Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

ADVANCE MECHANISM TO DETECT PACKET DROPPING ATTACK IN MOBILE AD-HOC NETWORK

Brijesh V. Patel
Computer Science& Engineering, Parul Institute of Engineering
Limda,Waghodia,Vadodara,Gujarat

Abstract— Mobile means to move any direction and ad-hoc means temporary infrastructure less network. In mobile ad-hoc network packet sending and receiving is most important things. Packet Dropping is highly Challenges in Mobile ad-hoc network. Packet Dropping due to link error, malicious node and energy of the node. In existing system energy consumption parameter not consider so energy of the node is important parameter. Here packet send to one node to another node at this time if node energy is less so few time node send packet to another node when energy is zero then link is fail and drop the packet and low network life time.

Keywords-Mobile ad-hoc network (MANET), malicious node, Packet drop Attack, selfish,Packet Delivery ration(PDR).

I. INTRODUCTION

Mobile ad-hoc network is infrastructure less network. It is internet protocol based network of mobile wireless mechanism nodes connected with each other. The node of MANET have not have centralized mechanism. Each device move to in any direction and will therefore change its link to other device frequently[1].

Types of mobile Ad-hoc network[2]:

A. Vehicular ad-hoc network(VANETs)

VANETS are used for communication among vehicles and road side equipment.

B. Intelligent Vehicular Ad Hoc Networks (inVANETs)

It is kind of artificial intelligence that helps vehicles to behave in intelligent manners during the vehicles to vehicles collision, accident, drunken driver etc.

C. Internet Based Mobile Ad Hoc network(iMANETs)

Ad-hoc networks that link mobile node to fixed internet gateway node. In such a type of networks normal ad-hoc algorithm is not apply.

In mobile ad-hoc network packet may be dropped using many ways:

A. Unsteadiness of the medium[3]
- When link is broken packet may be dropped
- When heavy traffic in medium packet may be dropped.
- When confusion in medium packet may be dropped.

B. Genuine of node
- When over flow of transmission queue.
- When lack of energy resources due to packet is dropped.

C. Selfishness of the node
- Packet dropped due to selfishness of node to save the resources.

D. Malicious of the node
- When malignant node acts of malicious node so packets are dropped.

II RELATED WORK

Related Work can be classified in following two categories

(1) High malicious dropping rates[5]

The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the impact of link errors is ignored. Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into four sub-categories.

- **Credit systems**

A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic.

- **Reputation systems**

A reputation system relies on neighbors to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. Consequently, a malicious node will be excluded from any route.

- **End-to end or hop-to-hop acknowledgements**

To directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route.

- **Cryptographic methods**

Bloom filters used to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates.

(2) Number of maliciously dropped packets is significantly higher than that caused by link errors[4]

The second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

III EXISTING SYSTEM ARCHITECTURE

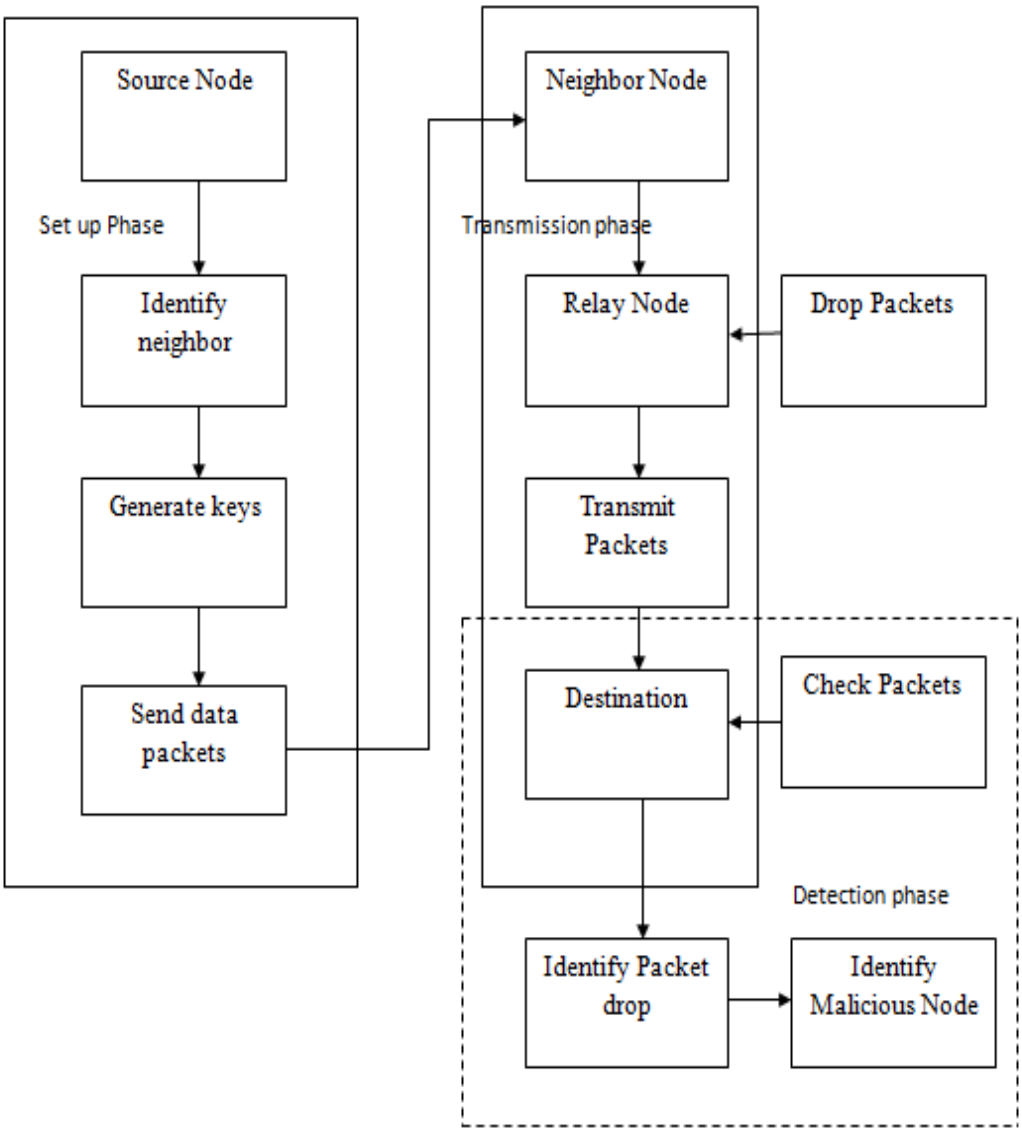
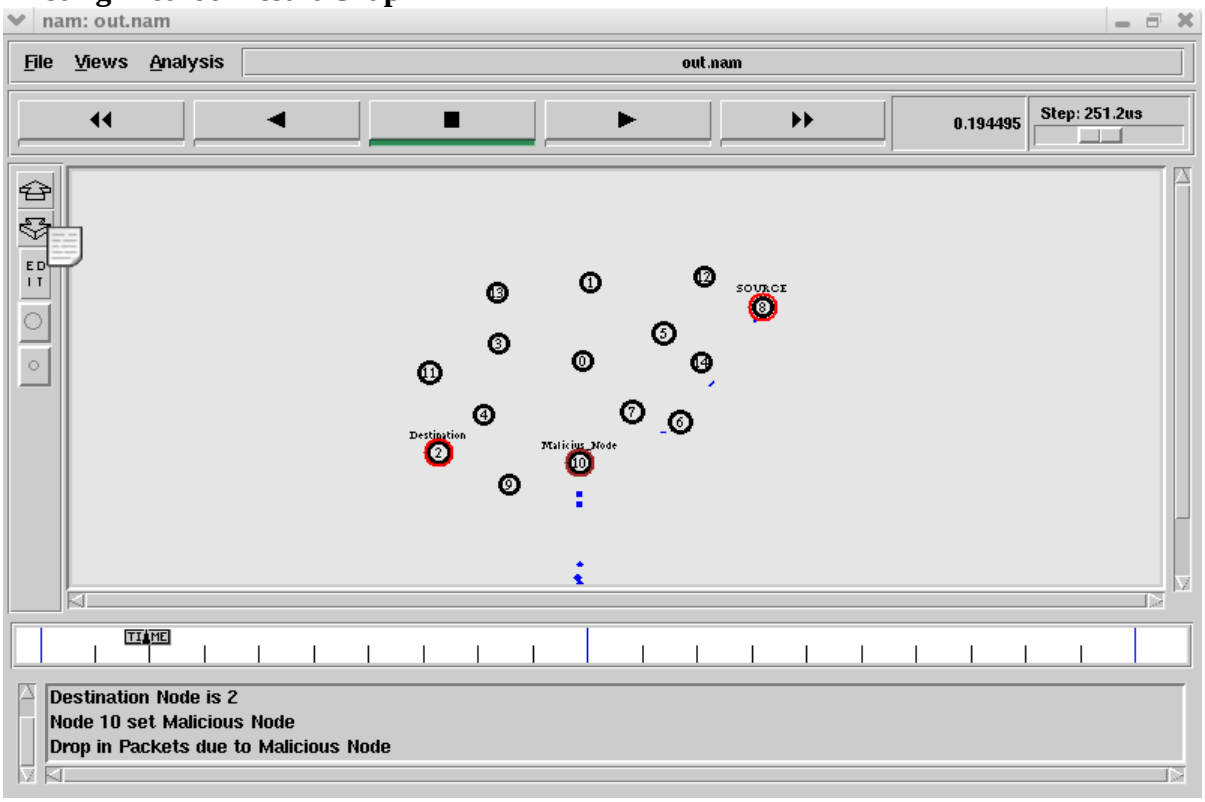


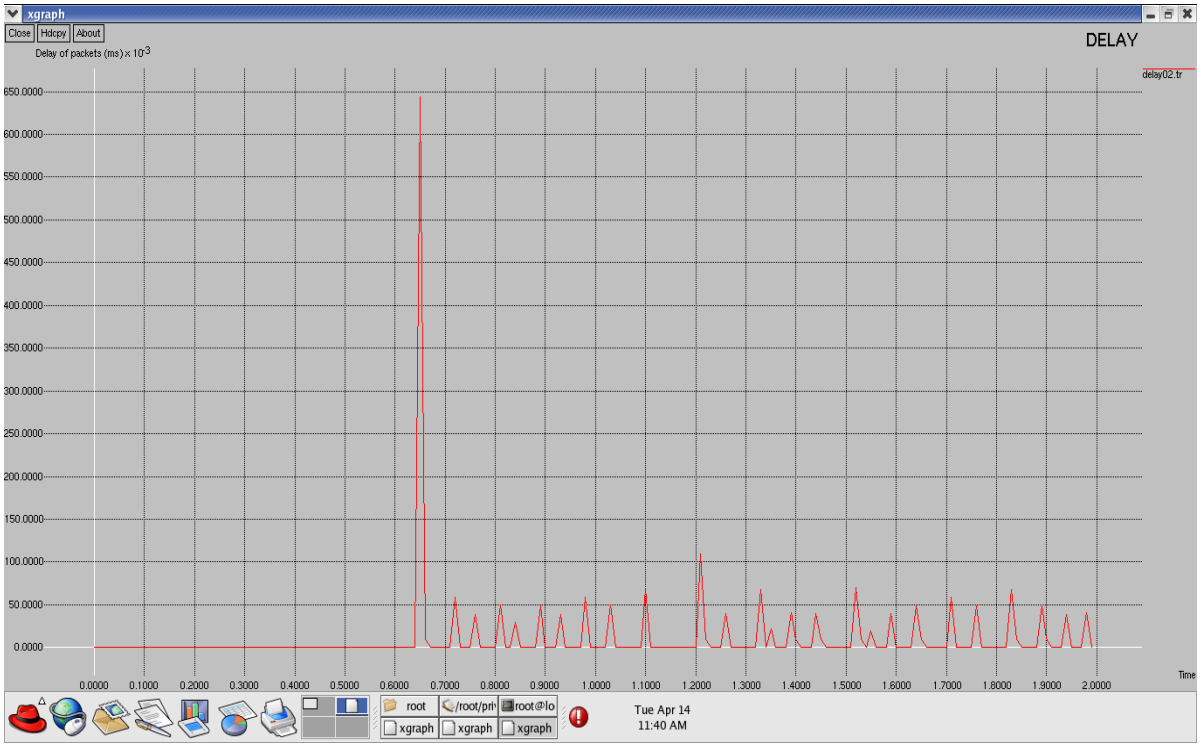
FIG 3.1 EXSTING SYSTEM ARCHITECTURE

Here above fig 3.3 existing system architecture there are three phase set up phase, transmission phase and Detection phase. In first set up phase source node indentify neighbor node where the packet is send or choose the route. After neighbor node decided generate the key send packet. So after this detection phase start in detection phase relay node drop the packet go to destination phase in this phase check the packet of identify packet drop and identify malicious node.

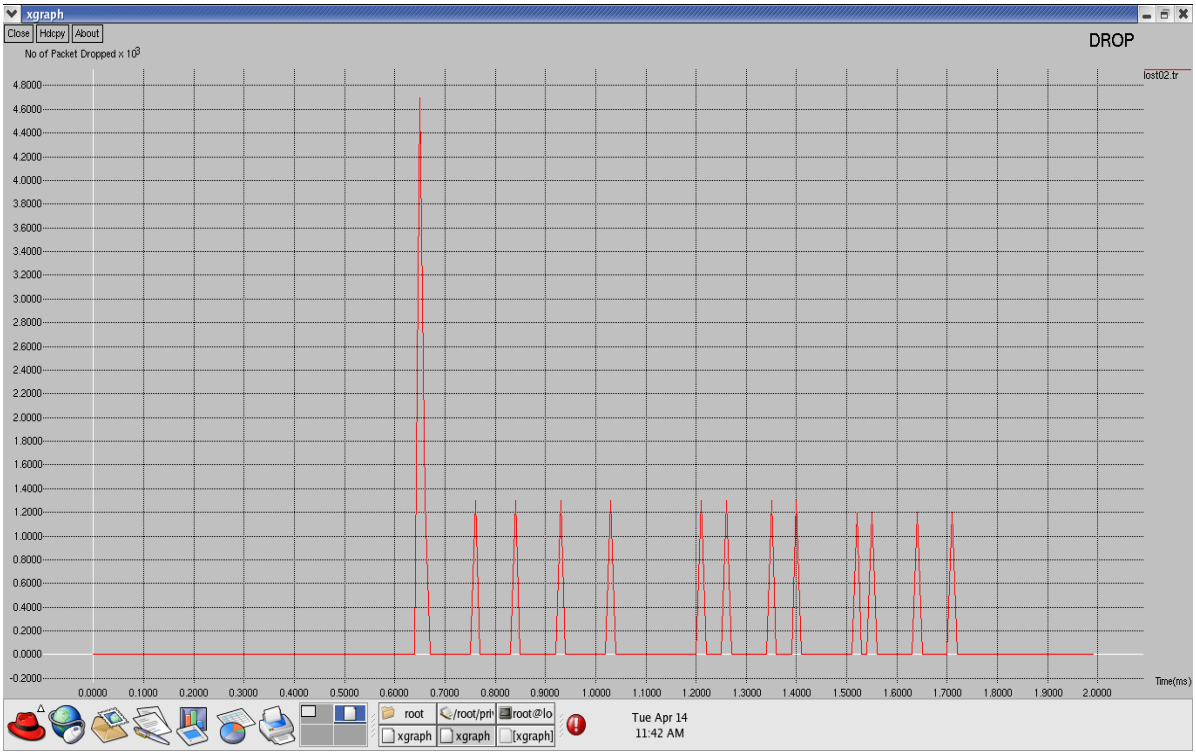
Existing Method Result Graph



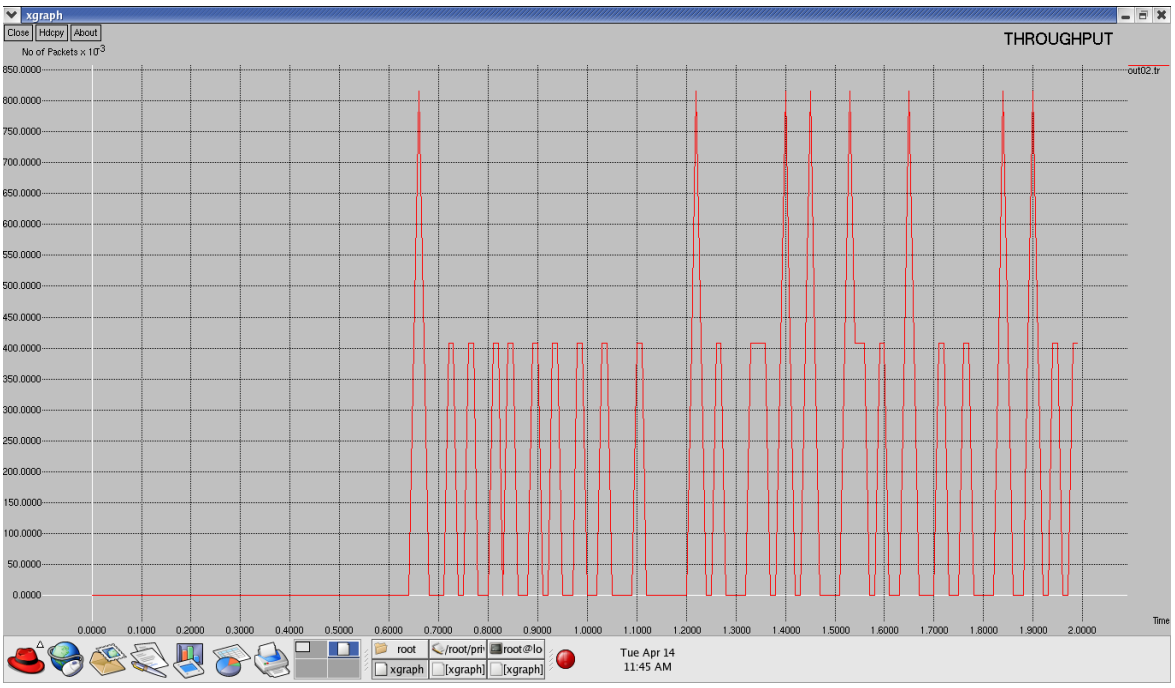
Identifying Source node and Destination node.Node 2 act as a destination node and node 8 act as source node.Drop in packet due to Malicious node.



Snap for Delay Time



Snap For Packet Drop



Snap For Throughput

In existing system Energy consumption is not considered. Here packet send to one node to another node at this time if node energy is less so few time node send packet to another node when energy is zero then link is fail and drop the packet and low network life time.

IV PROPOSED SYSTEM AECHITECTURE

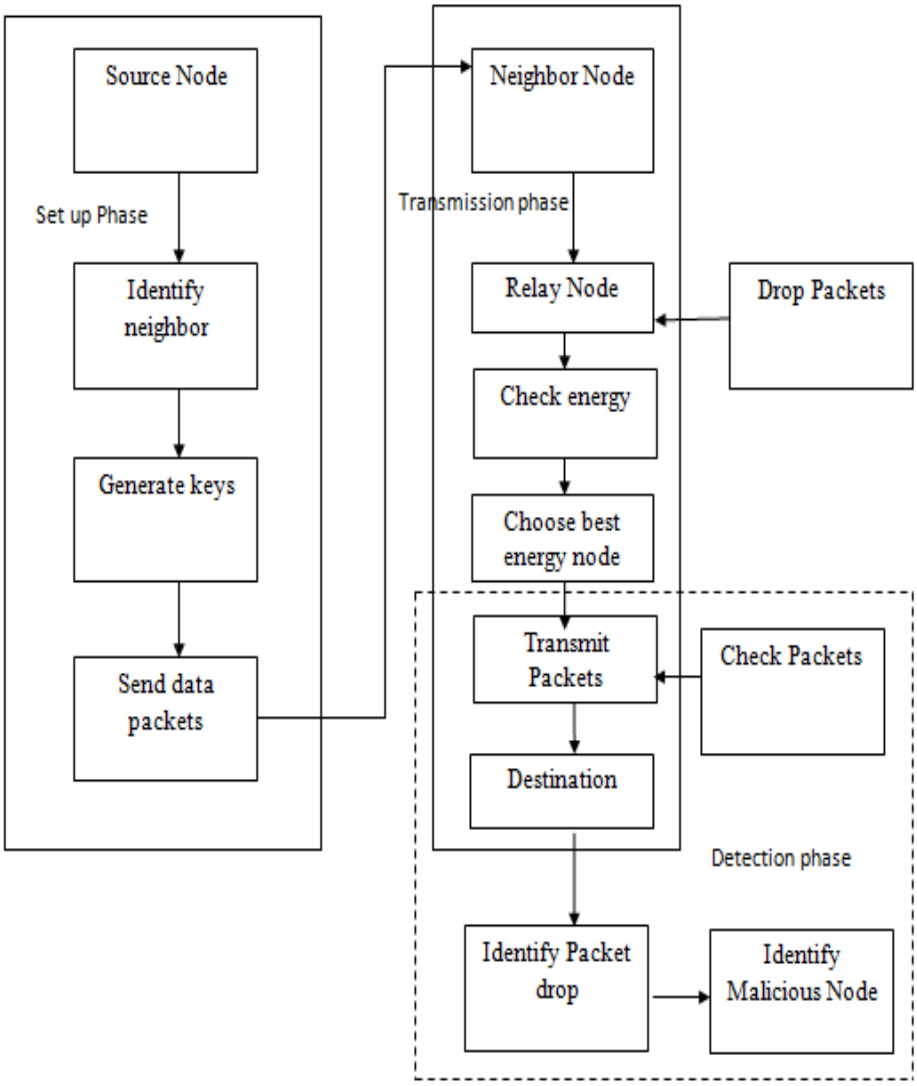
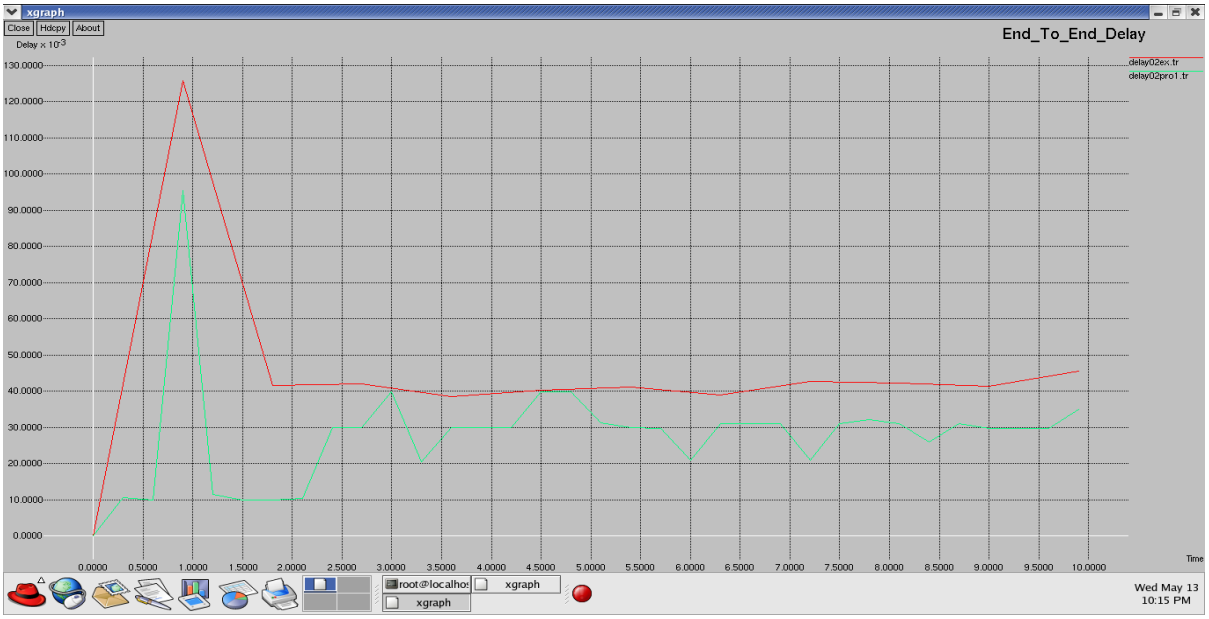
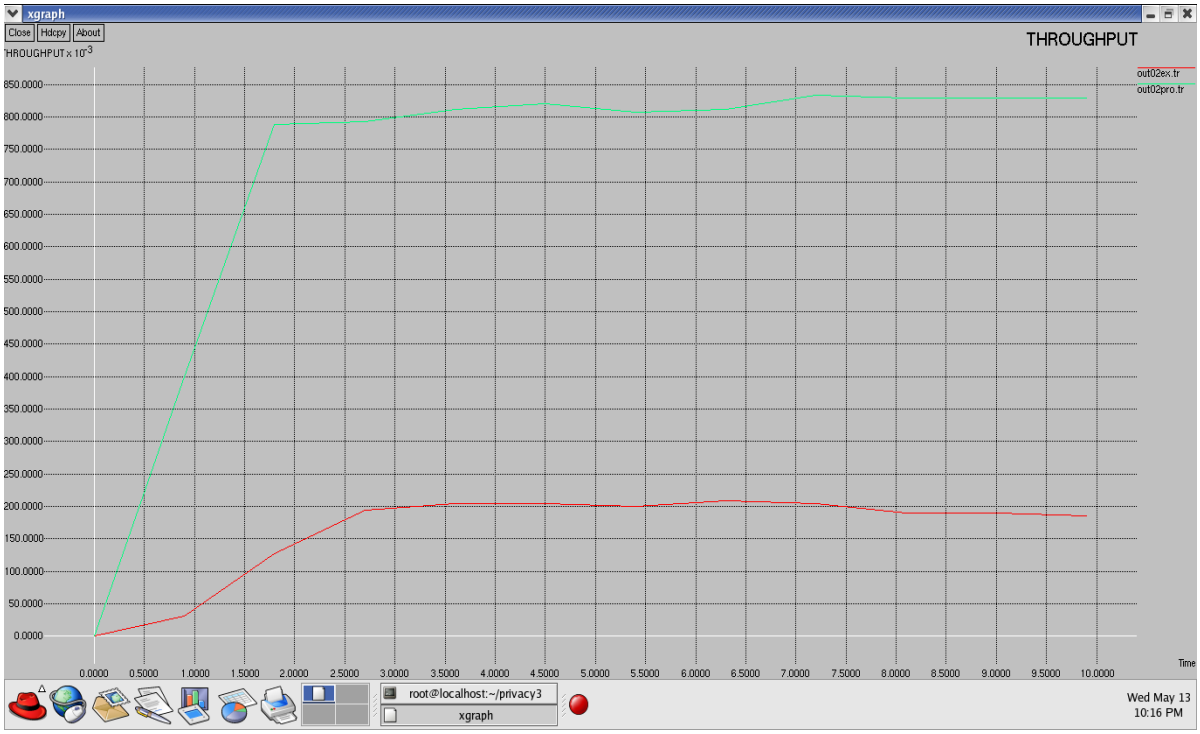


Fig 4.1 PROPOSED SYSTEM

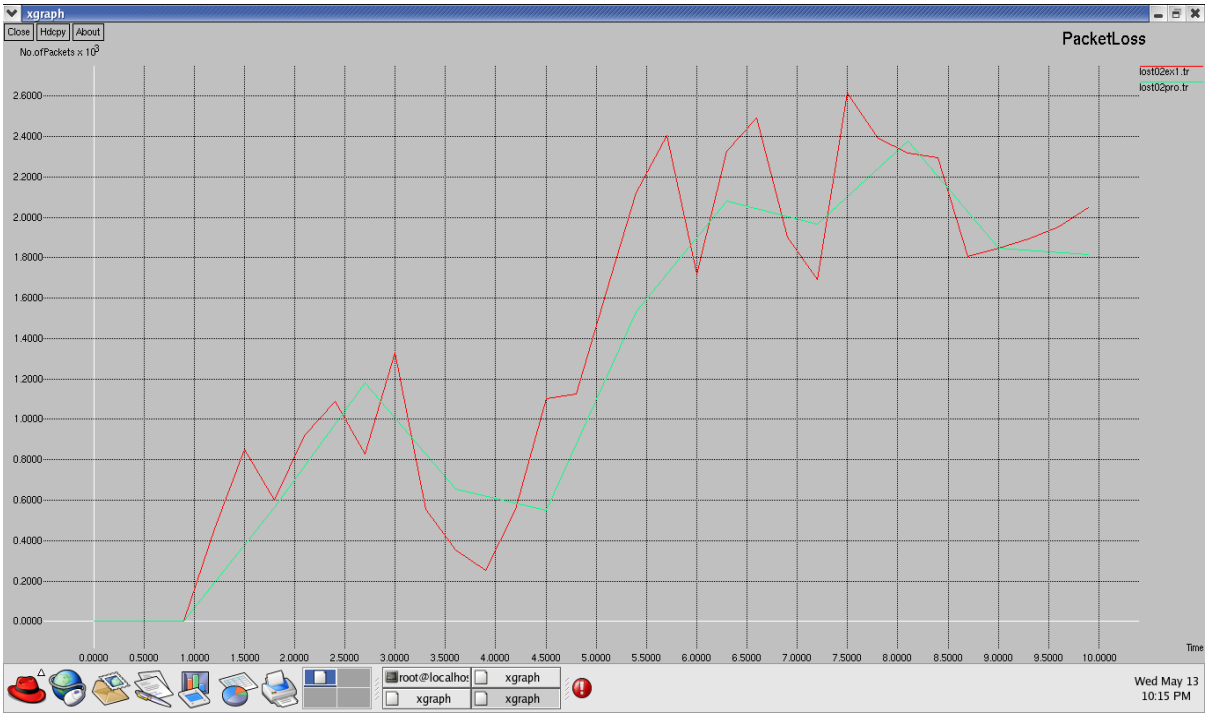
Here above fig 4.1 proposed system architecture there are three phase set up phase, transmission phase and Detection phase. In first set up phase source node indentify neighbor node where the packet is send or choose the route. After neighbor node decided generate the key send packet. So after this detection phase start in detection phase relay node drop the packet next to this step proposed system check energy and choose the best energy node. Finally indentify packet drop and indentify malicious node.



SNAP FOR END TO END



SNAP FOR THROUGHPUT



Here in proposed system we drive to best energy module formula in network simulator

IV IMPLEMENTATION ENVIRONMENT

Figure 4.1 shows the basic architecture of NS2. NS2 provides users with an executable command ns which takes on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation[5].

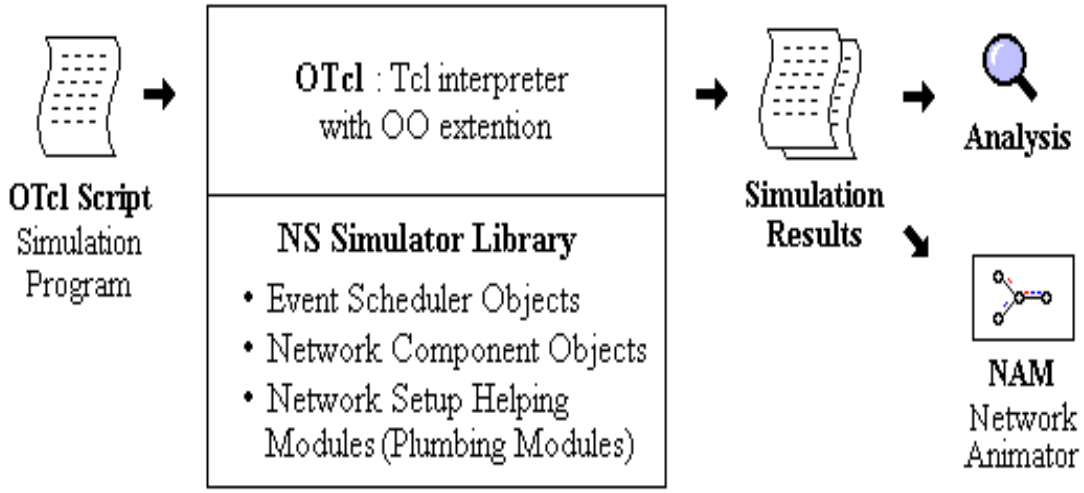


Figure 4.1 c++ and OTCL Duality

NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events

(i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles.

V CONCLUSION AND FUTURE WORK

Packet dropping attack in network is harmful threat in network. Some techniques and measurement has already been introduced to detect the packet drop, but problem still lies here so our proposed mechanism to indentify the energy efficient node. To improve the network performance.

To choose best energy node as well along route is truthful but in future work our system will secure about different type of attack so network will more secure.

REFERENCES

[1] P.seweth, vinod bhupati,unmasking packet drop attack in MANET,International general of emerging trends and Technolgy in computer science,Nov-Dec 2013.
[2] Wei liu,student menber,IEEE,hiroki nishiyan,member,IEEE,Nirwan ansari,fellow,IEEE jieyang and nei kato,senio member IEEE,Cluster based certificate reevocation with vindication capability of mobile ad-hoc networkIEEE,vol-24,Feb-2013.
[3] Haunyu zhao,xin yang and xiaolinLi,c trust: trust management in cyclic mobile ad-hoc network,IEEE,No-6 vol-62,july 2013.
[4] Tao shu, marwan krunz, privancy preserving truthful detection of packet dropping attack in wireless ad-hoc network,IEEE,1536-1233,10.1109/TMC 2014.2330818.2014
[5] Samyak shah and amit khadre, ‘‘Performance evaluation of ad-hoc routing protocol in ns2’’, veermata jijabai institute of technology,mumbai,india,2012.

