Volume: 6 Issue: 3 Pages: 2352-2358 (2014) ISSN : 0975-0290

Performance Comparison of Cluster based and Threshold based Algorithms for Detection and Prevention of Cooperative Black Hole Attack in MANETs

P. S. Hiremath
Department of Computer Science, Gulbarga University, Gulbarga
Email: Hiremathps53@yahoo.com

Anuradha T.
Department of Computer Science and Engineering,
P.D.A College of Engineering, Gulbarga.
Email: anuradhat26@gmail.com

----------ABSTRACT----------

In mobile ad-hoc networks (MANET), the movement of the nodes may quickly change the networks topology resulting in the increase of the overhead message in topology maintenance. The nodes communicate with each other by exchanging the hello packet and constructing the neighbor list at each node. MANET is vulnerable to attacks such as black hole attack, gray hole attack, worm hole attack and sybil attack. A black hole attack makes a serious impact on routing, packet delivery ratio, throughput, and end to end delay of packets. In this paper, the performance comparison of clustering based and threshold based algorithms for detection and prevention of cooperative in MANETs is examined. In this study every node is monitored by its own cluster head (CH), while server (SV) monitors the entire network by channel overhearing method. Server computes the trust value based on sent and receive count of packets of the receiver node. It is implemented using AODV routing protocol in the NS2 simulations. The results are obtained by comparing the performance of clustering based and threshold based methods by varying the concentration of black hole nodes and are analyzed in terms of throughput, packet delivery ratio. The results demonstrate that the threshold based method outperforms the clustering based method in terms of throughput, packet delivery ratio and end to end delay.

Keywords - **Mobile ad-hoc network, attacks in routing protocol, cooperative black hole attack, AODV routing protocol, clustering, server, cluster head, trust value.**

Date of Submission: October 08, 2014 Date of Acceptance: November 03, 2014

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have received increasing attention of the researchers in recent years due to their mobility feature and ease of deployment. MANET is a collection of independent wireless mobile nodes. MANET doesn't need any centralized management and so it is very vulnerable to attacks Each node can move freely in space. Therefore, the topology of network changes rapidly due to its mobility nature. Node can act as a router or as a host. Accordingly, an untrusted node can join the network to perform certain malicious actions that negatively affect the network performance. In MANETs, routing protocols are designed to guarantee efficient packet routing. Routing protocols can be classified into reactive, proactive and hybrid. Proactive protocols are called table-driven protocols. Reactive protocols are on demand protocols, e.g. Ad-hoc On-demand Distance Vector (AODV).Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disaster. The presence of dynamic and adaptive routing protocols enables ad-hoc networks to be deployed quickly.

Security is one crucial requirement for these network services. Implementing security [1] [2] is therefore of prime importance in such networks. Provisioning protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to disrupt network security, is a primary concern. If a node misbehaves, it should be removed from the network and cut off from all activities immediately. In the present research, the focus is on fundamental security problem of eliminating black hole attack and methods for detection and prevention of cooperative black hole attack in MANETs. In clustering based approach, for secure routing among different clusters of same MANETs, a node is designated as the CH (cluster head) in order to monitor

Volume: 6 Issue: 3 Pages: 2352-2358 (2014) ISSN : 0975-0290

each node's activity in its cluster during data transmission. Finally, the server (SV) that monitors the entire network calculates trust value of each node in the network and also checks all node's activity. It declares black hole node by channel overhearing method. Hence detected black hole node is listed in the black hole list[ ] and then server broadcasts a packet to all the nodes in the network. Attacks on mobile ad hoc networks can be classified into following two categories. A passive attack does not disrupt proper operation of the network [1] whereas the active attacks tries to destroy the data. Hence, there won't be the normal operation. These attacks can be classified into two categories, namely, external attacks and internal attacks. External attacks are supported by nodes that do not belong to the network. Internal attacks are due to nodes within the network or they are part of the network. Black hole and wormhole is categorized as active internal attack. In this paper, introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper.

BLACK HOLE ATTACK

Black hole attack is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming it has a shortest path or fresh route with it, and does not participate in forwarding the packets to next node and also to destination[2]. Black hole attack can cause error in routing information, or reply to node with wrong routing information. It is responsible for loop creation which can lead towards congestion in the network [3]. For instance, in Fig. 1 source node N1 wants to send data packet to destination node and initiates the route discovery process. Additionally, assume that node N3 is a malicious node, which claims that it has a route to the destination. Whenever it receives route request packets (RREQ), it immediately sends the response to node N1. In case the response from the node N3 reaches to node N1 the earliest, the node N1 thinks that the route discovery is finished. Further, source node N1 ignores all other replies and begins to send data packets to node N3. Finally, all packets through N3 are absorbed or lost, and thus N3 becomes a black hole.

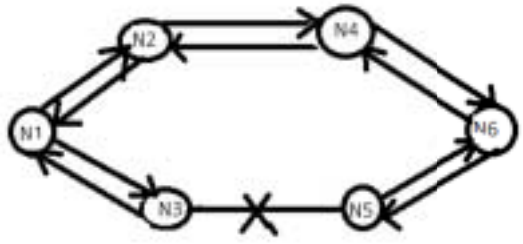

Fig.1. Black hole attack

A cooperative black hole attack is defined as an attack where there are more than one black hole nodes that collectively collaborate in the network and cause performance degradation of the network [6].

The rest of the paper is organized as follows: Clustering approach is presented in Section II. Related work is presented in Section III. Proposed work is presented in Section IV. In Section V simulation results are presented and discussed. Finally, Section VI contains the conclusions.

CLUSTER APPROACH

A MANET can be divided into several overlapped clusters. The nodes in a MANET are classified into cluster head node and cluster member node. The cluster head CH is one hop away from its cluster member. To facilitate the cluster head discovery process, a cluster member keeps the IP addresses of other cluster heads that can hear. When the former cluster head moves away or a cluster member does not receive three HELLO packets continuously from its cluster head, it considers that the wireless link between them is broken (or the cluster head has moved away). Thus, a cluster member adopts the latest refresh cluster head in its routing table as its new cluster head, which is one hop away from it, or becomes itself a cluster head if it cannot hear any existing cluster head. The selected cluster head is informed that a new cluster member has joined its group. The cluster member will obtain the confirmation of its new cluster head when it receives the HELLO packet that carries its IP address.

Message Type	Length	Reserve Word
IP		
IP (cluster member)		
IP (neighbor cluster heads)		

(a) Cluster head

Message Type	Length	Reserve Word
IP		
IP (cluster head)		
IP (cluster heads that can be heard)		

(b) Cluster member

Fig. 2. Hello message format of (a) cluster head CH and (b) cluster member

II. RELATED WORK

Recently, researchers pay much attention to MANET security issues. It is difficult to secure mobile ad hoc networks, due to vulnerability of wireless links, dynamically changing topology, and lack of infrastructure. Various kinds of algorithms for detection and prevention of a black hole attack have been proposed to enhance network security in the literature. But very less work is reported on detection and prevention of cooperative black hole attack using clustering approach. This section describes the related work of previous methodologies that are supporting our proposed work. It is observed in [4] that the trust based collaborative approach to mitigate black hole nodes is examined. In this methodology, every node

Volume: 6 Issue: 3 Pages: 2352-2358 (2014) ISSN : 0975-0290

monitors neighboring nodes and calculates trust value on its neighboring nodes. The black hole attack in wireless ad hoc networks is studied as a major issue in [5], where in two technologies for communication between server and access points and the access points to nodes are used. This leads the node to modify its routing table, so communication starts between node and server through access point. In [6], a novel approach for detection and prevention of cooperative black hole attack in a MANET, by thresholding RREP sequence number, is proposed by varying the concentration of black hole nodes. The enhancement of basic AODV routing protocol, which avoids black hole is discussed in [7]. A survey of black hole attacks in MANETs is presented in [8]. The cluster head selection is invoked on-demand, and thus it reduces the communication costs. A survey of different clustering schemas has been done in [9], which focuses on different performance metrics.

III. PROPOSED WORK

The proposed methodology is based on clustering approach for detection and prevention of cooperative black hole attack. Mobile nodes follow the law of independent mobility. These nodes are frequently taking part in communication. In addition, they are able to send, receive and route data during communication. Cluster heads(CHs) are access points which are designated nodes. The main responsibility of these nodes is to monitor the trusted nodes when intra-cluster communication occurs. When any node among its members sends and receives packet, the count of packets is monitored by CH and this information is called trust value. Also, this information is forwarded to server node (designated node). The RREQ-RREP messages of AODV routing protocol are used in real-time for route discovery. Each node exchanges hello message and construct neighbor list. Cluster formation takes place when the designated cluster head (CH) sends announcement to all the nodes in the network. The nodes, which reply that they are its cluster members, are trusted nodes with unique id assigned by the cluster head. Server checks all node's activity and declares black hole node by channel overhearing method. In this method Server(SV) listens to all channels, and observes each node's send and receive information. If any node lies, it will declare that particular node as black hole node. Black hole node receives data packets but never forwards these packets to destination. Server sends along with node id, the announcement by broadcasting to the entire network. The nodes which receive this announcement will mark the node with its id in its array blacklist[ ], Now the blacklist[ ] gets updated as and when the black hole nodes are detected, and also eliminates that node by not forwarding any more packets with that node id. Here the communication takes place between cluster head and server initially. If server is not reachable then communication takes between CH and CH and then through server, untill it reaches the destination.

Algorithm 1. Detection and prevention of cooperative black hole attack using clustering approach.

Step 1. Let N be the total number of nodes and x be the number of black hole nodes. Let blacklist [ ] be the array of size x of detected nodes. Let TV be the Boolean variable denoting the trust value (set to 0 or 1)in order to check the node's activity to monitor each node CH. CH[ ] needs to maintain a record of send and receive count of data packets at each node and it is declared as an array, SEND_COUNT = RECEIVE_COUNT = 0 (data packets). SV be the server (also checks all node's activity and declare the black hole node by channel overhearing method, where server listens to all channels . It can observe that each node send and receives information. If any node lies, it will declare the node as black hole), and CH[ ] be the array of Cluster Heads (CHs). NL be the neighbor list constructed by exchanging the hello messages from each node. Initialize the array blacklist[ ] with null values . Let S be the source node.

Step 2. Input the values of N and x.

Step 3. Randomly assign x% nodes as black hole nodes among N nodes.

Step 4. The CH sends the announcement to all the nodes in the network. Which ever nodes respond by sending the reply to it, they become its cluster members. If any node among members sends and receives packets, count is monitored by CH, and also CH forwards its member's information (sending, receiving and forwarding of data packets) to server. Every 10sec, CH will send announcement about its location. Receiving node verifies whether it has any CH_id already. If not store the current node as CH. If it has CH_id already, it computes distance of current and previous id, joins CH with less distance and leaves from previous or current CH. Joining nodes act as member's for that CH, through this intra cluster communication. Initially, CH participates in intra cluster communication.

Step 5. A cluster is denoted by C_1={M}, where M is the set of members existing in cluster C_1. Let CH_1 be the cluster head of C_1. Define the successor set of M as S and predecessor set as D. When a source node S ($S \in C_1$) seeks to set up a connection to a destination D, S sends a route request message (RREQ) to its cluster head (CH_1). The RREQ message includes the following fields (source address S, destination address D, session ID). If D is a member of cluster C_1 as well and hears the request message, then

(i) It sets up multiple paths from source node S to next hop nodes untill message reaches destination D. If all paths have been established, then it chooses the loopfree reliable paths.

Volume: 6 Issue: 3 Pages: 2352-2358 (2014) ISSN : 0975-0290

(ii) If destination node D is not in the same cluster as source S, the source node S sends a route request message (RREQ) to its cluster head CH_1. The CH_1 looks for which cluster the destination node D belongs to, and forwards the request to the next cluster head (CH_2) or server SV which has the information of all the CHs. At the same time, it sets up multiple links from source S to the destination node D.

Step 6. After route discovery phase, source node S starts sending the data packet to CH. First CH tries to communicate with the server SV (intra cluster communication). If SV is out of range, CH_1 sends RREQ to the next CH untill it reaches SV or CH which has cluster member as destination D.

Step 7. If SV receives a data packet from any of the CHs, (a SV monitors entire network and also CHs, SV has the information of each CH), SV computes the trust value (TV) of each node by checking the SEND_COUNT and RECEIVE_COUNT of the node. The intermediate node which receives a packet from the source node, checks the trust value (TV) of this node and forwards it to CH after establishment of the path, as and when data is transmitted, the Trust Value[ ] is computed based on SEND_COUNT and RECEIVE_COUNT of the receiving node as follows:

If RECEIVE_COUNT - SEND_COUNT = 0, then

TV is set to 1

else TV is set to 0.

Step 8. If TV=1 then the receiving node is not a black hole node. Forward the data packet to the next hop. Go to step 10. else (i.e. TV=0) declare the receiving node as a Black hole (it only receives the packet but, never forwards to destination as it will drop the packet). Go to step 9.

Step 9. The SV announces by broadcasting a packet with node id declared as Black hole. Then all the nodes receive this packet and update their blacklist[ ] and eliminate that node by not forwarding any more packets to it. Then go to step 7.

Step 10. Repeat steps 7 to 10 untill data packet reaches the destination.

Step11. Compute the performance metrics, namely, throughput, packet delivery ratio and end to end delay.

Step 12. The non-zero elements of blacklist [ ] are the detected black hole nodes among N nodes.

Step 13. Stop.

IV. EXPERIMENTAL RESULTS AND DISSCUSSION

The simulation experiments are conducted using NS-2.34 simulator by using the proposed algorithm. The simulation runs of 100sec, 200sec, 300sec, 400sec and 500sec are carried out and cooperative black hole attack using clustering approach is observed. The simulation parameters used in the experimentation are given in the Table 1.

Table 1.Simulation parameters and their Values.

Parameters	Value
Packet Size	1500bytes
Simulator	NS-2.34
Transmission range	250mts
Node placement	Randomly
Number of black holes	5%,10%,15%, 20% and 25% of total nodes
Simulation run time	100sec to 500sec
Number of Mobile Nodes	50 nodes
Topology	1500 * 1500 (m)
Routing Protocol	AODV
Traffic	Constant Bit Rate (CBR)

The results of simulation are presented graphically in the Figs. 3-7. The performance of the network is analyzed in terms of three metrics, namely, throughput, packet delivery ratio and end to end delay, by varying percentage of black hole nodes x% = 5, 10, 15, 20 and 25% of N = 50 total nodes.

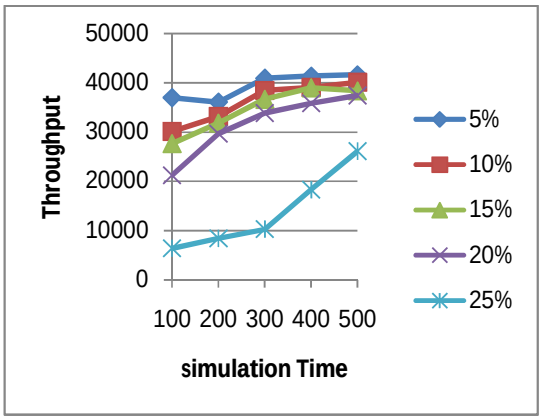

Fig. 3. Throughput for varying number of black hole nodes x=5, 10, 15, 20 and 25% of N=50 nodes: After detection and prevention of black hole attack.

Volume: 6 Issue: 3 Pages: 2352-2358 (2014) ISSN : 0975-0290

Throughput: It is the rate of successfully transmitted data packets per second in the network during the simulation. The Fig. 3 shows the throughput for varying number of black hole nodes and total number of nodes N=50, after detection and prevention of black hole attack using the proposed clustering approach. It is observed that, as the number of black hole nodes increases, throughput continues to be decreased . There is improvement in performance due to detection and prevention of black hole attack, as shown in Table 2. The throughput is increased by 26.02% by using the proposed method, in comparison with that in the presence of black hole attack with 5% of nodes as black holes. With increase in concentration of black holes, there is reduction in throughput. As concentration of black hole nodes increases, the available paths are fewer leading to further reduction in throughput.

Table 2. Comparison of throughput for MANETs in the presence of black hole attack and that after detection and prevention of the attack

Number of black hole nodes(x%)	With black hole attack	After detection and prevention	Increase in Throughput
5%	27330	36974	26.02%
10%	23301	30145	22.23%
15%	21853	27632	21.89%
20%	17741	21226	16.41%
25%	5586	6405	12.78%

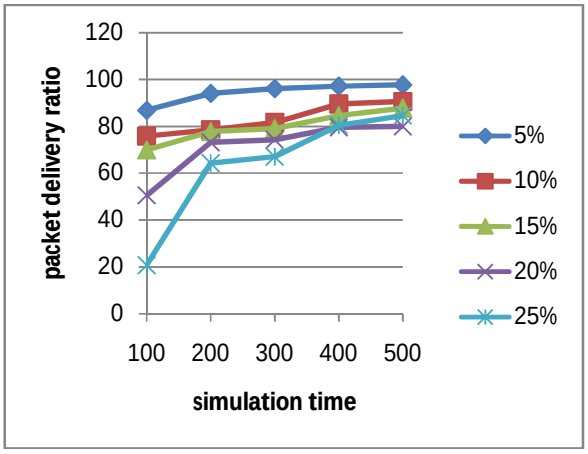

Fig. 4. Packet delivery ratio (PDR) for varying number of black hole nodes x=5,10, 15,20 and 25% of N=50 nodes: After detection and prevention of black hole attack.

Table 3. Comparison of packet delivery ratio (PDR) for MANETs in the presence of black hole attack and that after detection and prevention of the attack.

Number of black holes (x%)	With black hole attack	After detection and prevention	%Increase in PDR
5%	71.51%	86.76%	17.52%
10%	63.01%	75.89%	16.98%
15%	59.43%	69.53%	15.13%
20%	44.20%	50.81%	13.05%
25%	18.05%	20.72%	12.65%

Packet delivery ratio (PDR): It is the ratio of total number of data packets received successfully at destination to the number of data packets generated at the source. The Fig.4shows the PDR for varying number of black hole nodes x=5, 10, 15, 20and 25% of total nodes N=50, after detection and prevention of black hole nodes. There is improvement in performance due to detection and prevention of black hole nodes, as shown in the Table 3. As the concentration of black hole nodes increases, the performance degrades due to non available paths as nodes become black holes.

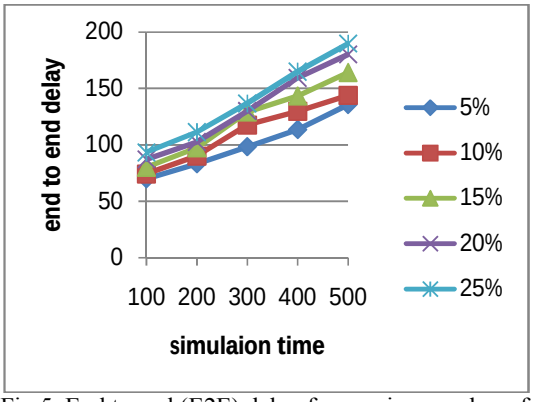

Fig.5. End to end (E2E) delay for varying number of black hole nodes x=5, 10, 15, 20and 25% of N=50 nodes: After detection and prevention of black hole attack.

Table 4. Comparison of end to end (E2E) delay for MANETs with black hole attack and after detection and prevention of the attack.

Numberof blackhole nodes (x%)	With black hole attack	After detection and prevention	Decrease in E2E delay
5%	86.452	69.921	23.64%
10%	100.768	74.233	35.74%
15%	111.254	80.180	38.75%
20%	123.278	87.100	41.53%
25%	147.198	93.434	57.54%

Volume: 6 Issue: 3 Pages: 2352-2358 (2014) ISSN : 0975-0290

End to End Delay: It is the average time interval between the generation of a packet at a source node and successful delivery of that packet at destination node. The Fig.5 shows the end to end (E2E) delay for varying number of black hole nodes x=5, 10, 15, 20 and 25% of total nodes N=50, after detection and prevention of black hole attack using the proposed clustered approach method. It is observed that there is a decrease in end to end delay due to detection and prevention of black hole attack. As the concentration of black hole nodes in the network increases, the performance degrades due to the non-availability of paths for data transmission, as shown in Table 4.

The Figs. 6-8 depict the performance comparison of proposed method based on clustering approach with that based on non-clustering approach [6] in terms of throughput, PDR and E2E delay, respectively. The numerical results of the two methods are compared in Table 5. It is observed that, in general, the clustering approach leads to network performance degradation and hence, is not desirable. The plausible reason for this network degradation in cluster based approach is the increase in computational overhead in data communication due to maintainance of cluster heads.

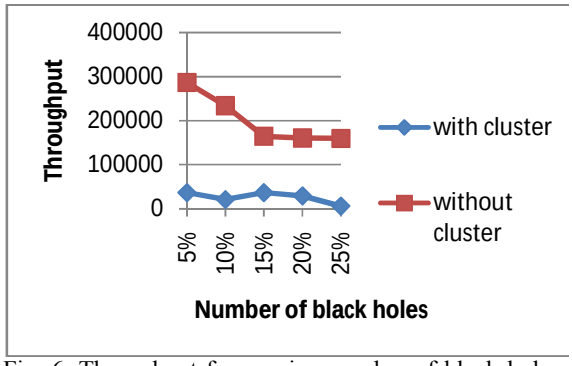

Fig. 6. Throughput for varying number of black hole nodes x=5,10,15,20 and 25% of N=50 nodes: Comparison of cluster approach and without cluster approach, after detection and prevention of black hole attack.

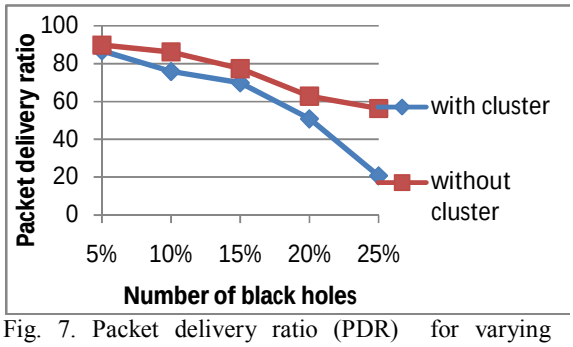

Fig. 7. Packet delivery ratio (PDR) for varying number of black hole nodes x=5, 10, 15,20 and 25% of N=50 nodes: Comparison of cluster approach and without cluster approach, after detection and prevention of black hole attack.

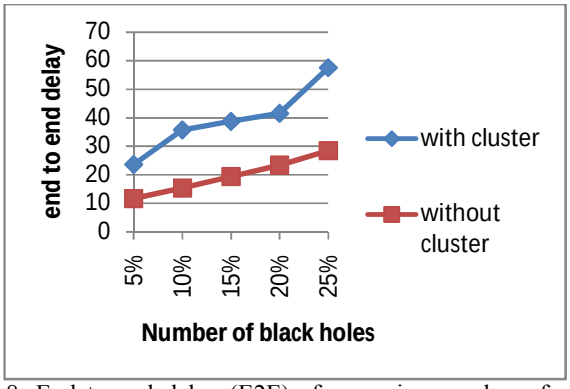

Fig. 8. End to end delay (E2E) for varying number of black hole nodes x=5, 10, 15, 20 and 25% of N=50 nodes: Comparison of cluster approach and without cluster approach, after detection and prevention of black hole attack.

V. Conclusion

In this paper, a clustering based approach is proposed, which distributes traffic among diverse multiple paths to avoid congestion, optimize bandwidth and improve the sharing rate of channel. It uses cluster hierarchical structure to decrease routing control overhead and improve the networks scalability. It can balance the network load, dynamically deal with the changes of network topology and improve reliability. The proposed method is a novel cluster oriented method for detection and prevention of cooperative black hole attack in mobile ad-hoc networks. The simulation experiments are carried out by varying concentration of black holes in the network and also by varying the simulation run time. The simulation results shows that, as the concentration of black hole nodes increases the performance of the network decreases, due to the non-availability of paths as more nodes, become black holes. After comparing the results for cluster approach and without cluster approach, it is observed that without cluster approach shows better performance than the cluster approach. It is attributed to the enhanced computational cost due to maintenance of cluster heads during data transmission.

ACKNOWLEDGEMENTS

The authors are grateful to the referees for their helpful suggestions and support.

REFERENCES

[1]. Sudhiragrawal, Sanjeev Jain and sanjeevshanna.,"A survey of Routing Attacks and Security Measures in Mobile ad- hoc Neworks", Journal of computing,volume 3, Issue 1, January 2011, ISSN 2151-9617, pp 41-47.

[2]. Pradip M. Jawandhiya and mangesh M. Ghonge, r. M.S Ali, Prof. J.S Deshpande., "A survey of Mobile ad-

Volume: 6 Issue: 3 Pages: 2352-2358 (2014) ISSN : 0975-0290

hoc Neworks", International Journal of Engineering Science andtechnology, Vol. 2(9), 2010, pp4063-4071.

[3]. Jitendra savner and Vinit Gupta., "Clustering of Mobile Ad hoc Networks: An Approach for Black Hole Prevention", International conference on issues and challenges in intelligent computing techniques (ICICT)2014, PP 361-365.

[4]. Fidel Thachil and K C Shet., "A Trust based approach for AODV protocol to mitigate black hole attack in MANET", IEEE 2012,978-0-7695-4817-3/12, pp 281-285.

[5]. Muhammad Raza and syedirfanhyder., "A Forced Routing Information Modification Model for preventing Black Hole Attacks in Wireless Ad Hoc Network",IEEE 2011, 978-1-4577-1929 -5/12, pp 418-422.

[6]. P. S. Hiremath and Anuradha T., "Detection and Prevention of Cooperative black hole attack in a MANET",International Journal of Research in Computer and Communication Technology, Vol3, Issue 5, May-2014, pp 604-609.

[7]. Tamilselvan L and Sankaranarayanan.,V. (2007). "Prevention of black hole attack in MANET", The IEEE 2nd International Conference on Wireless Broadband and Ultra Wideband Communications.(auswireless 2007).

[8]. Fan-hsuntseng,Li-Dier Chou and Han-Chieh Chao., "A Survey of Black Hole Attacks in Wireless Mobile Ad hoc Networks", Human-centric Computing and Information Sciences 2011,1:4, Springer, pp 1-16.

[9]. Ratishagarwal and Dr.maheshmotwani., "Survey of Clustering algorithms for MANET",International Journal on Computer Science and Engineering Vol.1(2), 2009, pp 98-104.

Table 5.Performance comparison of cluster based and threshold based methods after detection and prevention of the cooperative blackhole attack.

Percentage of blackhole nodes (x%)	Clustering (proposed method)			Without clustering (method in [6])		
	%Increase in throughput	%Increase in PDR	%Decrease in E2Edelay	%Increase in throughput	%Increase in PDR	%Decrease in E2E delay
5%	26.02%	17.52%	23.64%	51%	29.10%	11.67%
10%	22.23%	16.98%	35.74%	44%	24.10%	15.33%
15%	21.89%	15.13%	38.75%	42%	23.59%	19.37%
20%	16.41%	13.05%	41.53%	40%	22.53%	23.32%
25%	12.78%	12.65%	57.54%	37%	19.01%	28.43%