RESEARCH ARTICLE OPEN ACCESS

Intelligent Traffic System Using BAHG Protocol with Secured Intrusion Detection System

Rakesh Krishna SR
Dept. of Electronics and Communication
Francis Xavier engineering college
Tirunelveli
rakeshkrishnasr@gmail.com

Dr.M. Irulappan Ph.D
Dept. of Electronics and Communication
Francis Xavier engineering college
Tirunelveli
mirulappan@yahoo.com

Abstract—
A vehicular ad-hoc network (VANET) is a technology that is used to create a mobile network using moving cars. Here VANET will take the participating car, to form a router or node. VANET allows car to connect each other with an approximate range of 100 to 300 meters. Interconnecting the cars with each other will create a wide range network. Whenever a car falls out of the signal range or drop out of network, other cars can join to the network, so that the network is maintained. High movement of vehicles causes frequent disconnection of nodes which will lead to information loss. To reduce this problem a Greedy Perimeter Stateless routing (GPSR) is proposed. This routing scheme will use the shortest path with minimum number of intermediate intersection. The main aim is to reduce the connectivity time and disconnection between the nodes. A Back Bone Assisted Hop Greedy (BAHG) routing scheme is also proposed. Back bone is a set up that is used at the intersections. Hop greedy will ensure that the selected intersection has enough connectivity. This will lead to fast and reliable delivery of information between nodes in all scenarios. An Intrusion Detection System is also included to improve the security in VANET system.
Index Terms— Back Bone Assisted Hop Greedy (BAHG), Greedy Perimeter Stateless Routing (GPSR), Vehicular Ad-Hoc Network (VANET).

I. INTRODUCTION

VANET is one of the most popular types of networking used nowadays. It mainly concentrates on the growing number of wireless products that are used in vehicles. VANET mainly demand on Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) or Vehicle-to-Infrastructure (V2I) communication. This type of communication system is significantly used in both safety and non safety applications. Intelligent transport system makes use of wide range of support from V2V, V2R OR V2I communication. The main factors for the adaptation of VANET architecture is its low latency requirement in safety application and the interactive multimedia capability.

Ad-hoc network mainly lags a pre-existing infrastructure. Here we take moving vehicles as "nodes". Here each node will act as a router. The information is either forwarded or discarded by the router. Dynamic forwarding will be based on the network connectivity. Here the forwarding is mainly done by flooding. The nodes will be inter-connected with the "links". Linking of the nodes will be based on node resources, behavior property and link property. Node resources are analyzed based on the computing power, memory, transmitter power etc. Behavior property is the reliability of the node connectivity. Link properties include length of the link, interference and the noise in the system. In VANET each link is called as "paths". After links are established suitable path is selected as shown in the Fig.1.

VANET is used in Intelligent Traffic System (ITS) like emergency vehicle notification systems, automatic road enforcement etc. Vehicular networks share common characteristics with conventional ad-hoc networks, such as self organized and lack of central control. Potential high numbers of nodes, high mobility and frequent topology changes, high application requirement on data delivery, no confidentiality of safety information, privacy are the other keen characteristics of VANET.

Wireless Sensor Network mainly communicates through multi-hop network architecture. Communication will in bi-directional, also enables sensor activity control.

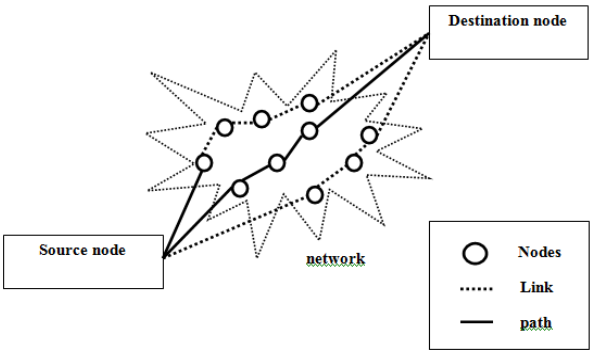

Fig.1. Wireless Network Multihop Architecture

Various forms of wireless communication technologies are Radio modem Communication on UHF, Short Range Communication and Longer Range Communication. Radio modem communication consists of ultra high frequency (300 MHz-3 GHz) and very high frequency (30 MHz - 300 MHz). Short Range communication technologies are best used in VANET's with a range of less than 500 meters. Longer range communications are best used in WiMAX with a range of around 30 miles.

This paper mainly uses a reply request method for source destination (src-dst) communication. Whenever the destination receives the request message, a suitable path is selected and the information is sent to the destination. Destination will calculate the shortest path with hop count and distance. Shortest path with minimum hop count is selected. We use a GPSR scheme for the shortest path selection. Usually road consists of intersection. In the intersection we go for BAHG setup to minimize intersection node problem.

II. RELATED WORK AND MOTIVATIONS

VANET routing protocols mainly came from Mobile Ad-Hoc Networks (MANET). MANET routing protocols are altered or enhanced to work in VANET environment. The protocols mainly used in VANET are Greedy Perimeter Coordinate Routing (GPCR)[4], Anchor Based Street and Traffic Aware Routing (ASTAR)[4] Geographic Source Routing (GSR)[4], Connectivity Aware Routing (CAR)[3], Greedy Traffic Aware Routing (GyTAR) etc.

GPCR uses a coordinate routing scheme. Here packets are forwarded by applying a restricted greedy method. The packets are forwarded by forwarding node. Forwarding node consists of junction and non junction node. Mainly junction nodes are used. ASTAR is mainly used in the city bus information. It is used to identify the anchor path. Here data will be sent through the path having more connectivity when compare to another paths. GSR uses street map and location information of node in a network. Here the intersection information is placed in a packet header to minimize the intersection node problem. Dijkstra's algorithm is used to find the shortest path. Computation time taken by Dijkstra's algorithm is high, which causes distance and connectivity based problems. CAR uses a reply request method. Source sends a source broadcast request message to find out the destination location. Destination will reply to source about the routing path with the connectivity and hop count information. Data packet will be sent from (src-dst) through the suggested path from the destination. GyTAR is an intersection based geographical routing protocol. Here sequence of intersections between source and destination is taken into account. A greedy forwarding node will adopt either greedy forwarding or a carry and forward mechanism.

Movement Prediction Based Routing (MOPR)[6] is routing concept for the position based routing used in VANET's. It used the most stable route in terms of the movement of vehicles. Mobility pattern aware routing for Heterogeneous Vehicular Networks (HVN) utilized a novel information and communication technology for the transport infrastructure of the vehicles. Here the HVN integrated the application of Wireless Metropolitan Network.

The routing protocols GPCR, ASTAR, GSR, CAR, GyTAR, and MOPR may face some problems at rural as well as urban environments. So a discussion can be done about the problems that we may face in the above mentioned routing protocols.

Problems are mainly faced at the intersections. Change of direction of vehicles and small intersection region will lead to intersection node problem as shown in Fig 2. Node is said to be unstable if the node crosses the intersection before receiving the data packet. This issue occurs when the vehicle get speeded up after receiving the beacon message. If there is no node ath the cross intersection error will arise.

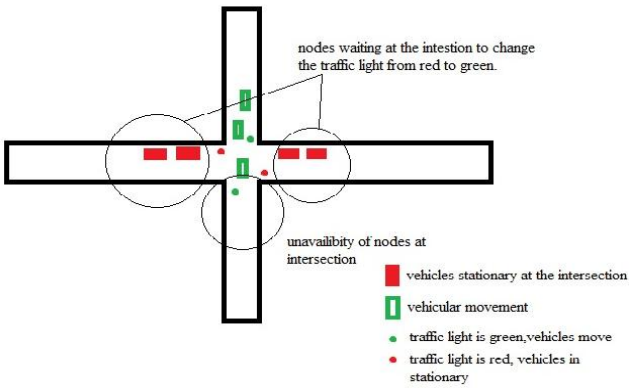

Fig.2. Intersction Node Problem Due To Unavailability Of Nodes.

If the SRC-DST is moving, it is difficult to find the actual position which will lead to requirement of service location problem. Information has to travel a number of hops in city area to reach the destination. We mainly use routing protocol to reduce the end to end delay. Increasing hop count will increase the end to end delay. The GPSR protocol uses Hierarchial Location Service (HLS) and the Grid Location Service (GLS). In these type of location service, lower beacon intervals is the factor of high efficiency. Sensors are used at the intersections to increase the accuracy of the actual position information of the information. Any change in destination position will change the path direction which will lead to increased hop count.

III. ROUTING PROTOCOLS USED IN THE VEHICULAR AD HOC NETWORK

In this section we combine the advantages of the GPSR scheme with the BAHG protocol. These are the position based routing protocols. Here minimum numbers of intermediate intersections are taken into consideration. A reply request method is used to find out the destination position. Since there is no addressing scheme for the sensors and are spatially deployed in the location region, information can be initialized for the data routing. So we go for the location based routing scheme called GPSR. We used a hop greedy routing scheme to reduce end to end delay and introduced a back bone node that plays a key role in providing connectivity status around an intersection.

A. Assumptions

Here the receiver section will be constantly moving in a system. So the movement of the vehicle is an important factor. The change of direction of the receiver vehicle is updated by Global Positioning System (GPS). GPS errors are minimized by precise monitoring, carrier phase tracing and augmentation. Here we make use of a digital map and navigation system.

B. System Design

1) Zone Formation In The City Map:

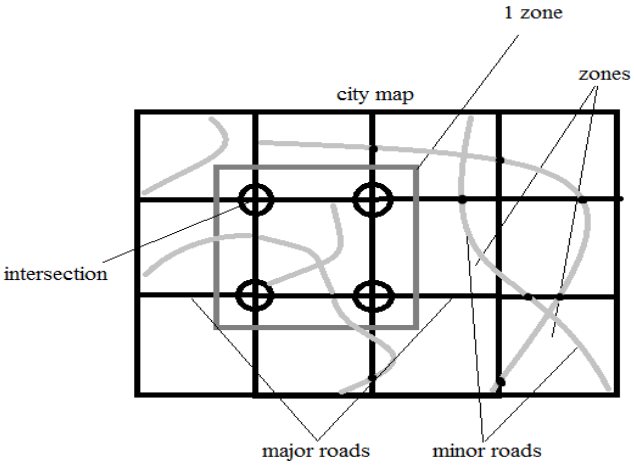

Fig.4.Zone Formation

The Fig.4 shows the zone formation in a city map. Here the city map is divided into several zones. Intersections are located at the outline of the zone. Roads are divided into Major and Minor roads. Intersection points are made at the intersection of two Major roads. At the major roads it is highly possible that a node will be present at the intersection. Intersection at the corner, zone border is called boundary intersection. Boundary intersections as shown in Fig.4 are the entry point of the packets. A unique ID is given to the packet as well as the packet is entered in the zone.

2) Connectivity Preservation

Key parameter in a rouitng protocol is connectivity. When a packet reaches an intersection, chance of changing the direction of the packet is highly possible. Wrong intermediate intersection will result in packet loss. So a Back Bone node setup is made to minimize the packet loss at the intersection during the intersection change over.

3) Back bone setup at the intersection

Back bone node provides a connectivity around an intersection as shown in Fig.6. Back bone will declare itself its presence as well as it reaches the intersection region. Here ordinary beacon messaging is not reliable, so we use a positional beaconing message. A back bone node consists of a stable, primary and a secondary back bones.

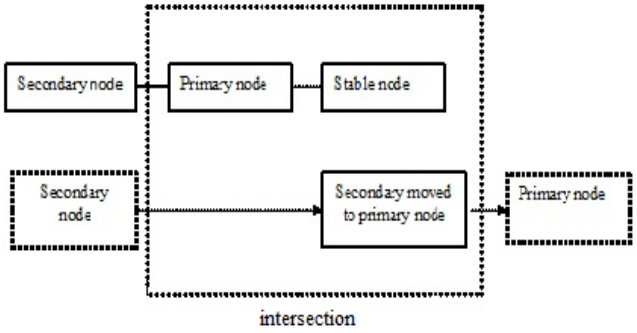

Fig.6. Back Bone Setup

A stable back bone is selected from the vehicles waiting at the intersection waiting at the intersection during the red traffic signal. During this process the vehicle which is closest to the intersection declares itself as the stable Back
Bone. Primary and the secondary nodes are selected from a Group of vehicles that is crossing the intersection when the traffic light is turned green. Primary node will be located at the intersection and the secondary back bone will be located outside the intersection. Primary will compare with the secondary to get the average speed of the vehicle and the position. When the primary node moves from the intersection the secondary will be the new primary and the process is continued.

4) Destination discovery and packet forwarding

Destination discovery is done by a simple hop greedy procedure. A reply request message is used to find the destination discovery. The reply message will be having the reply path by hop greedy algorithm. The reply message will be having the list of intersections to reach the destination. If the source is moving an update procedure is done to update the intersection list.

C. GPSR Routing Protocol

The wireless routing protocol GPSR proposes an aggressive use of geography to achieve the scalability factor. The scalability aim is under increasing numbers of nodes in the network, and increasing the mobility rate. Networks that push on mobility and number of nodes or both include the following factors:

- Ad-hoc networks:

It is the most investigated category, the mobile networks have no fixed infrastructure and support applications for military users and post disaster rescuers.

- Sensor networks:

It is comprised of small sensors; the mobile networks can be used with very high numbers of nodes, and has very low per-node resources. Minimization of node is another major factor.

- "Rooftop" networks:

Rooftop networks are mobile network that are placed on rooftop of building. They are not mobile in nature , which are wirelessly fixed in densely in metropolitan areas. The rooftop networks replaced the older telecommunication wired networks.

GPSR consits of greedy forwarding and perimeter forwarding. Here we go for greedy forwarding. The GPSR packets are marked with the unique used ID. They are marked by their originator with their destination location. Here we used a greedy choice in association with the GPSR to choose the packet next hop as shown in Fig.7. Here in the greedy forwarding of GPSR, if a node knows its radio position, the optimal choice of the next hop in the neighobour closest to the geographical packet destination. Forwarding is done until geographic hop closer to the destination is reached. A beaconing message periodically provides neighbour position to all nodes. Nodes will also transmit a beacon message to transmita its MAC adress to give its own identification and position. The postion is encoded by two,four byte floationg points. It will be provided in *x, y* coordinates. The main advantage of greedy forwarding is the knowledge of forwarding nodes next neighbor. The system is dependent on the density of nodes, not the number of destinations.

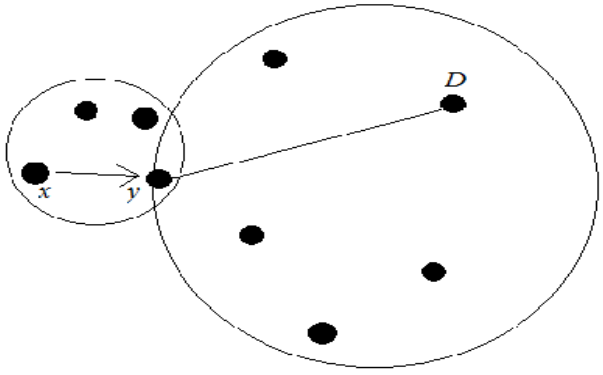

Fig.7.Greedy forwarding example. *y node is x' s* closest neighbor to Destination D.

Beacon message will be sent at an interval B. A mean interval beacon transmission will be uniformly distributed by intervals 0.5B, 1.5B, 2.5B etc. A time T will be given for the receiving the beacon message

from the neighbor. Not receiving a beacon from the neighbor will create a timeout message GPSR routing will be consider that the neighbor node has failed or gone out of coverage and deletes that node from its routing table.

D. Intrusion detection system for VANET

Used to detect false communications between V2V or V2I. Intrusion can be avoided, if history of node communication is analyzed, if previously passed vehicles have also got this false information. Digital Signature based system is used. System will be having a database behavior of certain attacks; it will be compared with the collected data. An attack is detected if the data coincide with the malicious behavior already registered. A DS gives recipient, that the message was created by a known center. By using cryptography type approach message is not altered during transmission. Can be used in association with firewall. Can detect both inside and outside attack.

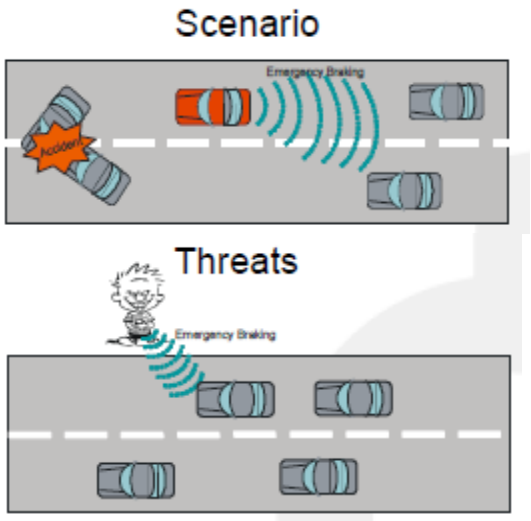

Fig.8 Threat and Scenario in Vanet

IV. PERFORMANCE EVALUATION

In this section we evaluate the performance of BAHG and GPSR protocol using the NS2 simulator. NS2 is an open source simulation tool. It supports the simulation of routing, IP, multicast routing protocols. Language used in NS2 is basically C ++ with OTcl (Object Tool Command Language)

A. Simulation Result

Here simulations are analyzed. Here in Fig.9. nodes are initialized. Here we have control station, source as well as destination base station. In the Fig.10 the mobile station node will send a request message to the base station regarding the destination node. The mobile node will also try to interconnect with the other mobile nodes to find the shortest path to the destination. And the shortest path is replied by Beacon messaging by adjacent nodes to the mobile node by GPSR scheme. Mobile node will also communicate with the base station. In the Fig.11 Mobile node a security attack is formed at the Source Base station. The fig 12. Shows the attack is continued in the destination base station, and the attack is denied successfully by IDS.

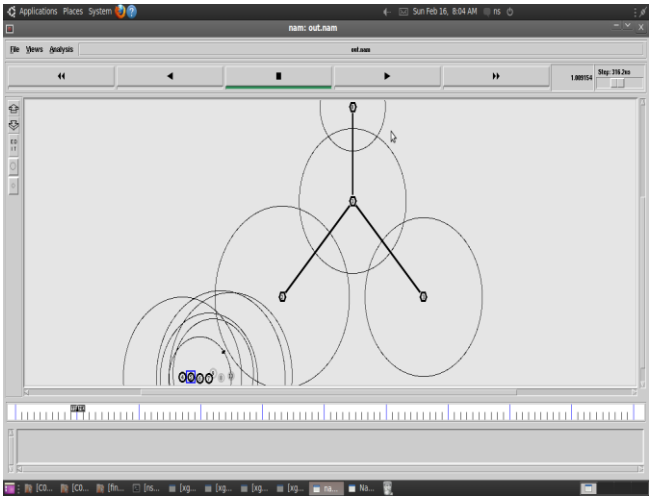

Fig.9. Node Formation and communication

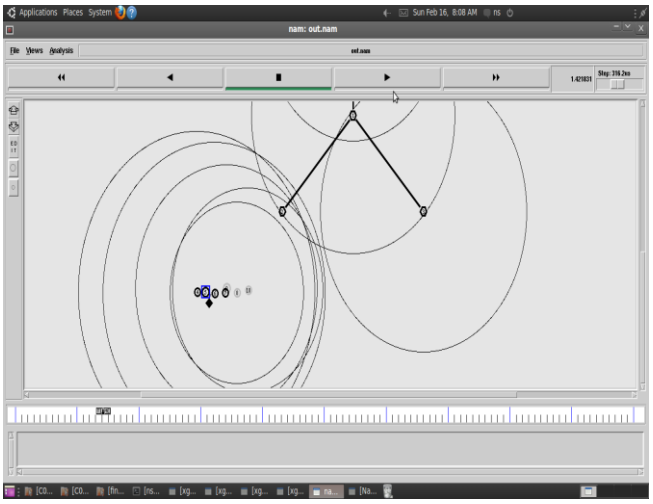

Fig.10. Reply Request Process

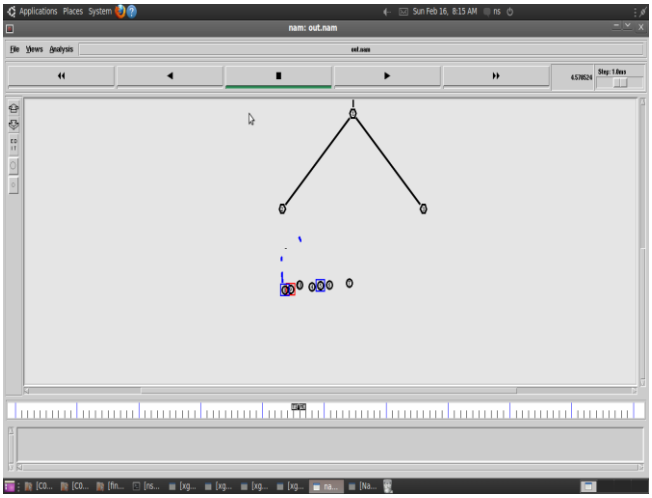

Fig.11.Intrusion Attack

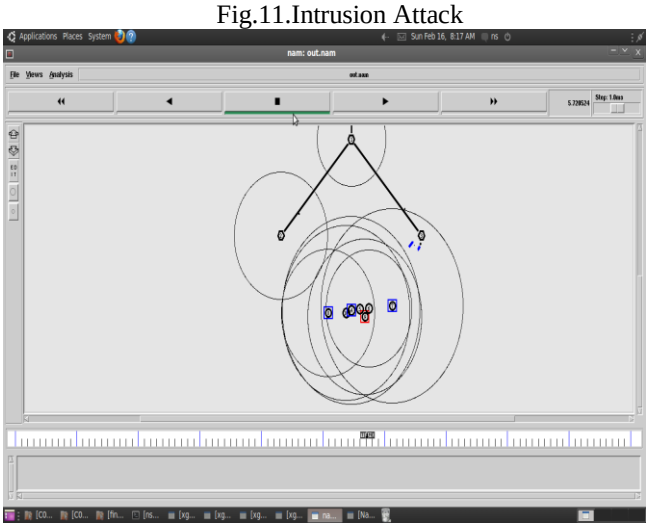

Fig.12.Intrusion Attack Detection And Rejection.

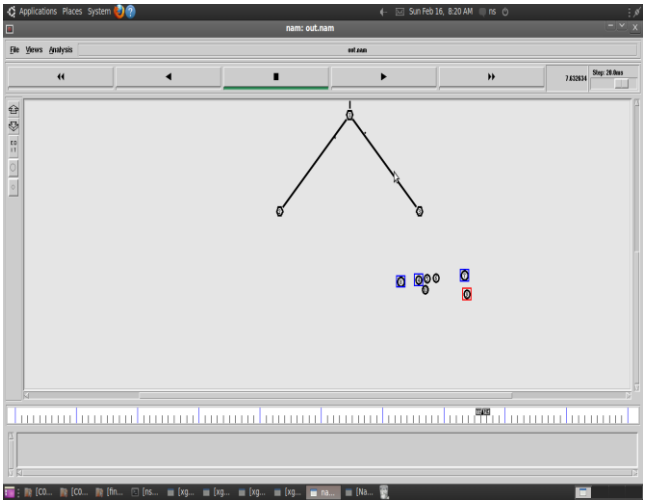

Fig.13. Node Reaching The Destination Securely

In the Fig.13, after communicating with the destination base station and adjacent mobile nodes, mobile node finally reached the destination successfully.

B. Analysis result

In this section we analyze the Overhead analysis, Packet delivery ratio, threshold calculation.

In the Fig.14.Overhead analysis we compared the normal and Priority based data communication. Here the delay is much reduced in the priority based communication when compared to that of normal communication. In the Fig.15 packet delivery is analyzed. In the priority based communication the packet delivery ratio is much high when compared to that of normal communication. The Fig.16 analyzed the threshold calculation. Here we calculate how much data is sent at a particular interval. The data rate will be high at the initial stage and will drop at the final stages.

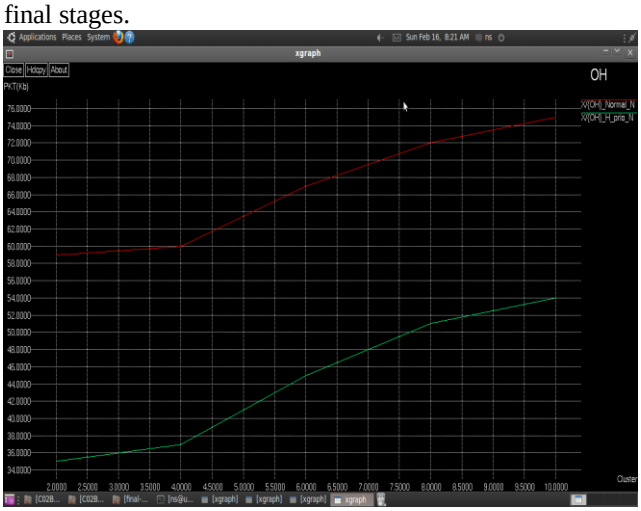

Fig.14. over Head Analysis

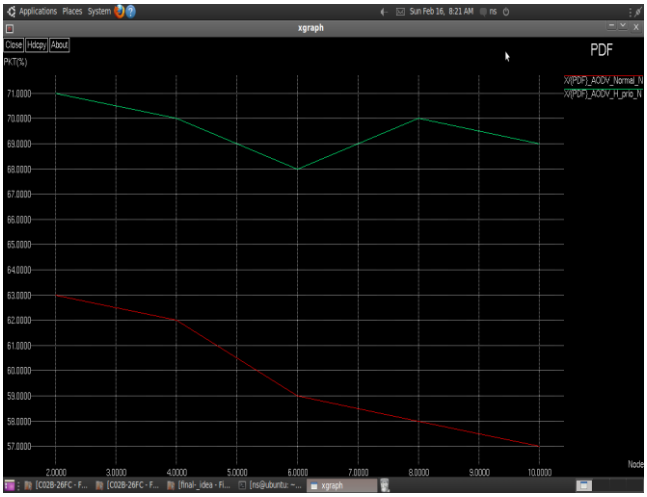

Fig.15. Packet Delivery

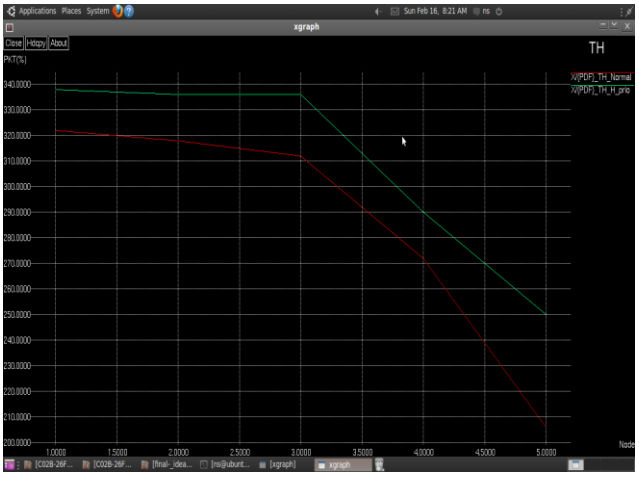

Fig.16. Threshold Calculation

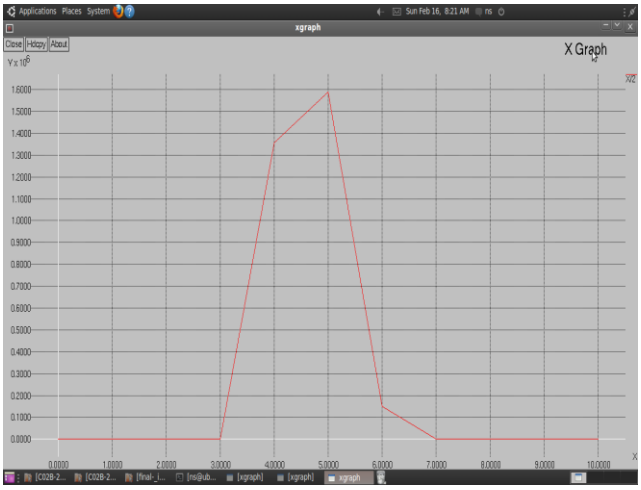

Fig.17. X Graph

V. CONCLUSION

VANET is a technology that uses moving car as nodes. The frequent disconnection of nodes has been minimized. The Greedy Perimeter Stateless Routing (GPSR) routing scheme used the shortest path with minimun number of intermediate interconnections. The connectivity time and disconnection problem between the nodes has minimized. Fast and reliable delivery of information between nodes has been achieved. A security scheme is included to make a safe VANET network. When we analysed the pacet delivery ratio is high and the delay time is high. İn future we will improve the delay time so that the system will work under all VANET conditions.

REFERENCES

[1] Pratap Kumar Sahu, Eric Hsiao- Kuang, "BAHG: Back-bone Assisted Hop Greedy routing for VANET'S city environment" IEEE Transactions on Intelligent Transportation systems, vol. 14, no.1, pp. 199-213, March 2013.

[2] J. Bernsern and D. Manivannan, "Unicast routing protocols for vehicular adhoc networks: A critical comparison and classification," Pervasive Mob. Comput., vol. 5, no. 1, pp. 1–18, Feb. 2009.

[3] V. Naumov and T. R. Gross, "Connectivity-aware routing (CAR) in vehicular ad hoc networks," in Proc. IEEE INFOCOMM 2007, pp. 1919–1927.

[4] C. Lochert, H. Hartenstein, J. Tian, H. Füßler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in Proc. IEEE Intell. Veh. Symp., 2003, pp. 156–161.

[5] H. Füßler, M. Mauve, H. Hartenstein, and D. Vollmer, "A comparison of routing strategies for vehicular ad-hoc networks," Dept. Comput. Sci., Univ. Mannheim,Mannheim, Germany, Tech. Rep. TR-02-003, Jul. 2002.

[6] H. Menouar, M. Lenardi, and F. Filali, "A movement prediction-based routing protocol for vehicle-to-vehicle communications," in Proc. 1st Int. V2VCOM, San Diego, CA, Jul. 2005.

[7] X. Jiang and T. Camp, "An efficient location server for an ad hoc networks,"Colorado School Mines, Golden, CO, Tech. Rep., MCS-03-06, May 2003.