# A Review on various Single and Collaborative Black Hole Detection Schemes in Manet

Prabhjot Kaur[#1], Kamaljit Kaur[*2]
*#Research Student, CSE, SGGSWU, Fatehgarh Sahib, India*
**Assistant Professor, CSE, SGGSWU, Fatehgarh Sahib, India*

***Abstract***
*A Mobile Adhoc Network (MANET) is infrastructure less dynamic network consist of group of a wireless mobile nodes. Each node in the network communicates with other node without any central point. Due to the Dynamic nature of MANET, security is the important concern of this Network. The dynamic topology of MANET allows nodes to join and leave network at any point. Security of MANET can be compromised by a various security attacks. The black hole attack is the most happening attack in the MANET. In this paper, a review on various detection techniques for single and collaborative black hole attack is presented with their drawbacks.*

**Keywords**
*MANET, Security issues, Single and collaborative black hole attack, comparison of black hole detection techniques.*

## 1 INTRODUCTION

A Mobile Adhoc Network consists of mobile nodes or devices which are free to move in any direction. The nodes can enter and exit a network at any time. The mobile nodes in network can change its link to other nodes immediately.

The mobile nodes are interconnected by wireless links, these nodes are agreed to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs are that every node is honest and cooperative but practically many of them act as a selfish nodes, they participate in the network but don't co-operate with other node because they save their resources for their own use. The infrastructure of MANET is not fixed that is changing with dynamic topology [1].

These nodes have limited battery and bandwidth. The security is the main issue in the MANET. The mobile adhoc network is the combination of nodes which are free to move in any direction. The wireless networks are generally more prone to security threats than wired networks. The selfish nodes can enter in the network and affects the whole performance of the network.

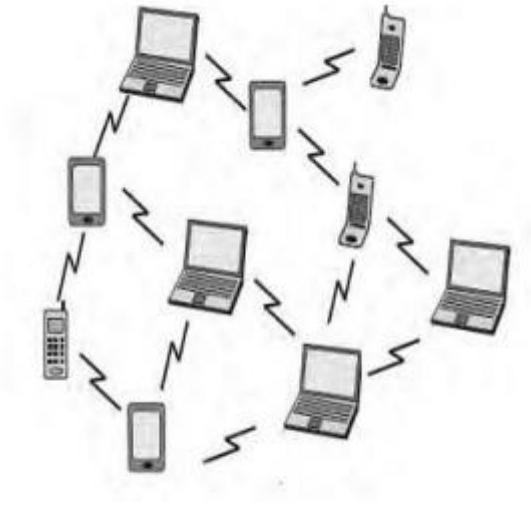

Fig: 1 Architecture of MANET [3]

## 2 SECURITY ISSUES

The security is the main issue of the MANET. Many unauthorized authorities can break the security of the MANET. In this section, the various security issues are explored.

### 1. No physical Boundary

There is no pre defined physical boundary present in the mobile adhoc network. The nodes can communicate with each other in an open environment. The mobile nodes are allowed to join and leave the wireless network at any time. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack [2].

### 2. Open nature of MANET

Due to the open nature of MANET, the selfish nodes can enter in the network and affects the performance of mobile adhoc network. Sometimes it is very difficult to find the selfish or malicious nodes tn the network.

### 3. No centralized control facility

MANETS do not have any centralized control facility which may lead to many security problems. It becomes very difficult to detect any attack. Traffic cannot be monitored from a centralized point instead the control is distributed at each node. The detection becomes more difficult when the advisory changes the attack pattern and the target of the attack. To the node a failure may be caused by an adversary or due to some network problem. [2]

### 4. Limited Battery Power

In the Mobile Adhoc Network, the all nodes are dependent on battery power for their communications with other nodes. When the malicious node joins the network, the malicious node can sent the huge traffic to the target node. The target node handles the whole traffic and loses its battery power.

### 5. Changing scale

The scalability of the mobile ad hoc network keeps changing all the time [2]. It is very difficult to find the total number of nodes in a mobile ad hoc network because nodes are free to move anywhere and nodes can join or leave the network at any time.

## 3 Black hole Attack in MANET

The black hole attack is the most happening attack in MANET. In the black hole attack, a malicious node sends the fake route reply packet with high sequence number to the source node. The high sequence number means that node has fresh route for the communication. Then the source node sends the data packets for further communication and malicious node drops the data packets. As a result the source node will not be able to communicate with destination node and black hole attack degrades the performance of network.

**Black hole Attacks are classified into two categories**

### 3.1 Single Black hole Attack

A single black hole attack means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but the malicious node drops the routing packets and does not forward packets to its neighbours [4]. In fig. 2, the source node 1 wants to communicate with destination node 4. The source node sends the RREQ (Route Request) to its neighbours for the communication. The neighbour nodes send the RREP (Route Reply) to the source node. But the malicious node 3 sends the malicious route reply and shows that it has a fresh route for the communication. Then the source node 1 sends the data packets to the malicious node, and malicious node drops all packets.

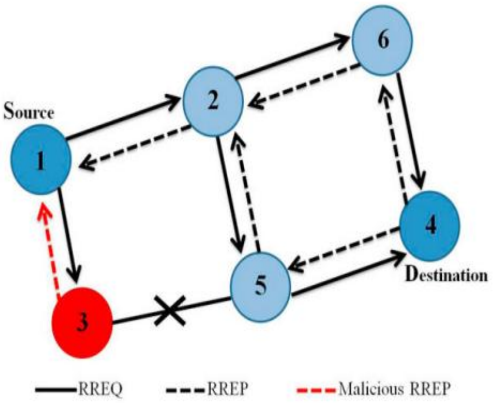

Fig: 2 Single Black hole Attack [4]

### 3.2 Collaborative Black hole Attack

If there are multiple adversary nodes, the attack is called multiple black hole attack. Collaborative or cooperative black hole attack is a special case of multiple black hole attack in which two or more black hole nodes are acting in collusion. Fig.2 is a pictorial representation of collaborative black hole attack. In Fig 2 node S is the source node and node D is the destination node. Here, node 4 and node 5 are malicious nodes working in collaboration. Hence, node 4 can either drop the data packets or forward them to node 5. Similarly node 5 can either drop the packets or sent them to the adjacent malicious node in alliance. [1]

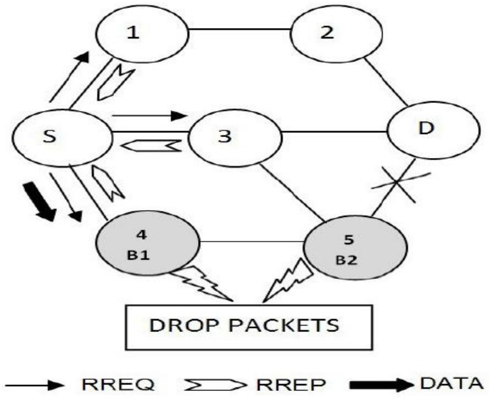

Fig: 3 Collaborative Black hole Attack [1]

### 4. Related Study

Existing single and collaborative black hole detection schemes are explored in this section.

**D-MBH & D-CBH [1]** In this paper, two algorithms are proposed for the detection of single and collaborative black hole attacks. In the D-MBH algorithm, source node sends a fake Route Request (RREQ) with nonexistent target address to the all nodes in the network. The malicious node sends the Route Reply (RREP) with large DSN because larger DSN implies fresh route. Then the D-MBH algorithm computes the average of DSN (ADSN) of all malicious RREPs. The RREP from black hole nodes has higher DSN in comparison with normal RREP.

The D-CBH algorithm creates a list of collaborative black hole nodes. The simulations result shows that the routing overhead and computational overhead has been considerably reduced. But there is no considerable improvement in storage overhead. [1]

**Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) [5]** The Data Routing Information Table and cross checking using Further Request (FREQ) and Further Reply (FREP) methods are introduced to identify black hole attack. The each node in network maintains a DRI table. The DRI table keeps the record of each node that the node did transfer and receives the data with its neighbour nodes. If the source node (SN) does not have the route entry to the destination node then SN will sends a RREQ (Route Request) message to its neighbor nodes to discover a secure and fresh route to the destination node. When any node received this RREQ message then node either replies for the request or again broadcasts it to the network. If the destination node replies for the route request, then all intermediate nodes update or insert routing entry for that destination. Source node always trusts on destination node and SN will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes between source and the destination. The proposed solution is simulated using the QualNet simulator. Simulation results shows that the proposed solution presents better performance in terms of better throughput rate and minimum packet loss percentage as compared to other solutions. [5]

**Distributed and Cooperative Mechanism (DCM) [6]** This solution can avoid, detect and mitigate the multiple black hole attacks. The DCM is composed of four sub-modules. These modules are Local Data Collection, Local Detection, Co-operative Detection and Global Reaction. The Packet Delivery Ratio is improved from 64.14 to 92.93% and the detection rate is also higher than 98% of this solution. The drawback of this scheme is that a control overhead is higher than AODV. [6]

**Message Authentication Code (MAC) and the Pseudo Random Function (PRF) [7]** The two authentication mechanisms are proposed for identifying multiple black hole attacks. These mechanisms provide fast message verification and group identification and also identify multiple black hole attacks and cooperative black hole attacks. The methods improve the routing security in ad hoc network and also prevent the network form further malicious attack. The simulations results show that these two solutions maintain relatively high data packet delivery ratio. [7]

**BDSR (Baited-Black-hole DSR) [8]** this is a DSR based secure routing protocol, named BDSR (Baited-Black-hole DSR). This solution can detect and avoid the black hole attack. Simulation results of this solution shows that BDSR presents better packet delivery ratio and network overhead is also reduced. [8]

**Backbone Nodes (BBN) and Restricted IP (RIP) [9]** In this paper they presented a BBN and RIP solutions to detect black hole and gray hole malicious nodes. The proposed solution identifies and remove any number of Black hole or Gray hole Nodes in a MANET and this solution discover a secure routing path from source to destination by avoiding the black hole and gray hole malicious nodes. [9]

**Fiedelity Table [10]** 'Fiedelity Table' is a solution to find a safe route avoiding cooperative black hole attack. In this solution fidelity levels are assigned to each participating nodes. This solution is more efficient than AODV in terms of packets received ratio in presence of cooperative black hole attack. This solution is simulated using the Global Mobile Simulator. It is found that this solution presents minimum overhead. Future works may be concentrated on ways to reduce the delay in the network. The drawback of this solution is that the end to end delay increased. [10]

**TRUST [**11] a trust based collaborative approach is proposed in this paper to mitigate black hole attack in AODV protocol for MANET. The simulation result shows that this solution presents an efficient packet delivery ratio at the presence of malicious nodes. And the packet delivery ratio increases when the malicious node is detected. The network avoids the malicious node to establishing routes to destination. [11]

**BHSODMRP Certificate chaining [12]** It is a certificate based authentication mechanism to counter the effect of black hole attack. ODMRP is on demand multicast routing protocol. It is a mesh based multicast routing protocol. This solution is implemented in two phases: certification phase and authentication phase. The simulation results show that the proposed solution reduces the packet loss ratio. [12]

**Router Request Table (RRT) table and sequence numbers** [13] This solution is used to find the safe route for the communication and prevents the black hole nodes in the MANET. This solution checks the sequence number of source node or intermediate node who has sent the back route reply (RREP). Then this solution compare the first destination sequence number with the source node sequence number, if there is large differences between sequence numbers, then that node is the malicious node. This solution immediately remove that node entry from the RRT. [13]

**Neighborhood-based method [14]** neighborhood-based method is used for detection of black hole attack. This method is also present a routing recovery protocol which is used to establish the path to the true destination. Simulation results shows that improvement in packet throughput is 15% and the false positive probability is usually less than 1.7%. [14]

**Redundant Routes and Sequence Number [15]** The two solutions are proposed in this paper. The first solution is to find more than one route i.e. redundant routes to the destination. In the second solution, the unique sequence number scheme is described. The simulations result shows that the solution 1 has a more delay as compared to solution 2 and AODV. But solution 1 is more secure as compared to solution 2. The drawbacks of solution 2 are that the malicious node can listen to the channel and also can update the tables. [15]

**Secure AODV (SAODV) [16]** in this paper, the enhancement of AODV protocol is proposed i.e. secure AODV. The SAODV (secure AODV) will be able to avoid black hole attack. The proposed solution increased the value of power delivery ratio as compare to AODV. The limitation of this solution is that end to end delay is slightly higher than AODV. [16]

## 4 Comparison of black hole detection schemes

In this section, the various techniques are compared with their attack types and limitations.

| Techniques | Type of attack | Limitations |
|---|---|---|
| D-MBH (Detection of Multiple Black hole Attack & D-CBH (Detection of Collaborative Black hole Attack) | Single and Collaborative | There is no considerable improvement in storage overhead**.** |
| DRI table and cross checking using FREQ and FREP | Collaborative | 5-8% more communication overhead of route request.<br>The secure route discovery delay slightly increases the packet loss. |
| Distributed Cooperative Mechanism DCM | Collaborative | Control overhead is higher than AODV |
| MAC and Hashbased PRF Scheme | Collaborative | Malicious node can forge a reply if the hash key of any node is to be disclosed to all nodes. |
| Bait DSR (BDSR) based on Hybrid Routing Scheme | Collaborative | The communication overhead is slightly higher than DSR. |
| Backbone Nodes (BBN) and Restricted IP (RIP) Scheme | Collaborative | This scheme might be crashed if the numbers of attackers are higher than the numbers of normal nodes. |
| Fidelity | Single and Collaborative | The routing overhead and end to end delay is slightly higher than AODV. |
| Trust | Single and Collaborative | Increased storage overhead and routing overhead due to exchange of trust tables. Increased end to end delay. |
| BHSODMRP-Certificate chaining | Single and Collaborative | Overhead in implementing Private keys, issuing and checking certificate makes it costly and difficult and causes delay of about 15% |
| Router Request Table (RRT) table checking sequence numbers | Single and Collaborative | Malicious node can act as source node and break security. |
| Neighborhood based and Routing Recovery | Single | Failed when attackers cooperate to forge the fake reply packets |
| Redundant Route and Unique Sequence Number Scheme | Single | Attackers can listen to the channel and update the tables |
| SAODV (Secure AODV) | Single | The end-to-end delay increases when the malicious node is away from source node |

Table1: Comparison of black hole detection schemes

## 4. Conclusion

MANET is a wide area in which security is a major issue. We have analyzed the single and collaborative black hole attacks and analyzed various techniques for detection of black hole attacks. In this paper a survey on various different existing techniques for detection of single and collaborative black hole attack in MANETs with their drawbacks is presented. From the Table 1, it is concluded that the routing, computational and storage overhead is the main drawbacks of the existing techniques. End to end delay is also increased in some existing techniques.

## REFERENCES

1. Arathy K S, Sminesh C N, “A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET”, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, Vol: 25, 2016, pp: 264-271.

2. Rashid Sheikhl Mahakal Singh Chandee, Durgesh Kumar Mishra3, “Security Issues in MANET: A Review”, ISSN: 978-1-4244-7202, IEEE 2010.

3. B.Praveen Kumar P.Chandra Sekhar N.Papanna B.Bharath Bhushan, “A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS”, Int.J.Computer Technology & Applications, Vol 4, pp 248-256, 2013.

4. Fan-Hsun Tseng, li-Der Chou, and Han-Chieh Chao, “A survey of black hole attacks in Wireless Mobile adhoc networks”, Human-centric computing and Information sciences, pp 1- 16, 2011.

5. Hesiri Weerasinghe, Huirong Fu, “ Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, Future Generation Communication and Networking, vol: 2, pp: 362-367, IEEE 2007.

6. Yu, Chang Wu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang. "A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks." In Pacific-Asia Conference on Knowledge Discovery and Data Mining, pp. 538-549, 2007.

7. Zhao Min, Zhou Jiliu, “Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Network”, International Symposium on Information Engineering and Electronic Commerce, pp 26-30, IEEE 2009.

8. Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO, Jiann-Liang CHEN, “Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs”, 13th International Conference on Advanced Communication Technology, pp 755-760, IEEE 2011.

9. Vishnu KA, Paul J: Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks.International Journal of Computer Applications, no 22, pp 38-42, 2010.

10. Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of co-operative black hole attack in MANET.", JOURNAL OF NETWORKS, VOL. 3, pp 13-20, MAY 2008.

11. Fidel Thachil, K C Shet. " A trust based approach for AODV protocol to mitigate black hole attack in MANET" , 2012 International Conference on Computing Sciences, pp 281-285, 2012 IEEE

12. E. A .Mary Anita, V. Vasudevan “Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining” International Journal of Computer Applications, Vol: 1 , pp 21-28, 2010.

13. Pooja Jaiswal, Dr. Rakesh Kumar “Prevention of Black Hole Attack in MANET” International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.2, pp 599-606, October 2012.

14. Sun B, Guan Y, Chen J, Pooch UW: Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, pp 490-495, April 2003.

15. Al-Shurman M, Yoo S-M, Park S: Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), pp 96-97, 2–3 April 2004 .

16. Tamilselvan L, Sankaranarayanan V: Prevention of Blackhole Attack in MANET. Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, pp 21-21, 2007 IEEE.