Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review

Harsh Pratap Singh
Technocrats Institute of Technology & Science,Bhopal (M.P)

Virendra Pal Singh
Technocrats Institute of Technology & Science, Bhopal (M.P)

Rashmi Singh
Barkatullah University Institute of Technology,Bhopal (M. P)

ABSTRACT
Mobile ad hoc network is an assembly of mobile nodes that haphazardly forms the temporary network and it is an infrastureless network. Due to its self-motivatedor mobility in nature the nodes are more vulnerable to security threats which stimulate the performance of the network. In this paper, a review on a various types of coordinated attack is deliberated such as blackhole / grayhole attack which are most serious threats in mobile ad hoc network. In cooperative blackhole attack more than one node collude to each other hence this attack is more challenging to identify. This paper presents a review of different security mechanism to eliminate the blackhole / grayhole attack from the network.

Keywords
Cooperative, Blackhole, Grayhole, Mobile ad hoc network, Routing protocol.

1. INTRODUCTION
The Mobile Ad-hoc Networks (MANETs) is more contrast from surviving networks by the fact that they do not depends onstaticinfrastructure. Each and every nodes itself act as host and router to performs all the functionality of network. Routing has been more severe concern in MANETs and anenormousextent of work has been done in the field of routing security but none of them are more applicable which provide the security so these protocols are more apprehensive of being attacked by numeroussorts of network attack.

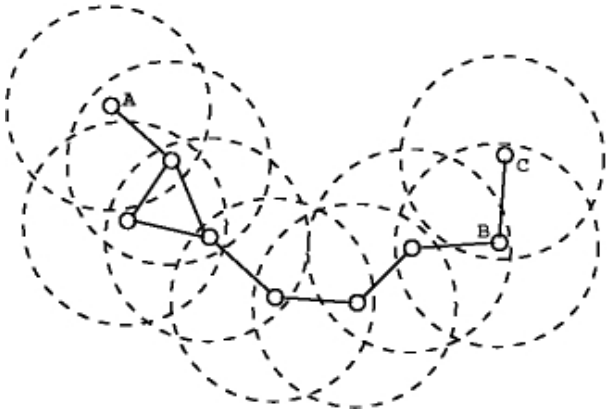

Figure 1 Mobile Ad hoc Network

Mobile ad hoc network nodes are influence by selfish or maliciousnodes, there are some communal type of attack such as wormhole, Denial of Services (DoS), flooding attack, packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks, Sybil attack etc. Alternativecharacteristic of a MANETisdynamic or mobility, limited bandwidth, limited battery power. These characteristic makes routing in a MANET an even harder task. Presently, several proficientsecure routing protocols have been anticipated in survey of literature. These protocols are mainly emphasis on the effective use of digital signature or secret keys toauthenticateand reveal the message and header routing. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [1], nodes find routes only when required. In this research paper we have deliberated a foremost type of common attacks such as cooperative blackhole/ grayhole attack in MANETs and review the various techniques to prevent and detect these attacks (blackhole/ grayhole). The paper is prearranged as follows: Explanation about the cooperative blackhole/ grayhole attack in section 2. Different techniques to prevent and detect these attacks describe in section 3.Presents the summary of the various techniques in terms of their efficacy in section 4.Presents conclusion and future work about the paper and future indirection in section 5.

2. COOPERATIVE BLACKHOLE/ GRAYHOLE ATTACK

2.1 Black Hole
The black hole [2] node passes two things. First, the node of the network exploits the routing protocol, such as AODV, which advertise itself as having a valid or shortest route to a destination node, whereas the route is forged, with the intent of intercepting packets. Second, the malicious node consumes the seizedpackets.

2.2 Cooperative Black Hole Attack
In AODV routing protocol, the source node S wants to communicate with the destination node D, then the source node S broadcasts the route request (RREQ) packet to theiradjacent active nodes and update their routing table with an entry for the source node S, and check if it is the destination node or has a freshest route to the destination node. If does not have, thenthe intermediate node updates the RREQ (by increasing the hop count) and passes the RREQ to the destination node D till it find their destination or any other intermediate node which has a fresh enough route to D, as described by example in Figure 2. The destination node D or the intermediate node with a fresh enough route to D, initiates a route reply (RREP) in the oppositepath, as described in Figure 3. The source node S starts sending the information packets to theiradjacentnode which answered first, and rejects the other replies. This works is satisfactory when the network has no mischievous nodes.

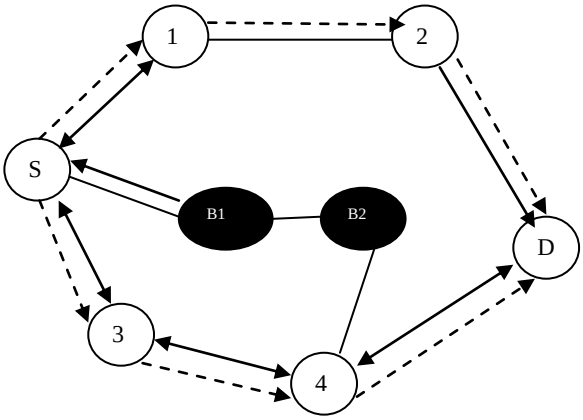

Figure 2 Flooding of RREQ

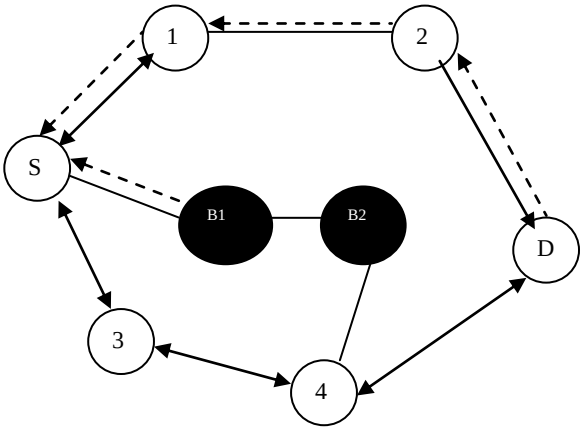

Figure 3 Propagation of RREP

Several authors have projected an algorithm and techniques to distinguish and eliminate a single black hole node [2]. Nevertheless, In case of multiple black hole nodes interim in coordination has not been addressed. For example, when compound black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its associativeblack hole B2 as the next hop, as describedin the figure 3. According to [2], the source node S sends a "Further Request (FRq)" to B2 through a different route (S-3-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "OK" to both the enquiries. Now as per the explanation suggested in [2], node S starts passing the data packets supposing that the route S-B1-B2 is secure. Though, in reality, the packets are consumed by node B1 and the security of the network is conceded.

2.3 Grayhole Attack

Grayholeis oneof the attacks found in ad hoc network.Which act as a slow poison in the network side it means we cannotsupposehow much data can be lost. In grayhole Attack [3] a malicious node trashes to precede certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Grayhole nodes in MANETs are very effective. 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 particular route if such a route is accessible in its routing table. If not, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighboring nodes. Bygettingthe RREQ message, the intermediate nodes bring up-to-date their routing tables in a reverse route to source node. A Route Reply (RREP) message is sent backward direction of the source node after the RREQ query reaches either the destination node itself or any other intermediate node that has a recent route to destination. Now we define the gray hole attack[4] on MANET'S .The gray hole attack has two significantphases.

In first phases, a malicious node exploits the AODV protocol to announce itself as having a valid route to destination node, with the intension of interjecting or humiliating packets, even though route is counterfeit.

In second phases, the malicious nodes drop the intermittent packets with a certain prospect. The process of finding gray hole is very challengingtask. In certain new grayhole attacks the attacker node acts maliciously for the duration until the packets are dropped and then switch to their ordinarynodes behavior. By these activities it's very challenging for the network to distinguish such kind of attack. In some cases grayhole attack is also called as node misbehaving attack. The discrepancy of black hole attacks is the grayhole attack, in which the affected nodes either drop packets selectively. Both categories of grayhole attacks look for to unsettle the network without being detected by the security measures in place [5].

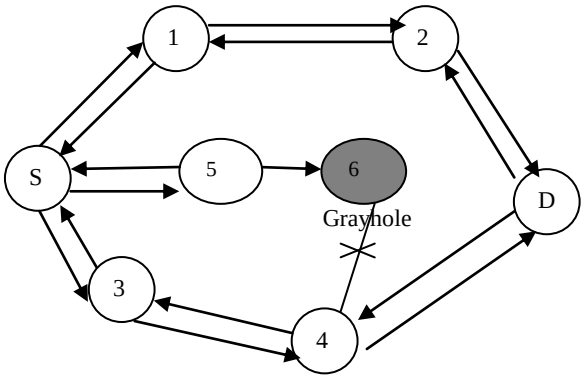

Figure 4 Grayhole Attack in Mobile Ad hoc Network

3. PREVENTION AND DETECTION TECHNIQUES FOR COOPERATIVE BLACKHOLE/ GRAYHOLE ATTACK

A various method has been proposed to detect and prevent blackhole/ grayholeattacks. Review of these methods is presented below:

3.1 For detecting packet forwarding misbehaviourGonzalez et al [6] presents an approach, which works on the principle of flow conservation in a network, which states that if all the

neighbours of a node Nj are interrogated for i) the amount of packets sent to Nj to forward and ii) the packets forwarded by Nj to them, the total amount of packets sent to and received from Nj must be identical. They assume a threshold value for non-malicious packet drop. A node Ni maintains a table with two metrics Uij and Vij, which contain an entry for each node Nj to which vi has respectively transmitted packets to or received packets from. Node Ni increments Uij on successful transmission of a packet to Nj for Nj to forward to another node, and increments Vij on successful receipt of a packet forwarded by Nj that did not originate at Nj. Everynode of the network uninterruptedly checks their neighbouring nodes and bring up-to-date the list of that nodes which they have overheardfreshly. In this algorithm it does not needvarious nodes to overhear each other's received and transmitted packets;neverthelessin its place it uses statistics hoarded by each node as it conveys to and accepts data from its neighbours. Subsequently there is no collaborative compromisemechanism; this method may lead to false allegationsalongside correctly behaving nodes.

3.2 The DRI (Data Routing Information) introduce by the H. Weerasinghe and H. Fu [7] whichhasthe track of past routing experience among moving nodes (router) in the network and verifying of RREP messages from intermediate nodes by start nodes to ascertain the cooperative black hole nodes, and exploitthe improved AODV routing protocol to accomplish this approach. Every and node of the network need to sustain a superfluous Data Routing table, in Y represents for true and N for false. The entry is self-possessed of two characters, from and through which stands for information on routing data packet from the node and through the node respectively. As shown in Table 1, the entry Y Yimplies that node Y has successfully routed data packets from or through node 5, and the entry of N N means that node Y has not routed any data packets from or through node 2. The source node (SN) sends route request packet to each node, and sends packets to the node which responses the route reply packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the INs honesty. After that, SN sends the further request to INs next hop node for asking its routing information, including the current next hop node, the next hop node DRI table and its own DRI table. At the end, the source node compares the above information by cross checking to evaluate the malicious nodes in the routing path.

Node#	Data Routing Information	
	From	Through
2	Y	N
4	Y	Y
B_2	N	N
3	Y	Y

Table 1 Data Routing Information table

Advantages

- Identification of multiple collaborative black hole nodes in a MANET.
- Discovery of secure paths from source to destination that avoid collaborative black hole nodes acting in cooperation.

Disadvantages

- The main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table. It is evident that maintaining past routing experiences wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication.
- The second drawback is over consumption of limited bandwidth. Cross-checking of the validity of routes contained in RREP message from an intermediate node is implemented by sending a FREQ (Further Request) message to the next-hop of the particular intermediate node. Sending additional FREQ messages consumesa significant amount of bandwidth from an already limited and precious resource.

3.3 The dynamic learning method is suggested by Kurosawa et al. [8] to discover the black hole node. In this approach, the normal nodes state views are updated periodically to adapt to the frequent network changes and clustering-based technique is adopted to identify nodes that deviate from the normal state. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. However, it does not involve a detection mode, such as revising the AODV protocol or deploying IDS nodes, thus, it does not isolate black hole nodes.
They have adopted the following 5-step process:

1. Feature selection: Multidimensional feature vector is defined to express the state of the network at each node.Typically the number of sent out route request RREQ and the number of received route reply RREP, The average of difference of destination sequence DstSeq in each time slot between the sequence number of RREP message and the one held in the list are taken as features.

2. Calculate mean: This features mean vector values are calculated, by the equation, where TD represents training data set for N time slot.

$$xTD = 1/N(Pn * Xi) \; Where \; i = 1$$

Therefore the initial training data T0 refer to the data collected in the first interval of the network.

3. Calculate threshold: It calculate the distance of each input data sample x to the mean vector for each time slot, as given here.

$$d(x) = |x - xTD| \wedge 2$$

The distance with the maximum value is extracted as threshold Th from the learning data set.

$$Th = d(x_i)$$

4. Anomaly detection: As soon as the distance for any input data sample is larger than the Th,then it is

reflecteddiverges from the normal traffic and therefore, judged as an attack.

$$d\{x > Th: \ attack \ d(x) \leq Th : normal$$

5. Dynamic training: The calculated mean vector will be used to detect the next period time interval by using data collected in initial time. If it is judged as normal, then the corresponding data set will be used as learning data set, otherwise, it behave as data with attack and thereforeit is discarded. This learning process is repeated for every interval.

Advantages

- Here adopt anomaly-based detection technique; detecting any deviation from the established normal profile.

Disadvantages

- This approach suffers from high false-alarm rate mainly when the normal behavior definitions are still unclear and non-standard in wireless ad hoc networks.

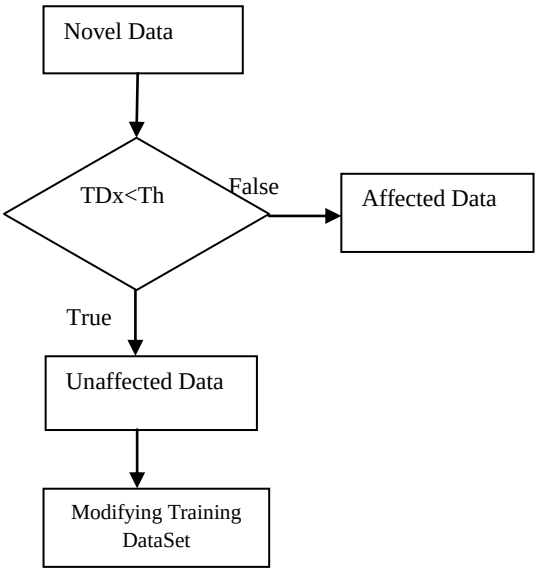

Figure 5 Flowchart for Dynamic learning system method

3.4 This method is proposed by Sarita Choudhary, Kriti Sachdeva et al. [9] which enlistall the malicious node locally at each node whenever they behave as a source node. As stated in the Notionthe protocol uses the concept of Core Maintenance of the Allocation Table i.e. as soon as a new node joins the network, it directs a broadcast message as aappeal for IP address. After receiving this message the backbone nodearbitrarilycarries out the normal functioning by transferring the data pick out form one of the free IP addresses. By receiving the allotted IP address the new node directs an acknowledgement to the backbone node. Now from the time when the allocation is only under the control of the backbone nodes then the dynamic pool of unused/restricted IP address of the network at any point of time is known only to the backbone node.

Grayhole/ Blackhole Elimination method Actions by Source node on receiving the RREP

Step 1: If the RREP is acknowledged only to the Destination & not to the Restricted IP (RIP), over the route.

Step 2: If the RREP is acknowledged for the RIP, it initiates the method of black hole recognition, by transmitting a request to enter into promiscuous mode, to the nodes in an alternate path.

3.5 The detection system proposed by Sun B et al. [10] which uses neighbourhood-based approach to identify the black hole attack and then broadcast a routing recovery process to construct the correct path to the destination. Based on the neighbour set information, suchtechnique is intended to deal with the black hole attack, which involves the two parts: detection and response. The detection procedure, two basic stages are:

Stage 1- In this stage collect the neighbour set information.

Stage 2-This stage is used to determine whether there exists a black hole attack or not. In Response part, a modify-Route-Entry (MRE) control packet is transmitted by the source node to the destination node to form anexact path by altering the routing entries of the intermediate nodesfrom source to destination. This is very efficient and effective to identifythe black hole attack deprived ofannouncing much routing control overhead to the network.

3.6 Two procedures proposed by A. Shurman et al. [11] to prevent the black hole attack in MANETs. The initialprocedure is to find at least two routes from the source node to the destination node. The functioning is done as follow. Initially the source node sends a RREQ message to the destinationthen the receiver node with the route to the destination will reply to this RREQ message and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are at least three received RREP message and after detecting a non-violent route it transmit the RREP message. It shows that there exist at least tworouting paths to route. Subsequently, the source node recognises the safe route by counting the number of hops or nodes and thus prevents black hole attacks.In the nextprocedure, a sequence number is used which is unique. The sequence value is amassed; therefore it is always higher than the current sequence number. This procedure involves two values which are documented in two supplementary tables. These two values of the next procedure are last-packet-sequence-numbers in which the first value is used to ascertain the last packet delivery to every node and the second one is used to the last packet received by the nodes. As soon as a packet are transmitted or received, the values of these two tables are updated automatically. By using these two values of the table, the sender can analysethat whether there is malicious nodes in network or not.

3.7 An algorithm is proposed byS Sharma et al. [12] which are designed using IERP protocol. In this some extra code is included for bluff probe packet and for noticing and avoiding black hole attack. An algorithm is separated into following parts (i) when an intra-zone communication takes place. (ii) When there is inter zone communication. The source node broadcast bluff probe packet when intra-zone communication takes place and the bluff probe packet comprises the address of destination node which really does not exist. The direct neighbor node receives this bluff probe packet. At this time the neighbor node check their routing table entries if they have entry for this non-existent destination node then they forward the packet to the next neighbor. If the non-existing node is assumed to be malicious node then they will give instant response to the source node over the intermediatenode. As per its response, the source node

labelled it as a black hole node and blocks this node. Then after, the source node report to their direct neighbor for altering their routing table entries.

3.8 An approach is proposed by Djamel Djenouri et al. [13] to monitor, detect, and isolate the black hole attack in MANETs. In the monitor phase, an efficient technique of random two-hop ACK is employed. The simulation result shows that random two-hop ACK hugely reduces the cost with a higher true and lower false detection than ordinary two-hop ACK scheme. A local judgment approach based on Bayesian technique is penetrated in the detection phase. The proposed Bayesian detection method does not use any periodic packets exchanging, therefore the familiar overhead problem can be eliminated from this solution. And after a mobile node is determined that it is a misbehaviour node by the proposed detection scheme, this judgment must be proved by all nodes. Hence, authors propose a witness-based protocol that forces the recognized node to ensure this decision from other nodes. Before isolating the misbehaviour node at the same time, the witness-based protocol enforces the detector to gather k witnesses atleast. However, the decision of k value is a trade-off problem. A higher k value eliminates the false detection and attack probability, but reduces the detection efficiency, and vice versa. The simulation shows that the proposed solution can achieve a lower false detection rate and higher true detection rate than watchdog (WD) approach. The solution utilizes cooperatively witness-based verification, nevertheless, it's difficult to prevent collaborate black hole attack for the judgment phase is only running on local side. It might be failed if some malicious nodes deceive the detection node cooperatively.

3.9 The hash based defending method is proposed by Weichao Wang et al. [14]to generate node behavioural proofs which involve the data traffic information within the routing path. The developing mechanism is based on auditing technique for preventing collaborative packet drop attacks, such as collaborative black hole and grey hole problems. The proposed solution is originated from an audit-based detection method videlicet REAct[15], which is also discussed in the subsection 0 in this survey. The vulnerability of REAct system is that cooperative adversaries can specialize in attacker identification phase by sharing Bloom filters of packets between them. The major difference between these two schemes is discussed as follows. A hash based node behavioural proofs is proposed to defend the collaborative attacks. The audited node ni is needed and settled by the source node S, and then S sends the sequence numbers of selected packets to auditing node. After source node sends out these packets, an additional random number t0 is attached to the tail of every packet. The intermediate node n1 combines the received packet and its own random number r1 to calculate its value t1, and this operation is continued within every intermediate node until ni receives the packet. Nevertheless, this paper doesn't give the results, so that it's hard to figure out the enhancement.

3.10 A new control packet called ALARM is used in DPRAODV which is proposed by Raj PN, Swadas et al. [16] while other main concepts are the dynamic threshold value. Unlike normal AODV, the RREP_seq_no is extra checked whether higher than the threshold value or not. If the value of RREP_seq_no is higher than the threshold value, the sender is regarded as an attacker and updated it to the black list. The ALARM is sent to its neighbours which includes the black list, thus the RREP from the malicious node is blocked but is not processed. On the other hand, the dynamic threshold value is changed by calculating the average of dest_seq_no between the sequence number and RREP packet in each time slot. According to this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment. In the simulation results, the packet delivery ratio is improved by 80-85% than AODV when under black hole attack, and 60% when traffic load increases. The advantage of DPRAODV is that it achieves an obviously higher packet delivery ratio than the original AODV, except for it takes a little bit higher routing overhead and end-to-end delay. But DPRAODV simply detects multiple black holes rather than cooperative black hole attack.

3.11 A mechanism is detected by Vishnu K. and Amos J. Paul et al. [17] to detect and remove the black and grayhole attack. This solution is able to find the collaborative malicious nodes which introduce massive packet drop percentage. An idea of the group of backbone nodes used in MANET was originated from [18]. Vishnu K. et al. refer this method to penetrate their system model, and also add a novel scheme videlicet restricted IP (RIP) to avoid collaborative black and gray attacks. The detailed procedure is characterized as the following. In this solution initially a backbone network is established which constructed from a set of strong backbone nodes (BBNs) over the ad hoc network. These trusted nodes can be allowed to allocate the RIP when there is new arrival node joining. A node acquires a RIP which means that it is provided with the routing authority.

The source node requests the nearest BBN to allot a RIP before transmitting data packets, then sending RREQ to the destination node and the address of RIP. If the source node only receives the destination node's RREP, it means that there is no black hole. In the case when the source obtains the RREP packet from RIP, it implies that adversary might be existed in the network. The RIP's neighbor nodes change to promiscuous mode as a result of the source node sends monitor messages to alert them. These neighborhoods not only monitor the packets of designate nodes but also the suspicious nodes. Furthermore, the source node sends few dummy data packets to test the malicious node. The neighbor nodes monitor the data packet flow and regard it as a black hole if the packet loss rate exceeds the normal threshold, and notify the source node that it is a malicious attacker. Then the neighbor nodes broadcast this alert message through the whole network, and add the malicious nodes to the black hole list. Finally, the attacker's authorization will be deleted and all of nodes drop the response from nodes in the black list.

The proposed solution not only detects black hole but also grayhole attacks, since its methodology does not utilize the trust-based method. However, it's hard to realize that how is the enhanced performance because there is no any simulation result or experiment outcome. Moreover, the proposed system might be crashed if the numbers of attackers are higher than the numbers of normal nodes.

The observation and analysis of different approaches to detect black hole based on different criteria are shown in table 2

S. No.	Approaches	Type Of Detection	Problems
1	Packet Forwarding Misbehaviour	Single Black Hole	Falsely Accusing
2	Data Routing & Cross Checking	Cooperative Black Hole	Over Consumption of Limited Bandwidth & Storage Overhead
3	Dynamic Anomaly Detection	Single Black hole	High False Alarm Rate
4	Core Maintenance of Allocation Table Approach	Collaborative black hole	Time delay
5	Neighbourhood-Based Approach	Single Black Hole	High False Positive
6	Authentication & Sequence No Based	Single Black Hole	Limited sequence No
7	Bluff- Based Approach	Single Black Hole	More Time Delay
8	Random two-hop ACK	Single Black Hole	Less Efficient
9	REACT(Hash Based Defending)	Single Black Hole	Resource consumption & Identification delay
10	DPRAODV	Single BlackHole	Time delay & Normalized Overhead

Table 2 Comparison of approaches based on different criteria

3. SUMMARY

By the study of different detection and prevention of cooperative blackhole and grayhole attacktechniques it'sshows that some of the approaches are suppositious postulation and some are the computational exhaustive. Some of methods are trust based which is not valid in mobile ad hoc network but some of the techniques have very high detection rate that do not reflect the node mobility. Many researchers proposed various techniques for the prevention of cooperative suspicious node but most of them are theoretical not implemented. In which some of the methods are fail to detect the grayhole attack because of it need initial trust formation.

4. CONCLUSION AND FUTURE WORK

Blackhole and Grayhole are one of the serious threats in mobile ad hoc network. It affects the performance of the different routing protocol such as AODV by injecting a false route reply message and it also increases the network traffic. A study of different security mechanism has been proposed for the detection and prevention of such attack which have better packet delivery ratio and correct detection probability but have high overhead. A lot amount of work has been done to make the reactive routing protocol free from such threats but these methods do not avoid totally. So there is need for perfect prevention and detection mechanism. The detection of blackhole is a very tough task. For future work is to find the effective method to eliminate the Blackhole and Grayhole totally and which has very low overhead.

5. REFERENCES

[1]. B.Revathi, D.Geetha, "A Survey of Cooperative Black and Gray hole Attack in MANET" International Journal of Computer Science and Management Research Vol 1 Issue 2 September 2012.

[2]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magazine, vol. 40, no. 10, October 2002.

[3]. Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.

[4]. Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[5]. Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.

[6]. Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehaviour in Mobile Ad-Hoc Networks Centre for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[7]. H. Weerasinghe and H. Fu. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future generation communication and networking (fgcn 2007), volume 2, pages 362–367. IEEE, 2007.

[8]. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato. A dynamic anomaly detection scheme for aodv- based mobile ad hoc networks. Vehicular Technology, IEEE Transactions on, 58(5):2471 –2481, jun 2009.

[9]. Sarita Choudhary, Kriti Sachdeva. Discovering a Secure Path in MANET by Avoiding Black/Gray Holes. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-3, August 2012.

[10]. Sun B, Guan Y, Chen J, Pooch UW, "Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[11]. Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[12]. Prof. Sanjeev Sharma, Rajshree, Ravi Prakash, Vivek , "Bluff-Probe Based Black Hole Node Detection and prevention", IEEE International Advance Computing Conference (IACC 2009), 7 March 2009.

[13]. Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6

[14]. Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009

[15]. Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009

[16]. Raj PN, Swadas PB (2009) DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. International Journal of Computer Science 2:54–59. doi: abs/0909.2371

[17]. Vishnu KA, Paul J (2010) Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks. International Journal of Computer Applications 1(22):38–42. doi: 10.5120/445-679

[18]. Agrawal P, Ghosh RK, Das SK (2008) Cooperative Black and Gray Hole Attacks in Mobile Ad hoc Networks. Paper presented at the 2nd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, January 31-February 01, 2008