Performance Analysis of Routing Protocols (ADSDV, OLSR and TORA) in Wireless Network

Sarbjeet Kaur[1] Akhilesh Bhardwaj[2]
[2]Assistant Professor
[1,2]Department of Computer Science Engineering
[1,2]SKIET Kurukshetra University, Kurukshetra, Haryana, India

Abstract— In routing process a node i.e. source transmit the data packets to another node i.e. destination. Routing in wireless networks have great challenges due to mobility, limited transmission range, There are several familiar routing protocols like DSDV, AODV, DSR, etc. which have been proposed for providing communication among all the nodes in the network. This paper presents a performance comparison of proactive and reactive protocols ADSDV, OLSR and TORA based on metrics such as throughput, packet delivery ratio and average end-to-end delay by using the NS-2 simulator.

Key words: WMN, Hybrid Wireless Mesh Network, Black Hole Attack, NS2

I. INTRODUCTION

A wireless mesh network (WMN) is an integration result of multi-hop communication and wireless local area networks (LANs) technology. Wireless Mesh Networks (WMN) is a new distributed broadband access network. Compared with the typical mobile Ad hoc network, it is with less mobility and usually not powered by the battery. This feature brings many advantages to WMN, such as low up-front cost, easy network maintenance, robustness, and reliable service coverage.

WMN has three layers, in which the lowest layer is "STA layer" including user devices, such as Mobile phone, portable computer and PDA etc. "STA layer" is also called "Access network". The layer above "STA layer" is "Mesh layer", which consists of Mesh Access Point (MAP) and Mesh Point (MP). MAP and MP have minimal mobility and form the backbone of WMN. They provide network access for both mesh station and conventional simple station. The third layer is called "Core Network", which provides users all kinds of Internet services via interconnection with different kinds of networks.

Wireless Mesh Networks (WMN) is a new distributed broadband access network. Compared with the mobile Ad hoc network, it is with less mobility and usually not powered by the battery. Therefore, the traditional mobile Ad hoc routing protocols are no longer suitable for WMN. In order to meet the performance requirements of multimedia traffic transmission, the routing protocol designed for WMN must take into account the load balance, fault tolerant and throughput, etc.

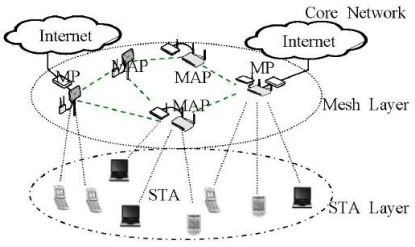

Fig. 1: Wireless Mesh Network Architecture

II. HYBRID WIRELESS MESH NETWORK

Wireless Mesh Networks (WMNs) are ever increasingly finding their way into modern society. This appreciation is owed primarily to their self-organizing, self-configuring and self-healing capabilities. A WMN consists of two major components, the Mesh Router and the Mesh Client. Mesh Routers are static, high powered devices that form the structure of the WMN, often consisting of multiple radios. Mesh Clients are generally single radio communication devices that can either be mobile or stationary. Hence, a static WMN and a mobile WMN combined to form a hybrid WMN, which provides a holistic framework where both Mesh Routers and Mesh Clients are actively involved in the routing and forwarding of data packets.

In order to guarantee that the paths established in hybrid WMNs offer optimum performance, the design of routing protocols must take into account the particular characteristics unique to hybrid WMNs. Characteristics that require attention by routing protocols include;

(1) Optimal use of multiple radios;
(2) Intra-flow and inter-flow interference; and
(3) Sudden changes in topology due to node mobility.

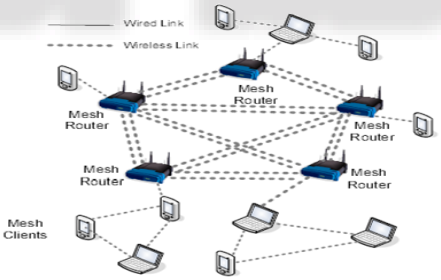

Fig. 2: Hybrid Wireless Mesh network

III. CLASSIFICATION OF ATTACKS

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can develop the network either as internal, external or/ as well as active or passive attack against the network.

A. External and Internal Attack

External attacks, in which the attacker aims to cause congestion, spread false routing information or disturb nodes from providing services. These attacks usually aim to cause network congestion, deny access to specific network function or to interrupt the whole network operations. External attackers are mainly outside the networks who want to get access to the network, once they get access to

the network they start sending fake packets, denial of service in order to interrupt the performance of the whole network. These attacks can be barred by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated.

In internal attack the attacker wants to have usual access to the network as well as contribute in the normal activities of the network. Internal attack is more strict attacks then external attacks. Internal attacks, in which the challenger wants to gain the normal access to the network and contribute the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a existing node and using it as a basis to conduct its malicious behaviors. Internal nodes might misbehave to save their limited resources, such as the battery powers, the processing capabilities, and the communication bandwidth. Attacks that are caused by the misbehaving internal nodes are hard to detect because to distinguish between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

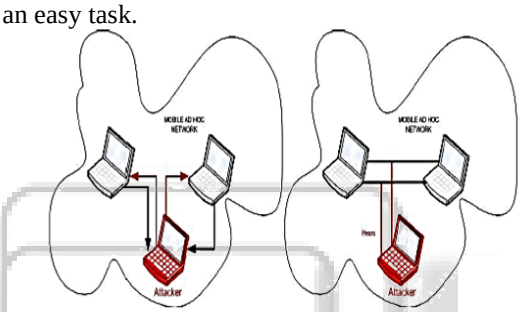

Fig. 3: External And Internal Attack

B. Active and Passive Attacks

In active attack the attacker disrupt the performance of the network, steal important information and try to destroy the data during the exchange in the network. Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of the network in such case the active attack act as an internal node in the network. Being an active part of the network it is easy for the node to make use of and takeover any internal node to use it to introduce false packets injection or denial of service. This attack brings the 18 attacker in strong position where attacker can modify, make and replays the massages. Attackers in passive attacks do not interrupt the normal operations of the network.

In Passive attack, it listens to the network in order to know and understand how they are located in the network, how the nodes are communicating with each other. Before the attacker start an attack against the network, the attacker has enough information about the network that it can easily capture and introduce attack in the network.

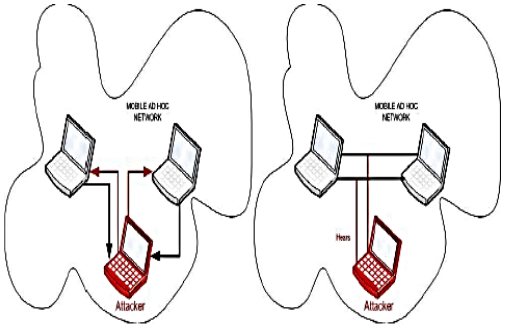

Fig. 4: Active And Passive Attack

IV. NETWORK LAYER THREATS

A. Gray Hole Attack

Every node maintain a routing table that stores the next hop node information for a route a packet to destination node, when a source node want to route a packet to the destination node , it uses a specific route if such a route is available in it's routing table. otherwise , nodes initiates a route discovery process by broadcasting Route Request (RREQ) message to it's neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination.

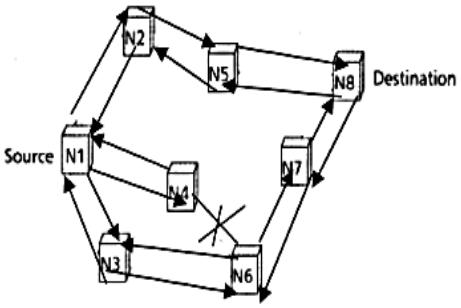

Fig. 5: Basic Idea about the Gray hole attack

The gray hole attack has two phases , In first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interrupting or corrupting packets, event though route is spurious. In second phase, nodes drops the interrupted packets with a certain probability. Detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack.

B. Black Hole Attack

In this type of attack, a malicious node falsely advertises good path (e.g., shortest path or most stable path) to the destination node during the path finding process. The intension of the malicious nodes could be to hinder the path finding process or to interrupt all the data packets being sent to the concerned destination node. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it .

In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

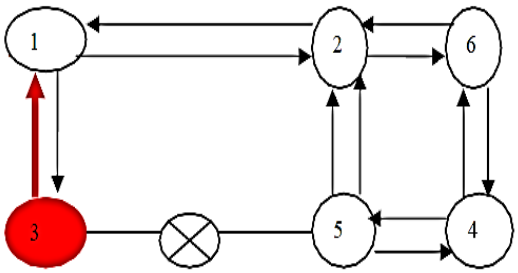

Fig. 6: Basic Idea about the Black hole attack

V. Related Work

QiangShen, Xuming Fang, Ying Shan[1] proposed An Integrated MetricsBased Extended Dynamic Source Routing Protocol for Wireless Mesh Networks. Wireless Mesh Networks (WMN) is a new distributed broadband access network. Compared with the mobile Ad hoc network, it is with less mobility and usually not powered by the battery. Therefore, the traditional mobile Ad hoc routing protocols are no longer suitable for WMN. In order to meet the performance requirements of multimedia traffic transmission, the routing protocol designed for WMN must take into account the load balance, fault tolerant and throughput, etc. This paper firstly introduces typical structures and characteristics of WMN, and several relevant WMN routing protocols. Then a method of integrated metrics based Extended Dynamic Source Routing (EDSR) protocol is proposed. The analysis and simulation results show that the proposed EDSR protocol improves the throughput of WMN significantly, which reaches the target of load balance simultaneously.

Bhavyesh Divecha, Ajith Abraham, Crina Grosan And Sugata Sanyal [2]Analyzed Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models. A Mobile Ad-Hoc Network (MANET) is self-configuring network of mobile nodes connected by wireless links to form an arbitrary topology without the use of existing infrastructure. In this paper, the effects of various mobility models on the performance of two routing protocols Dynamic Source Routing (DSR-Reactive Protocol) and Destination-Sequenced Distance-Vector (DSDV-Proactive Protocol). For experiment purposes, they have considered four mobility scenarios: Random Wayward Mobility, Group Mobility, Freeway and Manhattan models. These four Mobility Models are selected to represent the possibility of practical application in future. Performance comparison has also been conducted across varying node densities and number of hops. Experiment results illustrate that performance of the routing protocol varies across different mobility models, node densities and length of data paths.

Saad Khan, Asad Amir Pirzada And Marius Portmann[3] Analyzed an Comparison of Reactive Routing Protocols for Hybrid Wireless Mesh Networks. Wireless mesh networks have recently gained a lot of popularity due to their rapid deployment and instant communication capabilities. These networks comprise of somewhat static multi-radio Mesh Routers, which essentially provide connectivity between the mobile single-radio Mesh Clients. Special routing protocols are employed, which facilitate routing between the Mesh Routers as well as between the Mesh Routers and the Mobile Clients. AODV is a well known routing protocol that can discover routes on-the-fly in a mobile environment. The protocol is highly scalable and can support thousands of nodes making it an ideal protocol for wireless mesh networks. However, as the protocol was actually developed for single-radio nodes, it frequently lacks the ability to exploit the potential offered by the Mesh Routers and, hence, sub-optimal routing takes place in a mesh environment. This paper gives an overview of four variants of the AODV routing protocol that can potentially be used for mesh formation. In order to determine their aptness for application to hybrid wireless mesh networks, this paper presents their characteristics and functionality, and then provides a comparison and discussion of their respective merits and drawbacks.

YouitiKado, Azman Osman Lim, and Bing Zhang [4] analyzed an Of Wireless Mesh Network Routing Protocol For Push-to-Talk Traffic. Wireless mesh networks (WMNs) are becoming well-known as a new broadband Internet access technology through multihop transmission nowadays. With the tremendous popularity of the group communication, such as Push-to-Talk service, the need to deliver the traffic of Push-to-Talk over WMNs is becoming important. Since the Push-to-Talk traffic over WMNs is delay-sensitive traffic, a proactive routing protocol that keeps routes continuously updated is ideally best-suited protocol. Among the proactive routing protocols, a tree-based routing (TBR) protocol is a viable routing protocol for WMNs because traffic that is directed to/from a wired network can be well-handled via a portal (a root). However, the performance of TBR protocol can be degraded rapidly when the number of group talking increases, which also leads to the intra-mesh traffics increases in the network. To mitigate this problem, they proposed a centralized tree-based routing protocol, which enables the root to provide the best metric route for intra-mesh traffics. In other words, the proposed protocol can disperse the intra-mesh traffics around the root when an overwhelming traffic volume occurred. Their simulation studies reveal that the proposed protocol outperforms both AODV and TBR protocols in terms of packet delivery ratio, average end-to-end delay, and data throughput as the number of active users becomes larger.

VI. Purposed Work

This paper compare the three routing protocols ADSDV, OLSR and TORA which are reactive, proactive and hybrid routing protocol respectively in nature. Previously the works done on MANETs focused mainly on different security threats and attacks such as DoS, DDoS, and Impersonation, Wormhole, Jellyfish, and Black Hole attack. Among these attacks Black Hole attack involved in MANET is evaluated based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using Reactive, Proactive and Hybrid Protocols and to compare the vulnerability of both these protocols against the attack.

A. Simulation Parameters:

The communication pattern randomly created by the set dest tool defined in ns2 simulator. The tool contains following arguments. The Simulation Parameters which are used in my thesis work are shown in table 1.

Parameter	Value
Simulation Time	50 Sec
No. of Nodes	50
No. of Receivers	50
Traffic Type	CBR
Pause Time	10 Sec
Maximum X-coordinate value	1000 M
Maximum Y-Coordinate value	1000 M
Packet Size	512 byte
MAC Protocol	802.11
Mobility Model	Random Waypoint
Routing Protocols	ADSDV,OLSR,TORA
Observation Parameters	EED, Throughput, PDF

Table 1: Simulation Parameters

VII. Evaluation Of Simulation

A. LFD & GFD Technique

This technique uses two detector nodes:

(1) Local Fault Detector (LFD) (shown by blue color):- This node perform two steps
  (1) Perform Init(Initializing nodes in a network).
  (2) Send Packet information to GFD.
(2) Global Fault Detector(GFD) (shown by green color) :- GFD checks which node is malicious node in network and block that node.

In first case we have represent the network that contains the no black hole node

In the second scenario, Black Hole Node is created. Node 5 behave like Black hole Node. The first statement, "$ns node-config –adhoc Routing blackhole ADSDV" is to add the Black hole behavior to the nodes created from this point.

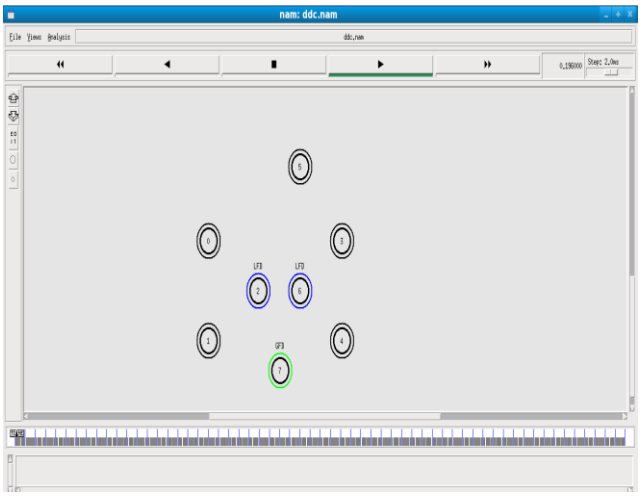

Fig. 7: No malicious node is present

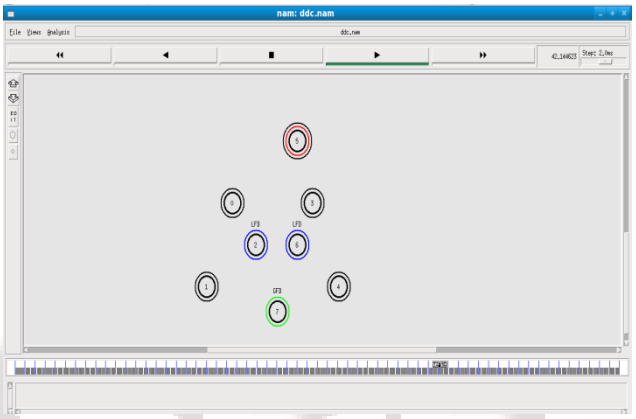

Fig. 8: Malicious node is present

B. Comparison between ADSDV, OLSR, TORA When Malicious node is present on the basis of Performance Parameter

For the purpose of proving our proposed algorithm better than other routing protocols, we have used some of the metrics i.e Packet Delivery Ratio, Average end-to end delay and Normalized Routing Load and comparison of our proposed algorithm is with ADSDV routing protocol. The metrics are as follows:

(1) Packet Delivery Ratio
(2) Average End-to-End Delay
(3) Throughput

1) Packet Delivery Ratio:

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source. It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ration, the more complete and correct the routing protocol. It is the ratio of the packets received by destination to those generated by the sources. CBR traffic type is used by source. This reflects the usefulness of the protocol. And provide good performance.

Packet Delivery Ratio = (Received Packets/Sent Packets)

Comparing the packet delivery ratio of routing protocol ADSDV, OLSR and TORA with the effect of Black hole attack:

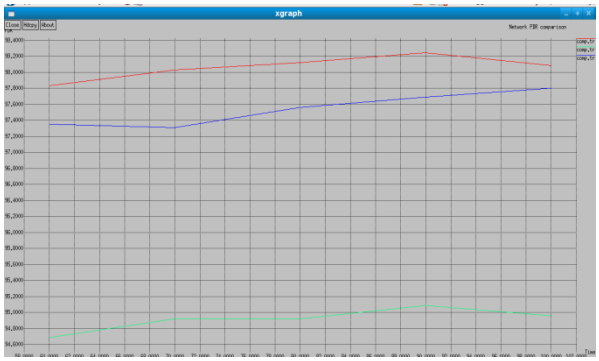

Fig. 8: ADSDV>OLSR>TORA

Figure 8 shows the PDR of the three protocols ADSDV, TORA and OLSR with attack. The PDR of ADSDV is greater than OLSR and TORA. With high mobility all three of protocols behave same but with less mobility ADSDV has maximum PDR, OLSR lies in between ADSDV and TORA. TORA has minimum PDR. Higher the PDR as good the routing protocol performed. In case of black hole attack PDR of these protocols decreases due to the present of malicious node present in the network.

2) Average End-to-End Delay

Average end-to-end delay is the average time it takes a data packet to reach to destination in seconds. It is calculated by subtracting "time at which first packet was transmitted by source" from "time at which first data packet arrived to destination. It includes all possible delays caused by buffering during latency, queuing at the interface queue, retransmission delays at MAC, Propagation and transfer times. It is the metric significant in understanding the delay introduced by path discovery.

Comparing the End-to-End Delay of routing protocol ADSDV, OLSR and TORA with effect of Black hole attack.

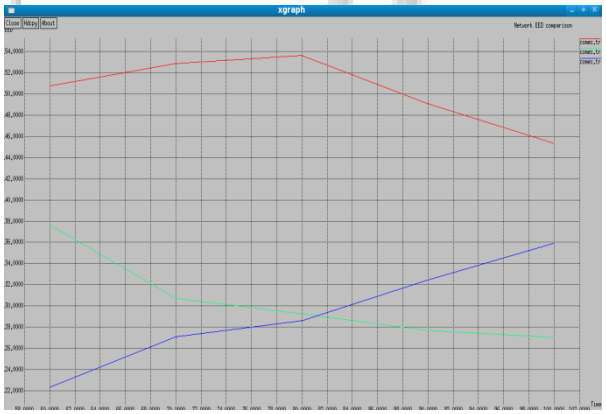

Fig. 9: ADSDV>OLSR>TORA

The graph illustrate higher delay when there is a malicious node present in the network. Due to the present of malicious node, it consumes the packets transferred between source and destination, the end-to-end delay increases. The end-to-end packet delay included the delay for the route discovery if necessary. In this figure, TORA exhibited the lowest average end-to-end delay, while ADSDV had the highest delay in case of with attack. TORA had lowest average end-to-end delay because it did not need to rediscover the route for the same destination by maintaining the route entry in the routing table.

3) Throughput

It is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds. Throughput may be affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

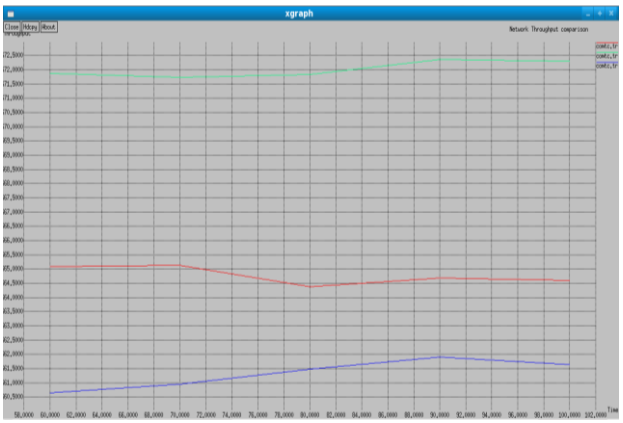

Fig. 10: TORA>ADSDV>OLSR

Fig 10 shows the throughput for ADSDV, OLSR and TORA with black hole attack. OLSR in case of no attack (no malicious node present) is higher than the throughput of OLSR under attack (in the presence of malicious node). This is because of the less routing forwarding and routing traffic. Here the malicious node rejects the data rather than forwarding it to the destination, thus effecting throughput.

VIII. CONCLUSION

In this Paper, I have analyzed the behavior and different performance matrices for WMS s using different protocols (ADSDV, OLSR and TORA) and compared their performance matrices, like End to end delay, Packet delivery Fraction and Throughput with black hole attack. In performance comparisons of routing protocols ADSDV, OLSR, TORA with and without black hole attack respectively are shown using ns2 simulator. For Throughput and PDF, AODV behaving the best and for End to End delay is concern TORA is taking less delay.

REFERENCES

[1] A Survey of Cooperative Black and Gray Hole Attack in Manet , B.Revathi & D.Geetha , Vol 1 Issue 2 September 2012.
[2] A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET, Vol.2 , 2011, 2607-3613.
[3] Dong-Won Kum, Jin-Su Park, You-Ze Cho , Byoung-Yoon Cheon, and Daejea Cho, "Mobility-aware Hybrid Routing Approach for Wireless Mesh Networks" { 978-0-7695-4092-4/10 $26.00 © 2010 IEEE }.
[4] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing".
[5] Mobility-aware Hybrid routing approach for Wireless Mesh Network, Dong-Won Kum , Jin-Su Park, You-

Ze Cho , Byoung-Yoon Cheon and Daejea Cho{978-0-7695-4092-4/10$26.00 © 2010 IEEE}.

[6] Prof. Sanjeev sharma, Rajshree, Ravi Prakash Pandey and Vivek Shukla, "Bluff-Probe Based Black Hole Node Detection and prevention"{ 2009 IEEE International Advance Computing Conference IACC 2009 }.

[7] Miguel Elias M. Campista, Luis Henrique M.K Costa , and Otto Carlos M.B. Duarte "WPR:A Proactive Routing Protocol Trailored to Wireless Mesh Network"{978-1-4244-2324-8/08/$25.00 © 2008 IEEE}.

[8] Bhavyesh Divecha, Ajith Abraham, Crina Grosan And Sugata Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models"{0-7695-2845-7/07 © 2007 IEEE}.

[9] Saad Khan, Asad Amir Pirzada And Marius Portmann, "Analysis of Comparison of Reactive Routing Protocols for Hybrid Wireless Mesh Networks"{ 0-7695-2842-2/07 © 2007 IEEE}.

[10] BhavyeshDivecha, Ajith Abraham, CrinaGrosan And SugataSanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models"{0-7695-2845-7/07 © 2007 IEEE}

[11] Muhammad ShoaibSiddiqui, Syed Obaid Amin, Jin Ho Kim, ChoongSeon Hong, "MHRP: A SECURE MULTI-PATH HYBRID ROUTING PROTOCOL FOR WIRELESS MESH NETWORK" { 1-4244-1513-06/07/$25.00 ©2007 IEEE }

[12] Asad AmirPirzada, Ryan Wishart and Marius Portmann, "anCongestion-Aware Routing In Hybrid Wireless Mesh Network "{ 1-4244-1230-7/07/© 2007 IEEE}

[13] Jing Xie, Luis Gironés Quesada and Yuming Jiang, "A Threshold-based Hybrid Routing Protocol for MANET" { 1-4244-0979-9/07/© 2007 IEEE}

[14] YouitiKado, Azman Osman Lim, and Bing Zhang, "Analysis Of Wireless Mesh Network Routing Protocol For Push-to-Talk Traffic "{ 1-4244-1251-X/07/©2007 IEEE.}

[15] QiangShen, Xuming Fang and Ying Shan, "proposed An Integrated Metrics Based Extended Dynamic Source Routing Protocol for Wireless Mesh Networks." {0-7803-9584-0/06/ (2006 IEEE.)}

