International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 03 – Issue 05 || May 2018 || PP. 121-126

Black and Grey Holes in AODV and Some Prevention Schemes

Anurag Misra
Training Specialist
Higher Institute of Plastic Fabrication
Riyadh, Saudi Arabia

Abstract: Mobile Ad-Hoc Networks are infrastructure less mobile networks. Routing in such networks is pretty hard due to so many constraints these networks face as these types of networks don't have fixed infrastructure. They have very limited bandwidth, limited energy and have great chances of connection failures. That's the reason providing a loop free and reliable route is very difficult in such networks. Ad-hoc On Demand Distance Vector (AODV) is one of the routing protocols used for MANETs. AODV is a reactive on-demand routing protocol. It is considered as one of the most efficient routing protocol for MANETs. Although AODV is quite good in providing loop free and reliable routes to deliver data but sometimes some malicious node can disrupt the transfer. This malicious node in a network replies to any route request sent on network with route update message and declares that it has shortest path available through it for destination. Sender immediately picks up the path and directs all the packets through this malicious router but instead of forwarding such packets this node drops all these packets. As no packets are forwarded from this router such type of malicious router is known as Black Hole (BH). The complexity of problem still doesn't end here because sometimes malicious node doesn't drop all the packets but it targets some specific traffic or it drops packets for specific time periods, then such phenomenon doesn't called black hole coz some of the traffic is getting through. This partial packet loss problem is known as Grey Hole (GH).

Detecting black hole and grey hole is quite challenging, especially in MANETs where resources are already very limited and to find some way to detect and resolve black hole or grey hole problem definitely consume some resources. So, the biggest challenge is to reduce overheads while detecting and solving the problem. There are several schemes to counter such attacks some of the schemes used for single black hole attack in AODV are as follows:

- Neighborhood based and Routing Recovery
- Redundant Route and Unique Sequence number
- Time Based Threshold Detection Scheme and
- Detection, Prevention and Reactive AODV (DPRAODV) etc.

All these schemes have different ways to counter the problem and have different effects but problem doesn't end here. All of the above mentioned schemes just apply when only one router is causing the problem. But there are scenarios where 2 or more router collaborates with each other to send false route replies. To counter such collaborative attack some other schemes are used. Some of them are as follows:

- Data Routing Information (DRI) and Cross Checking
- Data Routing Information (DRI) and Cross Checking using FReq and FRep
- Cooperative Mechanism (DCM) and
- Message Authentication Code (MAC) and Hash-based Pseudo-Random Function (PRF) Scheme etc.

In this paper we will discuss the problem of Black hole and Grey hole in reference to AODV in detail and we will also discuss some of the problem solving schemes to establish a firm foundation to provide a criterion to select best possible scheme to resolve black hole or grey hole problem.

General Terms: Distance Vector, Packet Delivery, Delay, Route Update, Routing, Loop Free.
Keywords: AODV, Black Hole, Grey Hole, Router, MANET, Protocol, Topology, Path Discovery

AODV as Routing Protocol for MANETs

Ad Hoc On demand Distance Vector (AODV) is a reactive routing protocol. In AODV full time routing tables are not managed. It's an on demand protocol, it doesn't use regular network updates, it starts to look for the route only when some data transfer is initiated and some node asks for the route. It uses sequence numbers to avoid loops and to ensure freshness of route. When a nodes wants to send data it broadcasts route requests (RREQ). All the nodes in network receives that broadcast and check if its destined to them or any node for which they have available path. If both the conditions are false then RREQ is forwarded and address of the node from which it was received is recorded. If any one of the conditions is true then that node replies with a RREP message by using one of the available temporary routes. This process provides all possible routes to source node. Source node then selects the route with minimum hop count to send the data. This selected route is

stored till the transmission is complete or the route is available, rest all the routes are discarded after reaching timeout. Selected route remains active till the data is transferred periodically. If no packets are transferred till the timeout, then transfer is assumed to be complete and route information is discarded from the routing tables of intermediate nodes. If any error occurs during the transfer route error (RERR) message is issued for the source with the information that destination is unreachable. The propagation of route error message can be visualized as a tree with the node at the point of error as root and the nodes using the failed link as leaves.

I) Propagation of Route Request (RREQ) II) Propagation of Route Request (RREP)

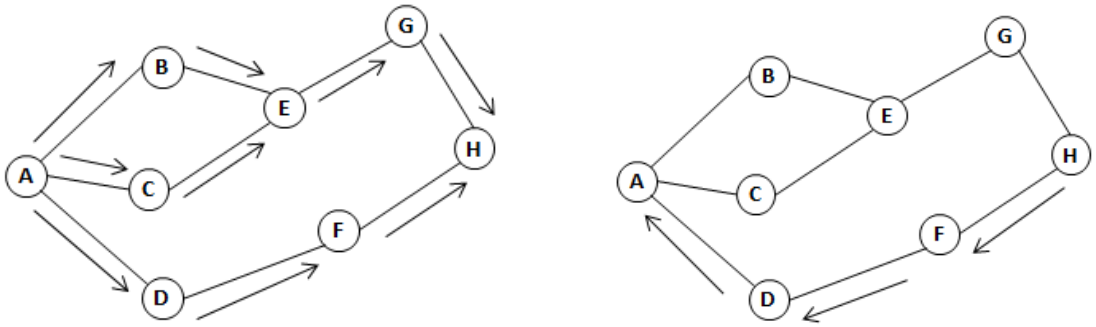

Figure 1 – Propagation of RREQ and RREP Packets in AODV

Black Hole

As we have seen in AODV when a node wants to send data, it broadcasts a RREQ message which is received by all other nodes. The nodes having the information about destination, come up with the RREP and all routes are sent to source. After receiving all the routes, route with the least hop count is selected. In normal circumstances, it's quite effective but sometimes network has some malicious node which replies to each RREQ with least hop count. Definitely this route with malicious node is always selected due to least hop count but when data is sent through this route, this malicious node drops all the packets instead of forwarding them towards destination. All the messages came to this node are dropped, that's why such phenomenon is called Black Hole.

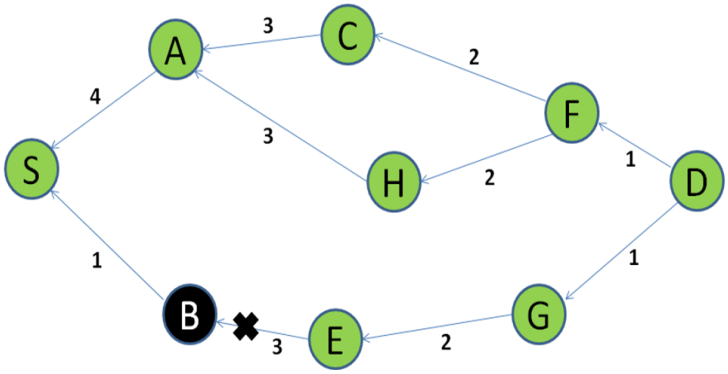

Figure – 2 Propagation of RREP packets in AODV and effect of Black Hole

Figure 2 shows the propagation of RREP packets in AODV. Route through node A, C, F and through node A, H, F both has same hop count and that too should be similar to the route through node B, E, G but in this scenario the bottom most route has an malicious node – node B. You can see that although actual hop count for this route should be 4 but this malicious node has sent RREP with 1 hop count. Now source will find that this route is the shortest one and transfer data through B but as B is the black hole it will drop all the packets instead of forwarding them. Although due to packet loss this problem will be detected eventually and source will re-route the packets but still it will harm the efficiency of the network considerably.

The biggest problem in detecting such errors quickly is that, such errors are mostly raised by neighboring nodes. If a single black hole is there neighboring nodes will identify the packet loss pretty quickly but it get worse when we have multiple black holes. In this scenario not only the packets are dropped but the neighbors who should detect and report the error also join the black hole in sending wrong information to the source. Such collaborative attacks are more difficult to find and does more damage to network performance.

Black Hole Detection

As we have we have the problem definitely solutions have to be looked for to keep our network working. There are different solutions proposed to identify the Black Hole in either single or collaborative attack. All have some different technique for identification and all have some or other advantages and disadvantages. Now we will try to compare some of the schemes to show how effective they are in improving the performance of the network. Some schemes are specific for Single Black Hole attack while some are used in detecting Collaborative Black Hole attack.

First we picked some schemes used to detect Single Black Hole attack.

1. Neighborhood Based and Routing Recovery

As the name suggests this is the combination of Neighborhood-based method and Routing Recovery protocol. It uses neighborhood based method to find the Black Hole and then Routing Recovery protocol comes into picture to establish new correct route. This method identifies the unconfirmed nodes as per neighborhood information and when any unconfirmed node is found source sends modified route entry control packet to establish new route.

Advantages:

Detection time is low
Achieved throughput is higher
Probability for accurate detection is achieved.

Disadvantages:

Based on public key infrastructure or still vulnerability is there in process of detection.
It fails when nodes co-operate in crating fake reply packets.

2. Redundant Route and Unique Sequence Number Scheme

To avoid the black hole attacks in MANETs, Mohammad Al-Shurman propose two solutions. First to find more than one route from source node to destination node assuming redundant nodes are available within the routing path. Author's assumption is that at least three routes are there in scenario. First source node sends a RREQ packet. All the receiver nodes having the route to the destination will reply with RREP packet. Now source node starts acknowledge examination and it will buffer the RREP packets sent by different nodes until at least 3 RREP packets are in buffer. After identifying the safe route it transmits the buffer packets. It shows that at least two paths are available to send data. After this source node selects the safe route by counting the number of hops. In second method a unique sequence number is used to identify the last packet sent to all nodes and another sequence number to identify the last packet received. On transmission or receiving of any packet these two values are updated automatically. By analyzing these two values a source can identify the presence of black hole. Second technique was to be found better than the first one.

Advantages:

Unique sequence number included with every packet contained in original routing protocol.
As per simulation it uses less RREQ and RREP packet than original AODV.
Inbound cryptography can reduce communication overheads.

Disadvantages:

Unique Sequence number could be changed by malicious node.
For co-operative attack both techniques fail to discover attack.

3. Time-based Threshold Detection Scheme

An enhancement to original AODV protocol is suggested by Latha Tamilselvan. The main concept is that after receiving the first request, set a timer for collecting other requests from other nodes in RimerExpiredTable. The packet sequence number and receiving time will be stored in Collect Route Reply Table (CRRT), counting timeout value as per the arrival time of first route request. Arrival time of first request and the threshold value will be used to determine that the route is valid.

Advantages:

Packet Delivery Ratio is higher.
Delay and overheads are minimal.

Disadvantages:

When malicious node is away from source end to end delay is quite high.
Not good to detect co-operative attack.

4. Detection, Prevention and Reactive AODV (DPRAODV)

DPRAODV is a modified variation of AODV. In this a new control packet is introduced which is called ALARM packet. It is used with dynamic threshold value to detect the attacker. In DPRAODV RREP sequence number is additionally checked to see if its value is higher than threshold value. If the condition is found true than the sender is supposed to be an attacker and included in black listed nodes. The ALARM packet which includes the blacklist is sent to the neighbors. All the RREPs from blacklisted nodes are blocked. The value of dynamic threshold is updated by calculating the average of destination sequence number between sequence number and RREP packet in each time slot. This scheme not only detects the black hole but also prevents it to update the threshold value for better protection.

Advantages:

Packet Delivery Ratio is improved by 80%-85%.
It can detect multiple black holes.

Disadvantages:

End to end delay is higher.
Routing overheads are also higher.
Can't detect co-operative attack.

Now I will try to present the results in tabular form so comparison will be easy to understand.

Table 1 – Comparison table for Single Black Hole Detection Schemes

Scheme	Effectiveness	Defects
Neighborhood Based and Routing Recovery	One attacker detection probability is up to 93%	Not successful on co-operative attack to create fake RReps.
Redundant Route and Unique Sequence Number Scheme	75% to 98% routes are verified	The tables can be updated for the last sequence number by listening to the network.
Time based Threshold Detection Scheme	For AODV Packet Delivery Ratio is around 80%. For Secure AODV it could be around 90% – 100%	If malicious node is away from source end to end delay increases.
DPRAODV	It improves PDR up to 80% - 85%	Routing Overheads and end to end delays is higher

All the schemes taken into consideration in above table 1 are used to detect single black hole attack but as we already know it's not the end of the problem. Instead of single black hole attack, network can be infected by collaborative black hole attack. In such attack all the techniques described are not very effective. To save our network from collaborative black hole attack, we have different techniques and some of those techniques are described below.

1. DRI table and cross checking using FREQ and FREP

The first technique we are taking into consideration modifies AODV a little bit. It uses an additional table called Data Routing Information (DRI) table and also uses two messages for cross checking called Further Request (FREQ) and Further Reply (FREP). Same as AODV at the time of need source node broadcasts a RREQ message to search the route to destination node. All the nodes which are receiving RREQ message re broadcast it until destination or a node which has the route to destination receives RREQ. This node replies with RREP message to inform the source about the route. All the intermediate nodes update their routing table as per RREP message and when RREP message is received on source, it updates routing table and start sending data using the route but in new method Source also updates Data Routing Information table with all the intermediate nodes. This data will be used with FREQ and FREP to detect black hole attack.

Advantages:

Packet Delivery Ratio is improved.
It can detect collaborative black hole attack.

Disadvantages:

End to end delay is higher.
Routing overheads are also higher.

2. Distributed Cooperative Mechanism (DCM)

As the name suggest DCM is a Distributed and Cooperative Mechanism to solve the problem of collaborative black hole attack. It is proposed by Chang Wu Yu. In DCM nodes can analyze, detect and mitigate multiple black hole attack by working cooperatively. DCM consists of four submodules – Local data collection, Local detection, Cooperative detection and Global reaction.

During local data collection phase each node creates and maintains an estimation table to evaluate the overhearing packets information and determine if there is a malicious node. If the node detects some suspicious node it starts Local Detection phase to confirm the existence of Black hole. In local detection phase the node which has detected suspicious activity asks a co-operative node by sending check packet. If co-operative node comes up with a positive reply then suspicious node is treated as normal node. If the value returned is not positive then Co-operative detection phase is triggered by the same initial node. In this phase initial node broadcasts to all one hop neighbors to notify them, so they all can join in decision making process. Although this notifying process is using constrained broadcast but still this broadcast wastes some of the communication resources. The hop count to be used for this broadcast is denoted as threshold. At last Global reaction phase is initiated and warning of black hole is sent to whole network.

Advantages:

Packet Delivery Ratio is improved by almost 30%.
Detection rate is higher, up to 98%.
It can detect collaborative black hole attack.

Disadvantages:

Too many broadcast messages.
Control overheads are higher.

3. MAC and Hash based PRF Scheme

This scheme to identify malicious nodes and to provide a secure route is proposed by Zhao Min and Zhou Jiliu. They proposed two hash-based authentication methods, one is Message Authentication Code (MAC) and other is Pseudo Random Function (PRF). These two methods are used to provide fast message verification and for group identification. It finds suspicious nodes participating in collaborative black hole attack and provide secure routing path to prevent the attack.

Advantages:

Packet Delivery Ratio is higher than 90%.
It can detect collaborative black hole attack.

Disadvantages:

As pause time raises, detection time increases.
Detection scheme could be affected, if malicious nodes forge a fake reply.
Control overheads are higher.

Now I will try to present the results in tabular form so comparison will be easy to understand.

Table 2 – Comparison table for collaborative Black Hole Detection Schemes

Scheme	Effectiveness	Defects
DRI table and cross checking using FREQ and FREP	Almost 50% higher throughput than the AODV	communication overheads of route requests are 5%-8% more
DCM	Almost 30% improved packet delivery ration with more than 98% detection rate.	Control overheads are higher
MAC and Hash based PRF Scheme	Packet Delivery Ratio is higher than 90%.	Detection scheme could be affected, if malicious nodes forge a fake reply

Conclusion

As we have seen in the paper, we two different type of Black Hole attacks and both are capable of affecting network performance. It's already clear that these attacks can be detected and alternative routes can be provided but that also at the cost of valuable resources. There are different schemes available to protect our network from these attacks and all of them has there pros and cons. So, when you choose a scheme always bear two things in mind, first it should provide quite a good PDR as well as it should not consume to much of the resources. If a scheme is providing very high throughput but consuming too much resources, it cannot be could especially in environment of MANETs where resources are already scarce. So, whenever choose a prevention scheme for Black hole either single or collaborative attack, just make sure to have a scheme with optimized solution with high throughput but still without consuming too much resources.

References

[1]. Niyati Shah, Sharada Valiveti, "Intrusion Detection Systems for the Availability Attacks in Ad-Hoc Networks", International Journal of Electronics and Computer Science Engineering, ISSN- 2277-1956, V1N3-1850-1857.

[2]. Hicham Zougagh, Ahmed Toumanari, Rachid Latif, Y. Elmourabit, "Discovering a Secure Path in MANET by Avoiding Black Hole Attack", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 5, No. 8, 2014

[3]. Disha G. Kariya, Atul B. Kathole, Sapna R. Heda, "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012.

[4]. Mr. K Chaitanya, Dr. S Venkateswarlu, "Detection of Black Hole & Grey Hole Attacks in MANET Based on Acknowledgement Based Approach", Journal of Theoretical and Applied Information Technology, ISSN: 1817-3195, 15th July 2016. Vol.89. No.1

[5]. H. A. Esmaili, M. R. Khalili Shoja, Hossein gharaee, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT), ISSN: 2221-0741, Vol. 1, No. 2, 49-52, 2011

[6]. Ketan Sureshbhai Chavda, "A Performance analysis of AODV under Blackhole Attack in MANET", International Journal of Technology in Computer Science & Engineering, Volume 1(2), June 2014, pp 82-87

[7]. Fatin Hamadah, M. A. Rahman, Thien Wan Au, "Performance Analysis of MANET under Black Hole Attack using AODV, OLSR and TORA", School of Computing and Informatics, Universiti Teknologi Brunei, Jalan Tungku Link, Gadong, Brunei Darussalam

[8]. B. Kondaiah, Dr. M. Nagendra, "A Black Hole Attack on Performance of AODV Routing Protocol in Manet", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 11, November 2015

[9]. Nidhi Gupta, Sanjoy Das, Khushal Singh, "A Comprehensive Survey and Comparative Analysis of Black Hole Attack in Mobile Ad Hoc Network", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:1, 2014