Implementation of Efficient Cooperative Message Authentication for Vehicular Ad-Hoc Networks

Mrs. Prathiba . N ,
Dept Of TCE , BMSIT&M,
Bangalore,INDIA
e-mail: pratibha.yashas@gmail.com

Mrs. Saritha I G ,
Dept Of TCE , BMSIT&M,
Bangalore,INDIA
e-mail: sarithaig1224@gmail.com

Mrs. Sowmyashree M S ,
Dept Of TCE , BMSIT&M,
Bangalore,INDIA
e-mail: mssowmya22@gmail.com

***Abstract*—** Vehicular Ad-Hoc Network(VANET) is a potential area in research field to bestow Intelligent Transportation System (ITS) services to the end users. It is a exigent topic for its high mobility and frequent network distraction. Lately researchers are carrying out task on many specific issues related to VANET like routing, broadcasting, Quality of Service (QoS), security, architectures, applications, protocols, etc. The augment in vehicles in today's life has lead to brutal road accidents and traffic jam in urban areas. One of the solution to this problem could be a means of communication between the vehicles for safety. Safety measures lack these days in VANET as malicious drivers in the network disrupt the system routine. In this paper , a new location Based Secure Routing Protocol(PBSRP) which is a hybrid of Most Forward within Radius and Border Node based Most Forward within Radius (B-MFR) routing protocols. A module for security is implemented in this protocol using station to station key agreement protocol for preventing system from several attacks. The module goes through three phases: initialization phase, optimal node selection phase and secure data delivery phase. The outcome of Simulation imparts that PBSRP has better performance than MFR in terms of end to end delay and packet delivery ratio when malicious drivers are included in the network.

Keywords-*VANET,PBSRP,B-MFR,ITS*

*****

I. Introduction

Vehicular Ad-Hoc Networks (VANETs) have emerged as a promising approach to increase road safety and efficiency, as well as improve driving experience. This can be accomplished in a variety of applications that involve communication between vehicles, such as warning other vehicles about emergency braking; however, if we do not take security and privacy issues into consideration, the attractive features of ANETs will inevitably result in higher risks for abuse, even before the wide deployment of such networks. While message authentication is a common tool to ensure information reliability, namely data integrity and authenticity, it faces a challenge in ANETs. When the number of messages received by a vehicle becomes large, traditional exhaustive (or per-message) authentication may generate unaffordable computational overhead on the vehicle, and therefore bring unacceptable delay to time critical applications, such as accident warning[3]. In this paper, we propose an efficient cooperative authentication scheme for VANETs. In order to reduce the authentication overhead on individual vehicles, and shorten authentication delay, this scheme maximally eliminates redundant authentication efforts on the same message by different vehicles. To further resist various attacks, including free-riding attacks launched by selfish vehicles, and encourage cooperation, the scheme uses an evidence-token approach to control authentication workload, without the direct involvement of a trusted authority (TA). When a vehicle passes a Road-Side Unit (RSU), the vehicle obtains an evidence token from the TA, via the RSU .This token reflects the contribution that the vehicle has made to cooperative authentication in the past, which enables the vehicle to proportionally benefit from other vehicles' authentication efforts in the future, and thus, reduce its own workload. Through extensive simulation, we evaluate the proposed cooperative authentication scheme in terms of workload savings, and the ability to resist free-riding attacks.

II. LITERATURE SURVEY

Vehicular networks are very likely to be deployed in the coming years and thus become the most relevant form of mobile ad hoc networks. In this paper, the security of these networks is been addressed . An appropriate security architecture is devised and threats are analyzed. A set of few security protocols has been considered to analyze their robustness ,efficiency and privacy protection .

A model has been proposed to identify the most relevant communication aspects ,major threats and achieve robustness [1].

In paper [2], a distributed key management framework based on group signature to provision privacy in vehicular ad hoc networks (VANETs) is proposed. Distributed key management is expected to facilitate the revocation of malicious vehicles, maintenance of the system, and heterogeneous security policies, compared with the centralized key management assumed by the existing group signature schemes. In this framework, each road side unit (RSU) acts as the key distributor for the group, where a new issue incurred is that the semi-trust RSUs may be compromised. Thus security protocols for the scheme are developed to detect compromised RSUs and their colluding malicious vehicles. The issue of large computation overhead due to the group signature implementation is addressed. A practical cooperative message authentication protocol is used to alleviate the verification burden, where each vehicle just needs to verify a small amount of messages. Details of possible attacks and the corresponding solutions are discussed. A medium access control (MAC) layer is developed to carry out NS2 simulations and examine the key distribution delay and missed detection ratio of malicious messages, with the proposed key management framework being implemented over 802.11 based VANETs.

In paper [4] , a Timed Efficient and Secure Vehicular Communication (TSVC) scheme with privacy preservation is proposed, which aims at minimizing the packet overhead in terms of signature overhead and signature verification latency without compromising the security and privacy requirements.

Compared with currently existing public key based packet authentication schemes for security and privacy, the communication and computation overhead of TSVC can be significantly reduced due to the short message authentication code (MAC) tag attached in each packet for the packet authentication, by which only a fast hash operation is required to verify each packet. Simulation results demonstrate that TSVC maintains acceptable packet latency with much less packet overhead, while significantly reducing the packet loss ratio compared with that of the existing public key infrastructure (PKI) based schemes, especially when the road traffic is heavy.

III. METHODOLOGY

Current advancement in wireless technologies leads tomany new types of networks to be deployed in various environments. VANET is such type of emergingnetwork which brings revolution in the field of wirelesscommunication. Vehicular communication simply means thecommunication between the vehicles. Many standards,protocols, architectures, etc. are used for the implementationof VANET in specific environment to spread the service. Themain goal is to provide safety services to the end users. As weknow, WHO provides the road accident death statistics ofevery country and it concluded that if the death rate increasesin such a manner then accident will be the third cause of deathafter 2020. VANET creates a communication channelbetween the vehicles to save the vehicles from dangerous roadaccidents. Driver Alarm System, Speed Reducing System,Media Downloading, Virtual Marketing, etc. are some of theVANET applications to the end users. Many countries likeUSA, Japan and European nations have successfullyimplemented VANET projects supported by the government and many car companies like BMW, Ford, Dailmer, etc.The importance of VANET in the real life situation is a greatadvantage for the human society to use the ITS services. VANET architecture mainly consists of roads, streets,vehicles, road Side Units (RSU), Certification Authority (CA),etc. RSU acts as a router which is used for storing informationand computation. It is installed with sensors to trace the vehicles speed and broadcasting messages. CA is thecertification authority which gives certificate to the vehiclesby signing with its private key. The certificate shows thelevels of trust on that vehicle by CA. Vehicles are installedwith Global Positioning System (GPS) by which the vehicleknows its own position as well as it can trace the positions ofother vehicles. It is also installed with an On Board Unit forwireless communication. Further it is installed with ElectronicLicense Plate (ELP) by which one can get the unique numberof a vehicle.VANET security is themain issue nowadays to handle because many maliciousdrivers are entering into the network to create disruptions andreduce the network performance. In this paper, PBSRP routingprotocol is designed to find an efficient routing path and relaythe data by encrypting it with the Session Key (SK) to prevent the data from getting trapped by an intruder.PBSRP is a hybrid routing protocol which include the concepts of MFR and B-MFR to find the optimal nodeto relay the data. After finding the optimal node the main thingis to check whether the node is genuine or not, for that stationto station key management protocol is used which does not uses a third party for checking the nodes genuineness but ituses the CAs certificates for the vehicles to check whether thenode is a genuine node or imposter node. Simulation resultsshows PBSRP shows better results than MFR and B-MFR in terms of end to end delay and packet delivery ratio whenmalicious drivers are included in the network.

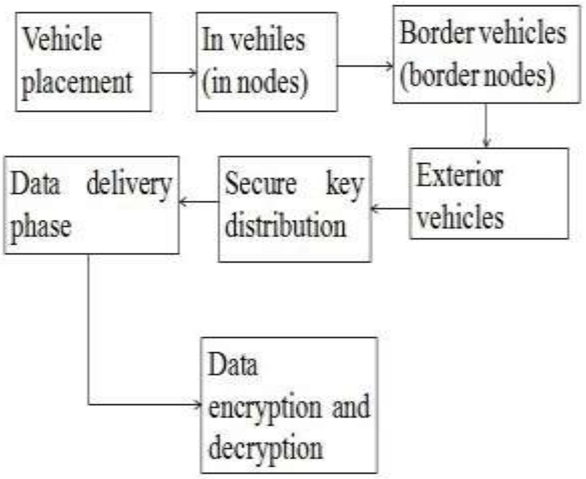


Fig 1: Block Diagram

VEHICLE PLACEMENT: In this phase an area under consideration is divided into 8 imaginary regions.In the present project each region is separated by a radius of 10 meters.Number of vehicles in a region is the input given by the user. Then the vehicles will be placed at random positions in each region.

FINDING IN VEHICLES: In vehicles are the vehicles which are within the GPS range of a particular vehicle.Flow chart for finding in vehicles will be explained in later sections

FINDING BORDER VEHICLES: Border vehicles are the vehicles which are present in the threshold GPS range of a particular vehicle. Flow chart for finding border vehicles will be explained in later sections.

SECURE KEY DISTRIBUTION: In this project we provide secure communication in vanets by the mechanism of secure key distribution.We use RSA algorithm for secure key distribution

DATA DELIVERY PHASE: In this phase a packet sent from source reaches destination by using PBSR protocol for routing.

SECURE KEY ENCRYPTION AND DECRYPTION: Secure key encryption is done at the source vehicle and decryption is done at the receiving vehicle. No intermediate vehicle can decrypt the message.

NODE DEPLOYMENT

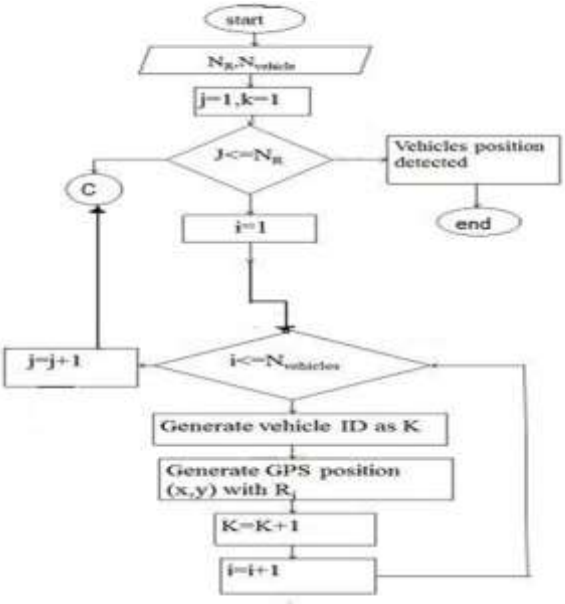


Fig 2: Node deployment

N_R=total number of regions

N_V=total number of vehicles

j=variable used to track number of regions

i=variable used to track vehicles in a single region

k=node ID of each vehicle

This flowchart is used to deploy the vehicles in a given region and create a map of vehicle ID, positions of nodes (GPS position).

DETECTION OF IN AND BORDER VEHICLES

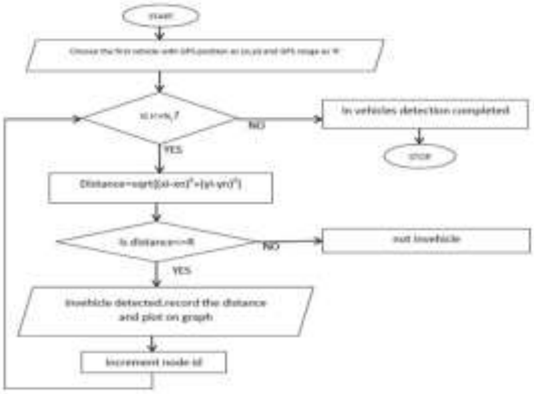

start
Choose the first vehicle with GPS position as (xi,yi) and GPS range as R
xi:i<=n,?
NO
In vehicles detection completed
stop
YES
Distance=sqrt((xi-xn)²+(yi-yn)²)
Is distance<=R
NO
out invehicle
YES
invehicle detected,record the distance and plot on graph
Increment node id

Fig.3: Finding IN Vehicles.

This flowchart shows the approach to find IN vehicles of a particular vehicle.

To find the border vehicles the condition statement in the above flowchart should be changed as $R<dist<=R+R_{th.}$

Where R is the GPS range and R_{th} is threshold GPS range of the vehicle under consideration.

POSITION BASED SECURE ROUTING PROTOCOL

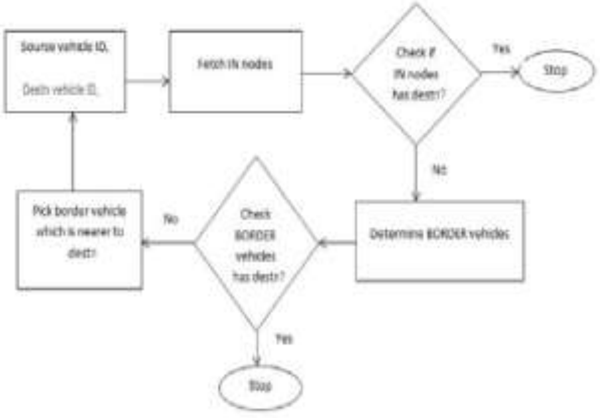

Sourse vehicle ID,
Destn vehicle ID,
Fetch IN nodes
Check if IN nodes has destn?
Yes
Stop
No
Determine BORDER vehicles
Check BORDER vehicles has destn?
No
Pick border vehicle which is nearer to destn
Yes
Stop

Fig 4:Position Based Secure Routing Protocol.

In PBSRP first source vehicle checks whether the destination lies within the GPS range. If it is present then direct communication takes place otherwise it checks in the border vehicles.If the destination is present in border vehicles range then the packet is delivered otherwise border vehicle nearer to destination is selected as source and procedure repeats.

IV. RESULTS

The figure below shows Region Formation considering for the Region of 180m square area. Each region is separated by 10m.There are 8 regions As shown in fig 5, Region 1 in Red colour, Region 2 in blue, region 3 in black, region 4 in green, region 5 in blue, region 6 in yellow, region 7 in Indigo , region 8 in dotted black.

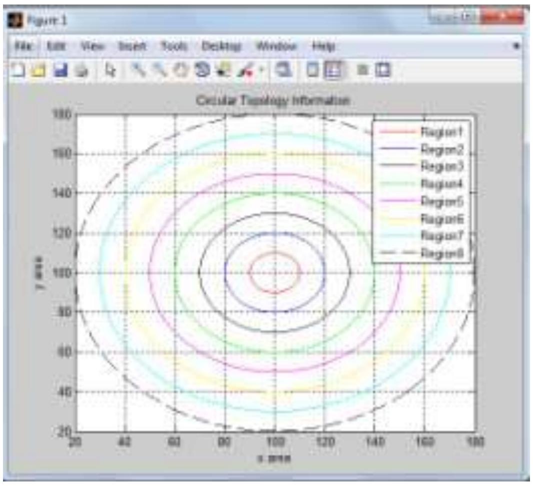


Fig.5: Region Formation.

The figure below shows vehicles deployment in each region. There are total of 8 regions and 3 vehicles in each region considered. As shown in the figure below , the vehicles deployed in Region 1 are vehicle id's 1,2,3. Vehicle id's 4,5,6 in Region 2. Vehicle id's 7,8,9 in region 3. Vehicle id's 10,11,12 in region 4. Vehicle id's 13,14,15 in region 5. Vehicle id's 16,17,18 in region 6. Vehicle id's 19,20,21 in region 7. Vehicle id's 22,23,24 in region 8.

Each vehicle wil have its GPS range and GPS Treshold Range. Vehices falling within GPS range will be considered as In vehicles. Vehicles falling out of GPS range but within GPS Threshold range will be considered as Border vehicles. Hence each vehicle will calculates its In vehicles and Border vehicles according to GPS range and GPS threshold range respectively.

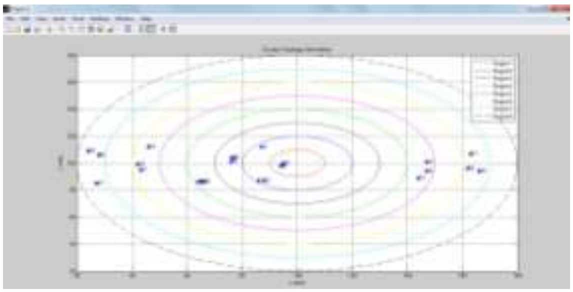


Fig. 6: Vehicles Deployment In Regions

As shown in the below figure ,In vehicles for vehicle 8 are vehicles with ids 1,2,5,6,7,11,12,15,16 with GPS range considered 30m. X-axis shows the no of vehicles, Y-axis shows the Distance from the considered vehicle.

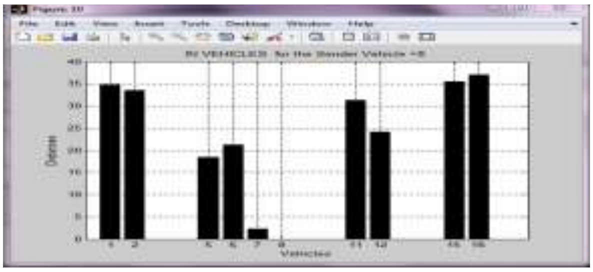


Fig .7: In Vehicles Calculation For Vehicle 8

As shown in the figure below , In vehicles for vehicle 16 are vehicles with ids 7,8,11,12,15 with GPS range considered 30m. X-axis shows the no of vehicles, Y-axis shows the Distance from the considered vehicle.

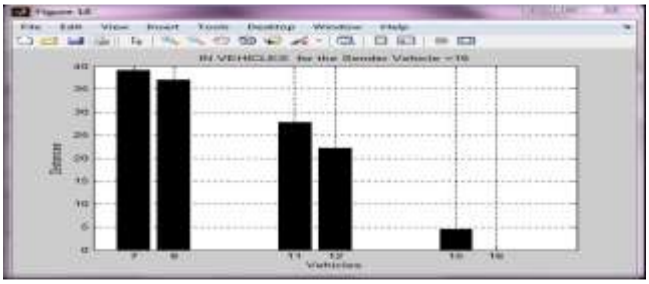


Fig .8: In Vehiles Calculation For Vehicle 16

As shown in the figure below Border vehicles for vehicle 1 are vehicles with ids 9,10,11,12 with GPS Threshold range considered 40m(30m GPS+10m Threshold).

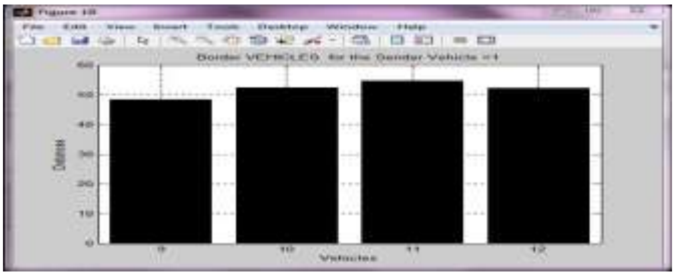


Fig. 9: Border Vehicles Calculation For Vehicle 1

As shown in the figure below Border vehicles for vehicle 12 are vehicles with ids 1,2 with GPS Threshold range considered 40m(30m GPS+10m Threshold). X-axis shows the no of vehicles, Y-axis shows the Distance from the considered vehicle.

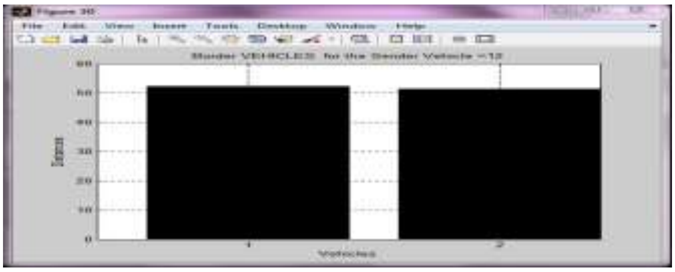


Fig .10 :Border Vehicles Calculation For Vehicle12

As shown in the fig above fig 5.7 Each vehicle wil have its unique token ID. Starting from the vehicle 1 upto vehicle 24 i.e 3vehicles in each region for a total of 8 regions considered. Token IDs will be distributed randomly for all vehicles.

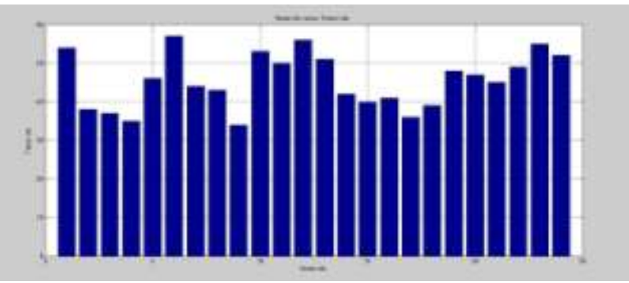


Fig .11: Secure Token ID Distribtion For All Vehicles

The figure below shows the route from source vehicle to destination vehicle. Hear we considering source vehicle to be vehicle 1 And destination vehicle to be vehicle 32.

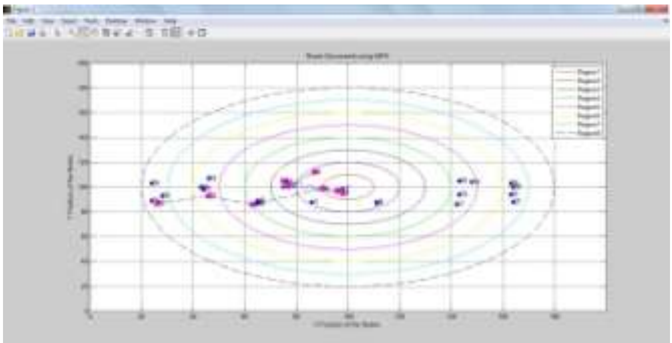


Fig .12: Route1 From Source Vehicle To Destination Vehicle

The Figure below shows the route from source vehicle to destination vehicle. Hear we considering source vehicle to be vehicle 1 And destination vehicle to be vehicle 32.

As shown in the figure below ,in MFR approach, when there are no vehicles within its GPS range it will take random routing and starts looping hence cause more delay and more number of hops.

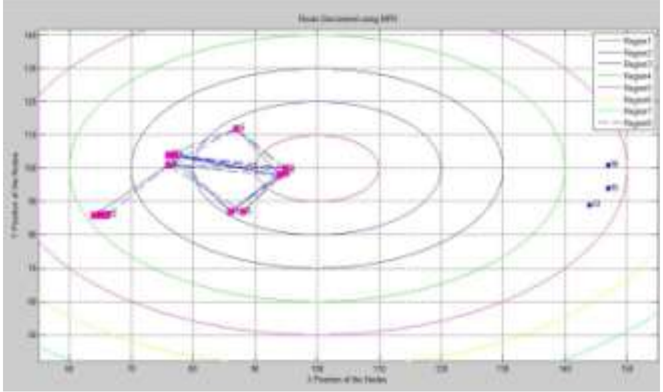


Fig .13: Route2 From Source Node To Destination Node

Looping Problem

The Figure below shows the secured data transfer using PBSRP. As shown in the figure below the initiator or sender vehicle is considered to be vehicle_1, intermediate vehicle is vehicle_11, destination vehicle is vehicle_24. Sender vehicle is encrypting data "bmsit" using encryption in ceaser as "lwcsd", at intermediate vehicle the data is still encrypted and at the receiver vehicle data is decrypted as"bmsit".

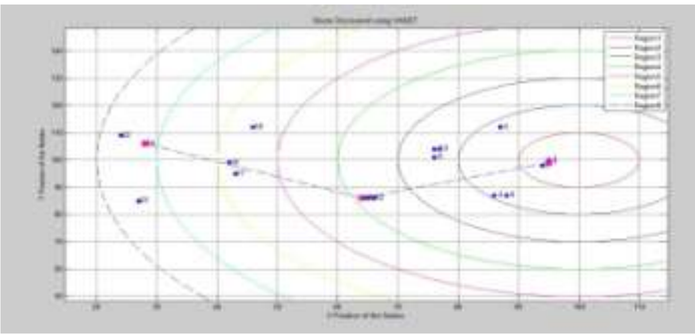
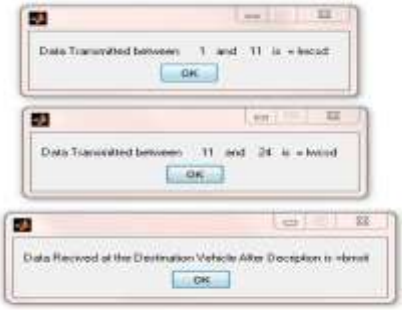


Fig.14:Best route from Source node to Destination node



Data Transmitted between 1 and 11 is = lwcsd
OK

Data Transmitted between 11 and 24 is = lwcsd
OK

Data Recived at the Destination Vehicle After Decription is =bmsit
OK

Fig.15: Encryption and Decryption of Data

The figure below shows route for malicious vehicle which is trying to receive and decrypt the message.

As shown in figure the malicious vehicle with ID 25 trying to receive a message sent to Vehicle 24. But since it’s a secured protocol and since it will not have the token it cannot decrypt the original message instead it will get an invalid message.

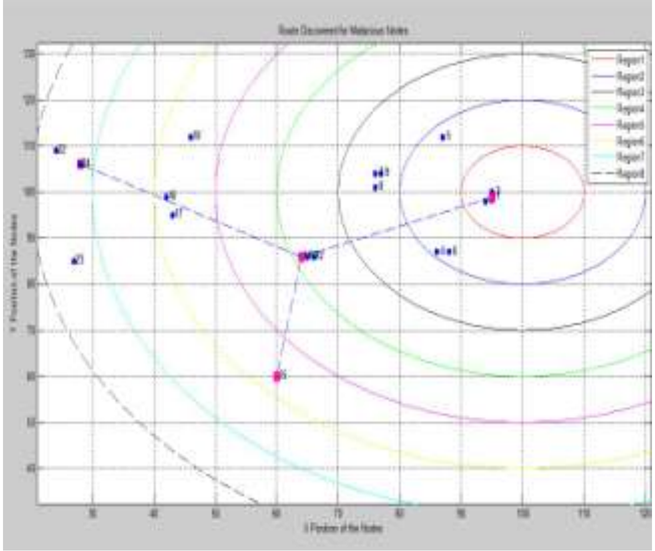
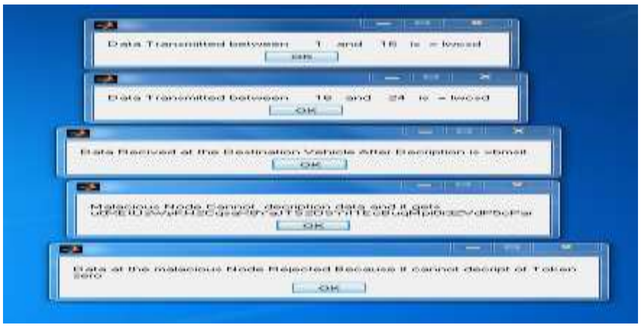


Fig.16: Route for Malicious vehicle



Data Transmitted between 1 and 16 is = lwcsd
OK

Data Transmitted between 16 and 24 is = lwcsd
OK

Data Recived at the Destination Vehicle After Decription is =bmsit
OK

Malacious Node Cannot decription data and it gets
[illegible]
OK

Data at the malacious Node Rejected Because it cannot decript of Token zero
OK

Fig.17: Malicious vehicle Decryption message

The figure below shows the route discovery time comparison of PBSRP versus MFR in the network. As shown in the figure the Route Discovery Time of the PBSRP is very much less as compared to MFR. Hence PBSRP performs better as compared to MFR with respect to Route Discovery Time or End to End Delay.

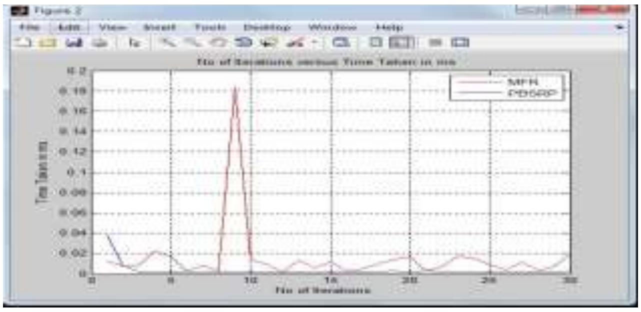


Fig .18:Route Discovery Time or End to End Delay MFR vs PBSRP

COMPARISON OF NUMBER OF HOPS

The figure below shows the number of hops comparison between MFR algorithm and the PBSRP algorithm as shown in the figure the MFR consumes more number of hops as compared to PBSRP algorithm.

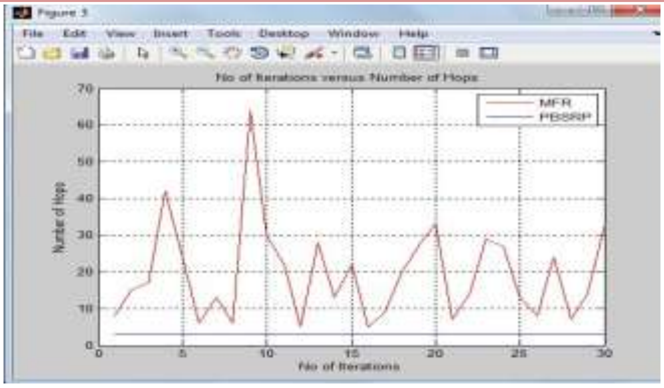


Fig .19: Comparison of Number of Hops MFR vs PBSRP

PACKET RECEPTION RATIO COMPARISON

The figure below shows comparison of packet reception ratio between MFR algorithm and the PBSRP algorithm as shown in the figure the MFR will have less number of packet reception ratio as compared to PBSRP algorithm.

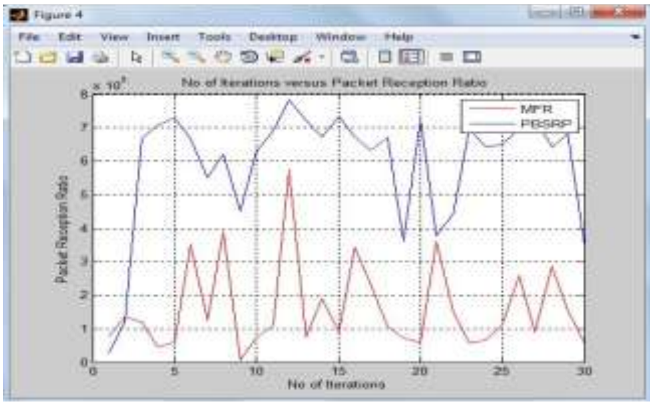


Fig.20: Comparison of Packet Reception Ratio MFR vs PBSRP

V. CONCLUSION & FUTURE WORK

The proposed system shows better performance than MFR routing protocols in terms of packet delivery ratio, number of hops and end-to-end delay. When packet dropping attack occurs to the system it is difficult for MFR to resists the attacks, but PBSRP uses a station to station key agreement protocol to generate a SK which helps the vehicles to recognize themselves. By this PBSRP prevent the network from the malicious drivers and make the system survivable from these active and passive attacks. PBSRP routing scheme with recovery strategy makes the system robust and it supports many real time applications like media downloading, marketing, safety communication, broadcasting advertisements, etc

Technology is always evolving, the application we have achieved is just a small milestone and there are a lot of ways in which our project can be improved in the future few of which are listed below. Trusted authority must have large data base to keep track of Selfish Vehicles and Malicious vehicles. Trusted authority should give Ratings to each vehicle based on the behavior in past. Sophisticated applications must be developed for vehicles in order to support advanced VANET technology.

REFERENCES

[1] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks,"Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.

[2] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 616?29, 2011.

[3] U.S. Department of Transportation, "National highway traffic safety administration," In Veh. Safety Commun.Project, Final Report. Appendix H: WAVE/DSRC Security, Apr. 2006.

[4] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Transaction on Wireless Communications, vol. 7, no. 12, DECEMBER 2008.

[5] Huang, I. Avramopoulos, B. L iu, and H. Kobayashi, "Secure dataforwarding in wireless ad hoc networks," inProc. ICC, Seoul, Korea,May 2005

[6] Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast authentication protocol," RSA Cryptobytes , vol. 5, no. 2, pp. 2-13, 2002.

[7] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks,"IEEE Trans Wireless Commun. 11, pp. 4136-4144, Nov. 2007.,vol.6,no.

[8] Nekovee, "Modeling the spread of worm epidemics in vehicular ad-hoc networks," in Proc. Veh. Technol. Conf., Montreal, Canada, Sept 2006