LOVELY
PROFESSIONAL
UNIVERSITY

AN ENHANCED APPROACH FOR TRUST BASED ROUTING IN MANET

A Dissertation submitted

By

PEDAMALLU LAKSHMI NARASIMHA MURTY

(11300724)

to

Department of Computer Science

In partial fulfilment of the Requirement for the

Award of the Degree of

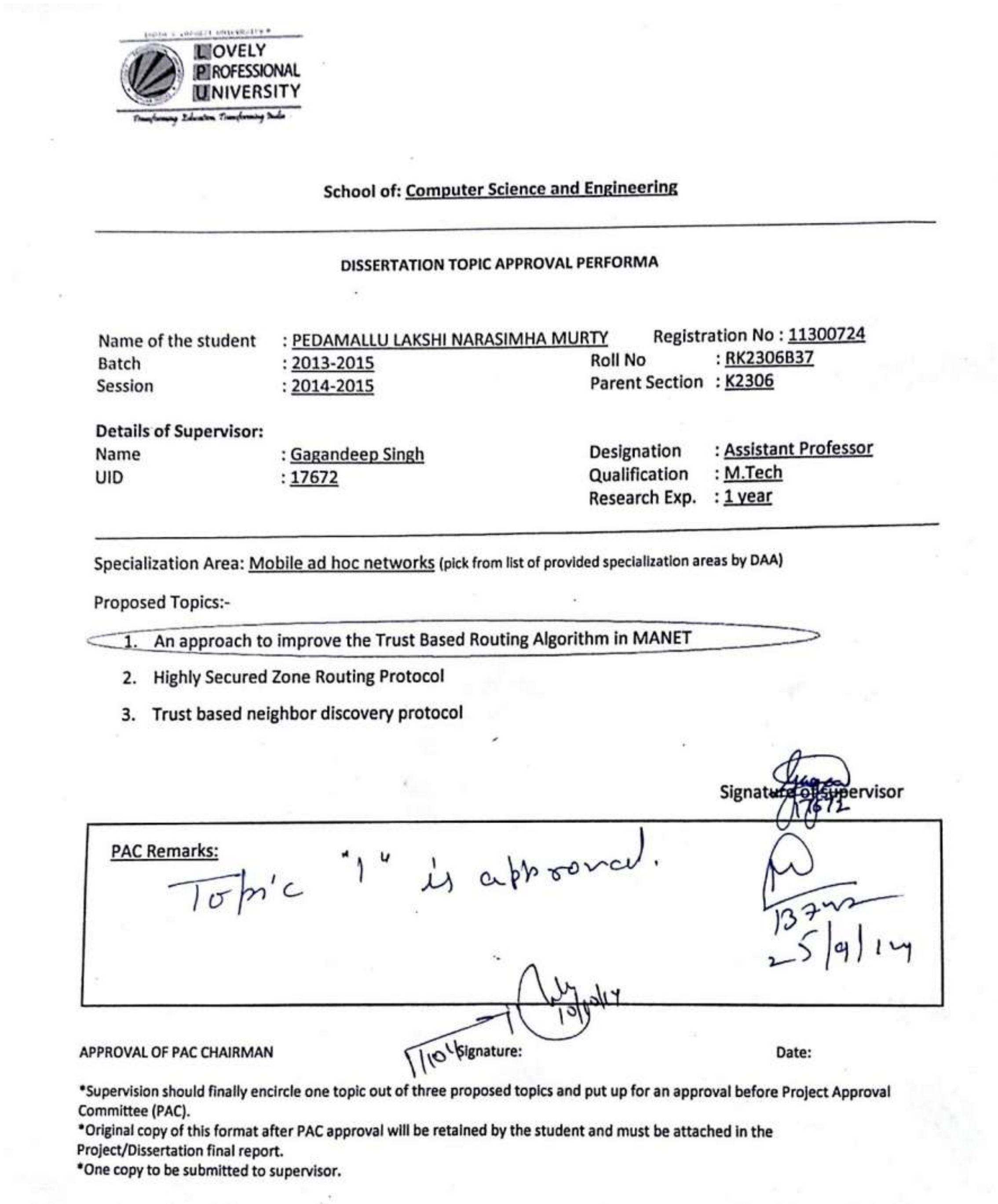
Master of Technology in Computer Science & Engineering

Under the guidance of

Mr. Gagandeep Singh

(APRIL 2015)

PAC APPROVAL FORM



LOVELY PROFESSIONAL UNIVERSITY

School of: Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the student : PEDAMALLU LAKSHI NARASIMHA MURTY Registration No : 11300724
Batch : 2013-2015 Roll No : RK2306B37
Session : 2014-2015 Parent Section : K2306

Details of Supervisor:
Name : Gagandeep Singh Designation : Assistant Professor
UID : 17672 Qualification : M.Tech
Research Exp. : 1 year

Specialization Area: Mobile ad hoc networks (pick from list of provided specialization areas by DAA)

Proposed Topics:-

1. [✓ An approach to improve the Trust Based Routing Algorithm in MANET]
2. Highly Secured Zone Routing Protocol
3. Trust based neighbor discovery protocol

Signature of Supervisor
17672

PAC Remarks:
Topic "1" is approved.

13742
25/9/14

10/10/14

APPROVAL OF PAC CHAIRMAN 1/10/14 Signature: 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

MANETS does not have any fixed topology and the nodes move from one location to another. To transfer a packet from sender to receiver it should follow a routing mechanism and data can be transferred securely such that the route should be trusted and nodes could not be compromised. In this paper we discuss about an enhanced approach for security in trust based routing algorithm by considering AOMDV as ET-AOMDV which is a multipath routing. We implement rail fence technique on the message and further encryption technique is performed and passed over the network to reach to its destination.

CERTIFICATE

This is to certify that Pedamallu Lakshmi Narasimha Murty has Completed M.Tech dissertation titled **“AN ENHANCED APPROACH FOR TRSUT BASED ROUTING IN MANET”** under my guidance and supervision. To the best of my knowledge the present work is the result of his 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 award of M.Tech Computer Science and Engineering.

Date: ________________

Signature of Advisor
Name: ________________
UID: _________________

ACKNOWLEDGEMET

I am very grateful to my dissertation guide **Mr. Gagandeep Singh,** Asst. Prof. in Department of Computer Science & Technology, Lovely Professional University, for his extensive patience and guidance throughout my project work. Without his help i could not have completed my work successfully. I would like to thank **Mr. Dalwinder Singh**, Professor and Head, Department of Computer Science and Engineering, Lovely Professional University, for having provided the freedom to use all the facilities available in the department, especially the library. I would also like to thank my classmates for always being there whenever I needed help or moral support. Finally, I express my immense gratitude with pleasure to the other individuals who have either directly or indirectly contributed to my need at right time for the development and success of this work.

DECLARATION

I hereby declare that the dissertation entitled, **AN ENHANCED APPROACH FOR TRUST BASED ROUTING IN MANET** 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: ______________

Investigator

Regn. No _____________

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Networks

A group of independent systems or persons to share the information and hardware is said to be and network. In a network each and every node is connected by a path where the communication can be done. Networks are broadly classified as wireless network and wired network. In wired network all the devices are connected to each other where we connect a printer , LAN cables etc. to represent wired network there are many topologies such as star,bus,mesh .these networks follow some fixed infrastructure. Wireless networks are quite equal to wired network but the devices are connected without using any wires and cables to decrease the mobility and increase the range. These type of networks does not have any fixed infra structure .the devices can connect to the computer without any wires through signals such adhoc networks, wifi access. Basically networks are divided as Local area network, Control area network, Wireless local area network, Wide area network, Metropolitan area network. This mainly deals with many forms like local, global and also in storage devices.

1.2 Mobile Adhoc Networks

Manets are the acronym for mobile adhoc networks. Manet is the acronym for mobile adhoc network. Mobile adhoc network is basically defined as mobile means moving objects or things and adhoc means temporary usage, so it can be defined as temporary mobile network. The nodes the network move from one place to another location, the nodes could not form any network topology, vary from time to time. To transfer the data between source and destination it follows a routing technique, it does not have any specific routing protocol to follow in the network, and it is difficult to determine which protocol can be implemented. Neither pre-defined network infrastructure nor centralized network administration exists to assist in the communication in MANETs. Nodes communicate with each another via direct shared wireless radio links. Each mobile node has a limited transmission range. Nodes wishing to communicate with other nodes outside their transmission range employ a multi-hop strategy. There are two types of MANETs:

closed and open . In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behaviour is termed selfishness or misbehaviour. One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

Manet consisting of a set of mobile hosts which can communicate with one another and roam around the network. A mobile host may not be communicate with the destination node directly in a single hop network design, in this view it should occur the multi hop scenario, where the packets can be sent through several nodes which acts as the intermediate between source and destination . We can trace the location of the specific node by the task of location aware routing protocols.

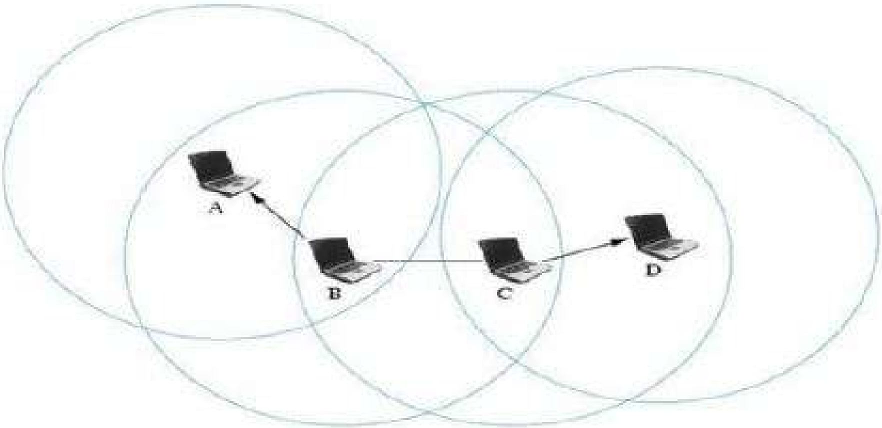


Figure 1.1: A Mobile Adhoc Network

Application of Manet is mainly used battle fields where the source node is constant and remaining the other entire node roams one place to the other within the region. Performance of the adhoc network depends upon the routing protocol being used and battery consumption being used by nodes.

1.2.1 Applications of manet:

a. Military fields

b. Emergency services like fire fighting , disaster recovery, hospital services

c. E-commerce , business

d. Home and office working

e. Education

f. Entertainment

g. Sensor networks

h. Personal Area network

1.2.2 Characteristics of manets :

a. **Distributed operation** – Each and every node act as relay node. To manage the network is equally distributed among the nodes. Each and every node in the network will work together with each other. the nodes use some particular functions such as routing and security

b. **Multihop routing** – when a node want to communicate with the other nodes then it traverse by many intermediate nodes and reach to the destination

c. **Autonomous terminal** – each and every node in the manet are the independent nodes they can uniquely act as a host and router

d. **Dynamic topology** - As the nodes do move from one location to another location there is no fixed topology. The nodes vigorously create routing among the nodes.

e. **Light weight terminals** – Nodes have low power and small storage capacity

To secure the adhoc network we must follow some of the aspects such as authentication, authorization, privacy, availability, data integrity and non repudiation. The attacks of adhoc network are basically divided into two types such as passive and active attacks.

Passive attack - which just reads the message but does not alter any data in the packet. This attack is very low. To decrease the passive attacks we follow some encryption techniques.

Active attack – an attack which the attacker modifies or removes the data from the message packet is said to be active packet. This type of attack is very harmful. This attack may change the operation of the network to be performed. The active attack again broadly classified into internal and external attack. Some of the advantages of MANET are

- Network can form at any time and place
- Nodes act as host and routers where the nodes are independent from each other no central organization
- These provide access to data and services apart from the location services
- More scalable

1.2.3 Routing Protocols in Manet:

Routing protocols helps us in defining the set of rules to transfer a packet from source to destination in the form of packets. In MANETs the routing protocols are broadly classified into 3 types

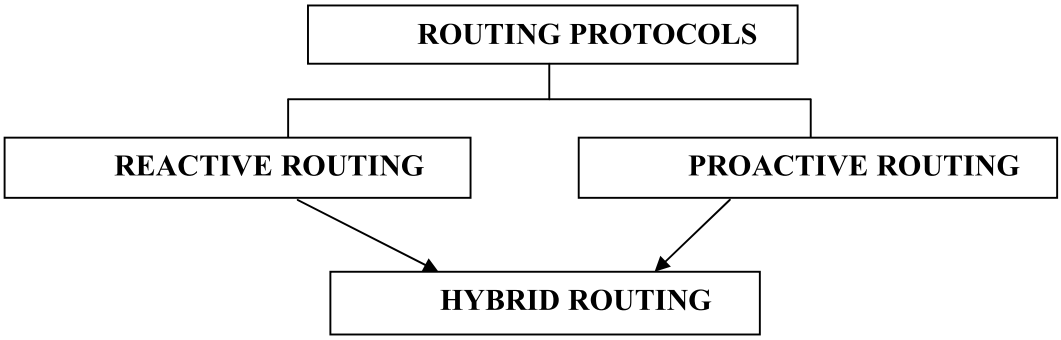


Figure 1.2: Overview of Routing Protocols

Reactive routing: in this routing protocol it creates s a new route whenever it is needed on the transfer of packet basis. The source node checks whether the route is available in the database to transfer the packet, if no route is available then it creates a new route. It is also defined as on demand routing protocol .examples such as AODV, DSR, and TORA Each and every routing protocol should follow the following characteristics:

route discovery: The main process of this component is when the source want to communicate to destination by sending packet, it will check the route that is available in the virtual memory, if the route is not present then it defines a new route in which the packet is to be travelled in which the packet contains the source id, destination address and intermediate nodes address to forward.

Packet relay: This mainly describes how the packet is to be transferred .this process can be mainly done by source routing and next hop routing. In source routing the message contains all the information regarding the packet transmission including the intermediate nodes, where as in next hop routing the message only contains the destination address where each and every intermediate node should follow a route table to forward the packet.

Route maintenance: The nodes in the network maintain different topologies so we cannot maintain specific route which contain error paths in the networks the main theme of the reactive protocol is it have acknowledgement service for each and every packet delivery to which route maintenance can be implemented.

proactive routing: In this routing protocol, each and every node maintains a route table for the possible nodes even it is not used to transfer the packet .if the topology of the network changes then the routing information will also be updated and this protocol cannot be used for larger networks and it is also called as table driven routing protocols. Examples such as DSDV, OLSR, WRP.

Hybrid routing: The combination of proactive and reactive routing is defined as hybrid routing. This protocol overcomes the all the disadvantages of both routings and follow in it, it uses the route discovery process of reactive routing and storing the information as proactive routing and implement in hybrid routing. Examples such as ZRP, SHRP etc.

CHAPTER 2
REVIEW OF LITERATURE

M Peralman , 2000 - This routing provides failure of the route and balancing of load among the nodes by distributing the traffic among a set of varied paths which can be make this alternate path routing scheme . In this routing is not fully recognized and realized because of route coupling where coupling mainly occurs due to where the paths share common intermediate nodes where it is a major issue in single channel networks and also coupling also occurs when one path covers another path area, where this protocol provides in negligible analysis mainly in quality of service.

Lee SJ , 2001 - Many of the on demand routing protocols build and rely on a single route and data session, when there is a link disconnection on the present route then there must be a route recovery process, basically multipath routing is popularly used in QOS routing technique in wired networks. Many of the multipath routing is developed by using link state and distance vector algorithms. Here author proposed a multipath routing which is defined to be split multipath routing which uses many routes of disjoint paths. by using many paths there helps in decrease in route recovery and message overhead where this protocol uses packet assign to transfer the packets over different multiple pats of the paths which are active and maintains the nodes from congestion and traffic situations.

T Sirigos , 2001 - As the node moves from one location to another location there will be change in topology from one position to another position. Here the author mainly describes how the multipath routing is performed when there is a change in topology in the network. The basic idea is that the time for packet transmission and the mean time of change in topology. Data packets are sent from source to destination using the code diversity mechanism. The main assumption is that topology never changes when the packet is being sent from source to destination.

Wenjing Lou , 2002 This paper mainly deals to gain the data confidentiality service in the Manets. Here the author proposed a security protocol which is named to be SPREAD (Security protocol for reliable data delivery). The main aim of this protocol is that to provide protection to secret messages from the compromised nodes and while reach to their destination in an insecure path or network.

Basically , the message is divided into multiple shares to transform by applying some schemes and deliver the packet by using different independent paths which reach to the destination where only some part only be compromised or leaked remaining part or message cannot be compromised .he mainly discussed about following issues are

a. Threshold secret sharing
b. Share allocation
c. Multipath routing and path set optimization

While discussing about the major issue which is an multi path routing how the message is shared between different nodes and passed through different independent paths as the topology changes as there is moving of nodes from one location to another very periodically . In this protocol he describes about independent paths and node disjoint paths as this protocol deals with node compromising problem.

Here in this protocol we mainly discuss about the link cache organization where each and every path that connects to the destination from source is defined into single links which will used setting the path to optimize the path. The path can be set based upon the topology and the optimization can be done by cost of the link according to the security level, where the security level can be defined as where the chance of path that number of nodes compromised to get the data. In DSR each node transmitting the packet is responsible that the packet has received to the neighbour node which can be done by link layer acknowledgement. When the packet is noticed by route cache then if there is any failure of route can only detect when there is a chance to transmit the packet. A link cache is referred to be a data structure in which each link referred to be an cached data unit which represent the present view of network topology.

Prayag Narula, 2007 – This paper mainly deals with soft encryption and routed over the network by using the DSR routing by following some trust management aspects. This mainly deals to get data of very less content to the malicious node where the data is divided into some parts called shares.

a. **Trust**: The trust value of a node is defined in the form of levels as -1 to 4. The node which has the trust value -1 that node will discard the packet which is said to be complete distrust. The node which having trust value as 4 it is defined to be complete trust. The trust value of node can also depend upon the number of packets that are traversed through that node.

b. **Trust level assignment:** Trust values are assigned to the nodes by using the direct interaction from the neighboring nodes and trust recommendation from peers. An ack is received from a neighbor that the packet is received, and then it denotes there is no malicious node in the path and assigns the trust value.

c. **Message encryption**: n-bits of data is divided into 4 parts named as a,b,c,d .

Encryption is performed as

A = a XOR c B = b XOR d

C= c XOR b D= d XOR a XOR b

These parts are routed using DSR routing algorithm. Routing paths are selected based on trust defined strategy.

d. **Trust defined strategy:** it is defined to be a node that has assigned some trust values. If a packet is sent over the nodes.

i. If node trust is 4 , it have full rights to read the message and decrypt it

ii. If a node have trust 3 then there is a chance of brute force attack b y a 2^n possible outcomes , where n denotes number of bits used in encryption in that part

iii. If a node have trust value 2 then it may have possible findings of 2^n * 2^n

iv. If it have trust value 1 then it have chance of 2^n *2^n *2^n

v. If it have trust value zero then it act as sink

vi. If it has trust value -1 then it completely drops the packet

e. **Decryption :**

a = B XOR D b = A XOR B XOR C XOR D

c = A XOR B XOR D d = A XOR C XOR D

f. **Routing:** DSR routing algorithm is implemented where RREQ is used to discover a route. When a packet reaches the destination then it resends the RREP packet back to the source node.

Cheolgi Kim, 2011 – In this paper he proposed a new protocol called grid protocol. The total deployment area is divide into small squares or cells which is said to be a grid. Each grid is occupying the size of the square and its area can be represented as s x s, where s is the side of the square .

Depending upon the number of intermediate nodes the delivery of packet may take large time. Now we classify a new a routing protocol called GRID protocol which is a fully location aware protocol where it defines the location of the node. This GRID protocol is a reactive protocol where it creates a route whenever it needs a route to transmit.

a. **Route maintenance***:* The main aspect is that to increase lifetime of route upon its mobility ,excluding source and destination each and every intermediate node have a leader which is also called as gateway which will be followed by following issues
    i. How to maintain the leader of each grid
    ii. How to maintain a route when its source and destination nodes roam around for electing a leader in each and every node election procedure should be followed. It can be done by good election protocol.
    iii. When a leader is elected the host which is nearer to physical centre of grid will be elected.
    iv. To eliminate the ping pong effect, when a leader is elected to grid, it cannot be changed until it roams.

b. **Grid construction:** The grids can be constructed according to the deployment region which is also called as cells. Each node is determined with some necessary information. Transmission of packets can be done at a time period t where the packet contains the node identifier, co-ordinates and sequence number of packet.

c. **Multi grid routing**: When a sender wants to send a packet to destination then the protocol attempts to discover a path in the small grid Neighbour node helps in selecting the source and helped in delivering the packet to destination. By delivering HELLO packets the neighbour will maintain a route table. If the larger grid is empty and source refresh the data and again run the algorithm that we have used that is dijkstras algorithm to compute the values and proposal of finding the new path or route.

Isaac Woungang, 2011 – In this paper mainly deals with multipath routing with software encryption to transfer the messages very securely over the network. This approach mainly contains three phases. They are

a. **Encryption**: The message is divided into some segments and those segments are done by XOR operation to the cipher text that is the encrypted text.

X = a XOR c   Y = b XOR c   z = a XOR b XOR c

b. **Decryption** : After the packet is received with the cipher text to the destination , to get the original text we decrypt the cipher text to get the original text and can be calculated as

a= Y XOR Z   b= X XOR Z   c = X XOR Y XOR Z

c. **Message Routing**: Where the message can be passed through various nodes and delivered to the destination by using various trust models such as

Trust Mechanism: The trust value of a node can be depending upon the delivering of packets. The node delivers more packets then trust value will increase, if it has more chances of failure of packets then trust value will decrease. If trust value is less then malicious nodes can be easily detected .the node trust value can be calculated as T = W1 * DT + W2 * TR. Where W1, W2 are weights and DT is the direct trust value, TR is the trust recommendation value. Success value is calculated as S and failure value is calculated as F, C is constant.

DT = DT + C S (for success nodes)
DT = DT – CF (for failure nodes)

When the node is transferred successfully then S is incremented by 1 or reset to zero. When the transfer fails then F will be incremented by 1. The values can be computed by monitoring of AOMDV packet forward process .HELLO packets are used to determine trust value such that when a message is received then it checks in table and find the nodes. If any node exists then it will receive a message.

Secure routing: When a source sends a request packet to the following node to deliver at the destination, it checks the hop count for the source node and sends a reverse path where the hop count will be recorded. After the packet is received to the destination then it sends reply packet through the nodes, if it sends a route error message then the path will be discarded. When the node will send the data RREQ packet to find destination it again sends reply packet and it compares the trust value of the node and reserved trust value. If the node trust is less than the reserved trust then it will be replaced by neighbour trust and further packet if forwarded. After the source receives all the trust values and reply packets then routing will be performed. If a path is chooses and not suitable to transfer data then the process will start again by considering other path.

Isaac Woungang, 2012 –This paper is that mainly explains that how to implement an enhanced trust based multipath dynamic source routing [ETB – MDSR]. Mainly consists of soft encryption, novel trust management strategy and multipath DSR routing. The main and basic view of the Manet is that the information exchange and delivery of packets can be performed without any pre existing infrastructure of the fixed network that gives a certain level of cooperation which occurs among the nodes before the routing occurs. Some of the solutions had been done for the secure transmission of packet . Multi path secured routing where the data will be splits into some parts before transferring and encryption is performed and routed in the available paths.

In TFT a bad node decreases it service and lower the performance that in which it did not involve in transferring the packet, main disadvantage in this is boot strapping. In cryptography implement security in Manets but the key mechanism which we cannot think it as guarantee. Process of passing the data

i. **Step 1**: Message is split into parts and transfer from source to destination by using some trust paths where we implement the greedy approach

ii. **Step 2**: trust strategy of the nodes

The more encrypted parts cannot be transfer through that node depend upon the assigned trust value.non trusted routes can be avoided which can be done by the brute force attacks.

In ETB-MDSR, the routing will be performed based upon the management model where the remaining process is continued as the TB-MDSR. History of interactions stores the data of process between the nodes. The HI value can be updated by using the HI module. TC (trust computation) selects the data value and checks to perform which type of computation. This can be mainly decided by the level of confidence, where the satisfying and unsatisfying interactions are calculated. If the confidence value is high then it compared by using the threshold value by performing the direct computation. If the confidence is low then indirect computation is performed. TC module uses the filtering method to get the honest recommendations and weighting method. TC can be calculated as the sum of violation for the path selecting routing. Trust values can be converted in the range of (x,y). The trust compromise of TBMDSR is always zero. If the malicious node increases then this protocol take less time to find the path. When the velocity increases then route selection time decreases.

Thanigaivel G , 2012 -This protocol ensures the trust among the nodes in the network and isolates malicious nodes in the network by using the non – cooperative movement. The main aim is to detect the malicious nodes and selfish nodes in the network. If any malicious node is seen y the neighbouring nodes then it will moved to quarantine by other nodes in particular network. This infected node will mainly occur due to low performance, high traffic or malicious node.

TRUNCMAN is mainly divided into two phases such as

a. **Suspicion phase:** In this protocol the neighbouring list is directly added to routing table. When a message is sent to the neighbouring nodes then it checks for the ACK whether it is malicious node and non cooperative node. Rep check will be set to 1. When there is no reply back then the node assume that it is a malicious node or with low performance or node with high traffic.

b. **Detection phase:** When the node got a message from source, if it is not a malicious node then it sends the ack-rep packet to the source. In this phase NR & BC will be set to 0. When it is lo performance mode then the BC will be set 1 such that it is broadcasted. When it is in the high traffic mode then NR will be set to 1 and send to the originator. Rep – check will be performed for both the actions. Whenever a node receives any ack it checks whether it is in list and in range , if it is not available then it detects an attacker in between the source and destination and discards the route and changing the non – cooperative reputation.

Naveen Kumar Gupta, 2013 – In this paper mainly describes about the concept of trust value and honest value by means of hop and protect from the malicious node. HAODV (honest adhoc on demand distance vector routing) where the honest value will be first set to value by based upon hop and trust value.

a. **CAODV (credit based):** Deals with the black hole attack. It will initialize a value to the next node in the route discovery process, when it is moved to the next hop then credit value will be decremented by 1 and after receiving to destination then it will send the ACK (acknowledgement) packet. The intermediate nodes receives credit ACK and moves to next hop if it is a trusted hop , if it does not receive then credit value will be set to zero.

b. **FRAODV (Friendship mechanism):** In this each node keeps a list of friends and its values, the more number of friends and values the more it trusts the node. IP and MAC address are used to check the friends.

c. **SAODV (secure):** here to implement the process we use the hash chains and digital signatures, where the hash chains are used to secure the hop count and digital signature is used for authentication. It prevents the black hole attack and signatures.

d. **TAODV (trust):** depending upon the trust value the routing can be performed .the three models that are used in this process are recommendation, combination and judging. It prevents external attacks and DOS attacks using signatures. Algorithm can be described as node creation and honest value initialization, path evaluation. By hop Current value = nodes count (S to D) * nodes count from (S to current node). By trust current trust value = Constant * nodes count.

Path can be evaluated as same as AODV routing protocol we use RREQ and RREP. If the present path has more honest values then the path will be continued until it reaches to the destination.

Chuanhao Qu, 2013 - This describes about the reducing of control overhead such as path error instead of route error. Here it is considering the multi hop routing where multiple paths can be considered to transfer the data in the region. When a data is sent from source there exists two paths and if the node F crashes then link fails and keeps the track and send through other , if it send through back to the node then source might think that the routes were crashed , so it will be in search of other routes. Each and every node in the system has an intrusion detection system to maintain the trust values and detect the malicious nodes. Trust of node is given as sum of weights of forwarding packets.

Trust model: There will be n mobile nodes in the network where the nodes may join, leave or crash in the network. The infected nodes may drop at any time in the network. The communication between the nodes is bidirectional. The mobility is defined as the node which has the maximum speed in the network. Trust value can be computed as direct trust value, indirect trust value and comprehensive node trust.

Direct trust $(T_d) = k_1 * T_h + k_2 * T_c$

k1 and k2 are constants

T_h is the history trust value = sum of forwarded to the target node / sum of packet forwarded from the node.

T_c is the current trust value = forwarded latest record to target node / forwarded target node.

Indirect Trust value (ID) = total trust of node to the target node / neighbor evolution.

We cannot identify the infected nodes only by using direct trust value computation. We calculate each node value of a node and send to the neighbors. If the results are less than the 20% then we can say that it is a malicious node.

Comprehensive node trust can be defined as the evaluation system will collect the packets and helps in selecting the best path. The initial value of every node is set to 100 % after every node passing the trust value will be updated by comparing with the threshold value. In the path selection mechanism it will verify that the trust value of next hop is greater than threshold value.

If it does not satisfy that condition then it is considered as a malicious node than path error occurs. In the form of reply packet the forward and reverse path values are noted to reply the packet, if the intermediate node founds a fresh path no reply packet to be send to the source. Route can be followed by the nodes by comparing with the trust values of that node and path trust value is calculated to detect the malicious nodes and discard it.

Dilli Ravilla , 2013 -The data is transferred securely by using zone routing protocol by using some security measures such as key management, discovery of neighbours, detecting malicious nodes and prevents the non- cooperative nodes. This routing protocol has following phases as

a. **Key generation:** It includes a pair of public and private key for generating a digital signature where node stores its private key and sends public key to its neighbours for access. Various attacks may occur by the use of pre-issued keys and certificates.
b. **Key management:** For overcoming the attacks by the pre-issued of data of keys and certificates. We use this system where we use some measure of security by keeping a unique identifier by using the public key which of 64 bit. The UI is linked with IP address where the intruder cannot get the value or by creating a new pair of keys.

$\mathbf{N_1 \xrightarrow{(MSG\ 1)} n_1 \xrightarrow{(MSG\ 2)} Z_1}$**(verifies msg1 & msg 2)**

and finalize data address and public key.

c. **Secure neighbour discovery protocol (SNDP):** Here we use HELLO packets to communicate or to find a neighbour of a node and after for authentication of message and at which it was sent, after verifying, if it satisfies the range of the threshold value then it accepts as a neighbour. here it follows steps :
   i. **Step 1:** Message contain authenticated time and location of the node
   ii. **Step 2:** After the packet has received, it computes the time and location and verifies with the original address, if the both values are equal then checks the digital signature and accepts the node as a neighbour.

d. **Secure intra zone routing protocol (SIARP):** Digital signature is used for packet authentication by using the RSA technique, signature is stored in every packet and then transmission is performed, where signature will help in authenticity and integrity of a sender and packet. Zone radius is considered and set to -1 where the sender has high trust and receiver calculates.

e. **Secure inter zone routing protocol (SIERP):** Here we use hash function as message digest to provide integrity in the network, where the packet is included with message digest and digital signature before transmission. The source computes digest and signature and forward to nodes. If the node already receives the packet then it discards or drops. Once the nodes accept by checking the signature and digest_with maximum trust value and can be computed. Once the process is done it can be computed as H[A , digest] and when it receives to the destination it verifies the signature and digest by using the key pair by the H[1],H[2]……….H[n]. Each and every node in the network has the pair of (public key, private key) and has the public key of remaining nodes.

f. **Broadcast resolution protocol (BRP):** The data is securely broadcasted to the particular nodes by taking the security measures and performed operations.

g. **Detection of malicious nodes:** If the node trust value of a particularly node is gradually decreased and assigned to 0 then it is detected as malicious node and moved to malicious table, alarm packet is generated with the address of malicious packet with its signature included .

CHAPTER 3
PRESENT WORK

3.1 Scope of study

i. By concerning the security of delivering the packet in the adhoc environment.

ii. In the base paper which I have used, there the author used only XOR operation which is less secure, then the node can be easily compromised.

iii. When the packet transfers through the malicious node the packet can be dropped or it can be compromised easily because it has less secure mechanism.

iv. Security is improved then we can protect the data more securely then the data cannot be compromised and there will be chance of decreasing the malicious nodes

v. Stream cipher is used when we process the data to convert into cipher text by using rail fence encryption algorithm.

3.2 Objectives of the study

i. The main objective of this paper is to provide secure data transfer by encryption and decryption using rail fence algorithm and route to the destination.

ii. While the packet being routed from source to destination our objective is to identify the malicious nodes and nodes trust value by delivery of the packets from that node.

iii. The input data is divided into equal bit chares to perform the XNOR operation by combining two of the shares.

iv. The output of the XNOR operation is an encrypted text which can be routed from source to destination securely by using AOMDV multipath routing.

v. When the packet is routed to destination successfully it decrypts the data and applies the derail fence technique to get the original text.

Terminology

AOMDV:

AOMDV deals with multiple loops free and link disjoint path technique. The main era is to get the path disjointness. For discovering a route request packets are sent over the network by several intermediate nodes which form multiple paths to the destination. As the nodes cannot opt for a fixed location, the change in node position may lead to change in path. An advertised hop count is maintained to get about the hop count in the path. If the hop count is less than the advertised hop count then the path is to be changed and another path is considered. if there is a change in location of node then that entry is updated in the routing table , where it can be changed for every time period .

NS2:

NS2 is an acronym for network simulator which is simulation script said to be Tcl simulation script. It uses Tcl as a scripting language. It provides support to TCP, UDP and HTTP protocols. NS2 consists of two languages said to be C++ and OTCL. C++ defines internal mechanisms. OTCL is an object oriented tool command language. It is a setup simulation by configuring the object. C++ and OTCL are linked using TCLCL. After the tcl file is executed we get a nam file which is network animator provide the trace of nodes and mobility of nodes. A graph is generated basis on the script files with link up to the generated trace file. Trace file is used to capture the particular environment. If a new algorithm is to be implemented we should include path in the make file so that it will help in creating object files for new algorithm by giving “make” command . This object files are used to link up with tcl file to process.

Rail Fence:

It is a transposition cipher where the message is divided into number of rails that can generate cipher text also called zig- zag cipher.

XNOR operation is a logical gate where it takes the input of the variables and process based upon the input we will get the output from the obtained cipher text. It will be in the binary form.

3.3 Research Methodology

We propose a new scheme such that it mainly contains four phases such that defines are

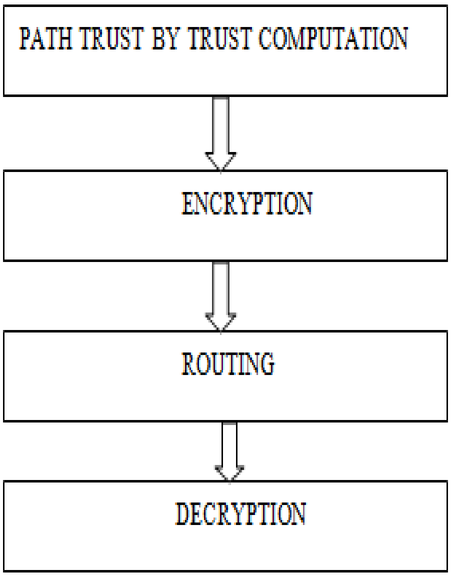


Figure 3.1: ET-AOMDV Process

a. Rail fence :

It is also called to be a zig – zag cipher. It is one of the forms of transposition cipher .In this cipher we write the plain text in the form of rails as downwards and up wards until the total message is completed. Now the message is read in the form of rows or rails and we get the cipher text .this cipher is not so secure because the intruder can try the number of rails and he can find the message. Suppose we consider a plain text “LOVELY PROFESSIONAL UNIVERSITY “and number of rails are to be 3 and the cipher can be as

L . . . L . . . O . . . S . . . A . . . I . . . S . . .

. O . E . Y . R . F . S . I . N . L . N . V . R . I . Y

. . V . . . P . . . E . . . O . . . U . . . E . . . T .

Now the cipher text is written as
LLOSSAISOEYRFSINLNVRIYVPEOUET

b. XNOR gate :

It is digital logic gate which is quite inverse of the XOR gate (exclusive OR). If the two inputs are equal then it gives an output as 1. If the two input are different then it gives an output of 0. If A and B are two inputs then XNOR of A and B is written as A Θ B
Representation of XNOR gate

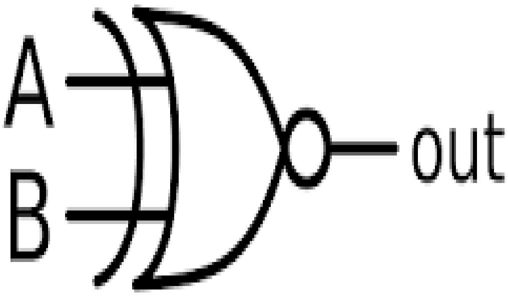


Figure 3.2: XNOR Gate

Truth table of XNOR gate

A	B	A XNOR B
0	0	1
0	1	0
1	0	0
1	1	1

PROPOSED ALGORITHM

a. Path trust by path computation

To deliver a message from source to destination or a from node to node we should follow a path by implementing a routing scheme. The path can be defined by giving its trusted value by getting up the path cost such that the nodes that are involved in that path. Path cost can be calculated and it can be define to be path trust. The trust value can be various levels and values are assigned to it as 4 to -1 where it can be defined to be that the trust with value 4 has complete trust with high recommendation and the value with -1 is that distrust value such that it drops the packet .The path with low trust can be defined to be it have a no trust means that the packet which are transferred through this path can be affected and gets compromised. We can define the range of trust values into group of classes such that the nodes with this trust belongs to this class range and level where each and every path must have some minimum trust value to select the path.

b. Encryption

Initially the message which we want to transfer over the network is taken and a cryptographic technique rail fence technique is used and after applying the rail fence the encrypted content is embedded into single content and further the content is divided into some parts known as shadows or shares as we propose them to define into three equal shares if any extra character beyond the length then we consider the null character to be placed in the text and we perform a encryption process as follows

$$\mathbf{a^1 = a \,\Theta\, c} \qquad \mathbf{b^1 = b \,\Theta\, c} \qquad \mathbf{c^1 = a \,\Theta\, b \,\Theta\, c}$$

c. Decryption

When the message is received at the receiver end then the receiver must perform a decryption process by decrypting them. After the message is decrypted we perform a derail fence technique which is quite vice versa to the rail fence technique and then the message is amended according to the sequence number of the shares and the decryption can be done as follows

$$\mathbf{a = b^l \,\Theta\, c^l} \qquad \mathbf{b = a^l \,\Theta\, c^l} \qquad \mathbf{c = a^l \,\Theta\, b^l \,\Theta\, c^l}$$

d. **Message routing or secure routing**

Here we perform the routing by considering the two aspects such as the trust mechanism and secure routing as follows.

Trust Mechanism: The trust value of a node can be depended upon the delivering of packets. The node which delivers more packets then its trust value will increase, if a node has more chances of failure of packets then trust value will decrease. If trust value is less than the threshold trust value then malicious nodes can be easily detected and message can be compromised .The trust value of a node can be calculated as T = W1 * DT + W2 * TR. Where W1, W2 are weights assigned to the nodes and DT is the direct trust value, TR is the trust recommendation value. Success value is calculated as S and failure value is calculated as F, C is constant.

DT = DT + (C* S) (for success nodes)

DT = DT – (C*F) (for failure nodes)

When the node is transferred successfully then S is incremented by 1 or reset to zero. When the transfer fails then F will be incremented by 1. The values can be computed by monitoring of AOMDV packet forward process. HELLO packets are used to determine trust value such that when a message is received then it checks in table and find the nodes. If any node exists then it will receive a message. The trust of the path is calculated as the

$$T_{AC} = 0.1 * T_{A \text{->} X} * T_{X \text{->} C}$$

If node A wants to transfer the packet to the destination node C then it should follow the route through node X which is an intermediate node for node A and C. Path trust is calculated as, if the trust value for the path A to X is 9 and trust value for the path from the path X to C is 6 then the trust recommendation value for the path A -> C is 0.1 * 9 * 6 =5.4 .The trust values of the routes are calculated based upon the trust table.

Secure routing: When a source sends a request packet to the following node to deliver at the destination, it checks the hop count from the source node and sends a reverse path where the hop count will be recorded. After the packet is received to the destination then it sends reply packet through the nodes, if it sends a route error message then the path will be discarded. When the node will send the data RREQ packet to find destination it again sends reply packet and it compares the trust value of the node and reserved trust value. If the node trust is less than the reserved trust then it will be replaced by neighbour trust and further packet if forwarded. After the source receives all the trust values and reply packets then routing will be performed. If a path is selected but it was not suitable to transfer data then the process will start again by considering other path.

CHAPTER 4

RESULTS AND DISCUSSION

Experimental Work

Parameters	**Setting**
Traffic type	**CBR**
Connection	**UDP**
X-axis	**1024**
Y-axis	**520**
Number of nodes	**17**
Routing protocol	**AOMDV**
Simulation area	**1200 X 600**
Trace file	**AOMDV.tr**
Nam file	**AOMDV.nam**
Transmission radius	**150**
Transmission rate	**600 kb**
Data packet size	**512 kb**

Simulation time	**100sec**
Interval	**0.05 sec**
MAC protocol	**802.11**

We have used ns-2.35 as simulation tool. We compared our proposed message security scheme [ET-AOMDV] against T-AOMDV. We have implemented our security scheme on AOMDV routing protocol. Simulation is done on the algorithm and a trace file is generated. By using trace file with combining awk script we can generate a graph said to be Xgraph , where we can show the difference between the two protocols .

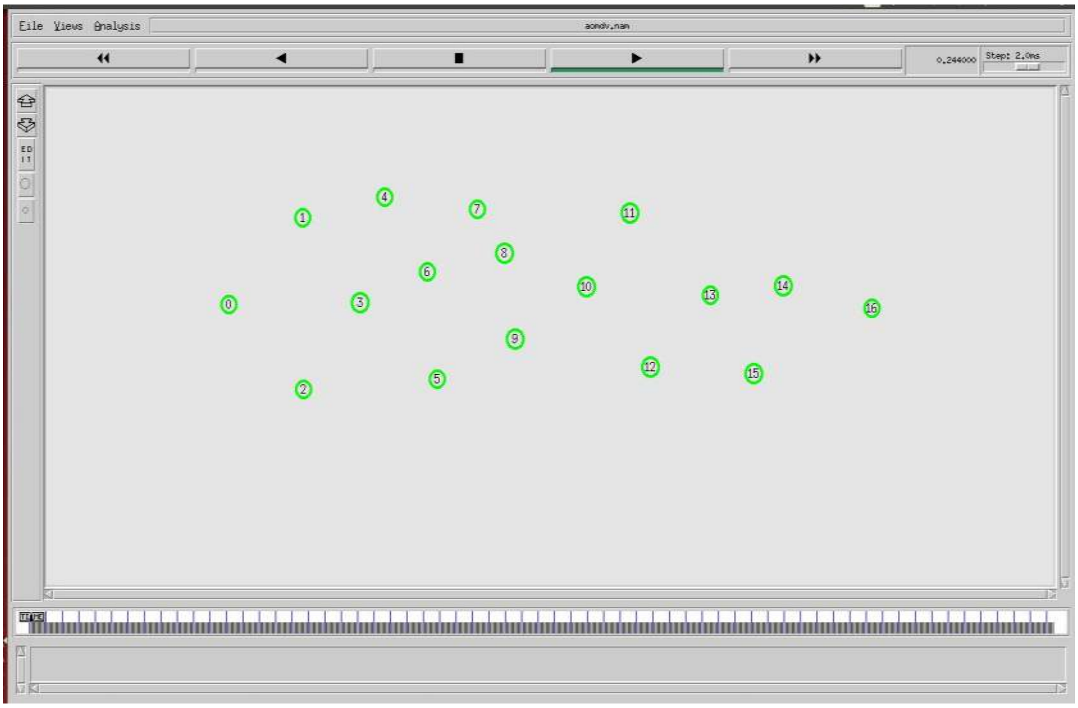


Figure 4.1: Simulation area

A trace file is generated by the algorithm to represent how the algorithm works by our routing protocol. Node movements are observed to secure the nodes from the intruders. By the below figure we can observe the node location and packet transferring from node to node by initial request of RREQ by the nodes**.** Route request will be processed up to the transmission range. The nodes which are in the region will get the request and if it is acceptable then it forwards to the next nodes within its range to find the route to the destination. Upon finding the route, the destination node will sends the route reply packet by its traversed path. All this nodes information will be stored in the routing table.

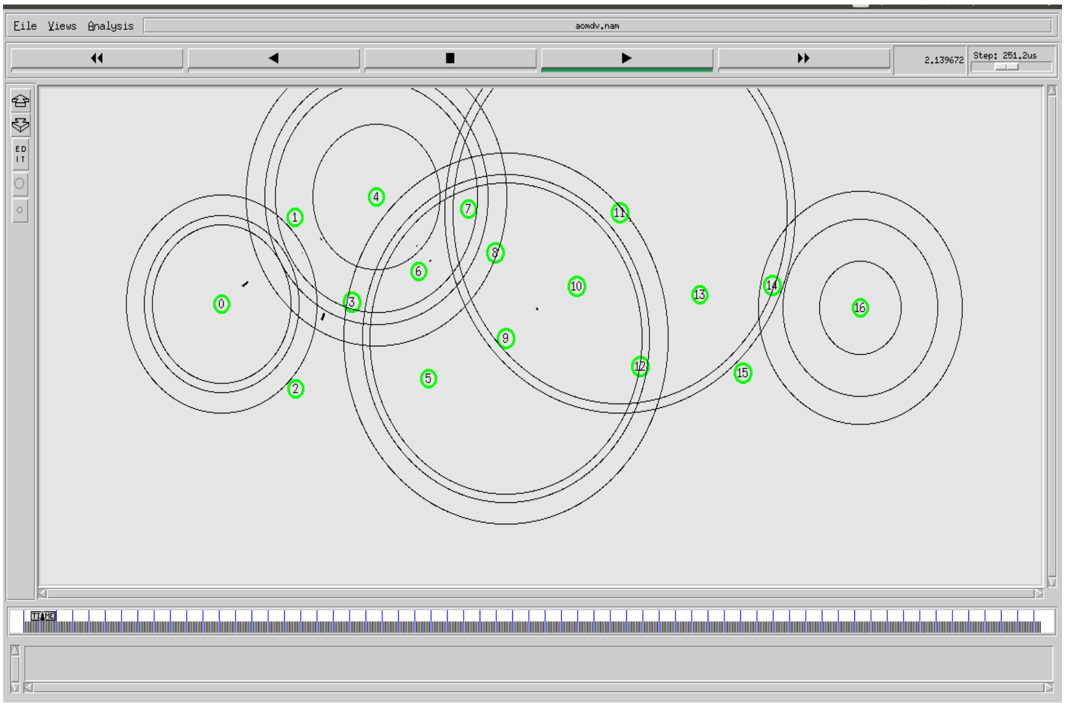


Figure 4.2: Packet Transformation by Request

As the nodes send the route request to the neighbouring nodes then the nodes which have the criteria will accept the request and sends the reply. The node which accepts the request will check whether it has route to the destination and stores in the routing table. When there is change in the path the data will be updated in the routing table for particular time period.

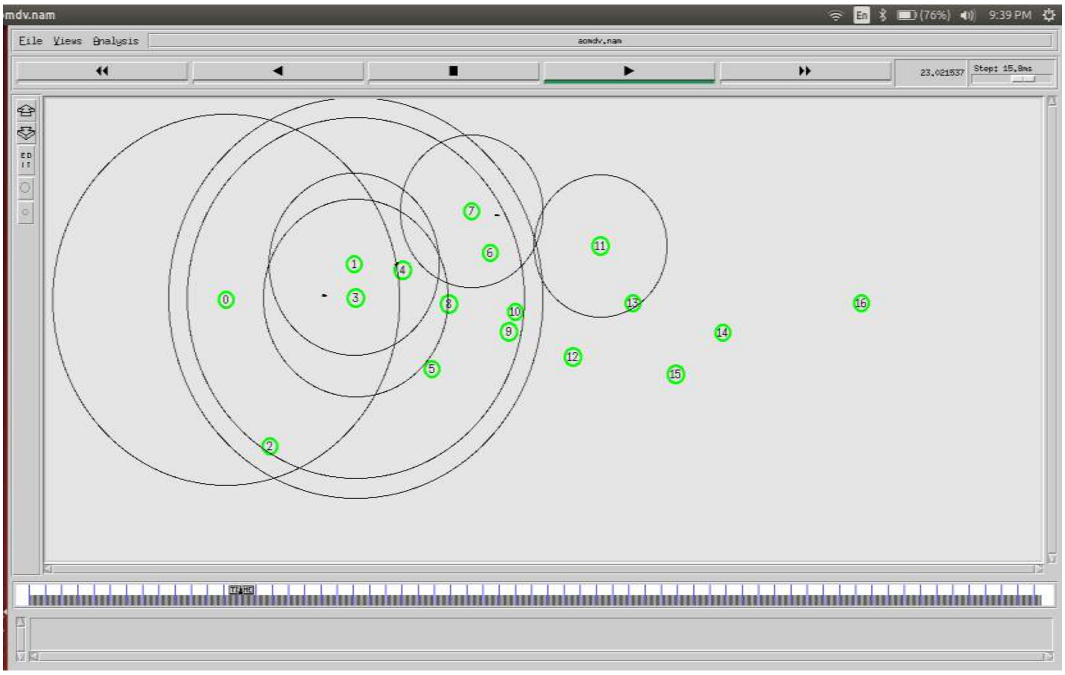


Figure 4.3: Route Request By Nodes

Data analysis and Interpretation:

Throughput:

As the time and number of nodes increases throughput also increases. Throughput is defined as number of packets delivered to the destination in a span of time. By comparing with T-AOMDV, ET-AOMDV has the best throughput. Due to the nodes mobility the throughput varies from time to time which is represented in the below graph

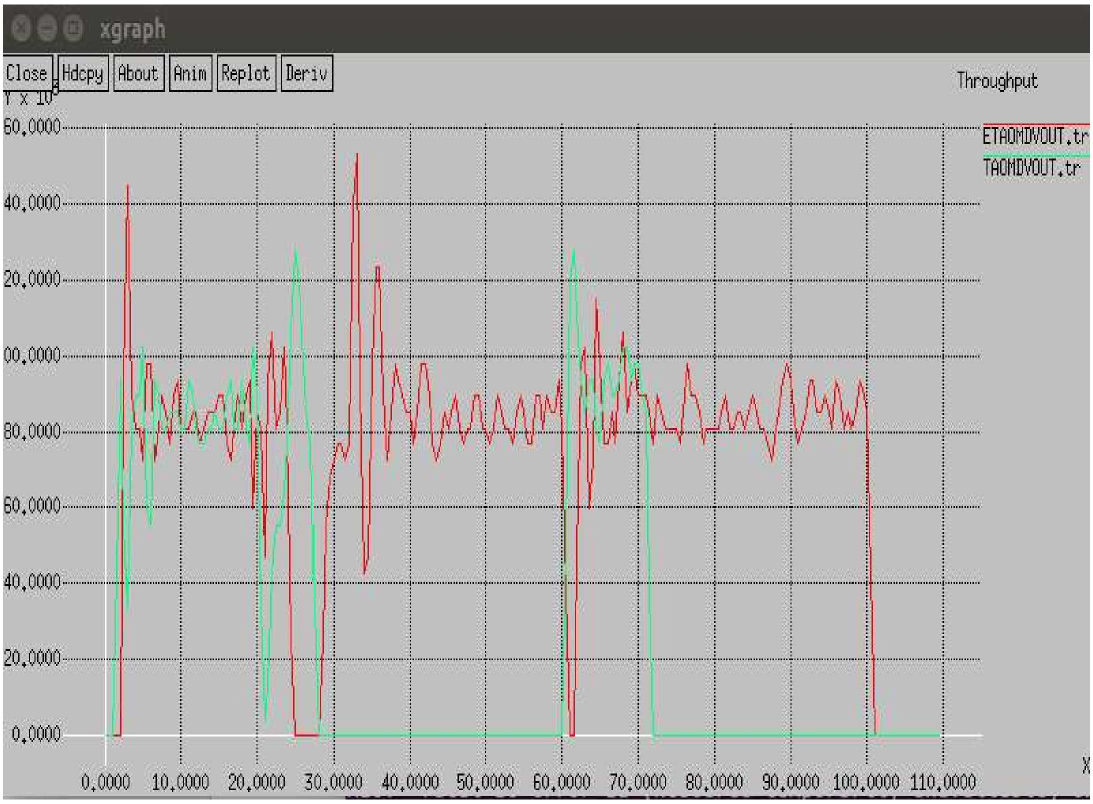


Figure 4.4: Throughput

Packet Loss:

As there is a huge traffic in the network, there will be loss of data due to congestion at the nodes in the network. If the congestion occurs then there will be huge packet loss. By comparing with T-AOMDV, ET-AOMDV has less packet loss which is shown in the following graph.

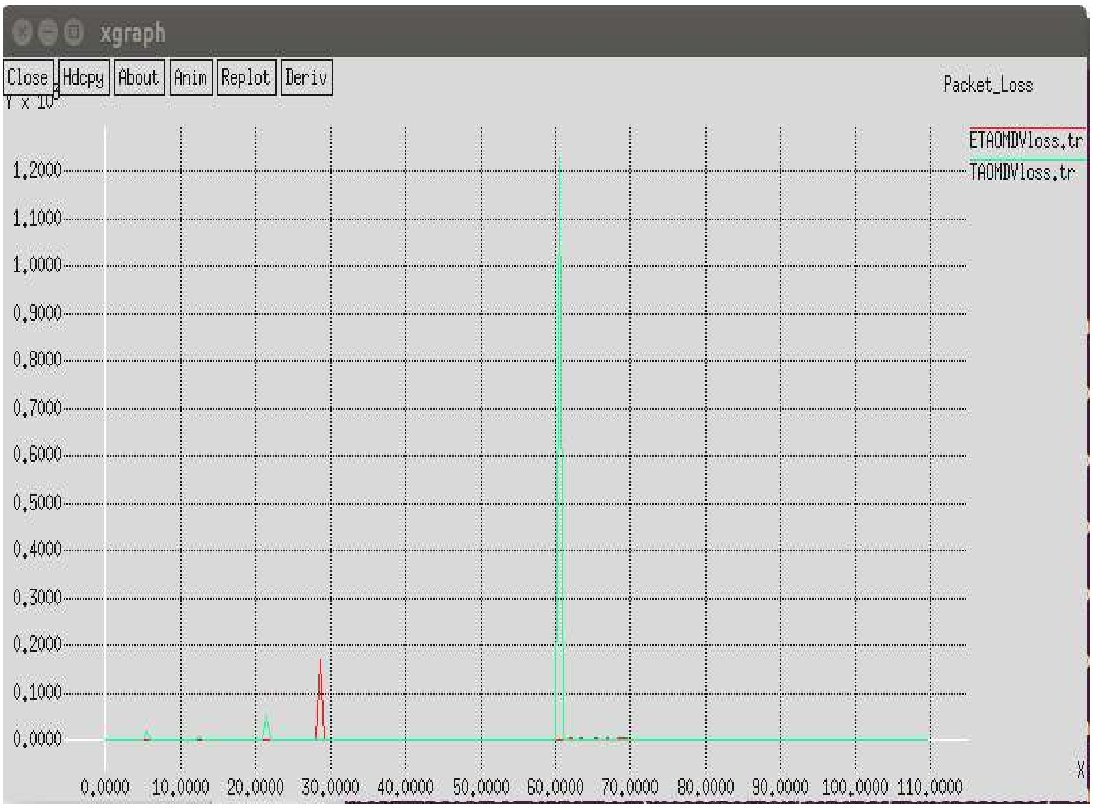


Figure 4.5: Packet Loss

End to End Delay:

As there are many nodes in the network there will be huge data traffic by the data transfer from the nodes. As the nodes do not have fixed topology then delay will be increased. ET-AOMDV has the best end to end delay than T-AOMDV which means it have less delay.

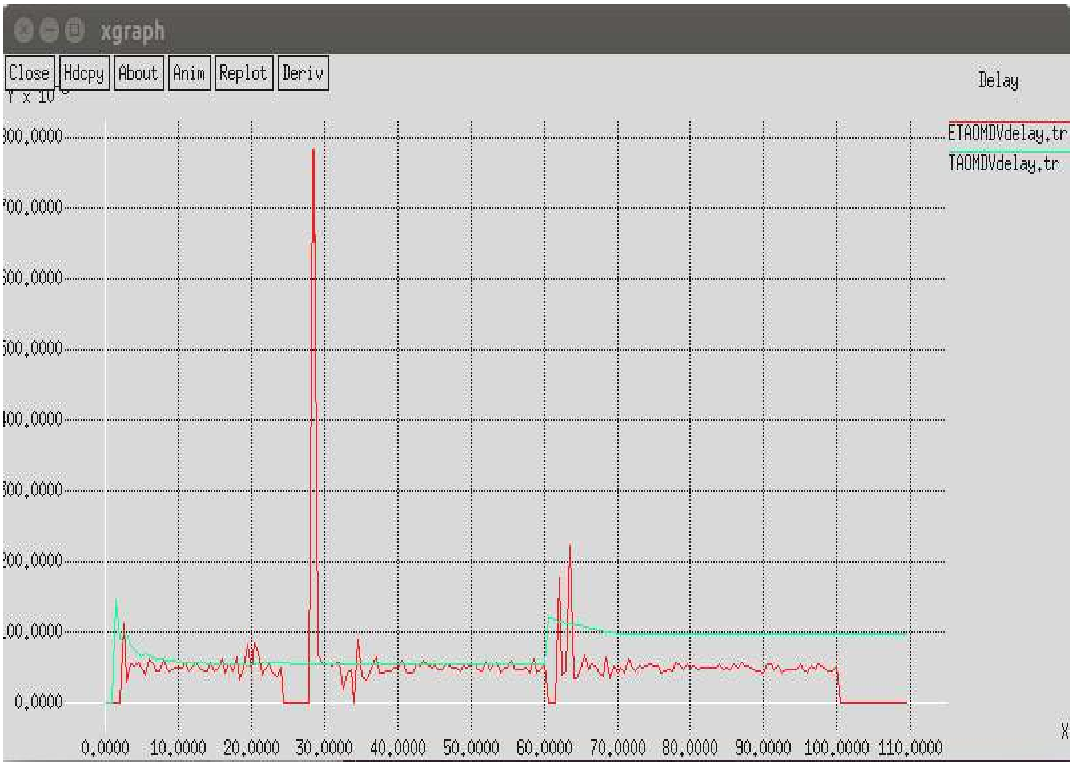


Figure 4.6: End to End Delay

Energy Deviation:

As there were many nodes in network the nodes uses power to process. The consumption of power by the nodes can vary from node to node. We can see the energy deviation of nodes at various time slots and we can know the average energy consumption nodes in the network.

Energy deviates from node to node and from time to time. When there is a huge load on the node then more work is processed at that node. So large amount of energy is consumed by node when there is load on that region or node. The graph is plotted based upon the time span and the energy consumed by the node.

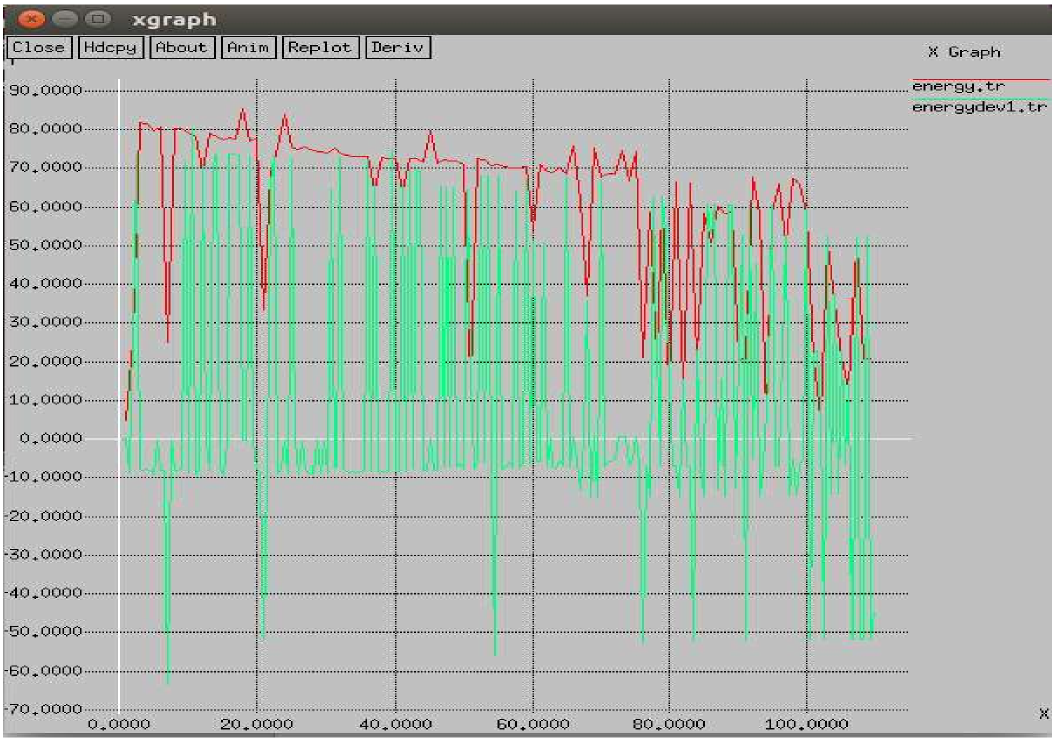


Figure 4.7: Energy deviation

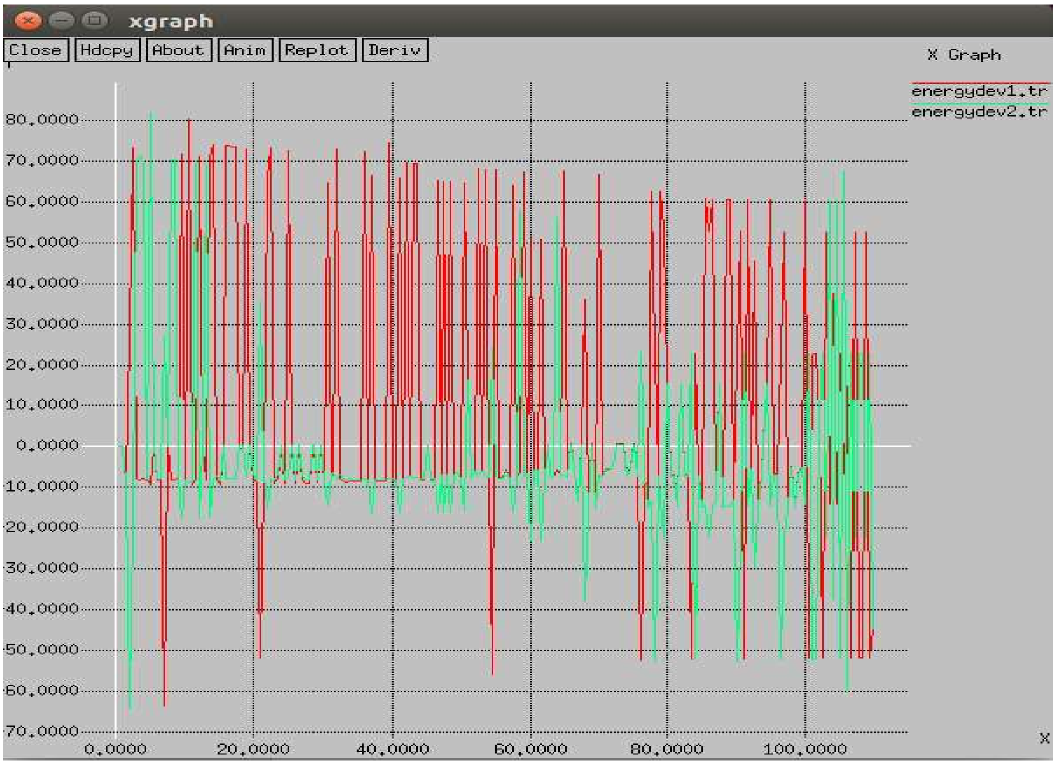


Figure 4.8: Energy deviation

Route Selection time:

The time which taken by nodes to deliver the packet to destination and a particular route is selected. In ET-AOMDV route selection time is less than the remaining algorithms. If congestion or any packet loss occurs or any of the nodes is compromised then source node immediately changes the path and secures the packets and path.

In the route selection time scenario, we have considered 17 nodes with some speed. Data success transfer will be different according to the network size. It is observed that ET-AOMDV has route selection time than T-AOMDV. Both the algorithms need trusted paths for routing. By comparing with number of malicious nodes in the network, ET-AOMDV has taken less time than T-AOMDV for selecting the route. We can observe in the following figure

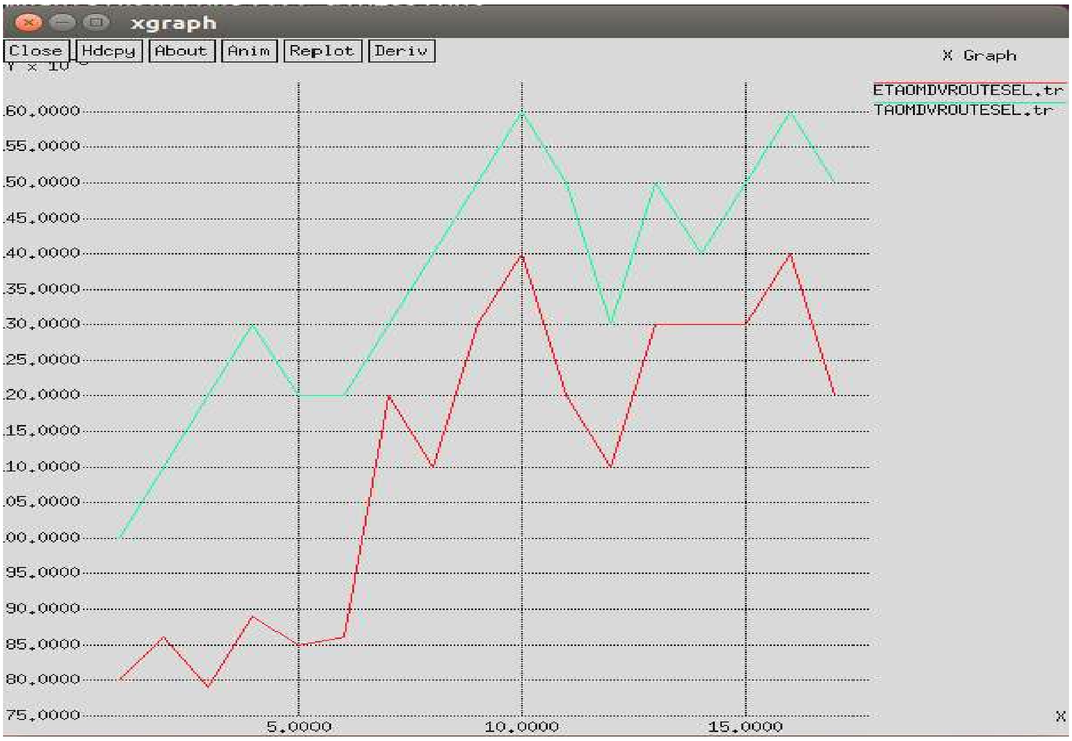


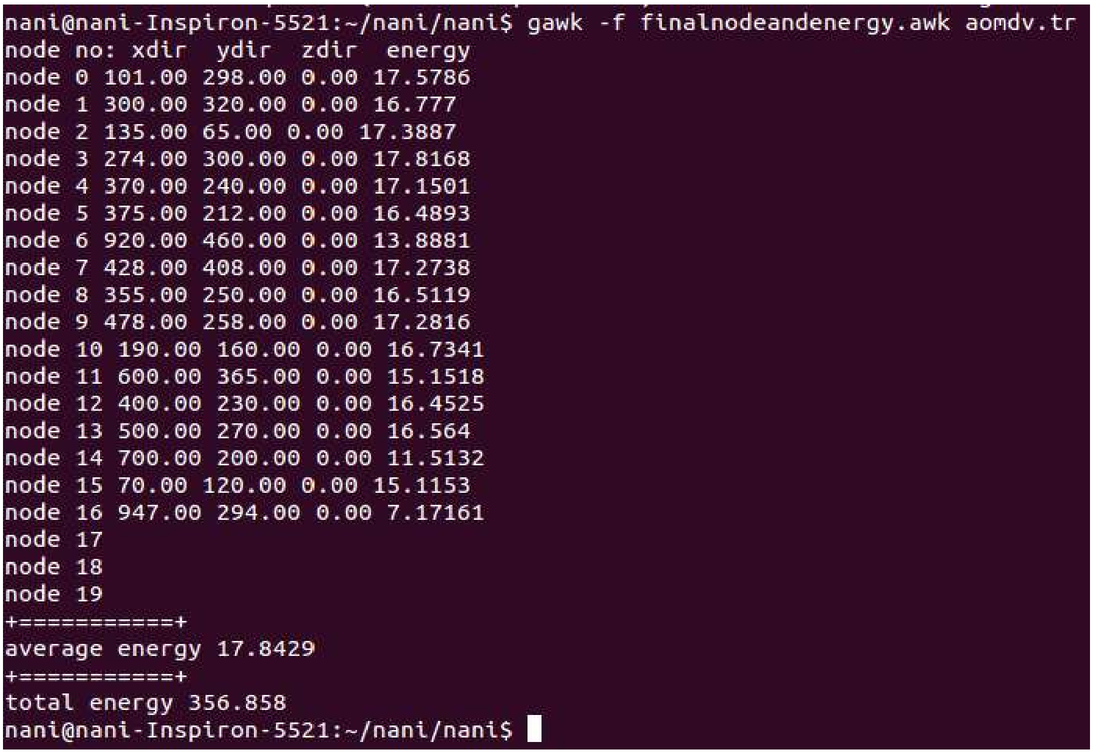
Figure 4.9: Route Selection Time

Trust Compromise:

As there will be many malicious nodes in the network, the data transfer through that nodes will dropped by that node or it may get that data. Some nodes can be compromised then if our data packet passes through that compromised node then the data can be compromised. As our algorithm is about for trust, it selects the path based upon the trust value which satisfies it configuration. There will be no trust compromise as same to the T-AOMDV and T-DSR. It has the zero compromise value.

Final Node and Energy:

After the movement of nodes in the network, the nodes does not have any fixed location, according to the scenario given in the simulation script, the nodes reach their final position by the axis of location and displays consumption of energy by each node in the network .By considering the energy of various nodes average energy of the node consumed is calculated. Also displays the total energy consumed by the nodes in the network. We can observe in the following figure



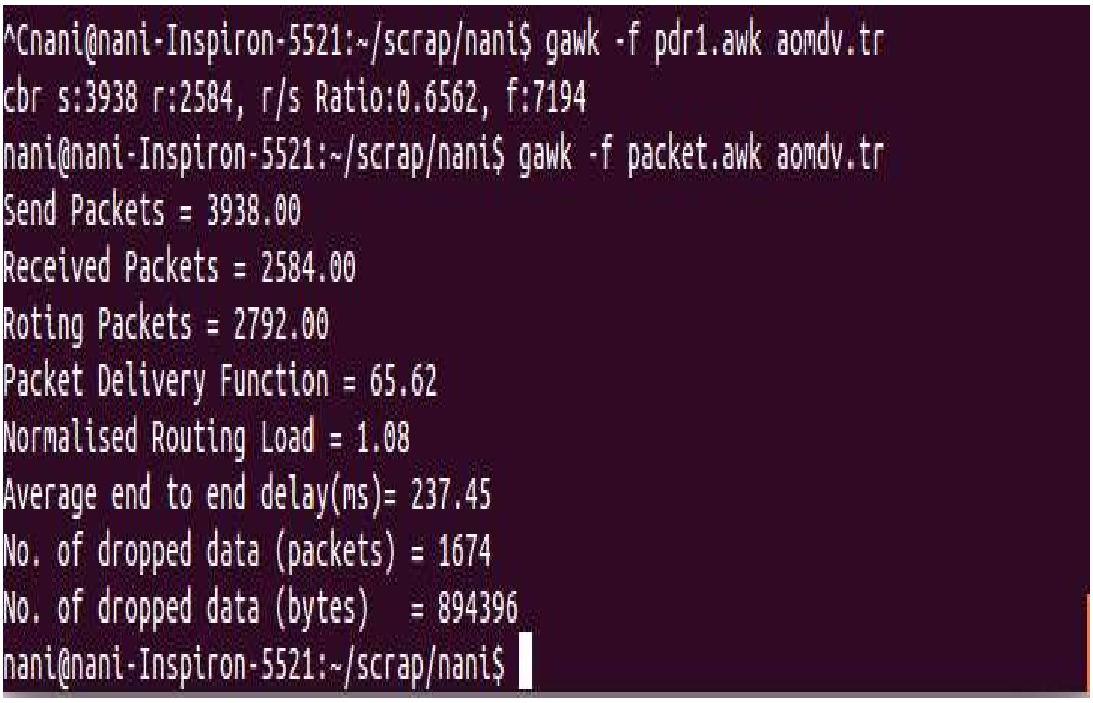
```
nani@nani-Inspiron-5521:~/nani/nani$ gawk -f finalnodeandenergy.awk aomdv.tr
node no: xdir  ydir  zdir  energy
node 0 101.00 298.00 0.00 17.5786
node 1 300.00 320.00 0.00 16.777
node 2 135.00 65.00 0.00 17.3887
node 3 274.00 300.00 0.00 17.8168
node 4 370.00 240.00 0.00 17.1501
node 5 375.00 212.00 0.00 16.4893
node 6 920.00 460.00 0.00 13.8881
node 7 428.00 408.00 0.00 17.2738
node 8 355.00 250.00 0.00 16.5119
node 9 478.00 258.00 0.00 17.2816
node 10 190.00 160.00 0.00 16.7341
node 11 600.00 365.00 0.00 15.1518
node 12 400.00 230.00 0.00 16.4525
node 13 500.00 270.00 0.00 16.564
node 14 700.00 200.00 0.00 11.5132
node 15 70.00 120.00 0.00 15.1153
node 16 947.00 294.00 0.00 7.17161
node 17
node 18
node 19
+===========+
average energy 17.8429
+===========+
total energy 356.858
nani@nani-Inspiron-5521:~/nani/nani$ █
```

Figure 4.10: Final Node Position and Energy

Packet information:

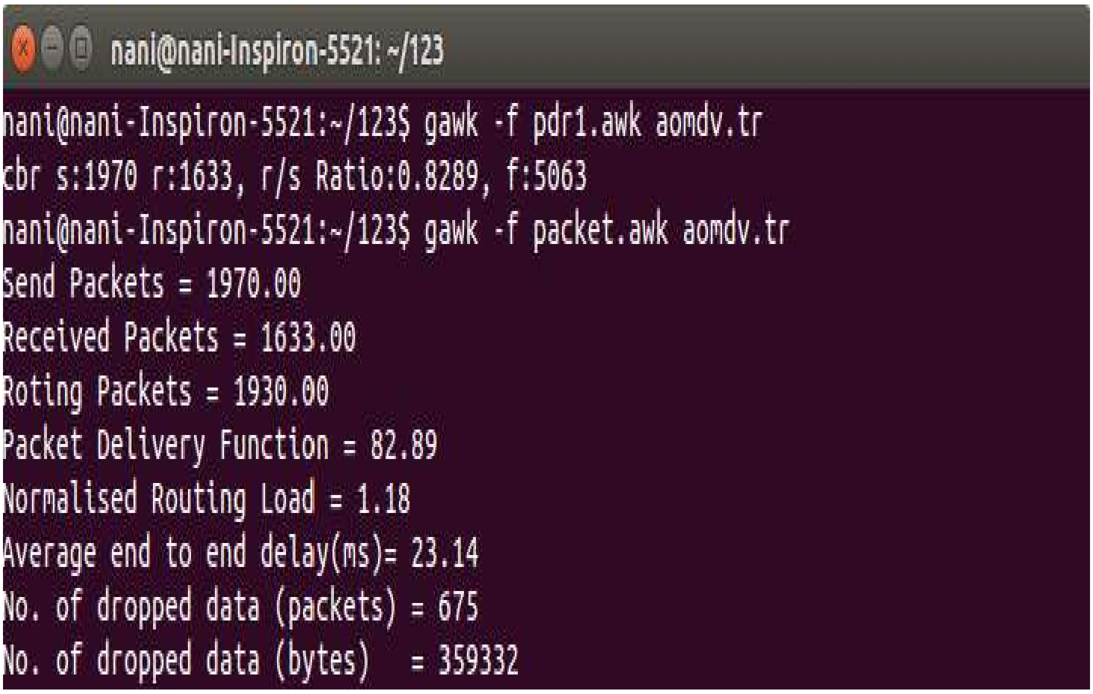
It mainly describes about the packet information such has number of sent packets, number of received packets, packet delivery function- as it displays the number of successful packet delivery in the network. Number of packets dropped in the packet and bytes extensions also gives the average end to end delay and normalized routing load in the network.

By the scenario we can express that ET-AOMDV has the best packet information than T-AOMDV in all the functions described above. All these can be analysed by the help of trace file generated at the time of simulation.



```
^Cnani@nani-Inspiron-5521:~/scrap/nani$ gawk -f pdr1.awk aomdv.tr
cbr s:3938 r:2584, r/s Ratio:0.6562, f:7194
nani@nani-Inspiron-5521:~/scrap/nani$ gawk -f packet.awk aomdv.tr
Send Packets = 3938.00
Received Packets = 2584.00
Roting Packets = 2792.00
Packet Delivery Function = 65.62
Normalised Routing Load = 1.08
Average end to end delay(ms)= 237.45
No. of dropped data (packets) = 1674
No. of dropped data (bytes)   = 894396
nani@nani-Inspiron-5521:~/scrap/nani$ 
```

Figure 4.11: T-AOMDV Packet Information



```
nani@nani-Inspiron-5521:~/123$ gawk -f pdr1.awk aomdv.tr
cbr s:1970 r:1633, r/s Ratio:0.8289, f:5063
nani@nani-Inspiron-5521:~/123$ gawk -f packet.awk aomdv.tr
Send Packets = 1970.00
Received Packets = 1633.00
Roting Packets = 1930.00
Packet Delivery Function = 82.89
Normalised Routing Load = 1.18
Average end to end delay(ms)= 23.14
No. of dropped data (packets) = 675
No. of dropped data (bytes)   = 359332
```

Figure 4.12: ET-AOMDV Packet Information

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

Conclusion and Future Scope

In this paper we are proposing a new technique on a T-AOMDV to increase the security in the packet called ET-AOMDV. Here we proposed a technique which increases more security by using some cipher techniques and further encryption is performed. The node cannot be compromised by where the packet routed in different independent paths. This paper can be extended by working upon several security algorithms to provide security and this can be worked on some of the routing protocols as DSR, DSDV. To improve better security we can compare by packet transfer. We would like to compare our algorithm scheme against other popular secured routing protocols for Manets.

CHAPTER 6
REFERENCES

I. Research Papers

[1]Huang Jing Wei, Woungang Isaac,Han Cheih Chao ,Mohammed S.Obaidat " *Multi Path Trust Based Secure AOMDV Routing in Adhoc Networks* "(IEEE Globe com 2011)

[2] Huang Jing Wei,Isaac Woungang,Han – Cheih Chao ,Mohammed S.Obaidat "*Trust Enhanced Message Security Protocol for Mobile Adhoc Networks* "(IEEE ICC 2012)

[3] Kaur Robinpreet , Mritunjay Kumar Rai "*A Novel Review on Routing Protocols in Manets* "(UARJ, ISSN :2278-1129 ,Volume -1, Issue -1 , 2012)

[4] Kim Cheolgi, Young-Bae Ko, Deepesh Man Shrestha *"A Reliable Multi-Grid Routing Protocol for Tactical MANETs*" (RACS '11, November 2-5, 2011, Miami, FL, USA.Copyright 2011 ACM 978-1-4503-1087-1/11/11)

[5] Kumar Gupta Naveen, Kavita Pandey "*Trust Based Adhoc On Demand Routing Protocol for MANET* " (IEEE 2013)

[6] Lou W , W.Liu ,Y.Fang "*SPREAD : Enhancing data confidentiality in mobile adhoc networks* "(INFOCOM 2004) .

[7] Lee S.J , M.Gerla *"Split multi path routing with maximally disjoint paths in adhoc networks"* (ICC 2001) .

[8] LOU WENJING and YUGUANG FANG *"Predictive caching Strategy for on Demand Routing Protocols in Wireless Adhoc Networks* "(2002)

[9] M Peralman R , Z.J.Haas , P.Sholander , S.S.Tabrizi "*On the impact of alternate path routing for load balancing in mobile adhoc networks* "(MobiHoc 2000)

[10]Narula P, S. K. Dhurandher, S. Misra, and I. Woungang, *"Security in mobile ad-hoc networks using soft encryption and trust based multipath routing"*, Computer Communications, Vol. 31, pp.760-769, 2008

[11] Qu Chuanhao , Lei Ju, Zhiping Jia, Huaqiang Xu, Longpeng Zheng *"Light Weight Trust Based on Demand Multipath Routing Protocol for Mobile ADHOC Networks"* (IEEE 2013)

[12] Ravilla Dilli , Dr.Chandra Shekhar Reddy "*Performance of Secured Zone Routing Protocol due to the Effect of Malicious Nodes in MANETs*" (4th ICCCNT – 2013 ,july 4-6 , 2013)

[13] Sanzgiri K, B. N. Levine, C. Shields, B. Dahill, E. M.Belding-Royer, "*A Secure Routing Protocol for Ad Hoc Networks*", Proc. of 10th IEEE Intl. Conf. on Network Protocols, Paris, France, pp. 78-89, Nov. 12-15, 2002

[14] Thanigaivel G, Ashwin Kumar N, Yogesh P "*TRUNCMAN : Trust Based Routing mechanism using Non – Cooperative Movement in Mobile Adhoc Network*" (IEEE 2012)

[15] Tsirigos A, Z.J.Haas "*Multipath routing in the presence of frequent topological changes*" (IEEE 2001) .

II. Websites

[1] http://www.isi.edu/nsnam/ns/tutorial/index.html

CHAPTER 7
APPENDIX

A

AODV – Adhoc on demand distance vector

AOMDV – Adhoc on demand multipath distance vector

B

BRP – Broadcast resolution protocol

C

CBR – Constant bit rate

D

DSR – Dynamic source routing

DSDV – Dynamic source distance vector

I

IARP – Intra zone routing protocol

IERP – Inter zone routing protocol

M

MANET – Mobile adhoc network

MSG - Message

N

NAM – Network animator

NDP – Neighbour discovery protocol

O

OTCL – Object oriented tool command language

P

PRP- Proactive routing

R

RReq – Route request

RRep – Route reply

RRP- Reactive protocol

S

SIARP – Secure intra zone routing protocol

SIERP – Secure inter zone routing protocol

SNDP – Secure neighbour discovery protocol

SPREAD – Secure protocol for reliable data delivery

U

UDP – User datagram protocol

Z

ZRP – Zone routing protocol