International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979, Impact Factor: RJIF 5.72
www.allsubjectjournal.com
Volume 3; Issue 6; June 2016; Page No. 79-81

Detection and prevention method compression of black and gray hole attack using AODV protocol: A survey

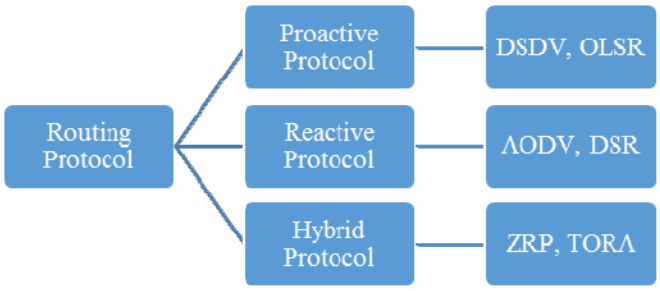
[1] Rathiga P, [2] Dr. Sathappan S

[1] Research Scholar, Department of Computer Science, Erode Arts & Science College, Erode, Tamilnadu, India
[2] Associate Professor, Department of Computer Science, Erode Arts & Science College, Erode, Tamilnadu, India

Abstract
In this paper proposed an innovative approach for the detection of the dangerous gray hole attack as well as black hole attack. AODV is an important on-demand distance vector routing protocol for mobile ad hoc networks. It is more vulnerable to black hole and gray hole attack. A Gray hole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. In a black hole attack, a malicious node sends false routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. Many researchers have given special solutions for preventing and detecting of these attacks.

Keywords: Gray hole attack and Black Hole attack, AODV

1. Introduction
There are many routing protocols available in the MANET. Whenever a node wants to communicate with goal node, it broadcast its current status to neighbors. Routing protocols can be classified into three types such as proactive, Reactive and Hybrid routing protocol.



A) Reactive protocols
They are known as demand driven protocol meaning that they find routing path only when it's needed. To discover fresh route these protocols makes use of route request and route reply messages. After receiving route reply messages the route is established by the nodes. Route discovery makes a big delay and it is the main drawback of these protocols.

B) Proactive protocols
These protocols are Table Driven Protocols. These protocols constantly preserve the network topology. In a network every node contains the information of the neighbor nodes. This information is stored in different tables and these table values are updated according to the changes in the present network topology.

C) Hybrid protocols
The combination of proactive protocols and reactive protocols is a Hybrid protocols. These type of protocols make use of distance-vector for more precise metrics to establish the best paths to end networks. In this type network every node has its own routing zones and the size of the zone is defined by a zone radius (i.e.) number of hops in one zone. Each node keeps a record of routing information for its individual zone. In hybrid protocols, routers only maintain about the adjacent routers information. Source initiates the establishment of routes to a specified destination on demand during reactive operation.

2. AODV
Ad–hoc on demand distance vector routing is on-demand routing protocol (AODV). It is classified under reactive protocol. Functions of AODV protocol is route detection and route maintenance. In Ad-hoc routing network, when a route is essential for particular destination, the protocol establish route discovery. Route discovery process begins with the creation of a Route Request packet. Each packet contains source node's IP address, source node's current sequence number, IP address of destination node, destination sequence number the broadcast identifier and the time to live field. AODV uses a destination sequence number to decide up-to-date path to the destination.

A network node updates its path information only if the sequence number of the current packet received is greater or equal than the last sequence number saved at the node. Destination sequence number indicates the newness of the route that is accepted by the source. All of the intermediate nodes having suitable routes to the destination, or the destination node itself is allowed to send Route Reply packets to the source. Every intermediate node, while forwarding a Route Request, enters the earlier node address and its Broadcast id. When a node receives a Route Reply packet, information about the earlier node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

Routing Attacks in MANETS
All of the MANETs routing protocols are depend on the active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The attacks on MANETs

can be categorized as active attacks or passive attacks. Within the passive attacks the attacker does not send any message, but it just listens to the channel. Passive attacks are non-disruptive, but is information seeking, which may be critical in the operation of a protocol. In a wireless surroundings it is normally impossible to detect this attack, as it does not produce any new traffic in the network. The action of an active attacker includes such as injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets and impersonating other nodes which violates availability, integrity, authentication and no repudiation paradigm. Some of the well-known routing attacks in MANETs such as black hole and gray hole attacks are discussed below.

Black Hole Attack

In this type of attack, the attacker node injects false route replies to the route requests claiming to have the shortest path to the destination node whose packets it wants to interrupt. Once the fictitious route has been recognized the active route is routed through the attacker node. The attacker node is then in a position to misuse or discard any or all of the network traffic being routed through it. The following figure-1 shows the black hole attack.

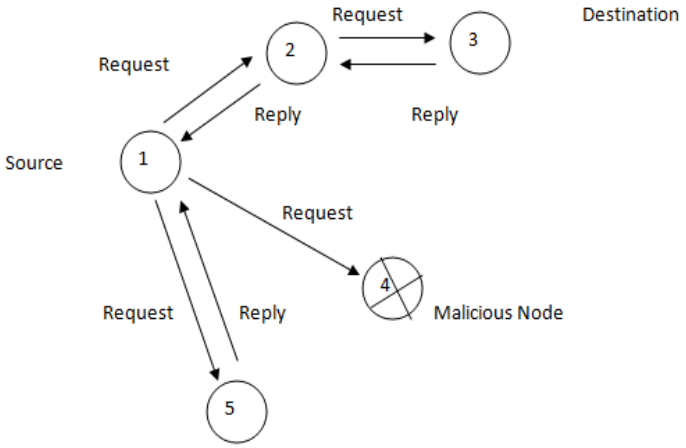


Fig 1: Black Hole Attack

AODV protocol works on the basis of the on-demand mechanism to create the paths among the nodes by the preferred source nodes. This protocol manages the paths till it is required for the source nodes. The same time it generates trees to associate with the multiple cast category branches. The tree consists of the category branches and the nodes should combine with its members. It is using the sequence number to protect the uniqueness of paths. A malicious node can be present at any place in the network. The following figure-2 shows the multiple black hole attack.

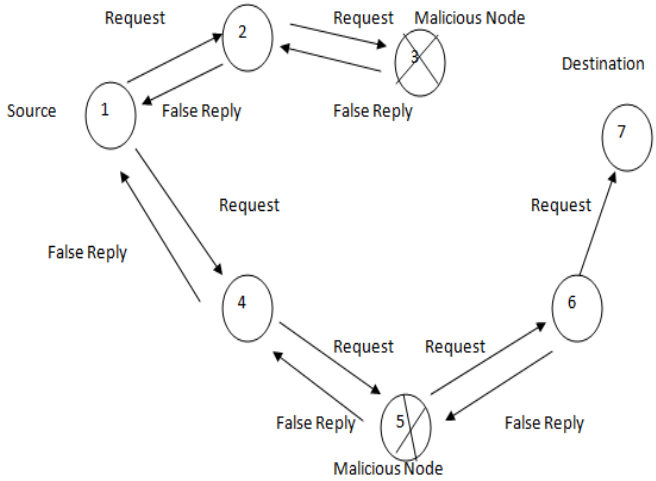


Fig 2: Multiple Black Hole Attack

Gray Hole Attack

A variation of black hole attacks us is the gray hole attack, in which nodes either drop packets selectively (Ex. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (Ex. Dropping 50% of the packets or dropping them with a probability distribution). Both types of gray hole attacks seek to disrupt the network without being detected by the security measures in place. The following figure-3 shows the gray hole attack.

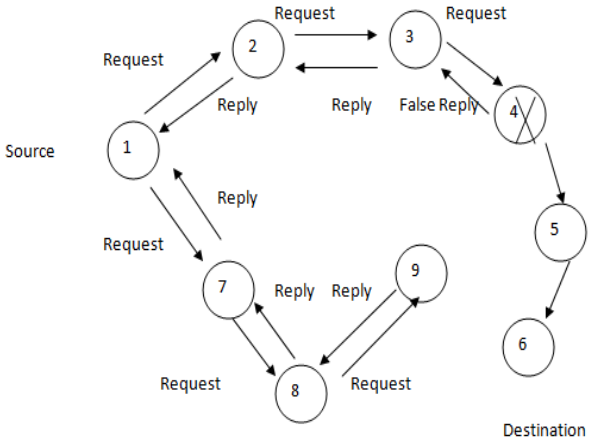


Fig 3: Gray Hole Attack

Comparison of methodologies in AODV protocol:
The following table-1 shows the comparison between the existing solutions using AODV protocol.

Table 1: Comparison of methodologies

S. No.	Author name	Title	Method used
1	Rashmi, Ameeta Seehra	Detection and Prevention of Black-Hole Attack in MANETS	lightweight methodology is based on simple acknowledgement scheme
2	Surana K.A., Rathi S.B. Thosar T.P. and Snehal Mehatre	Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms	Watchdog mechanism
3	Divya Khajuria Sudesh kumar	Detecting multiple Black hole and gray hole attacks in MANETS by modifying AODV	detection before route discovery and detection during route discovery
4	Manisha M. Jadhao	Detection of Gray Hole and Black Hole using EDRI Table in MANETs- A Review	Extended Data Routing Information (EDRI) table at each node with the Routing Table
5	Megha Arya and Yogendra kumar Jain	Gary hole attack and prevention in Mobile Adhoc Network	IDS based method IDSAODV for detecting and preventing Gray hole attack

3. Conclusion

Black Hole Attack and Gray hole is a main security threat which affects the performance of the routing process in Manet. The attack detection is the main matter of concern. Over the current past years, many researcher scholars proposed their own method for packet drop detection to improve the packet transmission. In this paper, many advanced methodologies have been discussed. The present detection techniques not properly working against co-operative black hole and gray hole attacks. The comparison between the existing solution shows that there is no reliable method to solve the security problems. In conclusion a lot amount of work has been done to make the reactive routing protocol free from malicious attacks but these techniques do not avoid totally such type of attack. So there is need for perfect prevention and detection mechanism. For upcoming work is to find the efficient method to reduce the Black hole and Gray hole totally and which has very low overhead.

4. References

1. Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey - International Journal of Advanced Research in Computer and Communication Engineering 2013; 2:10.
2. An Innovative Approach to Detect the Gray-Hole Attack in AODV based MANET- International Journal of Computer Applications (0975-8887). 2013; 84:8.
3. Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol- International Journal of Computer Applications (0975-8887). 2012; 41:5.
4. Trust Based Routing Mechanism Against Black Hole Attack Using AOMDV-IDS System In MANET Format - International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459 2012; 2:4
5. Surana K.A, Rathi S.B, Thosar T.P, Snehal Mehatre. Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms, World Research Journal of Computer Architecture. 2012; 1(1):19-23.
6. Detecting multiple Blackhole and Grayhole attacks in MANETS by modifying AODV, *IOSR Journal of Computer Engineering (IOSR-JCE), E-ISSN: 2278-0661, P- ISSN: 2278-8727*, 16:2.
7. Megha Arya, Yogendra Kumar Jain. *Gary hole attack and prevention in Mobile Adhoc Network* IJCA 2011; 27:10.
8. Simulation of Gray Hole Attack in Adhoc Network Using NS2- Ms. Meenakshi, Mr. Kapil Kumar Kaswan, International Journal of Computer Science & Engineering Technology (IJCSET).