LOVELY PROFESSIONAL UNIVERSITY

Efficient Scheme for Preventing Tunneling Attack in Vehicular Ad Hoc Networks

A Dissertation submitted
by

KOMAL
To

Department of Computer
Science and Engineering

In partial fulfilment of the Requirement for the

Award of the Degree of

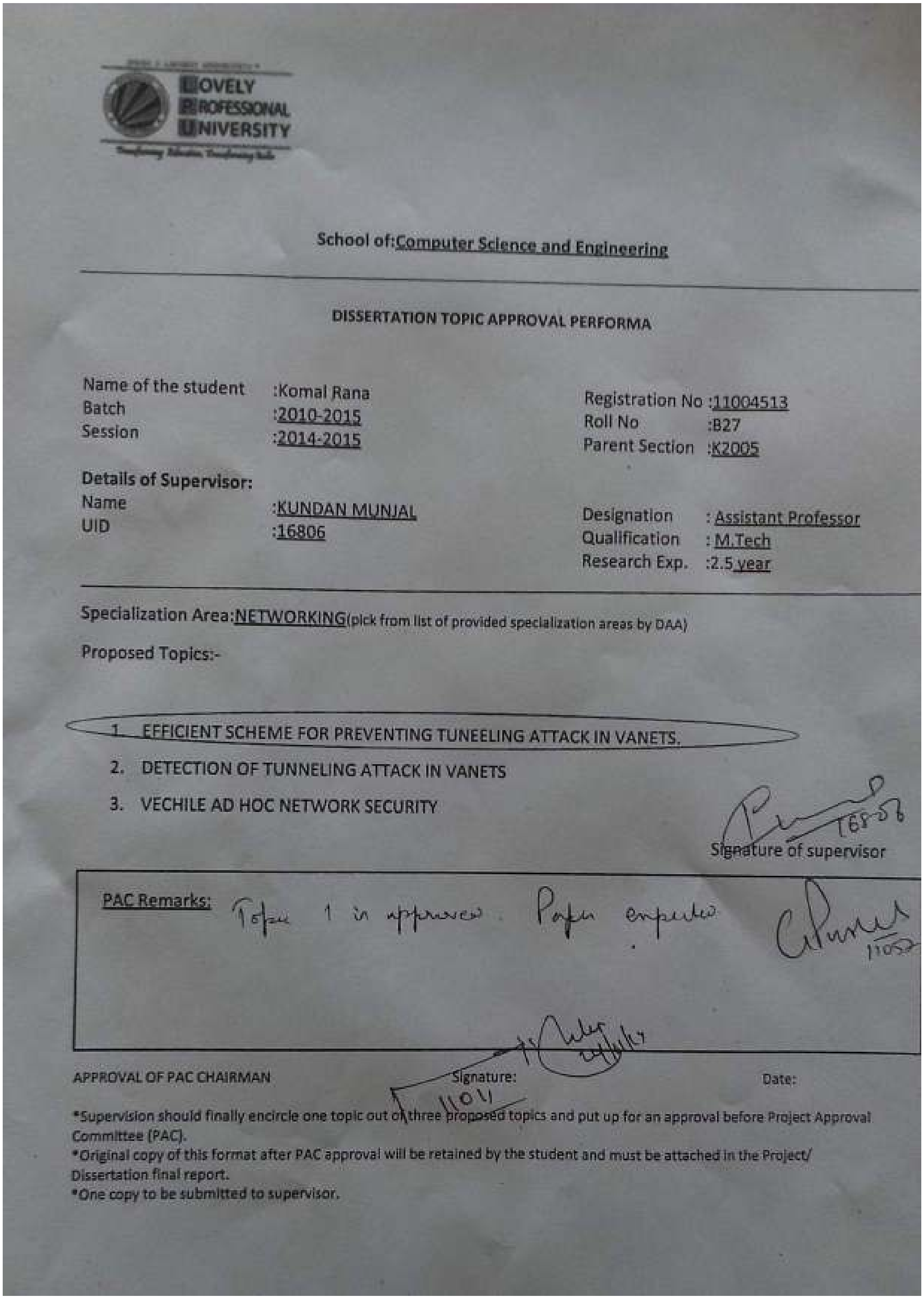
Master of Technology in
Computer Science and Engineering

Under the guidance of
MR. KUNDAN MUNJAL

Asst.Professor, Lovely Professional University

May, 2015

PAC Form



LOVELY PROFESSIONAL UNIVERSITY

School of:Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the student :Komal Rana
Batch :2010-2015
Session :2014-2015

Registration No :11004513
Roll No :B27
Parent Section :K2005

Details of Supervisor:
Name :KUNDAN MUNJAL
UID :16806

Designation : Assistant Professor
Qualification : M.Tech
Research Exp. :2.5 year

Specialization Area:NETWORKING(pick from list of provided specialization areas by DAA)

Proposed Topics:-

1. EFFICIENT SCHEME FOR PREVENTING TUNEELING ATTACK IN VANETS.
2. DETECTION OF TUNNELING ATTACK IN VANETS
3. VECHILE AD HOC NETWORK SECURITY

16858
Signature of supervisor

PAC Remarks: Topic 1 is approved. Paper expected.
11057

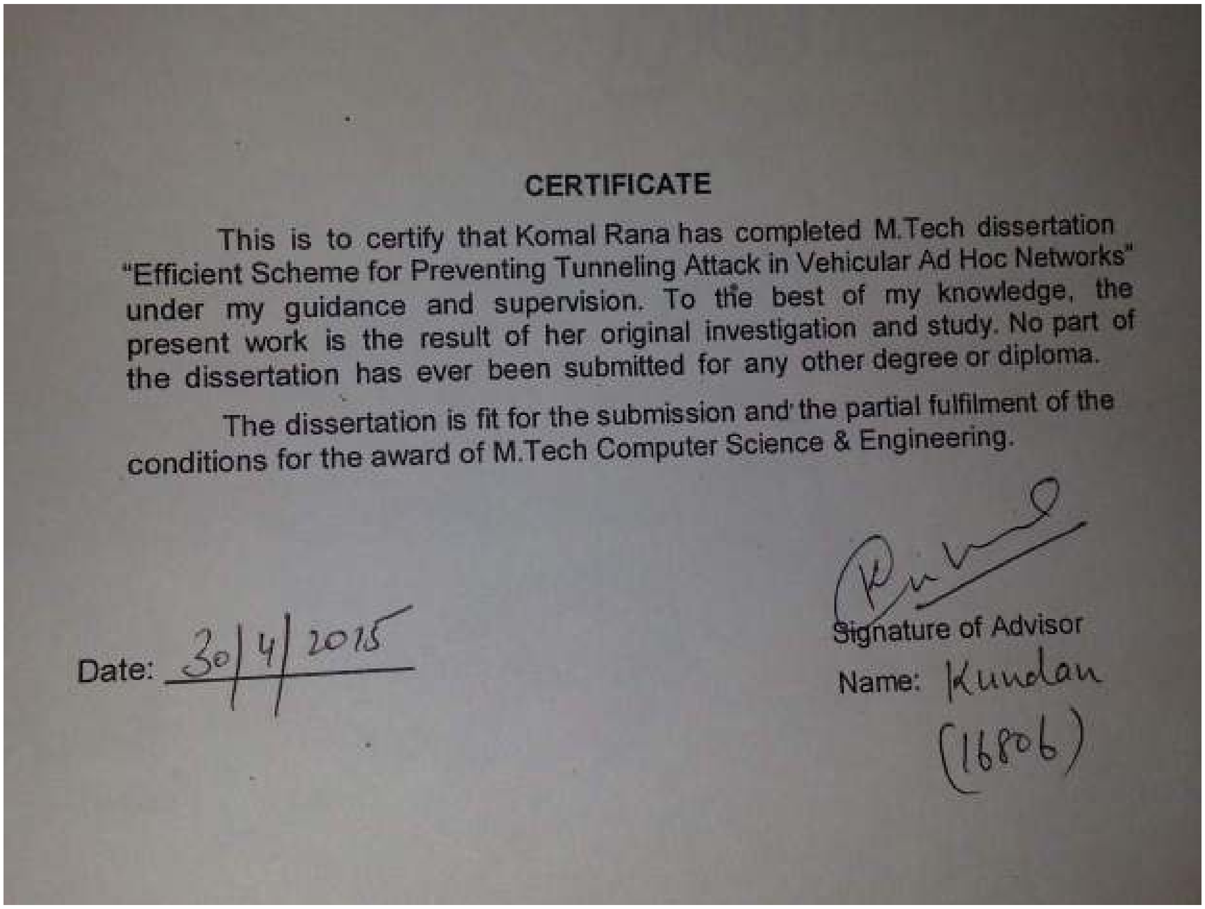
APPROVAL OF PAC CHAIRMAN Signature: 24/4/14 11041 Date:

*Supervision should finally encircle one topic out of three proposed topics and put up for an approval before Project Approval Committee (PAC).
*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/ Dissertation final report.
*One copy to be submitted to supervisor.

ABSTRACT

VANET is vehicular adhoc network. Vehicles are turned into the wireless nodes or routers of the network. There is mobility of host that is there is a change in topology in such a fashion so that interconnections between each node are capacious of changing on continual basis. When there is a tunnel or jammed area the chances of the attack becomes maximum as there is no network and since nodes are autonomous then the chances of intruder nodes to attack or be the part of network are more. VANET uses adhoc communication for performing efficient data transmission .This intercommunication includes data from roadside and from other vehicles. There are limitations of line -of –sight and ample processing delays. The router connectivity changes frequently and leads to the multi-hop communication. Routing protocols are there to facilitate communication within the nodes. These nodes arbitrary forms the topologies based upon their connectivity set up with each other. VANETS works with a decentralized approach where nodes can communicate with each other on the basis of mutual trust and thus there is more possibility of attacks inside the network. When any host wants to communicate with another then these nodes must lie within their range so that sender node can send data to destination and there can be the effective communication. During the communication there are intermediary nodes. Thus there are security issues in VANETS as there may be the failure of data while communication of sender and receiver. Due to dynamic topology of network that is change in position an attacker exploits information when a vehicle enters into a tunnel and thus attacker can now steal significant information within the network .There should be certain mechanism for providing security within tunnel.

CERTIFICATE



CERTIFICATE

This is to certify that Komal Rana has completed M.Tech dissertation "Efficient Scheme for Preventing Tunneling Attack in Vehicular Ad Hoc Networks" under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfilment of the conditions for the award of M.Tech Computer Science & Engineering.

Signature of Advisor

Date: 30/4/2015

Name: Kundan
(16806)

ACKNOWLEDGEMENT

A project cannot be said to be the work of an individual. Hence, a research is a combination of views and ideas, suggestions and contributions of many people.

I take this opportunity to present my vote of thanks to all those who really acted as lightening pillars to enlighten my way to successful and satisfactory completion of this report.

I am highly thankful to my mentor, **Mr. Kundan Munjal** for her active support, valuable time and advice, whole-hearted guidance, sincere cooperation and involvement during the whole process and in completion of this report within the stipulated time.

And last but not the least, I find no words to acknowledge the financial assistance & moral support rendered by my parents in making my efforts, a success. All this has become reality because of their blessings and above all, by the grace of Almighty God.

KOMAL (11004513)

DECLARATION

I hereby declare that the dissertation entitled, “Efficient Scheme for Preventing Tunneling Attack in Vehicular Ad Hoc Networks” submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: 30 April,2015

KOMAL

11004513

TABLE OF CONTENTS

List of Figures

Chapter 1

INTRODUCTION

There may be several situations where users of a network can’t rely on the infrastructure network .In these situations mobile adhoc network is the only choice. It’s important to note the network should be mobile and use wireless communication e.g. the use of such mobile, wireless, multi-hop, adhoc network are called adhoc network.

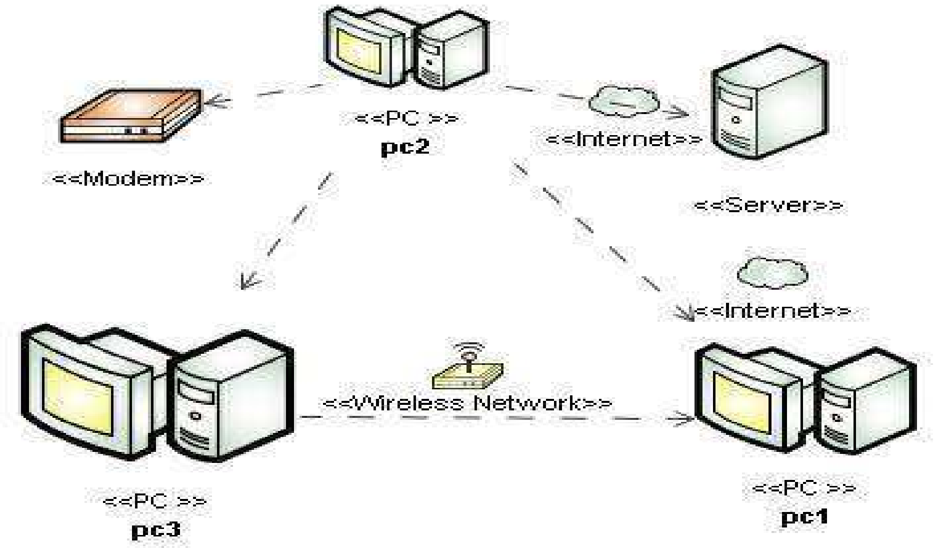


Fig1. Adhoc Network.

1.1 FEATURES

1. Instant infrastructure: Unplanned meetings and spontaneous communication of nodes etc. can’t rely on any infrastructure. Infrastructure needs planning and administration. It would take too long to set up this kind of infrastructure; therefore adhoc connectivity should be set up.

2. Disaster relief: Infrastructure typically breaks down in disaster areas. Hurricanes cut phone and power supply, flood destroy base stations fir can burn servers. No forward planning can be done and set up must be extremely fast, flexible and reliable. The same applies to many other military activities. So these are the major driving forces behind the mobile adhoc networking.

3. Remote Areas: It’s too expensive to set up any infrastructure in sparsely populated areas. Depending upon the communication pattern, adhoc network or satellite infrastructures can be the solution.

4. Effectiveness: Service provided by the existing infrastructure might be too expensive for certain applications. If after 1 minute a single message to be transferred then it will be too expensive to register each time for every small status .So application – tailored adhoc network can be a better solution**.**

Thus adhoc networking provides all these facilities and now a day people want more convenience. When we are using computer in internet and you leave home network, i.e. the network your computer configured for, and reconnect your computer at another place (if no additional mechanisms are available).The reason for this is quite simple if you consider routing mechanism on internet. A host sends an IP packet with the header containing a destination address with other fields. The address of the destination not only determines the receiver of the packet but also the physical address of the receiver.

eg. 129.13.42.99 shows that receiver must be connected to physical subnet with network prefix: 129.13.42.Routers in the internet now look at the destination address of incoming packets and forwards them according to internal look up address. To avoid explosion of routing tables, prefixes are stored and further optimizations are applied. A router would otherwise have to store the address of all the computers but these are quite infeasible tasks so it’s better to use Mobile Adhoc Network. Which continuously keeps changing thee topologies and each vehicular node itself serves as a router .MANET provide communication between nearby vehicles, vehicles and fixed infrastructures on the road.

VANET is the type of MANET but MANET is not able to provide the optimum throughput required for the last changing vehicular adhoc network. In MANET each node send the broadcast packet to all other nodes and all thee nodes have to update their routing tables this increases the computational overhead on all the nodes.

VANET is always changing the topology as vehicle is moving node in the network. Vehicles are moving at the speed of 70 to 80 Kmph and if distance between two vehicles is 120 m then the link between these vehicles would last at most 10 seconds.

Even in the transportation demand of safe infrastructure is increasing as the number of roadside accidents are increasing vary rapidly according to national highway traffic administration there are 43000 deaths, 2.7 million injuries every year. Because of this huge destruction there is need to make our vehicles intelligent enough so that we can decrease those figures up to certain number. A vehicular adhoc network adds this ability to the vehicles. There is a need of self-healing and self-organizing, network without the interference of centralized or established authority this type of network is called vehicular adhoc network. In vehicular adhoc network there are self-governing mobile nodes. The topologies are thus getting changed randomly.

Vehicular Adhoc network is a subclass of Mobile Adhoc Network. It simulates an influential role in intelligent vehicle transportation. In order to avoid any dangerous situation through Vehicle to Vehicle communication VANET supports drivers to communicate and coordinate among roadside units e.g. accidents, traffic jams, control on speed and obstacles etc. Besides these VANET also contributes to comfort applications to the way users. For example, information of weather, mobile e-commerce, access on internet and various multimedia applications. In order to perform efficient data transmission VANET uses adhoc communication. This communication includes data from roadside and from other vehicles. There are limitations of line -of –sight and ample processing delays. The connectivity of router changes frequently and leads to the multi-hop communication. There are routing protocols to facilitate communication within the nodes. These nodes arbitrary forms the topologies based upon their connectivity set up with each other. VANETS works with a decentralized approach where nodes can communicate with each other on the basis of mutual trust. During the communication there are intermediary nodes. Thus there are security issues in VANETS as there may be the failure of data while communication of sender and receiver because each node sends data based on mutual trust to others neighbour nodes.

1.2 CHARACTERISTICS OF VANET

1. Self-organizing behaviour: The nodes in the vehicular adhoc network are roadside units as well as serves as routers that govern the path for communication. Since topology of the network remains changing and routers keep maintaining the routing table and thus can manage the network .This network thus can maintain all the data and the routing behaviour of nodes with other nodes.

2. High mobility of nodes : Vehicles on the road side units keep moving and thus position get remain changing however new routing topologies also get updated in the routing table. Dynamic topology allows high mobility of nodes in the network.

3. Frequent disconnections: Since there is traffic across road side units and all the neighbours have their selective path thus there is change in the routing tables and a frequent change is observed in thee network. There may be communication between road side units and other roadside unit, roadside unit with infrastructure, infrastructure with infrastructure and thus frequent change is observed.

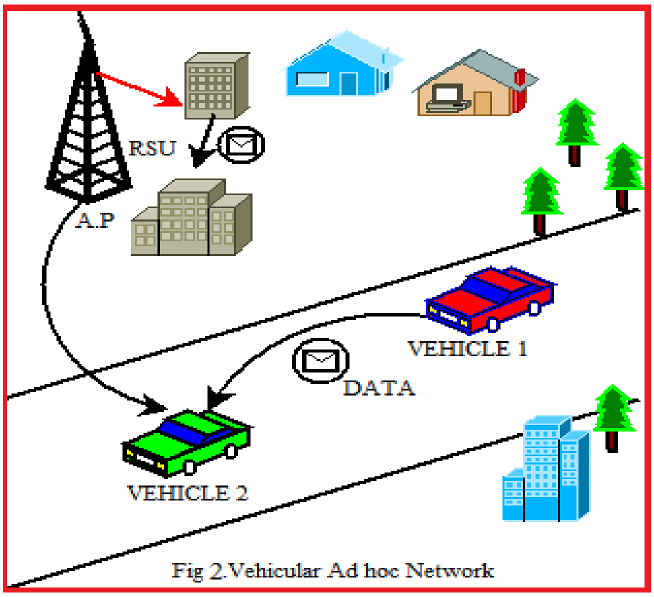


Fig2. Vehicular Adhoc Network

4. Dynamic changing topology: Since the roadside units wants to communicate with other roadside units, infrastructures and also keep moving along the destined path thus there is change in the topology and thus keeps updating the routing table and hence dynamic topology is observed.

5. Highly partitioned network : There are different types of the network unit that are participating while communication these nodes thus allows the portioning of network form other network as the communication is among the partitioning vehicles only and rest thus can separate the topology from other networks if desired thus there is highly partitioned network.

1.3 APPLICATIONS OF VANET

1. Safety: As the number of road side accidents are increasing every year and because of this reason there is a great requirement to improve the security .VANET provides this platform of safety. Since while moving the vehicle continuously keep changing their positions with time and due to this they form random topology and thus it is quite hard that we have infrastructure network for this scenario.

2. Infotainment: The data can be exchanged between all the nodes related to:

i. Position and distance covered.

ii. Speed of the neighbouring roadside units.

iii. Adjustment of speed with other road side units.

iv. Behaviour of the other roadside units.

v. Helps to assist the drivers.

3. Convenience: Since we can keep track of record of all the nodes as these nodes are themselves serves as a router and thus can store the information of the traffic and this helps in maintain the topology.

Convenience application of the VANET mainly helps in managing the traffic with boosting the efficiency and the convenience to all road side units and drivers. These Convenience applications of VANET can be categories as:

- **Diversions of the routs**: We can plan route and trip by checking thee congestion of the system or the roadside traffic.
- **Collection of electronic tool:** All the payments of the tool tax can be made electronically thorough the collection of tax at all collecting points. At tool collection booth there should be able to read the total distance of the journey and thus through GPS can detect the destination and hence can calculate the total amount to be paid by the road side units. This application is only beneficial to operators and not for drivers.
- **Parking:** In certain geographical areas the availability of parking in metropolitan cities helps to find out the free slots of parking. In case the space is available users can be easily notified.
- **Prediction:** It helps the driver to estimate the fuel usage by adjusting the speed .It also assists the driver so that driver can cop up with the adjusting behaviour of speed on the road.

5. Productivity oriented: We are calling it as the productivity oriented applications because these leads various productive results in the vehicular adhoc network.

- **Fuel Saving**: Since location of every node can be traced so it’s easy to detect the position of the tool tax booth and without stopping the vehicle 3% is saved as no vehicle now has to wait on the tool booth.

4. Comfort: Since we have the information about all the routes therefore there are lesser chances of the errors also the driver is assisted by easily navigating platform as each node is having the security information. There is information regarding the parking i.e. if the area of the parking is free for the desired slot. It also helps in detecting the nodes coming in the on way path and thus lesser chances of the errors and driver also feels comfortable in this environment.

6. Automated highway: In vehicular adhoc network we have the topologies and these topologies get changed with respect to the position of the vehicles. Thus driver is already aware about the nodes i.e. routing nodes, thus he treats this as an automated highway. There are lesser overheads for the driver and GPS can control the highway and for communication.

7. Commercial oriented: The various commercial oriented applications can be classified as:

- **Remote Vehicle Diagnostics:** In remote vehicle diagnostic each node can personalized vehicle settings .Uploading of the vehicle diagnostic reports by the infrastructure can be easily downloaded by any vehicular node.

  Vehicles can:

  - Download the settings required.
  - Personalized those settings.
  - Update and upload thee new settings.

- **Internet Access:** Vehicle can access the internet using VANET and can exchange information while transportation.
- **Location awareness:** Drivers of the vehicles can download the status of travelling area. Maps of required regions before travelling. All nodes can get important information from mobile hot spot or infrastructure.
- **Advertisement:** various advertisements for the service providers to attract the customers regarding the fuel, petrol pumps, restaurants and other services that are within the range of communicating node. These application domains are also applicable in the absence of internet.

1.4 ARCHITECTURE OF VANET

VANET is a mobile network where topology of the nodes remains changing on regular basis as vehicles keeps moving. It consists of RSU (Road Side Units) these are wireless

equipped road side units also provides medium of communication with other infrastructure such as internet. Road side units can be any equipment containing infrastructure e.g. GSM, WIMAX TOWERS, WLANs etc.
Thus VANET further consists of various types of networks and their interconnectivities.
Wireless Adhoc network don’t depend upon any infrastructure or fixed network for communication and exchange of information. The architecture of VANET has been categories into three parts:

1. Pure Cellular
2. Pure Adhoc
3. Hybrid.

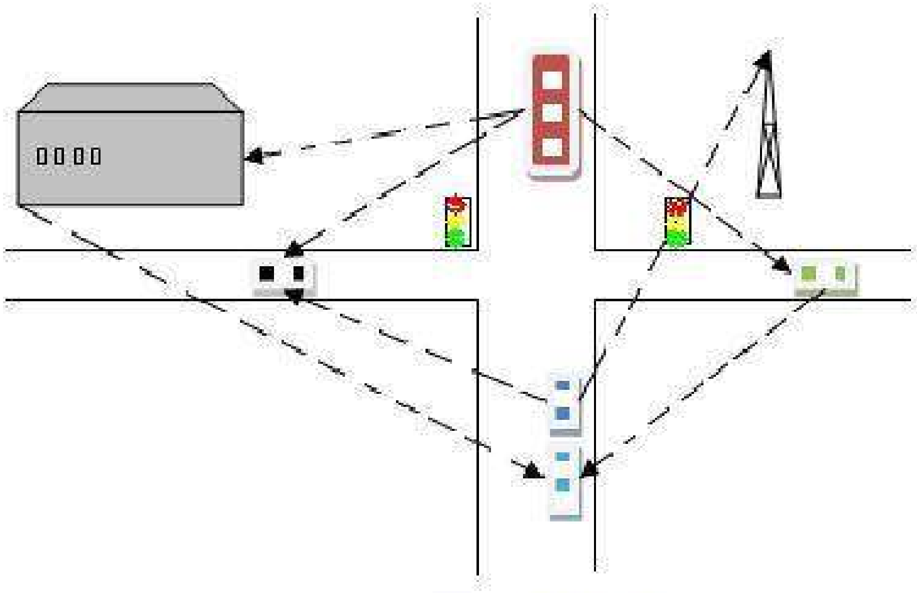


FIG 3:VANET ARCHITECTURE

1. Pure cellular:

In VANET there can be fixed or pure cellular network. In pure cellular network for routing purpose in the VANET we have access points at various traffic intersections so that it can be to connected to the internet and communication or information gathering is possible along road side units. This type of VANET architecture is called pure cellular network or WLAN.

As the diagrams depict the roadside units are connected to the access points (towers).This is pure cellular network.

2. **Pure Adhoc:**

Both the cellular network and WLAN are when combined forms a particular scenario in the VANET, this type of network is called pure adhoc network. Vehicles along the road are when connected to the gateways these gateways can be fixed or dynamic .These gateways provides the connectivity to these roadside units. All the devices and the roadside units thus form a pure adhoc network.

3. Hybrid:

VANET architecture that consists of pure cellular networks and ad hoc networks in the same scenario are called hybrid. There is no centralized authority in hybrid architecture. In VANET all nodes can organize and manage the information by themselves in a distributed fashion. Since the topology of the network is changing i.e. nodes are mobile then data transmission will be less reliable.

Since the roadside accidents are increasing day by day, over 4 million road accidents occur yearly. So, it's a basic concern in the studies. The Vehicular Ad hoc Network should be more reliable and various steps should be considered related to the node movements and security issues. There are various attacks in networks and tunneling attack is one the attacks.

1.5 Tunneling Attack:

Due to dynamic topology an attacker exploits information when a vehicle enters into a tunnel. Thus attacker now can steal significant information within the network. An attacker connects two distinct parts of the network using an extra communication channel as a tunnel.

This may be actual physical tunnel or jammed area. In Fig2 C1 and C2 are two units of communicational channel entering inside the tunnel; AP is access provider for both the communication channel. This tunnel is jammed area that is created by the intruder. Users assumes it as the same communication channel thus continues exchanging the data but in actual; it was a tunnel created by any false entity.

In tunneling attack there is:

***A. Attack on authentication*:** Since there is random change in the topology of the network within the tunnel any false host can readily enter into the tunnel as there is no appropriate method of authentication of nodes. Thus attacker can cause message alteration message suppression, traffic jamming by creating replica copies of same host into the tunnel.

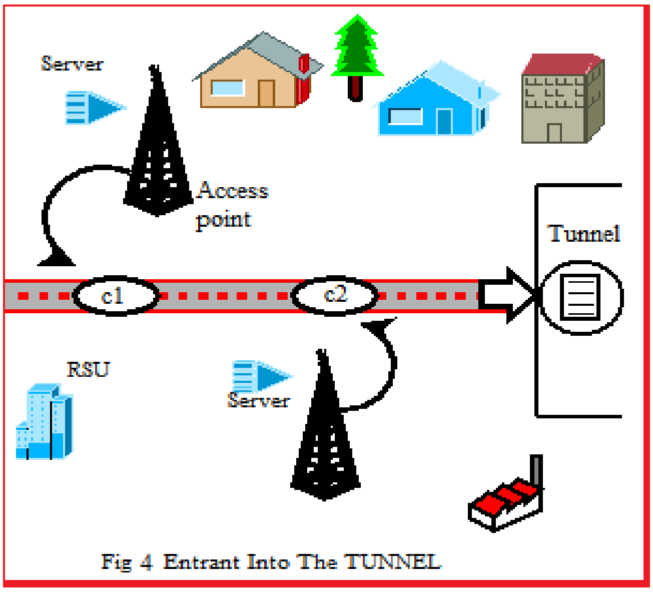


Fig 4 Entrant Into The TUNNEL

Hence there should be appropriate mechanism for authentication.

B. Attack on availability: There is Denial of Service attack by the vehicle inside the tunnel, communication channel must be available at all the time otherwise there is possibility of denial of service attack. This obstruction may cause entire network failure in delivering packets and thus data is not available all the time for other nodes in the network.

C. Attack on trust: No user wants to reveal the secret information about its time, locality, speed and data, transmitted into the mesh. All sensitive data must be taken care carefully. Lack of authentication, less availability of data thus there is less trust among the nodes of the tunnel.

D. Attack on driver confidentiality: Since in vehicular adhoc network there is no exchange of the secure information within the network. But data exchange should take place between the authenticated users only. So that only trusted users are within the tunnel and no loss to data confidentiality.

E. Attack on privacy: [2] Driver privacy is an important issue in vehicular adhoc network. They don’t want their private information to be accessed by another. Driver’s identity should not be steal by another attacker in the node because it may contain the speed, locality, time and data that to be transmitted into the network Thus when a node/vehicle enters into a tunnel then In order to setup a connection within a network at least three satellites are required but it's not practicable inside a tunnel to have a range of three satellites. Moreover GPS signals can't be used without effective network inside the tunnel. The work done here depicts the efficient scheme for preventing tunneling attack in Vehicular Ad hoc Network.

1.6 SIMULATION

For continuing the research Network Simulator -2 is used.

Procedures:

1. *# create simulator*

```
set ns [new Simulator]
```

2 . *# Open trace file*

```
set tracefile [open out.tr w]
$ns trace-all $tracefile
```

3. *# Open trace file*

```
$set namefile [open out.nam w]
$ns nametrace-all $namefile
```

4. *# define a finish procedure*

```
proc finish {} {
  global ns tracefile namefile
  $ns flush-trace
  Close $tracefile
  Close $namfile
  exec nam out.nam &
  exit 0
}
```

5 *.# calling finish procedure at 125*

```
$ns at 125.0 “finish”
```

6. *# Run simulation*

$ns run

1.7 Architecture of ns2:

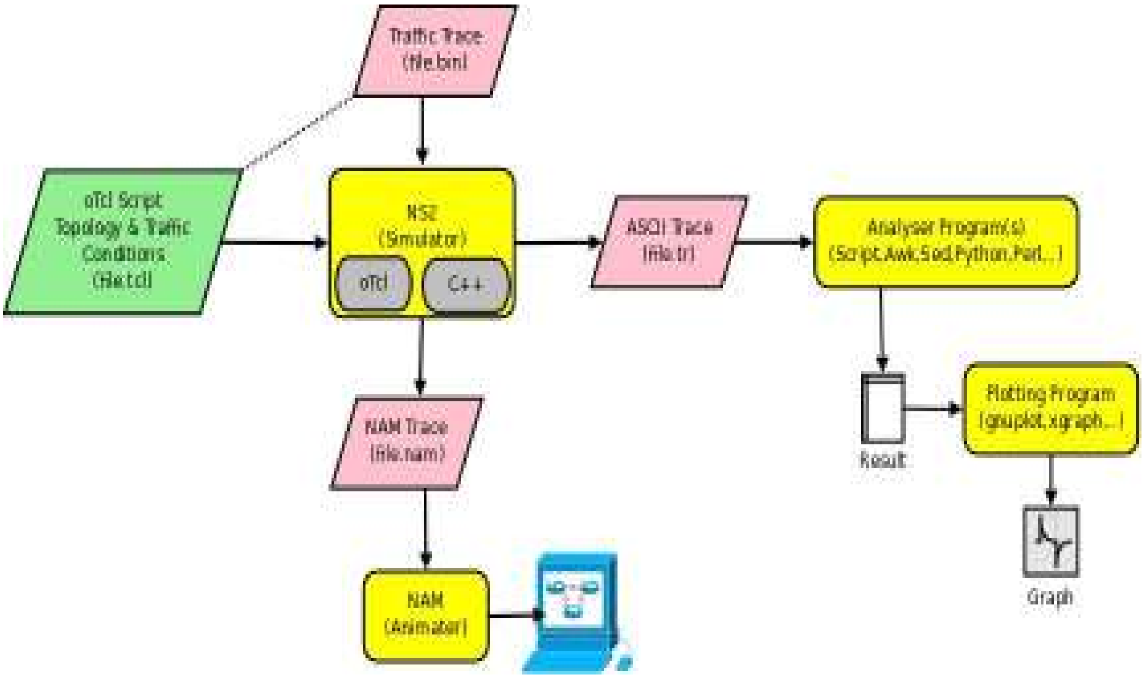


Fig.5

Step1. Create a TCL extension file. TCL is "*Tool Command Language*". This TCL file here is created in c++.

Step2. oTcl here is an interpreter and helps in generating output files.

Step3. NAM Trace is a tool that is used to visualize the output and real world packet trace data. In order to use a NAM file first create a .nam file. This file contains all the information regarding the topology of the network, links and connectivity.

Step4. Nam animator

Step5. .tr files are also generated for tracing and monitoring simulation and here gnuplot is used for plotting the graphs by extracting the values from the .tr files through grep command and storing the values in awk files which is a analyser. These extracted results are plotted using gnuplot and graphs are generated for result analysis.

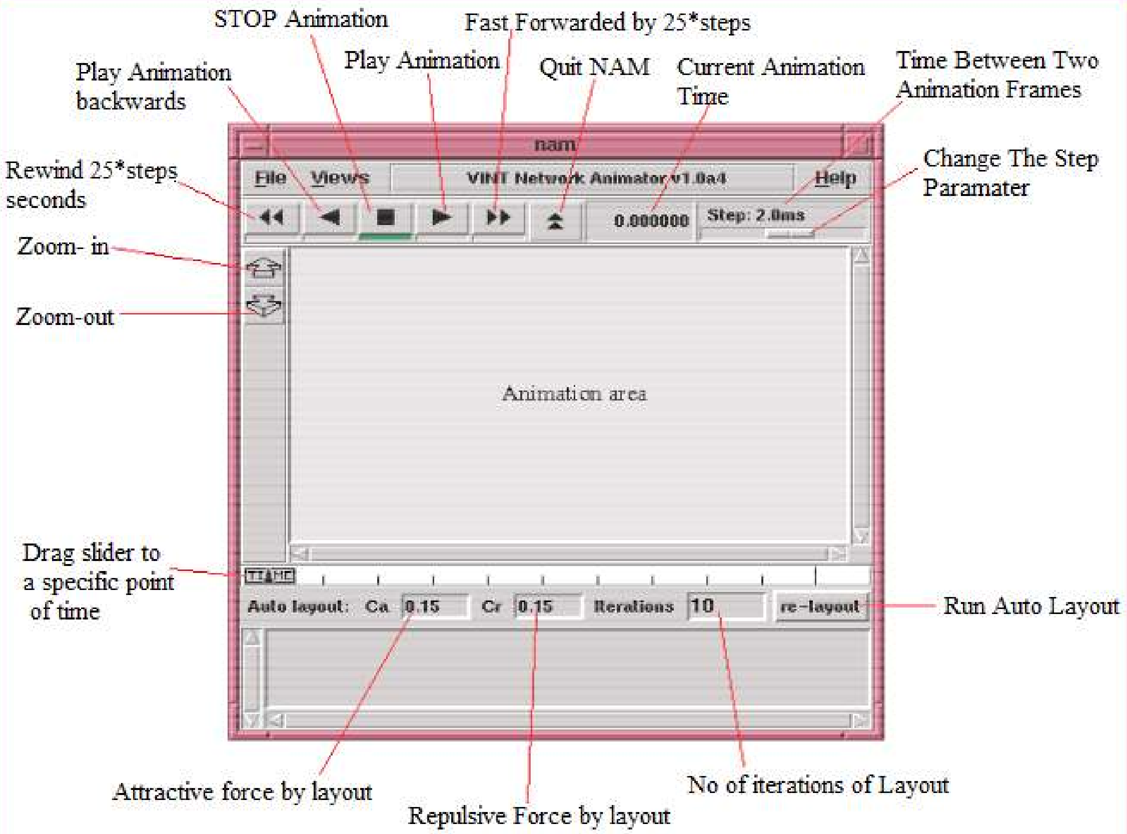


Figure 6 :NAM tool description

Chapter 2

REVIEW OF LITERATURE

Mohammad Saeed Ali –Kahtani from Computer Science Department, Salman Bin Abdulahziz University [1], described various security attributes considering in the vehicular adhoc network security.

Security is major concern in all the fields of communication. There are different types of security attributes that needs to be considered in VANET while depicting the security of the system.

A. Various Security Attributes

There are various security requirements that need to be considered

- **Authentication**: Vehicles should respond only to the messages transmitted by legitimate members of the network. Thus, it is very important to authenticate the sender of a message.
- **Data Verification**: Once the sender vehicle is authenticated the receiving vehicle performs data verifications to check whether the message contains the correct or corrupted data.
- **Availability:** The network should be available even if it is under an attack using alternative mechanisms without affecting the performance.
- **Non-repudiation:** A sender must not deny a message transmission whenever an investigation or identity of a vehicle is required.
- **Privacy:** The profile or driver personal information must be maintained against unauthorized access**.**
- **Real-time constraints:** Since vehicles are connected to VANETs for a short duration, real-time constraints should be maintained**.** Since each node in Vanet acts as both the roadside unit and the router so routers have topologies and knowledge of other routing paths and there can be less chances of the accidents .But in Vanet also there are different types of attacks and security issues we should emphasize more so that we can take advantage of the vehicular adhoc network.

Farzad Sabahi Faculty of Computer Engineering in Azad University, Iran discussed various security attacks in Vanet [2].

Attacks in Vanet: There are different types of attacks /threats in the network that breaches the security in thee network. Different types of attack discussed are:

Threats to Availability:

1. Black Hole Attack
2. Malware
3. Broadcast Tampering
4. Spamming
5. Greedy Drivers
6. Consuming the Node Resources
7. Denial of Service Jamming the Channel
8. D DoS

J.T. Isaac S. Zeadally J.S. Ca´mara [3] described Black Hole Attack

The black hole attack can occur in both VANET and also in MANET. it is formed when one node either drops out from the network or does not participates within network Here all the traffic of the network are redirected to specified places. Irrespective of checking its own routes in routing table a false node waits and supplies the fresh routes within the network. Thus a forged routing table is created. Since flooding mechanism is used here so the routes supplied by the false node are received earlier than the original node.

Anup Dhamgaye, Nekita Chavhan [4] described about Malware

Due to this attack there is a potential damage or disruption from the normal services. These attacks are carried by malicious nodes and can be inside or outside from the network. During the network updating the malware can be introduced from the roadside units. Thus the inserted malwares can be harmful to all adjacent nodes; here false node can gather all the sensitive information about the positions, network traffic, routes etc.

PARNO B., PERRIG [5] described Broadcast Tampering

Various false messages are introduced by the outsider or insider attackers inside the network. It may cause various accidents also by introducing false information into the network. So broadcasting the false information within the network may cause serious problems into the communications among roadside units.

FLORIAN D., LARS F., PRZEMYSLAW [6] discussed the Spamming

Since there is no centralized administration this may causes various serious problems in communication in VANET. Since the vehicles exchanges their positions based upon the mutual trust. Various nodes attack for their own benefits. These selfish nodes can cause problems for other nodes. The original prediction of the VANET thus becomes false .If the numbers of the selfish node increases then other users have to suffer from various problems.

Adil Mudasir Malla Ravi Kant Sahu [7] described security attacks with an Effective Solution for DOS Attacks in VANET

In DOS attack, evil minded nodes hinder certified nodes from acquisition of services delivered by network. DOS attack is directed by flooding of unusual and unnecessary packets to network and server resulting in bandwidth wastage, resource consumption, server crash which further hinders certified nodes from acquisition of services.

- ➢ On Physical and data link layer, evil minded nodes utilized jamming signal to destroy network or server.
- ➢ On Network layer, evil minded nodes get incorporated in routing process which further provokes routing protocol to destroy network or server.

José María de Fuentes, Ana Isabel González-Tablas [8] discussed about attacks on authentication.

Since there is random change in the topology of the network within the tunnel .Any false host can readily enter into the tunnel as there is no appropriate method of authentication of nodes. Thus attacker can cause message alteration /message suppression, traffic jamming by creating replica copies of same host into the tunnel. Hence there should be appropriate mechanism for authentication.in this paper we will discuss those methods in later sections.

Threats to Authentication:

1. Masquerading
2. Replay Attack
3. GPS Spoofing
4. Tunneling.
5. Sybil Attack
6. Message Tampering
7. ID Disclosure

Swapnil G. Deshpande department of computer sciences [9] discussed about

- **Masquerading**

  The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives. There can be message alteration and replay attack in the masquerading e.g. one vehicle pretend to be an emergency vehicle and thus slows down the speed of rest of the nodes inside the network. There can be a position faking message inside the network.

- **Replay Attack**

  The false host inside the network keeps sending the messages inside the network so as there is load inside the network and there are more chances of insider attack i.e. false node can attack after knowing the whole topology of the network.

- **Global Positioning System (GPS) Spoofing**

  The geographical location of all the nodes is maintained by the GPS satellite. An attacker can send the false information or false readings of GPS positions into the network. Thus the nodes don’t know about the actual positions and based upon mutual trust the false information is transferred within the network.

Mohammad Fanaei', Mehdi Berenjkoub, Ali Fanian [10] described the tunneling attack.

There may be actual physical tunnel or any jammed area. In case of actual physical tunnel there may attack on authentication, confidentiality, while if the entrant node inside the tunnel is malicious then there is more threat to security attributes. Sometimes there is jammed area that is also an artificial tunnel.

S. Park, B. Aslam, D. Turgut, Cliff C. Zou [11] Sybil attack In Sybil attack false nodes called Sybil nodes inserts multiple fraud copies of each identities and thus the behaviour of these nodes causes harms to each neighbouring nodes in the network.

F. Sabahi [12] described Impact of Threats on Vehicular Adhoc Network Security considering confidentiality as major concern.

Because of more mobility in VANET there will be more security issues than Adhoc. Thus there is more on all the security issues including confidentiality. The information of the neighbouring nodes, positions of each nodes and the time of travel all these information can be transferred to another network by the false node.

Mohammad Fanaei', Mehdi Berenjkoub, Ali Fanian suggested a resistant TIK-Based endairA against the Tunneling Attack [10]

Describes an overview of tunneling attack .But it is considering the time factor if there no reply within the specified time then there exist a tunnel.

Triki, Rekhis, Chammem and Boudriga [13] The RFID radio frequency identification number can be used to have a check on all the entering nodes within the network. RFID positioned the vehicular nodes and broadcasts the error message to neighbouring nodes. RFID system transmits an object identity using electromagnetic waves. While implementing we will check how it works and how much effective it is.

B. Parno and A. Perrig [14], described about the token based approach. That can be implemented within the tunnel where message can be broadcast to other nodes using a token.

Chapter 3

PROBLEM FORMULATION

VANET is vehicular adhoc network. Vehicles are transformed into the wireless nodes or routers of the network. Since, it is ad hoc network so there is mobility of host i.e. there is a change in topology in such a fashion so that interconnections between each host are capable of changing on continual basis. When there is a tunnel or jammed area the chances of the attack becomes maximum and since nodes are autonomous then the intruder nodes to attack or be the part of network are more because nodes exchange their positions based upon mutual trust . Thus any false node can send wrong information regarding routes and traffic inside the tunnel. This may cause various problems and road accidents. This report depicts the solution that how to authenticate each node and how to establish a reliable network to prevent tunneling attack.

In tunneling attack there is:

A. Attack on authentication: Since there is random change in the topology of the network within the tunnel any false host can readily enter into the tunnel as there is no appropriate method of authentication of nodes. Thus attacker can cause message alteration message suppression, traffic jamming by creating replica copies of same host into the tunnel.

B. Attack on availability: There is Denial of Service attack by the vehicle inside the tunnel, communication channel must be available at all the time otherwise there is possibility of denial of service attack. This obstruction may cause entire network failure in delivering packets and thus data is not available all the time for other nodes in the network.

C. Attack on trust: No user wants to reveal the secret information about its time, locality, speed and data, transmitted into the mesh. All sensitive data must be taken care carefully. Lack of authentication, less availability of data thus there is less trust among the nodes of the tunnel.

D. Attack on driver confidentiality: Since in vehicular adhoc network there is no exchange of the secure information within the network. But data exchange should take place between the authenticated users only. So that only trusted users are within the tunnel and no loss to data confidentiality.

E. Attack on privacy: Driver privacy is an important issue in vehicular adhoc network. They don't want their private information to be accessed by another. Driver's identity should not be steal by another attacker in the node because it may contain the speed, locality, time and data that to be transmitted into the network.

So, a proper mechanism for authenticating each node is required as well as there is no network into the tunnel so a RFID is used as a medium to provide communication between the nodes in the jammed area.

There are unique identifiers: RFID number. Radio Frequency Identification Number, used to electrically recognize the presence of any object. These numbers are provided to each and every host /vehicle which is entrant into the tunnel by certificate authorities.

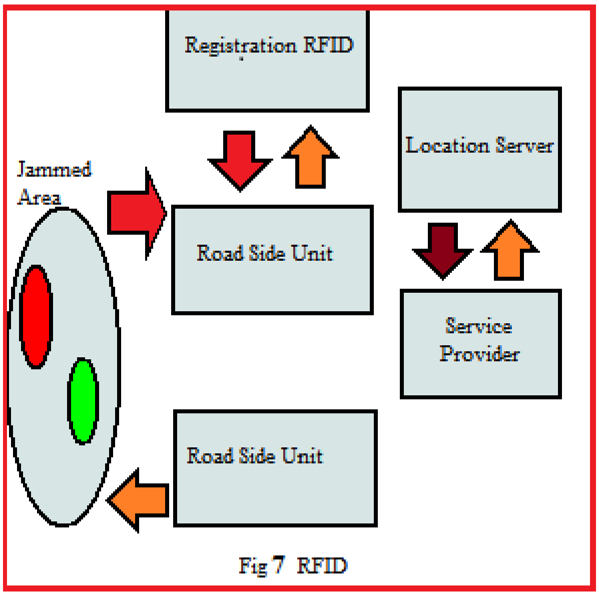


Fig 7 RFID

RFID are decided by these authorities and are saved into the databases for the entries of vehicles into the tunnel. Thus we have all the records of the nodes those are within the tunnel.

The RFID number represents the following field entries of vehicles into the tunnel:

- **Reserved Memory**

  This memory bank usually stores the access password and kill password is very infrequently used and is used to permanently disable the tags whereas accessibility password is set to lock and unlock the tag's read /write capabilities. But it can store only 2 tag information and it's applicable only in case of sensitive data. It's writable if you want to specify fixed password.

- **TID Memory**

  This tag is basically provided by the manufacturer it’s generally IC number. This memory portion is fixed and can’t be changed

- **EPC memory**

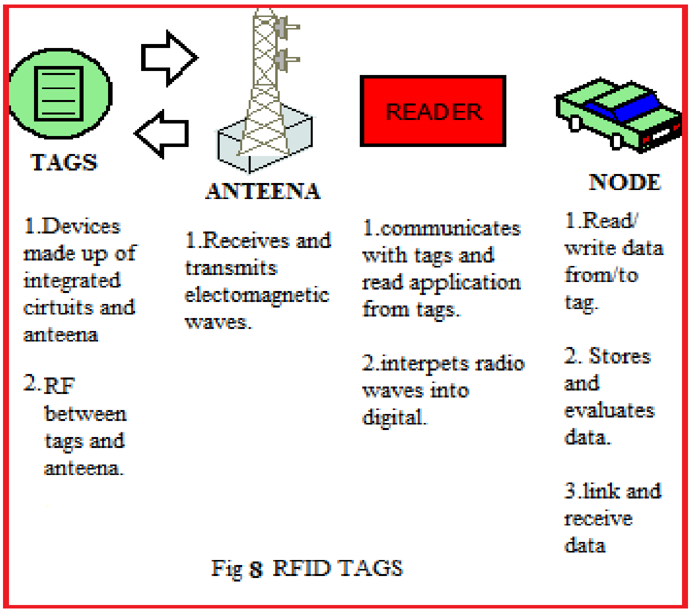
  This memory stores Electronic Product Code .its first writable memory bank with 96 bits of memory.

- **USER Memory**

  If there is need of more memory than EPC the ICs have prolong user memory which can store more information. But there are no standard that how many bits of memory are writable on each tag. This is second writable memory tag. Memory tag is prolonging up to 4K to 8K.

Thus we can store all the information concerning any vehicular host into our databases and there will be less probability of entrant any false node into tunnel.

Mechanism of RFID technology: There are RFID tags these are values assigned to the variegated entities/nodes entrant in the tunnel. These are made up of integrated circuits and antenna. These are readable and writable the antennas thus receive and transmit electromagnetic waves. The RFID readers can easily recognize these values and stores into the databases. These Readers transform the electromagnetic signals received from antennas into signals.



TAGS: 1.Devices made up of integrated cirtuits and anteena 2.RF between tags and anteena.

ANTEENA: 1.Receives and transmits electomagnetic waves.

READER: 1.communicates with tags and read application from tags. 2.interpets radio waves into digital.

NODE: 1.Read/ write data from/to tag. 2. Stores and evaluates data. 3.link and receive data

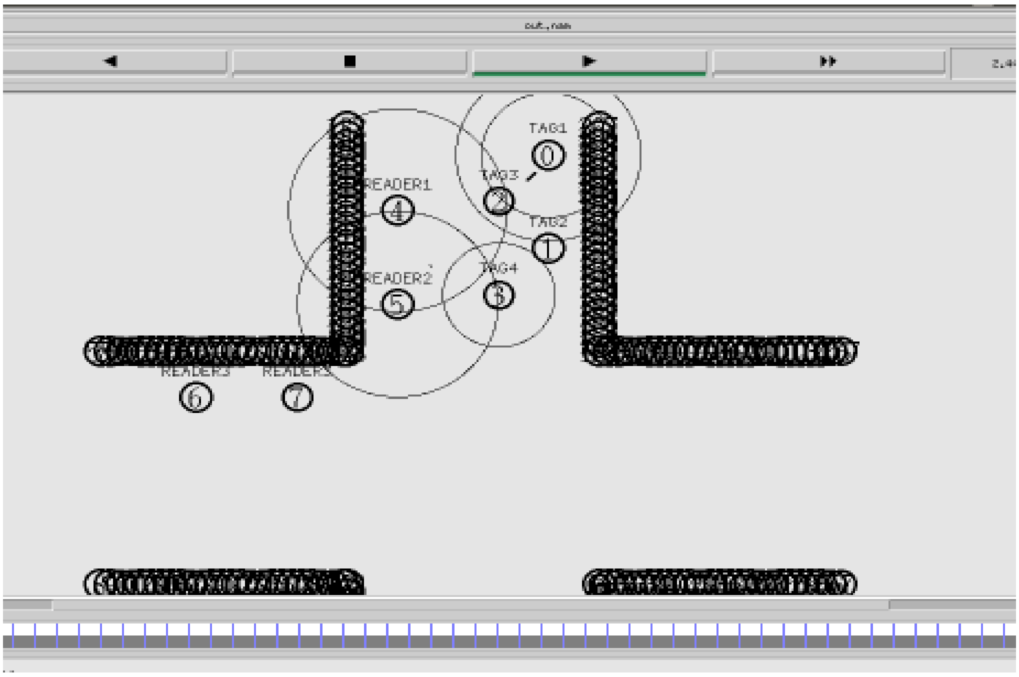
Fig 8 RFID TAGS

The values stored by RFID reader contains various fields as explained in above section. In order to check whether the entity is valid its value is checked into the database and hence can determine whether the node is fake or not.

This was all about the case that only the certified authorities are entering into the tunnel even in the case if the nodes within the network become selfish and may cause certain problem within the network then there should be another mechanism to control this effect.

These RFID thus use helps in providing a medium for communication between the nodes in even when there is jammed area or a tunnel.

All the nodes can communicate through RFIDs that are integrated into the network. The tags thus stored onto the vehicles are read by the READERS and helps in communication.



Snapshot: communication through RFID

The main issue is to provide the efficient scheme against tunneling attack. The false node may send wrong information about the tunnel sometimes there may be the case that there may be tunnel in reality but sometimes false node may inject wrong information into the network this may harm to our network .Thus in jammed area the signals are very weak or there may be the case of no communication. The main objective of the study is to provide a network even in case of tunnel or jammed area.

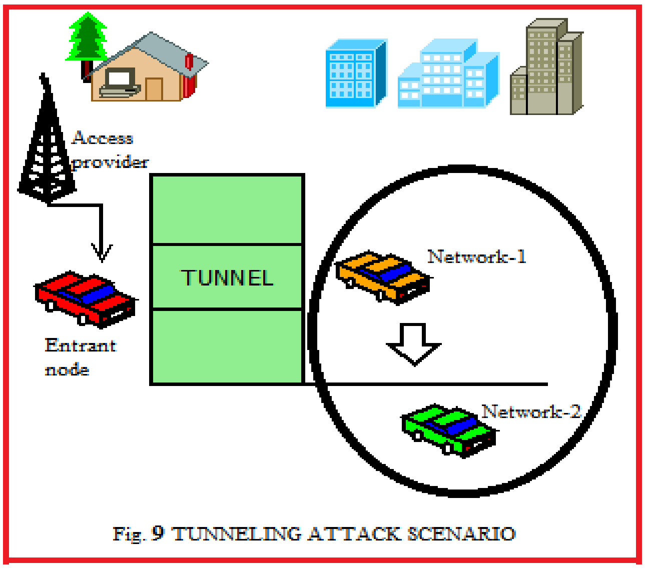


Fig. 9 TUNNELING ATTACK SCENARIO

RFID also here used for authentication purpose. The tags are attached on the vehicles are thus read by the readers and the entries are stored into the databases.

1. CORE (within the network): After RFID in the network there should be a mechanism so that within the network also if there is some self-cantered node we can discover them there will be a reputation table that will be containing:

1. All routes.
2. Entries of self-cantered node if any.

Reputation table is basically a data structure that is stored in each entity.
Each row in the table comprise of:

1. Behaviour of each node.
2. Identifier attached with each node.
3. List of secondary reputation path with another identity.

Thus we can have a watch on the node if the node is not forwarding packets to another nodes in the network then it’s a self-centred node.

From reputation table we can easily re-examine by the identifier and from list that which node is self-centred and thus selfish node can be easily removed from the network Thus now we have mechanisms before entering the tunnel, inside the tunnel discovery of false node then when any vehicle will come out of the tunnel then in that case also there should be certain mechanisms so that we can have secure network just outside the tunnel. There can be various mechanisms related to authentication of nodes so that only authenticated nodes can enter into the network.

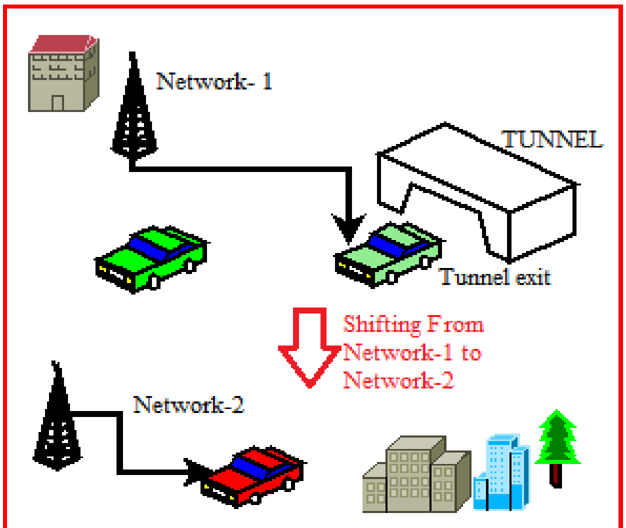


Fig. 10 Shifting From One Network To Another

Thus basically a mapping of two networks is shown here, entries of all the nodes is recorded in a table although its dynamic table but still there will be monitoring on all the nodes in order to detect a false node. We have a assured network because of the technologies incline while entering and also inside the tunnel and we can also detect the false node inside the tunnel. Therefore now we can simply use the mapping or the shifting of our network that is within the tunnel to other network while exiting the tunnel. Tunneling attack can be prevented as the methods suggested in the report. But in case if the false node is not detected within the network and then we can prevent the attack inside the tunnel by the help of RFID this will overcome for the several security issues also.

Chapter 3(c)

RESEARCH METHODOLOGY

Usually there are three types of approaches in order to solve any problem in research.

1. Quantative Approach.
2. Qualitative Approach.
3. Mixed Approach.

In our research we will use both the approaches and it is known as mixed approach.

3.1 Qualitative Approach: knowledge claims are based upon the case studies, grounded studies and phenomenon. In our study we used this approach in literature review .This Literature review helps us to locate and summarize the study to a specific topic .We have then a consistent approach that to be followed after the literature review. Various sources like IEEE research papers, journals, books on wireless network help us in the ethnographies and case studies.

3.1.1 Vanet Attacks

We thoroughly studied about the different types of attacks in the Vanet .The reason of conducting detailed literature review for Vanet attacks was to enhance the security in vehicular networks. Since Vanet provides the facility of the fast communication on the road and we want to minimize the number of the accidents and also the better communication in vehicular adhoc network. Tunneling attack is one of the common attacks in the Vanet. So we were able to analyse the challenge in the Vehicular adhoc network. Furthermore, literature review also assisted us in identifying which attack causes problem there are no preventive measures against tunneling attack i.e. even we don’t know how to minimize the chances of tunneling attack and better performance against tunneling attack.

3.2 Quantitative Approach

Exploring the “cause and effect relationship” is quantitative approach. Here we experiments and surveys and we will use various strategies in future .Statistical procedures are utilized on some data and we will simulate the data thus collected and can evaluate the performance of the findings by doing so we will be able to answer about our research and improved performance against tunneling attack.

Tools: tool selection is very important to validate all the findings we will use network simulation tools to prove our findings.

Since there may be various types of the threats that affect the outcome of our research

There are four different types of threats:

1. Internal validity threats.
2. External validity threat.

3.2.1 Internal validity threats

When we are not able to have correct inferences from the data in an experiment to overcome this threat we will collect the data and will process that data in the simulation environment so that we can conduct our research in better manner. The result is shown in the graphical from so that there may lesser threats and better qualitative work can be achieved.

3.2.2 External Validity Threat

Some external conditions may be responsible e.g. simulation environment so we will draw conclusion during the implementation considering all the threats.

3.3 ALGORITHM

Step1: Start the simulation environment.

Step2: Generate RSU.

Step3: Divide the network into 4 parts.

- Network1: RFID readers and other nodes containing tags. These tags are read by the RFID.
- Network2: FALSE NODE, RFID, Normal communication.
- Network3: No RFID, Lesser communication.
- Network 4: TUNNEL without RFID and no communication**.**
- Analyse the results

Step4: end simulation.

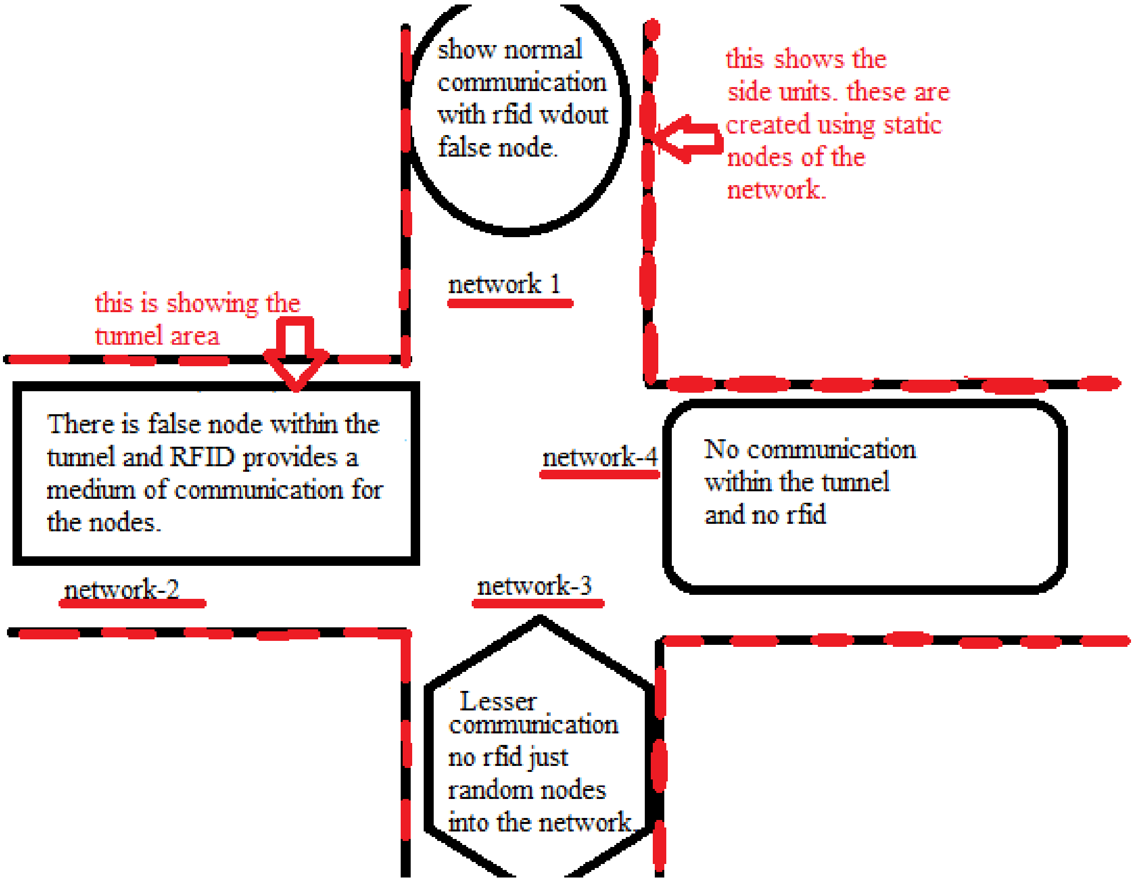
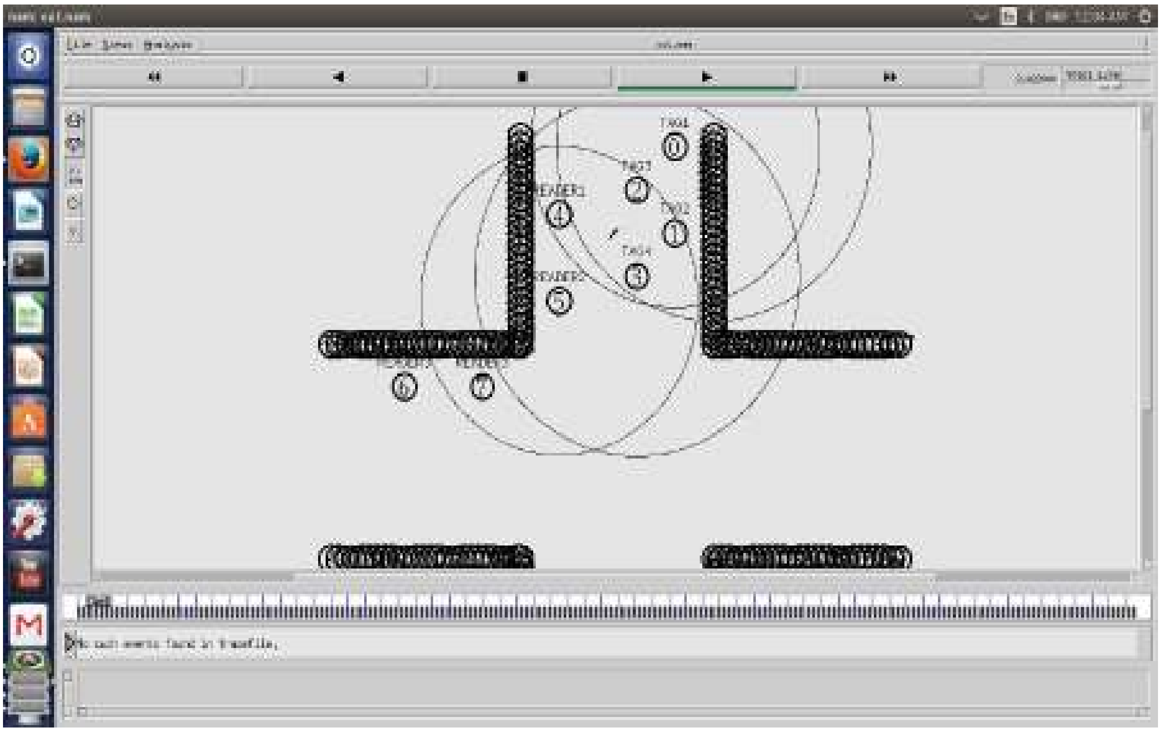


Fig.11 Diagramatic Representation of the Final Scenario

Description of the Network:

Network1: Normal network without tunnel and with RFID.

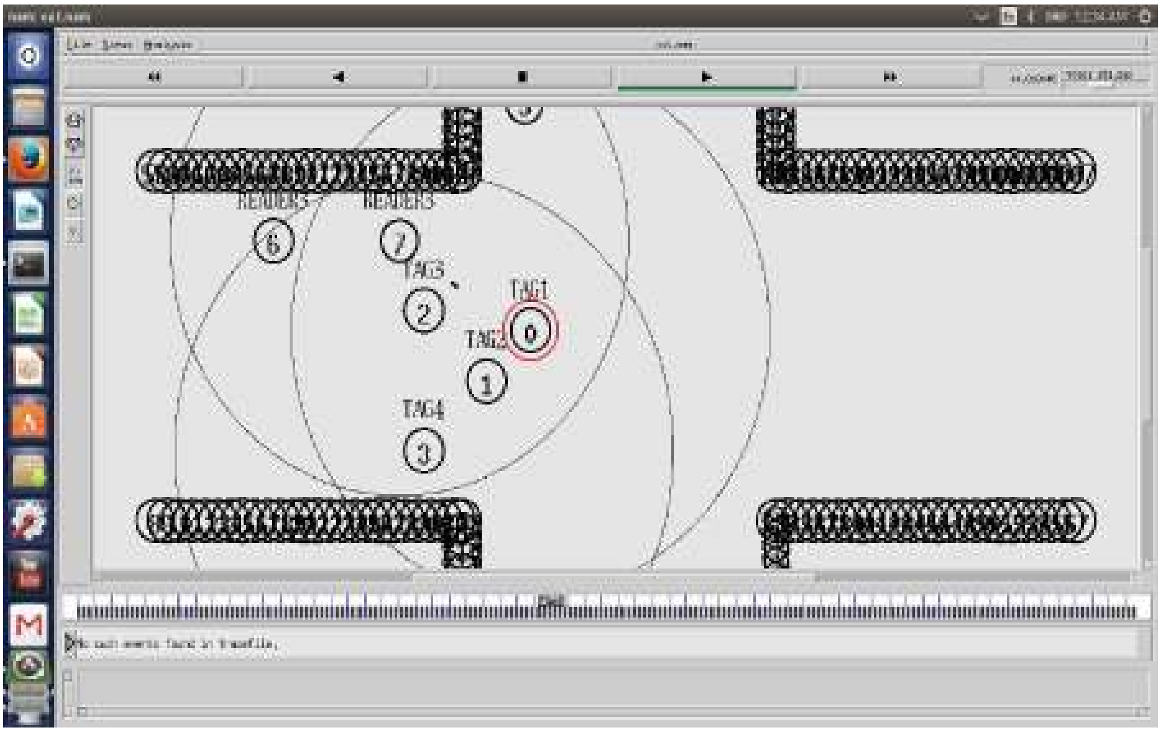


No such events found in tracefile.

Network1

Network 2: FALSE NODE, Tunnel, RFID

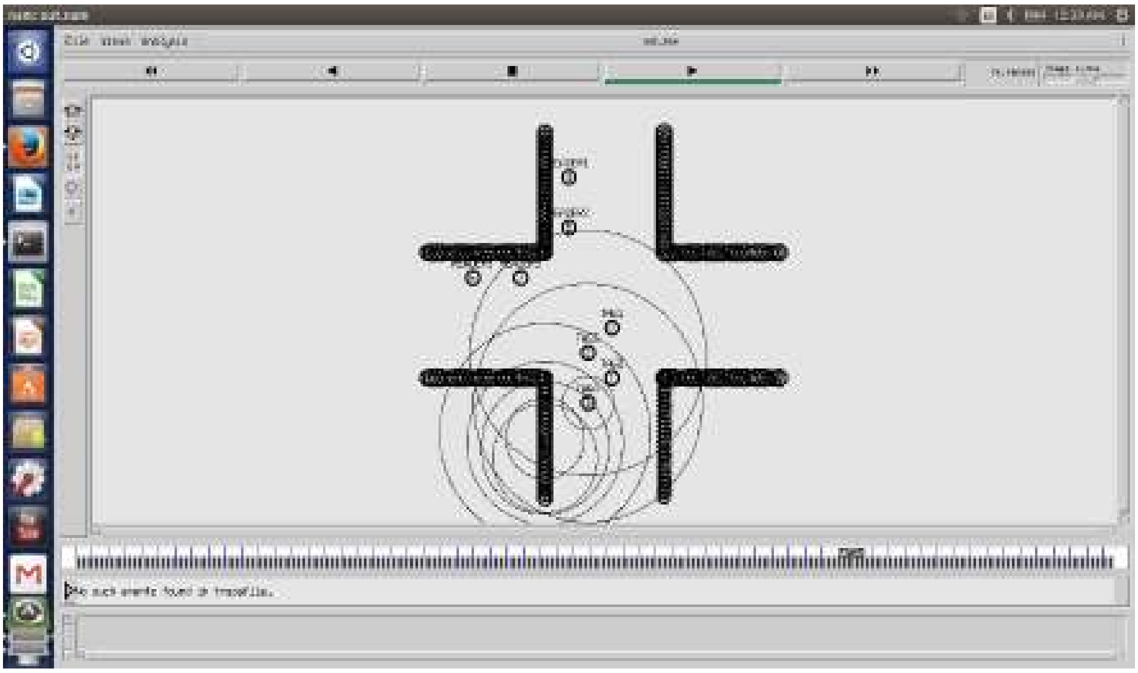
Still communication within tunnel due to RFID



No such events found in tracefile.

Network 2

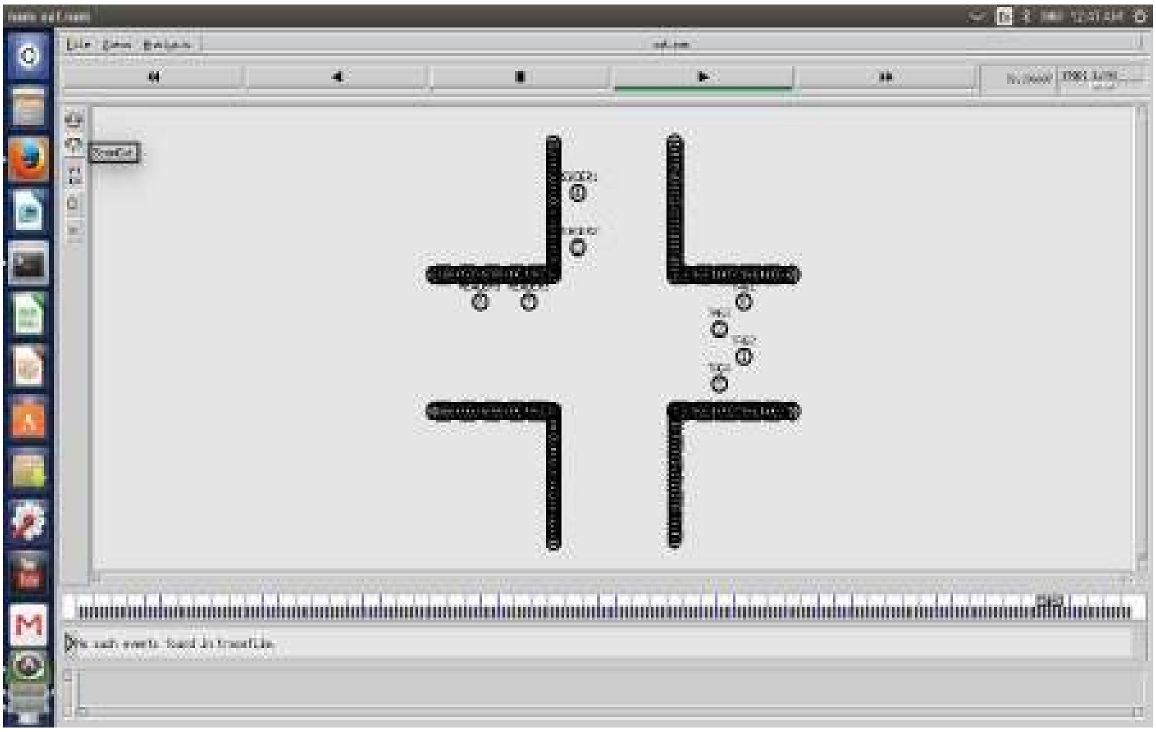
Network 3: lesser communication



No such events found in tracefile.

Network 3

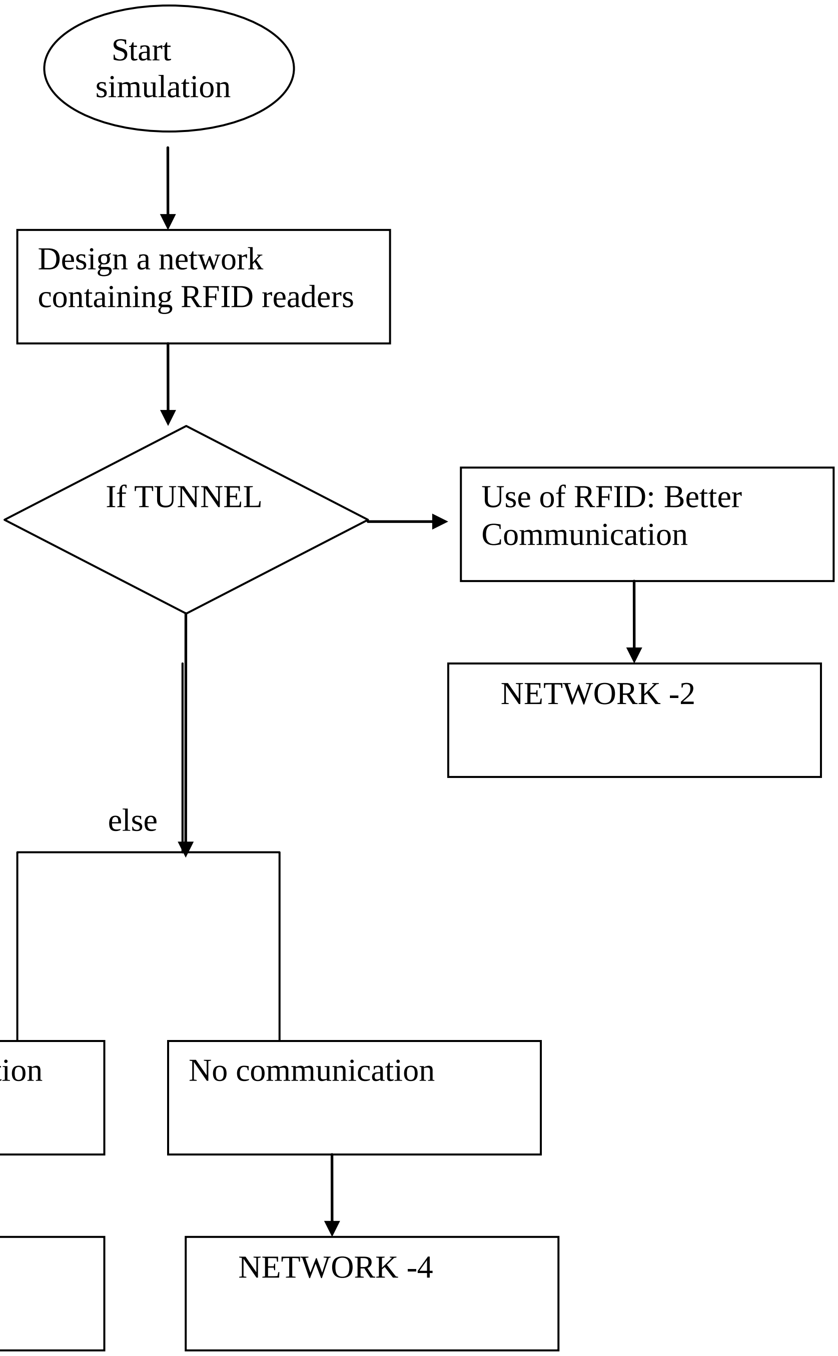
Network 4: no communication no RFID.



No such events found in tracefile.

Network 4

3.4 Flow Chart



Flowchart-1

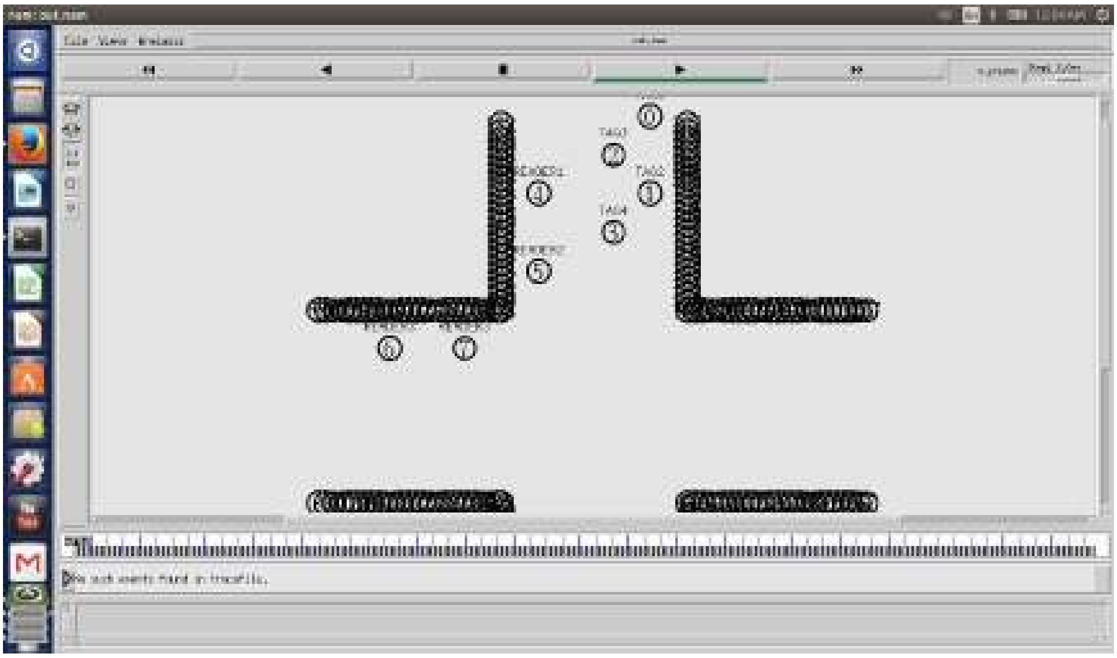
Chapter 4

RESULTS AND DISCUSSIONS

The network of simulation has been divided into four parts.

NETWORK-1

There are random nodes into the network. 4 , 5 , 6 , 7 are RFID READERS. These Radio-Frequency Identification devices use electromagnetic fields in wireless system to transfer the data. The nodes i.e. vehicles moving into the network contains tags attached to them. The tags are used to store important information which is stored electronically. There can be two types of tags 1. Having local source of inbuilt battery and another one collects energy from radio waves and acts as passive transponder and also known as passive RFID. No proper line of sight is required and reader may be embedded within the tracked object. RFID also provides a secure data transfer between the communicating nodes. There is software it may be either integrated into the RFID or may be separated from it the portable device can be a Datalogic jet. This is soft for network used security purpose so that more efficient data transfer can be there among the nodes.

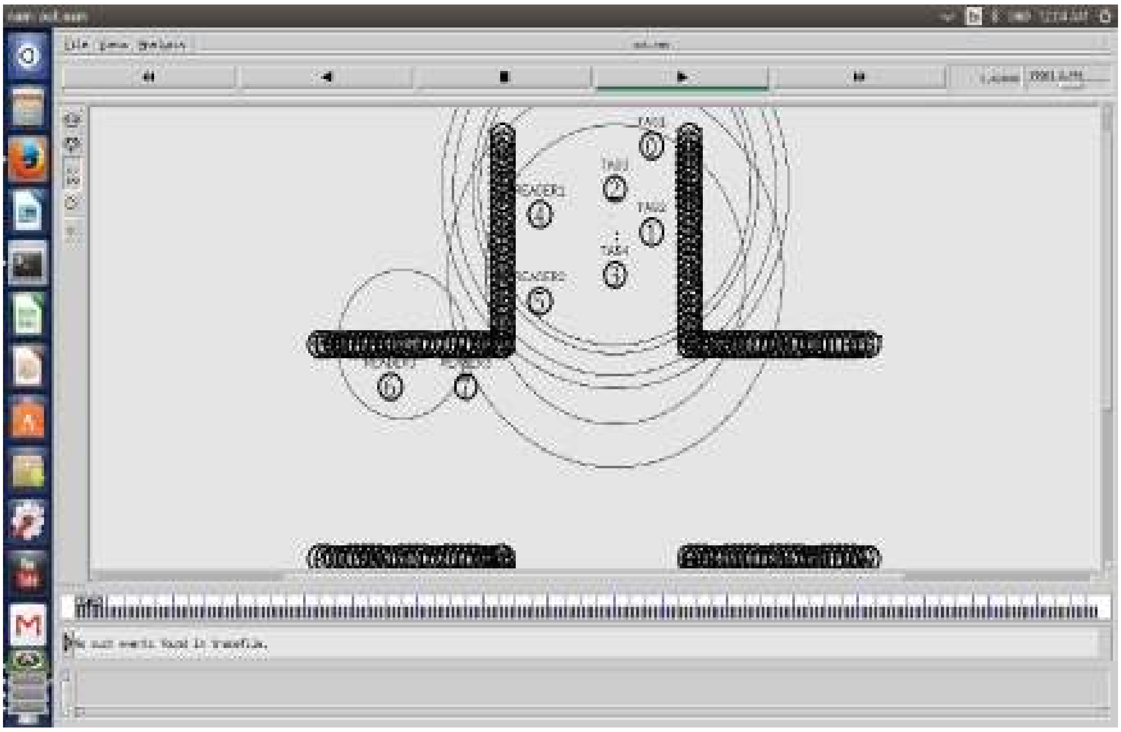


No such events found in tracefile.

Snapshot-1

Snapshot-2

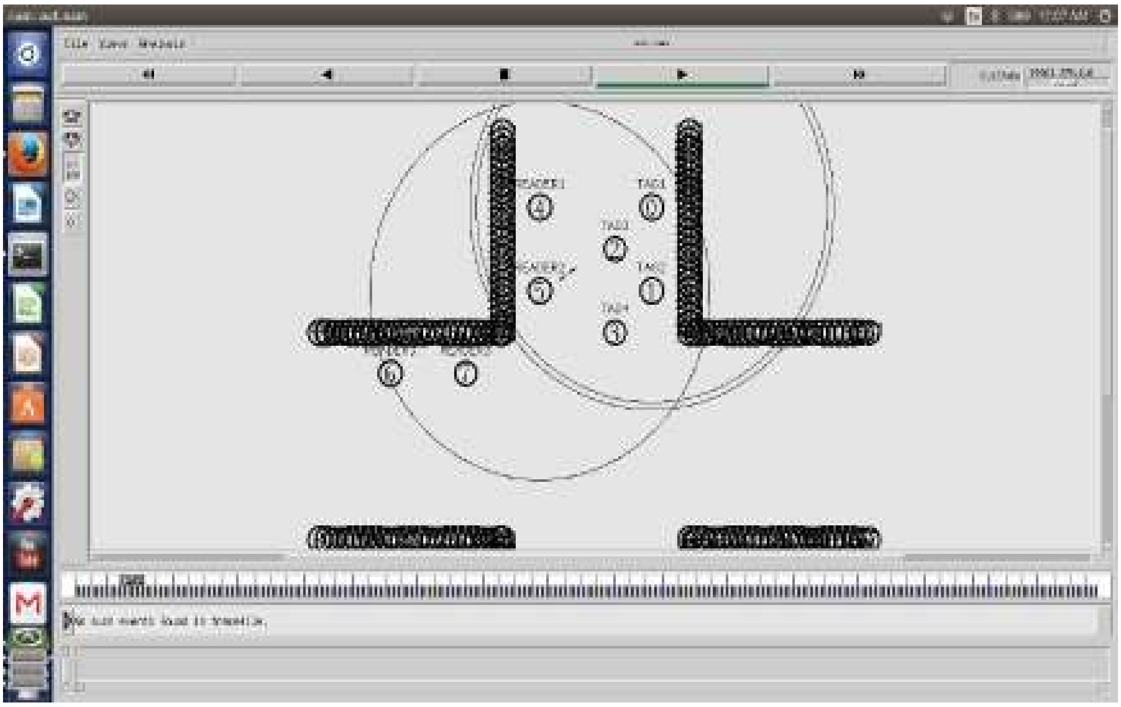
It describes the normal communication network without tunnel or jammed area. Communication between the nodes as well as there are RFID working into the system. There are 4 nodes communicating with each other and two READERS.



No such events found in tracefile.

Snapshot-2

Snapshot 3 describes the communication through RFID reader.



No such events found in tracefile.

Snapshot- 3

Snapshot-4, 5

Snapshot 4 and 5 describes the communication between tags and readers

READER- 4and READER-5 is a transmitter or receiver and based upon radio frequency and controlled by digital signal processors and microprocessors. These readers uses the attached antenna and captures data from RFID tags and then this data is further stored into the data bases where entries of each of the nodes is stored for further use and tracking the entries of nodes.

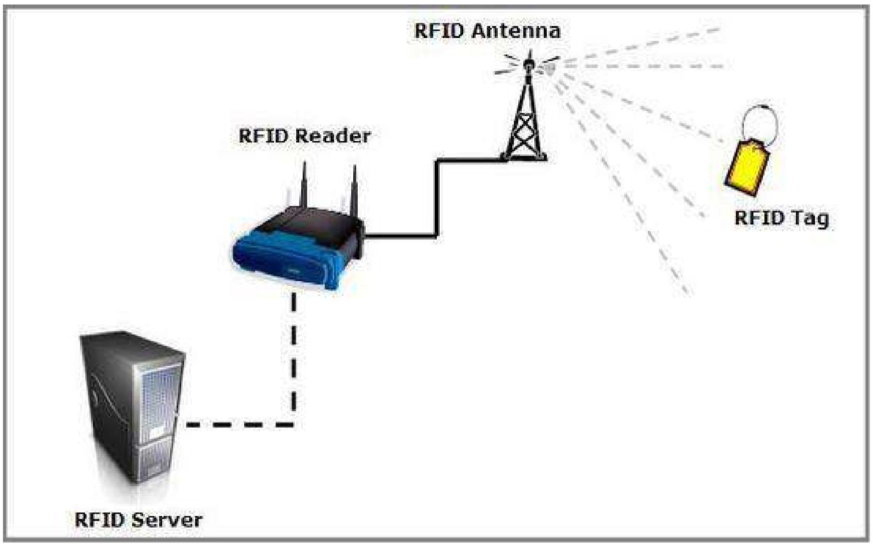
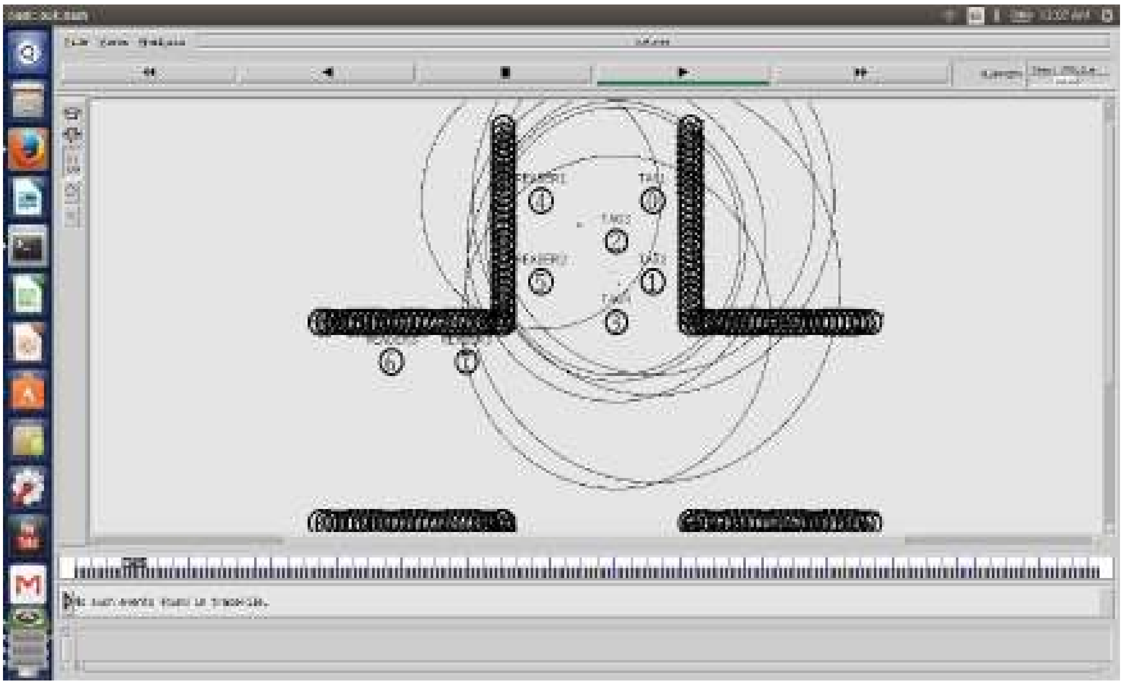
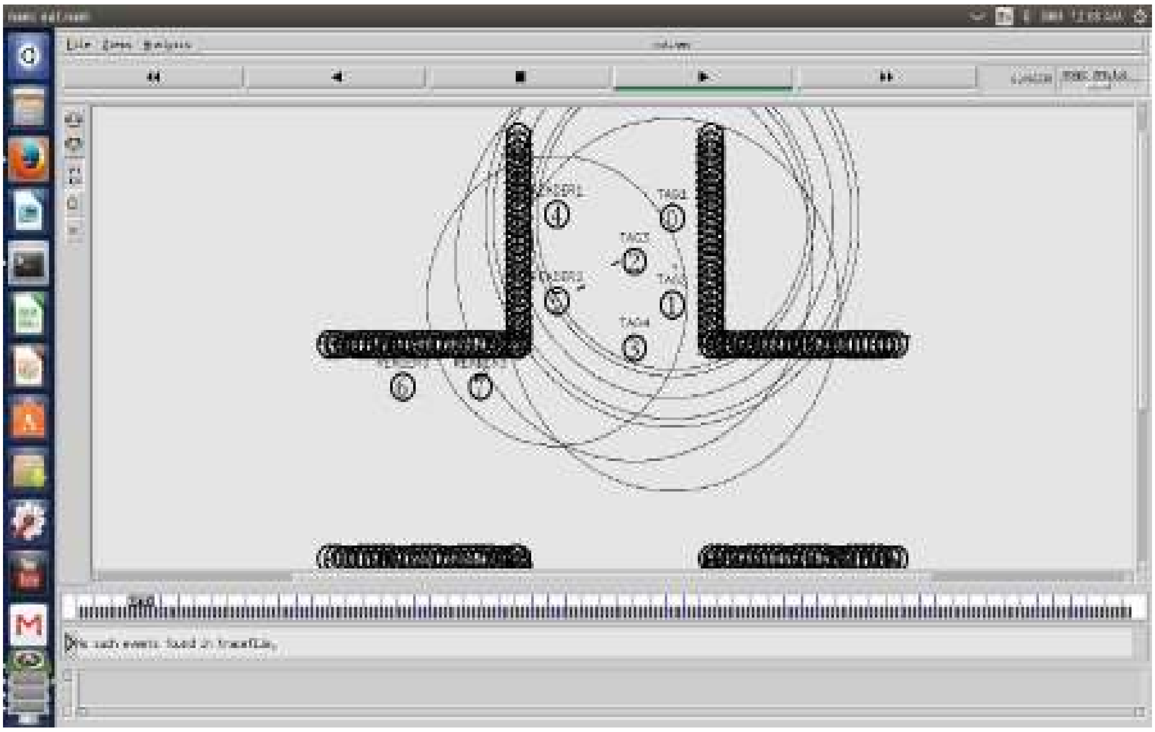


FIG- 12 working of RFID



Snapshot- 4



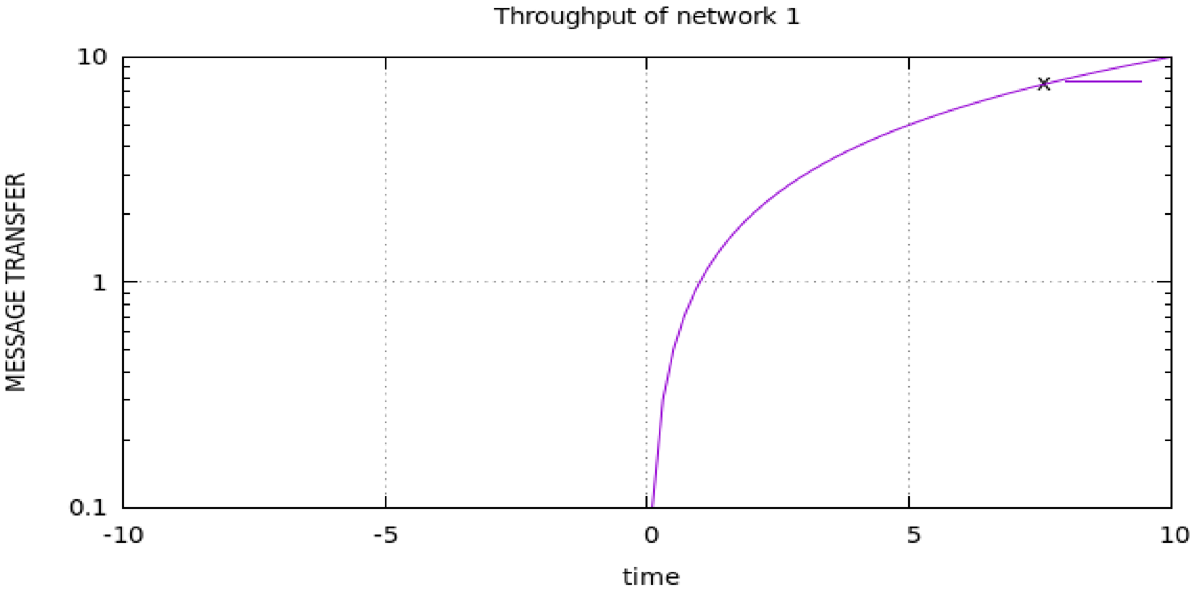
No such events found in tracefile.

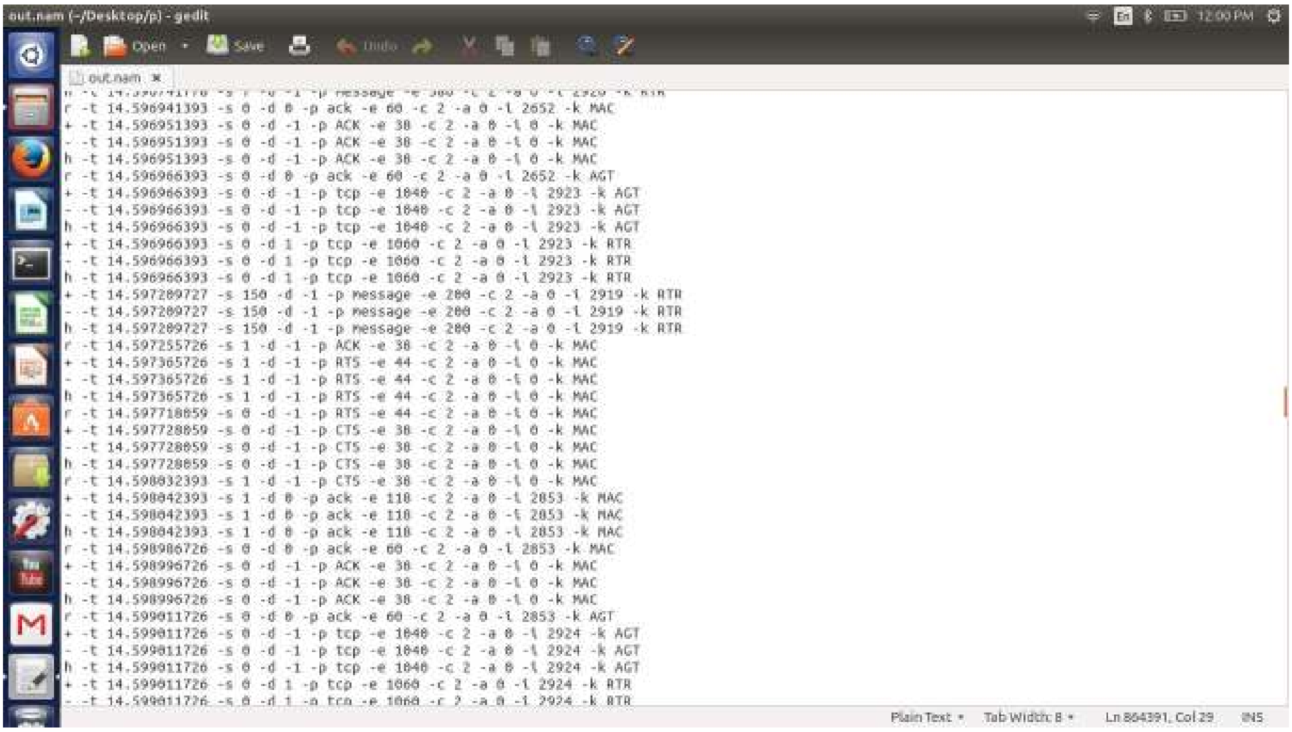
Snapshot- 5

Result analysis of Network 1:

The NS2 architecture as previously described contains output file and the values from this file are extracted through awk file and the results are fetched by grep command so that analysis can be performed on the values that are in the output file.

Graph- 1





```
r -t 14.596941393 -s 0 -d 0 -p ack -e 60 -c 2 -a 0 -l 2652 -k MAC
+ -t 14.596951393 -s 0 -d -1 -p ACK -e 38 -c 2 -a 0 -l 0 -k MAC
- -t 14.596951393 -s 0 -d -1 -p ACK -e 38 -c 2 -a 0 -l 0 -k MAC
h -t 14.596951393 -s 0 -d -1 -p ACK -e 38 -c 2 -a 0 -l 0 -k MAC
r -t 14.596966393 -s 0 -d 0 -p ack -e 60 -c 2 -a 0 -l 2652 -k AGT
+ -t 14.596966393 -s 0 -d -1 -p tcp -e 1040 -c 2 -a 0 -l 2923 -k AGT
- -t 14.596966393 -s 0 -d -1 -p tcp -e 1040 -c 2 -a 0 -l 2923 -k AGT
h -t 14.596966393 -s 0 -d -1 -p tcp -e 1040 -c 2 -a 0 -l 2923 -k AGT
+ -t 14.596966393 -s 0 -d 1 -p tcp -e 1060 -c 2 -a 0 -l 2923 -k RTR
- -t 14.596966393 -s 0 -d 1 -p tcp -e 1060 -c 2 -a 0 -l 2923 -k RTR
h -t 14.596966393 -s 0 -d 1 -p tcp -e 1060 -c 2 -a 0 -l 2923 -k RTR
+ -t 14.597209727 -s 150 -d -1 -p message -e 200 -c 2 -a 0 -l 2919 -k RTR
- -t 14.597209727 -s 150 -d -1 -p message -e 200 -c 2 -a 0 -l 2919 -k RTR
h -t 14.597209727 -s 150 -d -1 -p message -e 200 -c 2 -a 0 -l 2919 -k RTR
r -t 14.597255726 -s 1 -d -1 -p ACK -e 38 -c 2 -a 0 -l 0 -k MAC
+ -t 14.597365726 -s 1 -d -1 -p RTS -e 44 -c 2 -a 0 -l 0 -k MAC
- -t 14.597365726 -s 1 -d -1 -p RTS -e 44 -c 2 -a 0 -l 0 -k MAC
h -t 14.597365726 -s 1 -d -1 -p RTS -e 44 -c 2 -a 0 -l 0 -k MAC
r -t 14.597718059 -s 0 -d -1 -p RTS -e 44 -c 2 -a 0 -l 0 -k MAC
+ -t 14.597728059 -s 0 -d -1 -p CTS -e 38 -c 2 -a 0 -l 0 -k MAC
- -t 14.597728059 -s 0 -d -1 -p CTS -e 38 -c 2 -a 0 -l 0 -k MAC
h -t 14.597728059 -s 0 -d -1 -p CTS -e 38 -c 2 -a 0 -l 0 -k MAC
r -t 14.598032393 -s 1 -d -1 -p CTS -e 38 -c 2 -a 0 -l 0 -k MAC
+ -t 14.598042393 -s 1 -d 0 -p ack -e 110 -c 2 -a 0 -l 2853 -k MAC
- -t 14.598042393 -s 1 -d 0 -p ack -e 110 -c 2 -a 0 -l 2853 -k MAC
h -t 14.598042393 -s 1 -d 0 -p ack -e 110 -c 2 -a 0 -l 2853 -k MAC
r -t 14.598986726 -s 0 -d 0 -p ack -e 60 -c 2 -a 0 -l 2853 -k MAC
+ -t 14.598996726 -s 0 -d -1 -p ACK -e 38 -c 2 -a 0 -l 0 -k MAC
- -t 14.598996726 -s 0 -d -1 -p ACK -e 38 -c 2 -a 0 -l 0 -k MAC
h -t 14.598996726 -s 0 -d -1 -p ACK -e 38 -c 2 -a 0 -l 0 -k MAC
r -t 14.599011726 -s 0 -d 0 -p ack -e 60 -c 2 -a 0 -l 2853 -k AGT
+ -t 14.599011726 -s 0 -d -1 -p tcp -e 1040 -c 2 -a 0 -l 2924 -k AGT
- -t 14.599011726 -s 0 -d -1 -p tcp -e 1040 -c 2 -a 0 -l 2924 -k AGT
h -t 14.599011726 -s 0 -d -1 -p tcp -e 1040 -c 2 -a 0 -l 2924 -k AGT
+ -t 14.599011726 -s 0 -d 1 -p tcp -e 1060 -c 2 -a 0 -l 2924 -k RTR
- -t 14.599011726 -s 0 -d 1 -p tcp -e 1060 -c 2 -a 0 -l 2924 -k RTR
```

Snapshot- Out.tr

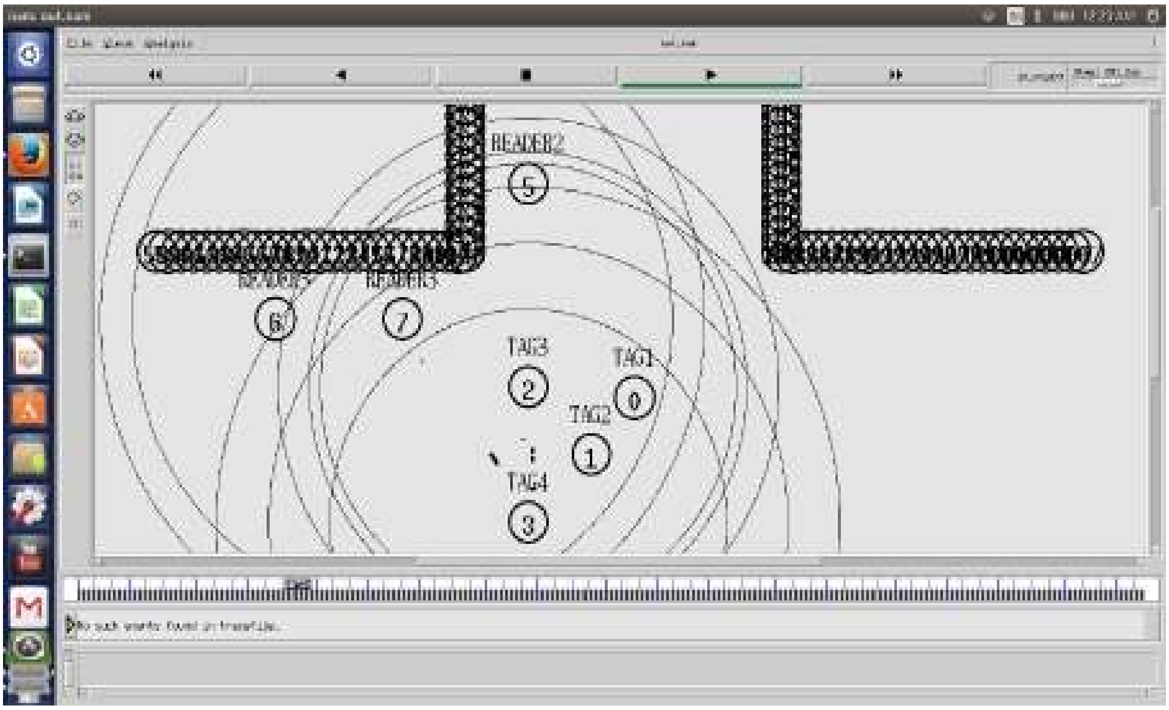
.tr files are also generated for tracing and monitoring simulation and here gnuplot is used for plotting the graphs by extracting the values from the .tr files through grep command and storing the values in awk files which is an analyser. These extracted results are plotted using gnuplot and graphs are generated for result analysis.

The value of time and message transfer are set from the -10 to +10 and the values of packet transfer thus varies between this time is thus considered for final evaluation and graph plotting.

The graph thus generated is a curve as at starting there was no communication between the nodes then nodes started moving and thus communication takes place and rate of message transfer thus increases.

Network 2:

Snapshot -6 shows the entries into the tunnel or jammed area. Here in network – 2 effective communications between nodes is possible because of RFID READERS. The important information exchange takes place through RFID.

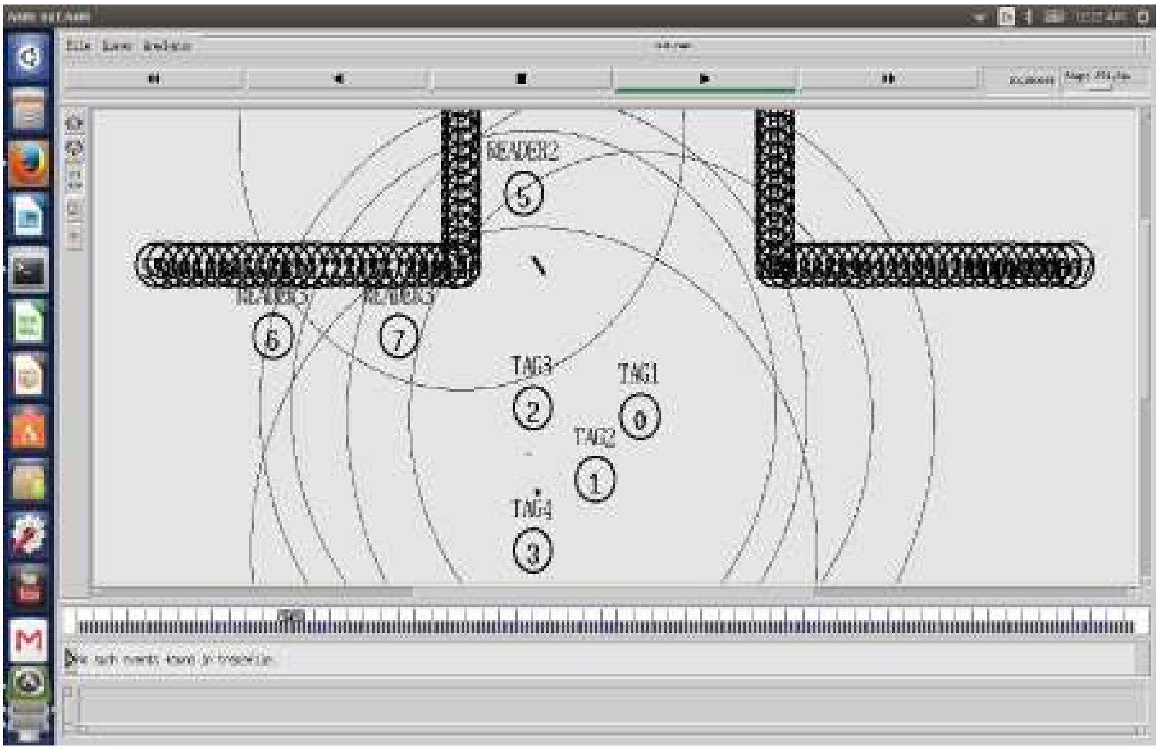


No such events found in tracefile.

Snapshot -6

Snapshot- 7

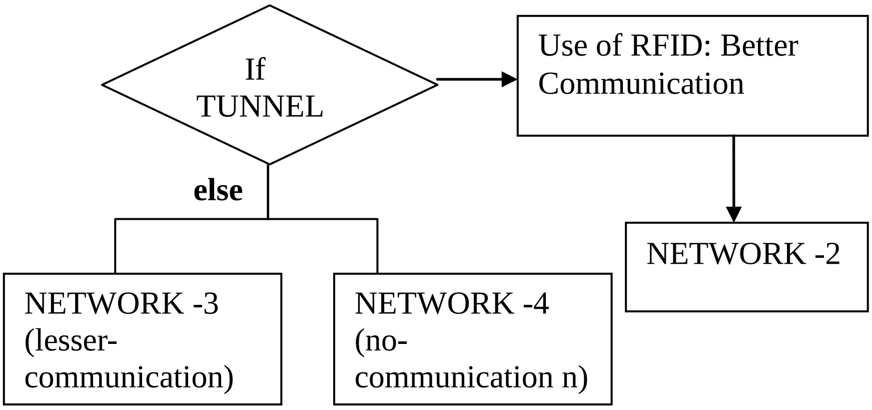
This is also the entrant nodes into the jammed area/tunnel but it shows that nodes are connected to previous network's RFID to which these nodes were connected earlier. This is the case of entrance to the network moreover these nodes will change their RFID readers when they will switch to another network.



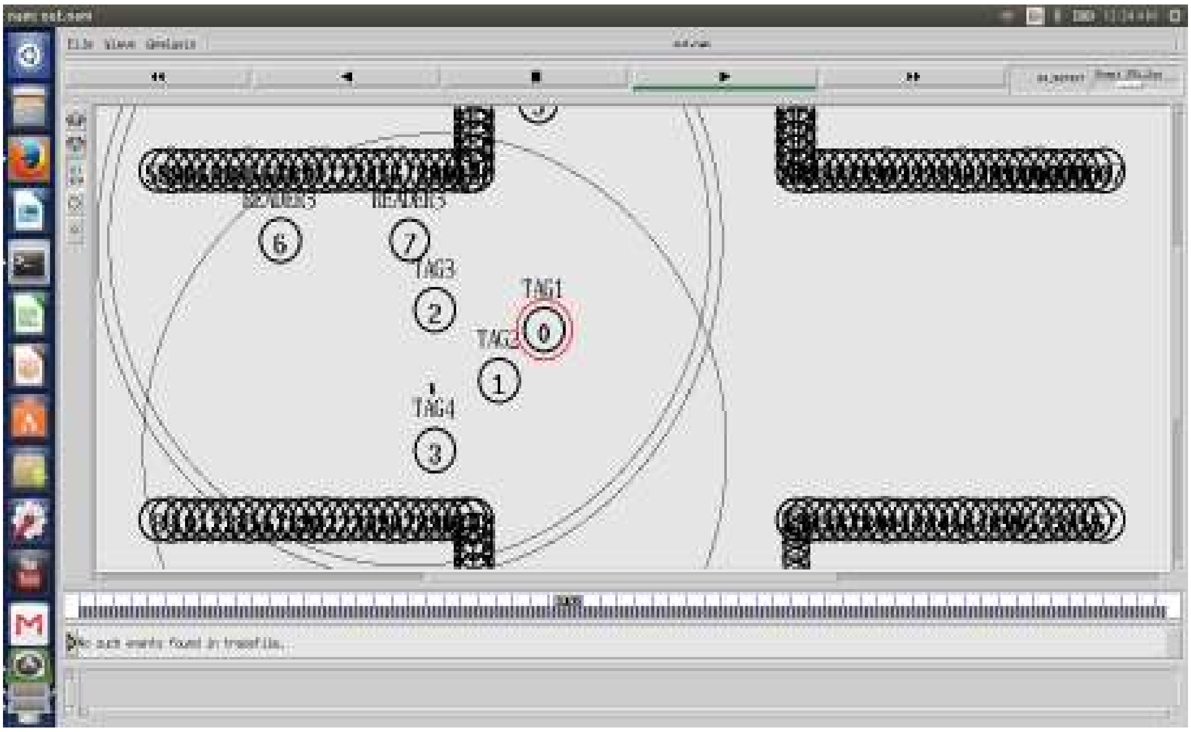
Snapshot- 7

Snapshot- 8

There is a false node in the network that will give wrong information about the paths and about the tunnel. The false node will broadcast the wrong information into the network and there will be better communication even in case of jammed area /tunnel in network -2 as there are RFID for medium of communication between nodes and in network- 3 and network-4 no RFID so lesser communication. False nodes is sending information that there is no tunnel nut in actual there is jammed area .In jammed area the exchange there is kisser network and there is difficulty in exchange of information between the nodes if we are not using RFID. But RFID in the network provides a medium of communication.



The false information is thus broadcasted among the nodes in the network. RFID serves as a medium of communication between the nodes as shown in snapshot-8



No such events found in tracefile.

Snapshot- 8

Information Exchange through RFID AGENTS in NETWORK- 2

There is DHCP server gets all the routing related information. READER of RFID is IP based that reads all the tags and writes the data in the RFID tags. READER works as IP router for all the tags. RFID READERS are polling continuously in the environment so that they can sense the new TAG and can record their entry. There are RFID agents is the application that are attached to reader and RFID tags are the IDs associated with each nodes in the network and agents perform the mapping between tag and IP address. There is one ID server it plays a dual role of storing all the TAG information so that all the nodes can communicate to TAG by taking information from this server as well as from the home agent to provide mobility in the network. An ID server also searches for the entries of the tags and also modifies the IP addresses which are stored into the databases so that they can be used for further communication in the network with the tags.

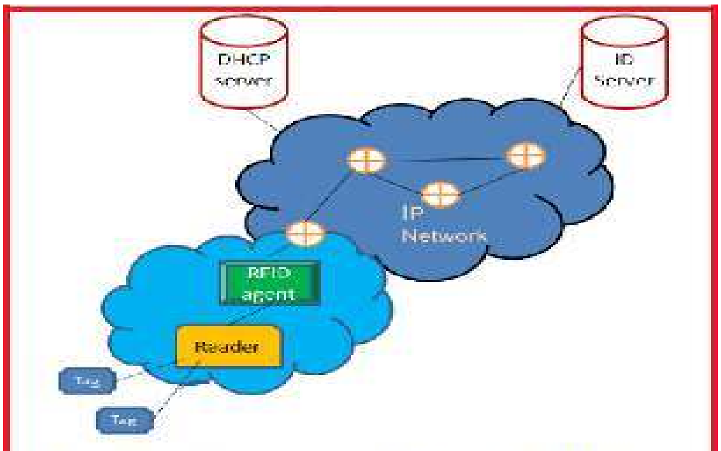
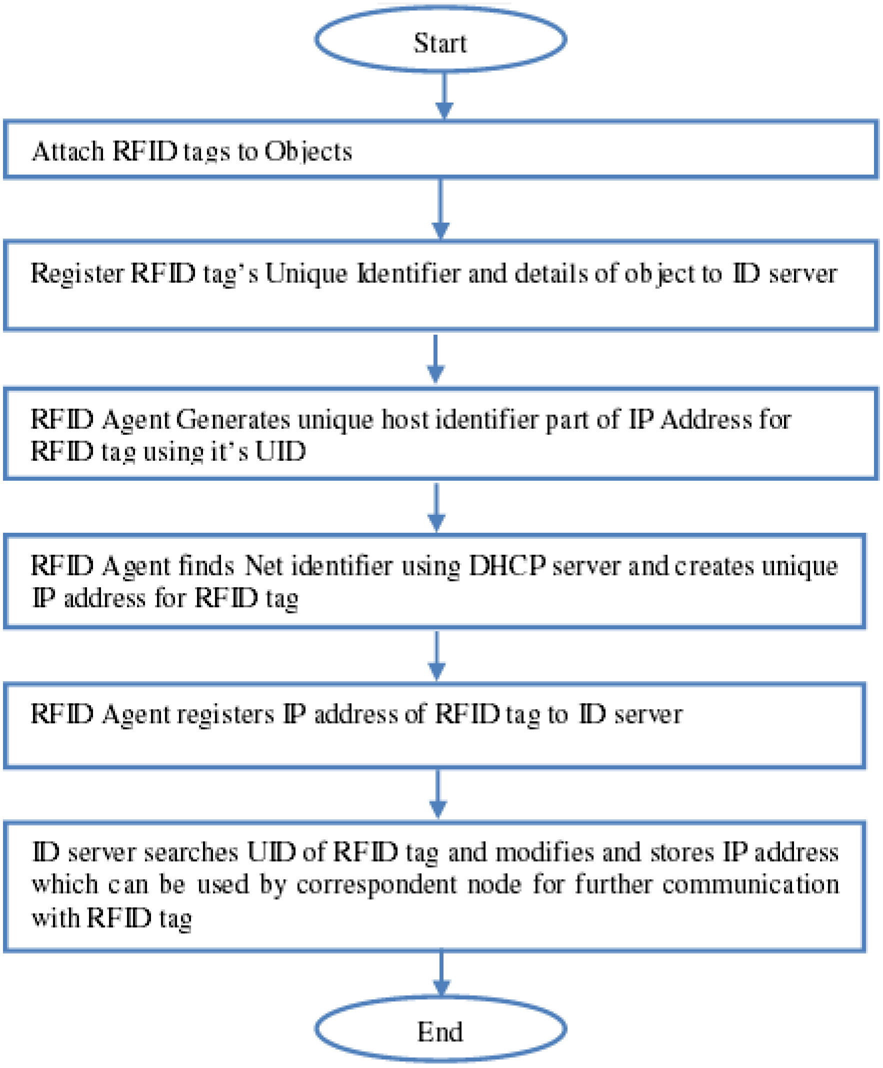


Fig. 13 communication Through RFID

Communication in NETWORK- 2 through RFID:



Start

Attach RFID tags to Objects

Register RFID tag's Unique Identifier and details of object to ID server

RFID Agent Generates unique host identifier part of IP Address for RFID tag using it's UID

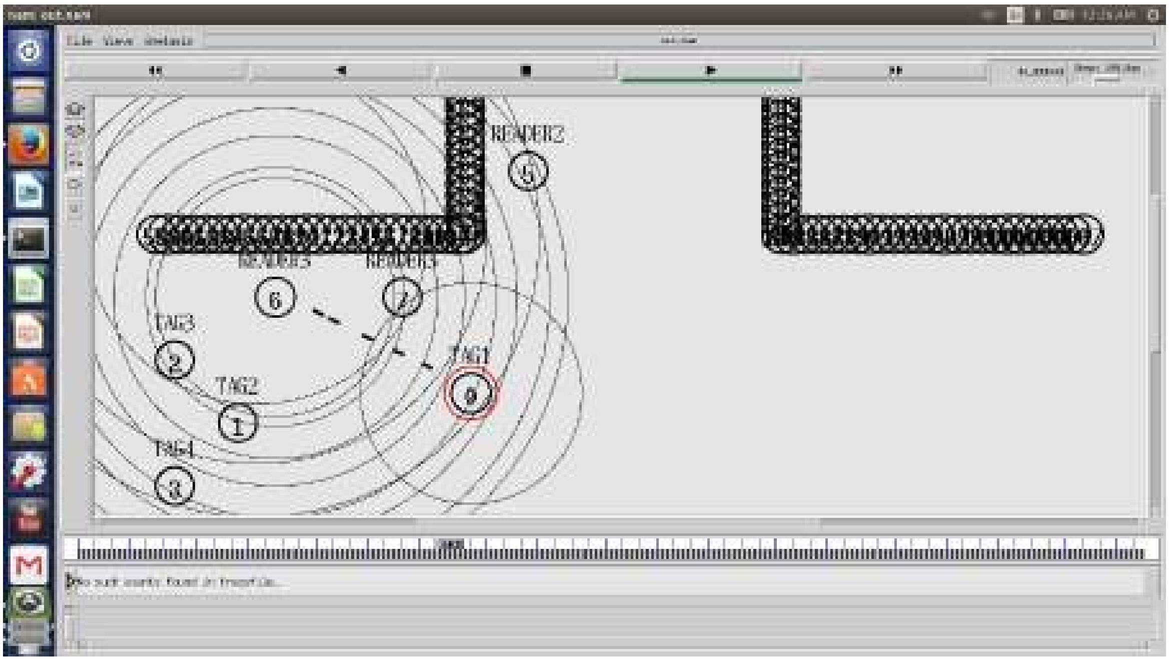
RFID Agent finds Net identifier using DHCP server and creates unique IP address for RFID tag

RFID Agent registers IP address of RFID tag to ID server

ID server searches UID of RFID tag and modifies and stores IP address which can be used by correspondent node for further communication with RFID tag

End

FLOW CHART-3 Communication through RFID

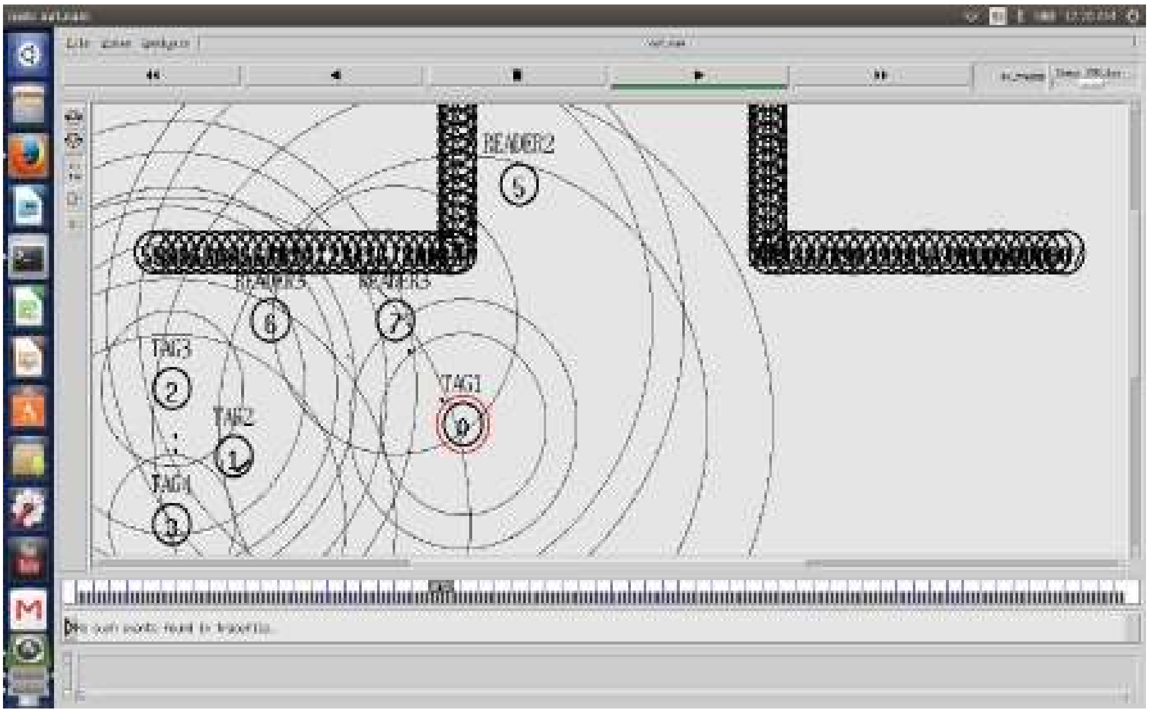


No such events found in tracefile.

Snapshot -9

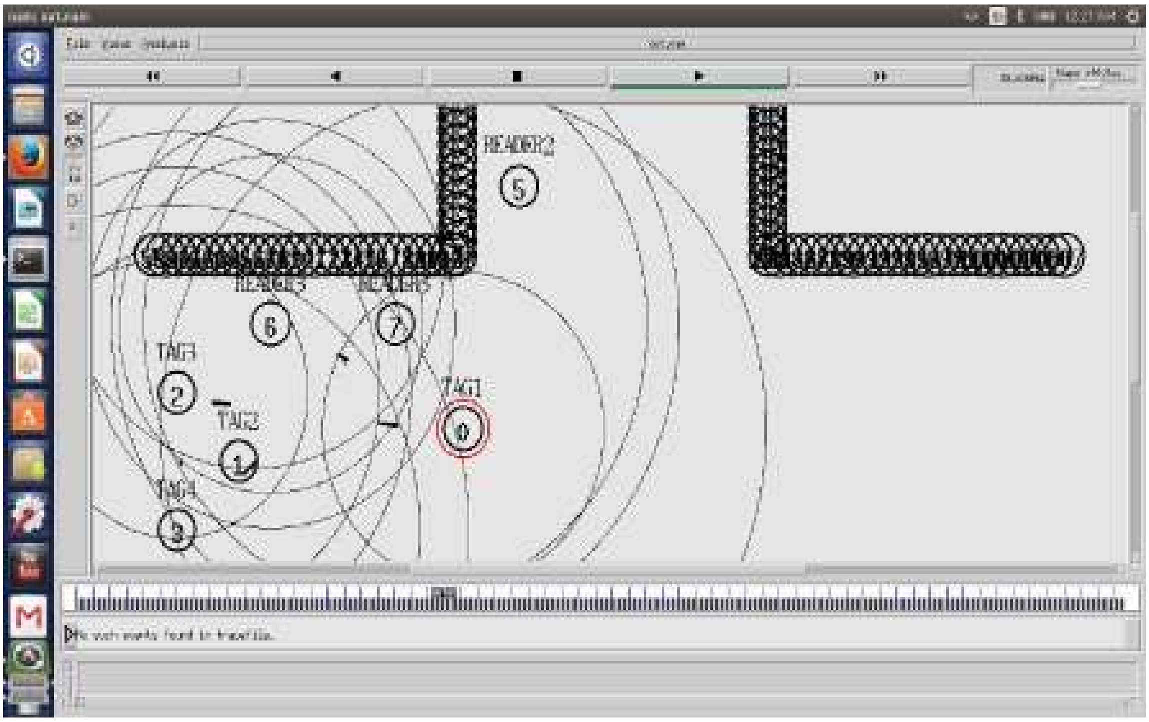
Snapshot- 10, **11**

False node is sending wrong information into the network further exchange of information takes place through RFID and also there is communication between the nodes.



No such events found in tracefile.

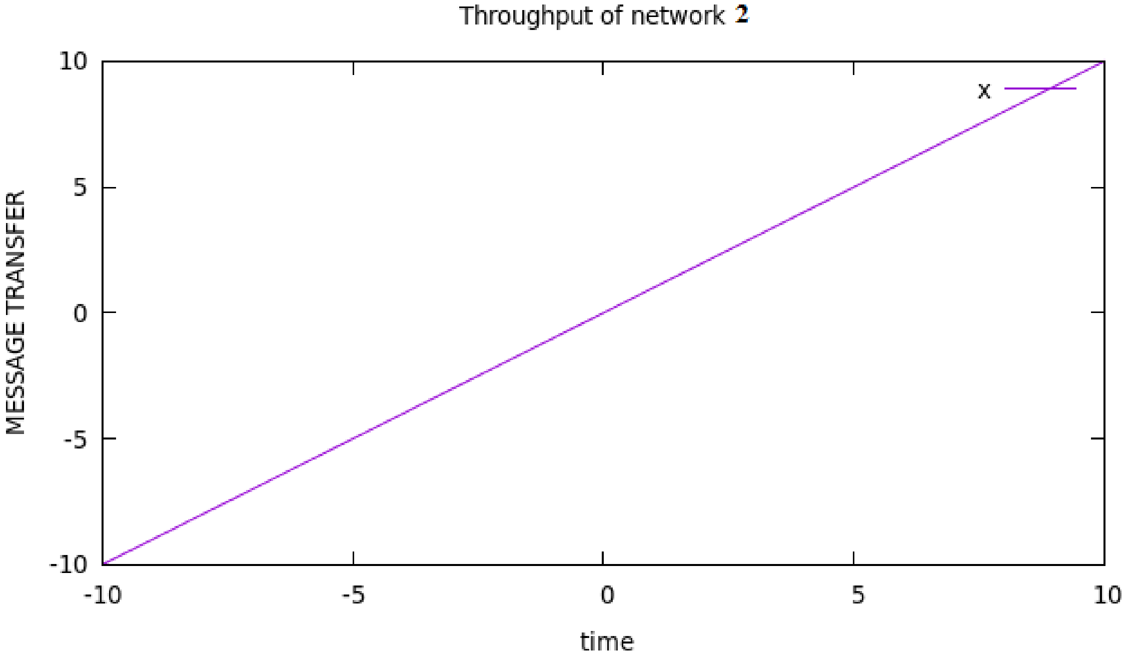
Snapshot -10



No such events found in tracefile.

Snapshot -11

Result Analysis (NETWORK -2)

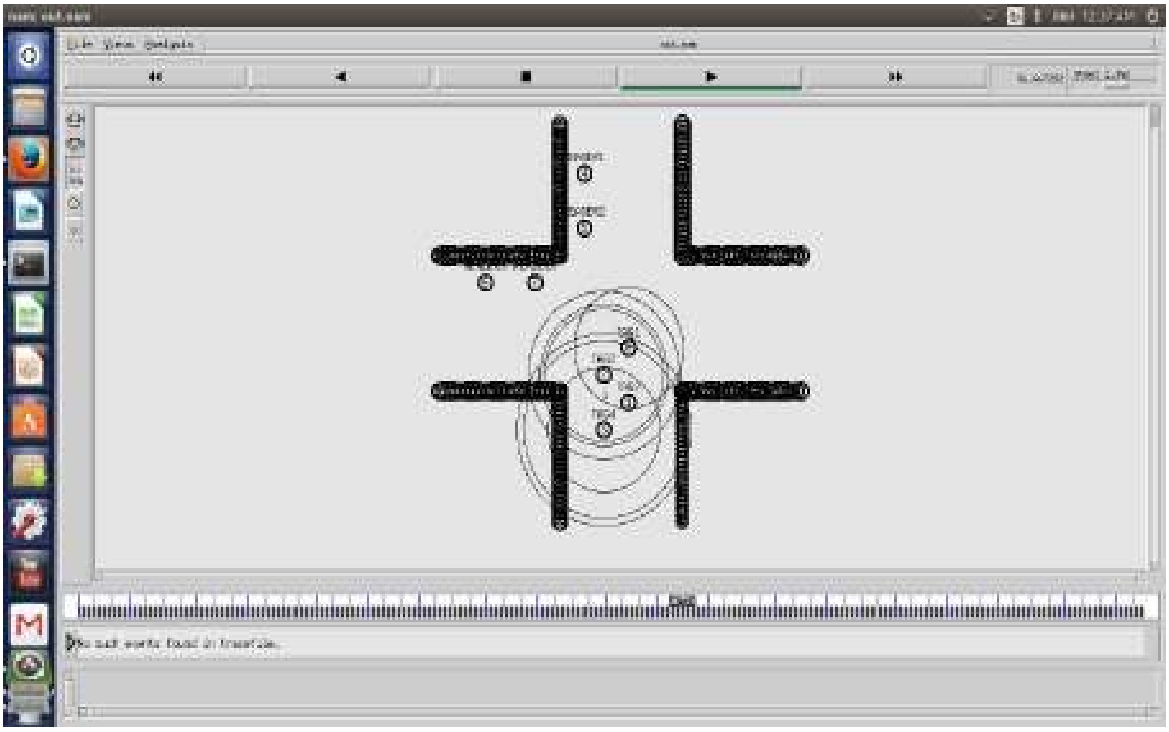


The time here represents the total transmission time it is= time at which packet is send-time at which packet is reached to the destination.

A straight cure is thus obtained after grep command the valued from out.tr files and this straight line represents the maximum communication range between the communicating nodes.

Entrant to network 3:

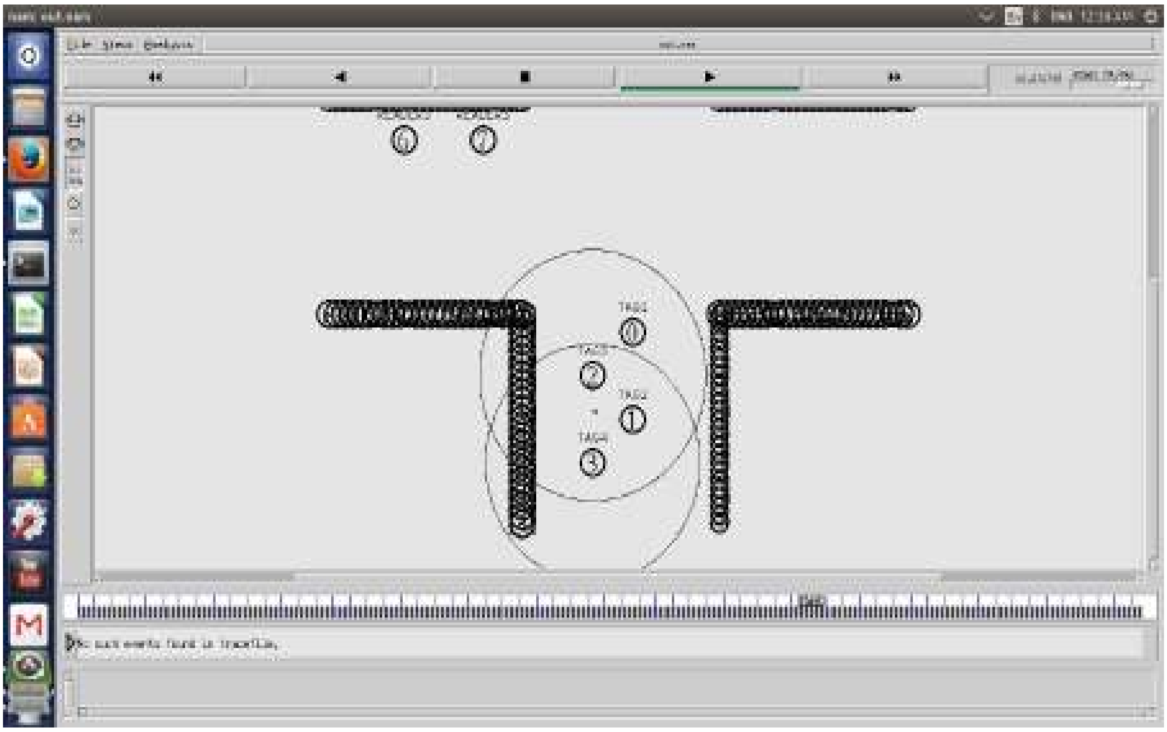
Snapshot -12 Here the nodes are entering into the network -3 .In this network there is no RFID and still a jammed area is there thus the chances of communication are less as no RFID into the network.



No such events found in tracefile.

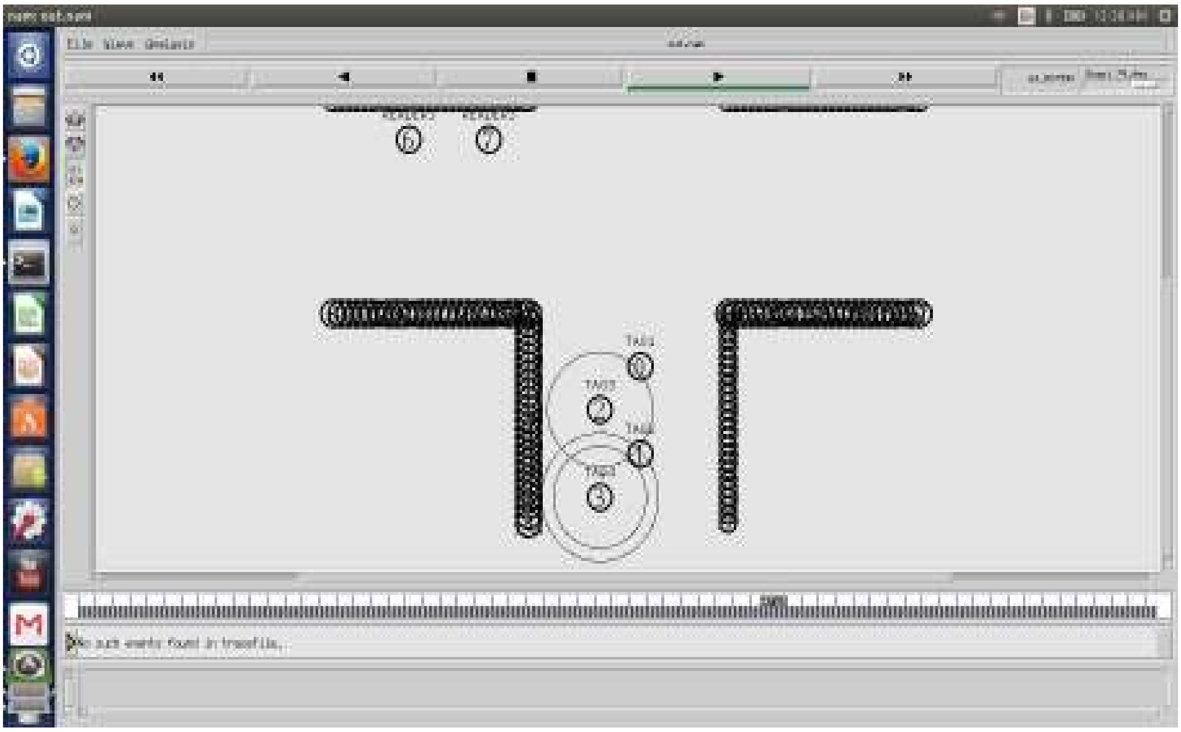
Snapshot -12

Communication takes place between the nodes 2 and node 3 only which is also not at frequent rate in snapshot 13 and 14.



No such events found in tracefile.

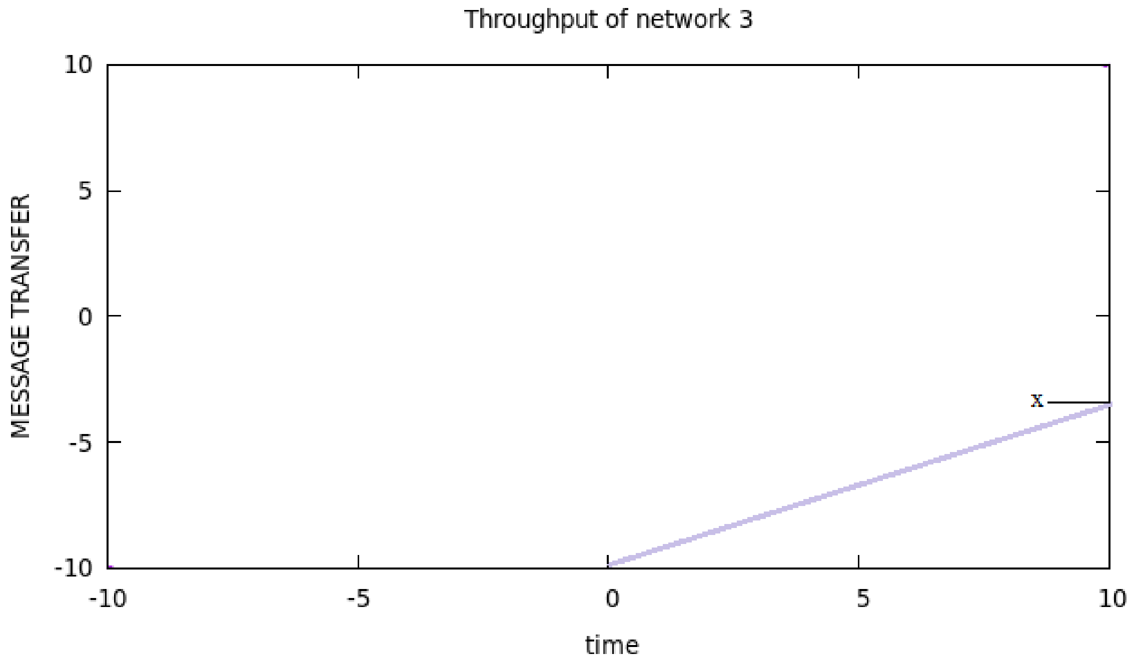
Snapshot -13



No such events found in tracefile.

Snapshot -14

Result analysis:



Time= time at which packet was sent- delivered time of packet.

Thus throughput is thus calculated a curve is obtained in gnuplot by awk file.

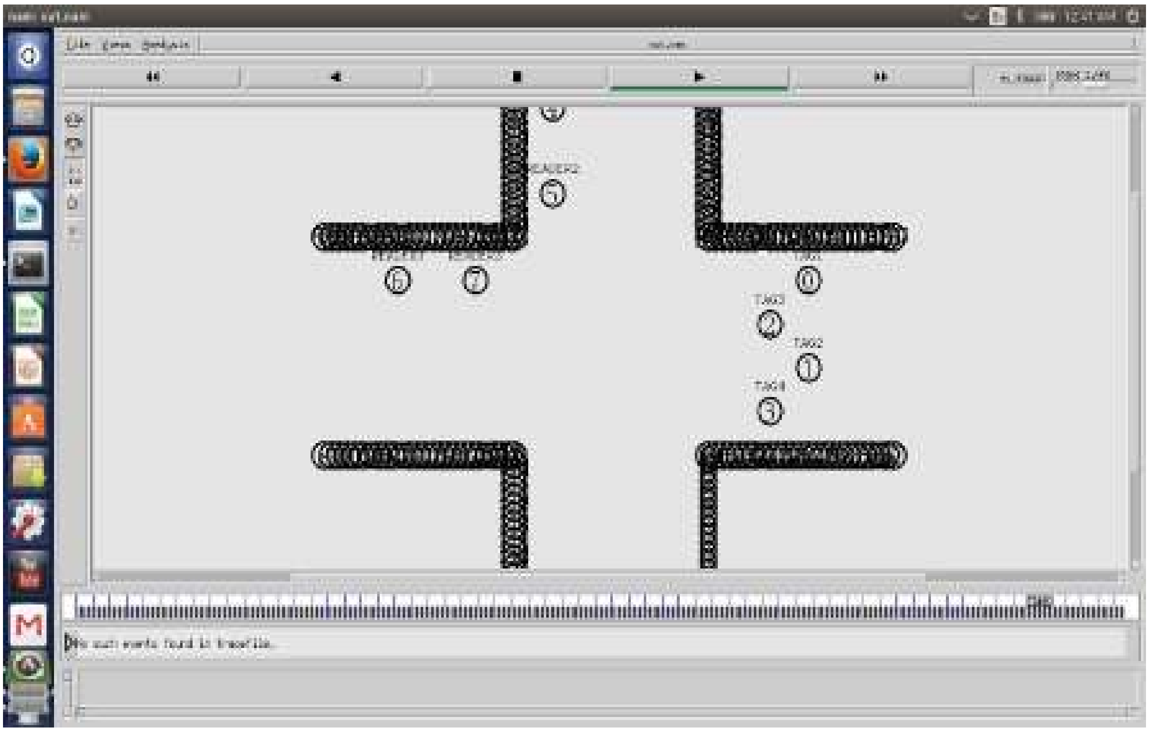
There is min throughput of the network thus resulted because of lesser communication into the network.

Since here no RFID is present into the network so there is lesser communication among the nodes and thus the graph shows minimum values traced in it.

Network- 4

Since network-3 represents the case that without RFID there is lesser communication in the jammed area. This network represents the case that there me be no communication between the nodes in absence of RFID in the jammed area.

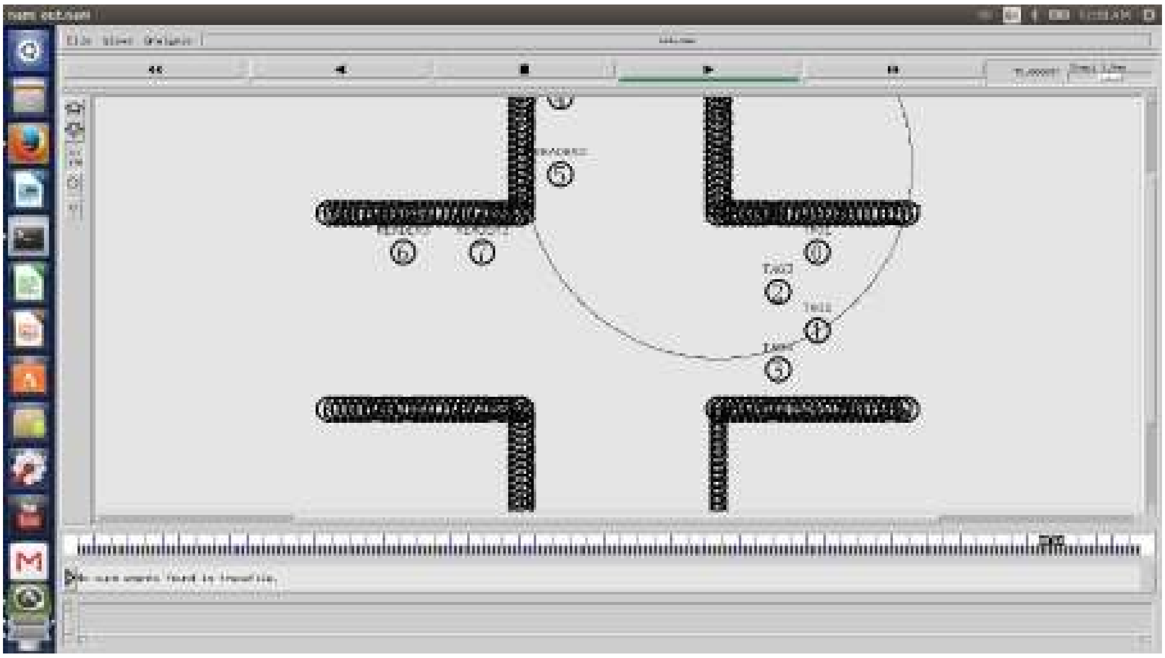
TAG1, TAG2, TAG3, TAG4 all are just moving entities into the network without any communication so there is no ID server to record entries of each node and thus no communication between the nodes takes place.



No such events found in tracefile.

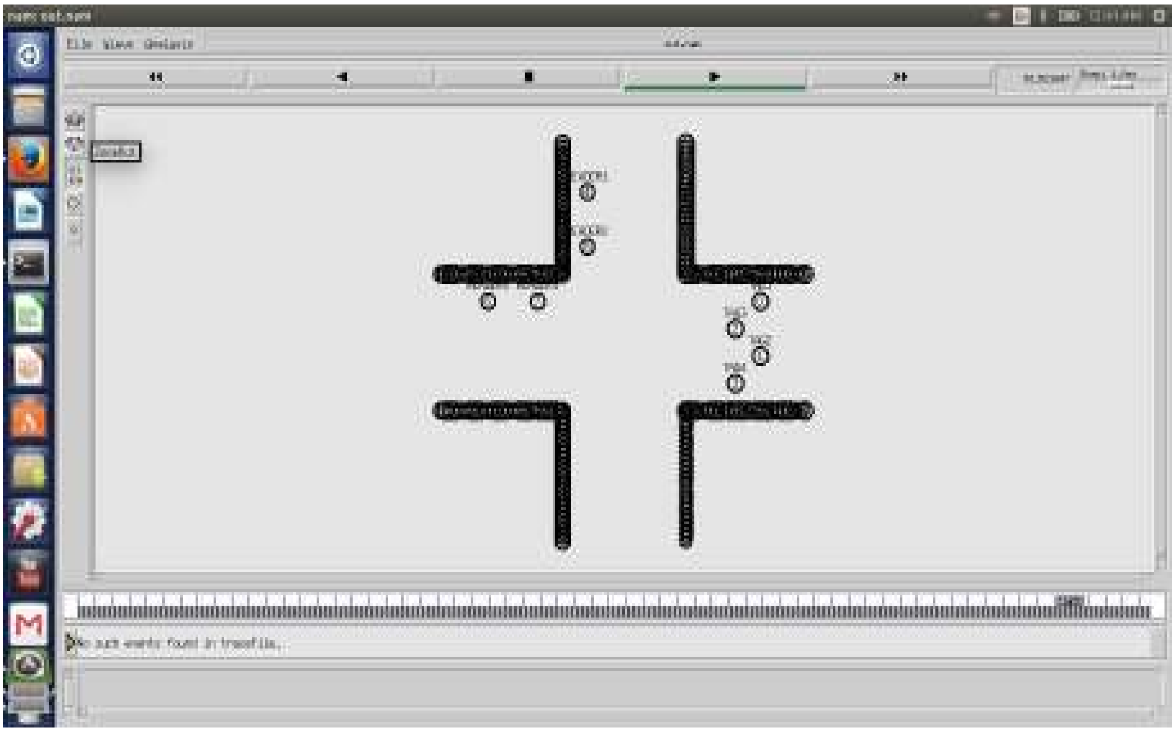
Snapshot -15

Snapshot 16, 17 represents all the four networks and network 4 without any communication between the nodes.



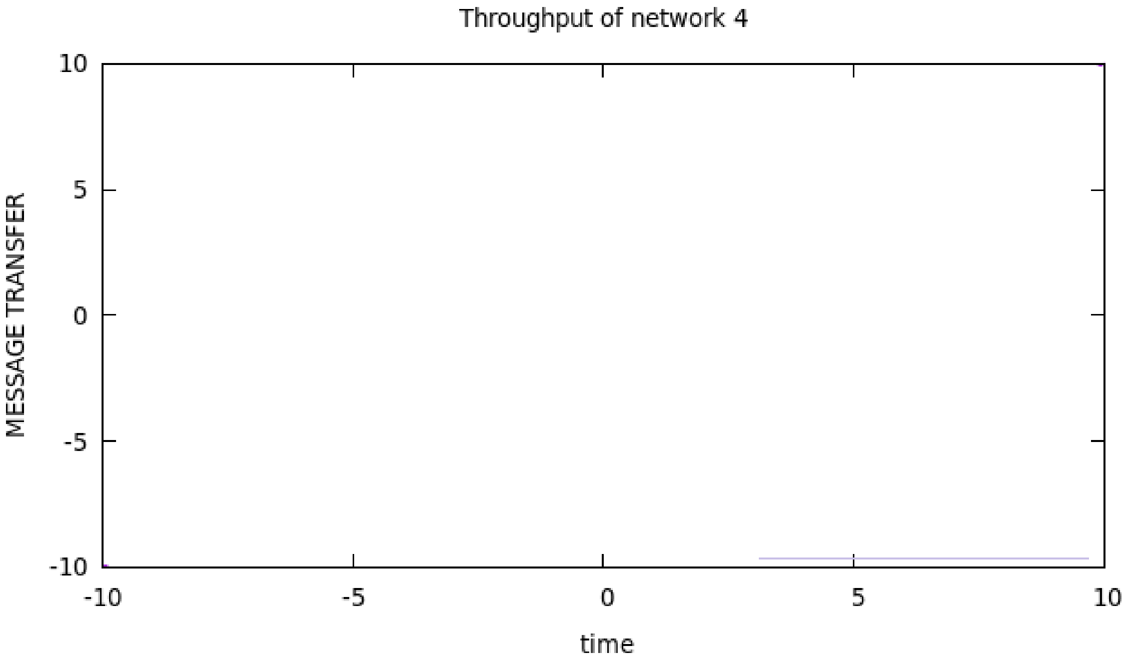
No such events found in tracefile.

Snapshot -16



Snapshot -17

Result analysis:



No communication so throughput of sending the message is negligible here as there is no communication among the nodes.

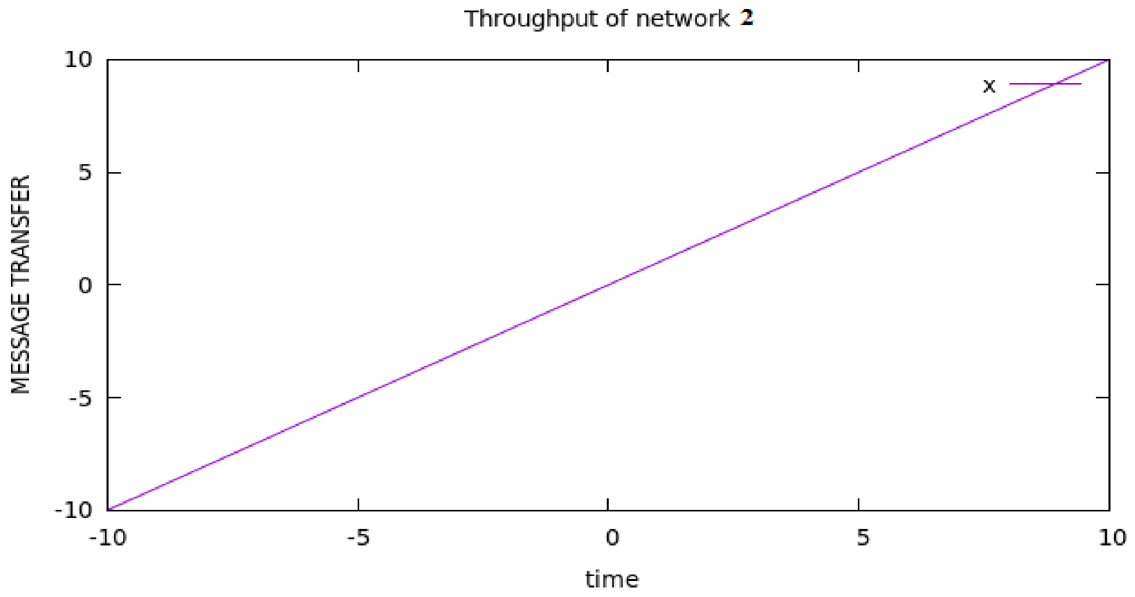
Comparison between the network performances

The throughput thus calculated for the message transfer rate depends on the transmission range and thus the difference between the two times the transmission and delivery is calculated

Transmission time= time of delivery – time to reach the packet to destination.

Transmission time* distance = throughput of the network.

Thus the comparison study shows that the throughput is more in case of network 2 where RFID are used in jammed area as a medium of communication.



Chapter 5

CONCLUSIONS AND FUTURE SCOPE

Sometimes there may be the case that there is a false node in the system that may also cause delay in the transfer of data between the communicating nodes.

By the help of groups we can track the location of false node from the node to which it was communicating. After detecting the location of the node we can detect whether the node was actually not transferring the data was false node or there was a problem in the network. RFID can sense the network and thus we can detect the status of the nodes whether there was a tunnel in reality or it was only because of the false node in the network.

In order to have more and more security from intruder into the network there should be the usage of RFID tags into the network within the tunnel it will help us in sustain our databases and records of all the nodes so that only the authenticated nodes can enrol into the network. We can also have a check on false node so that the availability of the nodes can be easily accused and we can preclude our network from false node. Since now network is secure then no attack on the confidentiality. As now we have a confidential network then there will be no attack on security of the network. These all are preventive measures for the attack while intruder is entrant or inside the tunnel and when all the traffic is exiting from the tunnel then we can deviate all the nodes onto a different network as all the nodes even a selfish node can be easily traced thus we have a better network security and no attack vulnerabilities while entering, inside the tunnel and after exiting the tunnel. Thus we have a secured network.

Tunneling attack can be prevented as the methods suggested in the report. But in case if the false node is not detected within the network and then we can prevent the attack inside the tunnel only by using RFID.

Since the ID server contains the record of each node but even if it’s not possible to find out the false node within the network then use watch dog mechanism to find out the false node into the network.

In watchdog mechanism a monitoring on the each activity in the system takes place.

Watchdog is basically a component which is used for the detection of false/ selfish nodes into the network. All the nodes sends packets into the network and then watchdog verifies the nodes which are in between the paths also forwards the packets into the network. When a packet is send by any node into the network then watchdog is set and also ensures that all nodes in the path are sending the information or forwarding the packets. If next adjacent node doesn’t forwards the packet into the network then watchdog listens to the transmitting nodes that are within the range and ensures that the node is misbehaving. If match confirms then it discards the node from the network thus the false node can be easily detected into the network.

Chapter 5

LIST OF REFERENCES

1. Mohammed Saeed Al-kahtani “Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)” Computer Engineering Dept., Salman bin Abdulaziz University, Saudi Arabia 2012.

2. Farzad Sabahi “The Security of Vehicular Adhoc Network, “Third International Conference of Computational Intelligence, Communication Systems and Networks, 2011.

3. Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, “A framework for reliable routing in mobile ad hoc networks,” in Proc. IEEE INFOCOM, Apr. 2003, pp. 270–280.

4.1. Anup Dhamgaye, 2.Nekita Chavhan “Survey on security challenges in VANET 1 Wireless Communication and Computing”, Dept. of CSE, G. H. Raisoni College of Engineering, Nagpur, India 2 Dept. of CSE, G. H. Raisoni College IJCSN International Journal of Computer Science and Network, Vol 2, Issue 1, 2013

5. PARNO B., PERRIG A.: „Challenges in securing vehicular networks". Fourth Workshop on Hot Topics in Networks (Hot Nets-IV), 2005

6. FLORIAN D., LARS F., PRZEMYSLAW M.: „VARS: a vehicle ad hoc network reputation system. Int. Conf. on a World of Wireless, Mobile and Multimedia Networks”(WOWMOM 2005), 2005, pp. 454–456

7. Adil Mudasir Malla Ravi Kant Sahu “Security Attacks with an Effective Solution for DOS Attacks in VANET ” International Journal of Computer Applications (0975 – 8887) Volume 66– No.22, March 2013.

8. José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda ,“Overview of security issues in Vehicular Ad-hoc Networks,”2007.

9. Swapnil G. Deshpande “Classification of Security attack in Vehicular Adhoc network: A survey” in the department of Arts, Commerce, Science College, Kiran Nagar, Amravati, Maharashtra, India.2011.

10. Mohammad Fanaei', Mehdi Berenjkoub, Ali Fanian ,“Resistant TIK-Based endairA Against the Tunneling Attack” Department of Electrical and Computer Engineering, Isfahan University of Technology (IUT), Isfahan, Iran2008.

11 S. Park, B. Aslam, D. Turgut, Cliff C. Zou, “Defence against Sybil attack in vehicular ad-hoc network based on roadside unit support”. In: MILCOM, pp. 1–7.

12 Farzad Sabahi “The Security of Vehicular Adhoc Networks” Computer Engineering in Azad University, Iran 2011

13.Bayrem Triki, Slim Rekhis, Mhamed Chammem, and Noureddine Boudriga, “A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Networks” Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP, Digital Object Identifier: 10.1109/WMNC.2013.6549051 Publication Year: 2013 , Page(s): 1

14. A. Perrig, and D. Song “Random key pre-distribution schemes for sensor networks”.

In IEEE Symposium on Security and Privacy, pages 197–213, Berkeley, California, May 11-14 2003**.**

15. LEE, E.-K., YANG, S., OH, S. Y., AND GERLA, M “RF-GPS: RFID assisted localization in vanets” Mobile Adhoc and Sensor Systems, 2009.IEEE 6th
International Conference on (October 2009).

16. M. Raya and J.-P. Hubaux, (2007) “Securing vehicular ad hoc networks.” Journal of Computer Security, 15(1), 39–68.

17. Jun-ZhaoSun, Machine Vision & Media Process Unit, Oulu Univ, Finland: “Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”, pp. 316 -321 vol.3, 2001.

18. L. Eschenauer and V. D. Gligor, “A key- Management scheme for distributed sensor networks”.In Proceedings of the 9th ACM conference on Computer and communications security, November 2002.

19. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile ad hoc networks,” in *MOBICOM*, 2000, pp. 255 –265.

20. R. Parker, S. Valaee: “Vehicle localization in Vehicular Networks” .in: Vehicular Technology Conference, 2006. VTC 2006 Fall 2006 IEEE 64th, 2006, pp. 1–5.

21. Hou Wang, Chunxiao Chigan, “Countermeasure Uncooperative Behaviour with Dynamic Trust-Token in VANETs” Communications, 2007. ICC ’07. IEEE International Conference on Digital Object Identifier: 10.1109/ICC.2007.652 Publication Year: 2007, Page(s): 3959-3964.

22. “IEEE trial-use standard for wireless access in vehicular environments (wave)- security services for applications and management messages,”IEEE, New York, NY, IEEE Std 1609.2, Jul. 2006.

23 S. Capkun, L Buttyan, J-P Hubaux, “SECTOR: Secure Tracking of Node Encounters in Multichip Wireless Networks,” Proc. ACM Wksp. Sec. of Ad Hoc and Sensor Networks, Fairfax, VA, Oct. 2003.

Chapter 6

APPENDIX

1. MANET	Mobile Adhoc Network.
2. VANET	Vehicular adhoc network.
3. RFID	Radio Frequency Identification Number.
4. WLAN	Wireless Local Area Network.
5. ADHOC	random change in topology of the network.
6. Tunneling Attack	An attacker connects two distinct parts of the network using an extra communication channel as a tunnel.
7. EPC	Electronic Product Code