PRIVACY PRESERVATION FOR NAVIGATION IN MULTIPLE ROADSIDE UNIT USING VANET

BY

R.KAVIPRIYA

(17PCS006)

Project Report Submitted

In Partial fulfillment of the requirements for the award of

Master's Degree in Computer Science

Department of Computer Science,

Avinashilingam Institute for Home Science and Higher Education for Women, (Deemed to be University),

Coimbatore - 641043

April – 2019

PRIVACY PRESERVATION FOR NAVIGATION IN MULTIPLE ROADSIDE UNIT USING VANET

BY

R.KAVIPRIYA

(17PCS006)

Project Report Submitted

In Partial fulfillment of the requirements for the award of

Master's Degree in Computer Science

Department of Computer Science

Avinashilingam Institute for Home Science and Higher Education for Women, (Deemed to be University)

Coimbatore - 641043

April-2019

Signature of the Head of the Department **Signature of the Supervisor**

Viva Voce Examination Held on _____

Signature of the Examiners

Acknowledgement

ACKNOWLEDGEMENT

I would like to express my sincere thanks to God Almighty, for his constant love and grace that he showered upon me.

I would like to express my deep sense of reverential gratitude and sincere thanks to **Padma Shri Dr. P. R. Krishnakumar, Chancellor,** Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for his support and encouragement during the course of my study.

I owe my great deal of gratitude to **Dr. (Mrs.) V. Premavathy Vijayan, Vice Chancellor**, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for extending all resources that facilitated the conduct of the present work.

I express my gratitude to **Dr. (Mrs.) S. Kowsalya, Registrar**, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for providing all facilities necessary for the work.

I also thankful to **Dr. (Mrs.) K. Udaya Chandrika, Dean, School of Physical Sciences and Computational Sciences,** Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, for granting the facility required.

I wish to place my deep sense of gratitude to **Dr. (Mrs.) V. Radha, Professor and Head, Department of Computer Science,** for providing all the facilities required to complete the project.

I heartily thank my esteemed project guide **Dr. (Mrs.) G.Geetha, Senior Technical Assistant, Department of Computer Science**, for imparting the tremendous assistance and well-timed support for triumph of my project.

I express my honorable thanks to my project coordinator **Dr. (Mrs.) G.Padmavathi**, **Professor, Department of Computer Science,** for her kind advice and knowledgeable suggestions which helped me to complete my project successfully.

Finally, I take pride to thank my parents and those who helped me directly or indirectly for carrying out this work.

Abstract

ABSTRACT

The project entitled as “Privacy preservation for navigation in multiple roadside unit using VANET”. Vehicular ad-hoc Network is the collection of vehicles and roadside infrastructure Units (RSUs).Vehicles are equipped with wireless communication devices which are called On-Board Units (OBUs).The wireless communication devices enables the vehicles to exchange traffic related information with each other and with RSUs. VANETs raise many security and privacy concerns at the same time. Malicious users can take advantage of VANET and disturb the whole system.

This new proposed system utilizes the online road information collected by a vehicular ad-hoc network to guide drivers to desired destinations in a real time and distributed manner. It has the advantage of using real time road conditions to compute a better route and at the same time, the information can be properly authenticated. To ensure the integrity of the messages, each message sent by a vehicle should be signed and verified when being received. Based on message batch verification, each vehicle receives traffic related message from other vehicles.

LIST OF ABBREVIATIONS

Abbreviation	Explanation
VANET	Vehicular Ad-hoc Network
MANET	Mobile Ad-hoc Network
OBU	On Board Unit
RSU	Roadside Unit
TA	Trusted Authority
GPS	Global Positioning System
ITS	Intelligent Transportation System
DSRC	Dedicated Short Range Communication
PKI	Public Key Infrastructure
RID	Real Identity
PWD	Password
HMAC	Hashed Message Authentication
IVC	Inter Vehicle Communication
NS	Network Simulator
NAM	Network Animator
OTcl	Object oriented Tool Command Language
DSDV	Destination Sequenced Distance Vector
DCP	Discovery and Configuration Protocol
LAR	Location Ad-hoc Routing

Contents

TABLE OF CONTENT

S.NO	PARTICULARS	PAGE NO
1.	**INTRODUCTION**	**1**
	1.1 VEHICULAR AD-HOC NETWORK	1
	1.1.1 COMMUNICATION TYPES	2
	1.1.2 CHARACTERISTICS OF VANET	3
	1.1.3 GOALS OF VANET	3
	1.1.4 APPLICATIONS OF VANET	4
	1.2 PROBLEM DEFINITION	4
	1.3 OVERVIEW OF THE PROJECT	5
2.	**LITERATURE REVIEW**	**6**
3.	**SYSTEM SPECIFICATION**	**14**
	3.1 HARDWARE SPECIFICATION	14
	3.2 SOFTWARE SPECIFICATION	14
	3.3 ABOUT THE SOFTWARE	15
	3.3.1 NETWORK SIMULATOR-2	15
	3.3.2 STRUCTURE OF NS2	16
	3.3.3 FACILITIES IN NS2	17
	3.3.4 FUNCTIONS OF NS2	17
	3.3.5 NAM	17
	3.3.6 XGRAPH	19
4.	**METHODOLOGY**	**20**
	4.1 MODULE DESCRIPTION	20
	4.1.1 VEHICLE TOPOLOGY CREATION	20
	4.1.2 VERIFICATION OF VEHICLE AND RSU	21
	4.1.3 BATCH MESSAGE SIGNING AND SIGNATURE VERIFICATION	22

4.1.4 PRIORITY AND NEGATIVE VEHICLE SIGNATURE IDENTIFICATION 22

5. EXPERIMENTAL RESULTS AND DISCUSSION 23

5.1 PACKET DELIVERY RATIO 23

5.2 THROUGHPUT 24

5.3 AVERAGE DELAY 25

6. CONCLUSION **26**

7. SCOPE FOR FUTURE ENHANCEMENT **27**

8. BIBLIOGRAPHY **28**

9. APPENDIX **29**

9.1 SYSTEM FLOW DIAGRAM 29

9.2 ACTIVITY DIAGRAM 30

9.3 SCREEN SHOTS 31

Introduction

1. INTRODUCTION

1.1 VEHICULAR AD-HOC NETWORKS

VANET is a widely discussed area of wireless communication at present. VANET is a subset of MANET where nodes represent vehicles moving at high pace and vehicle traffic determined regularity. This technology enables communication between vehicles and nearby road-side infrastructure and is made possible through a wireless sensing device installed in the vehicles. With the inception of VANET, new opportunities and related technologies like applications for traffic jam, accident control and weather updates have appeared. VANET performance can be tested in real situations but factors like cost, inaccurate results and protocol evaluation of complex environment may contribute towards a disappointing end. An automated tool called simulation can imitate the protocol and yield a similar result to that of the real world. VANET differs from MANET because in VANET the nodes strictly follow the traffic rules and their pattern of movement is very complex. To attain good results from VANET simulation, it is important to generate a realistic mobility model that is as realistic as real ad-hoc network communication.

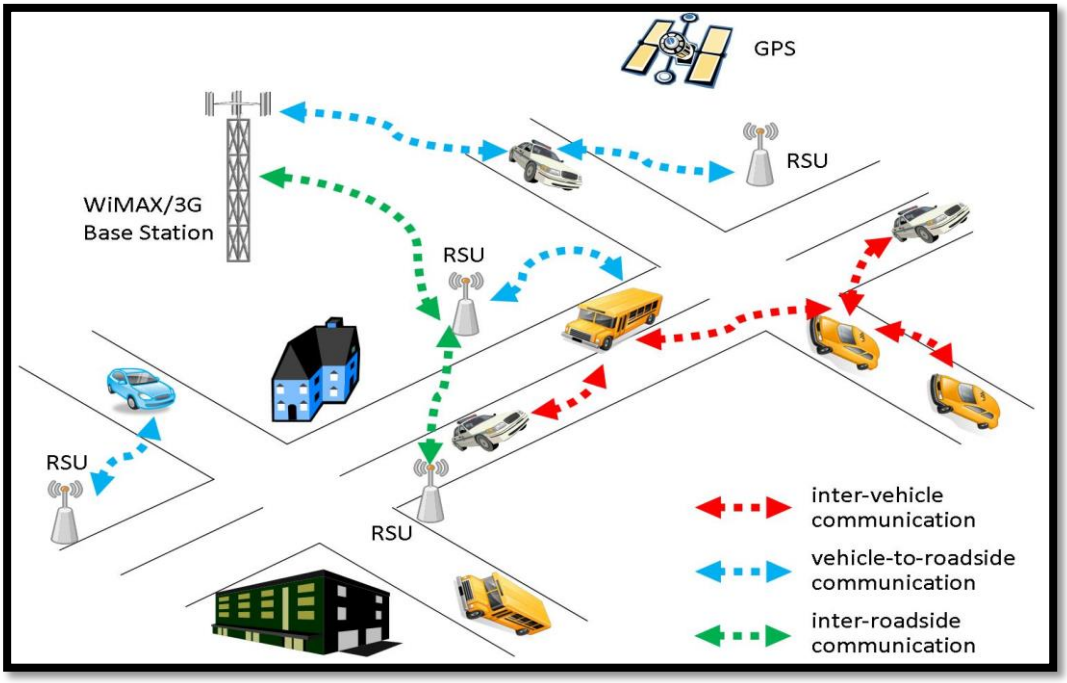

Figure 1.1: Structure of VANET

1.1.1 COMMUNICATION TYPES

The Communication types are Vehicle to Vehicle (V2V), Vehicle to Roadside (V2R) and Vehicle to Infrastructure (V2V)

- Vehicle to Vehicle (V2V) - It is suitable for short range Vehicular network. It provides real time safety, fast and reliable. It does not need any roadside infrastructure. In V2V warning messages are broadcasted from vehicle to vehicle.
- Vehicle to Roadside (V2R) - It provides communication between vehicles and the roadside units. It makes use of pre-existing network infrastructure such as wireless access points. In V2R warning messages are send to roadside units and then from that roadside units warning messages are send to vehicles.
- Vehicle to Infrastructure (V2I) - This communication provides longer – range vehicular networks.

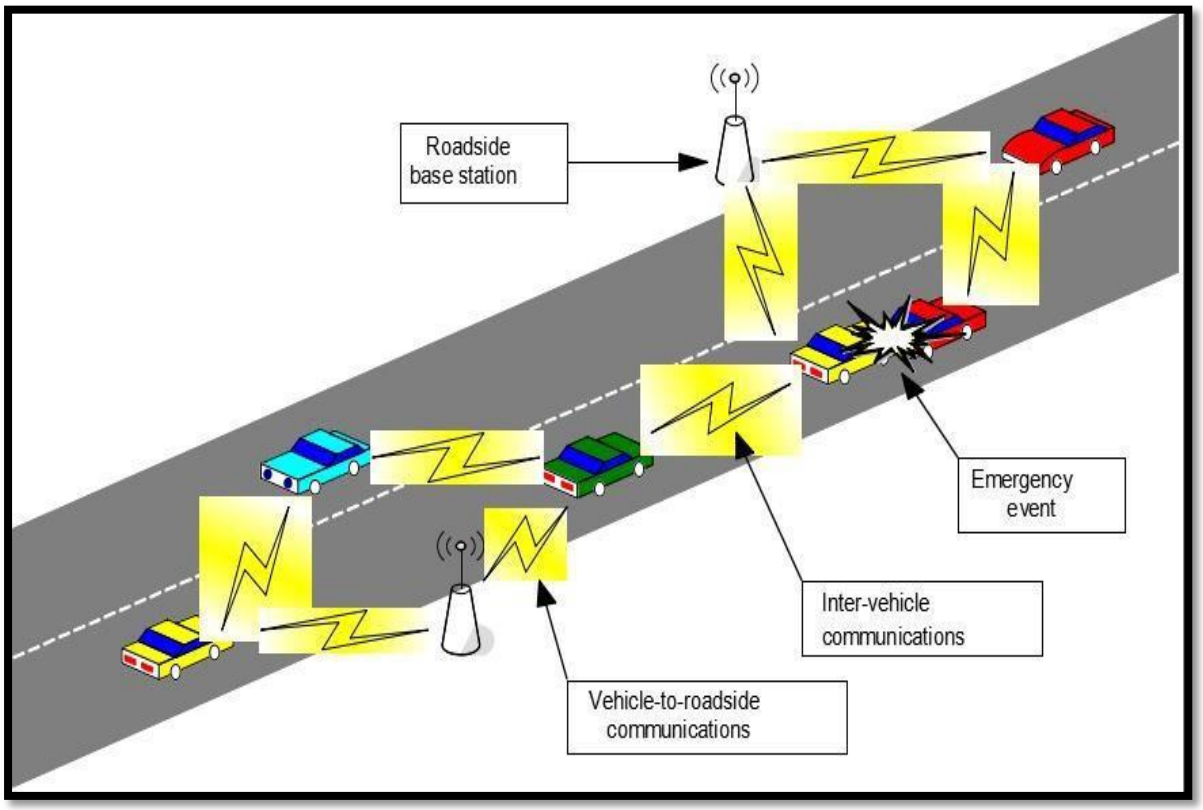

Figure 1.1.1: Communication in VANET

1.1.2 CHARACTERISTICS OF VANET

VANET is application of MANET but it has its own distinct characteristics which can be summarized as

- **High Mobility** - The nodes in VANETs usually are moving a high speed. This makes harder to predict a node's position and making protection of node privacy.
- **Rapidly changing network topology** - Due to high speed mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.
- **Unbounded network size** - VANET can be implemented for one city, several cities or for countries. This means that network size in VANETs is geographically unbounded.
- **Frequent exchange of information** - The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.
- **Wireless Communication** - VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measures must be considered in communication.

1.1.3 GOALS OF VANET

- Improve traffic safety and comfort of driving
- Minimize the accidents, Traffic intensity, locating vehicles
- Up-to-date traffic information
- Intersection collision warning
- Local danger warning
- Weather Information

1.1.4 APPLICATIONS OF VANET

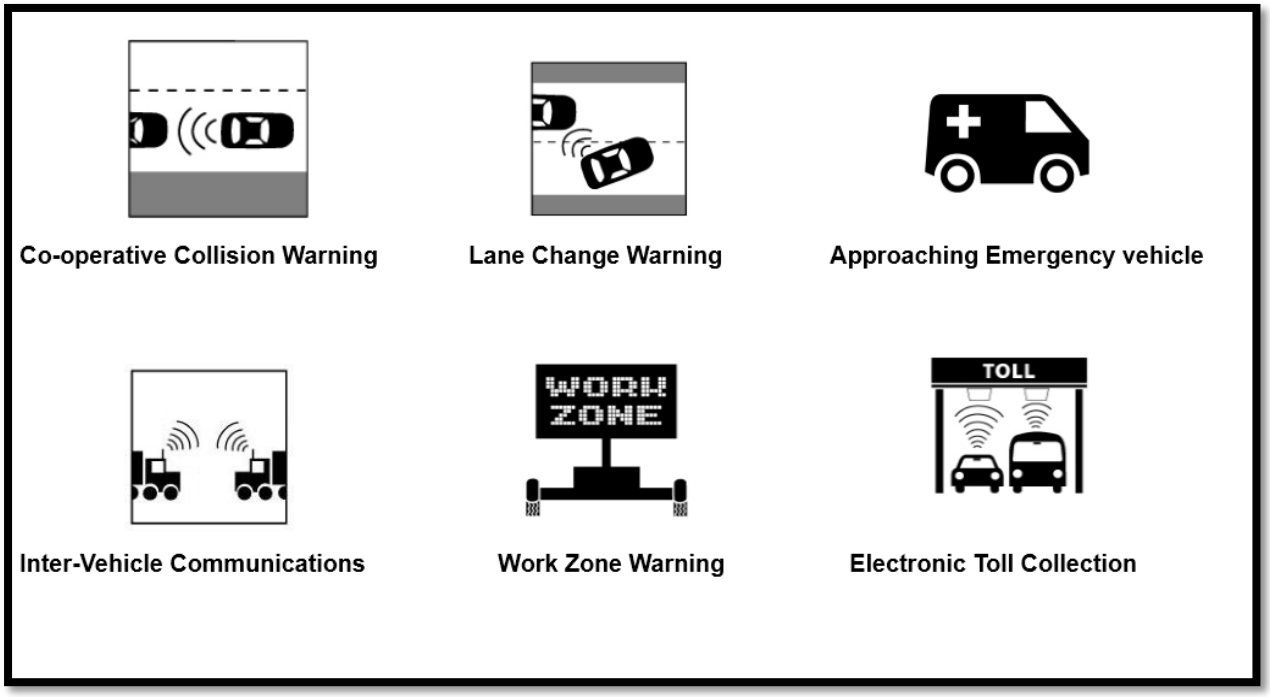

Figure 1.1.4: Applications of VANET

1.2 PROBLEM DEFINITION

In VANET vehicles requires continuous knowledge about the location of vehicles, routes and track including real-time traffic monitoring. Vehicle's On Board Unit (OBU) enable to exchange traffic related information among RSUs and neighbors vehicle with high mobility. In unavoidable circumstance road blocking condition suddenly appears which makes RSU (covering the destination) to immediately sends an urgent notification message to the target vehicle so that another route request can be made with Trusted Authority (TA). To ensure the integrity of the messages, each message sent by a vehicle should be signed and verified when being received. Message batch verification system presented in TA detects the Invalid Signature problem to find if any attacker has used the invalid identities when sending each message from tracing its real identity.

1.3 OVERVIEW OF THE PROJECT

In the earlier methods pseudo identity for authentication between two parties didn’t achieve the satisfactory result between Trusted Authority and vehicle. Vehicles OBU enable to exchange traffic related information with each other RSUs and neighboring vehicles. Vehicles finding a route to a desired destination assume that a road blocking condition suddenly appears and as a result, the returned route can no longer be used. At that moment, the RSU covering the destination immediately sends an urgent notification message to the vehicle so that another route request can be made.

Literature Review

2. LITERATURE REVIEW

2.1 VEHICULAR POSITION VERIFICATION

Tim Leinmuller et al.,2006 suggested that Inter-vehicle communication is regarded as one of the major applications of Mobile Ad- hoc Networks (MANETs). Compared to MANETs, Vehicular ad hoc networks (VANETs) have special requirements in terms of node mobility and position-dependent applications, which are well met by geographic routing protocols. Functional research on geographic routing has already reached a considerable level, whereas security aspects have been vastly neglected so far. Since position dissemination is crucial for geographic routing, forged position information has severe impact regarding both performance and security. The detection mechanisms that is capable of recognizing nodes cheating about their location in position beacons. Position verification system successfully discloses nodes disseminating false positions and thereby widely prevents attacks using position cheating.

2.1.1 EFFECTS OF FALSIFIED POSITION INFORMATION

The influence of false position data are generated by malfunctioning or malicious nodes on geographic routing. An example scenario where node A claims to be at two additional (faked) positions Avl and Avr. Based on a greedy forwarding strategy, nodes always select the node nearest to the destination as the next forwarding node. Assuming that F wants to send a packet to node K, it will first send the packet to its only direct neighbor G. G will then forward the packet to the node nearest to the destination from which it received beacons.

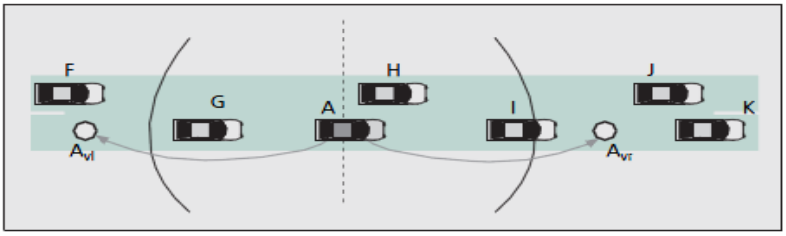

Figure 2.1.1: Position Verification

Whenever a malicious node is about to send a beacon message to announce its present position, it selects a random position on the field and applies it to the beacon (instead of its real position). Whenever a malicious node gets a data packet, depending on the simulation setup, it either forwards it correctly or it drops the packet. The influence of falsified position information on the overall number of successfully delivered messages has been measured with different percentages of position faking nodes.

2.1.2 POSITION VERIFICATION APPROACH

The concept of "Position Cheating Detection System" is similar to intrusion detection systems to detect, for example, selfish nodes in MANETs. In these systems each node uses multiple sensors to detect malicious or selfish behavior of nodes in the network. Based on the sensors' observations, each node calculates a trust value that determines whether nodes are trustworthy. Such a system can predict the trustworthiness of other nodes even when single sensors do not work reliably to hundred percent. Transferring this idea to the domain of position verification is only necessary to find suitable sensors that can be used to detect cheated position information. Basically, there are two classes of position verification sensors. Sensors of the first kind work autonomously on each node and contribute their results to the overall trust ratings of neighbors. The second class includes sensors that only work in cooperation with other nodes surrounding the neighbor node. All sensors suggested to have the benefit that they only rely on information that the routing layer delivers anyway, so there is no extra hardware involved.

2.2 SMART CARS ON TRANSPORTATION SYSTEMS

F. Wang, et al, 2006 suggested that Transportation systems play a critical role in virtually all facets of modern life. However, significant challenges remain in further improving their efficiency and safety and in developing related value-added applications. Opportunities to meet these challenges emerge continuously, largely owing to fast-paced developments in a broad spectrum of related engineering, communications, and information technology fields, including pervasive computing.

2.2.1 INTELLIGENT VEHICLES AND ROADS

The current generation of vehicles is already equipped with many different kinds of sensors, CPUs, software systems, and communication capacities. In the next few years, active in- and out vehicle environment sensing will become standard, enabling intelligent driver and passenger assistance and increasing driving safety, efficiency, and comfort. Eventually, road infrastructures will also significantly change to provide better sensing solutions but this will take more time. Several technologies already exist that can give vehicles additional information for safer operations and better performance. Examples include remotely controllable, locally activated, variable-message systems, RFID-type roadside sensors and embedded barcode-like road marks. Some of these developments are straightforward applications of existing pervasive computing frameworks, whereas others pose significant technical challenges and call for innovative solutions.

2.2.2 TRAVELING IN INTELLIGENT SPACES

Intelligent spaces are environments that can continuously monitor what's happening in them, communicate with their inhabitants and neighborhoods, make related decisions, and act on these decisions. Embedding such intelligence in an automobile would be a natural next step for intelligent vehicles. Current in-vehicle applications of GPS, ad hoc networks, and sensor networks have already led the way. Future cars will behave more like intelligent agents traveling in intelligent spaces. For example, traffic control at intersections could employ cooperative driving technologies implemented over ad hoc networks, instead of relying on traffic lights. Researchers working on such technologies aim for roads with zero fatalities.

2.2.3 AGENT-BASED CONTROL

As connectivity becomes ubiquitous, agent-based control offers an ideal approach to transportation management, addressing its geographically distributed and alternately busy-idle operating characteristics. Intelligent, autonomous agents will traverse traffic control centers, road intersections, highways, streets, vehicles, houses, offices. They will use the Internet as well as wireless and ad hoc networks to collect the right information at the right times and to make smart decisions. Agent-based control essentially transforms centralized

operational algorithms into distributed operational agents, letting networked transportation systems operate on a management-on-demand or service- on-demand basis.

2.3 LOCATION VERIFICATION FOR VANETS ROUTING

Ren Z and Wenfan Li et al., 2009 suggested that the Inter-vehicle communication among great deals of vehicles plays an important role in providing a high level of safety and convenience to drivers. Geographic routing protocol has been identified to be suited as a result of the special nature of vehicular ad hoc networks (VANETs), such as high dynamic mobility and large network size. Although there is considerable functional research about geographic routing, the security aspects have not been vastly concentrated.

The vehicular wireless network on the highway scenario, assume there are two directional antennas on every vehicle. The benefit of using directional antenna includes longer ranges as well as the reduced co-channel interference. The malicious nodes are randomly deployed in the networks. Geographic routing, e.g. GPSR, is a stateless protocol which makes localized optimal choice of next hop and achieves the global optimal routing path. Particularly, at every intermediate node, the farthest neighbor closest to the destination will be chosen as the next hop. Therefore, to affect the network performance, a malicious node could fake its position as the farthest one. In node m (malicious node) claims to be at a false position m, so it would be mistakenly considered as the farthest one from the view of node n1 which is current packet forwarder. After m receives the message, it can forward, modify or discard it at will. If node m does not fake its position, node n4 will be selected. Since there is no point of malicious node faking its position closer to the packet sender, in the following, that the malicious nodes are always trying to fake their position as the farthest one. Due to the nature of geographic routing, if the node selection of one hop is guaranteed to be safe, all nodes along the routing path can be trusted. Therefore, consider the detection of malicious nodes within one-hop neighbors instead of the entire networks.

2.4 IDENTITY-BASED BATCH VERIFICATION SCHEME

C. Zhang, R. Lu et al., 2008 Vehicular Ad Hoc Networks (VANETs), inherently provide us a perfect way to collect dynamic traffic information and sense various physical quantities related to traffic distribution with very low cost and high accuracy. Such functionalities simply turn a VANET into a Vehicular Sensor Network (VSN), which is

considered essential for achieving automatic and dynamic information collection and fusion in an Intelligent Transportation System (ITS). VSNs have been envisioned to have a great potential to revolutionize human's driving experiences and create a fresh new framework in metropolitan-area traffic flow control, and will undoubtedly take an important part of the future wireless metropolitan-area networks.

According to the Dedicated Short Range Communications (DSRC) protocol, each vehicle in a VANET broadcasts a traffic safety message every 100-300 ms, which keeps the vehicle's driving related information, such as location, speed, turning intention, and driving status regular driving, waiting for a traffic light, traffic jam, to other vehicles. With multi-hop forwarding, the messages will be either terminated by an RSU or dropped when exceeding over their lifetimes. When receiving a message, the RSU can either react to it if the sending vehicle of the message is nearby with some requests that can be handled locally or deliver the information to a traffic control center if the message is considered to contain any possible useful information. The RSU can also monitor and summarize the traffic situation of where it is located and report it to the traffic control center. With all the collected traffic related information, the traffic control center can generate an optimized control and management strategy for traffic light control by analyzing the current traffic load in each intersection. In addition to traffic information collection for traffic flow analysis and control, VSNs can equip current transportation systems with much new value-added functionality, such as serving as a virtual "black box" for each vehicle which keeps the driving record for resolving any possible traffic dispute and reconstructing scene of accidents. Although VANETs that support VSNs have been taken as the candidate for implementing the future context-aware intelligent traffic information collection system, many challenging security and privacy issues in VANETs have been identified. The implementation of VSNs can be put in a practical scenario for vehicular sensor networking purposes. To ensure both identity authentication and message integrity in VSNs, one appealing solution is to sign each message with a digital signature technique before the message is sent. However, conventional signature schemes that verify the received messages one after the other may fail to satisfy the stringent time requirement of the vehicular communication applications. The RSU could communicate with hundreds of On Board Units (OBUs) each sending a safety related message to the RSU every 100- 300 ms. In this case, verifying a large number of signatures sequentially could take a long time and will certainly become the processing bottleneck at the RSUs. For instance, in a high density traffic scenario, there could be roughly 180 vehicles

keeping within the communication range of an RSU, and each vehicle is sending a message every 300 ms.

2.4.1 PUBLIC KEY INFRASTRUCTURE

The maintenance of public key certificates under the traditional Public Key Infrastructure (PKI) also incurs huge communication overhead. In order to tackle the above mentioned problems and make VSNs suitable for the intelligent traffic systems, this paper introduces an efficient batch signature verification scheme for the communications between vehicles and RSUs.

1) Multiple signatures can be verified at the same time instead of one after the other as that in the previously reported approaches. Therefore, the signature verification speed can be significantly improved such that the computational workload of the RSUs can be alleviated.

2) Generating distinct pseudo identities and the corresponding private keys for signing each message with a tamper-proof device, privacy regarding user identity and location of the vehicles can be protected.

3) The identities of the vehicles can be uniquely revealed by the trusted authorities under exceptional cases.

4) Identity-based cryptography is employed by the tamper-proof device, efforts on certificate management and the transmission overhead can be significantly reduced.

2.4.2 PSEUDO IDENTITY GENERATION

To achieve privacy preservation to use the tamper-proof device, it is responsible to generate random pseudo identities and corresponding private keys based on identity-based cryptography. The tamper-proof device is composed of three secure modules: an authentication module, a pseudo identity generation module, and a private key generation modules. Authentication module: The authentication module works as an access control mechanism. A vehicle inputs its unique real identity RID and the password PWD to initiate the device, where the PWD can be the signature of the RID signed by the TA. If the RID and PWD successfully pass the verification of the authentication module, the RID is delivered to the next module, the pseudo identity generation module. Otherwise, the device denies

providing services for the vehicle. Obviously, the authentication module enhances the security of the tamper-proof device since a malicious adversary cannot take advantages of it even though the tamper-proof device is physically held by the adversary.

2.5 RSU AIDED MESSAGE AUTHENTICATION

C. Zhang, X. Lin et al., 2009 suggested that a Security issues have to be well addressed before we put these application scenarios into practice. First of all, message integrity must be guaranteed. Secondly, message senders should be authenticated in order to prevent impersonation attacks. In addition, user privacy concerns must also be well mitigated the identity, the position, and the movement track of a specific vehicle should not be obtained by the third party. To achieve both message authentication and anonymity, proposed that each vehicle should be pre-loaded with a large number of anonymous public and private key pairs and the corresponding public key certificates. There is a pseudo identity in each public key certificate. Traffic messages are signed with a public key based scheme, and each public and private key pair has a short life time to achieve privacy preserving.

2.5.1 AUTHENTICATE BATCH VERIFICATION

Each vehicle has only one public and private key pair. The public key is the same for all vehicles, and the private key of each vehicle is different. For a message signature, a vehicle only knows the authenticity of the signature, and the vehicle has no information on the identity of the message sender. It proposed a conditional privacy preservation scheme called ECPP, which divides privacy into three levels. In ECPP, RSUs are responsible for issuing temporary public key certificates to vehicles. Zhang et al. developed an identity-based batch verification scheme called IBV, which employs a tamperproof device to protect privacy. Although the above-mentioned studies respectively solved the security and privacy threats to different extents, they have all failed in taking the scalability issue and resultant communication overhead into consideration. First of all, they have not addressed the stringent time requirement for a vehicle to verify all message signatures sent by its neighboring vehicles especially when the traffic density becomes larger. HMAC code attached to each IVC message, the verification of message authenticity can be performed in an extremely fast and efficient way because HMAC is performed using fast symmetric decryption.

2.5.2 MESSAGE INTEGRITY FAST VERIFICATION

All messages should be delivered unaltered, and the origin of the messages should be authenticated to guard against an impersonation attack. Low communication overhead and fast verification: A large number of message signatures should be verified in a short interval. Conditional privacy preservation: The identities of vehicles should be hidden from a normal message receiver during the authentication process in order to protect the senders' private information.

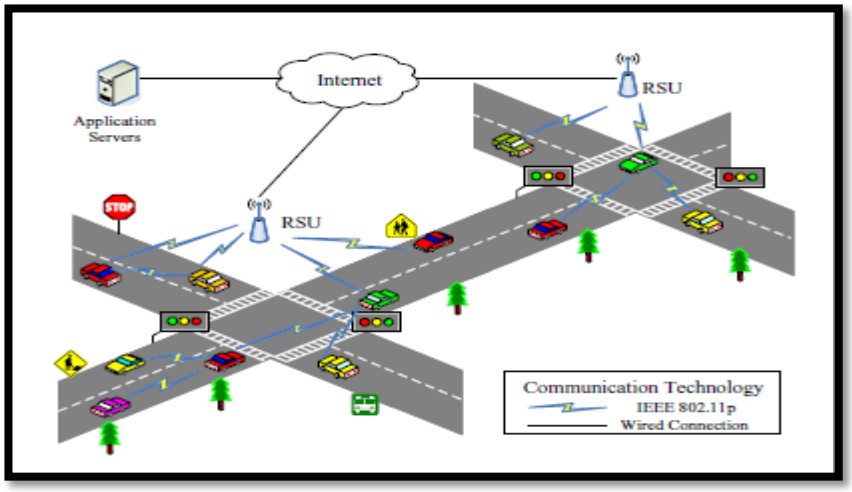

Figure 2.5.2: General Architecture of RSU

When an RSU is detected nearby, vehicles start to associate with the RSU. Then, the RSU assigns an unique shared symmetric secret key and a pseudo ID that is shared with other vehicles. With the symmetric key, each vehicle generates a symmetric keyed-hash message authentication (HMAC) code, and then broadcasts a message by signing the message with the symmetric HMAC code instead of a PKI-based message signature. Other vehicles receiving the messages signed with the HMAC code are able to verify the message by using the notice about the authenticity of the message disseminated by the RSU. The reason why the RSU knows the authenticity of the messages is that the RSU has the HMAC encryption keys shared with vehicles.

System Specification

3. SYSTEM SPECIFICATION

3.1 HARDWARE SPECIFICATION

The following are minimum hardware requirements for this project.

- Hard Disk : 285 GB
- Monitor : 21’ Color with VGI card support
- RAM : 4.00 GB
- Processor : Intel(R) Core(TM) i3
- Processor speed : CPU M 350 @ 2.27GHz
- System Type : 32-bit Operating System

3.2 SOFTWARE SPECIFICATION

The following are minimum software requirements for this project.

- Operating System : Windows XP/7/LINUX.
- Implementation : NS2
- NS2 Version : NS2.2.28
- Front End : OTCL (Object oriented tool command language)

3.3 ABOUT THE SOFTWARE

3.3.1 NETWORK SIMULATOR-2

A network simulator is a piece of software or hardware which predicts the behavior of a network, without an actual network being present. Network simulators serve a variety of needs. Compared to the cost and time involved in setting up an entire test bed containing multiple networked computers, routers and data links, network simulators are relatively fast and inexpensive. They allow engineers to test scenarios that might be particularly difficult or expensive to emulate using real hardware for instance, simulating the effects of a sudden burst in traffic on a network service. Networking simulators are particularly useful in allowing designers to test new networking protocols or changes to existing protocols in a controlled and reproducible environment.

Network Simulator-2 (NS2) is based on two languages, an object oriented simulator, written in C++and an OTcl (an object oriented extension of Tcl) interpreter, used to execute user's command scripts. NS has a rich library of network and protocol objects. There are two class hierarchies: the compiled C++ hierarchy and the interpreted OTcl, with one to one correspondence between them.

The compiled C++ hierarchy allows us to achieve efficiency in the simulation and faster execution time. This is in particular useful for the detailed definition and operation of protocols. This allows one to reduce packet and event processing time.

NS is a discrete event simulator, where the advance of time depends on the timing of events, which are maintained by a scheduler. An event is an object in the C++ hierarchy with a unique ID, a scheduled time and the pointer to an object that handles the event. The scheduler keeps an ordered data structure with the events to be executed and fires them one by one, invoking the handler of the event.

3.3.2 STRUCTURE OF NS2

NS2 is built using object oriented methods in C++ and OTcl (object oriented variant of Tcl.

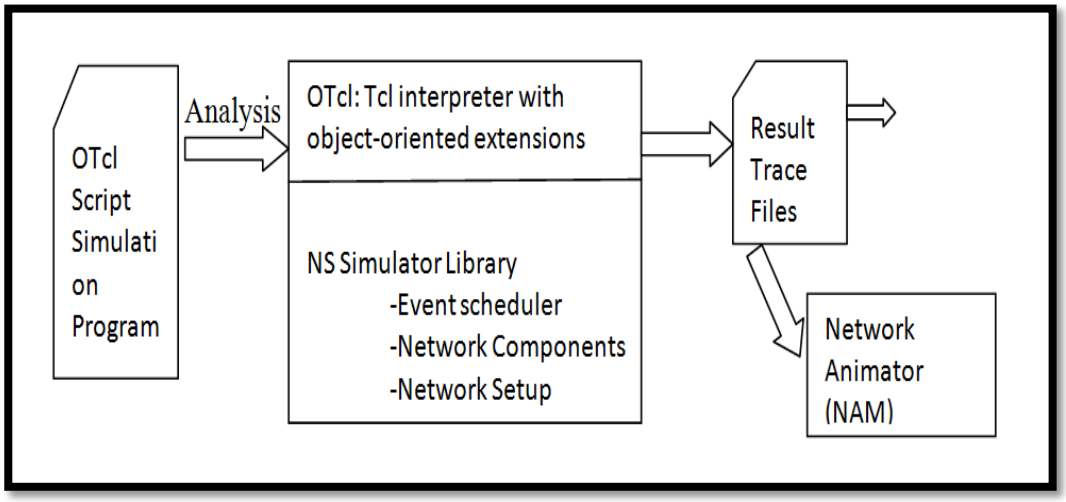

Figure 3.3.2: Structure of NS2

A user has to set the different components up in the simulation environment. The user writes his simulation as an OTcl script, plumbs the network components together to the complete simulation. The event scheduler as the other major component besides network components triggers the events of the simulation. Some parts of NS2 are written in C++ for efficiency reasons. The data path is separated from the control path. Data path object are compiled and then made available to the OTcl interpreter through an OTcl linkage which maps methods and member variables of the C++ object to methods and variables of the linked OTcl object. The C++ objects are controlled by OTcl objects. It is possible to add methods and member variables to a C++ linked OTcl object. NS is written in C++, with an OTcl1 interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower but can be changed very fast quickly, is used for simulation configuration. One of the advantages of this split-language program approach is that it allows for fast generation of large scenarios. To simply use the simulator, it is sufficient to know OTcl. On the other hand, one disadvantage is that modifying and extending the simulator requires programming and debugging in both languages.

NS can simulate the following:

1. Topology: Wired, wireless

2. Scheduling Algorithms: RED, Drop Tail,

3. Transport Protocols: TCP, UDP

4. Routing: Static and dynamic routing

5. Application: FTP, HTTP, Telnet, Traffic generators

3.3.3 FACILITIES IN NS2

One can set up network topologies and generate packet traffic and measure various parameters. (i.e.) performance analysis can be done by measuring delay, jitter and throughput. Graphical visualization is possible using Network Animator, X-Graph and GNU plot, Excel or X-plot. One can modify NS-2 to implement their own versions of protocols or even totally new protocols.

3.3.4 FUNCTIONS OF NS2

- The Network Simulator 2 takes care of the following functions:
- Reads and interprets the OTcl Script.
- Makes use of the objects compiled in C++.
- Creates trace files as output.
- Creates NAM input files.
- Measures statistics.
- By analyzing the trace file, data for output plot can be obtained.

3.3.5 NAM

NAM File in NS2 plays a significant role as without NAM, output cannot be visualized. It is Graphical user interface (GUI) tool for NS2, which makes it a significant component of NS2. The Network Animator (NAM) is a completely separate program that is

distributed with the NS simulator. This program is named NAM and it shows the progression of the packets through the network. The NAM program reads an input file (containing the packet transmission events) and draws the network events graphically.

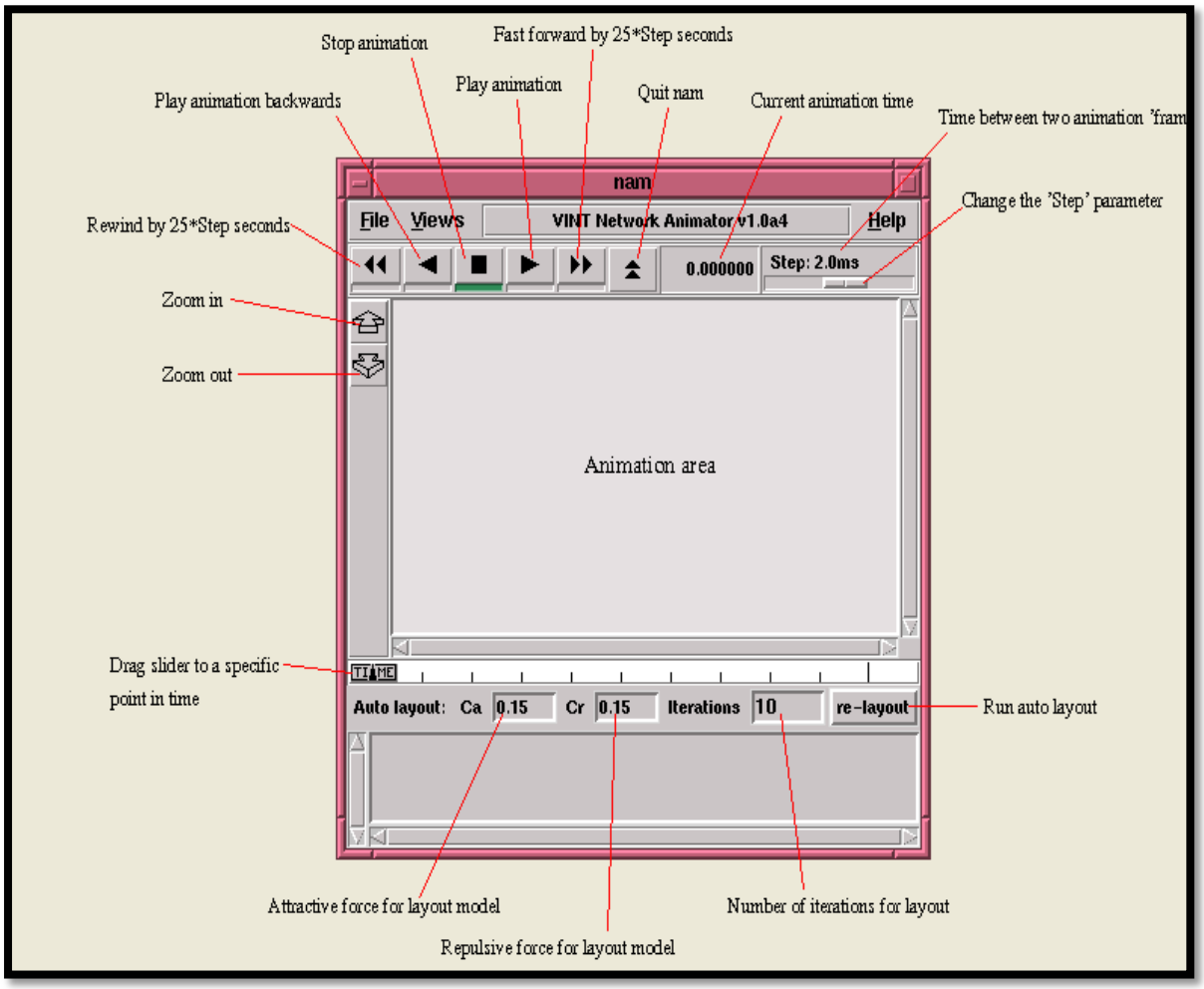

Figure 3.3.5: NAM File

NAM IN NS2 HIGHLIGHTS

- Provides visual interpretation of overall network.
- Executes from the TCL script directly.
- Provides controls for play, stop, pause, display speed controller, packet monitor facility etc.
- Supports for drag and drop interface for creating topology.

- Provides information regarding the overall throughput, number of packets transmission on each link etc.
- NAM graph shows the overall graphical representation of packet flow [i.e. when the packets are received or dropped].
- NAM files contains the work flow of TCL script.
- To execute a NAM, use the following command: *Exec nam $filename*

3.3.6 XGRAPH

XGraph is a plotting program that is used to create graphic representations of simulation results. InNS2, It is used to plot the network parameter characteristics like

- Throughput
- Delay
- Jitter
- Latency

XGraph includes the following:

- Animation and derivatives.
- Interactive plotting and graphing.
- Portability and bug fixes.

Methodology

4. METHODOLOGY

In this proposed system, the methodology is constructed into four phases. Each phase has its own task which is followed by the other. First phase is the Vehicle topology creation, Second phase is the Verification of Vehicle and RSU, Third phase is the Batch message signing and signature verification and Priority and negative vehicle signature identification.

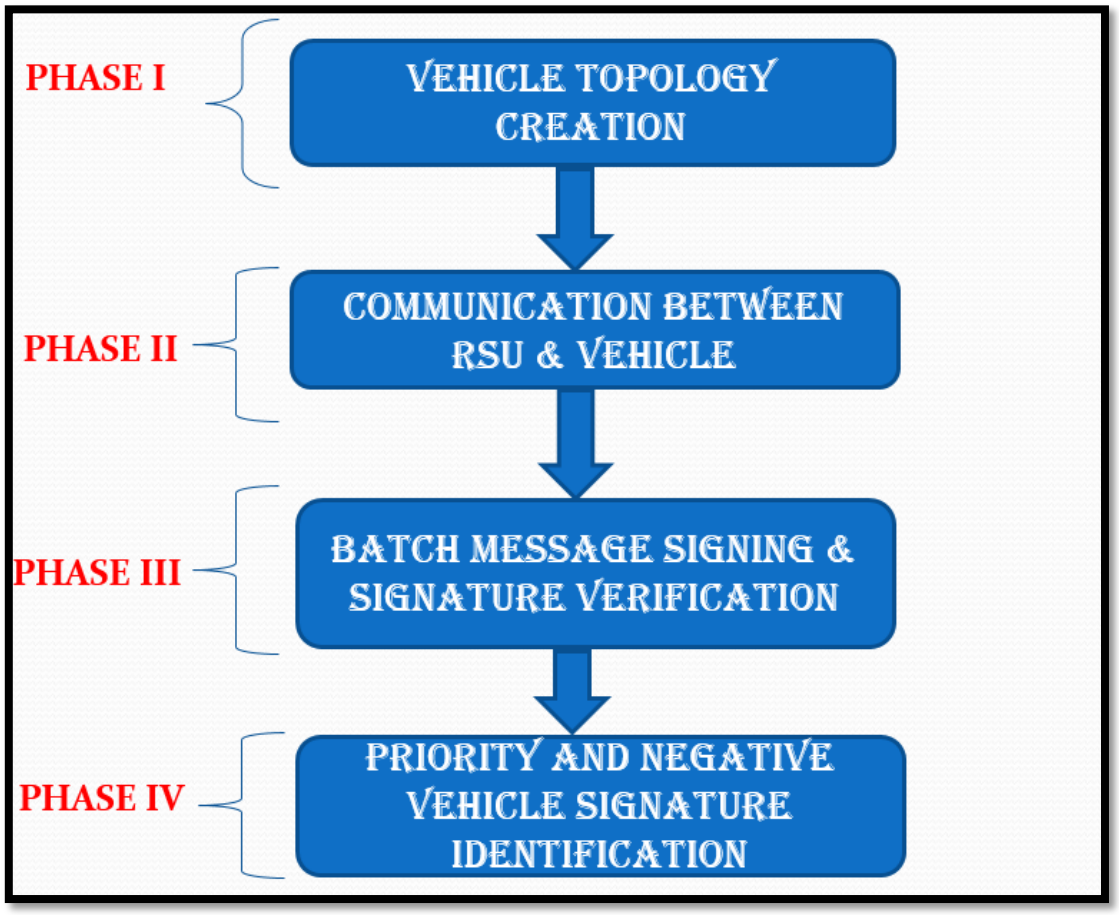

Figure 4: Various phases of this project

4.1 MODULE DESCRIPTION

4.1.1 MODULE I - VEHICLE TOPOLOGY CREATION

Vehicular ad hoc networks (VANETs) are being developed to provide on-demand wireless communication infrastructure among vehicles and authorities. Such an infrastructure is expected to deliver multiple road safety and driving assistance applications. Vehicles will

be equipped with sensors and communication devices that will allow them to cooperate with each other and with authority units to disseminate and exchange various road applications messages. Warning messages and traffic management instructions can be broadcast to increase driver's awareness of potential travel hazards, allowing them to respond earlier to avoid traffic congestion and collisions or to clear the way for inbound emergency response units.

Network promising for the applications requires knowledge of real-time events and neighboring vehicles' location specifications. A vehicle can determine its location using existing technologies such as Global Positioning Systems (GPS), map matching, dead reckoning, cellular localization, image and video processing and relative positioning. Enabling each vehicle to determine its location is necessary in VANET, but it is not enough. Vehicles also need to have information about events in their surroundings and proximal vehicles. This type of information can be exchanged between network members using beaconing, direct messaging, or group updates.

4.1.2 MODULE II – VERIFICATION OF VEHICLE AND RSU

In this module vehicle search the shortest path to identify a best destination route in order to transmit the query through Road Side Unit (RSU) and get the acknowledgement back to RSU. The TA will send a request to RSU to verify the vehicle's id based on secret key which is already installed in vehicles to identify authenticate user or not. After verification of vehicle's id, RSU receive the vehicles re-encryption key for encrypting the user query based on TA. Finally RSU encrypt the user query passed through destination (RSU travelling via neighboring RSUs). Based on user query destination RSU finds the best and shortest path in a travelling sequence. Then it transmits the required path to user's vehicle towards neighboring RSUs. The user's vehicle request receives the encrypted query and then it decrypts the message on its own private key only then user can able to view the shortest path. After decryption process, vehicle moves freely from one network to other networks.

Every vehicles store their information details in Trusted Authority (TA) to identify number of possible routes. The TA maintains the vehicle's connection information from one node to other. There are many available routes has localized so the vehicle can

connect through other vehicles in all the directions. Only the registered vehicle can get the information from central server i.e. TA. When the movement takes place TA will generate a revocation list for each vehicle from this case both the vehicle details and the vehicle status are noted separately. When the user is ready to transmit the query TA maintains re-encryption key and secret key for each vehicle to send the information securely.

Random Pseudo identity has two parts ID1and ID2 computing a private key based on ID1 and ID2. The resultant private key also contains two parts which are denoted as SK1 and SK2 respectively. Finally vehicle Vi can obtain a list of pseudo identities Idi = (ID1 , ID2) along with the corresponding private keys Ski=(SK1,Ski2). The pseudo identities and the private keys can be generated offline by the tamper-proof device; thus, no delay will be caused in the signing messages at the OBU side due to this process.

4.1.3 MODULE III – BATCH MESSAGE SIGNING AND SIGNATURE VERIFICATION

In this module a vehicle denoted by Vi first generates the traffic related message denoted by Mi. Vi picks a pseudo identity IDi = (ID1,ID2) and the corresponding private key SKi =(SK1 ,SK2) by way of the tamper-proof device. With the private key SKi= (SK1, SK2) .Vi can compute the signature σi of the message Mi, where σi = SK1 + H(Mi) SK2 and Vi broadcasts the final message ⟨IDi,Mi, σi⟩ to its neighboring vehicles.

4.1.4 MODULE IV – PRIORITY AND NEGATIVE SIGNATURE VEHICLE IDENTIFICATION

In this module, network allows each vehicle based on priority manner. The vehicle movement based on priority will leads to avoid collision. Network gives higher priority for emergency vehicles like ambulance, fire engines etc. It gives medium priority for registered vehicles, because those users installed the device in vehicles and frequently update the information to TA. Finally, the lower priority gives to unregistered vehicles. Negative signature in VANET can be identified based on the secret key (ID) installed in each vehicle and private key (SK) generated by the Trusted Authority (TA).

Experimental results and analysis

5. EXPERIMENTAL RESULTS AND ANALYSIS

The result can be analyzed in terms of Performance metrics like

- Packet delivery ratio
- Throughput
- Average delay

5.1 PACKET DELIVERY RATIO

Packet Delivery Ratio (PDR) is defined as the ratio between the received packets by the destination and the generated packets by the source. Packet Delivery Ratio is calculated by processing the trace file and produces the result in the form of XGraph.

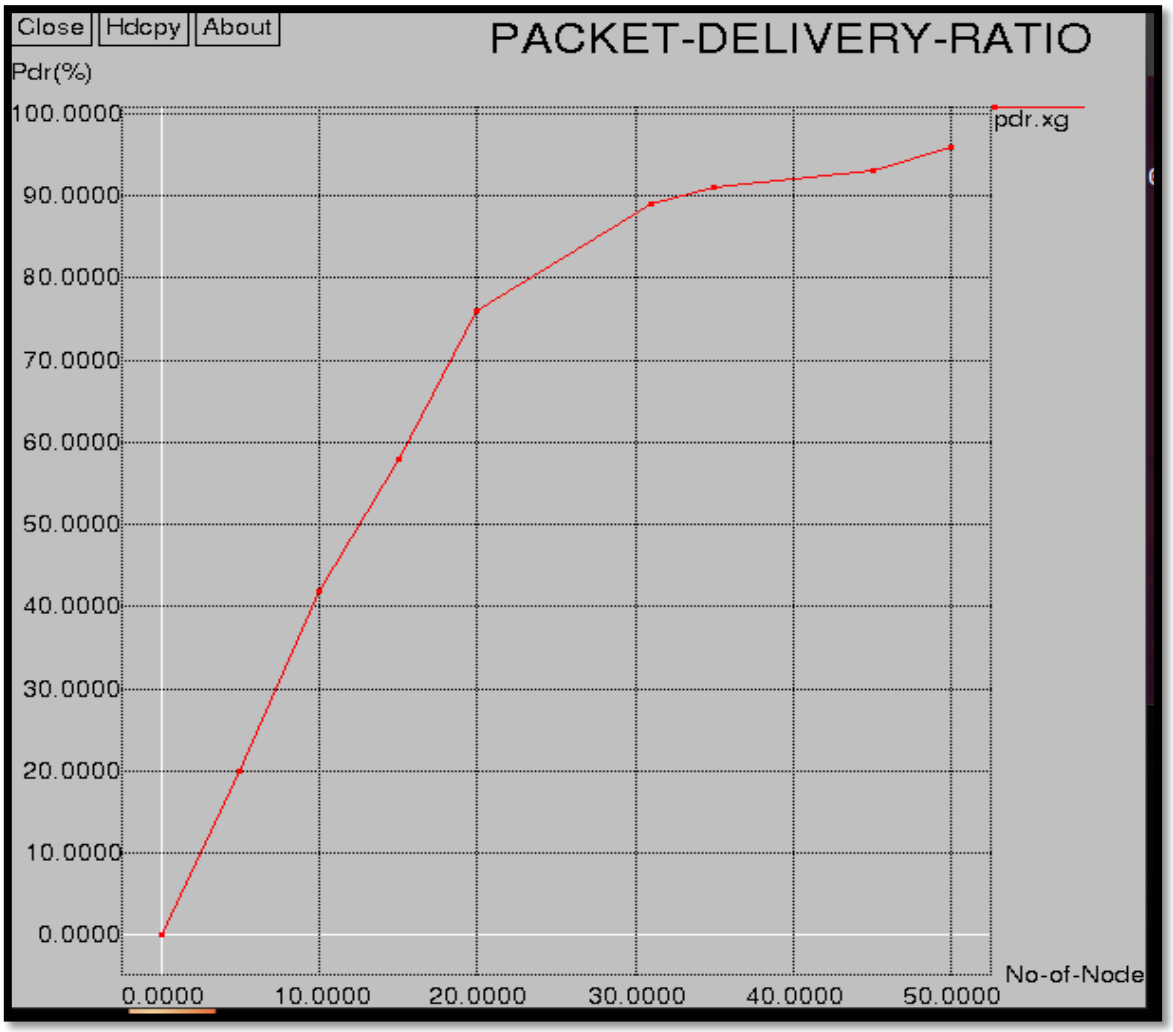

Figure 5.1: Packet Delivery Ratio

In Fig 5.1 the packet delivery ratio of the vehicular network increases with time. Here the packet delivery ratio of DSDV protocol is better compared to the proactive and reactive protocols. The packet delivery ratio of DSDV protocol is high because of low packet loss.

5.2 THROUGHPUT

Throughput is the number of successfully received packets in a unit time and it is represented in bps. Throughput is calculated by processing the trace file and produces the result in the form of XGraph.

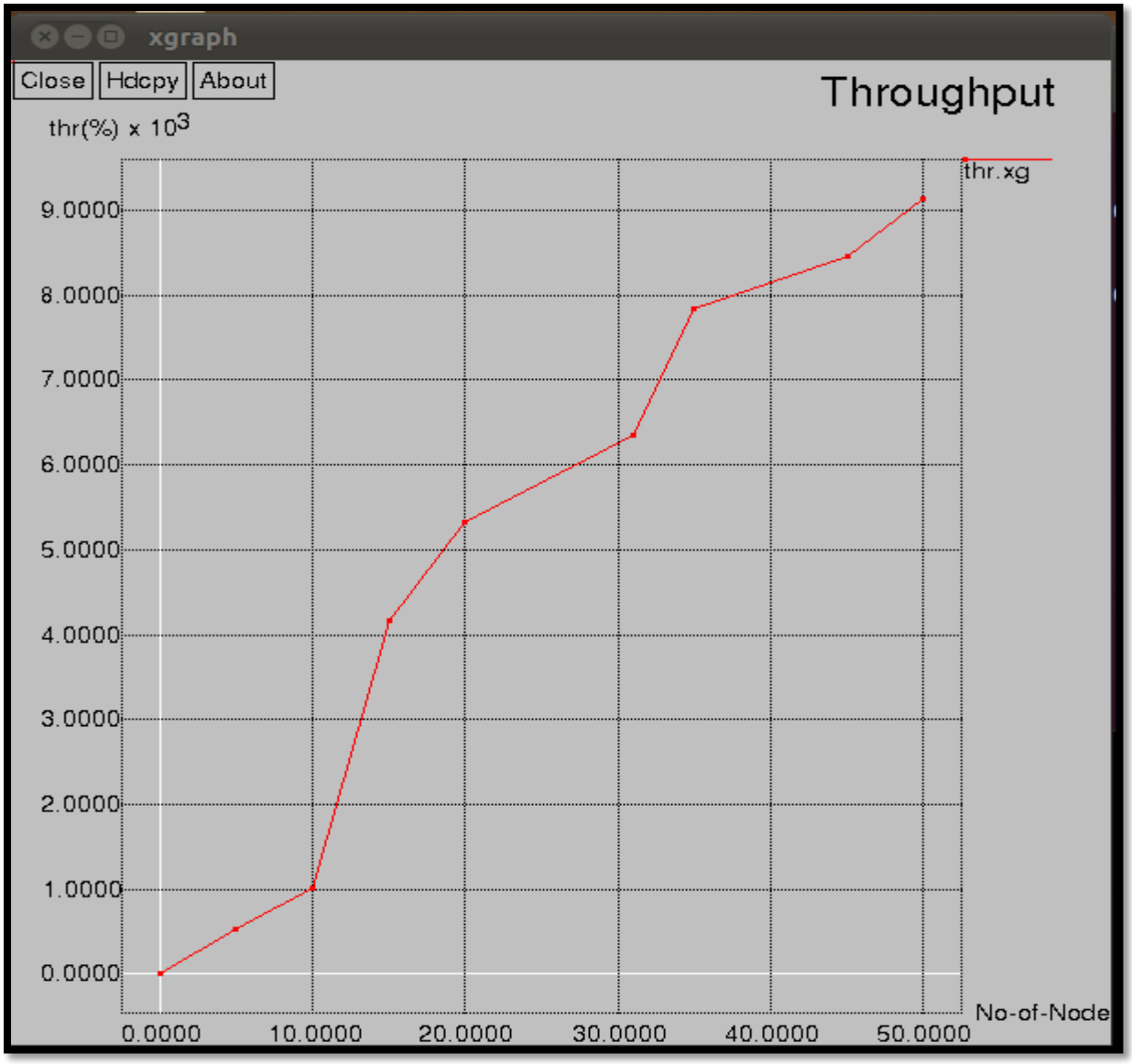

Figure 5.2: Throughput

As the packet delivery rate is very high. So the throughput gets increases. In Fig.5.2, the throughput of the vehicular network increases with time.

5.3 AVERAGE DELAY

Delay is the difference between the time at which the sender generated the packet and the time at which the receiver received the packet. Delay is calculated by processing the trace file and produces the result in the form of XGraph.

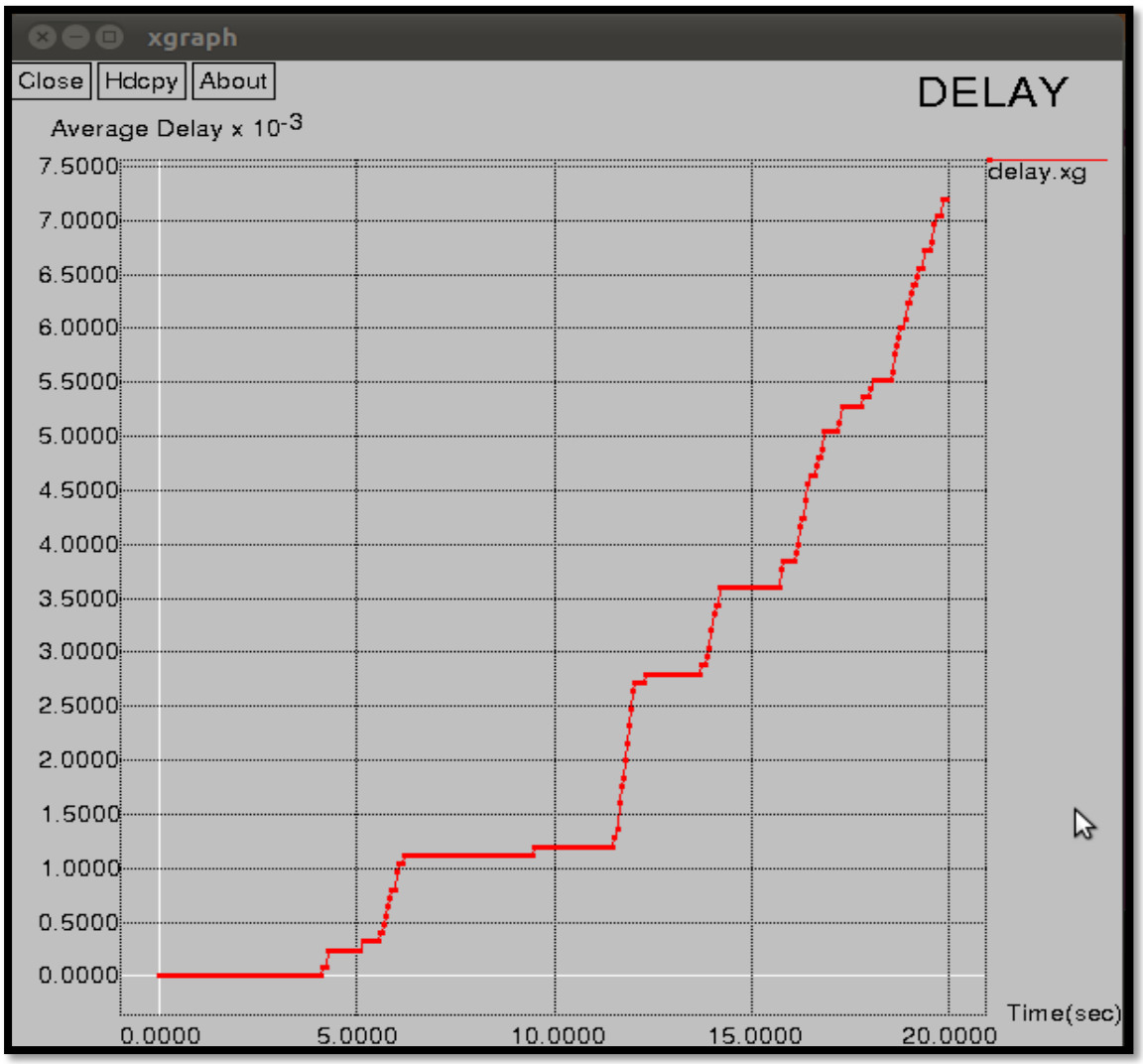

Figure 5.3: Average Delay

In Vehicular Ad hoc Networks the routing overhead gets decreased. So the delay gets reduced and speed gets improved. In Fig.6.2.3, the routing overload of the data transmission decreases with time.

Conclusion

6. CONCLUSION

In this Project Random Pseudo identity and Batch based signature identity for road vehicles are used in which they are travelling and periodically broadcasting traffic related information that could be extremely vital and life-critical information for neighboring vehicles. A navigation credential will expire after predefined expiration periods of time. The navigation credentials on different days are different. To ensure the integrity of the messages, each message sent by a vehicle should be signed and verified when being received. Message based batch verification in which the vehicle receives traffic related messages from other vehicles and each vehicle has to verify the signatures of the messages. This scheme can apply to the situation where the route searching process is done by a central server (TA), which collects and verifies speed data and road conditions from RSUs. The authentication process at vehicles can be even simpler because the vehicle only needs to check against the central server's signature on the processed result. Based on the destination and the current location of the driver, the system can automatically search for a route that yields minimum travelling delay in a distributed manner by using the online information of the road condition.

Scope for future enhancement

7. SCOPE FOR FUTURE ENHANCEMENT

The work can be further enhanced by concentrating on Directed Clustering Protocol (DCP) in which it increases the life time of network and can be used together with the Location Ad-hoc Routing (LAR) algorithm. DCP is a clustering algorithm. Clustering is a new approach to efficiently utilize the energy of vehicle sensor nodes. This routing mechanism will come up with better throughput, energy consumption and less packet loss.

Bibliography

8. BIBLIOGRAPHY

- C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008.
- Chenix Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuenmin, "An Efficient Message Authentication Scheme for Vehicular Communications" IEEE Transaction on Vehicular Technology,Vol.57, no.6, November 2008.
- F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update," IEEE Pervasive Computing, vol. 5, no. 4, pp. 68-69, Oct.-Dec. 2006
- Leinmüller T, Schoch Eand Kargl F, (2006) "Position verification approaches for vehicular ad hoc networks," IEEE Wireless Commun., Vol. 13, No. 5, pp. 16–21.
- Ren Z, Li Wand Yang Q,(2009) "Location verification for VANETs routing," in Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun, pp. 141–146.
- S.Kathirvel, D.Gautham Chakravarthy, Dr.S.Gunasekaran "A Survey on VANET based Secure and Privacy Preserving Navigation" International Journal of Scientific & Engineering Research, Vol. 6, Issue 4, April-2015.
- T.W.Chim, S.M Yiu, Lucas C.K Hui, "VSPN : VANET based secure and privacy preserving navigation", IEEE transactions on computers, Vol.63, No.2, Feb.2014.

REFERENCE WEBSITES

- https://pdfs.semanticscholar.org/78ad/76d1fc9c06e415f156866924d87ede0c909e.pdf
- http://www.rroij.com/open-access/vehicular-ad-hoc-networks-61-64.pdf
- https://www.cse.wustl.edu/~jain/cse571-14/ftp/vanet_security/index.html
- https://www.researchgate.net/publication/263629127_An_Efficient_Signature_Batch_Verification_System_for_VANET
- https://www.iosrjen.org/Papers/vol8_issue8/Version-1/D0808012532.pdf

Appendix

9. APPENDIX

9.1 SYSTEM FLOW DIAGRAM

System flow diagram is a graphical representation of the "flow" of data through an information system, modelling its process aspects. It does not show information about the timing of processes or information about whether processes will operate in sequence or in parallel.

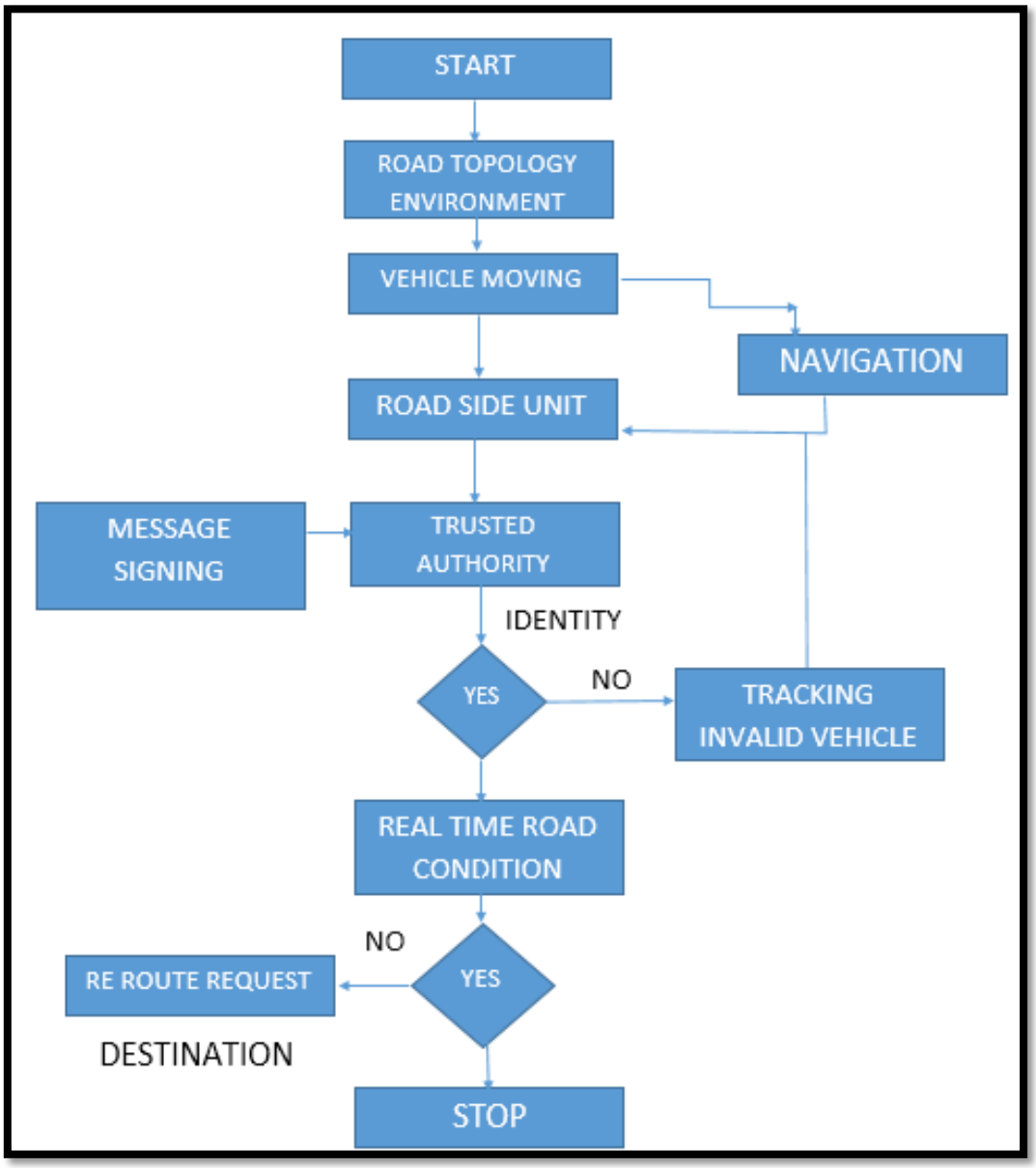

Figure 9.1: System flow diagram

9.2 ACTIVITY DIAGRAM

Activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system.

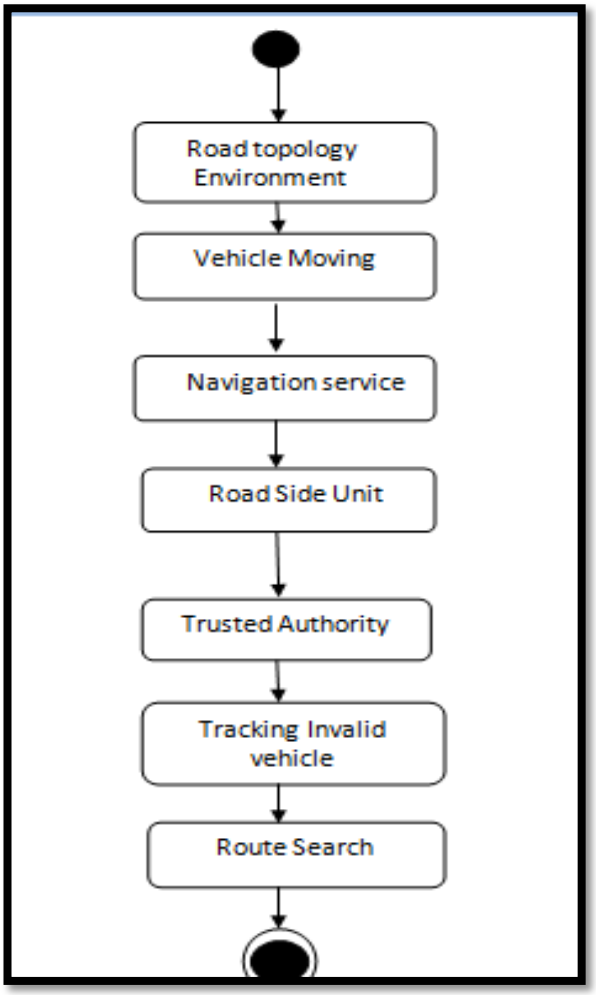

Figure 9.2: Activity diagram

9.3 SCREEN SHOTS

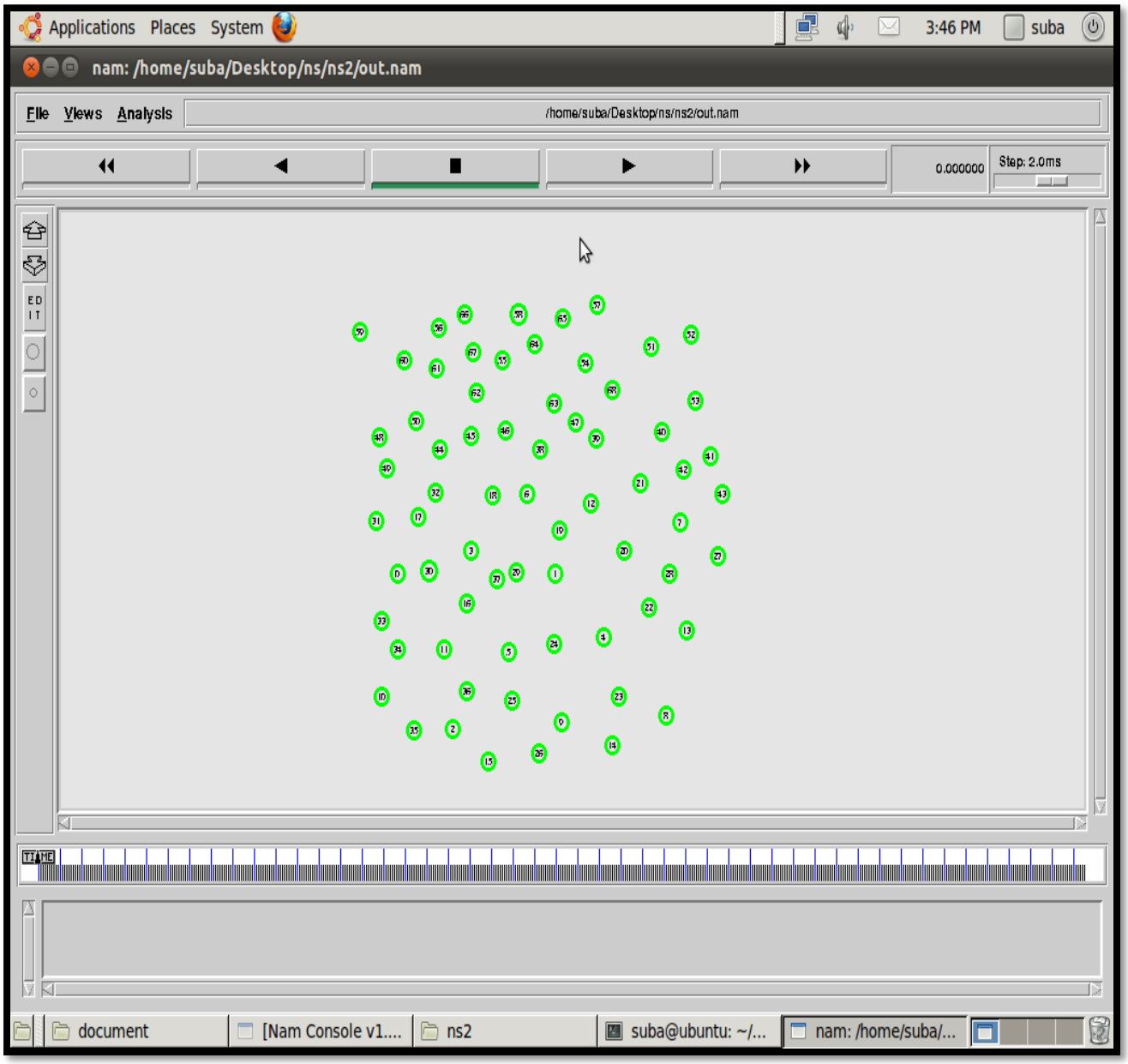

Figure 9.3.1: Creation of vehicle sensor nodes

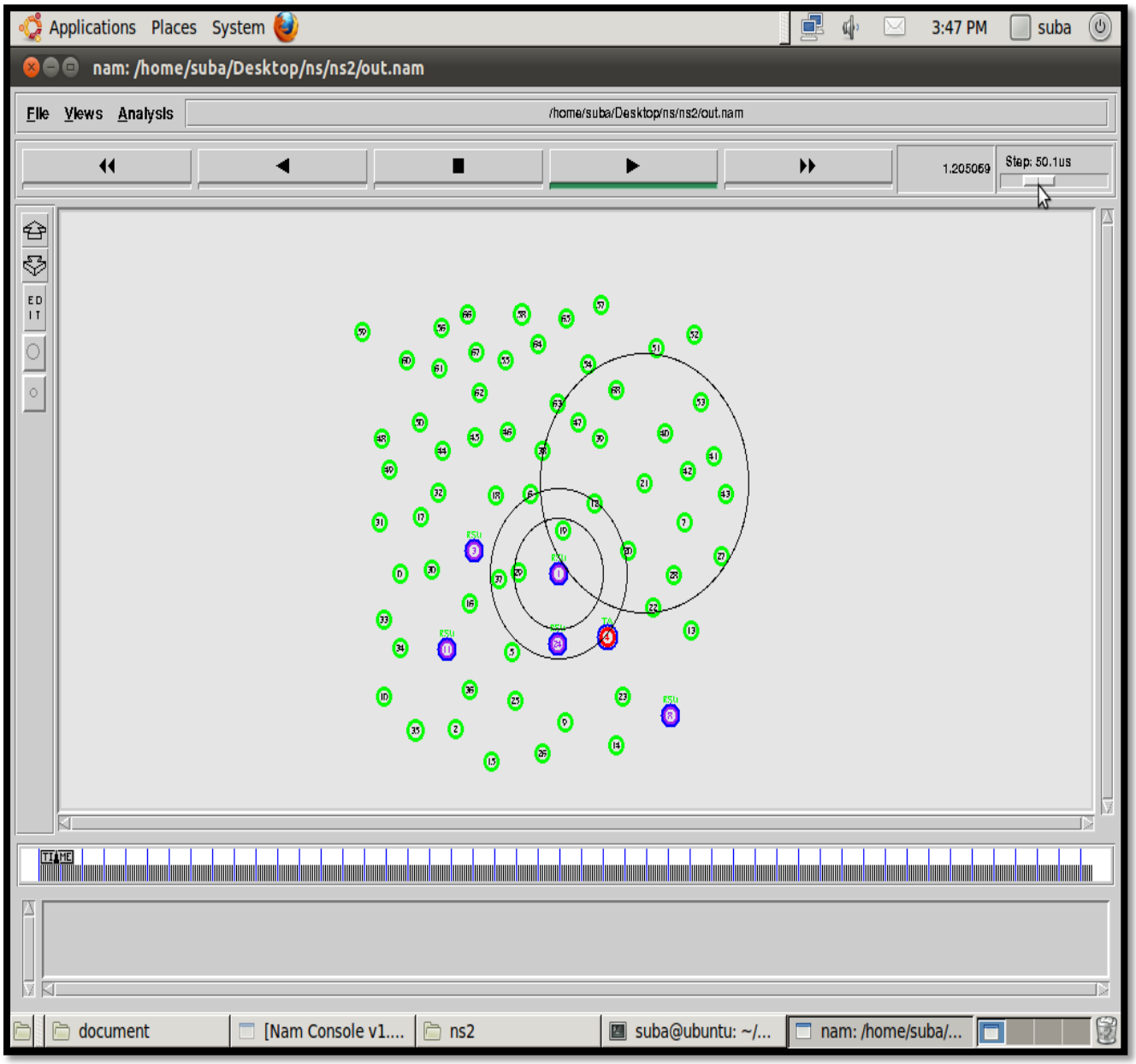

Figure 9.3.2: Communication between the Vehicle and RSU

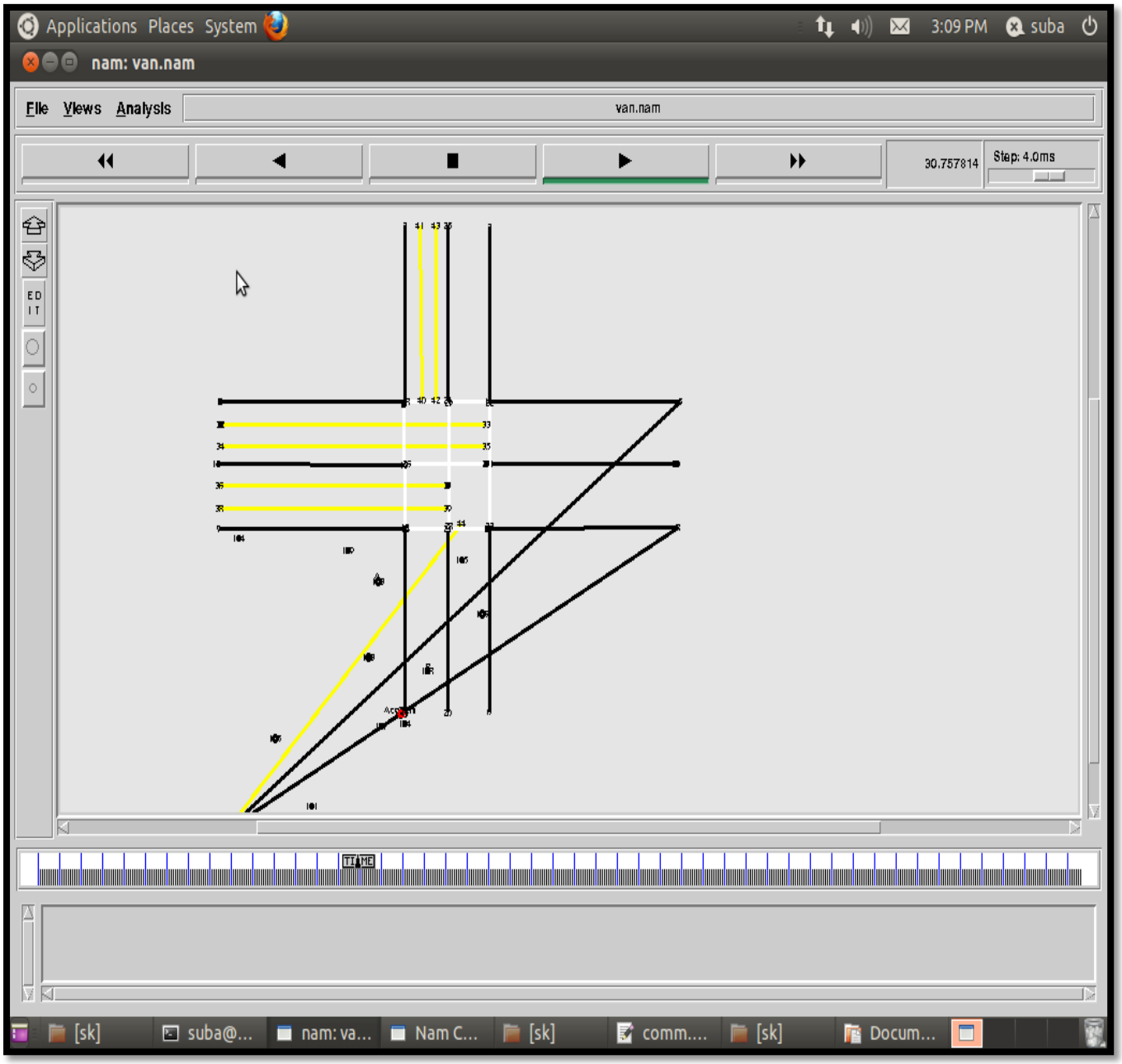

Figure 9.3.3: Road Topology environment creation

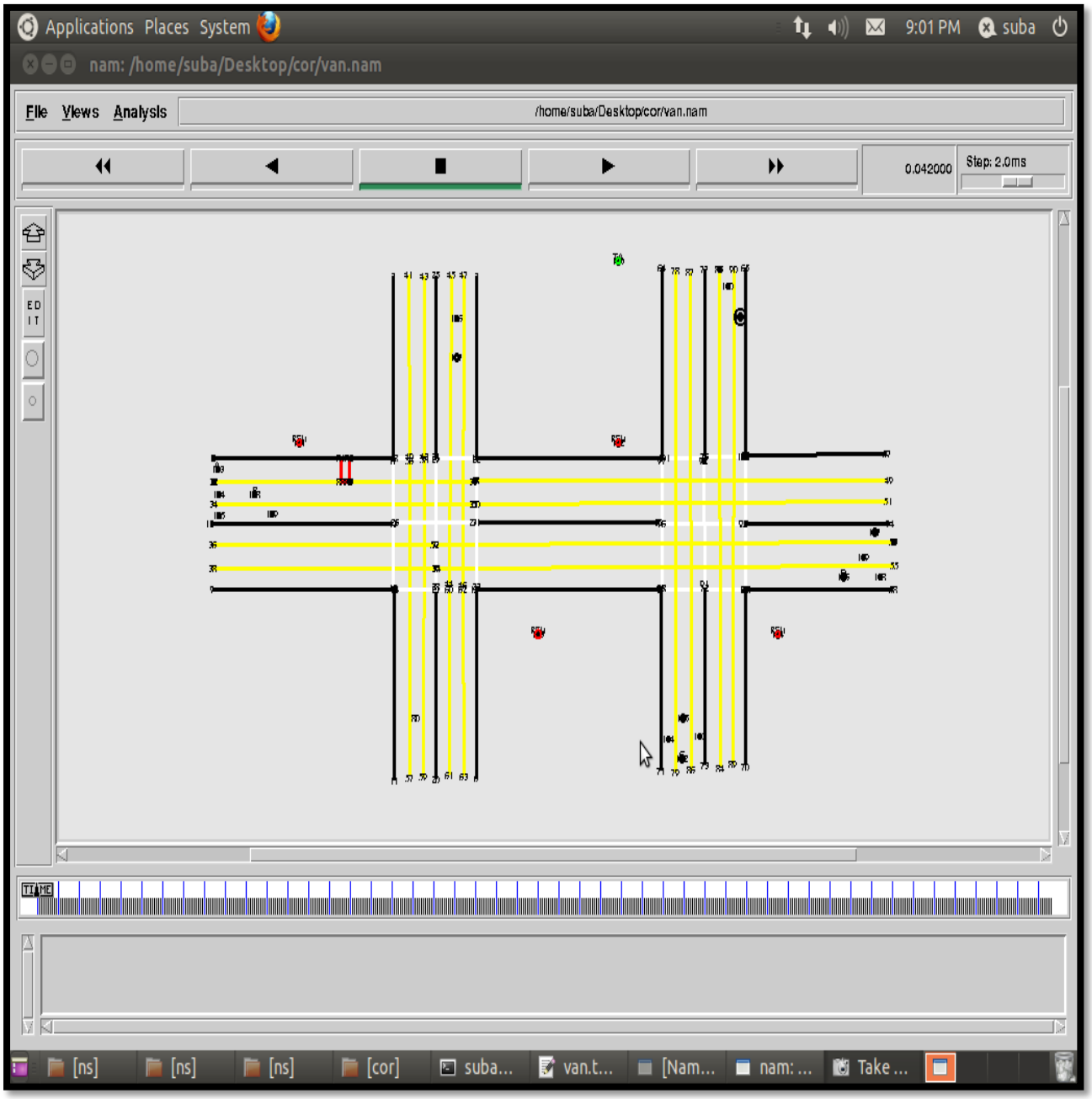

Figure 9.3.4: Road Topology environment

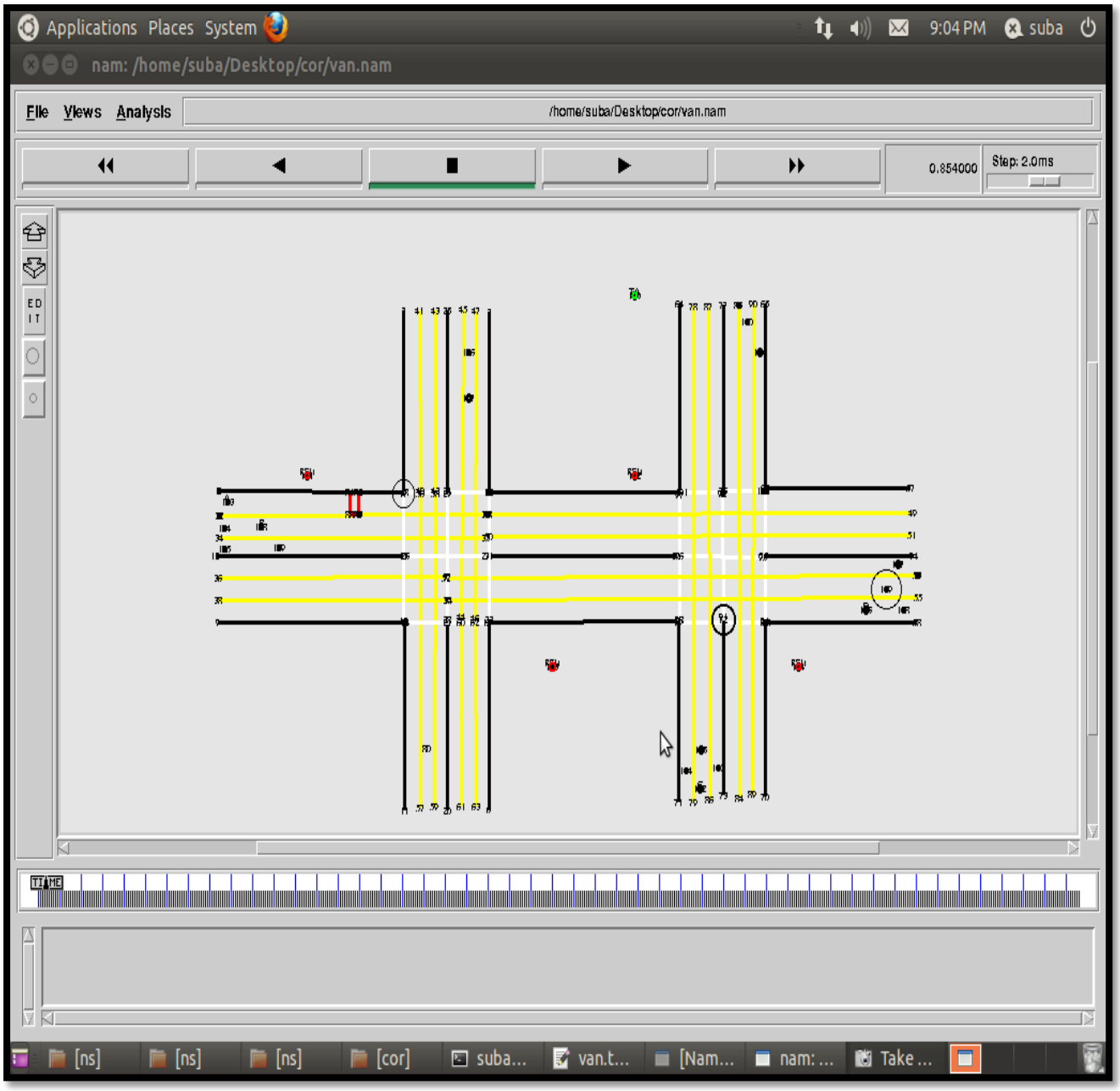

Figure 9.3.5: Communication between vehicle and RSU

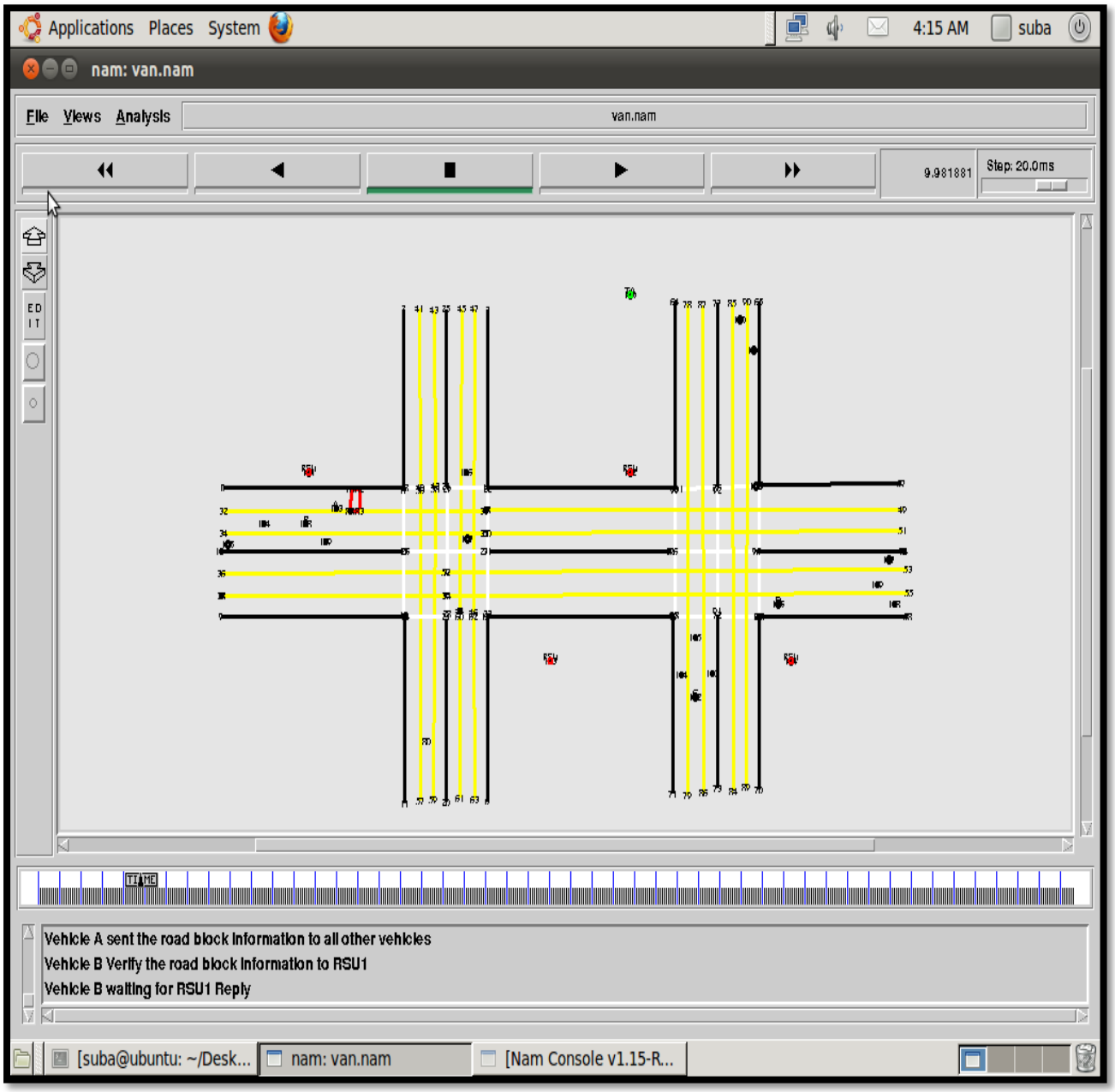

Figure 9.3.6: Vehicles transmitting the messages

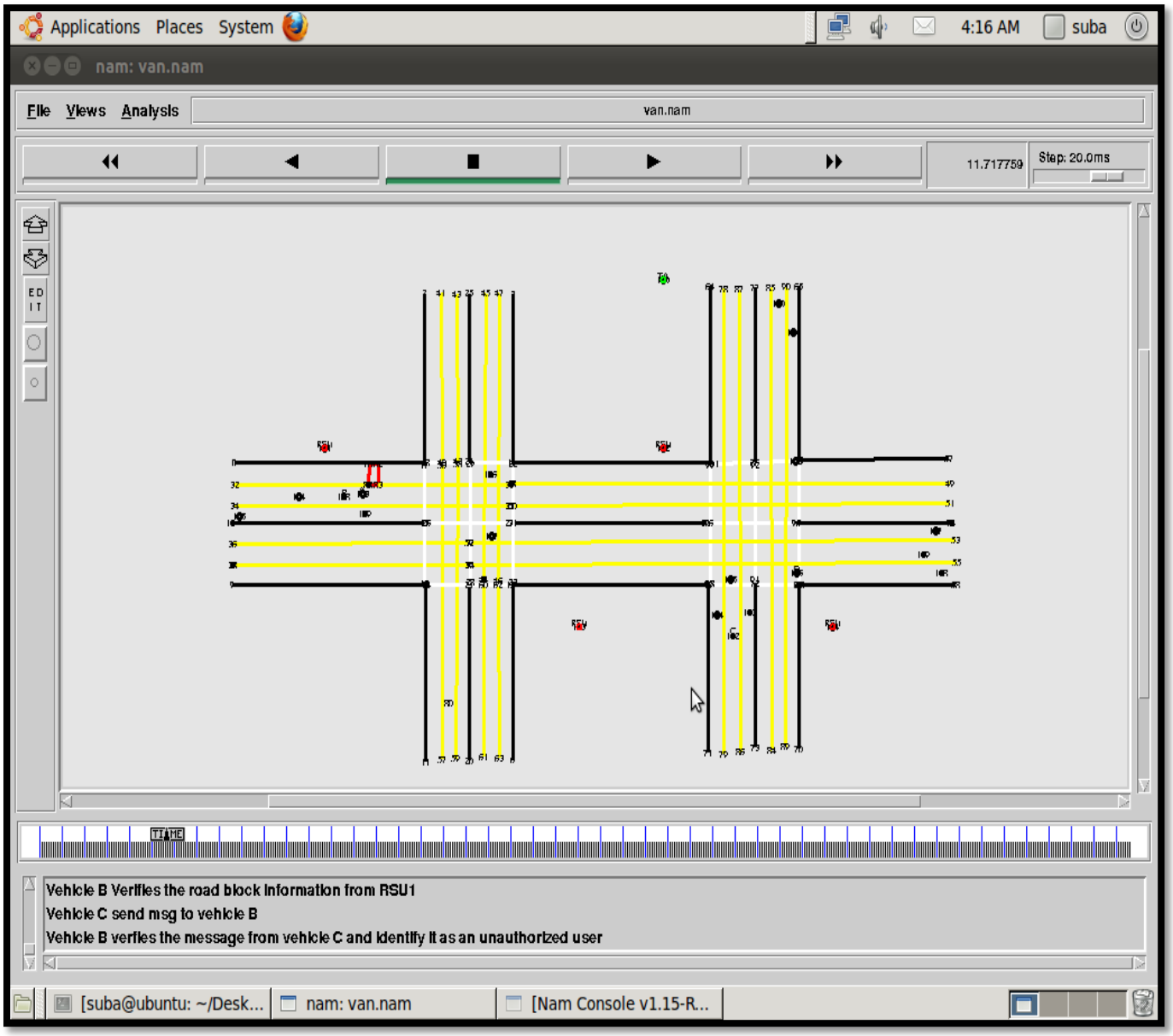

Figure 9.3.7: Road block condition and Message verification

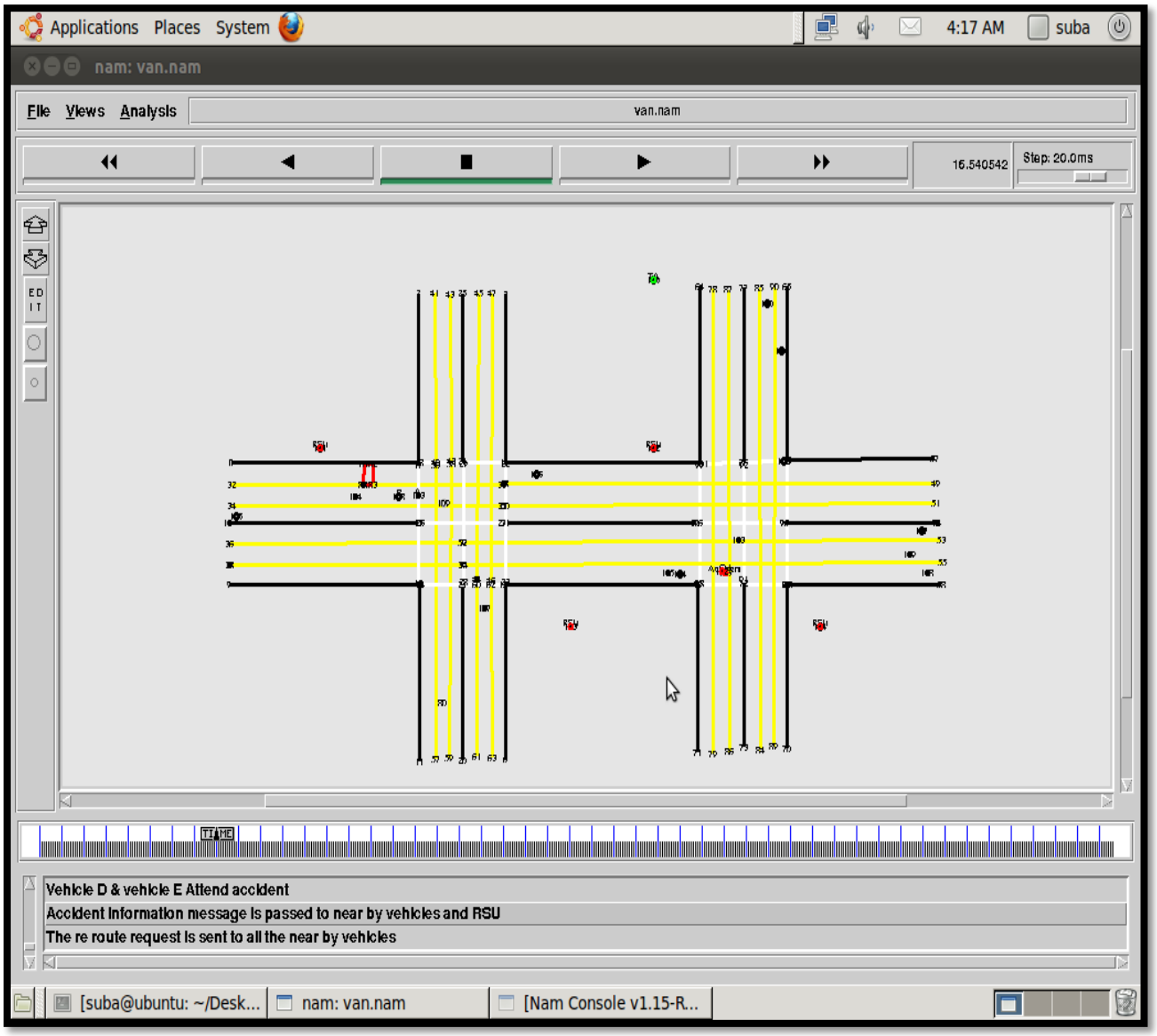

Figure 9.3.8: Accident information and reroute request