Avoiding Prankster Attack in Case of Selfish Driver using Location Aware VANET Nodes

Tanisha Saini
Department of Computer Science Engineering, Chandigarh Group of Colleges Gharuan, SAS Nagar, India

Maninderpal Singh
Assistant Professor, Department of Computer Science Engineering, Chandigarh Group of Colleges Gharuan, SAS Nagar, India

ABSTRACT
Vehicular Ad hoc Networks (VANETs) play a significant contribution in the field of Intelligent Transport Systems (ITS) which allow random vehicles to transmit security messages. Every node in VANETs works on the concept of single hop or multi-hop communication which means the nodes can move in a random manner within the network. The various vehicles which are moving in a random manner are considered as the moving nodes which are deployed in a haphazard behaviour in VANETs. Apart from these advantages, VANETs are much prone to security attacks which diminish the efficiency of network. The proper implementation of VANETs depends mainly on the security provided. Numerous techniques have been proposed in the last decade to provide security in VANETs. Hence, in this paper the main focus is being provided on the major attack in VANTEs which is called prankster attack. The nodes are deployed in the region having the information regarding the location with the help of Global Positioning System (GPS) where they get placed or located. The simulator used is NS-2. The simulated results reveal that the proposed methodology works in a similar way to minimize the prankster attack in case of selfish driver by the implementation of location aware nodes in VANETs.

Keywords
Vehicular Ad hoc Networks (VANETs), Intelligent Transport Systems (ITS), Global Positioning System (GPS), Selfish Driver, Prankster Attack.

1. INTRODUCTION
In the modern years, the concept of Vehicular Ad hoc Networks have gained the attention of many researchers because of their diverse set of applications. VANETs is one of the paradigm of Mobile Ad hoc Networks (MANETs) which is based on the concept of single as well as multi-hop routing scheme. VANETs play an important role in various applications such as the refinement in the transportation system, the collection of toll and the facilities of internet on the highways etc [1]. The concept of VANETs is same as that of Wireless Access in Vehicular Environment because of the use of Intelligent Transportation Systems (ITS). The Dedicated Short-Range Communication is also an important division of VANETs [2].

The architecture of VANETs is represented in the figure 1 as follows.

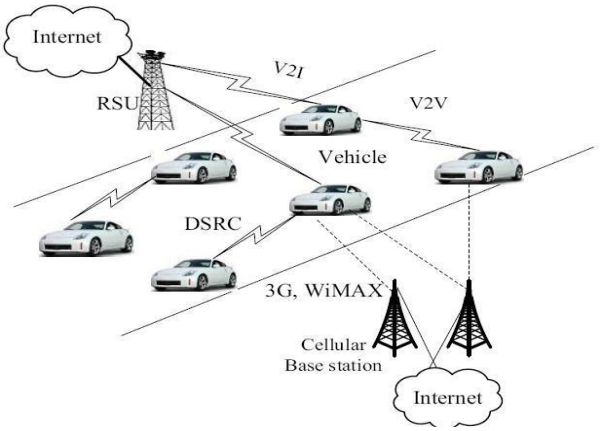


Figure 1: Architecture of VANETs [1]

VANETs primarily depend upon two types of communications which are elaborated in terms of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). For V2V communications the vehicles are integrated with the components like Omni directional antennas, microprocessors, integration with GPS and some of the sensor nodes having sensing, gathering and processing capabilities. The communication known as V2I are connected with roadside infrastructures positioned at fixed locations which is also called Road Side Unites (RSUs) [3] [4]. The locations in V2I are based on the communication range mechanism of roadside devices. These roadside devices are mainly named as RSUs which can only get interlinked with each either through wired or wireless communications [5] [6]. The major role of V2V communication is to transmit the real-time information and emergency messages. In case of any extremity on the road or highway, the V2V communication sends the information forthe alternative possible routes so that the congestion can be prevented [7] [8]. Apart from various pros of VANETs, still they are facing several cons in terms of security attacks or any loss of information within the network. These attacks may include the major attacks such are black hole or gray hole attacks, the transmission of fake or bogus information by malicious nodes or Daniel of service attack [9]. Therefore, to overcome these attacks, numerous techniques have been proposed in the last decade so that that the security attacks in the VANETs can be minimized and the performance can get enhanced [10] [11].

In this paper, the main focus is provided on Prankster Attack which transpires because of Selfish Driver. In this attack, the information is sent out by selfish driver by the means of false location and false driving messages. Hence, to prevail over this problem, in this paper, the vehicles or nodes get modelled with GPS i.e. all the nodes or vehicles are awaked and have

the information regarding their positions. By the integration of GPS module within the nodes, the location aware nodes will be aware regarding their positions and can easily discard the false or bogus information [7].

After introducing the concept of VANETs and various attacks in section 1, the rest of the paper is organized in five sections. Section 2 focuses on the literature survey regarding the VANETs and Section 3 proposes the proposed methodology. The simulation results and discussion have been carried out in Section 4. Conclusion and Future Scope is discussed in final section i.e. Section 5.

2. LITERATURE SURVEY

In the year 2013, the authors proposed a mobility pattern based misbehaviour [12] detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions (Misbehaviour), such as modify, fabricate, drop the messages in addition to, and impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse ordinal of the communications among VANET's nodes. Misbehaviour in VANETs can be viewed two perspectives: (i) physical movement and (ii) information security perspectives. Anonymous Location-Aided Routing for MANET (ALARM) is used for vehicular network which relies on the location information and corresponding time. This paper includes algorithms by which the misbehaviour can be detected. In [13], researchers discussed about challenges and problems of VANET and also talk about a solution to solve these challenges and problems. According to this paper each vehicle has OBU (On Board Unit).this unit connects vehicles with RSU via DSRC. and another device is TPD(Tamper Proof Device),this device hold the vehicle secrets like keys, drivers identity, trip **detail, route, speed etc.**

Various attacks discussed are DOS, Fabrication Attack, Alteration Attack, Replay Attack and various attackers are Selfish Driver, Malicious Attackers, and Pranksters. According to this paper several vehicular network challenges are Mobility, Volatility, Privacy VS Authentication, Privacy VS Liability, Network Scalability and various security requirements are Authentication, Availability, Non repudiation, Privacy, Integrity , privacy, Confidentiality In [14], again different issues concerned to effective security of VANET has been considered. Also two categories related to attack in VANET have been discussed. First category is physical attack which occurs because of tamper proof device and event data recorder and second category is logical attack which occurs due to the virus, Trojan horse and protocol weak spot.

A test bed performance evaluation of DTN-based routing protocols applied to VDTNs (vehicular delay tolerant networks) is proposed by the authors in [15]. The purpose of this work is to evaluate and understand how popular routing strategies perform in sparse or partitioned opportunistic vehicular network scenarios. Protocol used in this paper is Spray and Wait protocol. The idea behind using this protocol is to exploit the physical motion of vehicles and opportunistic contacts to transport data between disconnected parts of the network. According to proposed protocol the buffer size and bandwidth is reduced because this protocol manages the flooding by sending single copy of message but suffer from long delivery delay. In the year 2008, a new Heterogeneous Vehicular Network (HVN) architecture [16] and mobility prototype responsive routing has been introduced for HVN. According to paper HVN assimilates Wireless Metropolitan Area Network (WMAN) with VANET and reserves advantages of superior coverage in WMAN which results in higher data rates in VANET. Vehicles or nodes in HVN can make contact with each other and access the services of Internet universally. They chiefly spotlight the routing issue for HVN, because the routing protocol for HVN is different from those implemented in MANET or VANET. The Mobility Pattern Aware Routing Protocol (MPARP) for HVN to provide more reliable V2V service has been proposed.

A Geo-casting technique in an IEEE802.11p [17] based vehicular Ad hoc network for the management of road traffic is explained in paper. The authors discussed the geo-casting packet transmission scheme for the transference of security information in a vehicular network. The authors used simulation based on OPNET model to analyse the performance of planned protocol. According to authors the VANET can be seen as self organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. The proposed protocol selects the furthest vehicle for the rebroadcast with the help of new back off window design which reduces the number of packet transmission thus lowering the contention levels. The proposed protocol offer very low convergence and warning notification time compared to the other protocols and also generate lower broadcast overhead and packet loss ratio as compared to other protocols. In the year 2008, the authors proposed an overview on a priority based secure MAC Protocol [18] for vehicular networks and he assume that the MAC Protocol can achieve both QOS and security in vehicular networks. In this paper the authors proposed that the MAC Protocol is having massages with different priority for different application to access DSRC (Dedicated short range communication channel) channel .The proposed secure MAC Protocol will use a part of IEEE 1609.2.

3. PROPOSED METHODOLOGY

VANETs are the networks which work on the concept of MANETs. The role of VANETs focuses on the behaviour of vehicles which can act as nodes within a network. The communication between the nodes can be done on the basis of wired as well as in a wireless manner [19]. But, because of various advantages there are many security attacks exist in VANETs. In the proposed work, the GPS module is get modelled with the VANET's nodes which can get the information regarding the false data or fake messages. Therefore, the main focus of proposed work is to avoid the prankster attack in case of selfish driver using GPS module in nodes of VANET. The proposed work is represented in the form of flowchart as follows.

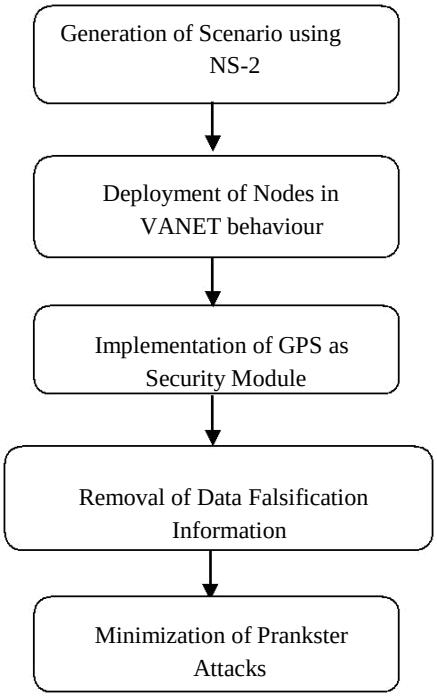
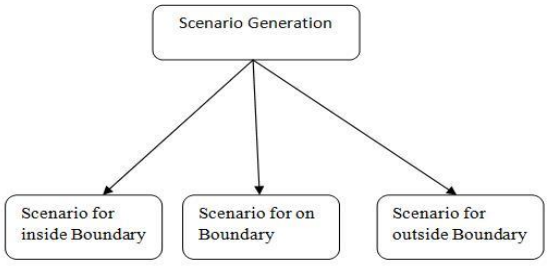


Figure 2.1: Flow of Scenario

Now, it become feasible to get information regarding the proposed work by constructing a flowchart in Figure 2 which shows the explanation of work proposed in a stair manner. The first part of flowchart is the generation of scenario in the Network Simulator i.e. NS-2 which is described further in next flow chart. The nodes are deployed in a random manner same as that of vehicle in VANETs behaviour. The third step is to integrate whole of the nodes or vehicles with world's best module named as GPS which reverts the false messages or information coming from the bogus or selfish drivers in the step 4. This results in the formation of secure network in the VANETs which is shown in the step 5 by minimizing the prankster attacks.

3.1 Types of Scenario

Every node has its some diameter so in this research three scenarios are considered. In first scenario prankster node is inside the boundary and try to falsify its location within the boundary, in second scenario the prankster node lies on the boundary and in third scenario the prankster node lies outside the boundary of victim node.



3.2 Work Flow

1.) Prankster node **P** send its location information (X,Y co-ordinates) to node **X**
2.) Node X receive the location coordinates X and Y of node P
3.) Node X stores its location coordinates in variables X1 and X2
4.) Node X receives the coordinates from node Y and stores them in Y1 and Y2
5.) Node X computes the position of the point within the circle between node X and Y using formula to know that point is within circle or not, i.e. within in transmission range or not

$$Res = (X1-Y1)^2+(X2-Y2)^2$$

If $R^2 < Res$, *Point is within the circle*
If $R^2 == Res$, *Point is on the boundary If* $R^2 > Res$, *Point is outside the circle Where,*

X1, X2 *are coordinates of target node*
Y1, Y2 *are coordinates of test node*
R *is transmission radius*

6.) Calculate the distance between node X and Y using formula:

$$Distance = \sqrt{(X1-Y1)^2+(X2-Y2)^2}$$

Where,

X1, X2 *are coordinates of target node*
Y1, Y2 *are coordinates of test node*

7.) Calculate the displacement of node Y using formula

$$Displacement = \sqrt{(oY1-nY1)^2+(oY2-nY2)^2}$$

Where,

oY1, oY2 *are old coordinates*
nY1, nY2 *are new coordinates*

8.) Node X makes the decision logic and updates other nodes in the cluster.

4. SIMULATION RESULTS AND DISCUSSION

In this research three scenarios are considered and some assumption are

a. All VANET nodes must be aware about its own location and direction of movement.
b. VANET nodes may be the part of VANET cluster.
c. VANET nodes must have processing power on their own. (Nodes should not depend on centralize node for the decision logic).
d. Nodes must be capable of sharing its information in step a. with other nodes in the neighborhood or cluster.
e. Every node has its some diameter and it can communicate with other nodes which are lie within its diameter.

4.1 Simulation Table

This table describe the values taken for particular parameters.

Parameters	Values
Routing Protocol	AODV, GPSR
Number of Nodes	20
Simulation time	900 sec
Mac Protocol	Mac 802.11
Queue Length	50
Radio Propagation Model	Two Way Ground
Antenna	Omni Antenna
Simulation Area	1000*1000 m
Transmission Range	250 m

4.2 Results of Scenario 1

Scene 1

In this scene nodes are initializing, nodes with yellow colour (i.e node number 5,6,7,8) are coming from that lane whose lights are green. Rest all nodes have to stop by reaching on lights. Node 2 is victim node here and node 3 is prankster. For this scene prankster is lie inside the boundary range of node 2 i.e victim node. Here 3 falsify its location to node 2 by sending message that it is in front of node 2 but as the system has GPS facility it can check by calculating GPS distance and match the same with the GPS coordinates. In this way the attack is prevented.

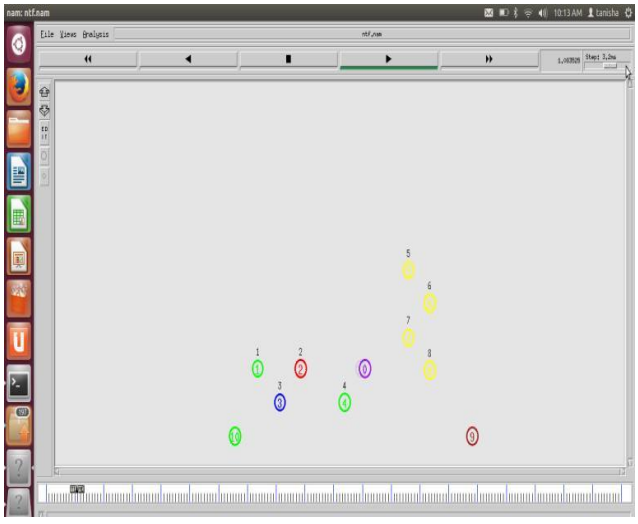


Figure 3.1 Represents initialization of nodes

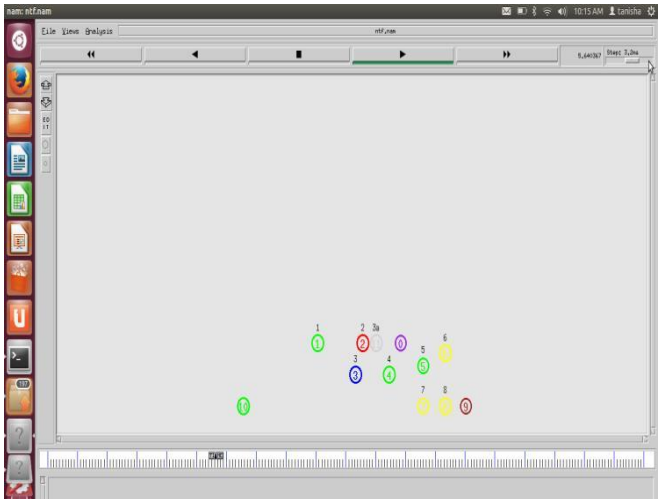


Figure 3.2 Represents communication between nodes

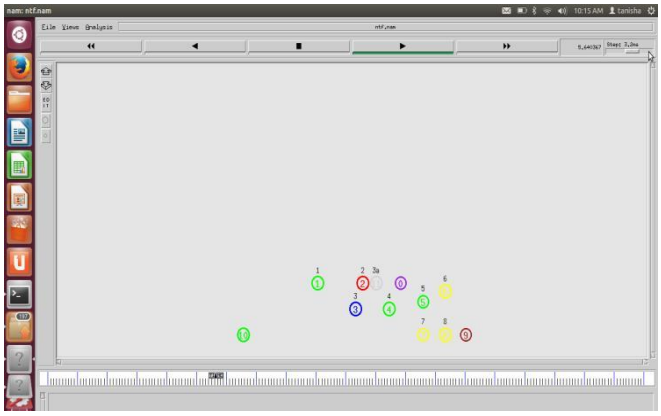


Figure 3.3 Represents falsify location of 3 in front node 2

Here node 3 falsifies its location to node 2 by sending message to node 2 that it is ahead node 2. Like in this scenario 3a is false location of 3.

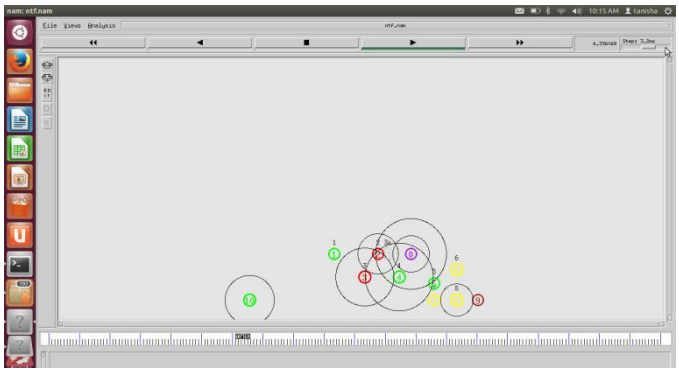


Figure 3.4 Checking of GPS coordinates

When node 2 gets message from prankster node then it will stop for some time and calculate distance of prankster place and match the same with GPs coordinates.

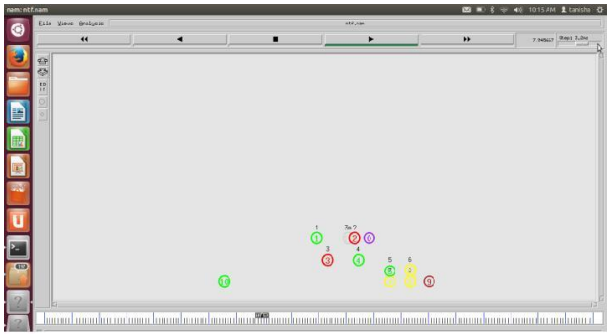


Figure 3.5 After Attack

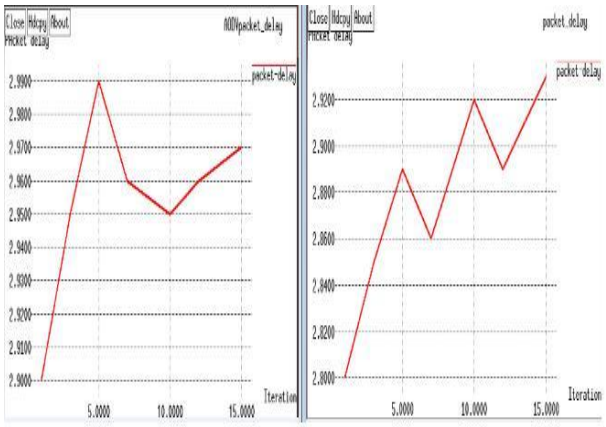


Figure 3.6 Represents X-Graph for Delay (AODV v/s GPSR)

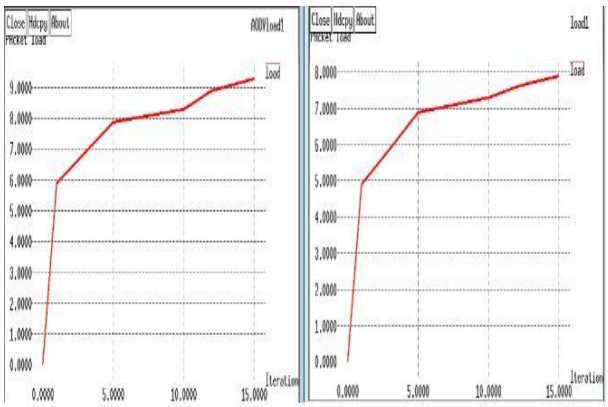


Figure 3.7 Represents X-Graph for Load (AODV v/s GPSR)

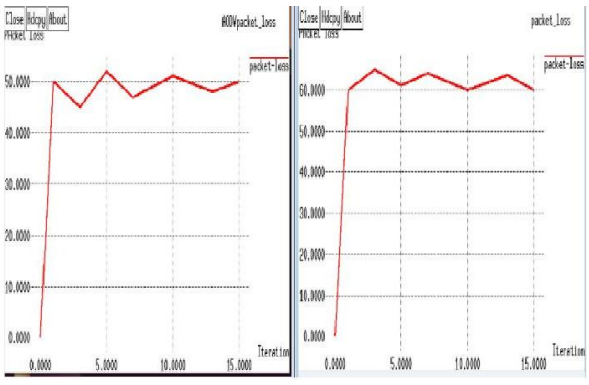


Figure 3.8 Represents X-Graph for Loss (AODV v/s GPSR)

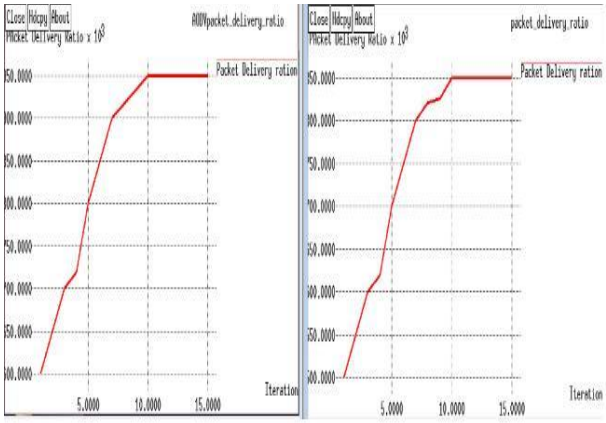


Figure 3.9 Represents X-Graph for PDR (AODV v/s GPSR)

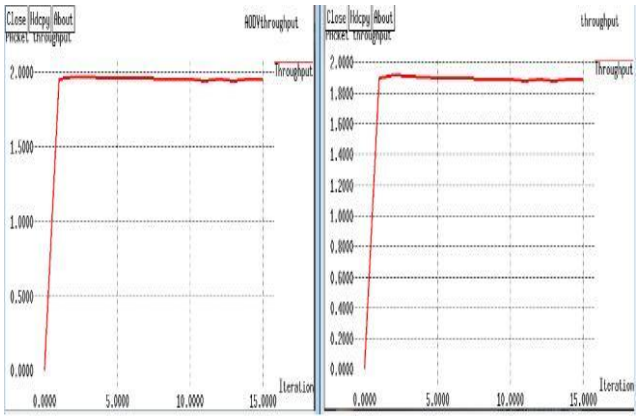


Figure 3.10 Represents X-Graph for Throughput (AODV v/s GPSR)

5. CONCLUSION AND FUTURE SCOPE

Security in VANETs is one of the major concerns in the safety of networks. But, because of security attack, VANTEs are facing so many serious issues which can degrade their performances. The attacks include Daniel of Service attack, the attacks because of gray and black holes and fake messages attacks in the form of prank messages. Hence, in this paper we proposed GPS module which overcomes this issue in an efficient manner. The simulation results have been carried out showing that the attacks can be minimized when the nodes within VANETs get modelled with GPS module. The simulated results also reveal that the proposed scenario works in an efficient manner to diminish the prankster attack by selfish driver after the implementation of location aware nodes in VANETs.

6. REFERENCES

[1] M.S. Al-Kahtani, "Survey on Security Attacksin Vehicular Ad hoc Networks (VANETs)," *IEEE,* 2012.

[2] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-Vehicle Wireless Protocols for Enhancing Highway Traffic Safety," *IEEE Communications Magazine*, vol. 44, no. 1, pp. 74-82, 2006.

[3] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", *IEEE Wireless Communications*, vol 13, 2006.

[4] GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks," in *proceedings of UBIROADS workshop*, 2007.

[5] M Raya, J Pierre Hubaux," The security of VANETs," in *proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, 2005.

[6] Car-to-Car Communications, www.car-2-car.org

[7] S. Zeadally, R. Hunt, Y. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges," *Telecommunication Systems*, pp. 1–25, 2010.

[8] V. Paruchuri, "Inter-vehicular communications: Security and reliability issues," in *International Conference on ICT Convergence (ICTC),* , 2011, pp. 737-741.

[9] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. Securing Vehicular Communications - Assumptions, Requirements, and Principles, *In Proceedings of the Workshop on Embedded Security in Cars (ESCAR) 2006*, November 2006.

[10] N. Sastry, U. Shankar and D. Wagner. "Secure Verification of Location Claims". *In ACM Workshop on Wireless Security*. WiSe 2003.

[11] T,W, Chim, S.M. Yiu, "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189-203, March 2011.

[12] F. A. Ghaleb, M. A. Razzaque, I.F. Isnin "Security and Privacy Enhancement in VANETs using Mobility Pattern," *IEEE*, 2013.

[13] G. Samara, A.H. Wafaa Al-Salihy, R. Sures "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," *IEEE*, 2010.

[14] P. Seuwou, D. Patel, D. Protheroe, G. Ubakanma "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".

[15] J. A. Dias, J. N. Isento, V. N. G. J. Soares, F. Farahmand, and J. J. P. C. Rodrigues "Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks," *IEEE*, 2011.

[16] Chia-Chen Hung, H. Chan, and Eric Hsiao-Kuang Wu "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks," *IEEE WCNC* 2008.

[17] M. A. Javed and J. Y. Khan "A Geocasting Technique in an IEEE 802.11p based Vehicular Ad hoc Network for Road Traffic Management," 2010.

[18] Y. Qian , K. Lu , and N. Moayeri "performance evaluation of a secure mac protocol for vehicular networks," *IEEE*, 2008**.**

[19] Ravinder singh "Design of trust model based on ideas of localization in opportunistic networks," IJSER , June 2013