SECURE COMMUNICATION IN MULTI-LANE ENVIRONMENT IN VANETS

Jagpreet Kaur (Assistant professor)
Lovely Professional University
Phagwara-Punjab
jagpreetkaur5@gmail.com

Priyanka Mittal
Lovely Professional University
Phagwara-Punjab
priyankalpu.mittal@gmail.com

Abstract: **VANETs, plays an important role in public safety communications. The fascination of mobility, accessibility and flexibility makes wireless technologies the dominant method of transferring all sorts of information. It serves a wide range of applications under different topologies. In this research, we will present a wireless technology with the help of which vehicles can communicate with each other. that is expected to be adopted by both governments and manufacturers in the very near future. It directly affects car accidents. It is the technology of building a robust network between mobile vehicles. This promising technology is literally called Vehicular Ad-Hoc Networks (VANETs).**

Keyword: ***VANET, OBU, RSU, MANET, NS2, SUMO, MOVE***

1. Introduction:

VANET is the technology of building an Ad-Hoc network between mobile vehicle-to-vehicle and between mobile vehicles and roadside units. There are two types of nodes in VANETs; mobile nodes as On Board Units (OBUs) and static nodes as Road Side Units (RSUs). An OBU resembles the mobile network module and a central processing unit for on-board sensors and warning devices. The RSUs can be mounted in centralized locations such as intersections, parking lots or gas stations. They can play a significant role in many applications such as a gate to the Internet.

This concept of network vehicle was first proposed by a team of engineers from Delphi Delco Electronics Systems and IBM Corporation in the year 1998. Vehicles are made little intelligent by loading them with sensors which are controlled by a telematics box inside the car. This box communicates with the driver and guides him. Nodes in VANETs are mobile as in MANETs but the mobility is not random as they are restricted to the boundaries of the road. Moreover node mobility and topology changes are quite high in VANETs.

VANET is a special class of mobile ad-hoc network (MANET). It is the first commercial instantiation of MANET. It is a self organized network that enables communications between vehicles and RSUs. The RSU`s are connected to a network backbone, so that applications and services of network also including internet access can be provided to vehicles.

Vehicle manufacturers are competing in equipping their vehicles with devices that collect data from the interior and exterior of vehicles and deliver it to a central processing unit that can analyze this data to boost the road safety while increasing the on-board luxury. Global positioning systems (GPS), Event Data Record (EDR) resembling the Black-Box used in avionics, small range radars, night vision, light sensors, rain sensors and navigation systems are well-known intelligent devices used in many newly produced vehicles, what is rather referred to as "Computers-on-Wheels". Communication researchers have been recently working on a prominent step; if each vehicle has a device that can communicate with other vehicles; vehicles will have a gigantic new source of information that extends beyond the capabilities of all previously mentioned devices. For example, all of these devices cannot warn the driver of a stopping vehicle in the next turn and of course cannot let travellers enjoy video chatting and file sharing at no charge.

This technology is not limited to following motivations:

1. Increase traveller safety
2. Enhance traveller mobility
3. Decrease travelling time
4. Conserve energy and protect the environment
5. Magnify transportation system efficiency
6. Boost on-board luxury

1.1 Properties of VANETs:

There are number of properties of VANET and these properties are used to express the problem statement. The properties are as follows:

a) **System assumptions**

System must be future compatible. To make the system future-compatible there are following assumptions which are based mainly on specifications of future products.

b) **Network model**

In VANET the communication nodes are vehicles or base stations. Vehicles can be of two types i.e. either private (belong to individual like cars etc) or public (like buses etc). Base stations can be service providers and also belong to government. The communication channels are supported by technology of IEEE 802.11. The mobile nodes which are vehicles or base stations will characterize by mobility, high speed and short time connections between the neighbours.

1.2 Attacks on vehicular networks:

There are number of security attacks which are faced by vehicular ad-hoc networks. It is not possible to enlist all possible attacks which will be mounted in future on vehicular ad-hoc networks.

1.2.1 There is a general classification of attacks and also describing the attacker.

1. Network attack: the main components of VANET are vehicular nodes and its infrastructure. These attacks have high priority because these attacks affect this network. The main objective of these attacks is to create problem for legitimate users of network. J.T. Isaac et.al mentioned number of attack in which comes under network attacks listed as network malicious vehicle, Brute force attack, misbehaving, faulty nodes.

2. Application attack: Safety and non-safety are two types of potential vehicular applications. This is used to change content of these applications and use it for their own benefits. The attackers change the content of actual message and send wrong or fake messages to other vehicle which causes accident. These wrong, messages directly affect the behaviour of user on the road. Warning message is important that is use in safety applications. This will create serious condition on the road if attackers change warning messages; many accidents are occurred on the road.

Non-safety application is related to users comfort while driving. The role of non-safety applications is to comfort the passengers and to improve the traffic system. Car parking is the major non-safety application. Roadside unit provides information about the availability of parking in shopping mall and sport complex.

3. Timing attack: This is the new type of attack in which attacker's main objective is to add some time slot in original message and create delay in original message. Attackers always create delay in original message rather than to disturb the content and these messages are received after it requires time. Safety application is time critical applications and non-safety is real time applications, if delayed occurred in these applications then main objective of the application are finished.

4. Social attacks: Purpose of these kinds of messages is to indirectly create problem in the network. Legitimate users show angry behaviour when they receive such kind of messages "Hello Idiot". When driver receives this message, directly affects his driving behaviour by increasing the speed of vehicle. This entire thing is indirectly disturb the other user in the network.

5. Monitoring attack: Monitoring and tracking of the vehicles attacks are lying in this attack. The attacker only monitors the whole network to listen the communication between V2V and V2I. If they find any related information then pass this information to concern person. For example police are planning to perform some operation against criminal and they communicate each other and guide about the exits location of the operation. Attacker only listen the whole communication and informed the criminal about the police operation.

2. Purposed problem/work:

In VANETS, the secure communication between vehicles depends upon the message broadcasting. This message broadcasting depends upon the message priority. The message with high priority broadcast first and the message with low priority broadcast later. In this way the secure communication takes place between the vehicles. In this, implementation of secure communication in multi-lane takes place. There are number of possibilities of the proposed work and that are explained below:

a) The proposed work is to secure the communication in multi-lane i.e. where vehicles move in two different directions. The previous work is related to single-lane i.e. vehicles move in only one direction.

b) There is a secure MAC protocol for dedicated short range communication (DSRC) applications in VANETs, with different message priorities for different types of applications to access DSRC and with this protocol we can increase the security of multi-lane communication.

c) The secure communication protocol for multi-lane is designed to guarantee:

i. The freshness of the message
ii. Message authentication and integrity
iii. Message non-repudiation
iv. Privacy and anonymity of the sender
v.Guarantee the reliability and latency requirements of safety related DSRC applications for VANET

The main importance of the proposed work is to implement the secure communication in multi-lane environment. In which vehicles are moving in two different directions and the messages are broadcast to all the vehicles. The main idea is that how the vehicles come to know that the message is for the vehicles which are moving in particular direction.

3. Objectives

My area of research will concentrate on the issues related with secure and efficient communication of vehicular Ad-hoc Networks & to propose an efficient solution for the secure communication in multi-lane network i.e. where vehicles move in different directions. The previous work provides secure communication in single-lane environment.

a) Objective is to create a method or way through which the accuracy can be maintain

b) Results should be good i.e reduce the number of accidents

c) Fast access of information transformation between vehicles

The main objective is to minimize the number of accidents in multi-lane environment. There are number of ways with the help of which the reduction in number of accidents takes place like sending alert messages, emergency messages etc. there is another ways that is maintain the minimum distance between the vehicles. When the condition of maintain the minimum distance between vehicles is break down then these accidents occur.

The secure communication in multi-lane means to reduce the number of accidents this can be implemented by introducing a MAC protocol and by sending critical information to other vehicles which are in the particular range. This critical information must be sent with high priority, reliability and efficiency. The message with the high priority is broadcast first and then other messages send according to their priorities. With this technique or method the number of accidents can be reduced.

4. Methodology

Implementation of method for secure communication in multi-lane environment is possible with the help of the method used in secure communication in single-lane environment.

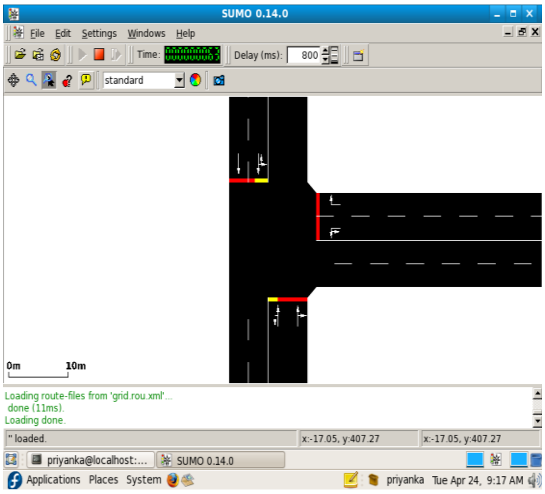
4. 1 Formulation of hypothesis:

The hypothesis behind the implementation of secure communication in multi-lane environment is that the existing techniques are better for single-lane communication where the vehicles move in single direction and now try to implement new method for secure communication in multi-lane environment. The previous techniques reduce the accidents by exchange warning messages to warn other vehicles about the hazards when it happens. When any danger is detected an emergency message need to be transmitted for a particular range, so that other vehicles aware of the danger before reaching it. This information must be sent with maximum probability, reliability and efficiency.

5. The results are discussed below in detail.

1. First of all, try to implement the basic scenario. In the basic scenario there is a road map which consists of the required lane. Lane is necessary for the moving vehicles. The implemented scenario is shown below in the figure 5.1. In this

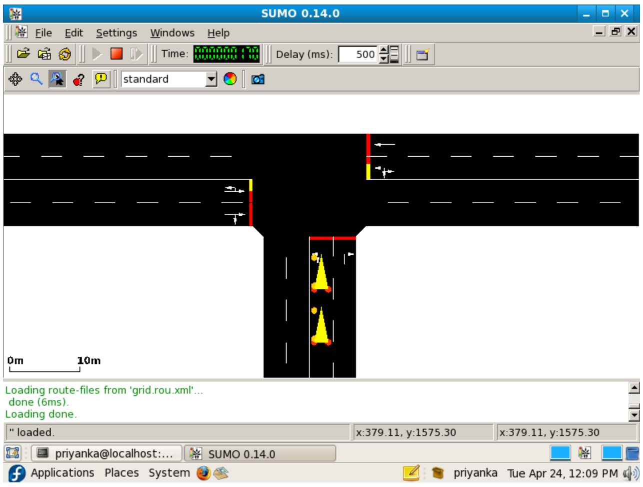
scenario there are three lane environments which are using algorithm implemented.



```
Loading route-files from 'grid.rou.xml'...
 done (11ms).
Loading done.
" loaded.
```

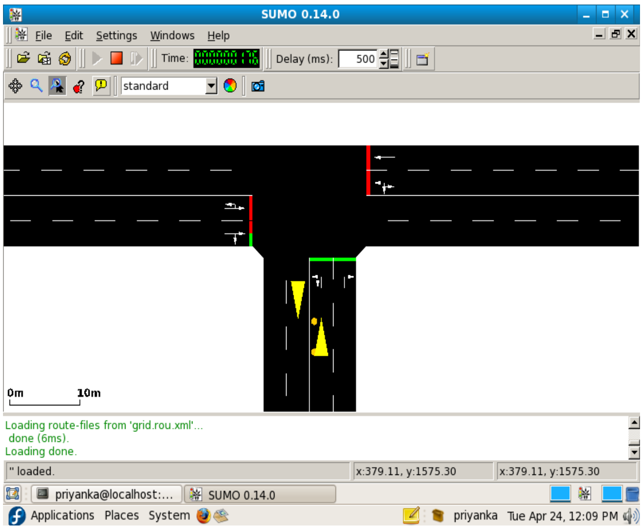
Figure 5.1: result 1

2. Next step is to implement the moving vehicles in the scenario. There may be any number of moving vehicles. These are shown in the following fig 5.2. In this scenario moving vehicles are shown.



```
Loading route-files from 'grid.rou.xml'...
 done (6ms).
Loading done.
" loaded.
```

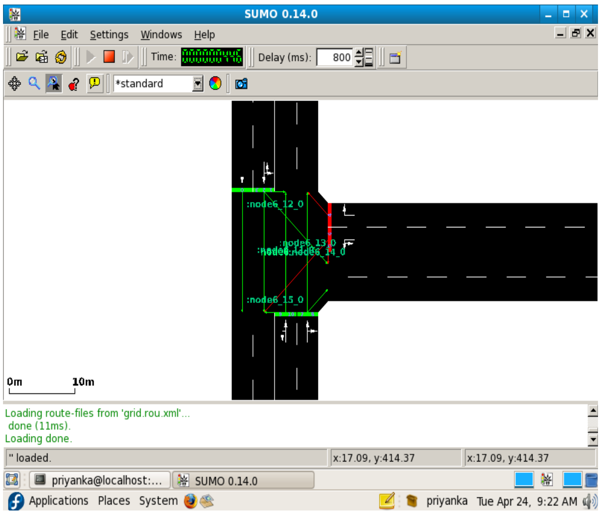
Fig 5.2: result 2



```
Loading route-files from 'grid.rou.xml'...
 done (6ms).
Loading done.
" loaded.
```

Figure 5.3: result 3

3. In next step there is a graphical representation which is shown in the figure 5.4. This scenario represents that when moving vehicles start to move and when they stop. With this approach, we can easily maintain the minimum distance between the vehicles. There are three scenarios with the help of which we can identify that with green light vehicles can move (shown in figure 5.5) but with red light vehicles have to stop their movement to reduce the number of accidents (shown in figure 5.6).

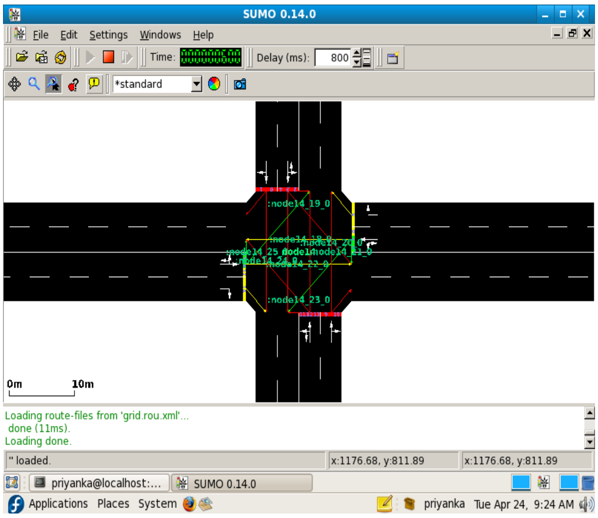


Loading route-files from 'grid.rou.xml'...
done (11ms).
Loading done.

" loaded. x:17.09, y:414.37 x:17.09, y:414.37

priyanka@localhost:... SUMO 0.14.0

Figure 5.4: result 4

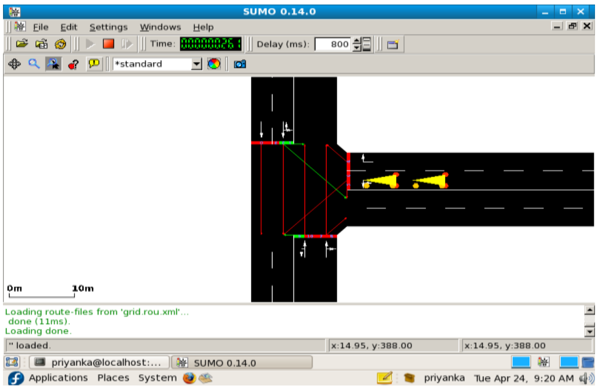


Loading route-files from 'grid.rou.xml'...
done (11ms).
Loading done.

" loaded. x:1176.68, y:811.89 x:1176.68, y:811.89

priyanka@localhost:... SUMO 0.14.0

Figure 5.5: result 5


SUMO 0.14.0
File Edit Settings Windows Help
Time:
Delay (ms): 800
*standard
0m 10m
Applications Places System
priyanka Tue Apr 24, 9:20 AM

Loading route-files from 'grid.rou.xml'...
done (11ms).
Loading done.

" loaded. x:14.95, y:388.00 x:14.95, y:388.00

priyanka@localhost:... SUMO 0.14.0

Figure 5.6: result 6

4. Nam output

In figure 5.7 the VANET environment is shown in which wireless nodes become moving nodes to create the vehicular adhoc network and take the moving nodes as moving vehicles.

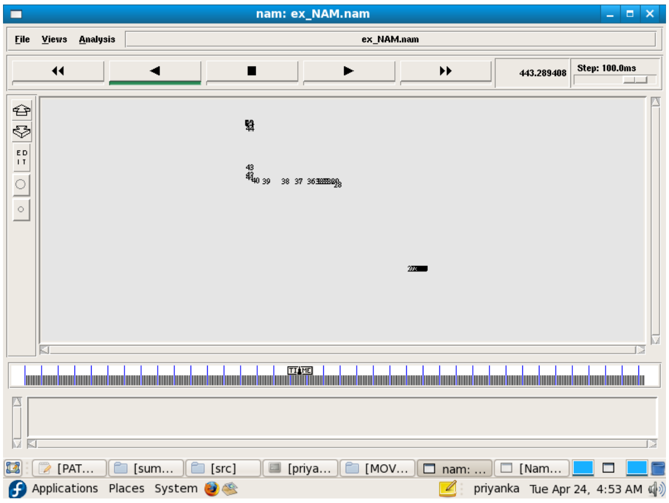

nam: ex_NAM.nam
File Views Analysis
ex_NAM.nam
443.289408
Step: 100.0ms
[PAT... [sum... [src] [priya... [MOV... nam: ... [Nam...
Applications Places System
priyanka Tue Apr 24, 4:53 AM

Figure 5.6: NAM output for High Density Environment

6. Conclusion and future work:

In this thesis we consider VANET based technology with the help of which moving vehicles can communicate. Vehicular adhoc network is a wireless communication technology for improving highway safety and information services. Special environments and applications cause that VANET cannot use the exiting protocols well. In this paper we utilize the exiting traffic infrastructures to improve the network effectively. Using NS2, SUMO, MOVE simulators implement the required scenario and find the results. Every technique has its own pros and cons. By analyzing the simulation results of different techniques, we presented an open research for secure communication in VANET. We can increases the performance of communication but it depends upon the technique to be used. With this technique we can reduce the delay in message sending which will help to reduce the number of accidents and also help to maintain the minimum distance between the vehicles.

In future work, use any particular algorithm and try to implement the environment in which vehicles can maintain the minimum distance from the lane side.

7. References:

[1] Aneel Rahim,Zeeshan Shafi Khan, Fahad T.Bin Muhaya,Muhammad Sher and Tai-Hoon Kim(2010) “*sensor based framework for secure multimedia communication in VANET*”, pp.10147-10154

[2] Abebneh N, Labiod H, Boukhetam N, (2010) “*Evaluation of routing protocols for VANETs in urban environments*”, IEEE, pp. 1-5.

[3] Baber Aslam and Cliff C. Zou (2011) *“One-way-linkable Blind Signature Security architecture for VANET*”, IEEE, pp.745-750

[4] Christian Lochert, Hannes Hartenstein, Jing Tian, Dagmar Hermann et al., (2009), **“***the routing strategy for vehicular ad-hoc networks in city environments*”, IEEE, pp. 1-6

[5] F. Karnadi, Z. Mo, K.-C. Lan (2010), “*Rapid Generation of Realistic Mobility Models for VANET*”, IEEE, pp. 20-45

[6] Fiore M, Harri J, Filali F, Bonnet C, “*Vehicular Mobility Simulation for VANETs Simulation*”, 2010, pp. 301 - 309

[7] G.Samara, W.A.H.A Alsalihy and S.Ramadass(2011) “*increase emergency message reception in VANET*”, journal of applied sciences 11(14), pp.2606-2612

[8] Hu Xiong,Zhiguang Qin and Fagen li(2010) “*secure vehicle-to-roadside communication protocol using certificate-based cryptosystem*”, vol.27,issue 3,pp.214-219

[9] Hao Jiang, Siyue Chen, Yang Yang, Zhizhong Jie, Henry Leung, Jun Xu, Lin Wang(2010) “*Estimation of packet loss rate at wireless link of VANET-RPLE”,* IEEE,pp.1-5

[10] Hind AI Falasi, Ezedin Barka(2011), “*Revocation in V ANETs: A Survey”*, IEEE, pp.214-216

[11] Josiane Nzouonta, Neeraj Rajgure, Guiling (Grace) Wang, Member, IEEE, and Cristian Borcea, Member, IEEE(2009) “*VANET Routing on City Roads Using Real-Time Vehicular Traffic Information”,* pp.3609-3626. 50

[12] K.Prasanth, Dr. K. Duraiswamy, K. Jayasudha and Dr. C. Chandrasekar (2010), "*Efficient Packet Forwarding Approach in Vehicular Ad Hoc Networks Using EBGR Algorithm*", IEEE, pp. 37-46

[13] Mostafa M. I. Taha(2008) "*Broadcasting Protocols in Vehicular Ad-Hoc Networks (VANETs)*", pp.1-96

[14] Paul Bijan, Ibrahim Md, Abu Naser Bikas Md, (2011) "*VANET Routing Protocols: Pros and Cons",* International Journal of Computer Applications, pp. 28-34

[15] Robert Lasowski, Constantin Scheuermann, Florian Gschwandtner and Claudia Linnhoff-Popien (2011), *"Evaluation of Adjacent Channel Interference in Single Radio Vehicular Ad-Hoc Networks",* IEEE, pp. 241-245

[16] Singh K. Pranav, Lego Kapang, Tuithung Themrichon, (2011) *"Simulation based Analysis of Adhoc Routing Protocol in Urban and Highway Scenario of VANET",* International Journal of Computer Applications, pp. 42-49