# Detection Of Gray Hole Attack In Mobile Ad-hoc Network

Nilesh Rokade, Madhav Pandhare, Nikhil Wani, Priyanka Patil

Sinhgad Institute Of Technolgy,Lonavala,Pune

## Abstract

Mobile ad hoc networks are highly susceptible to routing attacks because of their dynamic topology and lack of any infrastructure. Two of the major routing attacks are black hole and gray hole attacks. In a black hole attack, malicious node diverts most of the traffic in the network to itself, and later dumps it. A gray hole attack is a variation of the black hole attack, which changes its state from honest to malicious and vice versa. In this paper we have illustrated an algorithm to detect Gray hole attacks in MANET, which leads to improved network performance in terms of performance metrics. i.e. throughput, packet drop ratio and normalized routing overhead.

**General Terms** Routing Protocols, Security, Mobile Ad-hoc Network

**Keywords**

AODV protocol, Gray hole attack, malicious node

## 1. Introduction

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks. major security goals. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment.

They are mainly

1.Confidentiality
2. Integrity
3.Availability
4.Non-Repudiation
5.Assurance

## 2. Related Work

The black and gray hole attack will bring great harm to the performance of Ad Hoc network. In previous research, the authors have carried out experiment on black hole attacks and flooding attack . Sun et al presented a general approach for detecting the black hole attack. They devised a neighborhood-based method to detect the intruder and a routing recovery protocol to set up a correct path to the true destination. Patcha et al proposed a collaborative method for black hole attack prevention. A watchdog method is introduced to incorporate a collaborative architecture to tackle collusion amongst nodes. Gao et al proposed to use aggregate signature algorithm to trace packet dropping nodes. Shila et al presented a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks . Yi et al propose a distributed intrusion detection approach. Yi et alfocuses on investigating immunological principles in designing a multi-agent security architecture for intrusion detection and response in wireless mesh networks

Jhaveri R.H.[9] approach uses intermediate node dynamically calculating peak value, author used three parameters for calculation. RREP sequence number, routing table sequence number and number of replies received during time interval.

G. Xiaopeng proposed the detection scheme against gray hole attack [5]. It consists of three algorithms which are creating proof algorithm, the check up algorithm and the diagnosis algorithm. In creating proof algorithm, the source nodes are creating proof which is based on aggregate signature algorithm for received message. In check up algorithm, the source node suspects the malicious node. Reliability is good. Bidirectional links are not required. Security is satisfactory and bandwidth overhead is low. In diagnosis algorithm, the evidences are getting from the check up algorithm, it finds the malicious node. This mechanism is not detecting all malicious nodes

## 3. Type of Security Attacks

### 3.1. External vs. Internal attacks

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodesfrom providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

### 3.2 Passive attacks and Active attacks

The security attacks in MANET can be roughly classified into two major categories, namely passive attacks and active attacks are as described in the figure 1.

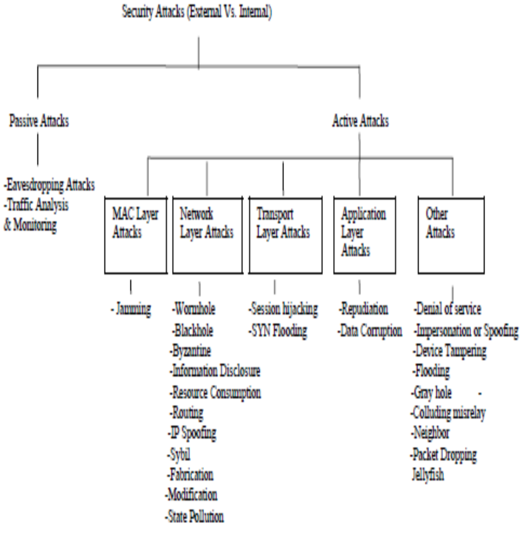


Figure 1: Different types of attacks on MANET

### 3.2.1 Passive Attacks

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted.

### 3.2.2 Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication.

## 4. Routing protocols in MANET

Any routing protocol are to ensure set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks.

### 4.1 Proactive routing protocols (Table driven)

The proactive routing protocols (e.g. OLSR) are usually use link-state routing algorithms flooding the link information. Link-state algorithms maintain a full or partial copy of the network topology and costs for all known links.

### 4.2 Reactive routing protocols (On demand)

The reactive routing protocols (e.g. AODV) create and maintain routes only if these are needed, on demand. They usually use distance-vector routing algorithms that keep only information about next hops to adjacent neighbors and costs for paths to all known destinations. Thus, link-state routing algorithms are more reliable, less bandwidth-intensive, but also more complex and compute- and memory-intensive.

### 4.3 Ad-hoc On-Demand Distance Vector (AODV)

AODV is a relative of the Bellmann-Ford distant vector algorithm, but is adapted to work in a mobile environment. AODV is a reactive hop-by-hop routing protocol, the routes are created only when they are needed.

AODV functions:

1. Route Discovery

2. Path table management

3. Path maintenance

### 4.3.1 Merits of AODV

1. It does not need any central administrative system to control the routing process.
2. It tends to reduce the control traffic messages overhead.
3. It saves storage place as well as energy.

### 4.3.2 Drawbacks of AODV

1. Broadcast storm problem
2. AODV can gather only a very limited amount of routing information, route learning is limited only to the source of any routing packets being forwarded.
3. The performance of the AODV protocol without any misbehaving nodes is poor in larger networks.

## 5. Black hole attacks Vs. Gray hole attacks

**Black hole Attack:**

Black hole attack is kind of DoS (Denial of Service attack) attack**.** Malicious node advertises itself as having shortest path to requested node and drops all data packet. It degrades the performance of the network

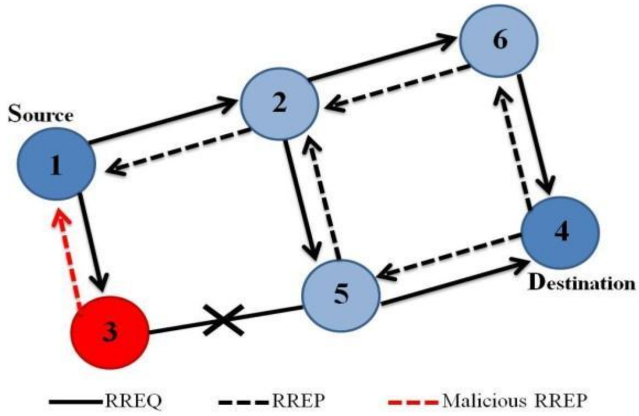


Fig .2 Black Hole Attack

### Gray Hole Attack

Gray hole is similar to Black hole attack, but nodes switches their states from black hole to normal and vice versa. Detection of Gray hole attack is difficult because its state is not stable.

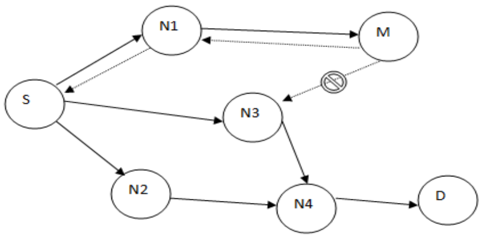


Fig.3 Gray Hole Attack

## 6. PROPOSED MECHANISM

Proposed algorithm is to detect gray hole node and eliminate the normal nodes with higher sequence number to enter in black list. The algorithm calculates the peak value and checks whether reply packet sequence number is less than or not. The parameters used to calculate the peak value are

a) Routing table sequence number.
b) Reply packet sequence number.
c) Elapsed time of adhoc network.
d) Total number of reply packets received by the intermediate/neighbor/replying node.
e) Reply Forward Ratio (RFR) of replying node.

### 5.1 Algorithm for Gray Hole Attack

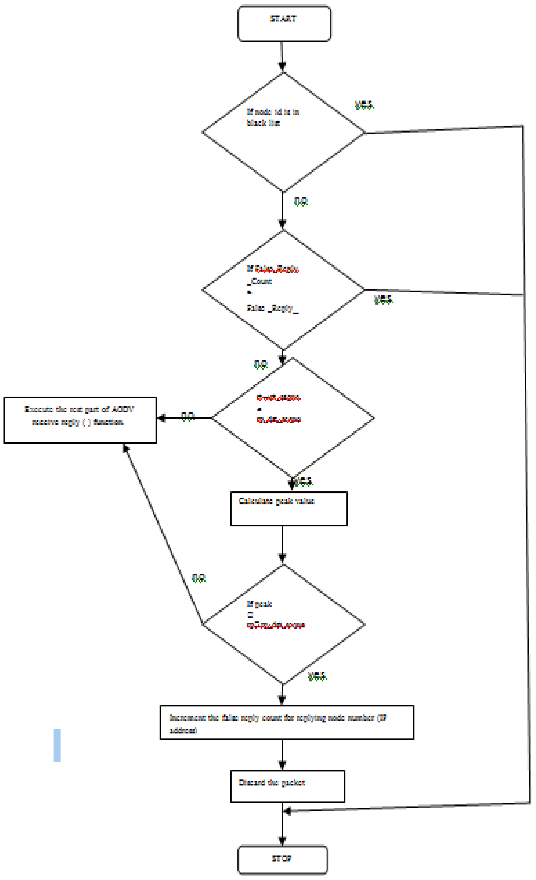
**Step 1:** Start (for each node which receives RREP).
**Step 2:** Check if a replying node has generated False_Reply_Count greater than False_Reply_Threshold
 if yes goto step 3,
 no goto step 4
**Step 3:** Black list the node, don't accept any RREP packet (discard) from this node further.
**Step 4:** Check if routing table sequence number is less than reply packet sequence number.
 if yes goto step 6
 no goto step 5
**Step 5:** Skip detection engine and
 goto step10.
**Step 6:** Calculate
 - Difference between routing table sequence number and route reply sequence (Diff.).
 - RFR- Reply Forward Ratio
 - Peak = ([((Diff) × RFR) + No. of replies received by replying node + Current Simulation Time])/3
**Step 7:** Check if peak < route reply sequence number
 If yes goto 8
 No goto 10

**Step 8:** Add/Increment the false reply count to corresponding replying node.

**Step 9:** Free the packet (RREP)

**Step 10:** Follow the remaining aodv recvreply() function.

## 6.2 Flowchart


START
If node id is in black list
YES
no
If False_Reply_Count
=
False_Reply_
YES
no
no
Execute the rest part of AODV receive reply ( ) function.
YES
Calculate peak value
no
If peak
=
YES
Increment the false reply count for replying node number (IP address)
Discard the packet
STOP

## 7. Simulation

We used simulation tool NS-2.35,

| **Parameter** | **Used in simulation** |
|---|---|
| DoS Attack | Gray hole attack |
| Protocols studied | AODV |
| Simulation time | 100 sec. |
| Simulation area | 1500*1500 |

### 7.1 Metrics

The metrics used to evaluate the performance of the mobile ad hoc networks are given.

**Throughput:** It is defined as the amount of data transferred over the period of time expressed in kilobits per second (kbps).

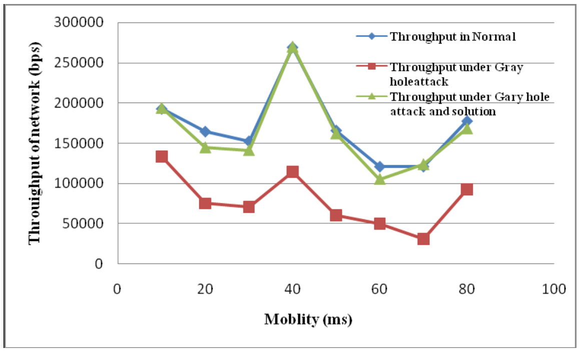
**Packet Drop Rate:** It is the ratio of the data lost at destinations to those generated by the CBR sources. The packets are dropped when it is not able to find the valid route to deliver the packets.

**Packet Delivery Ratio:** It is the ratio of data delivered to the destination to the data sent out by source.

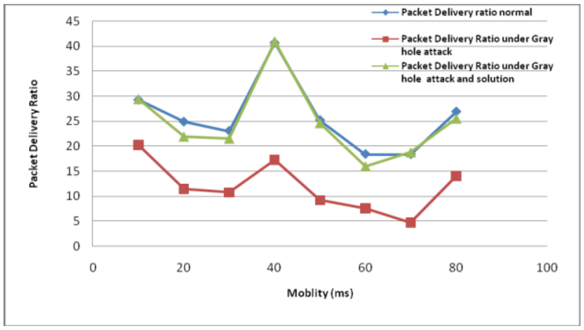
**Normalized Routing Overhead:** It is the ratio of routing transmissions to the data transmissions in the simulations. The routing transmissions are RREQ, RREP, RERR etc.

## 7. Simulation Results

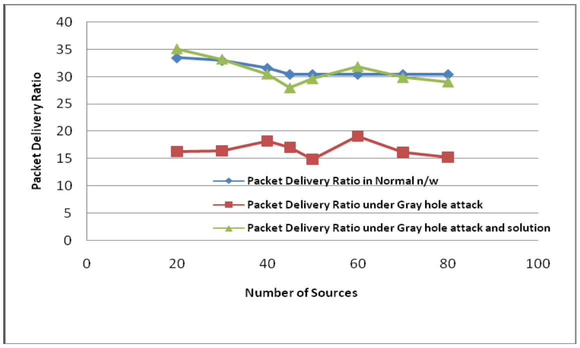
Performance of the AODV protocol is measured by varying the parameters in simulation like mobility, number of sources and number of mobile nodes. All the results are dependent on current position of nodes i.e. simulation scenario and may vary on next simulation because the gray hole is flashing between good and bad. Simulation studies shows that the performance of routing protocols in terms of throughput, packet dropping rate and end-to-end delay strongly depends on network conditions such as mobility, traffic and number of nodes. Here are some results.



**Throughput Vs. Mobility**



**Packet Delivery Ratio Vs. Mobility**



**Packet Delivery Ratio Vs. Number of Sources**

## 6. Conclusion And Future Work

In modified protocol, proposed approach uses effective way of providing security in AODV against gray hole attack. Proposed mechanism is to detect gray hole attack and eliminate the normal nodes with higher sequence number to enter in the black list. Effective decision making regarding black listing of nodes by keeping track on switching activity. Effective use of peak value and implementation of fresh approach of current elapsed time of adhoc network to make the proposed mechanism more efficient. It is not sending any alarm packets to other nodes when gray hole detected. Hence it is reducing extra routing overhead incurred by sending alarm packets.

## References-

[1] "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks" Rutvij H. Jhaveri1, Sankita J. Patel2 and Devesh C. Jinwala3
1Computer/IT Engineering Department, Shri S'ad Vidya Mandal Institute of Technology, Bharuch 392-001, Gujarat, India *1rutusoft@yahoo.com*
2,3Computer Engineering Department, Sardar Vallabh National Institute of Technology, Surat 395-007, Gujarat, India *2sjp@coed.svnit.ac.in*, *3dcj@coed.svnit.ac.in*

*[2]* "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks" Chen Wei Long Xiang Bai Yuebin Gao Xiaopeng School of Computer Science Beihang University Beijing, China buaacst@hotmail.com, {long, byb, gxp}@buaa.edu.cn

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

[4] "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network" Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU School of Information Security Engineering Shanghai Jiao Tong University Shanghai, China {goodcjw2, yiping, jeffcjl, seanwang, ningliu}@sjtu.edu.cn 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[5] "Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" Gao Xiaopeng Chen Wei *School of Computer Science BeiHang University gxp@buaa.edu.cn, buaacst@hotmail.com* 2007 IFIP International Conference on Network and Parallel Computing – Workshops.

[6] "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks" Piyush Agrawal and R. K. Ghosh Indian Institute of Technology, Kanpur - 208 016, INDIA {piyushag,rkg}@cse.iitk.ac.in