CHAPTER VII

A graph Vertex Colouring based Certificate less Authentication Techniques for Alert Message Dissemination in Vanet

This chapter provides an introduction, idea and the need for vehicular ad hoc networks. A brief knowledge about the challenges concerning the works are also discussed.

7.1 Graphs

A collection of graphs are mathematical structures used to model pair wise relations between objects. Especially vertex colouring Graphs can be used to model many types of relations and processes in physical, biological, social and information systems. Emphasizing their application to real-world systems, the term network is sometimes defined to mean a graph in which attributes are associated with the nodes and/or edges. Colouring Graphs are used to represent networks of communication, data organization, computational devices, the flow of computation, etc. The development of algorithms to handle graphs is therefore of major interest in computer science. The transformation of graphs is often formalized and represented by graph rewrite systems.

7.2 Vertex colouring graphs in vehicular ad-hoc networks

The communication in VANET occurs between Vehicle 2 Vehicle mode and Vehicle to road side unit forming an intelligent transport system. Routing plays an important role in forwarding the required data to the nodes or vehicles. VANET is a unique and special form of ad-hoc network [Ayaida, M et al., 2014]. For example, if a vertex colouring graph represents a road network, the weights could represent the length of each road. VANETs interface the few aspects of ad hoc networks, wireless and cellular technology to form a intelligent transport systems by communicating between vehicle to vehicle and vehicle to road side units. There may be several weights associated with each edge, including distance, travel time, or monetary cost. Such weighted graphs are commonly used to program GPS's, and travel-planning search engines that compare vehicle times and costs. Figure 7.1 explain the general vehicle ad-hoc network architecture diagram different road side

units. Figure 7.2 explain the representation for Vertex Colouring graph connectivity in vehicle ad-hoc network.

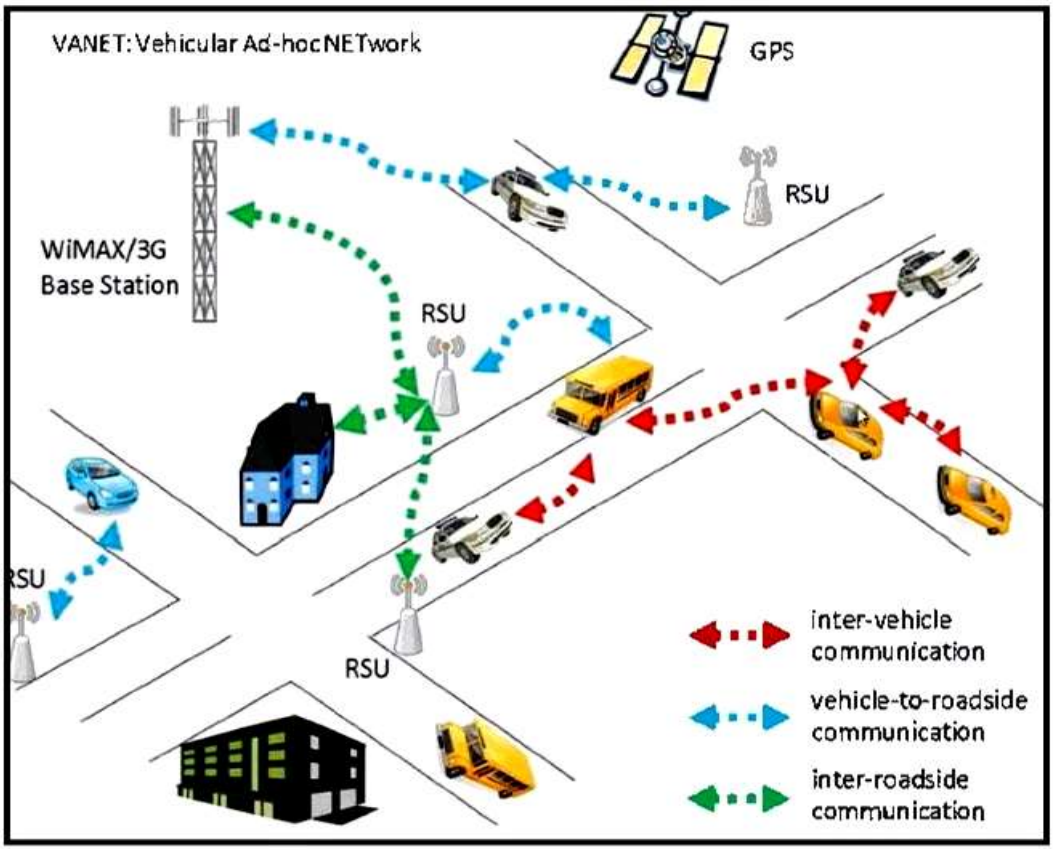

Fig 7.1: VANET Architecture

Vertex colouring graph are used to represent networks of communication, data organization, computational devices, the flow of computation, etc. For instance, the link structure of a website can be represented by a directed graph, in which the vertices represent web pages and directed edges represent links from one page to another. A similar approach can be taken to problems in social media, travel, biology, computer chip design, mapping the progression of neuro-degenerative diseases, and many other fields. The development of algorithms to handle graphs is therefore of major interest in computer science. The transformation of graphs is often formalized and represented by graph rewrite systems. Complementary to graph transformation systems focusing on rule based in-memory manipulation of graphs are graph databases geared towards transaction-safe, persistent storing and querying of graph-structured data. In this chapter

vertices colouring graph and Certificate Less Authentication Techniques (CLAT) used to find the nearby vehicle and signal carried to communicate V2V effectively. In this system three different types of RSU stations and twenty vehicle communications are used.

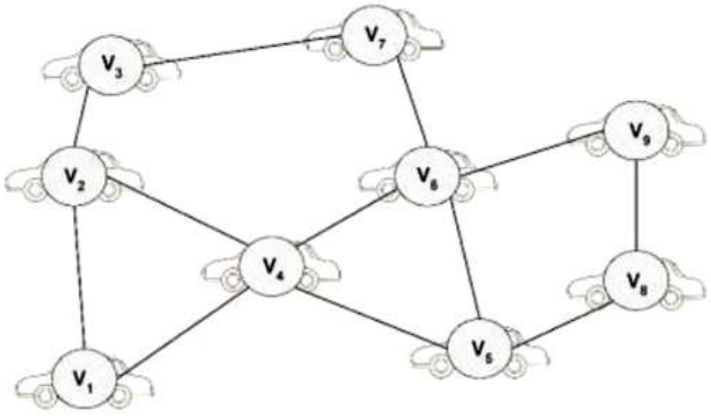

Fig 7.2: Evolving Vertex Colouring graph connectivity in VANETs

7.3 Need of vertex colouring graphs in vehicular ad-hoc networks

The main goal of VANET is to provide safety and security for citizens communicating with the drivers on the roads by informing about accidents or uncertainty conditions and traffic data. Each node or the vehicle is equipped with VANET device to form a Ad-hoc network instantaneously and can able to receive and broadcast the required messages through wireless network. The advantages of VANET are the safety driving, collision warning and exchanging of life critical warning messages using intelligent transport system equipped in vehicle which will make the driver aware of the situation and be safe.

The main motivation for vehicular communication systems is safety and eliminating the excessive cost of traffic collisions. According to World Health Organization (WHO), road accidents annually cause approximately 1.2 million deaths worldwide; one fourth of all deaths caused by injury. Also about 50 million persons are injured in traffic accidents. If preventive measures are not taken road death is likely to become the third-leading cause of death in 2020.

7.4 Vertex Colouring Graph based certificate less authentication techniques for Vanets [Yang, T et al., 2016]

It is really important to address the issue of unreliable links caused by vehicles in different speeds. The contributions are:

(i) A modified evolving Vertex Colouring Graph is modelled to display the unique properties of VANETs.

(ii) A link reliability value is calculated based on mathematical analysis of vehicular movements, their velocities and channel availability.

(iii) A novel and unique protocol called certificate less authentication techniques (CLAT) is developed using an evolving graph. New routes are discovered without the help of periodic beacons and it significantly reduces the overhead of a wireless channel.

A CLAT model is proposed for describing the VANET communication Colouring Graph. A new routing protocol is designed for reliable packet delivery among the vehicles. A strict routing constraint has to be followed when a route is searched from the source to the destination. As there should not be link failure, a new route discovery procedure is adopted so that the journey becomes valid and reliable. A new routing algorithm is used to find the most reliable journey and using the algorithm the route discovery procedure is designed for the proposed CLAT Reliable Graph Ad hoc routing protocol. The proposed algorithm has a database DB which has a collection of reliable data about all the vehicles and its associated most reliable value. It is collectively called as reliable data which is initialized as 1 for the source and for the other vehicles. The journey starts from the source vehicle and the other vehicles are unvisited at that current time instance. The reliability value is calculated from the source and the vehicle which has the most reliability value is chosen and is marked as visited. Thus, the process continues until it reaches the destination.

7.4.1 Proposed System

Security is one of the key issues in multicast group communication. Efficient message Prioritization for Rebroadcasting is proposed for message dissemination that will work efficiently in all types of network conditions. By exploiting multiple

keys the security can be enhanced. When a driver or a vehicle automatic system detects any problem in the vehicle or roadside, a message will be generated. This message will be distributed to all the nearby vehicles up to some target region. That incident may be any accident, break failure, traffic jam and weather conditions. Further, there is no optimal key management scheme. Proposed system, the security issues are addressed using the Diffie-Hellman method based Certificate Less Authentication Technique (CLAT) scheme. The process involved in the proposed CLAT scheme is depicted in Figure 7.3.

The overall flow of the proposed Certificate Less Authentication Technique (CLAT) scheme is shown in the figure 7.4. The key components of the proposed CLAT are as follows,

- Group key generation
- Generate Key (GK)
- Creation of Group Manager (GM)
- Encryption
- Decryption

7.4.2 Certificate less Authentication Technique (CLAT) Scheme for Addressing Vehicle Ad-Hoc Network

CLAT, key exchange algorithm is used for generating a shared secret between two vehicle thus provides a secure communication between them. Consider two vehicle say Alice, and Bob wants to share a secret key for using it in the symmetric cipher. But, there only means of communication is insecure because every piece of information is monitored by the attacker Eve.

By exploiting the key exchange mechanism a secure communication is provided between the users. In order to secure this group communication the Service Provider generates a set of session keys used for encrypting the contents to preserve secrecy. These session keys are changed when an existing user departs and new user joins the group. The forward and backward secrecy is achieved using re-keying phase. When compared to the existing methods, the energy consumption, privacy level, memory, key accuracy and time consumption of the proposed approach is optimal.

Implementation for developing the certificate less authentication technique uses network simulator tool 2.34. The algorithm will provide an optimal solution in VANET process in the real world and securely key pair communication manner.

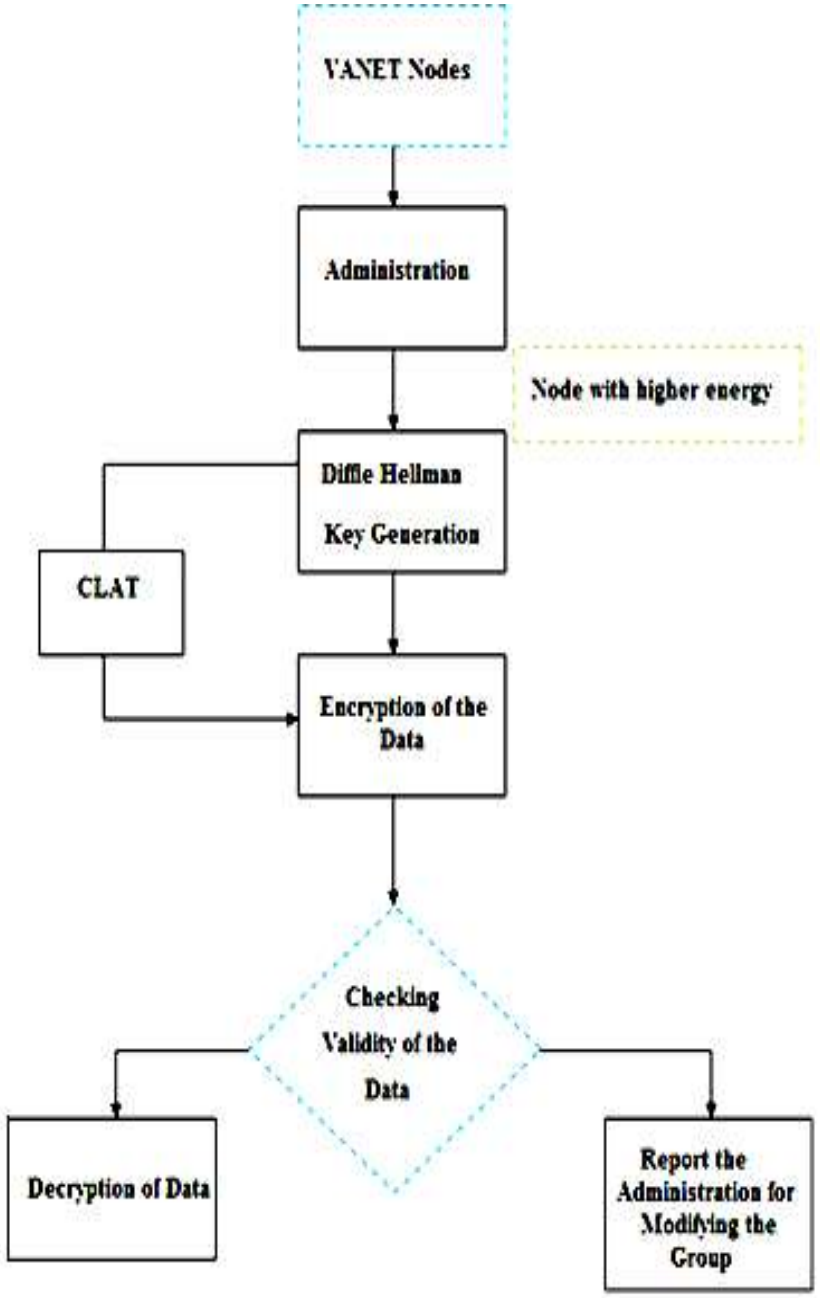

Fig 7.3 : Process involved in the CLAT scheme

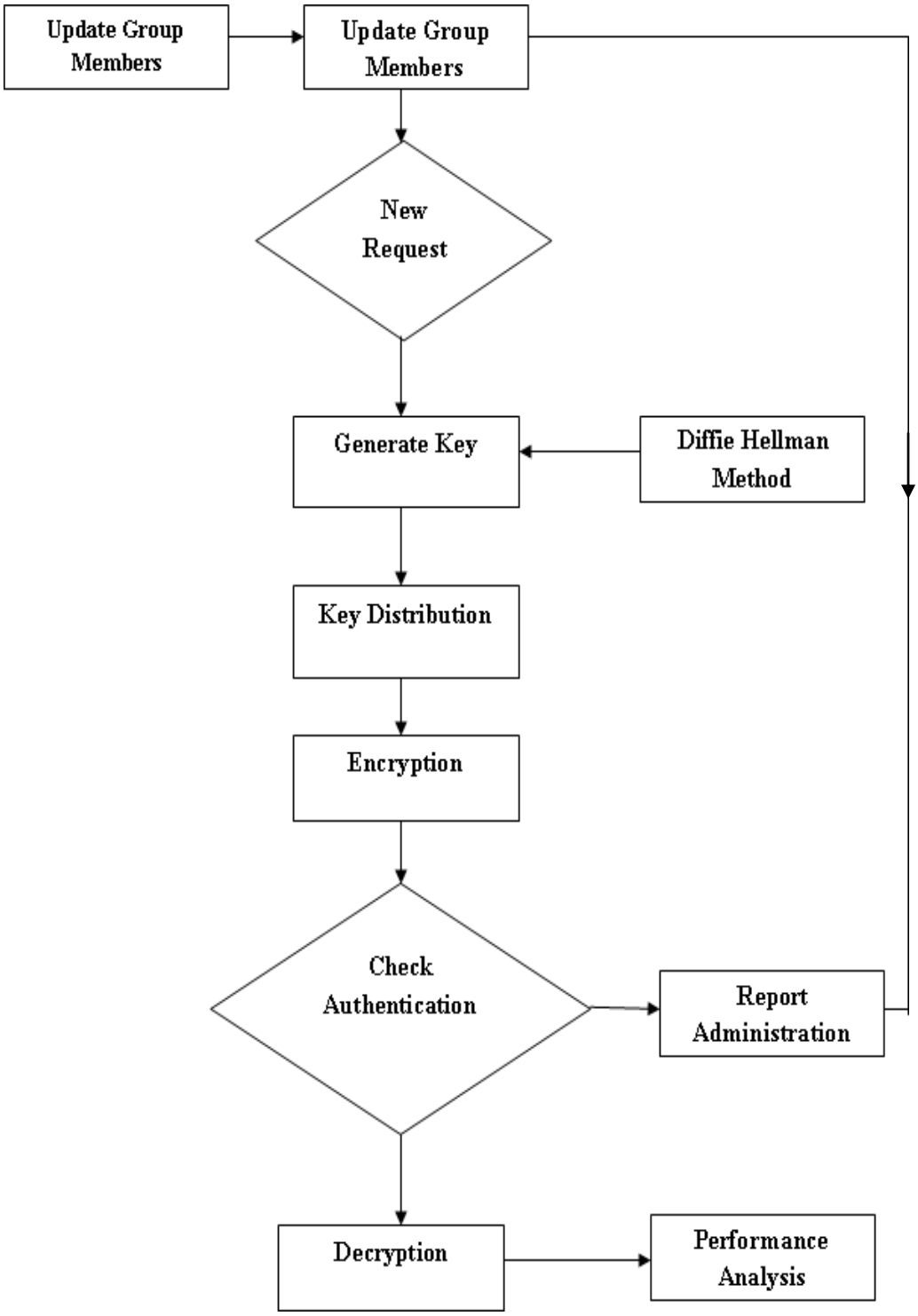

Fig 7.4: Overall flow of the proposed CLAT scheme

7.5 Result and Discussion

In this section, the performance of the proposed certificate less authentication technique (CLAT) scheme is validated. The simulation parameters used for the deployment of CLAT scheme is depicted in Table 7.1.

To analyze the performance of the proposed model, number of nodes, simulation time, area, number of keys and file size were used for evaluating classification results used for evaluating regression results. Certificate less authentication technique (CLAT) scheme was chosen to solve this problem.

Table 7.1: Parameters and values of CLAT VANET

Simulation Parameters	Specifications
Simulator	NS-2.34
Frequency	5.9 GHz
Channel model	Free space
Antenna type	Omni-directional
Transmission range (m)	300-1000
Vehicle density	10-50
Number of lanes/direction	1
Vehicle speed (m/s)	5-25 m/sec
Simulation time	1000 s
Beaconing interval	1/10 s
Packet size	512bytes
Simulation model	Random way point
Interface queue length	30
Interface queue type	Queue/Drop Tail/PriQueue
Routing Protocol	CLAT

7.5.1 Nodes Generation:

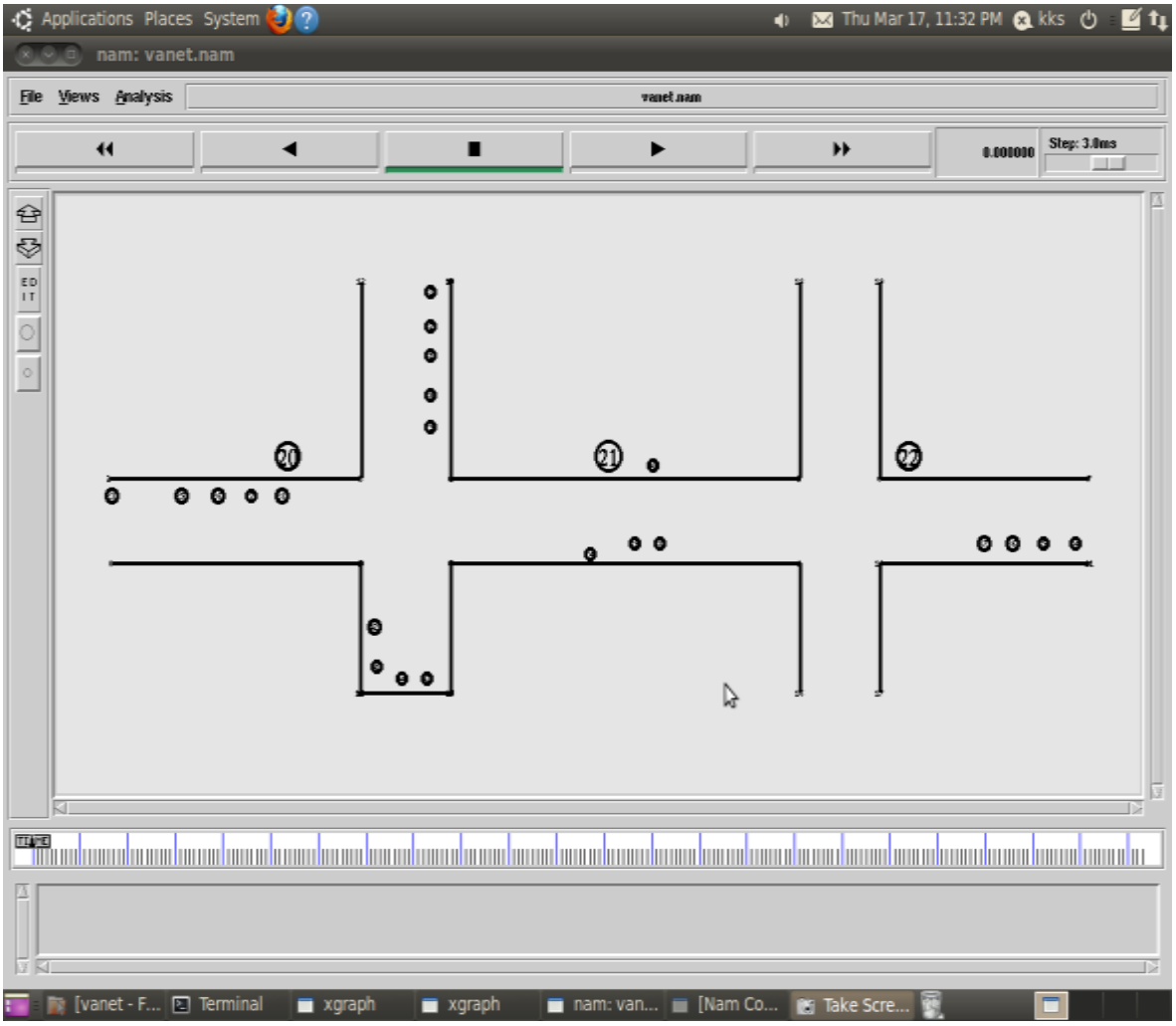

Fig 7.5: CLAT method based VANET node generation

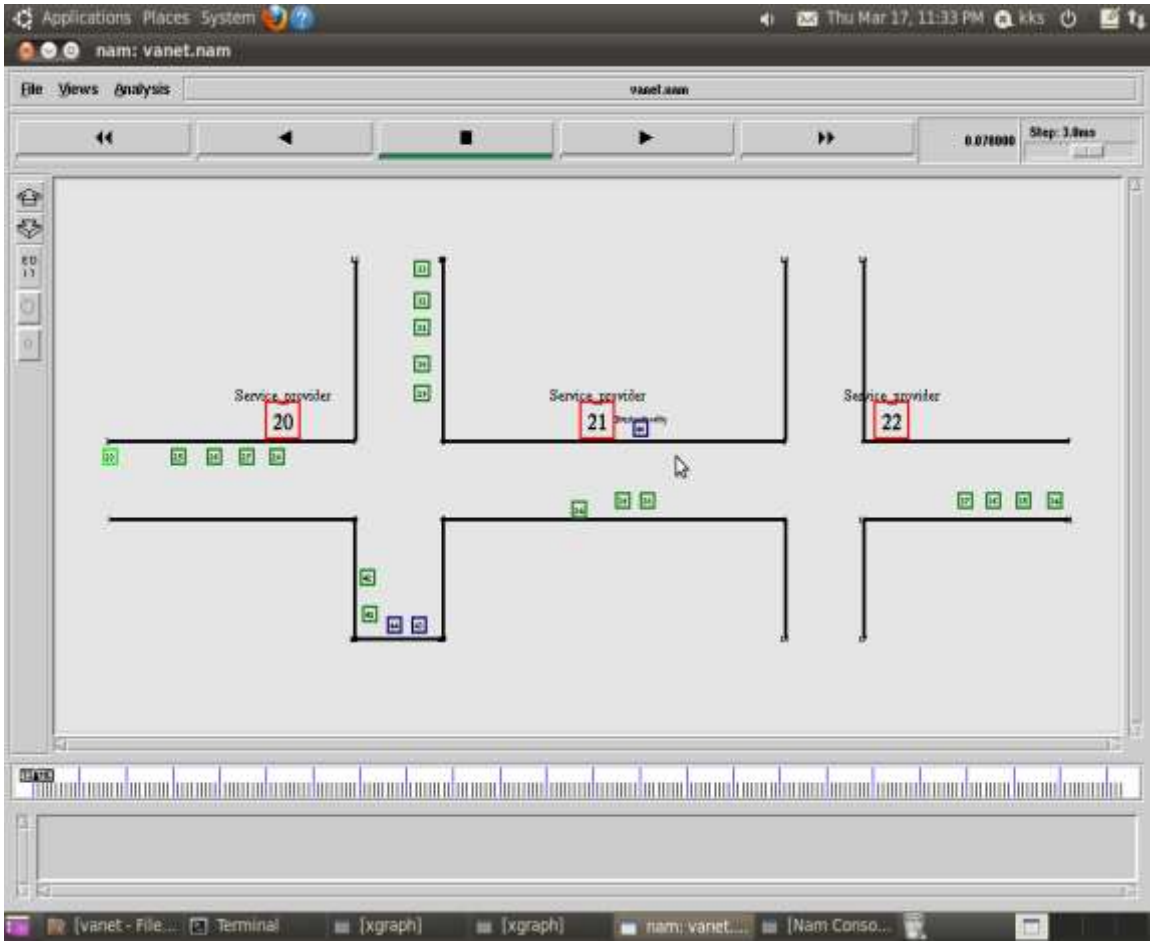

Fig 7.6: CLAT method based VANET node separation

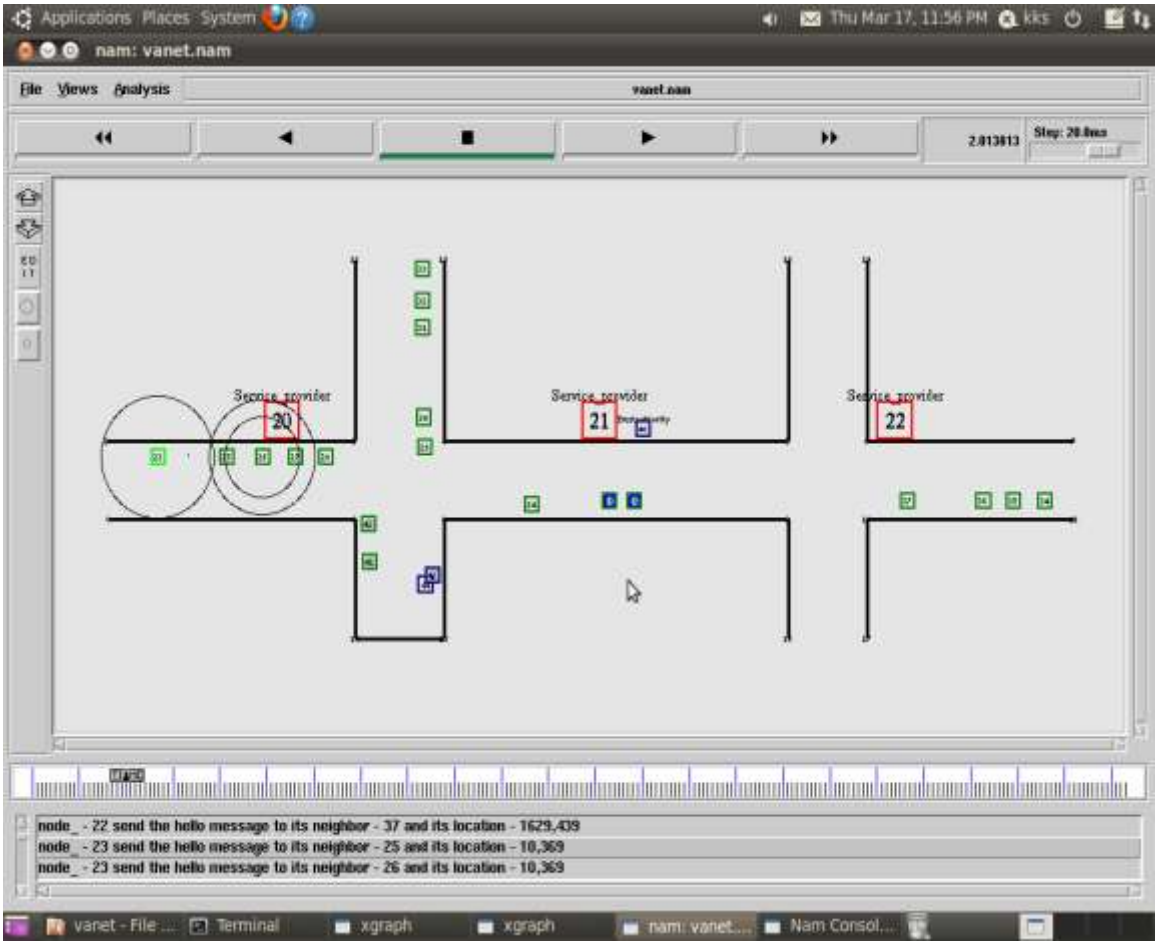

Fig 7.7: Creation of the Group Managers

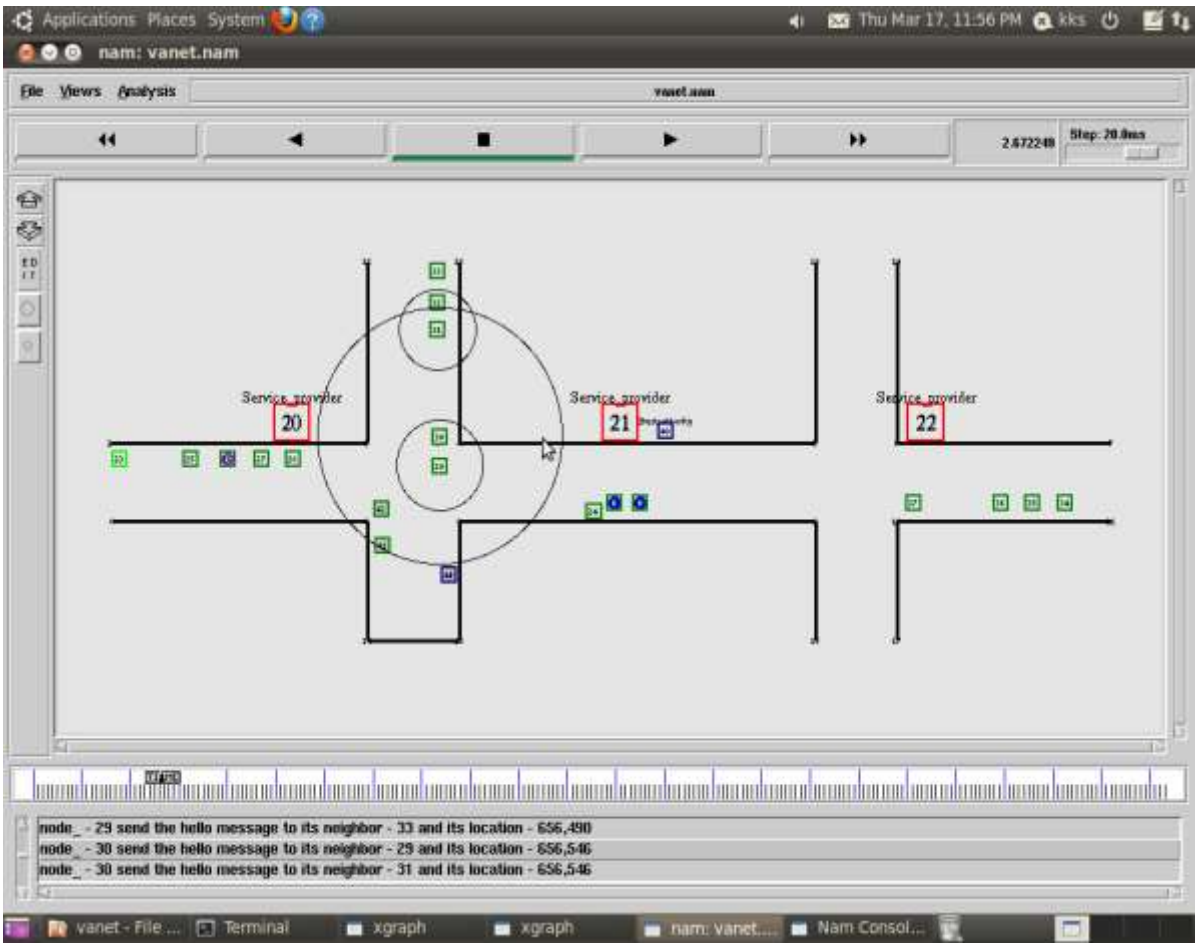

Fig 7.8: Node compromised and Investigates suspicious Node

Summary:

To obtain the discrimination of VANET node generation and separation based on number of nodes and defined area width in users are noticed with respect to the generated values as shown in the figures 7.5, 7.6, 7.7 and 7.8. The figures conclude the Roadside side unit considered (user define) if node disappears area for a certain period of time 30 seconds, the RSU must investigate the suspicious node.

7.5.2 Key Encryption:

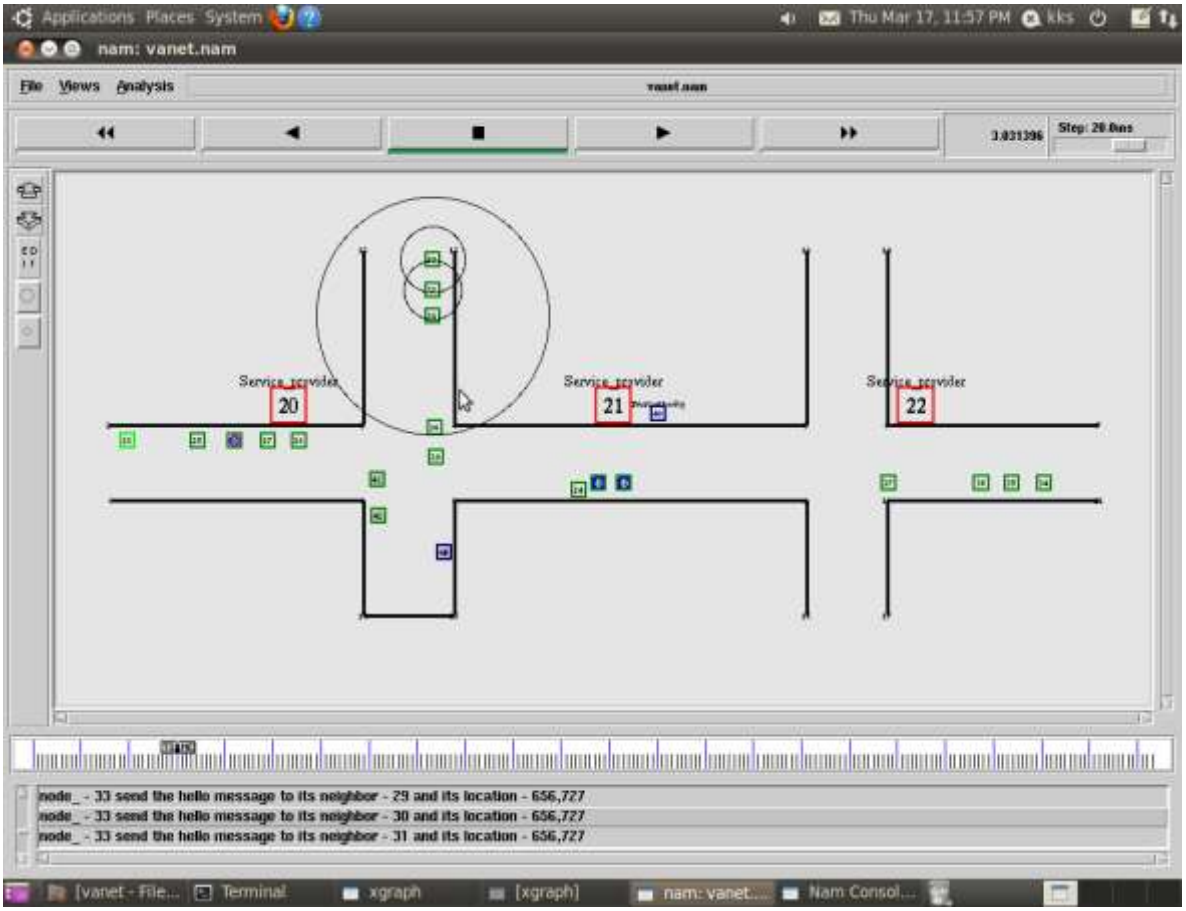

Fig 7.9: Establish the pair wise encryption

Summary:

To obtain the discrimination of VANET establish the Diffie-Hellman key encryption as shown in the figures 7.9. The figures conclude the Road side unit considered (user define) must investigate the suspicious node and establish the pair wise encryption with the random certificate less key values and legislative master certificate key (CLAT).

7.5.3 Key Decryption

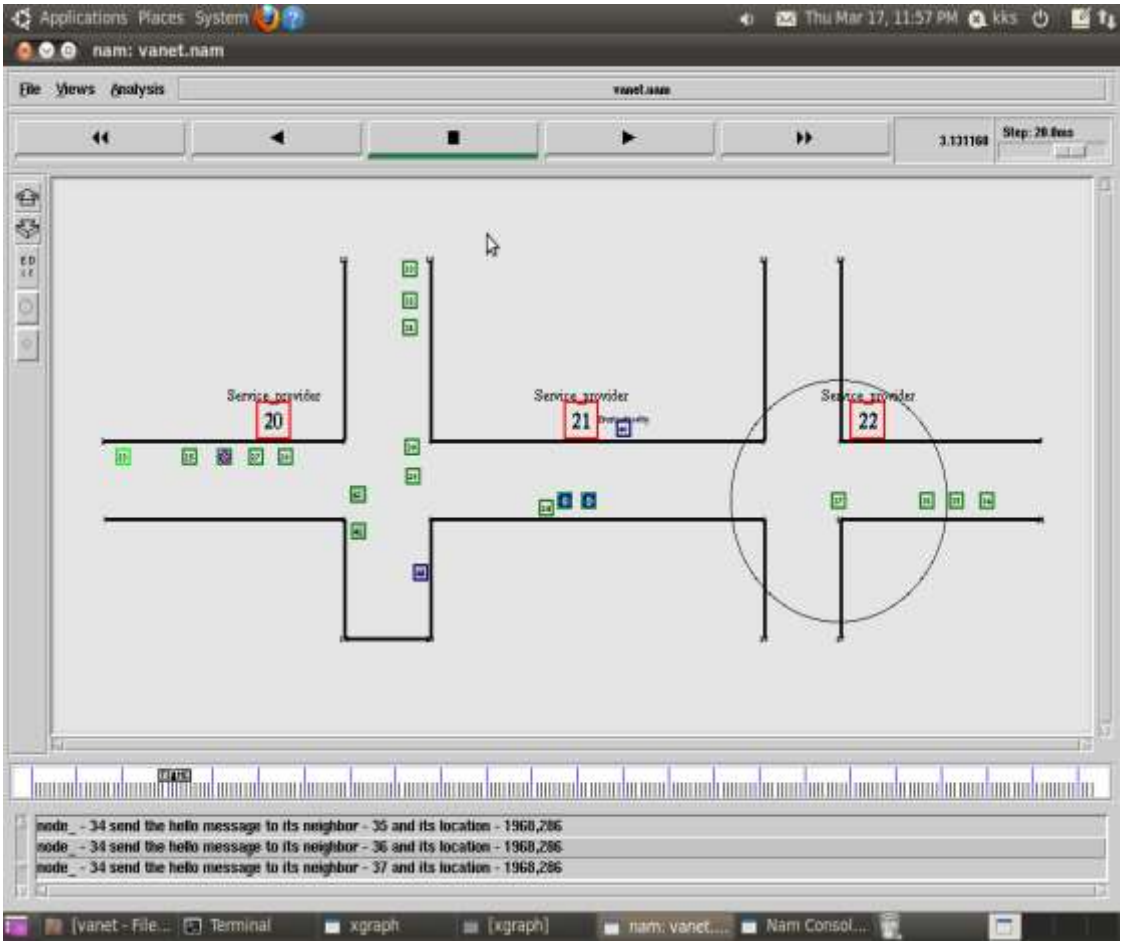

Fig 7.10: Key sharing node path generation

Summary:

To obtain the discrimination of VANET establish the Diffie-Hellman key decryption as shown in the figures 7.10. The figures conclude the Road side unit considered (user define) and node communication establish the pair wise decryption with the random certificate less key decryption and certificate key decryption (CLAT).

7.5.4 Key Exchange

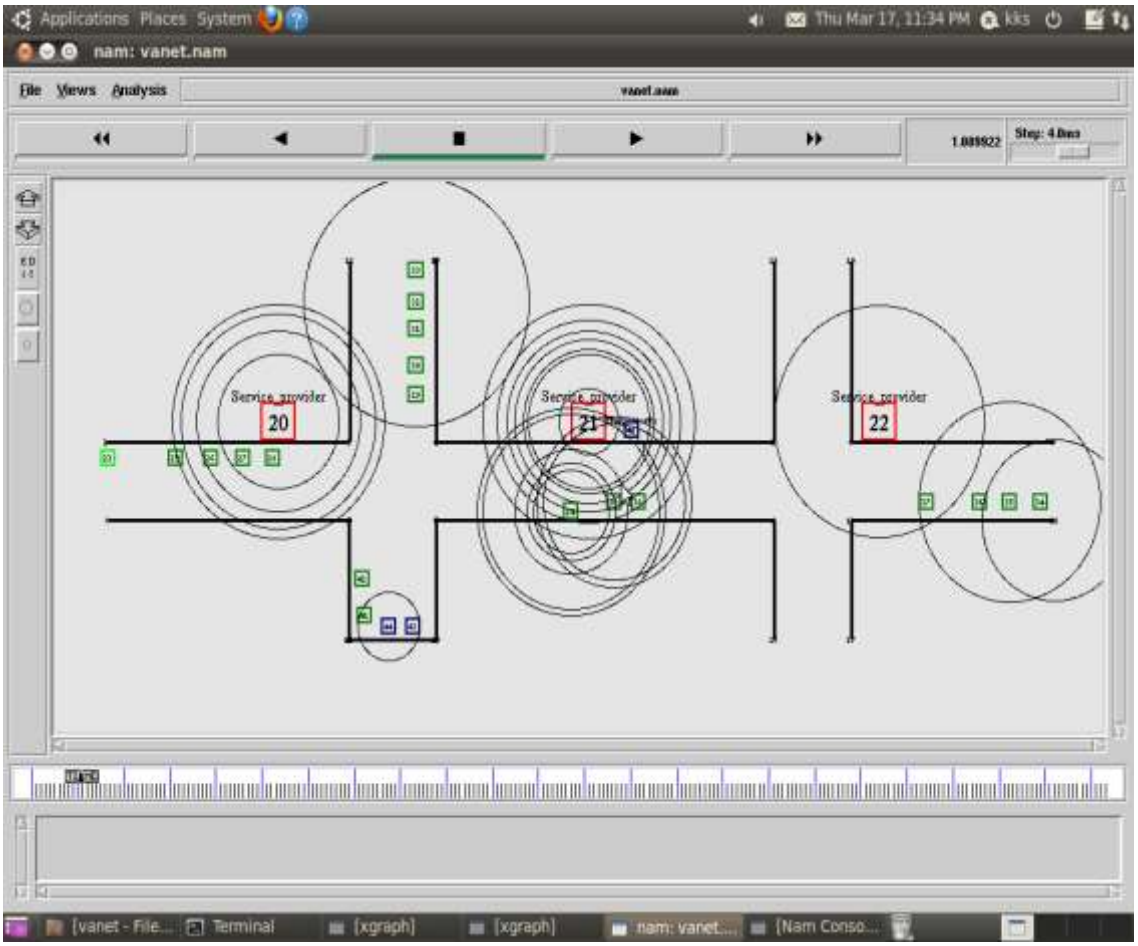

Fig 7.11: Key Pair Share through the Path

Summary:

To obtain the discrimination of VANET establish the Key Pair Share through the Path as shown in the figures 7.11. The figures conclude node to node communication key pair wise through the path, the pair communication communicate efficient to various nodes as user defined figure 7.7 to figure 7.10 explained nodes.

7.5.5 Road side event Identification

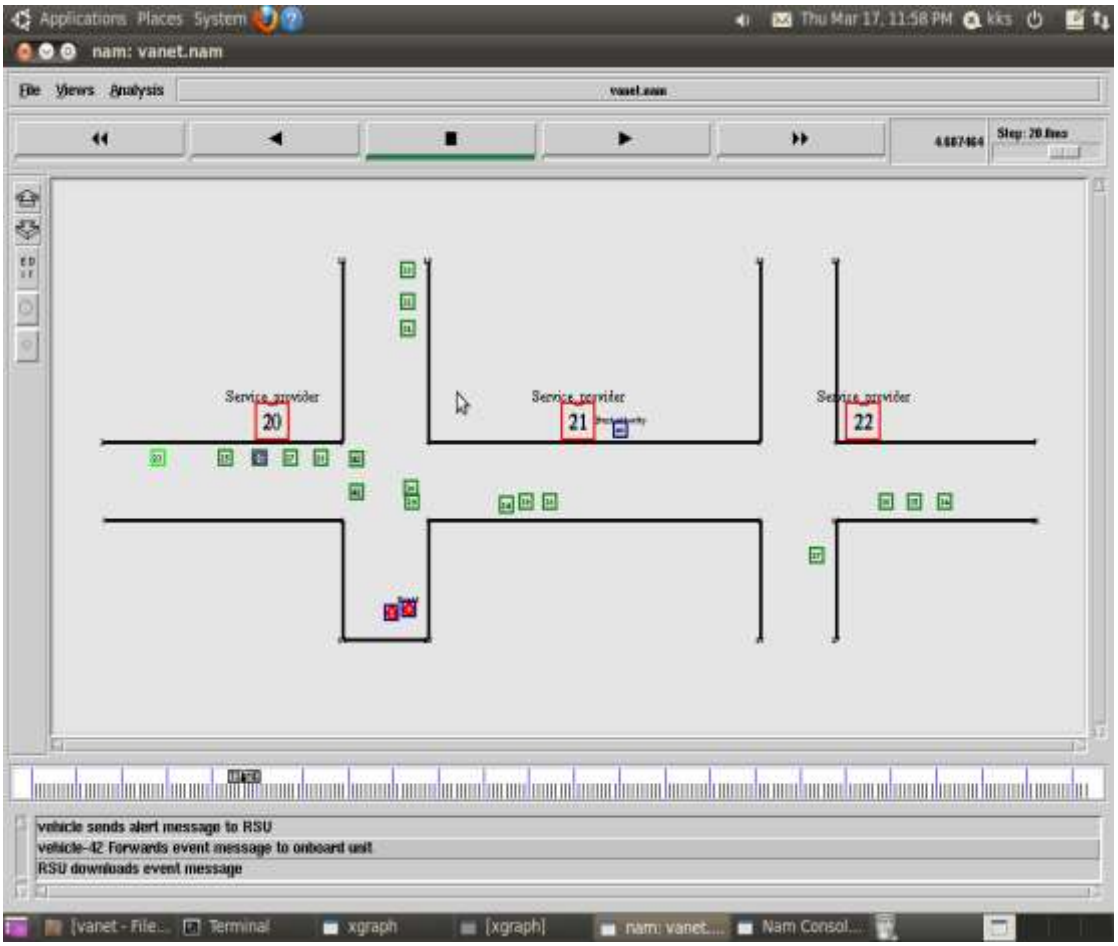

Fig 7.12: Vanet node detects the roadside event

Summary:

To obtain the discrimination of VANET establish the events occurred in the road as shown in the figures 7.12. The figures conclude the VANET node detected the unusual event in the road side and node forwards the event message to the onboard unit. Then the vehicle sends the alert message to the Road Side Unit (RSU) and finally RSU downloads the event message.

7.5.6 Message dissemination among the nodes

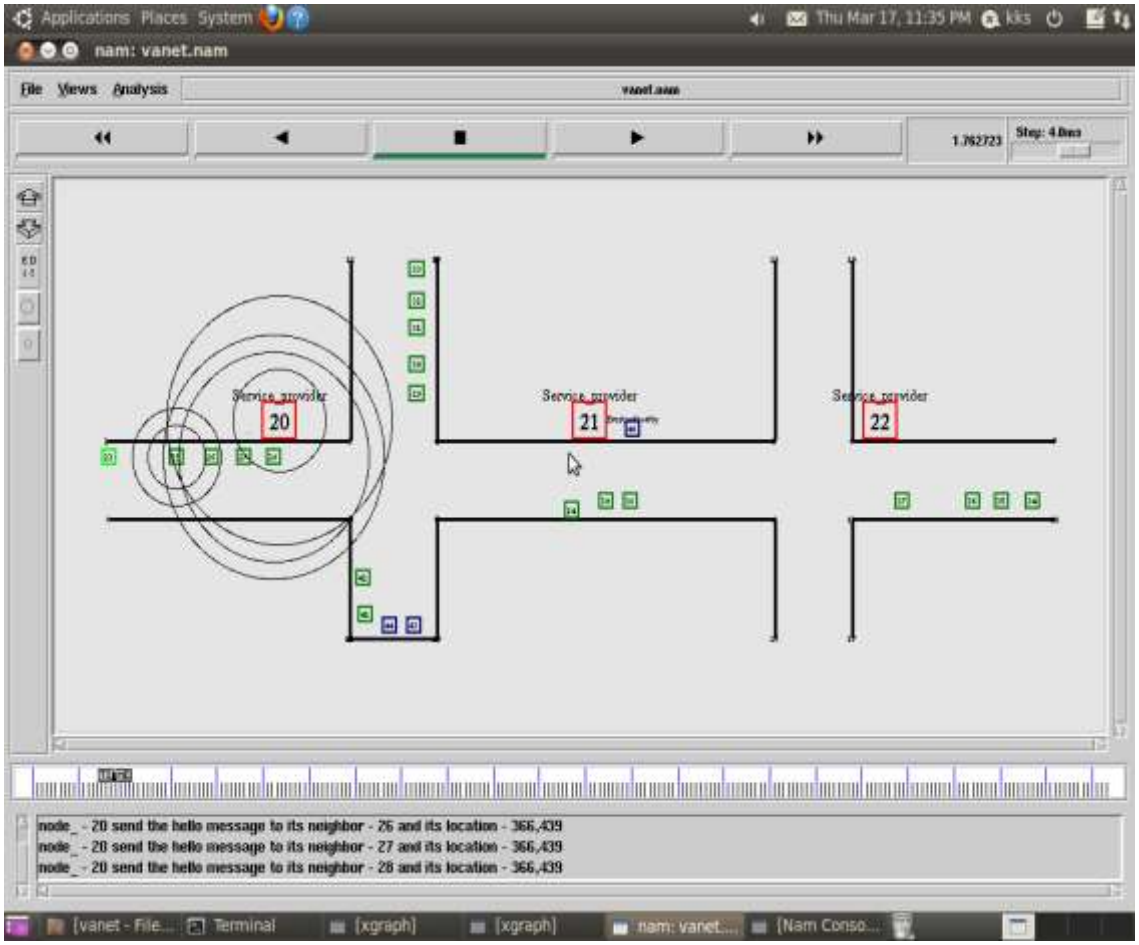

Fig 7.13: RSU1 disseminates the alert messages to its communication range.

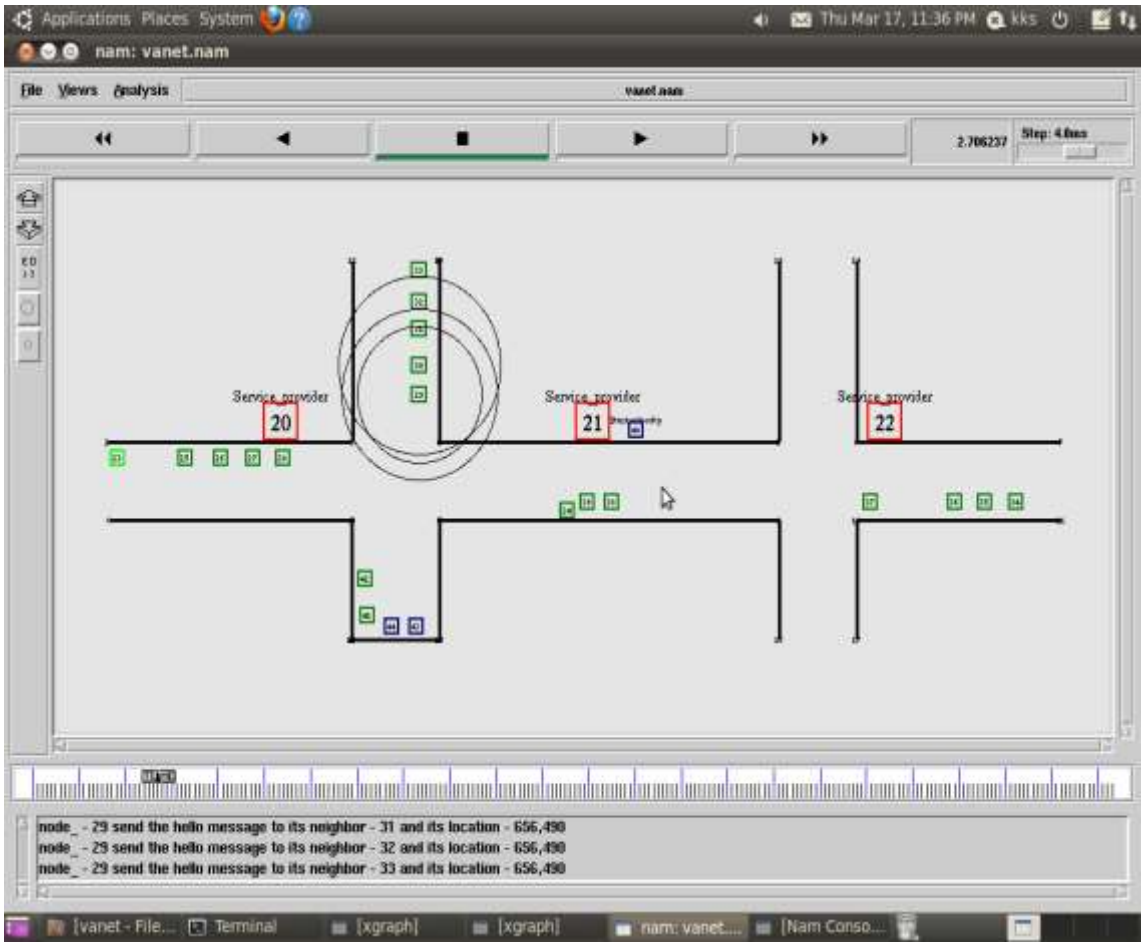

Fig 7.14: VANET nodes disseminates the alert messages to the nearest nodes

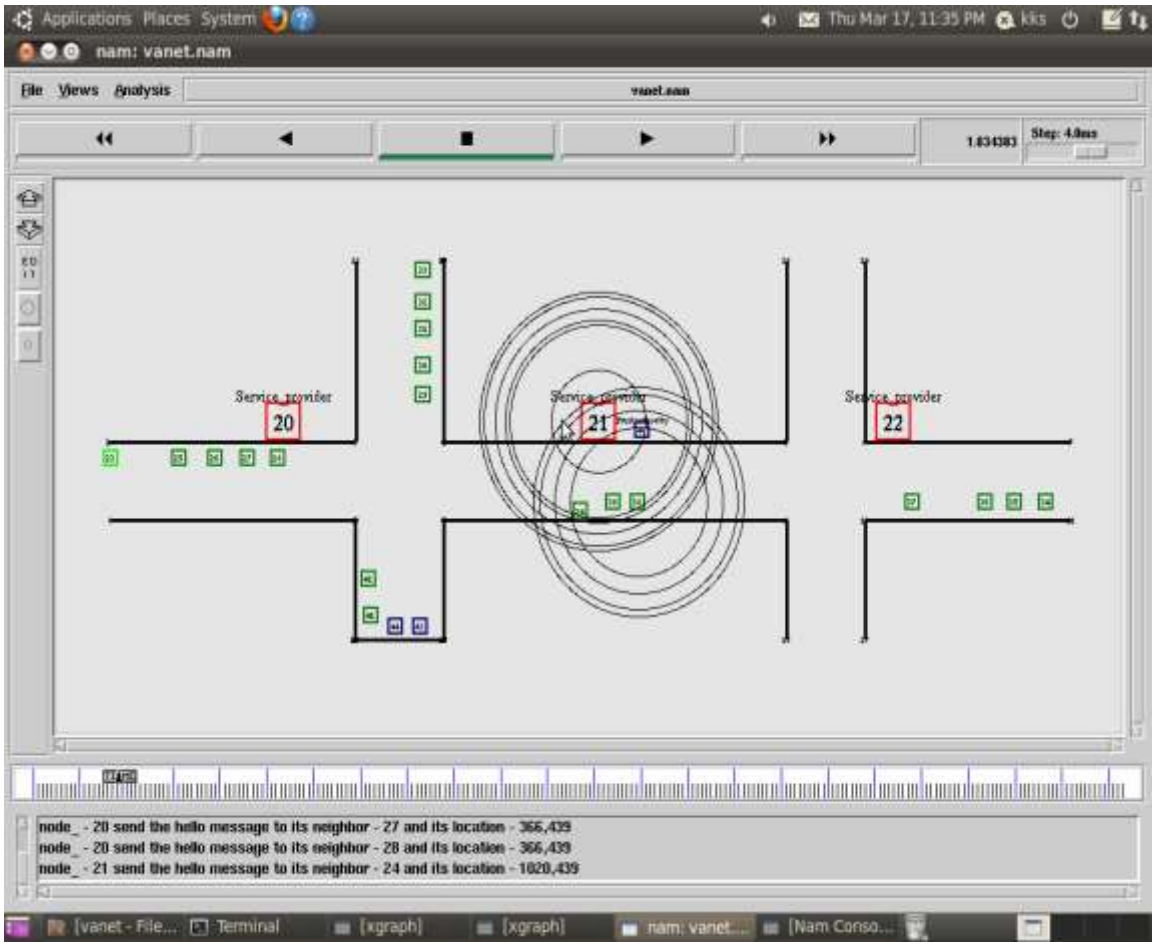

Fig 7.15: RSU2 disseminates the alert messages to its communication range from RSU1

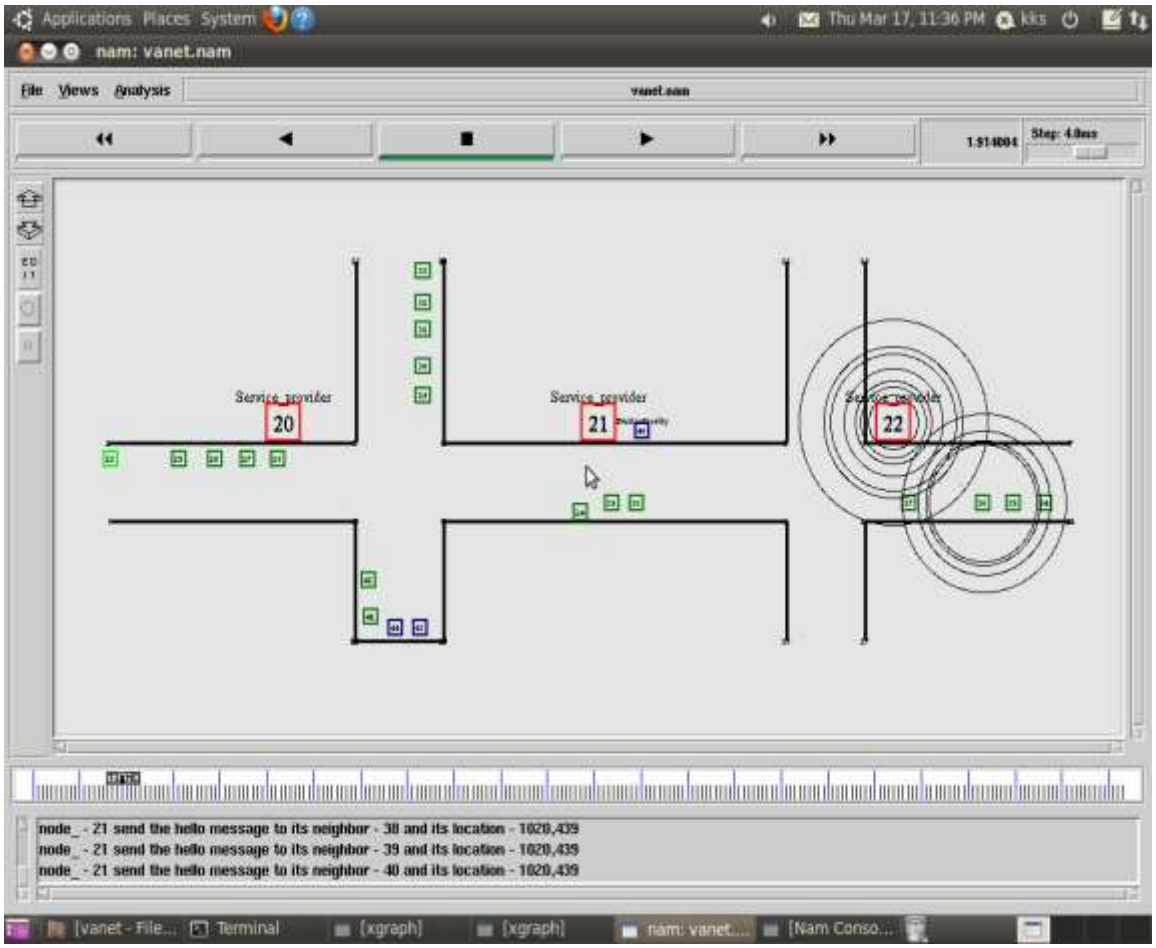

Fig 7.16: RSU3 disseminates the alert messages to its communication Range from RSU2

Table 7.2: Communication of nodes through RSU

Figure number	VANET Communication nodes	Road Side Unit
Figure 7.11	37, 36, 35, 34	RSU3
Figure 7.12	23,25,26,27,28,41,43,42,21,22,23 24,29,31,32,33	RSU2, RSU1
Figure 7.13	23,25,26,27,28	RSU1
Figure 7.14	29,30,31,32,33	RSU1
Figure 7.15	24,38,39	RSU2
Figure 7.16	37,36,35,34	RSU3

Summary:

To obtain the discrimination of VANET establish the Key Pair Share through the Path as shown in the table 7.2. as in the figure 7.11 and figure 7.12 The alert message disseminated to nearest nodes through the different Road side unit (RSU) is shown in the table 7.2 as in the figure 7.14 to figure 7.16. The node 42 identifies the unusual event along the road side and transmitted the event message to the nearest RSU as shown in the figure 7.13.

Nature of the evolving graph model

The evolving graph theory is a strict generalization for active networks and a Method of time evolution in a formal way [Elaraby, S et al., 2021]. Figure 7.17 represents the colouring graph connectivity in VANETs and explains the table 7.2 V2V communication for each and every vehicle with three different road side unit (RSU). There can be more than one route from the source to the destination and choosing the most optimal route is a big task also It is demonstrated that the inter-data relationship is greatly simplified in the MST representation. A vertex colouring of a graph G (using colours 1,2,...,k) is a colouring of the vertices of G such that (i) three neighbours have various colours (RSU1- Blue, RSU2- Orange, RSU3-Green) and (ii) for each colour vehicle there exists a communicate vertex which is adjacent to all other k-1 colour vehicles with any continues route.

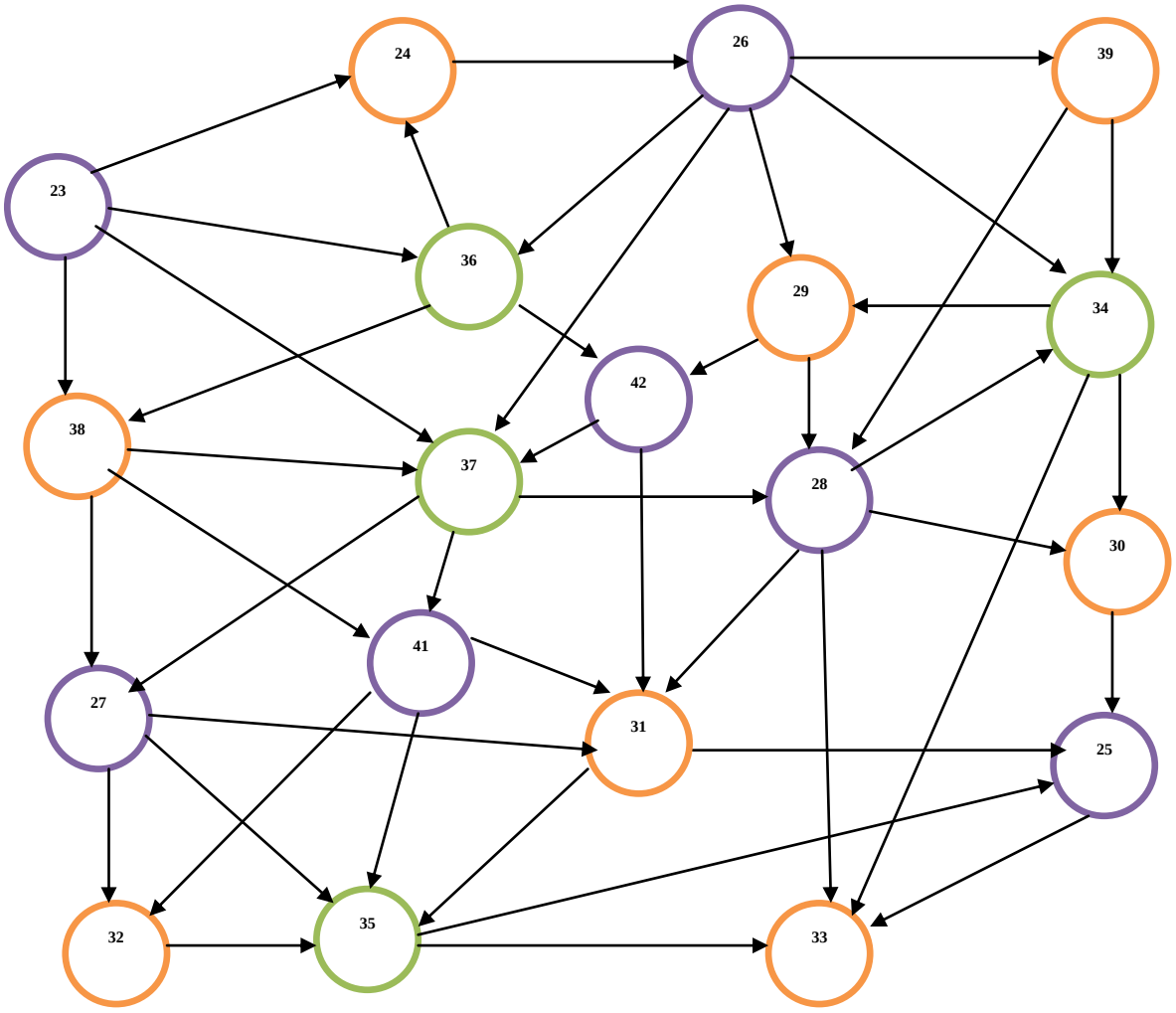

Fig 7.17: Vertex Colour Graph for communication of nodes through RSU

7.5.7 Vanet node communications

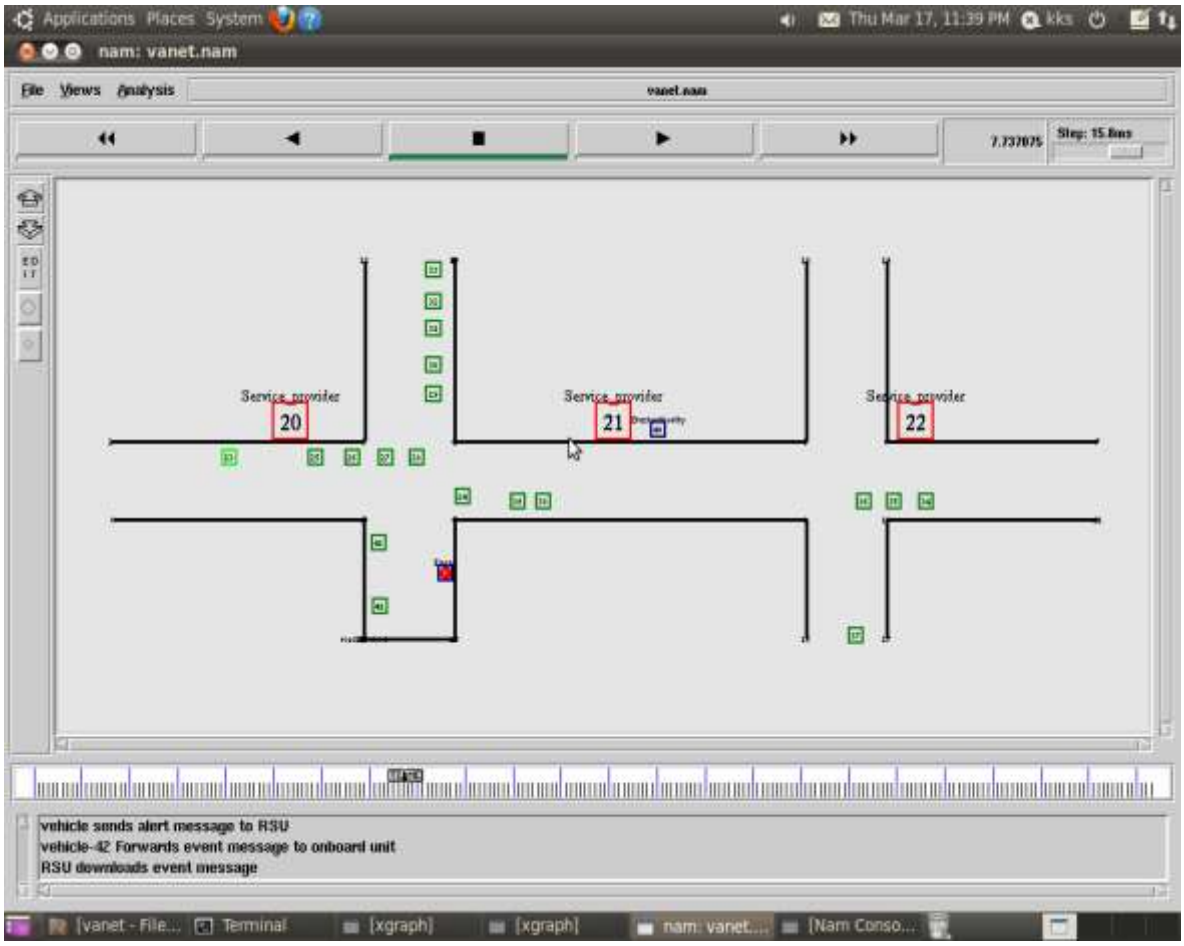

Fig 7.18: Alert message exchanges between the VANET nodes 41-42-24

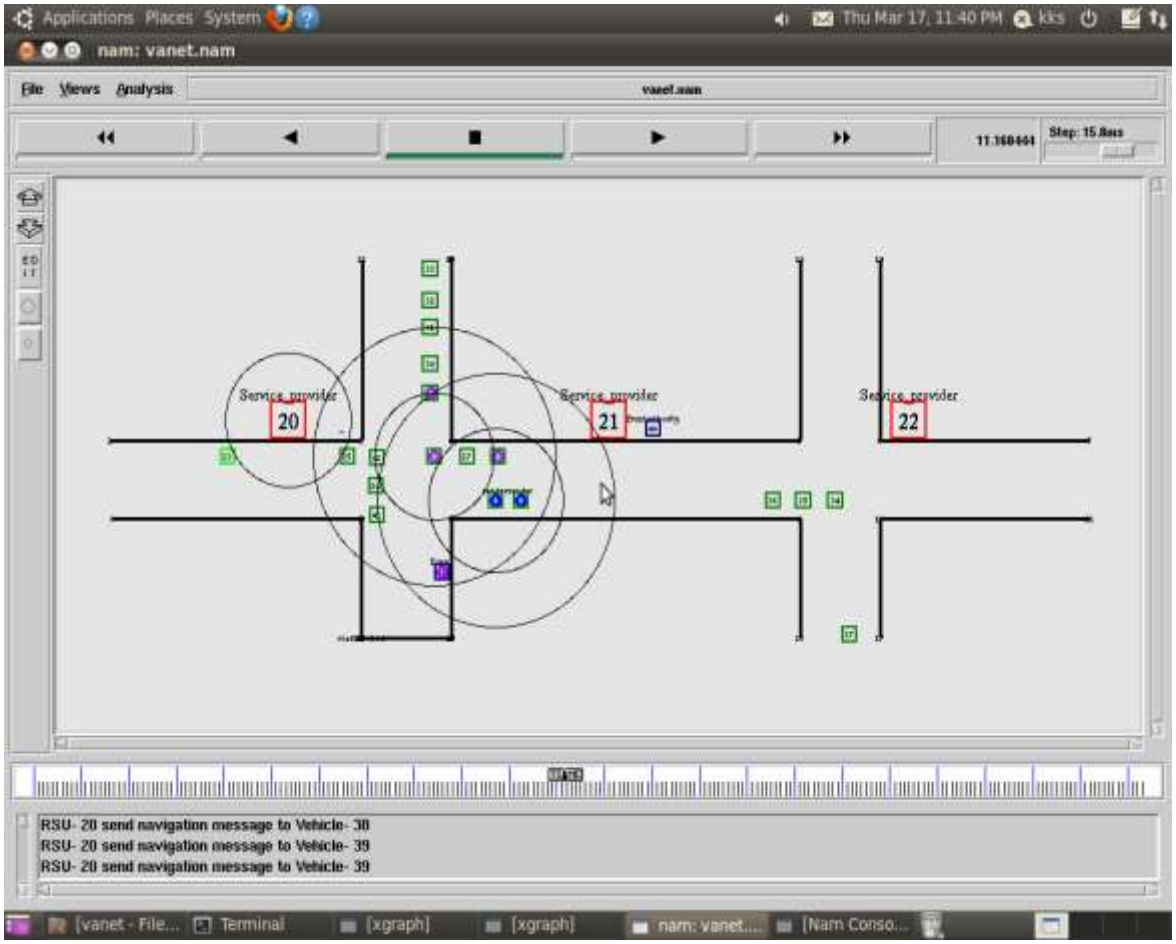

Fig 7.19: Communication of nearest nodes in the network topology

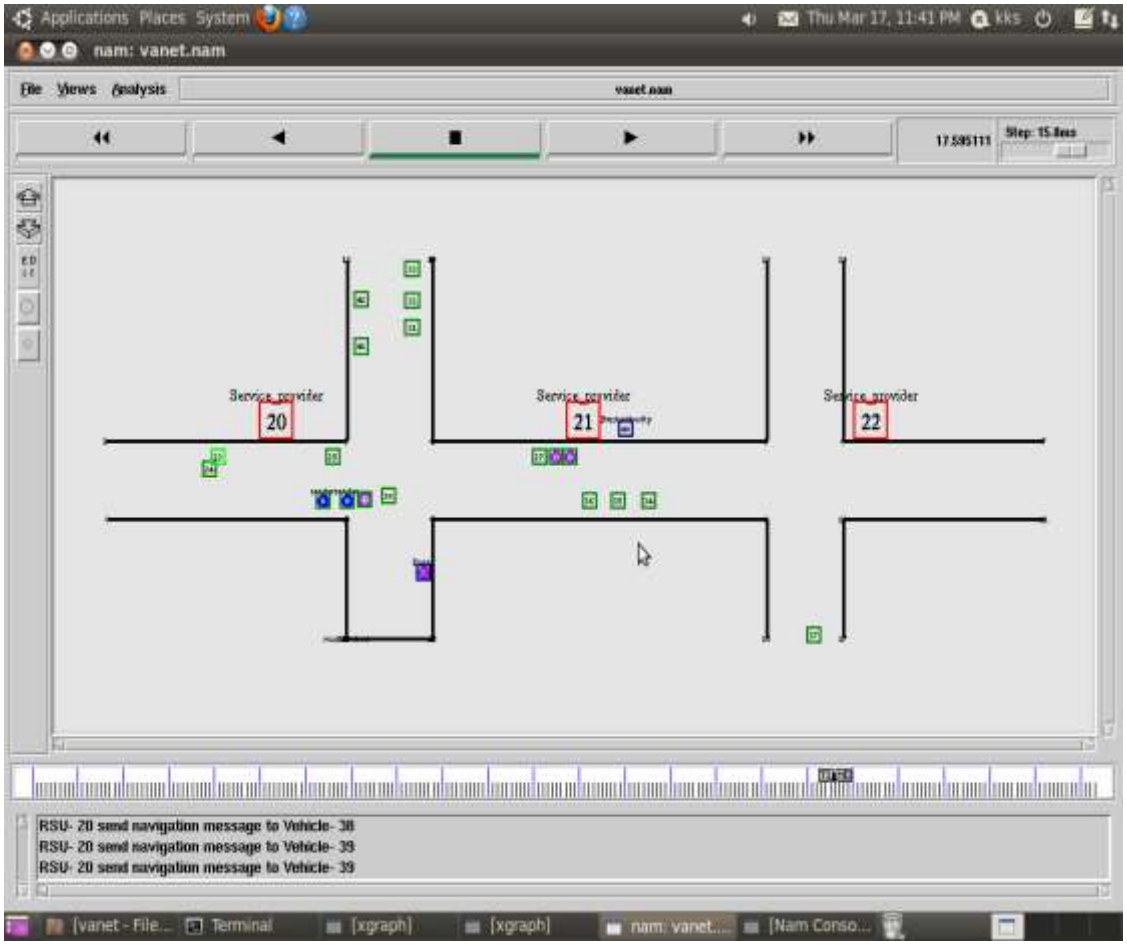

Fig 7.20: Nodes moving in the safe directions after communicating with nearest nodes

Table 7.3 Communication between the nodes

Figure Number	VANET Communication Nodes	Coverage
Figure 7.18	43	RSU1
Figure 7.19	23,25,26,27,28,41,43,42,21,22,23 24,29,31,32,33	41-42-24
Figure 7.20	23,25,26,27,28,41,43,42,21,22,23 24,29,31,32,33, 37,36,35,34	RSU1,2,3

Summary:

To obtain the discrimination of VANET establish the communication through the Path as shown in the table 7.3 as in the figure 7.18 and figure 7.19. When the node 43 indentifies the events along the road side, initially it will communicate with the nearby nodes and transmit the security message after the verification of the key pairs. If the key value pair doesn't matched the security message will not be sent. After receiving the alert message from the neighbour nodes, the nodes in the topology had started to move in the safe directions as shown in the figure 7.20.

Figure 7.21 represents the colouring graph connectivity in VANETs and explains the table 7.3 V2V communication for each and every vehicle with three different road side unit (RSU). Three neighbours have various colours (Road Side Unit1- Blue, Road Side Unit2- Orange, Road Side Unit3-Green) and (ii) for each colour vehicle there exists a communicate vertex which is adjacent to all other k-1 colour vehicles with any continues route [Yang, T et al 2016].

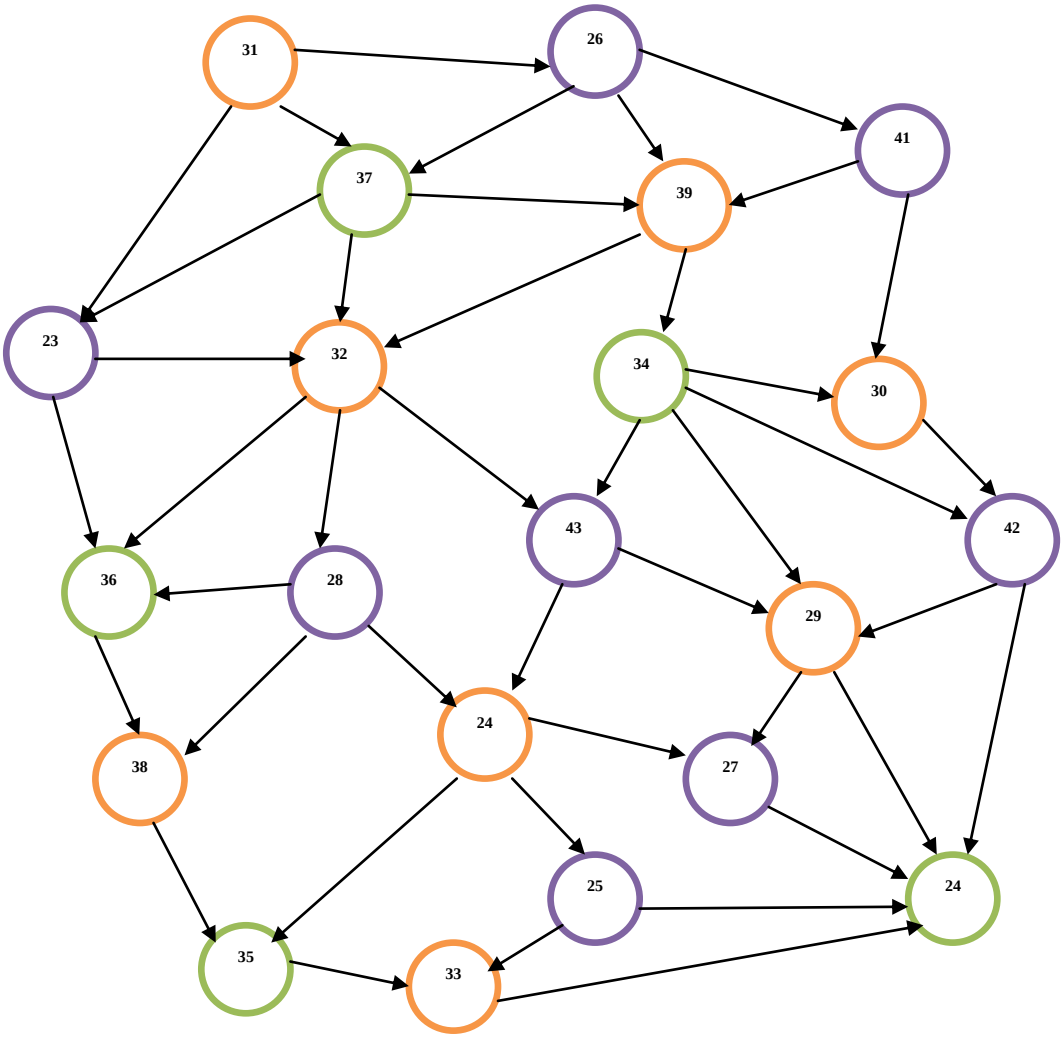

Fig7.21: Vertex Color Graph for communications between the nodes

7.6 Performance Evaluation

The performance of CLAT method was compared with that existing algorithm Chinese remainder theorem (CRT). Prediction results of the NETWORK SIMULATOR and statistical analysis comparisons are shown in Figure 7.22, 7.23 and table 7.24.

Figure 7.22 comparative differences of alert message dissemination between the certificate less authentication technique (CLAT) and Chinese remainder theorem (CRT), figure 7.23 pocket size (kb) vs Pocket delivery ratio and figure 7.24 numbers of nodes vs energy consumption in joules.

Comparatively proposed CLAT algorithm improves and compared for Chinese remainder theorem (CRT) in various parameters like alert message dissemination, Pocket delivery ratio, number of nodes vs. energy consumption in joules). Based on the result algorithms are ranked as CLAT and CRT.

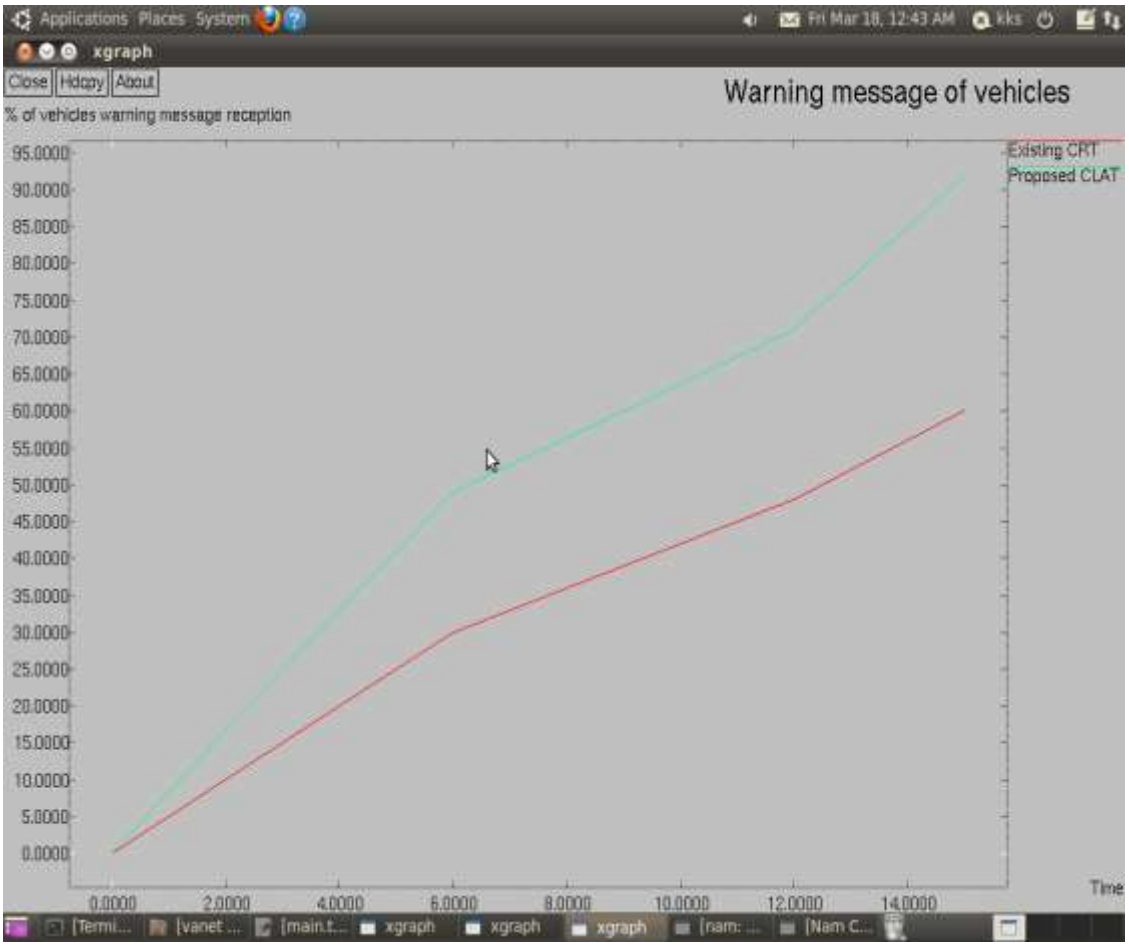

Fig 7.22: Alert message dissemination comparison results for CRT and CLAT algorithms

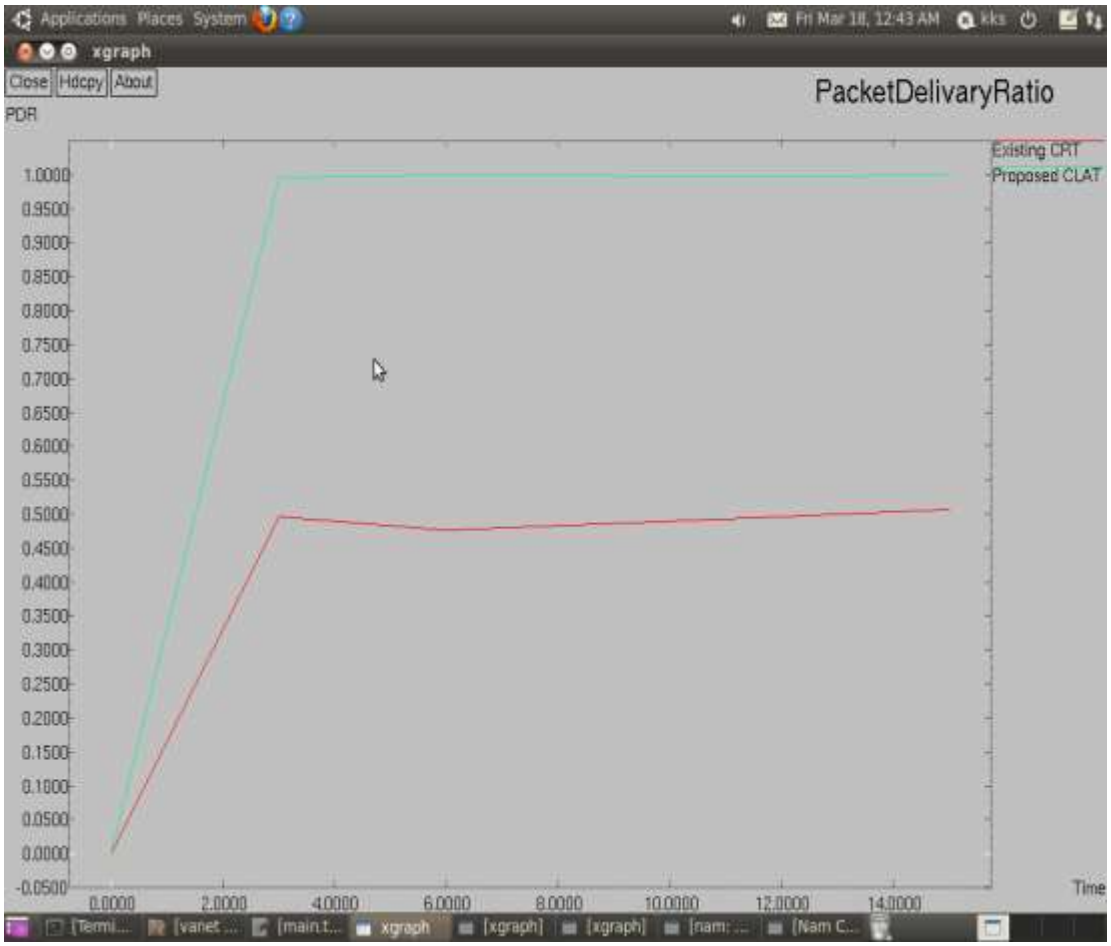

Fig 7.23: Packet delivery ratio comparison result for CLAT and CRT algorithms

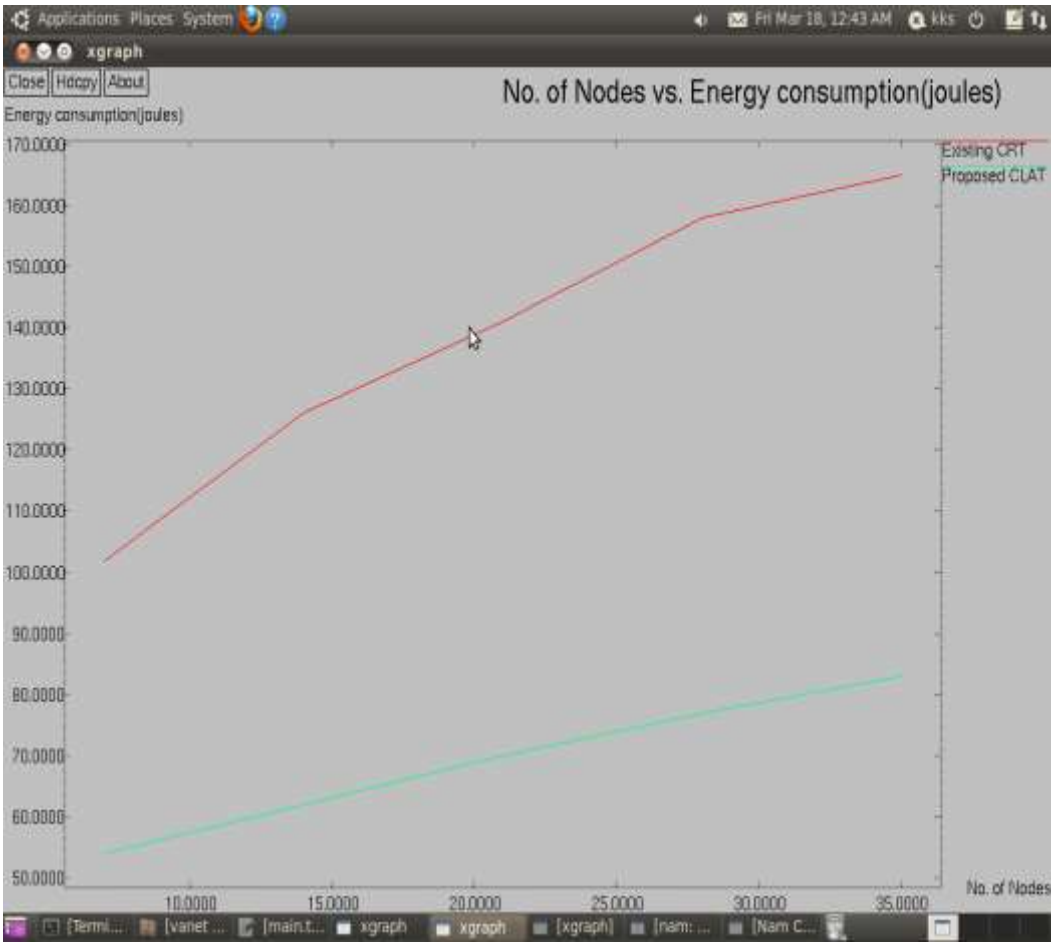

Fig 7.24: Number of nodes vs. energy consumption comparison result for CLAT and CRT algorithms

Summary

Nowadays, VANETS are being developed with improvements in wireless communication technology. However, as those applications have impact on road traffic safety, strong security requirements should be taken care of to provide a satisfactory performance in the network. New mechanisms have to be developed for dealing with the inherent features of these networks such as dynamic speed of the nodes, decentralized infrastructure, etc., VANET is an emerging research area with a promising future as well as great challenges especially in its security. Security is the major issue in VANET considering many new types of attacks being generated.

This chapter has dealt with the investigations on security approaches towards establishing a trusted communication in VANETs using Vertex Colouring graph. The challenges and issues with respect to Authentication, Confidentiality and reliability related to the operation of VANETs have been studied.

CLAT with Vertex Colouring graph being promising techniques for the architecture of the VANET, it is important to address its mobility in face of increased delay when considering real-time applications with strict delay requirements. Existing CRT method consume the long time to solve huge network problem, with an approach of using Certificate Less Authentication Technique (CLAT). The proposed algorithm exploits both the secret key, and group key for encrypting the message. Once the messages are encrypted, the validity of the message is checked. If the message is authentic, the message is decrypted; else, the group member updation process is performed. The comparison of performance for the existing CRT and the proposed CLAT schemes prove that the proposed CLAT with Vertex Colouring graph scheme minimizes the throughput, pocket size (kb), Pocket delivery ratio, number of nodes and energy consumption in joules.