International Journal of Future Generation Communication and Networking
Vol.10, No.9 (2017), pp.37-48
http://dx.doi.org/10.14257/ijfgcn.2017.10.9.04

Study of Black Hole Attack in AODV

Shariq Aziz Butt* and Tauseef Jamal

PIEAS University Islamabad Pakistan
Shariq2315@gmail.com, jmltsf@gmail.com

Abstract

The Mobile Ad-hoc Networks (MANETS) are decentralized, multi-hop networks where the intermediate nodes act like routers to pass data packets to destination. The Routing protocols are playing very vital role in effectiveness of MANETS due to mobility and dynamically changing of topology. Now many routing protocols are susceptible to attacks because of the nature of broadcast wireless medium and not have central control. Ad hoc On-Demand Distance Vector routing (AODV) is a very trendy routing protocol and it is very susceptible to black hole attacks. In black hole attack a mobile node mistakenly publicize the route and sinks data packets to incorrect destination instead of sending to accurate destination. Hence the paper is in context of black hole attacks in AODV. It analyzes the related work and position a solution based on analysis.

Keywords*: Ad hoc networks; routing; black -hole attack; malicious node; packet dropping*

1. Introduction

Wireless network is direct or indirect communication between two digital devices which are not physically connected to each other. Nowadays the requirement of mobility and roam free connectivity demand of wireless networks has risen rapidly. Over the last few decades' the bandwidth, range and reliability of wireless network has been boosted by the research and development. The users are more dependent on wireless communication in the form of wireless electronic gadgets. As a matter of fact, these devices have advantages and usability according to the state of the art environment.

Wireless networks have few major advantages (Five Reasons to Go Wireless) such as increased mobility and collaboration, improved responsiveness, better access to information, easier network expansion and enhanced guest access. Many advantages are evolved in wireless networks in last century but major changes evolved in last two decades. In spite the advantages, usability and enhancement of wireless networks, the issues in wireless networks still present. Some of the issues (such as overhearing, protocols design *etc.*,) are used by attackers to launch attacks on wireless networks.

Ad hoc networks are also a category of wireless networks, which are easy to deploy because they don't need any fixed communication path such as routers, access points and base stations. These types of networks have the shared medium; they have self-organizing nature and consist of small nodes. Thus they can connect rapidly with other nodes to create ad hoc network. That is why they are flexible and can be used in places where sensors are deployed such as hospitals, industries and city monitoring environments.

Received (April 7, 2017), Review Result (August 4, 2017), Accepted (August 25, 2017)

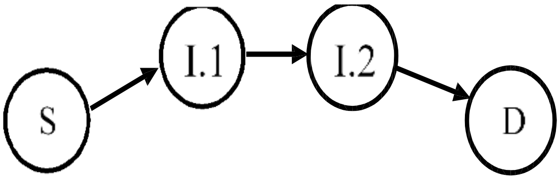


Figure 1. Multi-hop Ad Hoc Network

MANETS are the type of networks which can establish connectivity on ad hoc basis. Nodes in MANET are quite cooperative to create a routed network. These networks can be counted in type of multi hops networks. In such networks the nodes that interconnect source to destination are known as intermediate nodes, they create route from source to destination. There can be multiple routes to destination but priorities are assigned to routes on basis of various factors such as hop count, energy, bandwidth and reliability of channels for every hop. The above Figure 1 is presentation of an example of a route between source node and destination node. In the figure the S is denoting the source and D is denoting destination where the data has to reach. The route consists of 3 hops, where the data packet passes via node 1.1 and node 1.2 to reach the final destination.

As a matter of fact, there are multiple nodes which communicate over an open and shared medium through different channels; security, transmission and delivery are major concerns. Many routing protocols are introduced in MANETS such as Ad-Hoc On-Demand Distance Vector (AODV), Optimized Link State routing (OLSR) (OLSR.org, 2004), Dynamic Source Routing (DSR), Border cast Resolution Protocol (BRP) and hybrid Zone Routing Protocol(ZRP). AODV and OLSR are both accepted as experimental RFCs by the IETF and they are probably the two most popular MANET routing protocols at the current time (OLSR.org, 2004).

Both protocols DSR and AODV designed too earlier even at a time when security was not major issue but now a day's security and reliability is major concern. There are many security issues that can be listed but black hole, wormhole, gray hole and sinkhole attacks are now a day's common attacks. The remaining part of the paper is organized as following. In Section II, we will explain the black hole attack, while in Section III we explain AODV protocol in detail. Section IV covers the related work, while in Section V we analyze the related work and propose a solution. Finally, Section VI concludes the paper.

2. Black Hole Attack

In networking, sink hole points to a malicious activity or failure in which incoming or outgoing data is dropped without any responses to source about data delivery. In MANETS the attack can be initiated by some external entity. The external entity that configured the node tries to deliver a fake response related to delivery that didn't take place. The configuration of malicious node depends upon network topology that is created on ad hoc basis but also depends upon the routing protocols.

Black hole attack is closely related to the packet drop attack and little bit related to sink hole and gray hole attack all of these attacks leads a system to denial of services. Black hole attack is mainly layering 3 attacks, i.e. attack in routing protocols. For that reason, black hole attack has strong impact on MANETS and this is because of these routing protocols Ad-Hoc On-Demand Distance Vector (AODV) or Optimized Link State routing (OLSR) that used by MANETS. These protocols face different security threats to target their performance and services.

OLSR is mostly used proactive routing protocol, that floods topology table of its neighbors to all nodes in network which than compute the optimal forwarding path. OLSR takes too much time to rediscover upon reconnecting a broken link, doesn't handle distribution delay of packets and more processing power is required to discover an alternate route. AODV one the other hand is reactive routing protocol for on demand routing that's why this protocol has less overhead [1], which makes it better than OLSR. It is capable to unicast and multicast routing.

A. Black Hole Attack in Nutshell

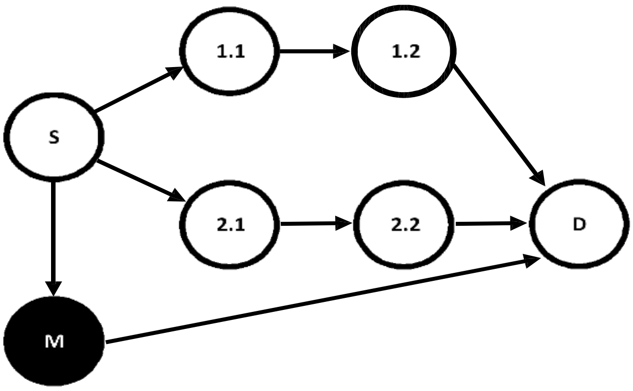


Figure 2. Black Hole Attack Example 1

In black hole attack there is a spiteful node that tries to introduce itself as an intermediate routing node in such a way that provides selfish data about routing decision. This node doesn't care about priority of data, source and destination. The node is specially designed to keep performance blacked out if traffic is passing through it. This node pretends to be nearest to the destination *i.e.*, showing minimum hops. The Figure 2 is explaining the malicious node M with shortest path to destination D.

Black hole is one of most effective and shocking routing attack in ad hoc networks. Sometimes such attacks mislead the whole network where all nodes prefer to pass data and connection through the malicious node (c.f., Figure 3), making the network to be choked.

AODV is widely used in MANETS due to its instant connectivity however; it is prone to various attacks especially to black hole [2]. In AODV when a source request for route to particular destination then at that time the intermediate nodes re-broadcast the request in order to reach the destination. The spiteful node is intermediate node that sends a quick response result back to the source to make sure that destination has been found. Source starts sending data packets to destination but malicious node receives and drop packets. In order to identify and mitigate the black hole attack, it is necessary to understand the routing protocol implementation; therefore, in next section we study the AODV in detail.

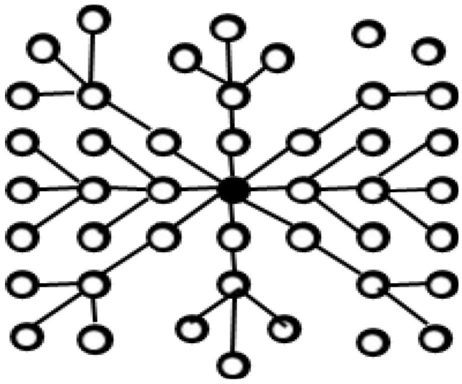


Figure 3. Black Hole Attack Example 2

3. AODV PRPTOCOL

3.1. Operations

AODV algorithm is designed for self-organizing, dynamic and multi-hop routing between two or more participating mobile nodes in MANETS. Till now AODV is the best for quick response to obtain fast, reliable and suitable route for new destinations. Also in this algorithm it doesn't require to compute route in advance but this has been designed for instant routing as it is required. When a link breaks during transmission and information sharing AODV notify all nodes to invalidate the route.

From many of AODV's features one feature is that the AODV use a sequence number of destination to enter route. This destination sequence number is created by destination which is included along with any route information sent to source node.

In order to establish a route, AODV define 3 types of messages as given below:

1. Route Requests (RREQs)
2. Route Replies (RREPs)
3. Route Errors (RERRs)

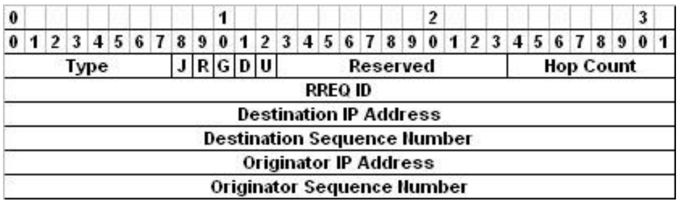
AODV is an on-demand routing protocol in which route discovery process starts when it is demanded. AODV operation includes two phases; one is route discovery and second is route maintenance. The first discovery route phase is started when a source node need to deliver packets to destination and the destination entry doesn't exist in table called routing table (RT). Hence the source node broadcasts a request for route called route request (RREQ) to neighbor nodes in network. When all these neighbor nodes receive RREQ then nodes check their RT if the destination entry exists or not. When RREQ message is received the intermediate nodes update their routing table forming reverse route to the source. The intermediate nodes then increment the hop count for distance vector and forward new RREQ to its neighbor to get to destination. This procedure of sending RREQ repeats until destination is found. In the next step the Route Reply (RREP) message is sent by intermediate node or destination node to the source node to establish route.

AODV is different from other reactive routing protocols because it uses the sequence number to determine the fresh route. Every entry in routing table RT is associated with a sequence number which acts like timestamp for the route to determine the freshness of route. When the intermediate node is received the RREQ message then the intermediate node compare sequence number of incoming RREQ message with its existing sequence number and if the sequence number of message is greater then the intermediate node updates its route.

3.2. Message Formats

3.2.1 Route Request RREQ

This message originated from source to the destination by broadcast protocol as discussed already. This message size is 192 to 256 bits which is subdivided into blocks of 32bit size. And every block contains specific information that is predefined by AODV and presented by the Figure 4 while details are listed in Table 1.



0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type								J	R	G	D	U	Reserved											Hop Count							
RREQ ID																															
Destination IP Address																															
Destination Sequence Number																															
Originator IP Address																															
Originator Sequence Number																															

Figure 4. RREQ Message Format

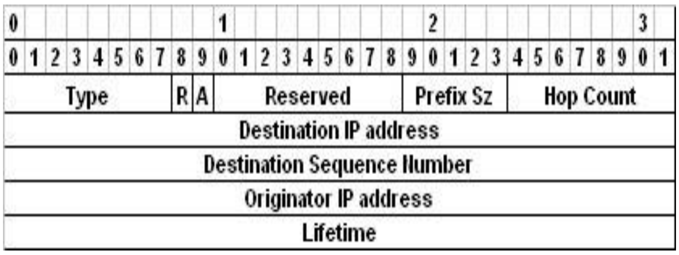
Table 3. RREP Message Format Details

<table>
<tr><td>Name</td><td colspan="2">Description</td><td>Size (bits)</td></tr>
<tr><td>Type</td><td colspan="2">1 (fix)</td><td>8</td></tr>
<tr><td>J</td><td>Join flag; multicast reservation.</td><td>
<table>
<tr><td>D</td><td>only Destination flag; this flag only indicates destination may respond to this route request.</td><td>1</td></tr>
<tr><td>U</td><td>Unknown sequence number; which indicate that the destination sequence number is unknown.</td><td>1</td></tr>
<tr><td>Reserved</td><td>Sent as 0 and is ignored on reception.</td><td>11</td></tr>
<tr><td>Hop Count</td><td>The hop count represents the number of hops from IP Address creator to the node handling request.</td><td>8</td></tr>
<tr><td>RREQ ID</td><td>Route request ID is a sequence number that is exclusively identify the exacting route request when it is taken in conjunction with the creator node's IP address.</td><td>32</td></tr>
<tr><td>Destination IP Address</td><td>To desire the route the IP address for destination is required.</td><td>32</td></tr>
<tr><td>Destination Sequence Number</td><td>The sequence number that is received in past from originator for any route towards destination.</td><td>32</td></tr>
<tr><td>Originator IP Address</td><td>The IP address of the node which originated the Route Request to send data to destination.</td><td>32</td></tr>
<tr><td>Originator Sequence Number</td><td>The sequence number is used in the route entry pointing.</td><td>32</td></tr>
</table>
</td><td>1</td></tr>
<tr><td>R</td><td colspan="2">Repair flag; for multicast.</td><td>1</td></tr>
<tr><td>G</td><td colspan="2">Gratuitous RREP flag; the flag represent that whether a gratuitous RREP should be unicast to specified node in the Destination IP Address field.</td><td>1</td></tr>
</table>

D	only Destination flag; this flag only indicates destination may respond to this route request.	1
U	Unknown sequence number; which indicate that the destination sequence number is unknown.	1
Reserved	Sent as 0 and is ignored on reception.	11
Hop Count	The hop count represents the number of hops from IP Address creator to the node handling request.	8
RREQ ID	Route request ID is a sequence number that is exclusively identify the exacting route request when it is taken in conjunction with the creator node's IP address.	32
Destination IP Address	To desire the route the IP address for destination is required.	32
Destination Sequence Number	The sequence number that is received in past from originator for any route towards destination.	32
Originator IP Address	The IP address of the node which originated the Route Request to send data to destination.	32
Originator Sequence Number	The sequence number is used in the route entry pointing.	32

3.2.2. Route Reply RREP

In route reply there is slightly difference in message format it also consists of 160 to 256 bits however it has the minimum size of 160 bits. RREP message format is given in Figure 5 and details are given in Table 2.



0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type | R | A | Reserved | Prefix Sz | Hop Count

Destination IP address

Destination Sequence Number

Originator IP address

Lifetime

Figure 5. RREQ Message Format

Name	Description	Size (bits)
Type	2 (fix value)	8
R	Repair flag	1
A	Acknowledgment required	1
Reserved	Sent as 0 and is ignored on reception.	9
Prefix Size	If Prefix Size is nonzero then 5-bit Prefix Size specify that the indicated next hop used for any node is with the same routing prefix destination.	5
Hop Count	The hop count is the count of number of hops from the Originator IP Address to the Destination IP Address.	8
Destination IP Address	Is the destination address to for route.	32
Destination Sequence Number	Destination sequence number the number is associated with route.	32
Originator IP Address	The originator create an IP address for route request in route.	32
LifeTime	The time period in milliseconds for node to receive route request for valid route.	32

3.2.3. Route Error RERR

RERR message is sent if there is route error or destination is not found. This message consists of 96 bits and can be extended to 256 bits for additional information. The bit format of this message is given in Figure 6 and description is given in Table 3.

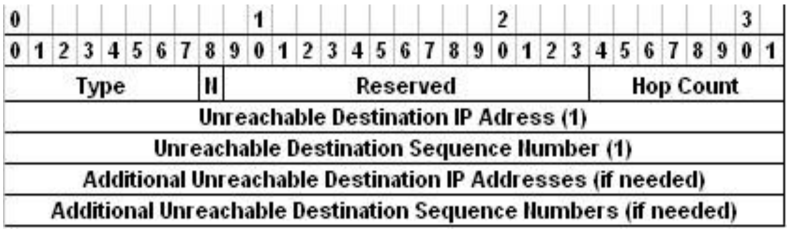

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
N
Reserved
Hop Count
Unreachable Destination IP Adress (1)
Unreachable Destination Sequence Number (1)
Additional Unreachable Destination IP Addresses (if needed)
Additional Unreachable Destination Sequence Numbers (if needed)

Figure 6. RERR Message Format

IP Address	Smash.	
Unreachable Destination Sequen	Is the sequence number in the route table entry for the destination unreachable Destination IP Address field.	32

4. AODV Operations

In MANETS there can be multiple routes from source to destination through numerous intermediate nodes similarly each intermediate node can be part of multiple path as shown in Figure 7. For example, there are two paths passing through node C, one is S→C→B→D and other one that is possible through C is S→C→E→D. Now C has two paths to destination D, which path has to be selected to route through D, according to the AODV the decision is based on hop count as well as fresh route (*i.e.*, sequence number).

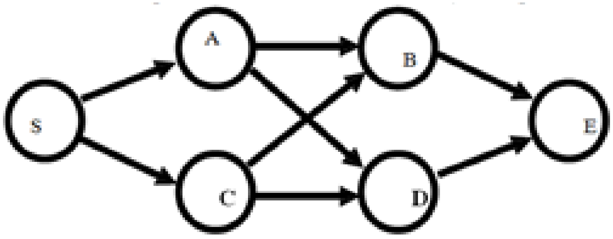


Figure 7. AODV Example 3

5. Black Hole Attack in AODV

There are two phases of this attack which take place sequence, in first phase malicious node detects routing algorithm such as AODV and participate by showing that it is intermediate node and can be trusted because it is nearest to destination. In second phase it shows fake establishment of route by minimum hop count and high sequence number. As a result it starts receiving packets from the source and drops these packets without forwarding them.

6. Related Work

This section includes the discussion of some suggestive solutions presented by many different researchers to detect black hole attacks in MANETS. Ramaswamy *et al.*, [1] is one of these researcher and he address that the multiple black hole in a group can attack synchronize and he present a technique to identify multiple black hole's cooperation with each other to attack and solve by discover a solution that is safe route to avoid the cooperative black hole attack. Kurosawa *et al.,* [2] is an other researcher and he suggested an anomaly detection scheme by using dynamic training method. In this technique the training data is updated at standard time intervals. Tamilselvan *et al.*, [3] researcher proposed an approach to fight with the black hole attack that make sense of a 'Fidelity Table'. In the table every node assigned a fidelity level to measure the reliability of those participating nodes. When any nodes which measure level fall down to 0 then it is considered as a malicious node (Black Hole) and departed. Weerasinghe *et al.*, [4] proposed a solution to declare and safe the route from cooperative black hole attack. This proposed solution finds and indentify the safe and secure path/route between source and destination. Ming Yang Su *et al.*, [5] proposed an intrusion detection system to alleviate the black hole attacks in MANETS. In this solution the node set in a mode called sniff mode to perform the ABM (Anti-Black hole Mechanism) function and in this function the node is mainly used to detect the suspicious value of a node which is according to abnormal difference between the routing messages transmitted from node and when this suspicions values exceed from a threshold value then nearest IDS broadcast a message called block message. The purpose of this block message is to inform all nodes on that network and ask all nodes to cooperatively isolate the malicious node. Gupta *et al.*, [6] is proposed a protocol to avoid black hole attack without the use of special hardware and dependency on physical medium of wireless network. This protocol establish a link disjoint multi-path during finding of route to provide higher path selection in order to avoid malicious nodes in the path by the using legitimacy table that is maintained by every node in network. Non-malicious nodes slowly but surely isolate the black nodes based on the values collected in their legitimacy table and avoid them while making route between source and destination. Rutvij Jhaveri *et al.*, [7] proposed a method for AODV protocol in this method an intermediate node detects the malicious node by sending some false information such as routing information and routing packets. This routing packet not only used to pass the routing information but also use to pass the information about malicious nodes in network. The main goal of this method is not only detect malicious nodes on other hand remove these entire malicious node and make the communication path/route safe and secure. Nabarun Chatterjee *et al.*, [8] proposed a technique to avoid black hole in AODV routing protocol using Triangular Encryption in NS2. In this triangular encryption technique computation level is low a head. Saryvuth Tan *et al.*, [9] proposed a mechanism that works with the source code and destination node. In this mechanism sequence number in the RREQ and RREP messages in verified and after the confirmation/verification the communication path set between the source and destination to transfer data. This section includes the discussion of some suggestive solutions presented by many different researchers to detect black hole attacks in MANETS. Ramaswamy *et al.*, [1] is one of these researcher and he address that the multiple black hole in a group can attack synchronize and he present a technique to identify multiple black hole's cooperation with each other to attack and solve by discover a solution that is safe route to avoid the cooperative black hole attack. Kurosawa *et al.*, [2] is an other researcher and he suggested an anomaly detection scheme by using dynamic training method. In this technique the training data is updated at standard time intervals. Tamilselvan *et al.*, [3] researcher proposed an approach to fight with the black hole attack that make sense of a 'Fidelity Table'. In the table every node assigned a fidelity level to measure the reliability of those participating nodes. When any nodes which measure level fall down to 0 then it is considered as a malicious node (Black Hole) and departed. Weerasinghe *et al.*, [4] proposed a solution to declare and safe the route from cooperative black hole attack. This proposed solution finds and indentify the safe and secure path/route between source and destination. Ming Yang Su *et al.*, [5] proposed an intrusion detection system to alleviate the black hole attacks in MANETS. In this solution the node set in a mode called sniff mode to perform the ABM (Anti-Black hole Mechanism) function and in this function the node is mainly used to detect the suspicious value of a node which is according to abnormal difference between the routing messages transmitted from node and when this suspicions values exceed from a threshold value then nearest IDS broadcast a message called block message. The purpose of this block message is to inform all nodes on that network and ask all nodes to cooperatively isolate the malicious node. Gupta *et al.*, [6] is proposed a protocol to avoid black hole attack without the use of special hardware and dependency on physical medium of wireless network. This protocol establish a link disjoint multi-path during finding of route to provide higher path selection in order to avoid malicious nodes in the path by the using legitimacy table that is maintained by every node in network. Non-malicious nodes slowly but surely isolate the black nodes based on the values collected in their legitimacy table and avoid them while making route between source and destination. Rutvij Jhaveri *et al.*, [7] proposed a method for AODV protocol in this method an intermediate node detects the malicious node by sending some false information such as routing information and routing packets. This routing packet not only used to pass the routing information but also use to pass the information about malicious nodes in network. The main goal of this method is not only detect malicious nodes on other hand remove these entire malicious node and make the communication path/route safe and secure. Nabarun Chatterjee *et al.*, [8] proposed a technique to avoid black hole in AODV routing protocol using Triangular Encryption in NS2. In this triangular encryption technique computation level is low a head. Saryvuth

Tan *et al.,* [9] proposed a mechanism that works with the source code and destination node. In this mechanism sequence number in the RREQ and RREP messages in verified and after the confirmation/verification the communication path set between the source and destination to transfer data.

7. Analysis

As in previous section, we discussed some solutions proposed by different researches to countermeasure the black hole attack. In this section we will discuss the drawback of some of these solutions so that this study will help the readers to keep these side effects in mind and propose a more efficient solution to detect black hole attack.

The first drawback which exists in most of the solutions is the delay in route discovery process. Because most of the solutions add additional functionality in order to verify the route. This delay affects the network efficiency. Secondly, some solutions add extra traffic to the network by introducing new packets for the destination verification through other routes. These additional packets cause congestion in the network. The third side-effect which can exist in black hole solutions is to make the decisions based on the neighboring nodes by the process of voting or by calculating the trust value. In these kinds of solutions, a malicious node can provide the fake trust values of legitimate nodes to declare them malicious. The fourth negative effect which can be present in a solution is the use of additional hardware which increases the complexity of the network as well as the cost of the network. By keeping in mind the above cones, we require a solution which will not add delay in route discovery, making congestion in network, increase false positive rate and/or will not increase the cost of network. In our opinion a solution can perform better if it uses two or more parameters for detection of black hole nodes. These parameters can be the previous history of the source and destinations nodes and the trust values collected from the neighboring nodes.

8. Conclusions

Wireless networks developed rapidly during last decade and are making our lives much easier. Mobile ad hoc networks are infrastructure fewer networks are a common form of wireless networks. In MANETS routes are established through intermediate nodes as each node also work as router. There are special routing protocols used for MANETS, AODV is the one of the most common protocol used. Due to their wireless nature, MANETS has much vulnerability and are prone to different attacks. The one of the very famous attack on wireless network is the black hole. In which a malicious node attracts traffic toward itself by advertising the fake hop count and sequence number. Black hole node drops all the data which it receives from other nodes. In this paper, we presented the basic information about black hole attack and the AODV routing protocol. We have discussed some solutions proposed by different researchers to countermeasure the black hole attack. We identified some of the side effects of these solutions which reduce the network efficiency and make it more complex and expensive. We also proposed a solution which will work based on two parameters; history and trust value to validate the route. We hope this study will help the researchers who are working on MANETS security.

References

[1] S. R. Wany, H.-R. Fu, M. Sreekantaradhya, J. Dixon and K. Nvgard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Netwroks”, International Conference on wireless networks (ICWN), **(2003)**; Las Vegas.

[2] S. Kurosawa, H. Nakayama, N. Karo, A. Jamalipour and Y. Nemoto, “Detection Black Hole Attack on AODV- based mobile Ad-hoc network by dynamic learning method”, International Journal of Network Security, vol. 5, no. 3, **(2007)**.

[3] L. Tamilselvan and V. Sankaranayaranan, “Prevention of Co-operative Balck Hole Attack in Manet”, Journal of Networks, vol. 3, **(2008)**.

[4] H. Weerasinghe and H.-R. Fu, “Preventing Coperative Balck Hole Attack in Mobile Ad-hoc Networks: Simulation, Implementation and Evaluation”, International Journal of Software Engineering and Its Applications, **(2008)**.

[5] M. Y. Su, K.-L. Chiang and W. Chang, “Mitigation of Black Hole Nodes in Mobile Ad-hoc Networks”, International Symposiums of Parallel and Distributed Processing with Application, **(2010)**.

[6] S. Gupta, S. Kar and S. Dhamaraja, “BAA: Black Hole Avoidance Protocol for Wireless Network”, Internation Conference on Computer and Communication Technology (ICCCT), **(2001)**.

[7] H. Rutvjj, S. Jhaveri, J. Patel and D. C. Jinwala, “A Novel Approach for Grayhole and Black Hole Attacks in Mobile Ad-hoc Networks”, Second international Conference on advanced computing and communication technologies, **(2011)**.

[8] N. Chatterji and J. K. Mandel, “Detection of Black Hole Behavior Using Triangular Encryption in NS2”, Ist International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), **(2013)**.

[9] S. Tan and K. Kim, “Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETS, ICT convergence (ICTC) International Conference, **(2013)**.

[10] C. E. Perkins and E. M. Royer, “Ad-hoc on Demand Distance Vector Routing, Mobile Computing Systems and Applications”, Second IEEE Workshop WMCSA, **(1999)**.