheme also depends on the value chosen for the reforwarding probability *p*.

Method of analysis :

a) **Performance Metrics** :

For Single Lane Topology metrics used are link load and Packet penetration rate. However, in multilane topology which is modelled using many single land networks
Packet loss ratio and total end to end delay (Latency) has been used as metrics.

b) **Analysis of simulated/measured data** :

1) Single lane Topology **:**

Assumptions :-Each node has a broadcast range of 500 m. The slot size is assumed to be 100 m so that the broadcast coverage can be divided into five time slots. The reforwarding probability is assumed to be 0.5

Link Load :— The link load measures the amount of broadcast traffic received at each node over a unit time. Obviously, the higher the load, the lower the useful throughput
The link load is reduced dramatically when the slotted scheme is employed.

Figure 5 shows the link load, normalized with respect to the link load measured from the 1-persistence case

Packet Penetration Rate:- In a typical route discovery case where the source seeks to establish a route to a known destination, Packet penetration rate also affects the route acquisition time: the faster the packet penetration rate, the faster the route acquisition time.

Figure 5 shows the packet penetration rate normalized with respect to the rate achieved by the conventional 1-persistence scheme.

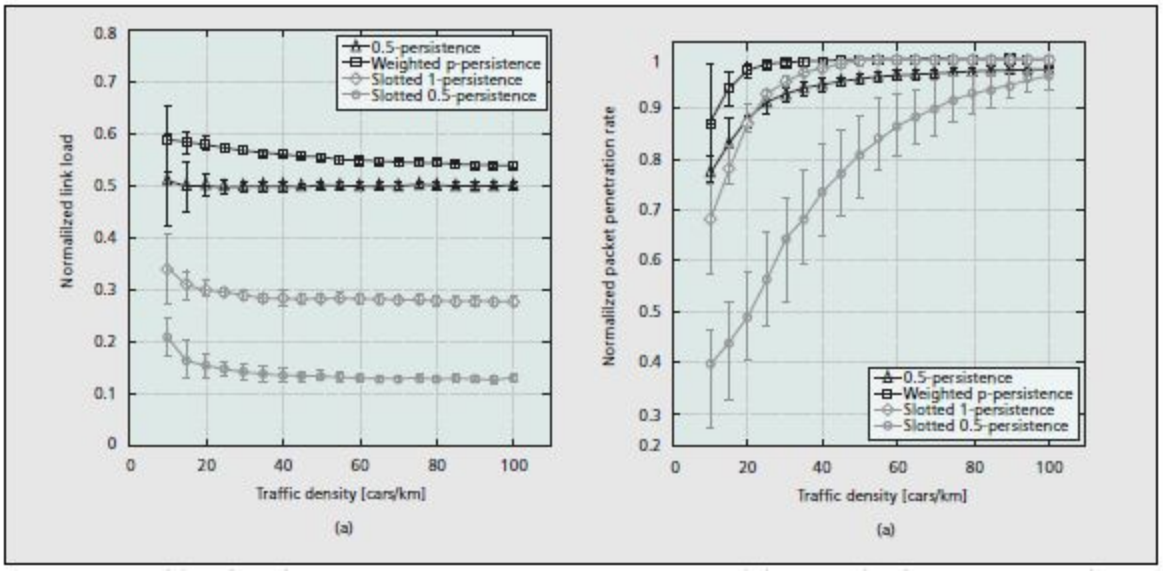


Figure 5 : Link load and Packet Penetration ratio measured from a single-lane network with random traffic distribution

2) Multilane Topology**:**

Assumptions: A multilane network is simply a collection of multiple single-lane networks. In this paper, authors have assume that the traffic in each lane is identically distributed, overall traffic density will increase by *n*-fold in an *n*-lane network.*They have* considered 1000 simulation runs of a 10 km road section with four lanes and random traffic, The WAIT_TIME is assumed to be 5 ms, and the slot size is approximately 200 m, so there are approximately five slots. The forwarding probability is set to 0.5

Packet Loss Ratio *:* Without using any of the suppression schemes, the packet loss ratio is 60 percent in the worst case. By making use of GPS or RSS information, it is possible to reduce this high loss ratio in the worst case by up to 90 percent; that is, from 60 percent down to about 5 percent if one uses the slotted p-persistence approach .**Fig. 6(a)** shows that among the three schemes proposed, slotted p-persistence yields the best performance while the worst scheme is weighted p-persistence.

Latency*:* The total end-to-end delay of the proposed schemes, on the other hand, is significantly longer than that in the 1-persistence case, especially in a sparse network. As shown in **Fig. 6(b)**, the total delay increases from 15 to 125 ms under light traffic conditions with 10 cars/km/ lane when slotted p-persistence is used.

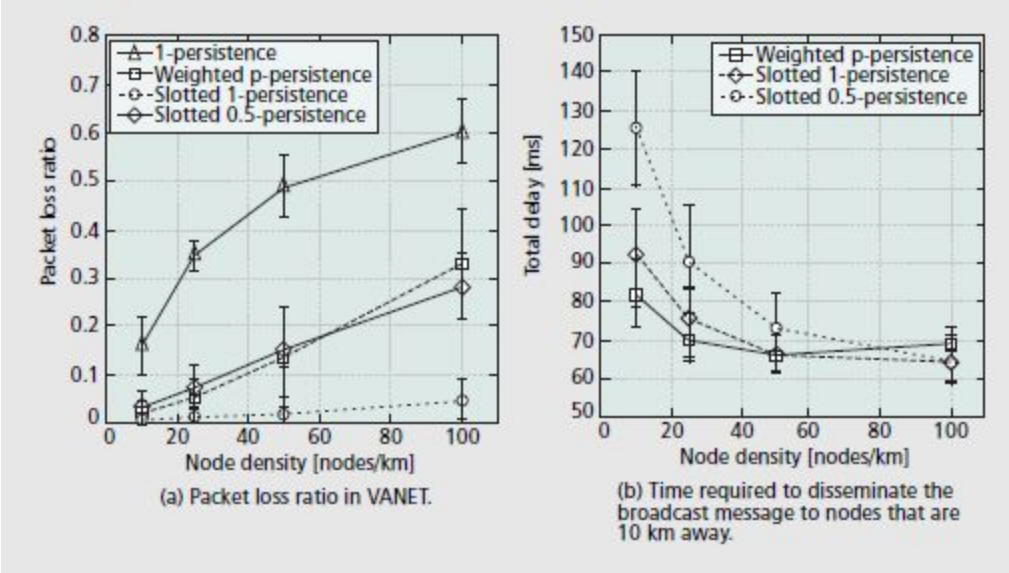


Figure 6: (a) Packet Loss Ratio ; (b) Total delay (ms)

Conclusion :

The proposed schemes are tested against single-lane and multilane topologies. The results show that the proposed slotted 1-persistence and slotted p-persistence schemes can reduce broadcast redundancy and packet loss ratio by up to 70 percent while still offering acceptable end-to-end delay for most multihop VANET applications(e.g., using a roadside unit to inform drivers about detours, construction)

SECTION 3: PROBLEM SOLUTION AND METHODOLOGY

PROBLEM ALGORITHM

To determine the density of traffic so as to determine

>> ***begin***
>> at each ***node (N_i)*** initialize ***state (S_i) = 0*** (i= 1,2,3…., k : k is the no. of nodes)
>> initialize ***avg1****=0;*
>>initialize ***avg2 =****0;*

#here state refers to the value of fields in i-table maintained at each node.

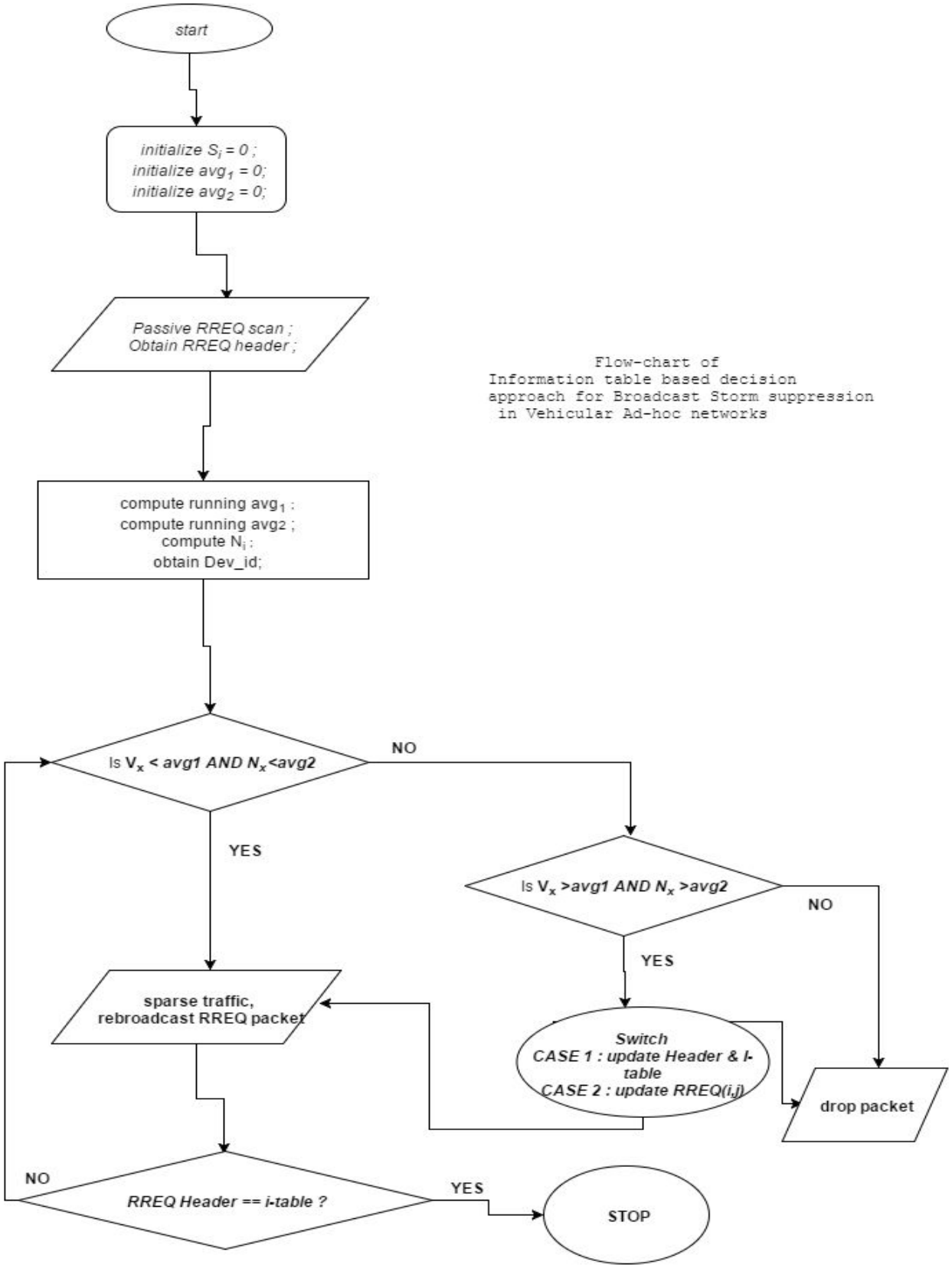
>>On hearing ***RREQ packet*** at node ***(N_i)***;

#on the basis of preliminary scan and Hello ***packet exchange***

>> Get the Number of neighbors $\mathbf{N_x}$;
>> Scan ***i-table*** and update S_i ;
>> Obtain ***Dev_id*** and update the ***i-table*** at N_i ;
>> compute running average ***avg1*** of V_x ***;***
>> compute running average ***avg2*** of N_x ***;***

Decision criteria for packet forwarding or dropping

>> **If** *packet RREQ* received for the first time then
If (V_x < *avg1 AND* N_x<*avg2*)
Node N_i has a sparse traffic, rebroadcast RREQ packet;
Else if (V_x >avg1 AND>avg2)
Node Ni has dense traffic,
Switch **header condition**
Compare S_i and RREQ ID header;
Case 1 : S_i & RREQ(j) header same ;
Drop RREQ packet;
Case 2 : S_i & RREQ(j) header not same ;
Update **S_i at N_i ;**
Update **RREQ(i,j);**
Rebroadcast **RREQ Header ;**
End
End
Else Drop **RREQ(i,j)** packet;
End



Flow-chart of
Information table based decision
approach for Broadcast Storm suppression
in Vehicular Ad-hoc networks

SECTION 4: SIMULATOR AND ALGORITHM IMPLEMENTATION

EXata is a network emulator to evaluate on-the-move communication networks faster and with more realism than any other emulator. With the optional Cyber Model Library, EXata can be used as a toolkit for research and development, test and evaluation, and training of cyber warfare technologies. It uses a software virtual network (SVN) to digitally represent the entire network, the various protocol layers, antennas, and devices. EXATA_HOME can interoperate, at one or more protocol layers, with real radios and devices to provide hardware-in-the-loop capabilities. EXata can also be connected to systems with real applications, which run on the SVN just as they would run on real networks.

EXata is a comprehensive suite of tools for emulating large wired and wireless networks. It uses simulation and emulation to predict the behavior and performance of networks to improve their design, operation, and management. EXata SVN provides a cost-effective and easy-to-use alternative to physical testbeds that typically have high equipment costs, complex setup requirements and limited scalability.

EXata Graphical User Interface (GUI)

EXata GUI consists of Architect, Analyzer, Packet Tracer, and File Editor.

• Architect is a network design and visualization tool. It has two modes: **Design mode** and **Visualize mode.**

In Design mode, one sets up terrain, network connections, subnets, mobility patterns of wireless users, and other functional parameters of network nodes. One can create network models by using intuitive, click and drag operations. One can also customize the protocol stack of any of the nodes. One can also specify the application layer traffic and services that run on the network.

In Visualize mode, one can perform in-depth visualization and analysis of a network scenario designed in Design mode. As simulations are running, users can watch packets at various layers flow through the network and view dynamic graphs of critical performance metrics. Real-time statistics are also an option, where one can view dynamic graphs while a network scenario simulation is running. One can also assign jobs to run in batch mode on a faster server and view the animated data later. One can perform “what-if” analysis by setting a range of values for a particular protocol parameter and comparing the network performance results for each of them.

• **Analyzer is a statistical graphing tool** that displays hundreds of metrics collected during simulation of a network scenario. One can choose to see pre-designed reports or customize

graphs with their own statistics. Multi-experiment reports are also available. All statistics are exportable to spreadsheets in CSV format.

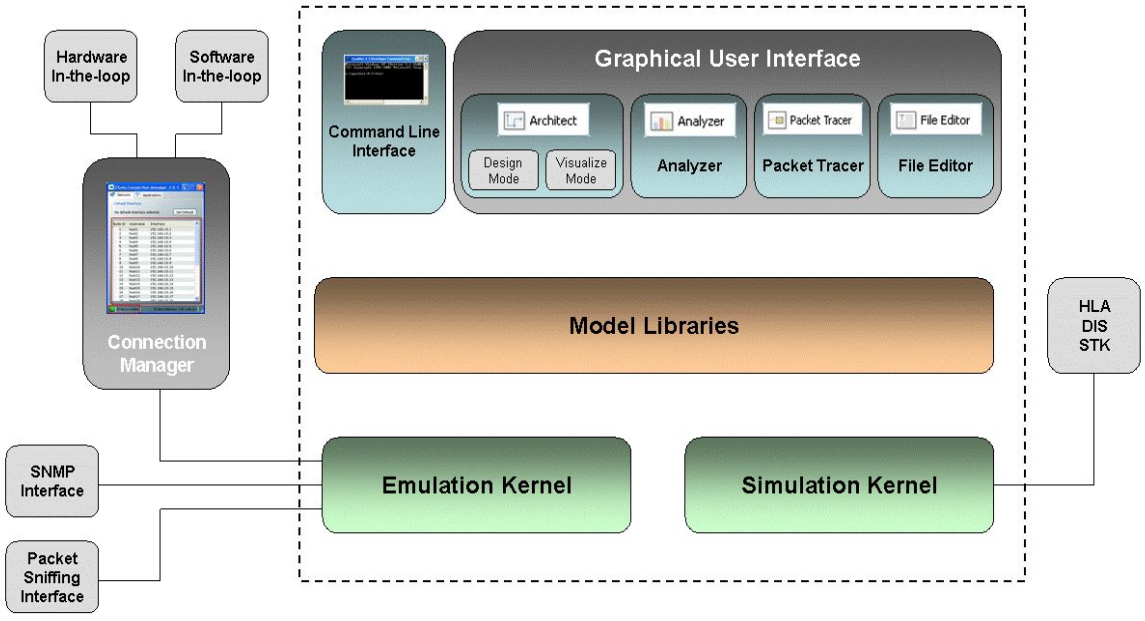
• **Packet Tracer provides a visual representation of packet trace files** generated during the simulation of a network scenario. Trace files are text files in XML format that contain information about packets as they move up and down the protocol stack.

• **File Editor is a text editing tool** that displays the contents of the selected file in text format and allows the user to edit files.

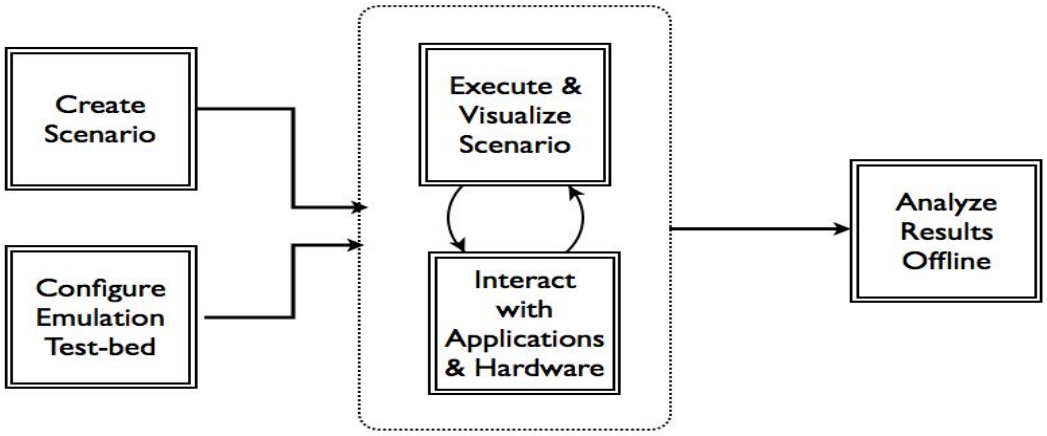
EXata Command Line Interface

The EXata command line interface enables a user to run EXata from a DOS prompt (in Windows) or from a command window (in Linux). When EXata is run from the command line, input to EXata is in the form of text files which can be created and modified using any text editor. Building and running scenarios with the command line interface takes less memory and scenarios typically run faster than with the GUI. With the command line interface the users have the flexibility to interface with visualization and analysis tools of their choice.

EXATA PLATFORM ARCHITECTURE



The Block diagram of emulation process using Exata Cyber is-



ADDING THE PROTOCOL 'MARS' IN EXATA –

The following list summarizes the actions taken to add our proposed network layer routing protocol – 'MARS' to EXata /Cyber :

1. **Creating of header and source files for the protocol MARS.**
2. **Modifying the file network_ip.cpp to include the protocol's header file.**
3. **Including the protocol in the list of Network Layer protocols and trace protocols.**
4. **Defining the data structures for the protocol.**
5. **Implementing the decided format for the protocol-specific configuration parameters.**
6. **Calling the protocol's initialization function from the routing initialization function, IpRoutingInit.**
7. **Writing the initialization function for the protocol.**
   a. Read and store the configuration parameters.

   b. Initialize the state variables and routing table.

   c. Register the protocol's callback functions with IP.

   d. Initialize timers.
8. **Calling the protocol event dispatcher from the IP event dispatcher, Network IP Layer.**
9. **Declaring new event types used by the protocol in the header file EXATA_HOME /include/api.h**
10. **Writing the protocol event dispatcher.**

11. **Modifying the IP function NetworkRoutingGetAdminDistance.**
12. **Implementing the protocol's routing packet handler.**
    a. Defining an IP Protocol Number for the protocol.
    b. Writing a function to handle routing packets.
    c. Calling the routing packet handler function from the IP function DeliverPacket.
13. **Writing the router function and any other call back functions used by the protocol.**
14. **Including code in various functions to collect statistics.**
    a. Declaring statistics variables.
    b. Initializing the statistics variables in the protocol's initialization function.
    c. Updating the statistics as appropriate.
    d. Writing a function to print the statistics.
    e. Adding dynamic statistics to the protocol, if desired.
15. **Calling the protocol finalization function from the IP finalization function, NetworkIpFinalize .**
16. **Writing the protocol finalization function. Call the function to print statistics from the protocol finalization function.**
17. **Including the protocol header and source files in the EXata/Cyber tree and compile.**
18. **To make the protocol available in the EXata/Cyber GUI, modifing the GUI settings files.**

THE SCENARIO

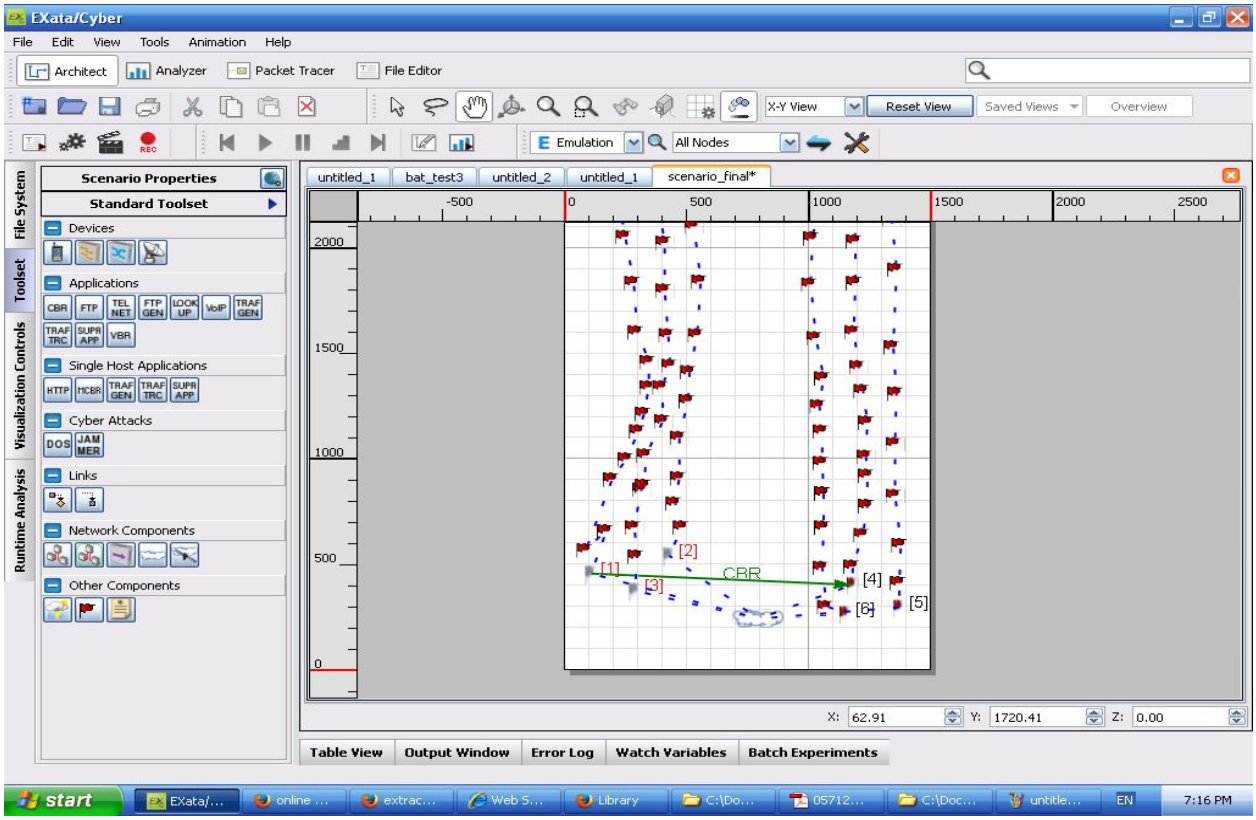
A 1500 x 6000 m^2 area is considered, where a regular traffic of vehicles is assumed. Six vehicles are scrutinised for their packet transmission and receptance, each being connected to a single cloud network. They have been divided into two group namely

- Group1 consisting of vehicles with Node Id 4,5 & 6.
- Group2 consisting of vehicles with Node Id 1,2 & 3.

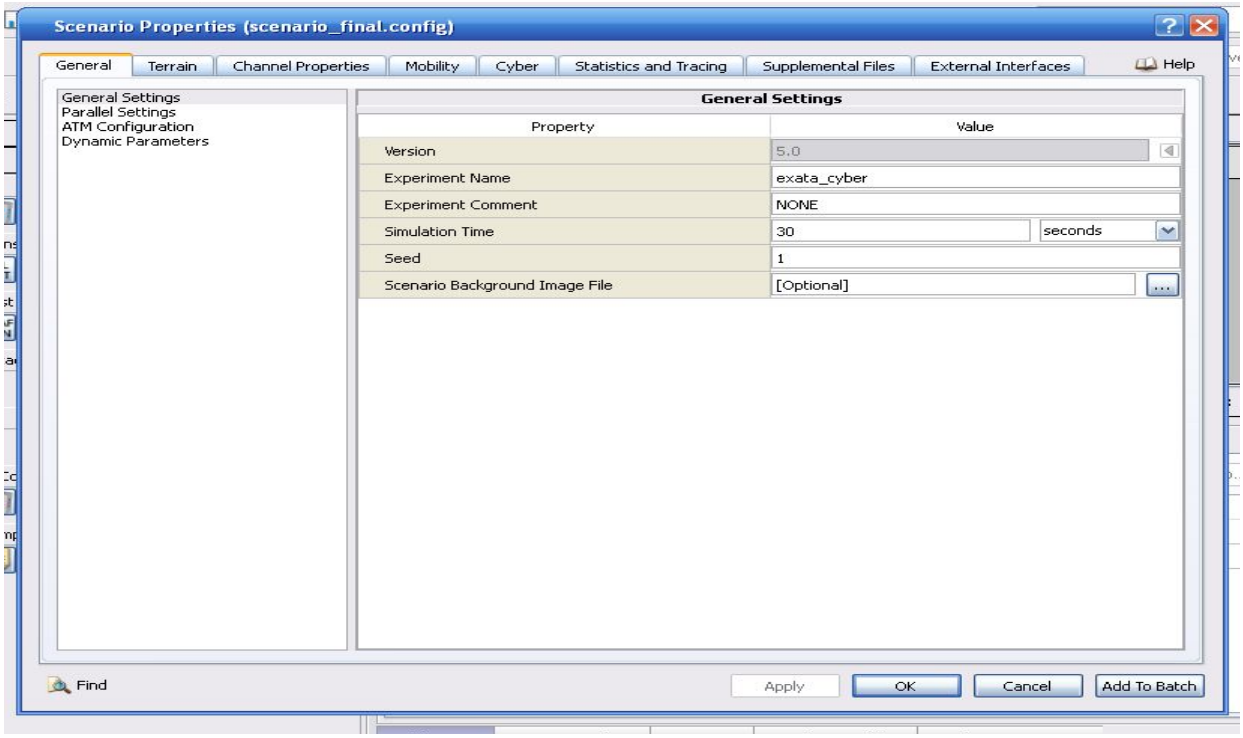
Each group is assigned a particular minimium and maximum speed, along with the random waypoint motion within the group. The movement constraints with respect to area, for both the groups, have been specified to imitate the near real- road scenario. With the aim of transferring data from vehicle with Node Id 1 to the vehicle with Node Id 4, the constant bit rate (CBR) is set between the two. Ten packets are sent by 1 and the no. of packets received by 4 is monitored.

The entire simulation is done for different simulation time (i.e. 10 seconds, 20 seconds & 30 seconds) for applying different routing protocol i.e. AODV, EIGRP and MARS. The different parameters like throughput, total bytes sent, no. of hop counts, no. of request packets forwarded,

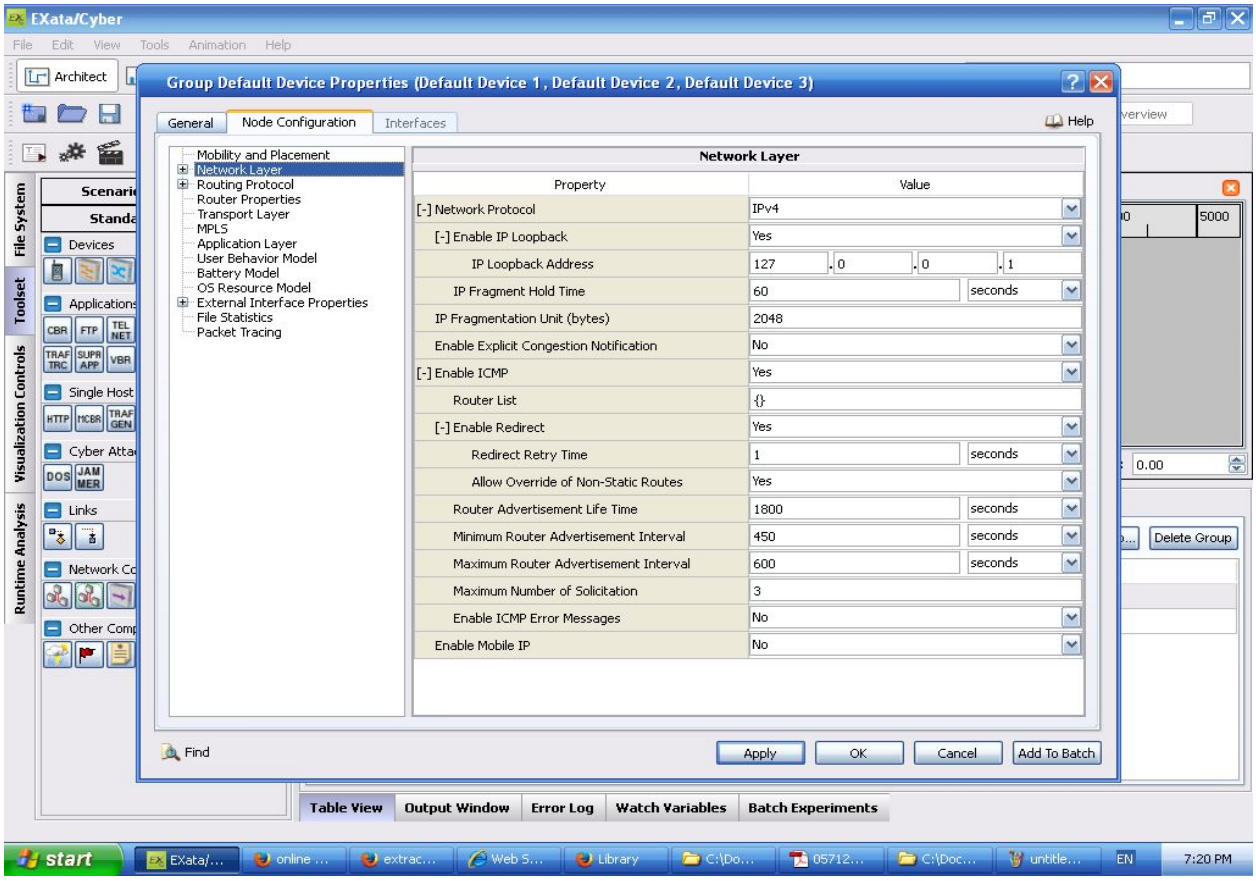
end-to-end delay, jitter in the packets, etc, are analyzed using the Analyzer tool available in Exata Cyber.



GENERAL SETTINGS OF THE SCENARIO

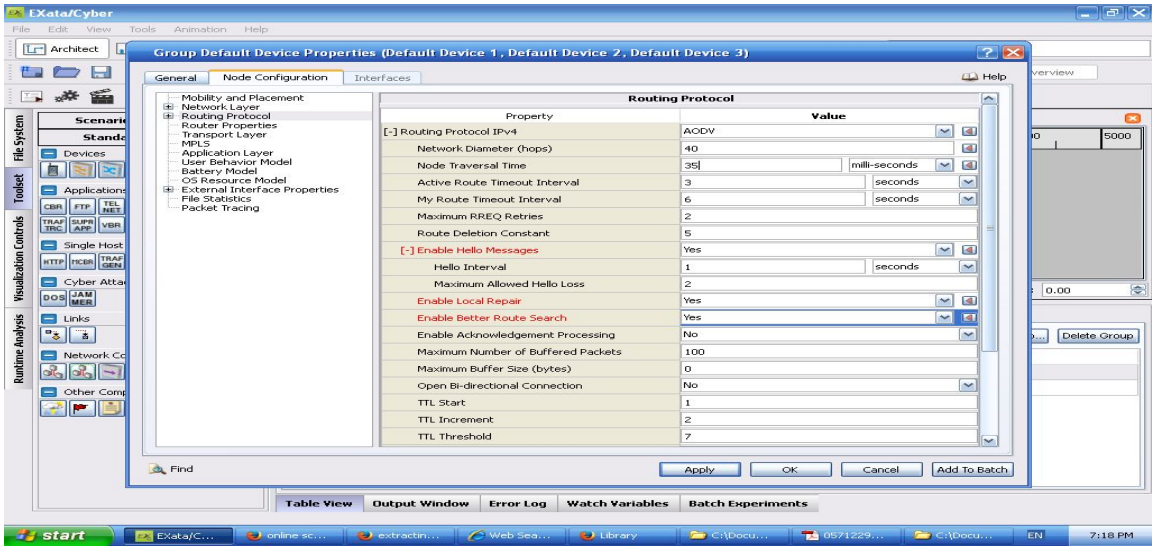


NETWORK LAYER SETTINGS

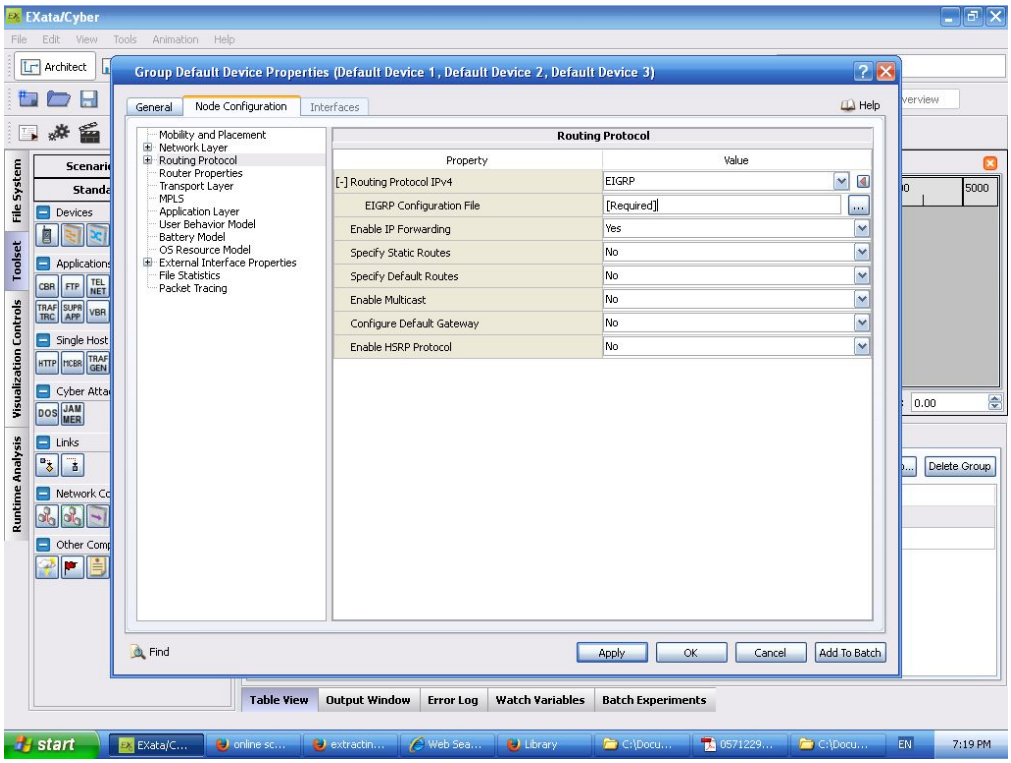


ROUTING PROTOCOL SETTINGS :

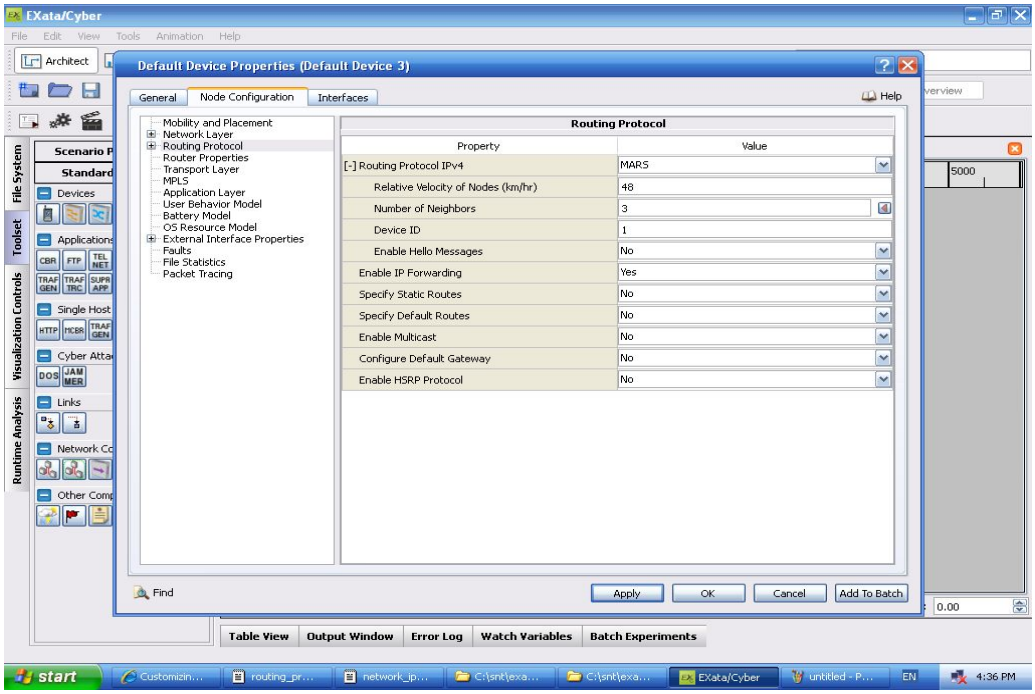
For AODV



For EIGRP

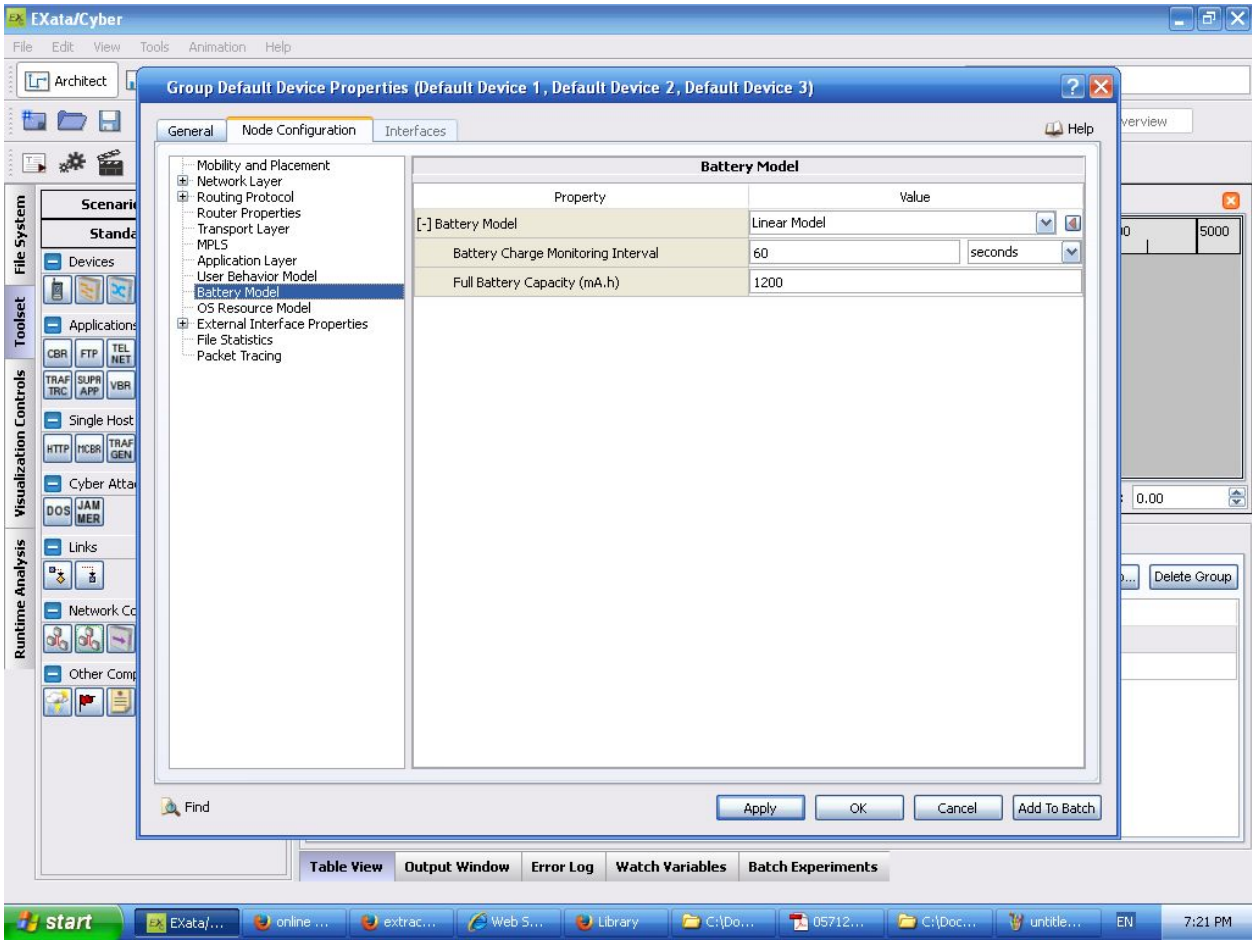


For MARS

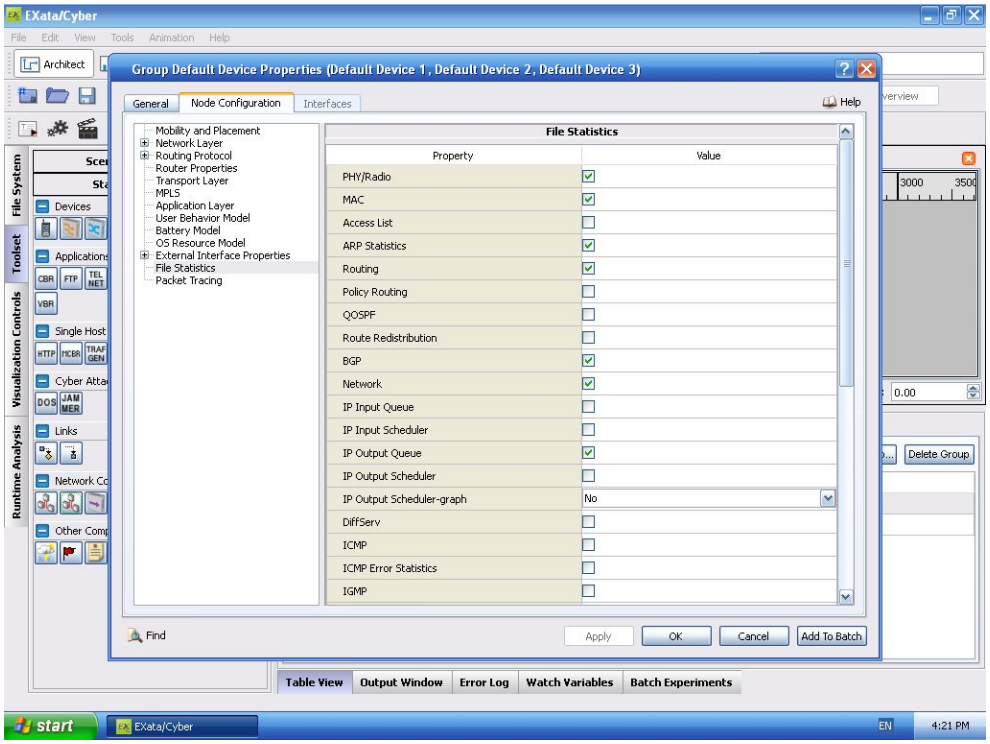


BATTERY MODEL USED

Among the battery models available, linear model for the battery has been used.

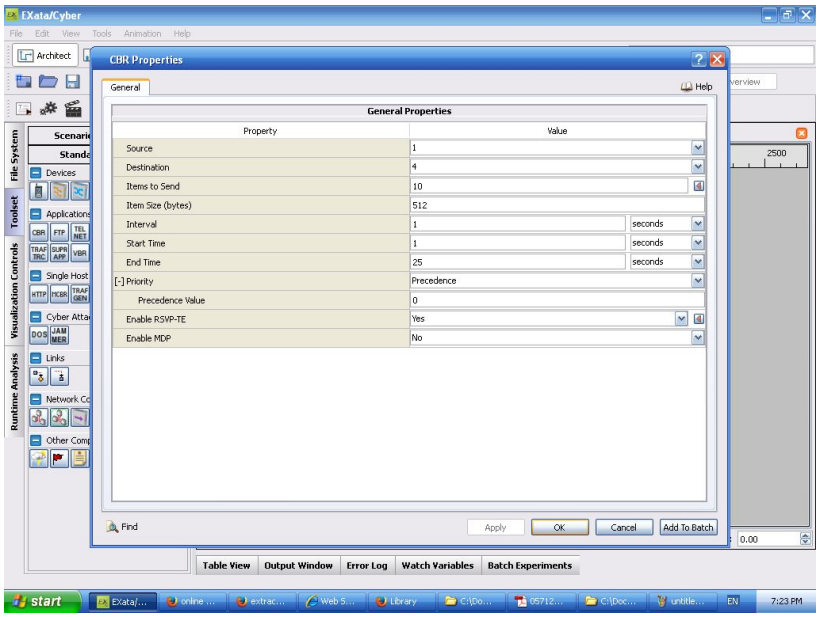

EXata/Cyber
File Edit View Tools Animation Help
Architect
Group Default Device Properties (Default Device 1, Default Device 2, Default Device 3)
General
Node Configuration
Interfaces
Help
Mobility and Placement
Network Layer
Routing Protocol
Router Properties
Transport Layer
MPLS
Application Layer
User Behavior Model
Battery Model
OS Resource Model
External Interface Properties
File Statistics
Packet Tracing
Battery Model
Property
Value
[-] Battery Model
Linear Model
Battery Charge Monitoring Interval
60
seconds
Full Battery Capacity (mA.h)
1200
Find
Apply
OK
Cancel
Add To Batch
Delete Group
Table View
Output Window
Error Log
Watch Variables
Batch Experiments
File System
Toolset
Visualization Controls
Runtime Analysis
Devices
Applications
Single Host
Cyber Attac
Links
Network Co
Other Comp
start
7:21 PM

PARAMETERS TAKEN TO ANALYZER FOR STATISTICAL COMPARISON



CBR SETTINGS

Here, the properties of CBR is set. Every time 512 bytes of data is sent.



PERFORMANCE METRICS

1. Throughput

2. End-to-end delay

3. Average no. of packets dropped

EXTRACTING PERFORMANCE METRICS

At the end of a simulation, EXata generates a statistics file containing information for analyzing the behavior of protocols, network performance, etc. The rules that determine the name of the statistics file depends on the scenario of the road and which has to be specified in advance. The statistics file is a plain text file that can be opened by using any text editor. It can also be viewed graphically using EXata Analyzer. Normally, the simulation runs for the configured simulation time. However, the simulation can be terminated before the configured simulation time (for example, by typing Ctrl+C). A statistics file is generated in either case. The first two lines of the statistics file indicate the configured simulation time and the simulation time when the simulation actually ended. If the simulation is allowed to run for the configured simulation time, then these two entries are identical. Lowest node ID in the scenario is typically 1. Maximum configured simulation time, in seconds, or the maximum simulation time is configured by setting the parameter SIMULATION-TIME in the scenario configuration (.config) file. Simulation time, in seconds, when the simulation ended. The statistics in the rest of the file are collected from the beginning of simulation to this time.

SECTION 5: RESULTS & DISCUSSION

COMPARISON WITH EXISTING PROTOCOLS

1. THROUGHPUT

$$Throughput = \frac{\sum No.\ of\ packets\ received\ at\ destination\ node}{\sum total\ time}$$

Figure 1.1 : AODV throughput

AODV						
S No.	% throughput (for 10 sec simulation)	No.of bytes sent (10 s)	% throughput (for 20 sec simulation)	No.of bytes sent	% throughput (for 30 sec simulation)	No.of bytes sent
1	40.96	4608	45.51	5120	48.56	6555
2	40.55	4562	46.2	5198	45.62	6158
3	41.02	4614	47.45	5338	50.14	6768
4	39.52	4446	49.89	5612	47.57	6421
5	41.5	4668	45.84	5157	46.5	6277
6	40.96	4608	47.89	5388	48.1	6493
7	40.29	4536	45.33	5098	44.78	6045
8	41.49	4667	41.9	4713	46.51	6278
9	39.95	4494	42.8	4815	45.48	6139
10	40.08	4501	43.66	4911	46.14	6228
Average values	40.632		45.647		46.94	

Figure 1.2 – Graph of AODV Throughput

(X-axis : No. of iterations, Y-axis: Percentage throughput)

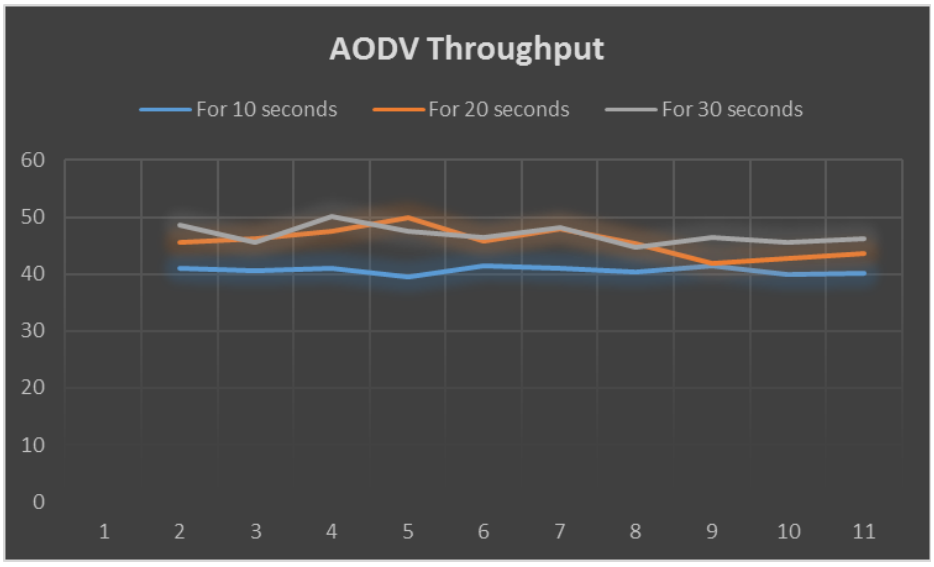


Figure 2.1 – EIGRP throughput

EIGRP						
SL No.	% Throughput(For 10 seconds)	No. of bytes sent (10 s)	% Throughput(For 20 seconds)	No.of bytes sent(20 s)	% Throughput(For 30 seconds)	No.of bytes sent (30 s)
1	35.46	3989	38.45	4325	40.89	5520
2	36.15	4066	34.89	3925	38.47	5793
3	34.47	3877	36.48	4104	40.14	5418
4	33.86	3809	35.72	4018	40.45	5460
5	34.4	3870	39.68	4465	43.57	5881
6	35.29	3974	41.67	4687	42.96	5799
7	32.84	3694	40.78	4587	43.79	5911
8	34.5	3881	39.75	4471	44.48	6007
9	36.58	4115	42.19	4746	45.72	6172
10	35.14	3953	42	4725	44.47	6001
Average value	34.869		39.161		42.494	

Figure 2.2 – Graph of EIGRP Throughput

(X-axis: No. of iterations, Y-axis : percentage throughput)

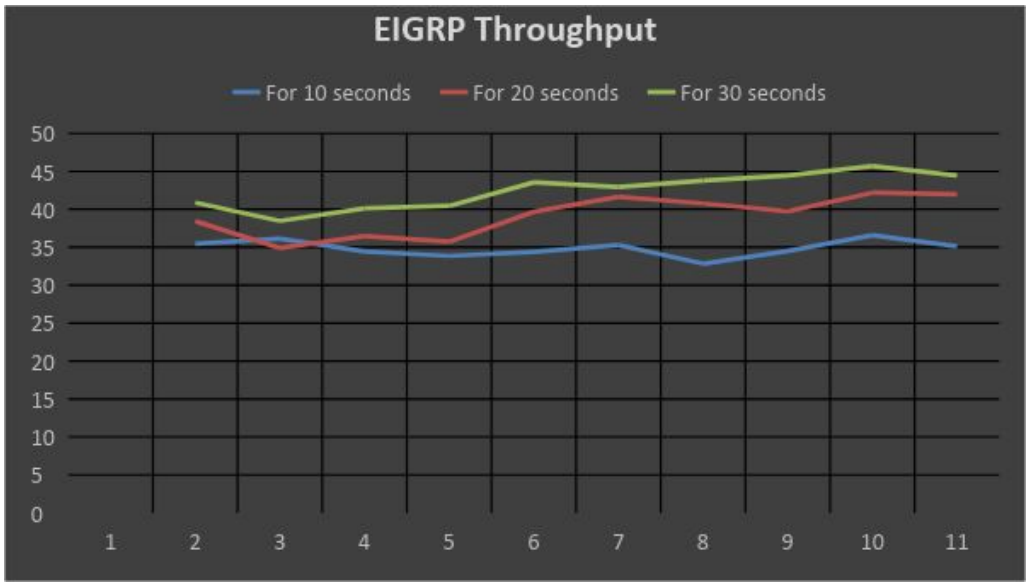


Figure 3.1 – MARS throughput

MARS						
SL No.	% Throughput (10 s)	No.of bytes sent (10 s)	% Throughput (20 s)	No.of bytes sent(20 s)	% Throughput (30 s)	No.of bytes sent (30 s)
1	38.58	4340	39.47	4441	44.14	5958
2	40.62	4569	37.64	4234	43.78	5910
3	37.15	4178	40.82	4592	46.64	6296
4	36.45	4100	43.48	4891	42.93	5796
5	34.6	3892	42.36	4765	45.19	6100
6	38.47	4327	44.79	5038	47.63	6430
7	35.15	3954	43	4837	46.28	6247
8	37.94	4268	45.69	5140	43.54	5877
9	34.66	3899	41.24	4639	47.42	6410
10	38.45	4325	40.15	4516	48.92	6604

Average Value	37.207	41.864	45.647

Figure 3.2 – Graph of MARS Throughput

(X-axis: No. of iterations, Y-axis : percentage throughput)

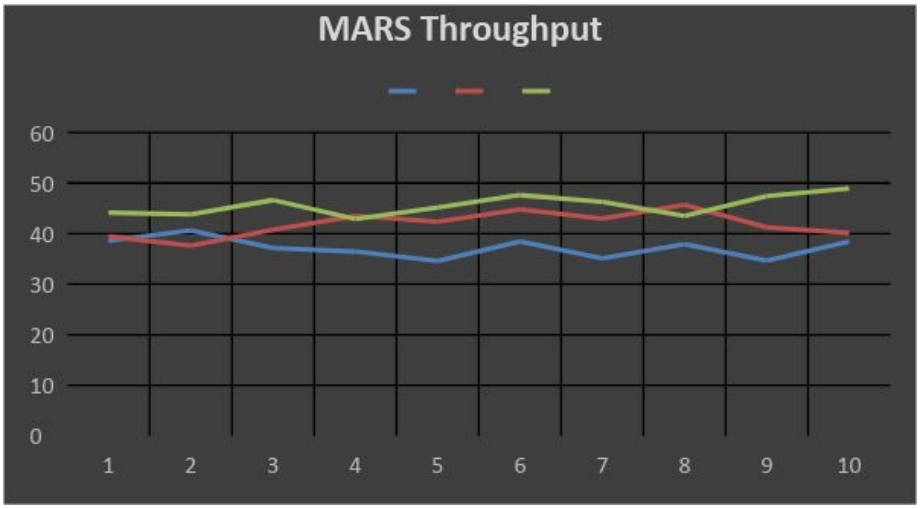
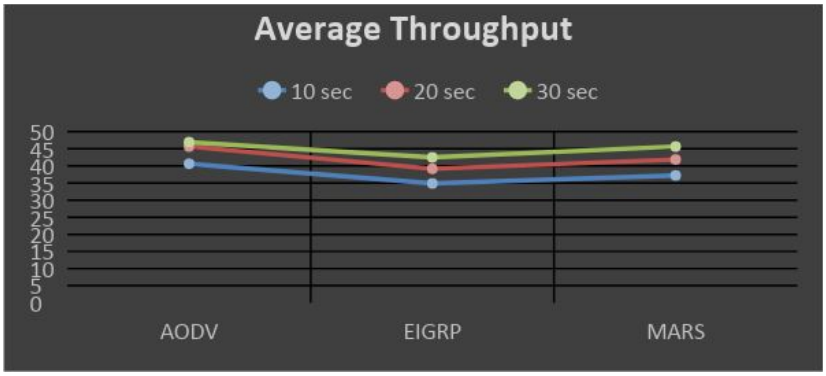


Figure 4.1 Average Throughput values for AODV, EIGRP and MARS

S. No.	Simulation Time (in sec)	AODV	EIGRP	MARS
1.	10 sec	40.632	34.869	37.207
2.	20 sec	45.647	39.161	41.864
3.	30 sec	46.94	42.494	45.647

Figure 4.2 – Comparison of AODV, EIGRP and MARS on the basis of throughput



2. END-TO-END DELAY

This metric is used to measure average transmission time of packets from a node to the node at which rebroadcasting is terminated because all nodes in a logical neighborhood have their i-table updated.

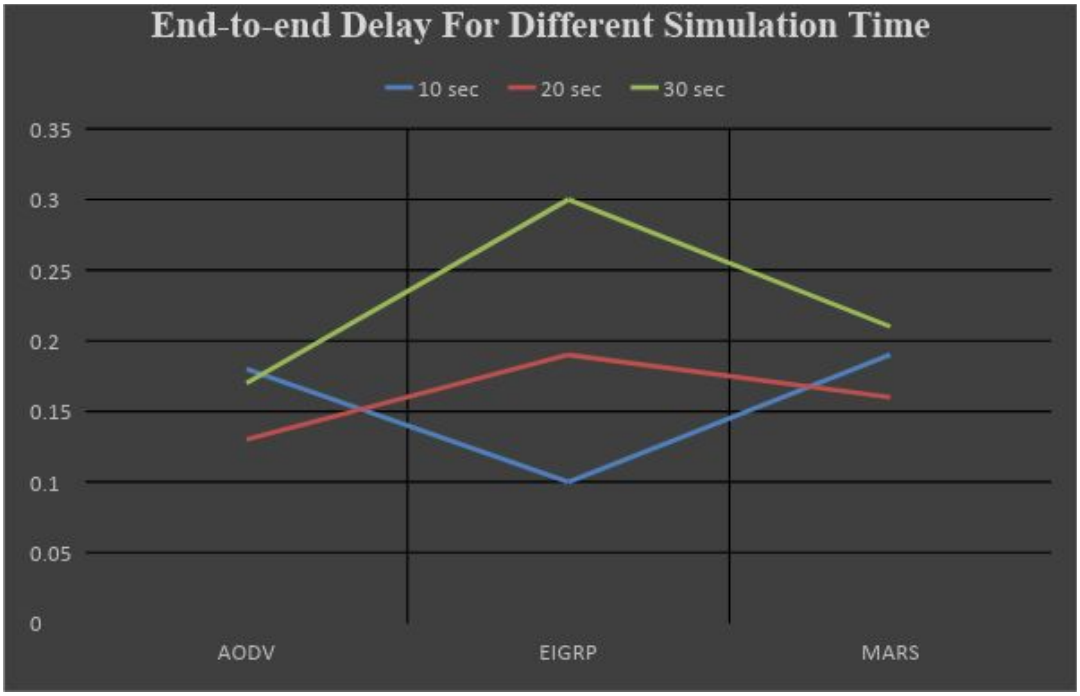
$$EED = \frac{\sum_{i=1}^{n} (t_{2i} - t_{1i})}{N}$$

$$EED = \frac{\sum_{i=1}^{n} (t_{2i} - t_{1i})}{N}$$

N = No. of packets received
t_{2i} = packet delivery time to rebroadcast termination node.
t_{1i} = first packet exchange time from initial node.

The values of t_{2i} & t_{1i} were obtained from the .stat file for each simulation run of the scenario. The results are plotted as below for various run time.

Figure 5.1 – Comparison of AODV, EIGRP and MARS on the basis of End-to-End Delay



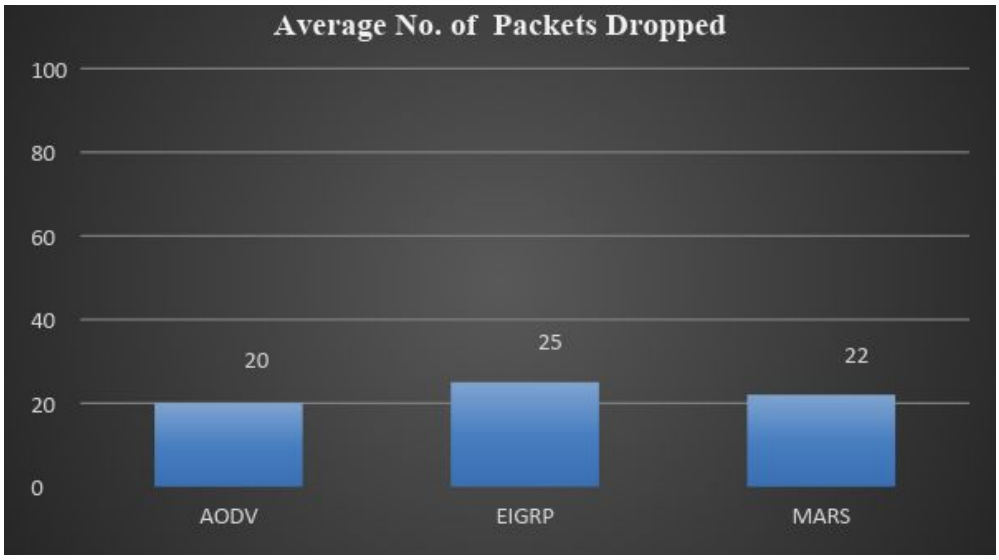
3. AVERAGE NO. OF PACKETS DROPPED

Number of Packets sent = 100

Figure 6.1 – Average number of packets dropped for AODV, EIGRP and MARS

	AODV	EIGRP	MARS
Average Number of packets dropped	20	25	22

Figure 6.2 – Comparison of AODV, EIGRP and MARS on the basis of average number of packets dropped.



SECTION 6: CONCLUSION

In this paper we have showed how to effectively mitigate Broadcast Storm Problem using the i-table approach. The proposed algorithm's performance was evaluated in the Exata Cyber versus distance based broadcast algorithms as implicated in industry standard protocols – EIGRP and AODV. Proposed algorithm uses i-table based selective packet forwarding criteria instead of blind broadcasting or distance based decision criteria and thus yields lesser contention, packet redundancy and end-to-end delay performance metric values.

SECTION 7: FUTURE SCOPE

The results obtained and used for comparison with standard routing methods in EIGRP and AODV have been done with simulation times of 10s, 20s and 30s of simulation run times. For more accurate results the scenario performance needs to be evaluated for larger run-times of 1 minute to 3 minutes. Also, obtaining data sets for larger values of performance and introduction of new performance metrics such as data bit rate will give a more realistic and accurate performance comparison basis against our proposed routing algorithm based on i-table approach. Also, during deciding a data structure for i-tables an analogy has been taken from routing tables which are based on hash tables and i-tree. Hash tables, bit by bit checking methodologies have their own limitations, which is why despite routing tables are implemented in industry standard protocols, a drawback on security always exists. Therefore, future work may require a re-visiting approach and looking it from data security perspective.

SECTION 8: REFERENCES

1.DYMO as routing protocol for IEEE-802.15.4 enabled Wireless Sensor Networks - By Dr. Ajay Singh Raghuvanshi and Dr. Sudarshan Tiwari.

2.Simulation and Performance Analysis of Routing Protocols in Wireless Sensor Network using QualNet – By Anjali Goyal , Dharmendra Kumar Jhariya , Sandeep Vijay.

3.EXata 5.2 User's Guide- By Scalable Networks.

4."Mitigating Broadcast Storm Problems in Vanets"- Khaleel Ur Rahman Khan and Mohd Umar Farooq-DOI 10.5013/IJSSST.a.15.05.04

5."Broadcast Storm Mitigation techniques in vehicular Ad-Hoc Networks"- N.Wisitpongphan and O.K.Tonguz ,J.S.Parikh ,P.Mudalige,F.Bai and V.Sadekar –ieee Wireless Communications , December 2007.

6."The Broadcast Storm Problem in a Mobile Ad Hoc Network "- Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu-Wireless Networks 8 , 153-167,2002.

7. "A Technique to Mitigate the Broadcast Storm Problem in VANETs" : Manoel Rui P. Paula, Daniel Sucupira Lima, Filipe Maciel Roberto, Andre Ribeiro Cardoso, Joaquim Celestino Jr.

8."An Efficient Counter-Based Broadcast Scheme for Mobile Ad Hoc Networks " : Aminu Mohammed, Mohamed Ould-Khaoua, and Lewis Mackenzie

9."Simulation and Performance Analysis of Routing Protocols in Wireless Sensor Network using QualNet" – By Anjali Goyal , Dharmendra Kumar Jhariya , Sandeep Vijay.

10."New Adaptive Counter Based Broadcast Using Neighborhood Information in MANETS"- A. Al-Dubai, M. Bani Yassein, M. Ould Khaoua, Omar M. Al-Jarrah-2009 ieee.

11."An Effective Way of Broadcasting Alert Messages in Vehicular Ad hoc Network"- Mohd Umar Farooq ,Junaid Ahmed Shadab,Khaleel Ur Rahman Khan-Proceedings of the International Conference on Communication and Computational Intelligence – 2010 ,Kongu Engineering College, Perundurai, Erode, T.N.,India.27 – 29 December,2010.pp.132-137

12."Inspired Counter Based Broadcasting for Dynamic Source Routing in Mobile Networks"- Muneer Bani Yassein ,Ahmed Y. Al-Dubai-2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications;Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.

13."ProbT: A Temporal Probabilistic Protocol to Mitigate the Broadcast Storm Problem in VANETs"- Daniel Sucupira Lima, Manoel Rui P. Paula, Filipe Maciel Roberto,Andr´ e Ribeiro Cardoso and Joaquim Celestino J´unior- IEEE 2015

14."Intelligent Broadcast in Wireless Ad Hoc Networks Using Live Packet Information"- Chun- Hsin Wu and Chi a-Wei Li- IEEE 2013.

15.J. Jakubiak and Y. Koucheryavy, "State of the art and research challenges for VANETs", Consumer Communications and Net-working Conference, 2008. CCNC 2008, pp. 912-916, Jan. 2008.

16. Fan Li and Yu Wang, “Routing in Vehicular Ad Hoc Networks: A Survey”, IEEE Vehicular Technology Magazine, vol. 10, no. 3, pp. 12-22, JUNE 2007.

17. P. Kyasanur, R. R. Choudhury, and I. Gupta. Smart gossip: “An adaptive gos- sip-based broadcasting service for sensor networks”, in Mobile Ad-hoc and Sensor Systems (MASS), 2006 IEEE International Conference , pp. 91-100, Oct. 2006.

18.Wireless Communications, IEEE, vol. 14, no. 6, pp. 84-94, December 2007.

19. K. Suriyapaiboonwattana and C. Pomavalai. “An effective safety alert broad-cast algorithm for VANET”, International Symposium on Communications and Information Technologies. ISCIT'08, pp. 247-250, Oct. 2008.

20. F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni. “City-mob: a mobility model pattern generator for VANETs”, IEEE Vehicular Networks and Applications Workshop (Vehical-Mobi, held with ICC), Beijing, China, May 2008.