International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Issue 07, Volume 3 (October 2016) ISSN: 2349-7009(P)
www.ijiris.com

A SECURE SCHEME FOR MONITORING SAFETY IN VEHICULAR ADHOC NETWORK

Devika.M*
Assistant professor Electronics & Communication Engineering
Sathyabama University,Chennai,India

Abstract *— Vehicle ad-hoc networks has significantly used in automobiles for an effective communication with one another. The decentralized nature of this network provides an extensive range of applications which makes passenger safety and comfort. Providing security in a physical environment is considered to be the main issue to cope with. Vehicle-to-vehicle communication is the wireless transmission of data between the vehicles. It is more efficient and it enables 360 degree awareness of the surrounding threats. To overcome this issue a popular approach is recommended in VANET, is that cars are connected together via V2V,which are able to share data with one another, so that there is, less possibility of collision and other mischievous behaviour i.e. drunken drive. Although there are many proposed solutions for improving securities in VANET but security still remains a delicate research subject. The main objectives of this paper is to improve the security issues in VANET.*

Keywords*— Vehicle Adhoc Networks (VANET), Vehicle to Vehicle Communication (V2V), Vehicle to Infrastructure Communication (V2I), Road side Unit (RSU).*

I. INTRODUCTION

Intelligent Transport System (ITS) is a technology applied to transport and infrastructure to transfer information between systems for improved safety. The advancement in vehicular ad hoc networks (VANETs) have elevated the intelligent transportation systems (ITSs) to higher levels and also made vehicle telematics more attractive to the public. In VANETs, each vehicle is equipped with an on-board unit (OBU) communication device, which allows them to communicate not only with each other, i.e., vehicle-to-vehicle (V2V) communications, but with roadside units (RSUs), e.g., vehicle-to roadside (V2R) communication. Due to this hybrid architecture of VANETs, a variety of promising applications, ranging from safety (e.g., Emergency and Accident) to non-safety (e.g., infotainment), can be enabled to improve the road safety and better driving experiences. With an immense improvement in technological innovations, we find Vehicular Communication as a solution to many problems of our modern day communication system in roads. VC involves the use of short range radios in each vehicle, which would allow various vehicles to communicate with each other which is also known as V2V communication and with road side infrastructure V2I communication. These vehicles would then form an instantiation of ad hoc networks in vehicles, popularly known as Vehicular Ad Hoc Networks.

A Vehicular Ad-Hoc Network, or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created. VANET is mainly designed to provide safety related information, traffic management, and infotainment services. Safety and traffic management require real time information and this conveyed information can affect life or death decisions. Simple and effective security mechanism is the major problem of deploying VANET in public. Without security, a Vehicular Ad Hoc Network (VANET) system is wide open to a number of attacks such as propagation of false warning messages as well as suppression of actual warning messages, thereby causing accidents.

This makes security a factor of major concern in building such networks. VANET are of prime importance, as they are likely to be amongst the first commercial application of ad hoc network technology. Vehicles are the majority of all the nodes, which are capable of forming self-organizing networks with no prior knowledge of each other. The capacity of VANET technology is high with a wide range of applications being deployed in aid of consumers, commercial establishments such as toll plazas, entertainment companies as well as law enforcement authorities.

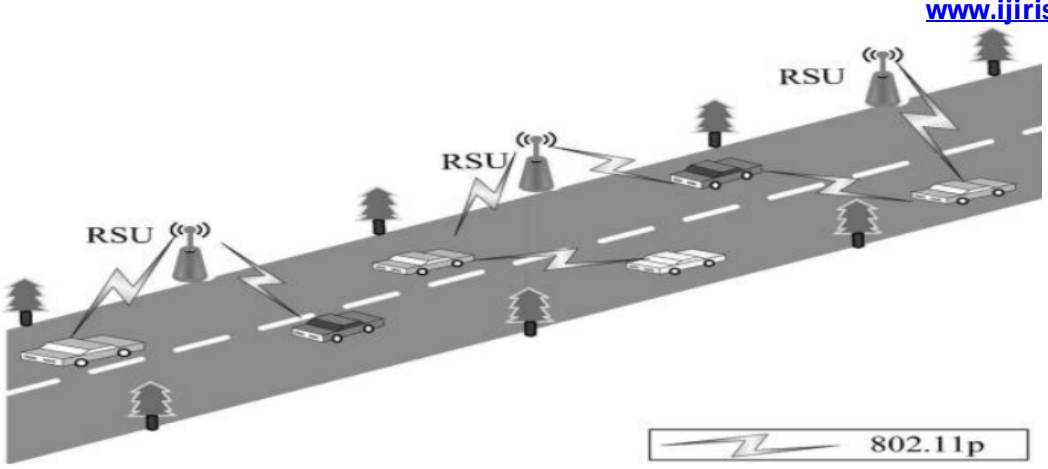

Figure 1. VANET

In the figure 1, the basic structure of the vanet deployed have been shown: However, without securing these networks, damage to life and property can be done at a greater extent. Goal of this project is to come up with an entirely new solution that can be implemented in designing a VANET. Vehicle to Vehicle communication approach is most suited for short range vehicular networks. It is fast and Reliable and provides real time safety. It does not need any roadside Infrastructure.V2V does not have the problem of Vehicle Shadowing in which a smaller vehicle is shadowed by a larger vehicle preventing it to communicate with the Roadside infrastructure. In V2V the connectivity between the vehicles may not be there all the time since the vehicles are moving at different velocities due to which there might be quick network topology changes. The anonymity problem: The addresses of vehicles on highways are unknown to each other.

[2]Periodic broadcasts from each vehicle may inform direct neighbours about its address, but the address-position map will inevitably change frequently due to relative movements among vehicles. It is the receiver's responsibility to decide the relevance of emergency messages and decide on appropriate actions. Location based broadcast and multicast are the proper communication methods for collision avoidance in V2V Communication. Without any roadside infrastructure, multi hop forwarding must be enabled to propagate the messages or signals. Hence, V2V communication is not very useful in case of sparsely connected or low density vehicular networks.

II. RELATED WORKS

L. Buttyan, et al., [3] proposed a simple straightforward solution, where an OBU device equipped on a vehicle possesses a large number of anonymous short-time keys that are authorized by a TA. By this conditional privacy can be achieved by randomly changing the pseudonyms. [4]Julien Freudiger et al., defined third parties can track the location of mobile nodes by monitoring the pseudonyms used for identification. A frequently proposed solution to protect the location privacy of mobile nodes suggests changing pseudonyms in regions called mix zones. He proposed a novel metric based on the mobility profiles of mobile nodes in order to evaluate the mixing effectiveness of possible mix zone locations. Then, as the location privacy achieved with mix zones depends on their placement in the network, we analyze the optimal placement of mix zones with combinatorial optimization techniques shown in figure 2. Pseudonym based schemes have been proposed to preserve the location privacy of vehicles.

However, those schemes require the vehicles to store a large number of pseudonyms and certifications [5], and do not support some important secure functionalities such as authentication and integrity. Cheng.S et al., [6] describes mobile users tend to return regularly to certain locations (e.g., home and workplace), indicating that despite the diversity of their travel locations, humans follow simple reproducible patterns. Giorgio Calandrielloy et al., [7] proposed, how to achieve efficient and robust pseudonym-based authentication. We design mechanisms that reduce the security overhead for safety beaconing, and retain robustness for transportation safety, even in adverse network settings. Moreover, we show how to enhance the availability and us- ability of privacy-enhancing VANET mechanisms: Our proposal enables vehicle on-board units to generate their own pseudonyms, without affecting the system security.

M. Gerlach explained [8] GSIS is a group-signaturebased (GSB) technique that can achieve conditional location privacy without PC. However, the pure group signature verification is usually time consuming, which may be not suitable for some time- constraint VANET applications. Dan Boneh et al., [9] described A short signature scheme that is strongly existentially unforgettable under an adaptive chosen message attack in the standard security model. Our construction works in groups equipped with an efficient bilinear map, or, more generally, an algorithm for the Decision Diffie-Hellman problem.

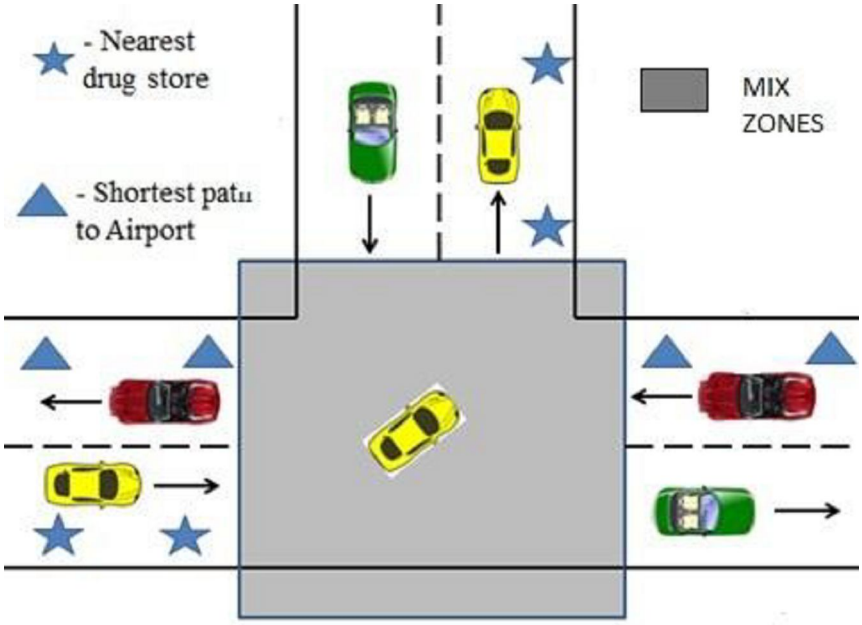

Figure 2. Collision at Road Intersection

The security of our scheme depends on a new intractability assumption we call Strong Diffie Hellman (SDH), by analogy to the Strong RSA assumption with which it shares many properties. Signature generation in our system is fast and the resulting signatures are as short as DSA signatures for comparable security. We give a tight reduction proving that our scheme is secure in any group in which the SDH assumption holds, without relying on the random oracle model.

III.EXISTING SYSTEM

In this model, VANET model has been deployed with set of required parameters. The architecture [10] of the vehicle to vehicle communication is given below:

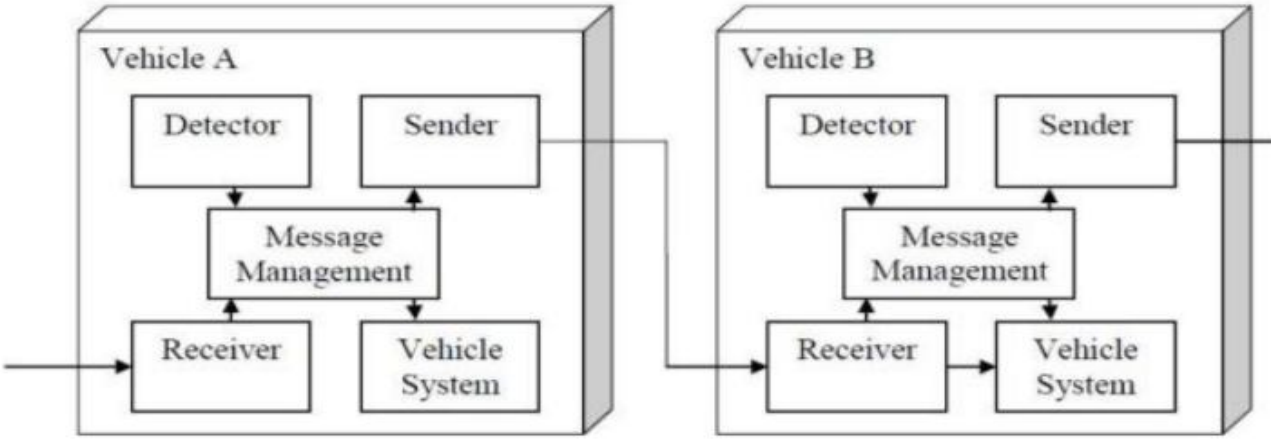

Figure 3. Vehicle to Vehicle Communication Architecture.

First identify the conditions required for two or more vehicles to collision. Suppose t, is Arrival Time and t, is Exit Time is the time at which the vehicle exits at any intersection place x. If a vehicle A communicate with another vehicle B is in the intersection place, their intervals must overlap. Two vehicles being inside the same intersection at the same time is a necessary, but not sufficient condition for a collision. A scenario in which vehicle A is coming from the east and turning right while the other vehicle B is coming from the west and also turning to its right. In this case, both vehicles can cross the intersection point at the same time without a collision.

A collision occurs if Same Intersection, Time Conflict, and Space Conflict of vehicle condition are true. If any of the above three conditions is false, then there will be no collision and vehicles can safely continue along their route [11].The collisions are described in a finite manner, It needs time to inform the RSU's available near to the location. Vehicle used to communicate with one another in the form of simple messages like STOP, CLEAR, CONFIRM and DENY.

By this, the vehicle can control themselves to avoid collision. If any chance of intruder arrives, they can able to steal the identity and show them as a benign vehicle to send false messages.

IV. PROPOSED MODEL

In this model, the work is divide into three parts: Collision Avoidance, Drunk & Drive Detection and Fake ID Control. So, the proposed model overcomes the existing scheme for collision and message generation.

A. COLLISION AVOIDANCE

This can be carried out using Orthogonal Amplify and Forward Algorithm (OAF), which has the control over the vehicles in the same infrastructure. The communication between the vehicle and the Road side unit is orthogonal, hence the message transfer is effective. It can be seen that the collision can be controlled by the control messages between the vehicle and the Road side Unit's. For example, a road consists of four lanes in which the vehicles are travelled in their respective depends upon their velocity, in case any chance of collision occurs, it will be avoid by the following sequence of steps.

Step-1: Start
Step-2: Set the orthogonal path between the Vehicle and the RSU
Step-3: Control the communication
Step-4: Record speedometer and GPS readings.
Step-5: Transfer GPS, speedometer reading and angle of turn are reported through VANET.
Step-6: Generate Cone movement.
Step-7: Estimate Collision area.
Step-8: Avoid collision by generating control messages.
Step-9: Stop.

B. DRUNK AND DRIVE DETECTION:

The Vehicle driver who have consumed alcohol may also be a cause to create sudden accidents in broad road ways. We can protect this by keeping advance hardware mechanisms to detect the irregular functionalities. From the figure 4 , if the vehicle driver consumes alcohol, it will be detected by the gas sensor. The working of gas sensor is Sensitive material of MQ-6 gas sensor is SnO2, which with lower conductivity in clean air. When the target combustible gas exist, the sensor's conductivity is higher along with the gas concentration rising.

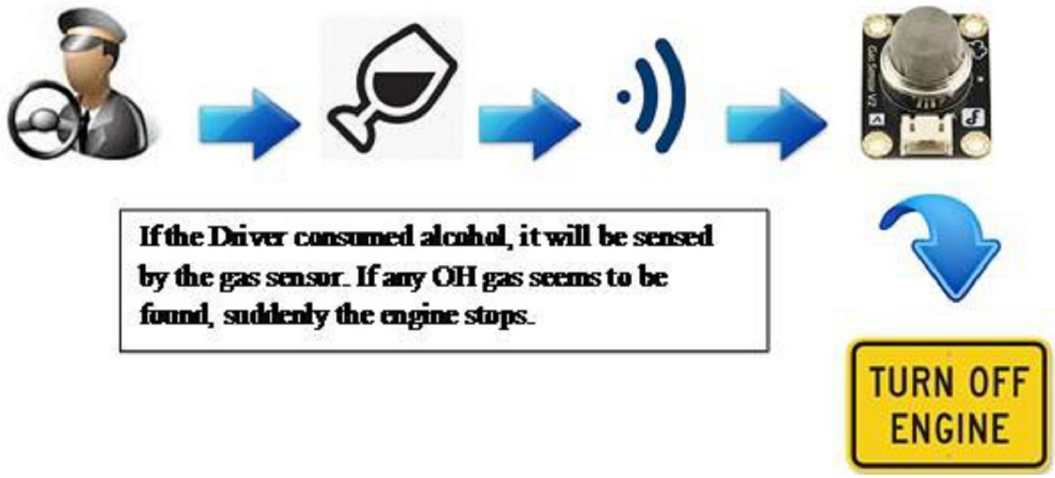

Figure 4. Drunk and Drive detection

Convert change of conductivity to correspond output signal of gas concentration. MQ-6 gas sensor has high sensitivity to Propane, Butane and LPG, also response to Natural gas. The sensor could be used to detect different combustible gas, especially Methane, it is with low cost and suitable for different application.

From the figure 5, shows the typical sensitivity characteristics of the MQ-6, ordinate means resistance ratio of the sensor (Rs/Ro), abscissa is concentration of gases. Rs means resistance in different gases, Ro means resistance of sensor in 1000ppm LPG. All test are under standard test conditions. If any characteristics of alcoholic gases sensed by the Gas sensor, suddenly it sends electrical signal to the controller. The controller has a relay which will be acting like a switch, a relay is an electrically operated switch.

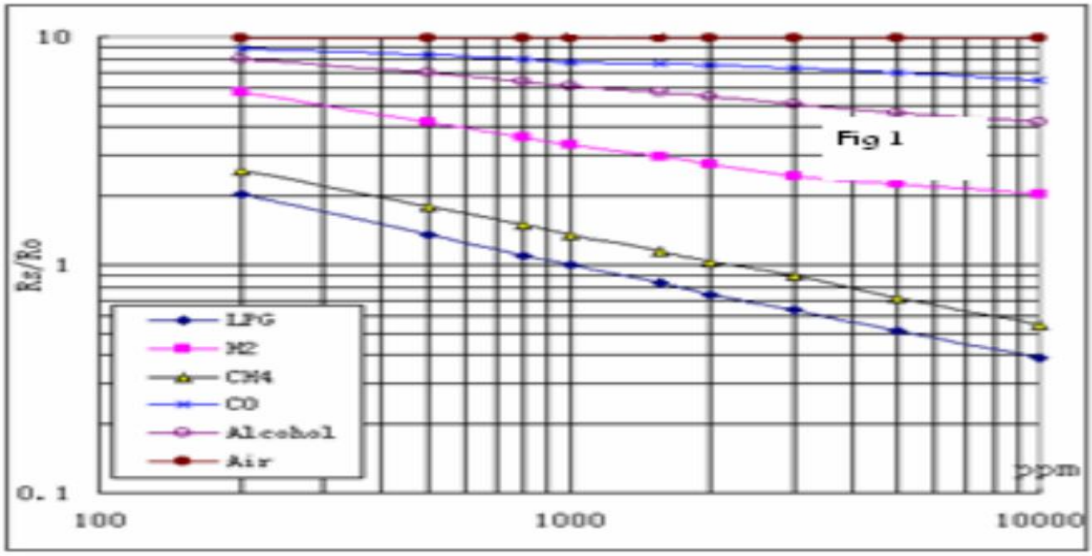

Figure 5. Sensitivity of MQ-6

Many relays use an electromagnet to operate a switching mechanism mechanically, but other operating principles are also used. Relays are used where it is necessary to control a circuit by a low-power signal (with complete electrical isolation between control and controlled circuits), or where several circuits must be controlled by one signal. If the switch is on, electrical signals produce the effect to turn off the engine. This may reduce the collision considerably.

V. SIMULATION

In this section, we are going to evaluate the collision avoidance by observing the various privacy preservations that has been already created [12],[14]. In particular, extensive simulations are conducted to demonstrate the impacts of different parameters on the performance metrics in terms of delay and verified signatures. Our simulations are based on a discrete-event simulator coded in C++, where the simulation parameter is listed for the collision level at the junctions. We can repeat the simulation 100 times with different random seeds and calculate the average value. For making the network and absorbing the values we first set up the network model using MOVE (Motor Vehicle Emission Simulator), SUMO (Simulation Of Urban Mobility) and NS2(Network Simulator 2.34)

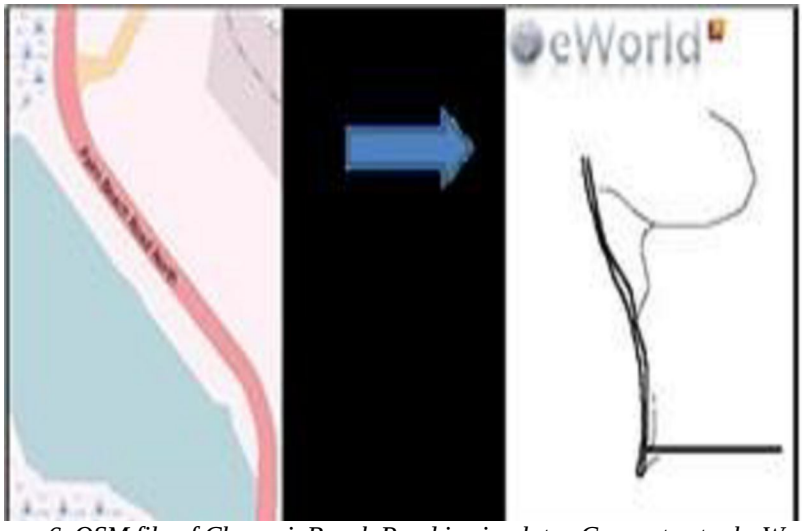

Figure 6. OSM file of Chennai, Beach Road in simulator Connector tool eWorld

- *Using the www.OpenSteetMap.com website for [13] extracting map data. Enter the location and select the needed road surface where you need to do the simulation. Once the selection of road map is done we select the OpenStreetMap XML data, so that we can get the OSM file and save it.*

- *The OSM file will be given as the input to eWorld which is an open source project that provides the methodology to convert map data from the OSM file to format that can be used for road traffic simulator including SUMO. The output of road network given by the eWorld has to be given as the input to SUMO, should be an XML format.*
- *The network and route XML files are generated by eWorld, this XML files are provide to MOVE, MOVE is a GUI based tools that help for integrating SUMO and ns2 for generating realistic scenario. Basically it converts SUMO mobility XML files to .tcl extension files use in ns2. Mobility traces are generated for ns2 from the net and rou XML files.*
- *Once we get the .tcl file, henceforth we do the network simulation process. For Network Simulation we are using ns2.34 version tool which support 802.11p.*

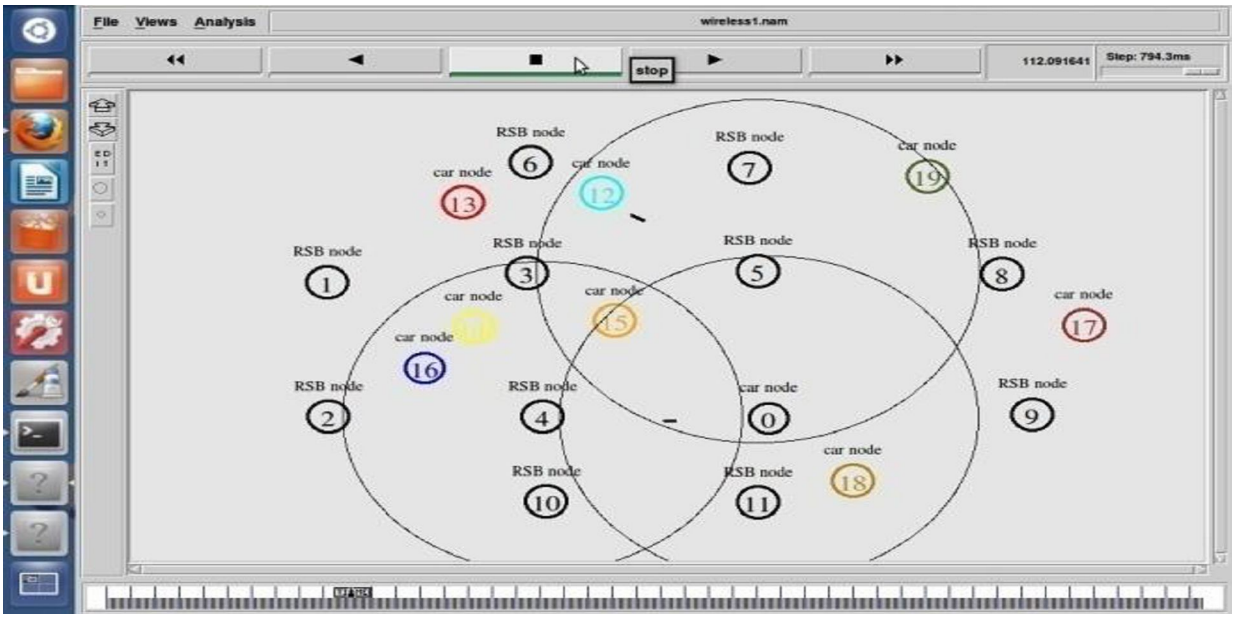

Figure 7. Network Set-up in Ns2.34

VI. PERFORMANCE EVALUATION

After simulating the paths required, compare the scheme with existing scheme that has been deployed already

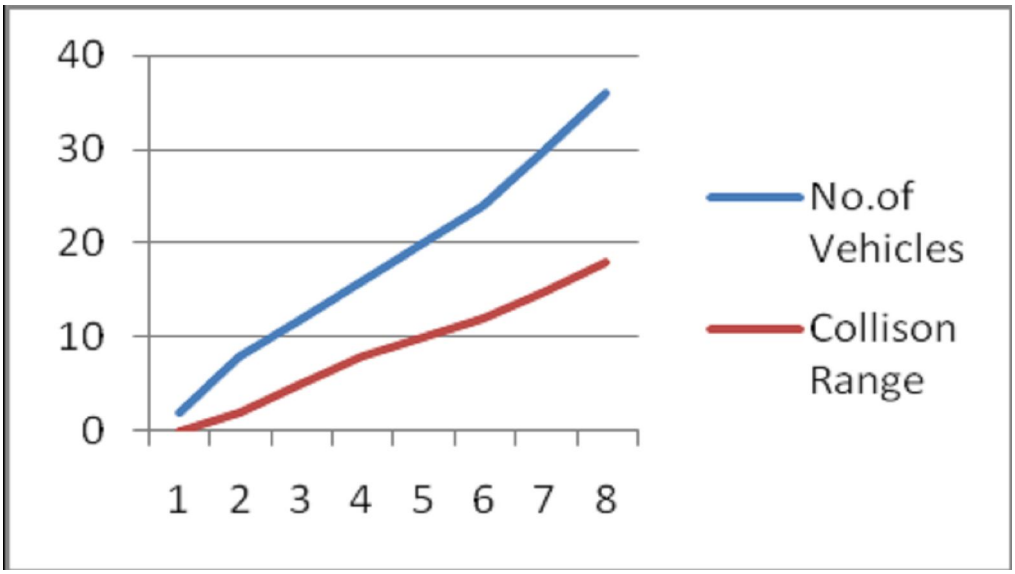

Figure 8. Collison Range for Vehicles

From the figure 8, the collision range is considerably less according to the vehicles accumulated in the signal. The x-axis is the range of collision and the y-axis is the number of vehicles accumulated at the signal, to turn the signal to green. As per the number of vehicles, our collision standards would be deployed.

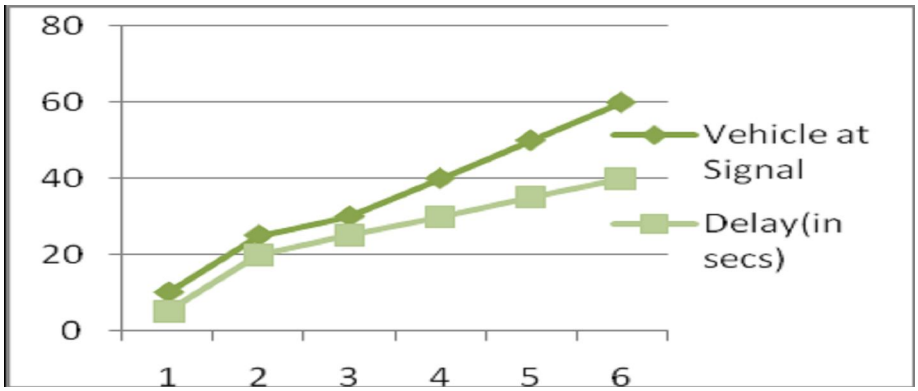

Figure 9. Delay at Signals

VII. CONCLUSION

In this paper, we proposed the design for vehicle to communicate with one another called vehicle-to vehicle communication and vehicle to communicate with the infrastructure, to address these core issues of safety. We believe that accidents can be diminished and endured altogether utilizing V2V technology. Since installation of wireless environment at every cross point would be costly. A V2V-based methodology appears to be more reasonable for implementing. We have depicted V2V-based conventions to be specifically for collision avoidance using OAF algorithm and detect drunk & drive. We stretched out VANET test system to backing these conventions. Despite the fact that our conventions are intended for independent vehicles that utilization V2V correspondence for co-agent driving additionally they might be adjusted to a driver-caution framework for manual vehicles at roadways.

REFERENCES

[1] Andreas Pfitzmann and MaritKohntopp "Anonymity, unobservability, and pseudonymity"proposal for terminology. in Workshop on Design Issues in Anonymity and Unobservability, pages 1–9, 2000
[2] Beresford and Stajano .F, "Mix zones: User privacy in location-aware services," in Proc. 2nd IEEE Annual Conference Pervasive Computing Communication Workshops, March 2004, pp. 127–131.
[3] Buttyan .L, Holczer .H, and Vajda .I, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in Proc. ESAS, 2007, Volume 4572, pp. 129–141.
[4] Freudiger .J, Raya .M, and Feleghhazi .M, "Mix zones for location privacy in vehicular networks," presented at the Workshop on Wireless Networking for Intelligent Transportation System, Vancouver, BC, Canada, Aug. 2007, LCA-CONF-2007-016.
[5] Sam Mathews M, Bevish Jinila Y, " An Effective Strategy for Pseudonym Generation And Changing Scheme with Privacy Preservation for Vehicular Communication" in IEEE Proc.,Conference on Electronics and Communication System, Coimbatore, India.,2014 ISBN978-1-4799-2321-2, Sept.2014
[6] Cheng S.-M., Lai W.-R., Lin P., and Chen K.-C., "Key management for UMTS MBMS," IEEE Transaction Wireless Communication, vol. 7, no. 9, pp. 3619–3628, Sep. 2008.
[7] Calandriello .G, Papadimitratos .P, Hubaux .P, and Lioy .A, "Efficient and robust pseudonymous authentication in VANET," in Proc. VANET, Montreal, QC, Canada, September 2007, pp. 19–28.
[8] M. Gerlach, "Assessing and improving privacy in VANETs," in Proc. 4thWorkshop ESCAR, Nov. 2006, pp. 1–9.
[9] Boneh .D and Boyen .X, "Short signatures without random oracles and the SDH assumption in bilinear groups," J. Cryptology, Volume. 21, no. 2, pp. 149–177, February 2008
[10] Usha Devi Gandhi, Arun Singh, Arnab Mukherjee and Atul Chandak," Smart Vehicle Connectivity for Safety Applications" in International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, India, Feb 6-8 2014
[11] Yang, X., Liu, 1.Zhao, F., & Vaidya, N (2004), Vehicle to-Vehicle Communication Protocol for Cooperative Collision Warning.
[12] Y. Bevish Jinila, K. Komathy, " A Safer Scheme to Secure VANETs from Sybil Attacks", International Journal of Network and Mobile Technologies, Vol. 2, No. 1, Jan – June 2011.
[13] Saurabh D. Patil et al., " DEMO: Simulation of Realistic Mobility Model and Implementation of 802.11p (DSRC) for Vehicular Networks (VANET)," International Journal of Computer Applications (0975 – 8887) Volume 43– No.21, April 2012
[14] Y. Bevish Jinila, K. Komathy," Location Privacy in Vehicular Networks for Safety Message Communication based on t-closeness Model.