ENHANCED SECURITY MECHANISM TO MITIGATE BLACKHOLE ATTACK IN MANET USING FUZZY LOGIC

Monika Nandal[1], Deepak Goyal[2] , Pankaj Gupta[3]
[1]*M.Tech Student, Vaish College of Engineering, MDU, Rohtak, Haryana (India)*
[2]*Associate Prof., Vaish College of Engineering, MDU, Rohtak, Haryana (India)*
[3]*Professor , Vaish College of Engineering, MDU, Rohtak, Haryana (India)*
[1] monikanandal90@gmail.com
[2] deepakgoyal.vce@gmail.com

Abstract— A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by radio links and maintaining connections with each other in a decentralized manner. Security is a major challenge for wireless networks due to several features such as open medium of communication, dynamic topology, absence of centralized accessing points etc.[7,10]. In this paper, Blackhole attack is discussed. A Black hole node[5] is actually a bad node which seems to promise sender that it will direct the message to the correct receiver, but in actual it either drops the packets, not try o send the message to proper destination or disturb the contents stored in packets. So, to protect the network layer of a MANET from this black hole attack is an important issue. We try to use fuzzy approach to detect and prevent node to be black hole[4]. Here, three parameters –throughput, packet loss, packet delay are used to ensure which neighbor node will be next hop to reach destination We use AODV protocol. While selecting the next routing node a fuzzy analysis is performed to identify the maximum throughput node, minimum packet loss and the minimum delay node. The work generates a new routing path for the communication. The obtained results show that the proposed approach has improved the overall communication over the network and reduced the packet loss.

***Keywords**: Mobile ad hoc network (MANET), black hole attack, packet dropping attack, malicious node, routing misbehavior, collusion,, multicasting, fuzzy logic*

I. INTRODUCTION

A wireless ad hoc network is a decentralized network where topology changes constantly and no need of centralized infrastructure, no access points. Wireless devices include laptop, palm devices, cell phones etc. Each node acts as routers by forwarding data to the other nodes. Therefore, no need of routers.

Types of Ad-hoc Network

A. *Wireless Mesh Network: No*des communicating through radio links in a mesh topology. Mesh clients, mesh routers are terms used. The mesh clients may be laptops, cell phones and other network devices and the mesh routers Wireless mesh network (WMN) is a wireless network consists of forward traffic to and from the gateways need not connect to the Internet

B. *Wireless Sensor Network :* WSN is a wireless network consisting of distributed autonomous devices having sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, pressure etc, at different locations .A wireless sensor node consists of sensation, computation, communication, actuation, and power components. These components are integrated on to a single or multiple boards, and packaged in a few cubic inches. These sensor nodes are responsible for self-organizing an appropriate network configuration. Location and positioning information about a node can also be obtained through the global positioning system (GPS) or local positioning algorithms. This information can be gathered from across the network.

C. *Manet:* A Mobile ad hoc network(MANET) is a group of wireless nodes in which nodes collaborate by forwarding packets to each other to communicate outside range of direct wireless transmission without the aid of any established infrastructure such as router because it itself act as router, A high risk of attacks. AODV is vulnerable to the well-known black hole attack[35],

Advantages of Manet:

- They provide access to information and services regardless of geographic position of nodes.
- Dynamic Networks can be set up.

Disadvantage of Manet:

- Resources constrained and less security.
- Vulnerable to attacks.
- Limited battery power
- Lack of authorization facilities.
- Dynamic network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

Applications of Manet:

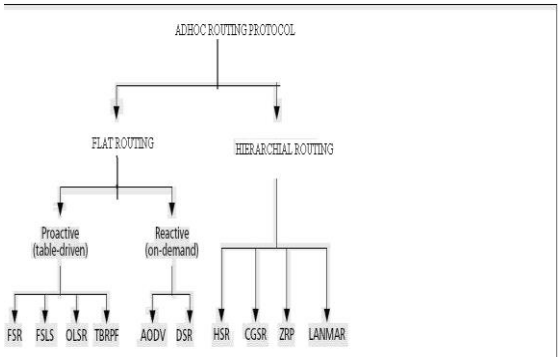
- Military or police exercises.
- Disaster relief operations.
- Mine cite operations.
- Urgent Business meetings.

II ROUTING PROTOCOLS[8,9]

There are different routing protocols in MANET are used, The routing protocols can be classified into Flat, hierarchial routing protocols.

- Flat routing protocols: These protocols are divided mainly into two classes; the first one is proactive routing /table driven protocols and other is reactive /on-demand routing protocols. One thing that is common in both protocols is that every node participating in routing plays an equal role. They have further been classified according to their design principles; proactive routing uses link-state algorithm while on-demand routing uses DV (distance-vector routing protocol).

A. *Pro-Active / Table Driven routing protocols[6]:* Proactive MANET protocols are also called as table-driven protocols and here regular exchange of packets between nodes



determine the layout of the network and an absolute picture of the network are maintained. Hence, there is minimal delay in determining the route to be taken. The main disadvantages of such algorithms are:

- Respective amount of data for maintenance is to be kept.
- amount of traffic overhead generated
- excessive expenditure of energy is desired.
- work best in networks that have low node mobility or where the nodes transmit data frequently

B. *Reactive (On Demand) protocols:* Various Portable nodes-Notebooks, palmtops or even mobile phones usually comprise wireless ad-hoc networks. This brings out a concept of mobility which is a key issue in ad-hoc networks. Because to retain dynamic topology is not an easy task, and too many resources are consumed in signaling. DSR and AODV are popular protocols. We use AODV protocol for fulfill our task.

AODV[2,3] is a routing protocol mainly used for MANET and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is combination of on-demand and distance-vector routing protocol, It means that a route is established from a destination only on demand by using AODV. AODV has capability to unicasting and multicast routing .Only on requirement, a connection is established. Additionally, AODV creates trees which connect multicast group members to leaves. The sequence numbers are mainly used by AODV to ensure the freshness of routes used. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV protocol defines mainly three types of control messages for route establishment and maintenance:

RREQ- A route request message is transmitted by a node that requires a route to reach a destination. Every RREQ carries a time to live (TTL) value that indicates for how many hops this message should be forwarded. This value is set to a predefined value initially and increased at retransmissions. Retransmissions occur if no replies are received or an error occurred. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ). Every node maintains two different counters: one for a node sequence number and other for broadcast_ id. The RREQ contains the following fields

Source Address	broadcast ID	source sequence no.	Destination address	destination sequence no.	Hop Count

The pair <source address, broadcast ID> uniquely identifies a RREQ. Broadcast_id is incremented whenever the source issues a new RREQ.

RREP- A route reply message is sent back to the originator in the same direction if the receiver is either the intermediate node using the requested address, or it has a valid route to the sender address. The reason is that every route forwarding a RREQ caches a route back to the originator.

RERR- Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is found, a RERR message is sent to notify other nodes of the no availability of the link. In order to enable this reporting mechanism, each node keeps a ―precursor list", that contain the IP address for each its neighbors that are attached to each other to reach destination.

III. METHADOLOGY USED:

Algorithm Description:

The proposed work is about to prevent Black Hole attack occurs in a network when there is a communication taken place between the source and the destination. In this work a fuzzy based approach is carried out to prevent and resolve the problem of Black Hole attack. In this work each node acts as an intelligent node that keeps the information about its neighboring nodes and arrives at a decision based on statistical information of neighboring nodes. As a node start the communication it check the links available or not on each neighbor node by sending the hello message. It will check whether the neighboring nodes reply effectively or not. The basic decision taken here is on the basis of driven throughput ,packet delay and the packet loss. As the node reply, it checks out -is the response time is greater than its estimated response time? If it so then it will exclude that particular node from the list. There also exists some diagnostic algorithm to transfer the data with true decision making. The complete process is repeated node by node till the destination node is not achieved.

Algorithm **:**

The algorithm of the presented work is given as under:-

1.Define the Network with N Nodes with dynamic topology and communication parameters.
2.Define the Source Node Si and Destination Node Di.
3.Generate the route between Si and Di respective
To AODV protocol. Let the path is Si,N1,N2,N3…..Nn, Di
4.For i=1 to n
[Repeat Steps 5 to 10]
5.NList=FindNeighbour(i)
6.for j-1 to Length(NList)
{
7. Paramter1=Throughput (j)
Paramter2=Packet Delay(j)
Parameter3=Packet Loss(j)
8 .FuzziFy the Parameters
9. If **(**High(Parameter1) and Low(Parameter2) and median(Parameter3))
{
No black hole node exists
Set NList(i) as Next Communicating Node
}
Elseif(High(Parameter1) and median(Parameter2) and low(Parameter3))
{
No black hole node exists
Set NList(i) as Next Communicating Node
}
Elseif(low(Parameter1) and high(Parameter2) and median(Parameter3))
{
Set NList(i) as Black hole node pointed in red color
Derive to find out other path to reach from source to
destination
}
Else(low(Parameter1) and median(Parameter2) and high(Parameter3))
{
Set NList(i) as Black hole node pointed in red color
Derive to find out other path to reach from source to
Destination
}
}
10. Move to Next Node
11. End.

IV. CONCLUSION AND FUTURE WORK**:**

Conclusion:

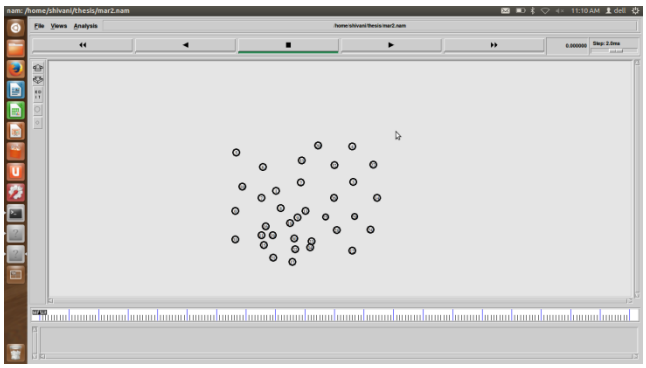
The proposed work is about the detection of Black Hole attack. The main objective of this proposed algorithm is to improve the AODV protocol related to security issues. As in case of multicast network or broadcast network, the network suffer from some attack during communication that results the packet loss over the network. The proposed work is about to minimize the packet loss and packet delay over the network. The work will increase the throughput with this improved AODV protocol algorithm The work is implemented in a wireless network using AODV protocol by using a fuzzy based approach system to provide the network security by detection Black Hole attack. For this we try to find out a new algorithm which stands out fully on proposed task. The implementation is performed in ns2 simulator and analysis is represented using xgraph. 7 parameters output are shown: Generated_packets,received_packets,packet_loss, packet_delievery ratio,average_throughput,route_overhead and packet_delay.The output is shown on the basis of these parameters by applying on 15,25,30,35 number of nodes. .The comparison is done between existing algorithm and proposed algorithm on the same number of nodes. The following simulation results show that our proposed work will increase the overall network throughput and minimize the delay and loss of packets in the network as comparison to existing methodology in fuzzy logic.

Parameter	**Value**
Number of Nodes	35
Topography Dimension	1000 x1000
Traffic Type	CBR
Propagation Model	Ground Model

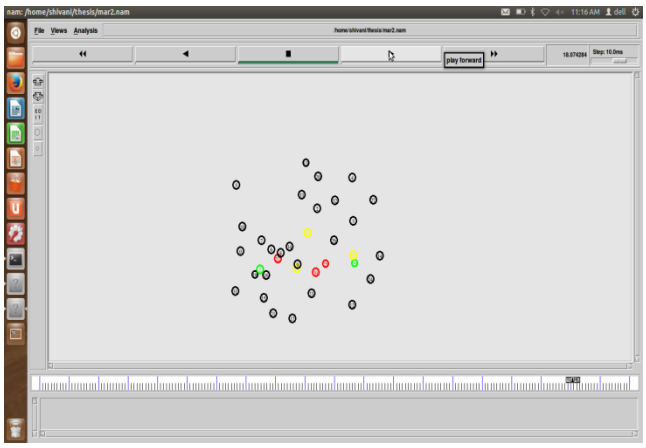
Packet Size	512 bytes
MAC Type	802.11.Mac Layer
Antenna Type	Omni directional
Protocol	AODV

Presented Scenario:

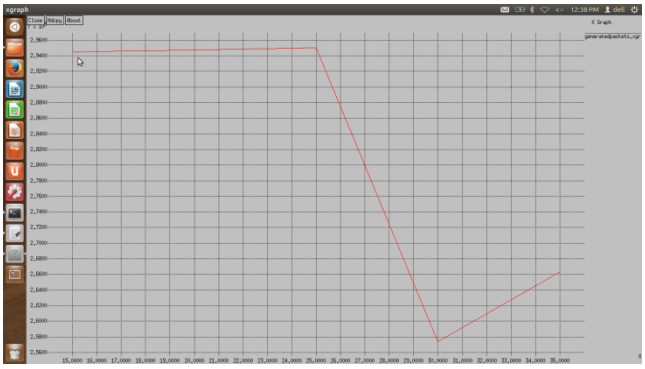
This is the initial representation of our presented application. This scenario consists 35 nodes that are distributed randomly in a work area of 1000x1000.



Below Figure is showing the black hole node which are pointed out in red color that may affect network badly. These nodes do not allow to pass data through it. A node with less forwarding ratio is presented as a bad node. Green nodes show source and destination while yellow nodes indicate intermediate nodes which help to reach data from source to destination. Whenever a black hole node exists in the midway, another path is chosen.

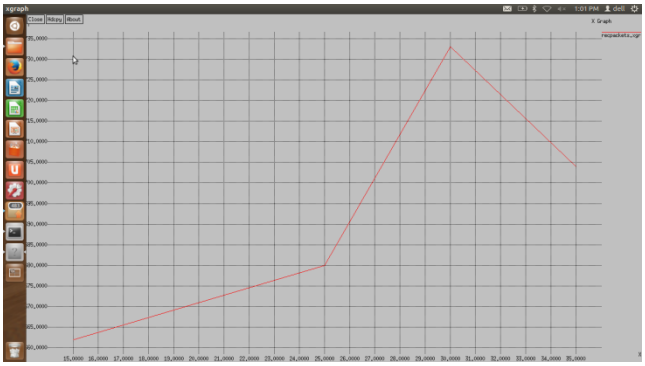


Generated packets:



From above diagram we can see easily that number of packets generated high when we try to simulate it on 15 nodes. The graph begins to decline at 20 to25, but from 25 to 35 number of packets generated begins to increases.

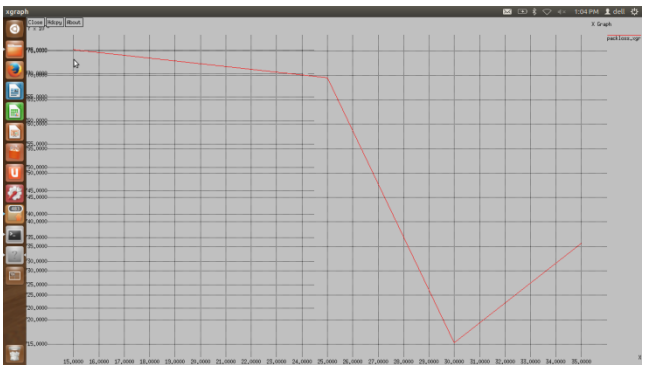
Received packets:



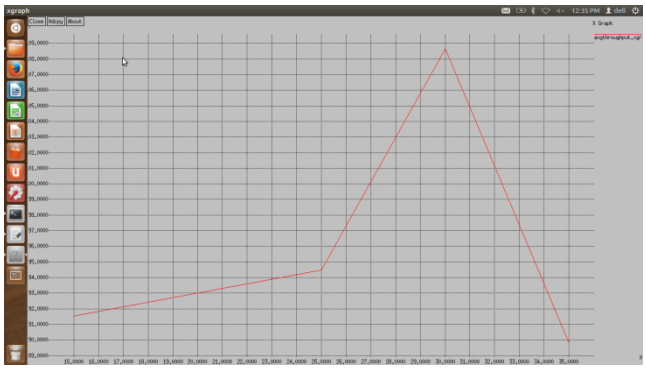
From above diagram we can see easily that number of packets received high when we try to simulate it on 30 nodes. The graph begins to decline from 25 to 35.

Packet loss:

From above diagram we can see easily that number of packets loss is maximum at 15 while minimum at 30.and slightly increases from number of nodes to 30 to 35.



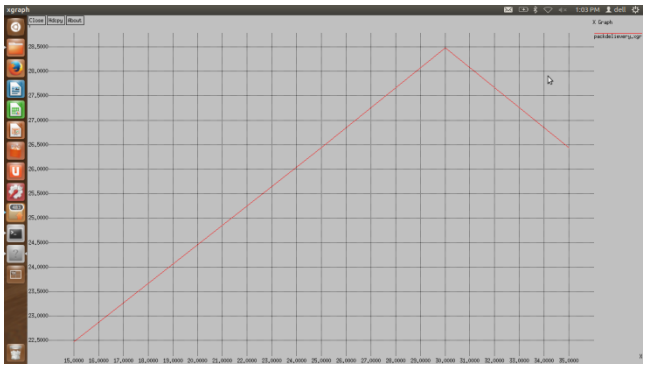
Average throughput:



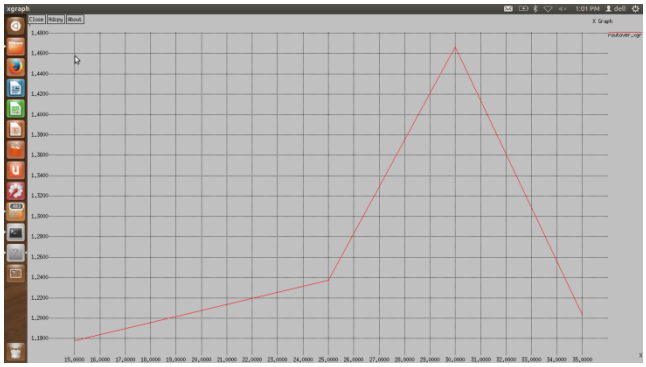
The average throughput at different number of nodes is shown in above diagram. Throughput first increases then decreases.

Packet_Delievery_ratio:

The below figure shows the packet delivery ratio calculated at different number of nodes by using same proposed algorithm.

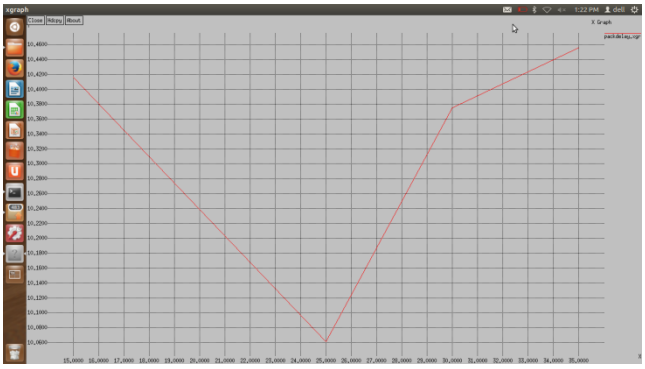


Route overhead:



Above figure tells us the calculated value of route overhead at different number of nodes using similar type of proposed mechanism.

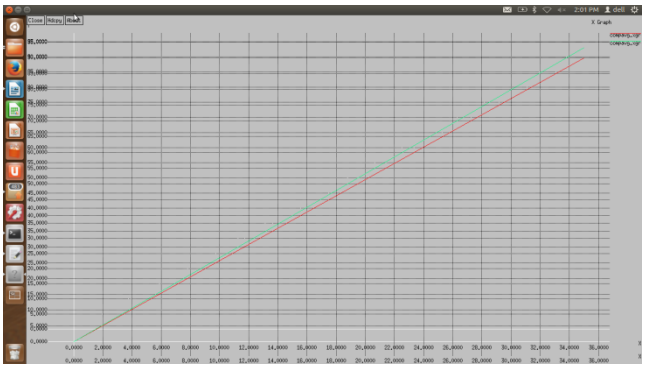
Packet delay ratio:



This figure shows the packet delay ratio of the proposed algorithm on various number of nodes.the delay ratio is analysed low on value 20.

Average throughput value (existing algorithm

Vs proposed algorithm):



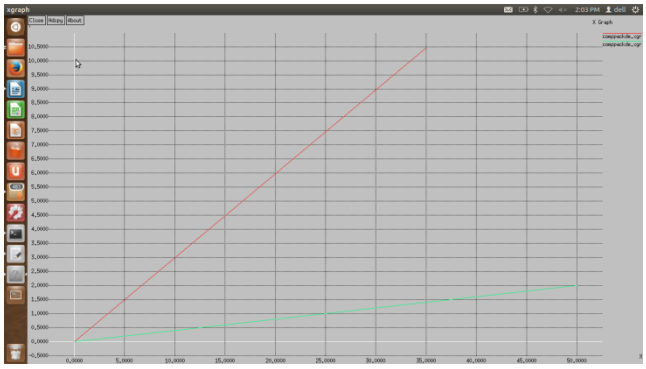
Indicates proposed work

Indicates existing work

Average throughput value of proposed algorithm is better than the existing algorithm.

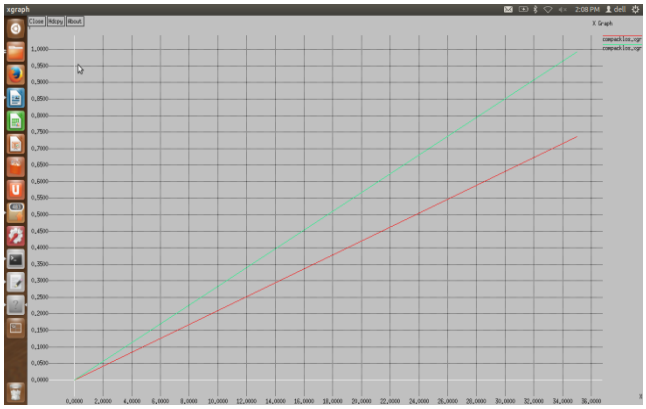
Packet_delay (existing vs proposed):

The comparative analysis of packet delay over the network is shown in above figure. Here similarly, x axis represents the time and y axis represents the packet delay during communication. The comparative analysis of packet delay over the network is shown in above figure. Here similarly, x axis represents the time and y axis represents the packet delay during communication. After implementing the proposed method, we can see the packet delay during communication over the network is decreased.



Packet_loss ((existing vs proposed):

The packet loss over the network is also decreased after implementing the proposed approach .here green line shows existing and red line shows proposed algo.



Future scope:

The proposed work can be enhanced by other researchers in the future in the following manners:

- As we try to resolve black hole problem by using AODV protocol. The work can be implemented and analyzed by other protocols.
- We try to prevent only Black Hole attack; the work can be enhanced by others to implement this in some other attack such as worm hole, flooding attacks, DOS etc.
- We have presented the work with a fuzzy decision approach in a wireless network. The work can be implemented on some specific network such as PAN, WiMax etc.

REFERENCES

[1]Pei Tingrui," An Improved Hierarchical AODV Routing Protocol for Hybrid Wireless Mesh Network", 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing 978-0-7695-3610-1/09 © 2009 IEEE

[2]Gowrishankar.S, SubirKumarSarkar," Performance Analysis of AODV, AODVUU, AOMDV and RAODV over IEEE 802.15.4 in Wireless Sensor Networks", 978-1-4244-4520-2/09©2009 IEEE

[3]LIU Jian," An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks", 2009 Fifth International Conference on Information Assurance and Security 978-0-7695-3744-3/09© 2009 IEEE

[4]Sanjay Keer," To Prevent Black hole Attacks Using Wireless Protocol in MANET", Int'l Conf. on Computer & Communication Technology 978-1-4244-9034-/10©2010

[5]Yih-Chun Hu," Black hole Attacks in Wireless Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS 0733-8716© 2006 IEEE

[6] Farid Na¨ıt-Abdesselam,"Detecting and Avoiding Black hole Attacks in Optimized Link State Routing Protocol", WCNC 20071525-3511/07©2007 IEEE

[7] Xia Wang," An End-to-end Detection of Black hole Attack in Wireless Ad-hoc Networks", 31st Annual International Computer Software and Applications Conference(C0MPSAC 2007) 0-7695-2870-8107@2007 IEEE

[8]C.Siva Ram Murthy and B.S.Manoj. "Ad Hoc Wireless Networks Architectures and Protocols." PRENTICE HALL, 2004.

[9]Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. "A review of routing protocols for mobile ad hoc networks". Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.

[10] Security issues, challenges & solution in MANET Dept. of EC, RGGI (Meerut), India

