iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** Issue- II **Month of publication:** October 2014

DOI:

Special Issue-2, October 2014
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

A Layered Security Approach through FEMTO CELL using Onion Routing in MANET

T. Sathish[1], M.Senthil Kumar[2]
[1]*M.E. Scholar,* [2]*Assistant Professor*
Department of Computer Science and Engineering, Anna University,
Sree Sowdambika College of Engineering, Aruppukottai, TamilNadu, India.

***Abstract*— In earlier process, making a secure routing only discussed and never discuss about how to transfer data in a secured manner. Even though we performed routing in a secured manner, there will be chances of data should be dropped or revealed by an illegal persons. We use an onion routing to make a highly secured routing, so this routing includes the mechanism of layered by layered approach from one node to another node's. And we transfer the data in secured manner by sending dummy packets from source to destination, and these dummy packets are mold up by the mechanism of node characterization technique. And in earlier process they never looked for time and speed reduction. That is, in existing system, they use the concept of secured routing each and every time when data will be sent. So this will increase the speed reduction process which is at every moment of transaction we need to perform separate routing, to overcome this we proposed onion routing and node characterization. And we using femto cell device for strengthening the signal when there is no sufficient signal to work on the process.**
***Keywords*— MANETs, Routing Protocols, Secure Onion Routing, Layered Approach, Packet authentication, Femto cell, NS2.**

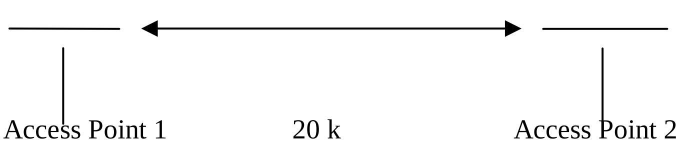
I. INTRODUCTION

A. MANET

The term MANET refers to Mobile Ad-hoc NETwork. MANET is a less infrastructure network; nodes are under mobility. It should be moved here and there and it won't rely stable. Mobile Ad-hoc networks are most familiar to security issues due to the characteristics of such networks such as a wireless medium and dynamic topology. It is very harder to provide trusted and secure communications in enemy environments such as battle fields. On one hand, the malicious persons outside the network may have an idea to reveal the information about the communicating nodes, even when communications are encrypted. On the other hand nodes involved inside network will always be trusted, since a trusted node may be hold by illegal person and become malicious.
In MANET, a set of interacting nodes should cooperatively implement routing functions to enable end-to-end communication along dynamic paths composed by multi-hop wireless links. Several multi-hop routing protocols have been proposed for MANET, and most popular ones include:
Dynamic Source Routing (DSR), Optimized Link-State Routing (OLSR), Destination-Sequenced Distance-Vector (DSDV) and Ad Hoc On-Demand Distance Vector (AODV). Most of these protocols are do their function on assumption of trusted manner. But sometimes it could not been trusted it behaves like secured less, because when there is a presence of malicious node at that time it emerges the weakness of MANET to cause various kinds of attacks.

B. ADHOC

Ad-hoc is a Latin word which refers to "all purpose". For example, take two access points as access point 1 and access point 2. There will be twenty kilometer distance in between those two access point.



If user A starts to download the data from access point 1, immediately user A tends to travel from access point 1 to access point 2. Now download is under half fulfilled. When user A which comes under out of coverage from access point 1 due to travelling. They face a problem about downloading.
Due to these criteria, we go for intermediate nodes concept to prevent interrupts which occurred in data transfer. So, that time the concept of Ad-hoc is established i.e. intermediate node is formed. Now data could be transformed very successfully but there will be a problem occurred under security concept. Because now the job is hold under intermediate nodes, we does not known details about intermediate nodes i.e. either it is a legal or illegal. When it is illegal, data will not been under secured way. So the major cause of this paper is about,

- Done secure routing
- Along with that the data transfer also will be in an secured manner

The remainder of this paper is organized as follows. The basic concepts and routing processes are analyzed in Section II. The protocol design is presented in Section III. The protocol evaluation is discussed in Section IV. Performance analysis is evaluated in Section V and Section VII concludes this paper. The future scope is conferred in Section VII.

II. BACKGROUND AND RELATED WORK

In existing system, they tell about how to perform a secure routing. They choose the main concept of secure routing as onion routing. Why they named as secured means, how an onion makes different layers when we start to cut it into small pieces, likewise here also they we forms different layers for checking each and every nodes as an one by one. It is like a layered i.e. what is the action handled by two nodes as a one layered. So we can name it's for our understanding as onion routing is also known as layered approach.

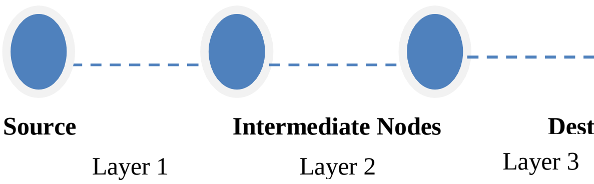


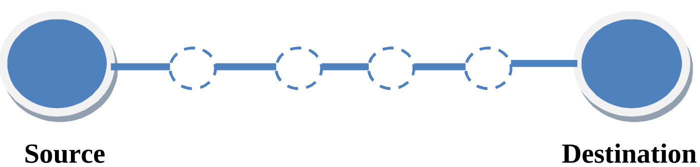
Fig.2.1 Layered approach

The main concept done in existing system is they did how to do secure routing for providing path. This will be discussed as follows. To accommodate secure rating these cases requires three kinds of techniques, they are:

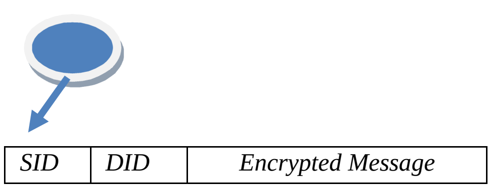
- Setting a trap
- Routing by means of layered approach(onion routing)
- Signature process

A. Setting A Trap

The general meaning of trap is to find out an unidentified or illegal person by without knowing an alert for the person whom is involved. The main concept involved in this technique is as follows. Let consider, there are six nodes from source to destination.



To set a "trap" separate id is given to each node. The id should also been included for source and destination node too. For Source Node,



I1→ identity "id" for Node 1

So, these processes are going on until data or message reaches the destination node. By setting an identity for each node 'I' can able to find the illegal persons, because illegal persons do not have their identity number. So step by step, it travels from source node to destination node which comes across through different intermediate nodes. The nature cause of this mechanism is to set a route request message from source to destination node.

B. Onion Routing

Once a route request message is perfectly reached by destination node, the destination node again they start a work about route reply. The ROUTE REPLY is a main process for this mechanism, by the mechanism using in my project is about onion routing. In setting a trap, the route request message is starts from source node to destination node. But here in route reply it starts from destination node to source node.

C. Working process of onion routing

Special Issue-2, October 2014
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology(IJRASET)

It is a simple process here we are going to removing the identity number of each intermediate nodes from destination end points to source end points(reverse process).

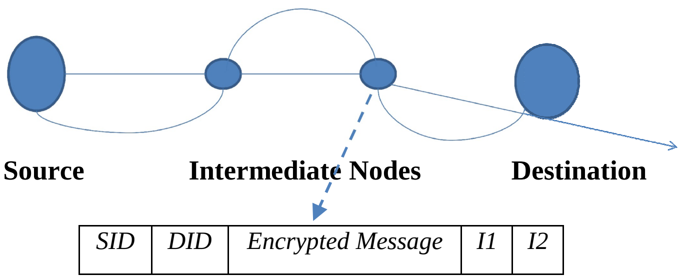
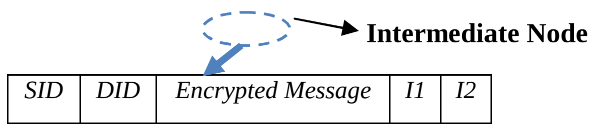


Fig.2.2 Process of Onion Routing

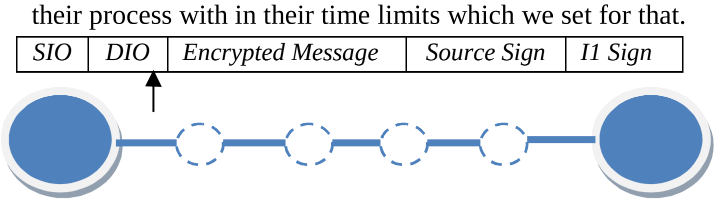
In the above diagram route reply request is send from destination node and its moved to the intermediate node. Here how they will choose intermediate node means that the path which the route request came across. So its starts from the intermediate node first its goes for last intermediate node. In that it removes the top of the key which is present.



From this diagram, I2 will be removed. This is a top of the key. Once it is finished then it will be moved for another node. This process is known as layered approach and finally its came to source node and delivered the route reply message.

2.1 SIGNATURE PROCESS

In signature process, we are going to generate group signature and along with that session key. The main process key is to finish their process with in their time limits which we set for that.



For example, the session number=5 packets means, there should be five packets could be sent at a time. If there is exceeding of any packet count there will be some jobs did by an illegal person

III. PROTOCOL DESIGN

We invent a much effective method to make an protection under both packet dropper and modifier's, in this method let's take upon routing tree which is at sink it will be accomplished very first. At the time of sensor data are make an survey along the tree structure towards the sink, every packet sender adds upon small number of extra bits to it, which is also known as packet marker's to the packet. And then runs up the node characterization algorithm for identifying node's which hold packet dropper and modifier. This is the one of the way to identify the bad nodes.

A. Node Characterization Algorithm

This algorithm includes the following methods. They are,

- Stepwise ranking method
- Global wise method
- Hybrid ranking method

Using this algorithm, we are going to send dummy packet with sequence number, random number and padding.

- *Sequence number* is for the packet which we are going to sent.
- *Random number* for the node, here why we choose random number for node means, to find out the hacker which is either it was good node or bad node.
- *Padding* shows the position of the node. If it is a
first node means, it shows the position as 0th node (zeroth node).

SID	*DID*	*Sequence Number*	*Random Number*	*Padding*

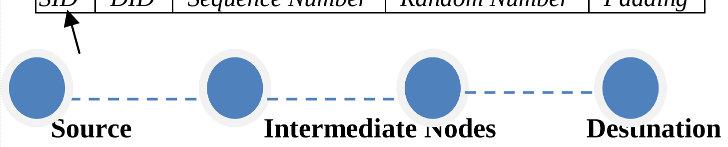


Fig.3.1 Parameters of Node Characterization Algorithm

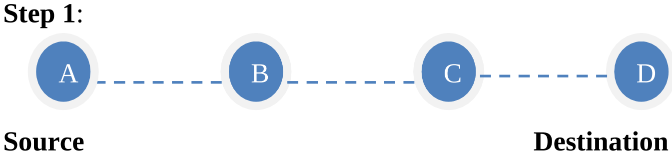
- For example, I need to transfer 50 kp packets means, I split as 10 kp as first packet and 20 kp as second packet and 20 kp as third packet and it is an automated one.
  From the above diagram, first packet of node includes,

SID	*DID*	*Sequence Number*	*Random Number*	*Padding*

This information will be in the source node only and this is a general concept.

- PROCESS WHICH ARE GOING

Step 1:



When the first dummy packets are in Node ‘A’ that is under source node it holds the information of,

SID	*DID*	*Sequence Number*	*Random Number*	*Padding*

0^{th} node

Here sequence number provides some identity number for first packet as for example: ‘1’. And random number also has been provided. After that padding will be stored as 0^{th} position because it’s a first position of the node.

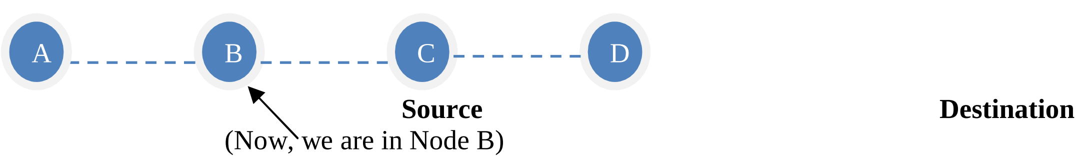
Step 2:

Similarly the same first packet will be moved from Node A to Node B. The Node B holds the information like,

SID	*DID*	*Sequence Number*	*Intermediate Random Number*	*Intermediate Padding*

1^{st} Node

When same first packet will be moved from Node A to Node B, it should contains same sequence number, and also been with source random number id, along with that new intermediate node random number, and finally intermediate node padding position is 1^{st} Node.



Step 3:

The same first packets move from Node B to Node C. For example, we found that we have packet modification. So, this packet modification shows that the presence of changed packet information. That is an anonymous person could modify the data. For example, how can we find our data will be modified means?

1. There will be changed in sequence number example we use ‘1’ as an sequence number means these will be changed as 1.4 or 1.7 which what we given it won’t present here.
2. The random number should not been generated for illegal person.

Step 4:

If we are going to send second packet means, the sequence number will be changed as ‘2’ then its move from Node A , Node B, Node C.

- *General Rule:*
  - First packet → ‘1’ sequence number
  - Second packet → ‘2’ sequence number

Special Issue-2, October 2014
ISSN: 2321-9653

- Third packet → '3' sequence number

IV. PROTOCOL EVALUATION

The proposed system has the following features:

- Identifies both a kind of malicious activity like packet dropping and modifying.
- Achieving low communication and overheads.
- Much more suitable for existing false packet filtering schemes that is this scheme will make an end point for malicious packets.

We going to deployment large number of sensor nodes in an two dimensional area. The nature job of each sensor node's generate the data regularly and intended to forward packets towards an sink and the sink is located inside the network.

A. Step wise ranking method

Yet now we find the one will be safer node. So, now we going to note which node will be good node or which will be bad node. So for finding, I will just make all nodes under tree formation. That is the nodes which are nearby.

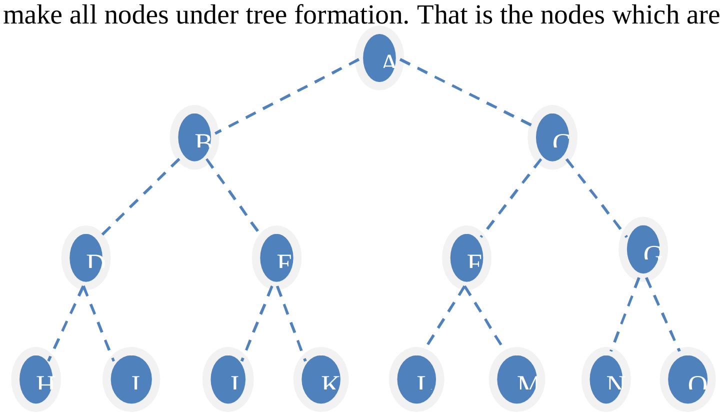


Fig.4.1 Tree Structure of Nodes Formation

For example, in node A we have 10 packets, now we going to check of these whether this remaining nodes are good node or bad node. Node A sent 10 packets to every nodes which are present in the tree (b,c,d,e,f,g,h,i,j,k,l,m,n,o).

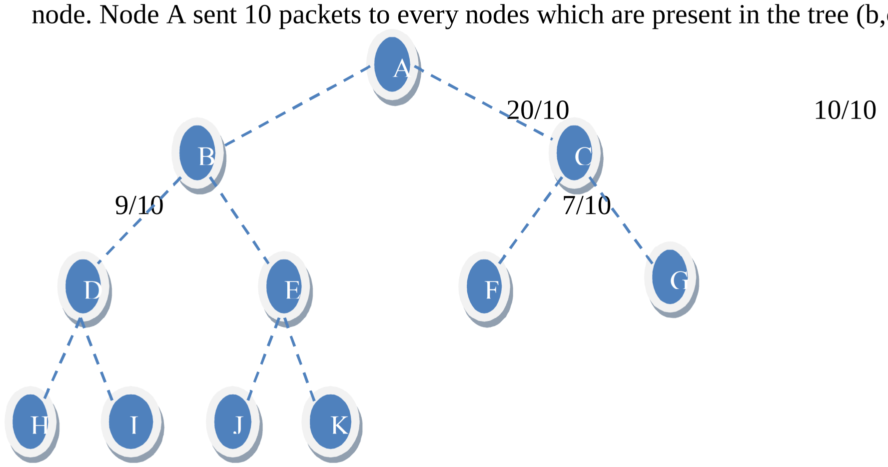


Fig.4.2 Step Wise Ranking Method

- Good Node – 10/10
- Bad Node – 20/10, 8/10, 7/10
- Unknown Node (Either Bad or Good) – 9/10,11/10

By using this, we may find either which one will be good node or which one will be bad node. It is a step wise ranking method. We are going to see step by step which is from top layer of the tree. When we seen, Node B as 10/10 means it will be good node and it will be selected. Similarly, take Node 'D', it has 9/10 so it is under the scenario of unknown either bad or good. If we reject these nodes, their child node also deleted and it is a drawback of this method.

Special Issue-2, October 2014
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology(IJRASET)

B. Global wise ranking method

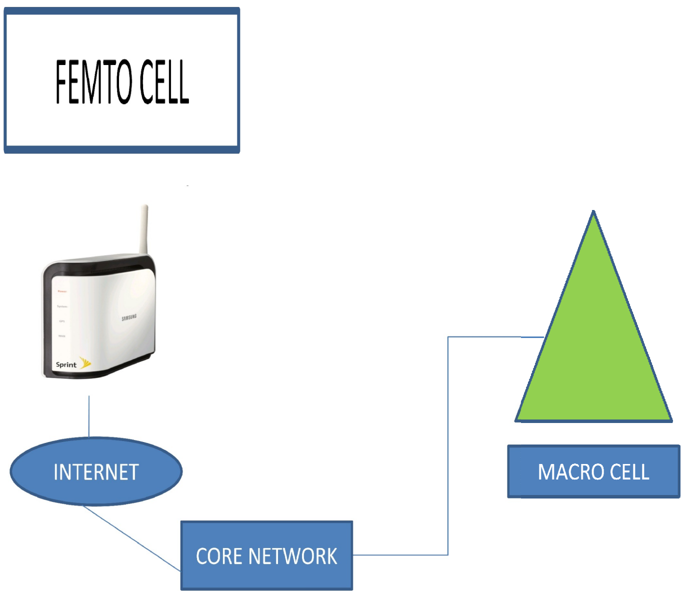
To overcome the drawback which are comes under stepwise ranking method we need to seen these node under over all view that is which one will be best. By selecting that best one, we are going to use the best one for our process that is for packet transaction.

C. Hybrid ranking method

These methods are combination of stepwise ranking method and global ranking method. Here the node which is having highest priority will choose as first and it is most likely bad node.

D. Femto cell

Femto cell is an device which act as wireless access point , its used to strength the signal and to provide the same signal range whatever its came from the core network and the range of femto cell process about 10 metres. These femto cell are particularly designed for small environment, so this theme got correlated with my project which is after selecting an particular route for my data transmission here I'll have some less amount of node's , so the data starts to travel across the node which I framed. The main problem is node coverage will be differs according to distance of each node from the core network's and this leads to higher time consumption in data transfer. So when we use femto cell near to node which does not have fulfilled coverage means we can able to successful in over-come these drawback.



V. PERFORMANCE ANALYSIS

A. Network Configurations

TOPOLOGIES

In our research the network area is about 1500m x 600m with 80 nodes normally and it should be equally distributed. Here the function of distributed coordination IEEE 802.11 is used as the MAC layer. And the capacity of channel is about 3Mbps, transmission range is occurred was 250m.The mobility in node should be there by using random way point model. The total of 20 UDP based CBR sessions are used to create the network traffic.

2) Attacking Models

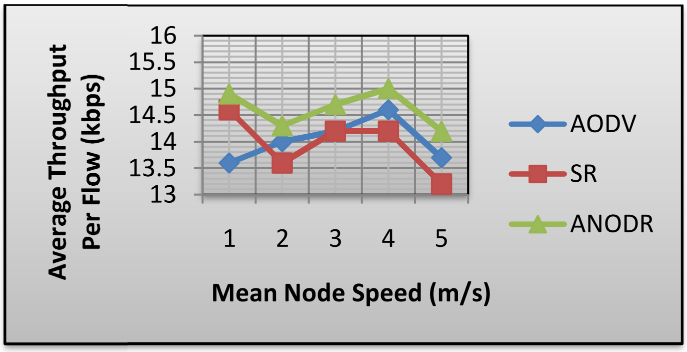
The general assumption about the intermediate nodes along the route may become malicious If there is any malicious node then the routing packets are randomly dropped. For example in previous routing like ANODR and AODV will suffer more packet loss. The AASR detect the malicious node by using the signature method and find out the details of attackers in routing table.

3) Simulation Results

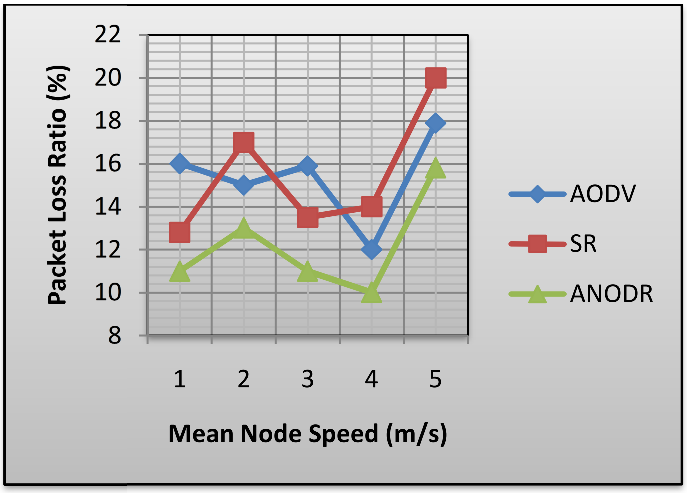
a. Effects of Mobility Scenario

Special Issue-2, October 2014
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology(IJRASET)

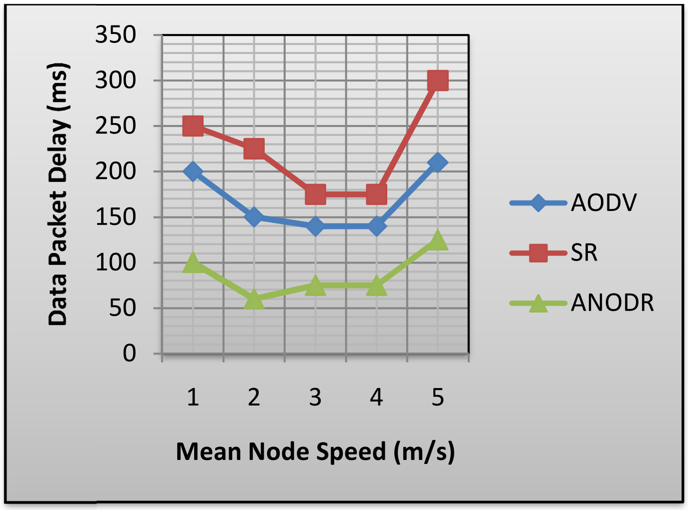
To simulate the enemy environment, we are going to choose twenty percentage of total nodes, which is ten nodes as malicious nodes and then we can able to change the network mobility from one to eight m=s and record the performance results. From the results the average nodal speed increases, similarly the throughput also varies because nodes have an capability of move randomly. Due to performance variation secure routing always achieve highest throughput. The following figures a, b, c describe the performance of different mobility settings.



a. Per Flow Throughput



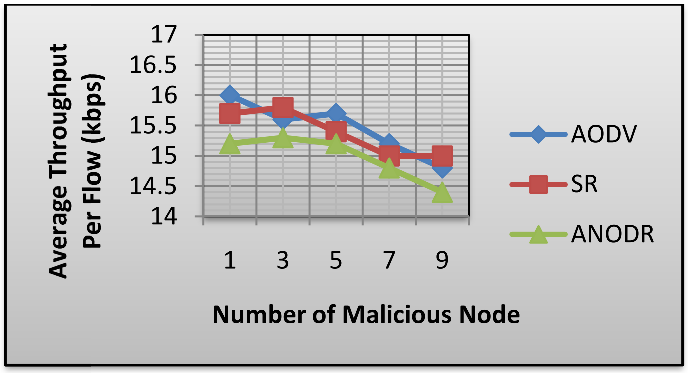
c. Packet Loss Ratio



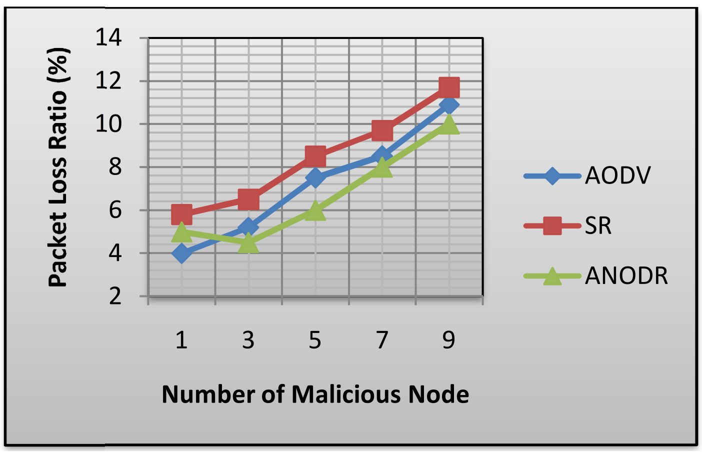
c. End-to-end Delay

b. Effects of Malicious Attacks

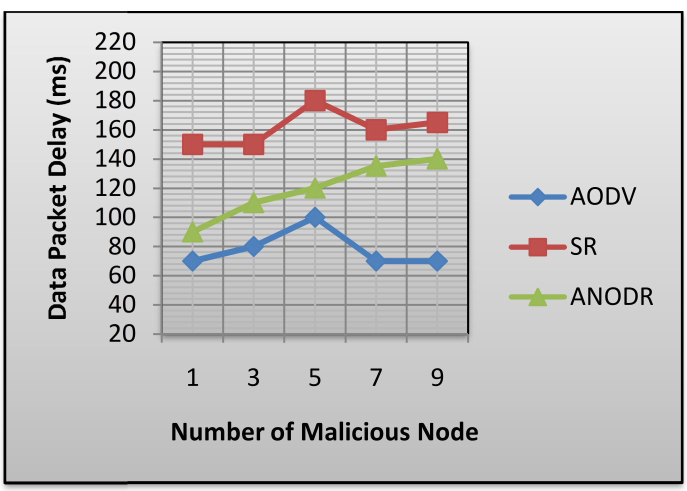
The configuration of mobile network with an average as 4m=s, therefore in general the number of malicious nodes increases similarly the throughput decreases. The following figures a, b, c show the performance in the presence of different number of malicious nodes



d. Per Flow Throughput



e. Packet Loss Ratio



f. End-to-end Delay

Special Issue-2, October 2014
ISSN: 2321-9653

VI. CONCLUSION

There will be lot of MANET security routing concept can be obtained, but yet now there will be no intimation to secure packet authentication. If there is any malicious activity means those packet will be dropped so the information might be destroyed. Therefore this is a correct solution for an hackers or intruders they achieve their task which means they finish their main job. But I'll find a solution by introducing the dummy packet concept with some secured mechanism, this will helpful for lightning a successful path of conveying original information from source to destination. And I'll used femto cell to make more strengthened signal coverage for achieving more efficient process.

VII. FUTURE SCOPE

The nature cause of anonymous is come due to a confidential message or data which is sent through an intermediate node. So I first focused about how to make an malicious intermediate node into trustable intermediate node. I'll going to accomplish this task by generating survey about nodes by finding out good node, bad node and unknown status about either good or bad node. It is an attainable solution by using the ranking method concepts.

VIII. REFERENCES

[1] (Nevin) Lianwen Zhang and David Poole, "Stepwise-Decomposable Influence Diagrams", Department of Computer Science, University of British Columbia, Vancouver, B.C, V6T/Z2, Canada.
[2] N.Vanitha, G.Jenifa, "Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3,Issues 3,pp.69-74, March 2013.
[3] Hussein Al-Bahadili and Khalid Kaabnel, "Analyzing the Performanceof Probabilistic Algorithm in Noisy MANETs", International Journal of Wireless and Mobile Networks, pp.82-94, Vol.2, No.3, August 2010.
[4] Shio Kumar Singh, M.P Singh and D.K Singh, "Routing Protocols in Wireless Sensor Networks - A Survey", International Journal of Computer Science and Engineering Survey, Vol.1, No.2, November 2010.
[5] Hee Yong Youn, Chansu Yu, Ben Lee,"Routing Algorithms for Balanced Energy Consumption in Ad-hoc Networks".
[6] Zaiba Ishrat, Pankaj Singh, "An Enhanced DSR Protocol Using Path Ranking Technique", International Journal of Engineering Research and Applications, Vol.3, Issue 3, pp.1252-1256, May-JUNE 2013.
[7] Wenjia Li, Anupam Joshi and Tim Finin, "SMART: An SVM-Based Misbehavior Detection and Trust Management Framework for Mobile Ad-hoc Networks".
[8] Ruchi Rani, Manisha Dawra, "Performance Characterization of AODV Protocol in MANET", International Journal of Advanced Research in Computer Engineering and Technology, Vol. 1, Issue 3, May 2012.
[9] Kannan Govindan, Member IEEE and Prasant Mohapatra, Fellow IEEE, "Trust Computations and Trust Dynamics in Mobile Ad-hoc Networks: A Survey".
[10] Changbin Liu, Yun Mao, Mihai Opera, Prithwish Basu, Boon Thau Loo, "A Declarative Perspective on Adaptive MANET Routing", August 2008.
[11] Mamatha.T, "Network Security for MANETs", International Journal of Soft Computing and Engineering, Vol.2, Issue 2, MAY 2012.
[12] Muhammad Arshad Ali and Yasir Sarwar, "Security Issues Regarding MANET (Mobile Ad-hoc Networks): Challenges and Solutions", Master Thesis, Computer Science, Thesis No: MCS-2011-11, March 2011.
[13] DSF for MANETs (Distributed Services Framework for Mobile Ad-hoc Networks).
[14] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs in Protocol Stack A-Review", International Journal of Engineering and Advanced Technology, Vol.1, Issue 5, June 2012.
[15] WWRF/WG4/Ad-hoc Networking-Subgroup WhitePpaper, Version 1.0, 17th June 2002.