International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

# A survey on detection of Blackhole and Grayhole attacks in Mobile Ad-hoc Networks

**Rajesh Chowdari[1], Srinivas K [2]**

[1] *PG student, Dept. of Information Science & Engineering, AIT Bengaluru, Karnataka, India*
[2]*Assistant Professor, Dept. of Information Science & Engineering, AIT Bengaluru, Karnataka, India*

---

**Abstract -** Mobile ad-hoc Network (MANET) has more recognition due to two main characteristics, no need of centralized management and dynamic topology. But due to these characteristics mobile ad-hoc networks prone to severe denial of service (DoS) type of security attacks. Blackhole and grayhole attacks come under DoS type of attacks and presence of these attacks in network impacts integrity, confidentiality and availability of network. Various research works carried out to identify and prevent blackhole and grayhole attacks. This paper primarily focused on how blackhole and grayhole attack reduces the network performance. This paper also concentrated on different defense mechanisms that are available to detect and mitigate blackhole and grayhole attacks.

***Key Words*: MANETS, Blackhole attack, Grayhole attack, Proactive routing, Reactive routing.**

## 1. INTRODUCTION

Mobile ad-hoc network are frequent self-configuring and infrastructure less network of nodes connected in wireless fashion. MANET can be easily setup in situations where fixed network infrastructure is not available. Moreover any node can enter or depart at any time into network due to dynamic topology characteristic.

The communication among the group of nodes takes place only when nodes are available to each other and should be present within their transmission range. Due to infrastructure less and no need of centralized administration characteristic mobile ad-hoc networks widely used in military operations, rescue operation and natural disasters.

An ad-hoc network functioning is depends on trust and mutual co-operation among the neighbor nodes. Nodes help each other in managing network and conveying information about network topology. Thus as a host every node involves in routing function and transmits data for all other mobile nodes.

The routing and network maintenance are the most important network operations. Routing protocols are classified into two types proactive, reactive and hybrid based on mechanism involved in routing topology. The table-driven protocols come under proactive routing protocols examples of proactive routing protocols DSDV, WRP. On-demand source initiated protocols or reactive protocols, in contrary; the routing information is not periodically updated but triggers mechanism only when necessary. AODV, DSR and ABR are the examples of reactive routing.

The proactive and reactive approaches are integrated together to provide a hybrid protocols ZRP and TORA are examples of hybrid protocols. Ad-hoc networks face major concern of security due to inherent nature. Due to this slew of attacks are existed that are performed on MANET.

In this paper section 2 detailed about the proactive and reactive routing mechanism and comparison between them. In section 3 explained in detail about the blackhole and grayhole attacks and their adverse effect in MANETS. Section 4 detailed about some mechanisms provided by different authors to detect and mitigate the balckhole and grayhole attack.

## 2. ROUTING IN MANET

The routing process in MANET is carried out without using any central entities. The individual nodes participate in routing process, where source node acts as router while sending data to destination and as a host while receiving the data from destination. Ad-hoc network function depends on mutual co-operation and trust between the nodes. The routing protocols are categorized into proactive, reactive and hybrid protocols.

### 2.1 Proactive (Table-driven) protocol.

The table-driven protocol is a part of proactive routing, protocols comes under this are destination sequenced distance vector (DSDV) and link-state routing protocols. The nodes in proactive routing transmit their routing information to its connected neighbor nodes. Every node in network maintains the routing table along with updated information of adjacent node. The proactive routing protocol has an advantage of reflecting network status quickly if any malicious node deploys attack on the network. The disadvantages associated with proactive routing protocol are 1) large quantity of information for maintenance 2) time-consuming for reactive on reorganization and failure 3) Overhead increases with increase in network size.

### 2.2 Reactive (on-demand) protocol.

The on-demand routing protocol is also known as reactive routing protocol. Unlike proactive routing protocol, reactive routing is triggered only when nodes demand for transmission of data packets when required. Ad-hoc on-demand distance vector protocol (AODV) and dynamic source routing (DSR) comes under reactive routing mechanism. Reactive protocols are designed for networks having low latency with high storage capacity. Advantage of reactive routing over proactive mechanism, is effective utilization of bandwidth and prevents wastage of bandwidth from the broadcast that can be reduced. Main disadvantage is large delay involved in path finding and extreme flooding can guide to network closing and passive packet loss occurs.

**Table -1:** Proactive routing v/s Reactive routing protocols

| Proactive routing V/S Reactive routing protocols | | |
|---|---|---|
| **Parameter** | **Proactive Routing** | **Reactive Routing** |
| Protocols | DSDV,OLSR | AODV,DSR |
| Routing overhead | Low routing overhead. | High routing overhead |
| Multiple Routes | Possible | Possible |
| Route discovery Scheme | On-demand | Before request |
| Packet latency | High | Low |
| Storage capacity | Low | High |

## 3. ATTACKS IN MANET

### 3.1 Blackhole attack

Blackhole attack is a most common type of DOS attack. In this attack compromised node tries to misguide source node by sending false reply's stating that it's the ultimate destination node might affect the network performance. The malicious node sends the extremely high sequence number i.e. the source node might believe that destination node is malicious or it may have new node to reach destination.

As shown in figure1 source node S wants to exchange information with the destination node D, where source node S broadcasts route request (RREQ) packet to its neighbor nodes node 1 and node 3.

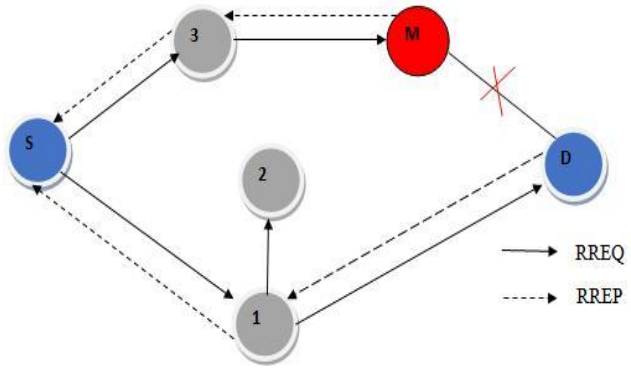


**Fig-1:** Operation of blackhole attack

Nodes upon receiving the RREQ packet it checks entries in the routing table, if node 1 and 3 finds a route to the destination then these nodes send reply to the source node with route reply (RREP) packet. Else it starts forwarding the RREQ packet further to its neighbor nodes.

The Compromised node 'M' upon receiving the route request from node 3 sends false route reply to source without checking its routing table entries saves its battery to forward its own packets. Source node S receives the reply from malicious node M and believes that the path is available to the destination node and starts forwarding the packets. Upon Packets arrival at the node 'M' it starts dropping the packets and also intercepts the control packets that causes serious network issue.

### 3.2 GRAYHOLE ATTACK

Grayhole attack is also a denial of service type of attack. The nature of grayhole attack is highly vulnerable and unpredictable in the network. Because in grayhole attack first the malicious node acts as a real node through route discovery process and forwards the packets to destination node. After some duration the malicious node starts dropping the packets arriving from the actual nodes and forwards the false packets to the destination node. Grayhole attack is extension of blackhole attack and the possibility of packet drop cannot be predictable.

In figure 2(a) the compromised node acts as a real genuine node during route discovery process and also involves in forwarding the packets to the destination. After some duration the malicious node 'M' starts dropping the packets as shown in figure 2(b).

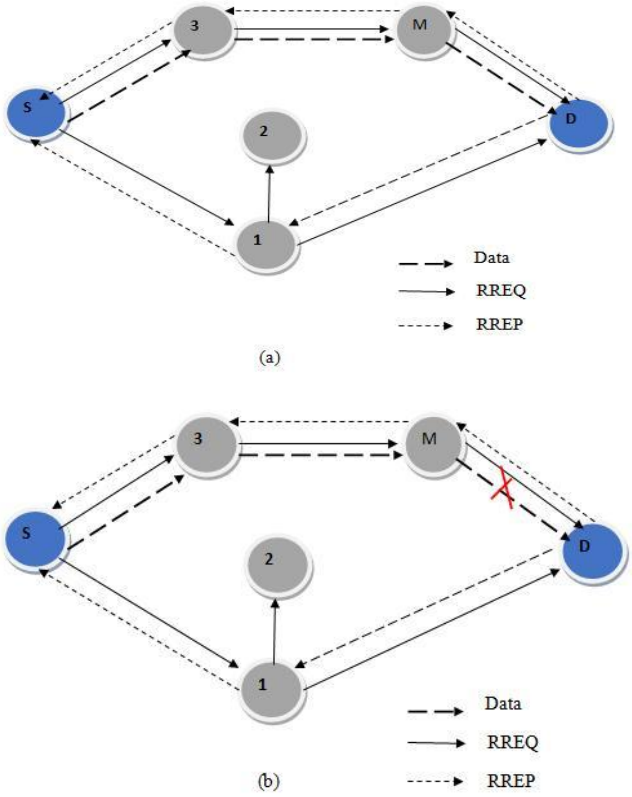


**Fig -2:** Operation of Grayhole attack

Packet loss in grayhole is unpredictable that may cause the more deviating damages to the network. As the blackhole attack can be easily identified and prevented but the grayhole attack detection and prevention becomes difficult. Until the destination node sends the acknowledgement to the source node informing about the packet drop beyond fixed threshold value.

## 4. RELATED WORK

[1] Fidel Thachil, K C Shet, proposed a collaborative technique based on trust model to avoid blackhole nodes MANET using AODV protocol. This approach involved in where every node calculates trust value of neighbor node dynamically and monitors neighbor nodes. In case monitored node trust value crosses the predefined threshold, then node is considered as malicious node and avoids from routing process. The proposed model secures AODV protocol for MANET by preventing blackhole and grayhole nodes.

[2] Kejun Liu, Jing Deng proposed a 2ack method that serves as a best method for routing methods used to discover routing misbehavior and mitigating the adverse effect. The 2ack scheme main plan is sending a 2 hop acknowledgement packets in opposite direction of routing path. The part of only received data packets are acknowledged in 2ack scheme to decrease additional routing overhead and also overcome various problems together with tentative collisions, receiver collusions and insufficient transmissions powers.

[3] P.Rathiga, Dr.Sathappan proposed a novel hybrid approach for black hole and gray hole attack detection in dynamic source routing (DSR) protocol for MANET. DSR protocol dynamically finds the suitable path from source to the sink in MANETS. The monitor node collects the packet flow information of neighbor nodes and information distance metric is computed using two different detection thresholds are determined. The distance metric of a node is compared with first threshold, if the information distance metric is less than first threshold then node is malicious node. If the information distance metric is below the second threshold and not less than first threshold they are considered as grayhole attack and if information distance metric is less than second threshold then it is considered as blackhole attackers. This approach provides better throughput, packet drop rate, packet delivery ratio and routing overhead.

[4] Yugandhara S.Patil, DR. Ashok M proposed a method that implements false reply count to identify grayhole attack in mobile adhoc networks. In this method the nodes sends false replies to request message to capture the traffic through the path setup among source and sink. False reply count detects the gray hole without additional routing overhead by reducing the network traffic helps in finding gray hole attack without increased network traffic. He also proposed a true link concept for path authentication against the node that acts as a genuine node during path establishment and acts a malicious once path is established and communication takes place.

## 5. CONCLUSION

Securing MANET is most challenging and serious issue. This paper review most significant and exposed blackhole and grayhole attacks. Due to these attacks the performance of network is degraded, thus it's essential to detect such attacks prior as possible. Some methods listed are used to mitigate the malicious node attacks in MANET, i.e. every method has its own merits and demerits involved. In this paper we also proposed the proactive and reactive routing mechanism under which several protocols are categorized and are being used for route discovery, path maintenance and detection of node misbehavior in MANET. Additional research must be carried out to extend several techniques to detect and prevent misbehaving nodes with minimum limitations.

## REFERENCES

[1] Fidel Thachil, K C Shet "A Trust Based Approach for AODV Protocol to Mitigate blackhole attack in MANET" International conference on computing sciences IEEE DOI 10.1109/ICCS.2012.7.

[2] Kejun Liu, Jing Deng "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE transactions on mobile computing, vol. 6, no. 5, may 2007.

[3] P.Rathiga, Dr. S. Sathappan "Hybrid Detection of Black hole and Gray hole attacks in MANET", 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions 978-1-5090-1022-6/16/$31.00 ©2016 IEEE.

[4] Yugandhara S.Patil, Dr. Ashok M "Gray Hole Attack Detection using False Reply Count and True Link based Path Authentication in MANET".

[5] Kusumlata Sachan, Manisha Lokhande " An Approach to detect Gray-hole Attacks on Mobile ad-hoc Networks" 978-1-5090-5515-9/16/$31.00 ©2016 IEEE.