International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

# A Review on Implementation of AODV Technique for Isolation of Gray Hole Attack in MANET

**Er. Shalika[1], Dr. Jatinder Singh Bal[2], Dr. Vijay Dhir[1]**
[1]Computer Science Engineering Sant Baba Bhag Singh University Jalandhar, Punjab, India
[2]Prof .Computer Science Engineering Sant Baba Bhag Singh University Jalandhar, Punjab, India

## ABSTRACT

The mobile ad hoc network is the decentralized and self-configuring type of network in which mobile nodes can join or leave the network when they want. Due to decentralized nature malicious nodes enter the network which is responsible to trigger various type attacks. The security attacks reduce network performance in terms of various parameters. In this paper, various techniques are reviewed to increase security of the mobile adhoc networks .

**Keywords :** MANETS, Gray Hole, Active, Passive

## I. INTRODUCTION

A network is a group of two or more computer systems which linked together. It is mode of exchange of information to communicate with one another. It is a connection of computer devices which are attached with the communication facilities [1]. When number of computer are joined together to exchange information they form networks and share resources. Networking is used to share information like data communication. Sharing resources can be software type or hardware types. It is central administration system or supports these types of system [2].

Different types of networks are as following:

1. Transmission media based networks like wired network and wireless network. Network Size based network like MAN, and WAN.

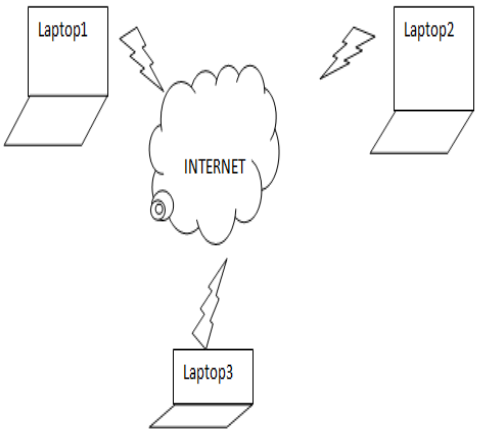


**Figure 1.** Diagrammatically representation of Computer Networks.

2. Management based networks like peer-to-peer and client/server
3. Topology based networks called connectivity like bus, star, ring topology.

### 1.1 Wireless Networks

Wireless Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication.. The IEEE standard for wireless network is 802.11. Wireless

Networking is a technology in which two or more computers communicate with each other using standard network protocols and without the using of cables [3].

There are two types of Wireless Operating modes:

1. Infrastructure Mode
2. Adhoc Mode or Infrastructure less Mode

### 1.1.1 Infrastructure Networks:

In infrastructure based network, communication is takes place only between the wireless nodes and the access points. The communication is not directly takes place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks.

### Infrastructure less Networks:

The infrastructure less network does not need any infrastructure to work. In this network each node can communicate directly with other nodes. So in this network no access point is required for controlling medium access [5]. Here Figure shows a simple peer to peer network with three nodes. The outermost node is outside of transmitter range of each other. To forward packets between the outermost nodes, the middle node can be used. Three nodes have formed an ad-hoc network middle node is behave like a router [6]. It is of three types. The subcategories are given below:

1. Wireless Sensor Networks
2. Manet
3. Wireless Mesh Network

### 1.1.2 Ad hoc network:

Ad hoc network is the separate type of wireless network. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it is depended Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. All the nodes act as router in adhoc network. The wireless network offers certain advantages over the wired networks that are as follows [7].

### Classification of Adhoc networks:

There are two types of classification available in adhoc networks which are as following:

1. Single-hop
2. Multi-hop

**Single-hop:** In this hop nodes are in direct communication and both nodes are in range of each others. The chances of link failure are more in this hop [8].

**Multi-hop**: In this hop nodes are communicate with the help of internal nodes not directly. To reach from source to destination internal nodes participate.

### Types of Adhoc Network:

There different types of adhoc network available. These are as following:

1. MANET
2. Wireless Sensor Networks (wsn)
3. Wireless Mesh Networks (wmn)

### 1.1 MANET

MANET stands for the Mobile Ad hoc Network. It is the robustness infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly linked with each other and forming arbitrary topology [9]. They can act as both routers and hosts.

1. OLSR (Adhoc on Demand Distance vector)
2. DSR (Dynamic Source Routing)
3. OLSR (Optimized Link State Router)
4. Wireless Routing Protocol (WRP)
5. Zone Routing Protocol (ZRP)

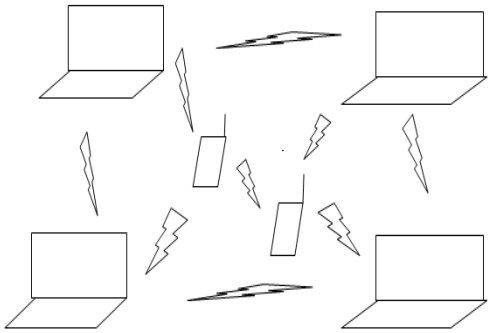

**Figure 2.** Diagram of MANET

### 1.2.2 Attacks on MANET [11]:

There are two types of the attacks are presented in the MANET which break the security of the networks. These attacks are as follow:

1. Passive Attacks
2. Active Attacks

### 1. Passive Attacks:

A passive attack obtains data exchanged in the network without upsetting the connected operation. The passive attacks are difficult to detection. In its, operations are not affected. The operations can be supposed to be sharp by a malicious nodes of the ignored and essay to recoverable benefical data during listens to the channel [12]. Examples of Passive Attacks are eavesdropping, snooping etc.

### 2. Active Attacks:

An active attack is that attack which any data or information is inserted into the network so that information and operation damage. It involves adjustment, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing [13].

### 1.3 Routing Protocols in MANET:

Routing protocol specifies how to connect with help of the routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest route from source to destination [14]. There are mainly two types of routing protocol available. These are two protocols as following:

1. Proactive Routing Protocol ( Table-driven)
2. Reactive Routing Protocol (On- demand)

### 1. Proactive Routing Protocol:

Proactive protocol contains fresh list of the route and their destination from source. In this type of protocol one node contains more than one table for each node in the network. All the nodes are update regularly [15]. If the topology frequently changes than update information propagate to every node of the network and update table.

### 2. Reactive Routing Protocol:

It is on-demand protocol. It is lazy approach in which all the node are not contains the information of the all the nodes and maintains table only on demand. To find the path route discovery process is follow. Reactive routing protocols are bandwidth efficient. In this, routes are built as and when they are required. This is achieved by sending route requests across the network. There are disadvantages with this protocol that it offers high latency when finding routes and other is the possibility of network clog when flooding is excessive. In this thesis, we considered OLSR, DSR and DSDV [16]

### A. Adhoc On-demand Distance Vector

OLSR is an on-demand routing protocol used in ad hoc networks. This protocol is like any other on-demand routing protocol which facilitates a smooth adaptation to changes in the link conditions. This one is the distinguishing feature of this protocol. Requesting nodes in a network send Destination Sequence Numbers (DSNs) together with all routing information to the destination. It selects the optimal route based on the sequence number [17].

### B. Dynamic Source Routing

DSR is a reactive routing protocol for ad hoc wireless networks. It also has on-demand features like OLSR

but it's not table-driven. It is based on source routing [19]. The Dynamic Source Routing protocol is the smoothing designed by the specifically for use in multi-hop wireless adhoc networks of the mobile nodes and efficient routing protocols. DSR allows the network to be fully self-organizing and self-configuring.

## II. LITERATURE SURVEY

**Lalar Sachin ,Arun Kumar Yadav (2018),** There are the various kind of routing protocols presented for the ad hoc networks and these can be categorized in three schemes: Proactive, Reactive routing protocols and Hybrid protocols. In MANET, the routing protocol should be capable to handle a very large number of nodes with limited resources. The main issue associate with the routing protocos of the l involved being acrose and leave of nodes in various locations. It is necessary to reduce routing message overhead despite the increasing number of nodes.

**Meenakshi Patel et.al (2017),** projected [39] in this paper a mechanism for defeding the malicious attack that occurs within the AODV. This is done here with the help of involvement of SVM and three other metrics that are Packet Delivery Rate (PDR), Packet Modification Rate (PMR) and Packet Misroute Rate (PMISR). These parameters are utilized for deciding the behavior of the node. From all nodes present within the network the information is gathered by these respective metrics. Against the threshold parameter all the values are checked and the malicious node is detected in this manner. This method is simple and has higher speed. It provides a quick response for the nodes that are suspicious or are the malicious nodes for sure.

**Jaspal Kumar et.al (2017),** analyzed [40] in this paper the effect of the black hole attack towards the routing protocols. The AODV as well as Improved AODV protocols are utilized here. The multipath is supported by the Improved AODV in which the route discovery is very important when all the routes are expired. It is seen through the experimental results that the IAODV is very less affected by the black hole attack as compared to the AODV. There is an enhancement in the packet delivery ratio of IAODV with an increment in the routing overhead that is prevented by handling the black hole attack within the network.

**Sisily Sibichen et.al (2016),** demonstrated [41] that there is a need of authentication keys in the ad hoc networks for providing security. The spanning tree is also utilized within the proposed method for providing communication amongst the member of nodes within the network. There is a different certificate for each of the node and the certificate is signed only by the trusted party that is the third party. The base for all the communications between the nodes is provided by this certificate. The certificate is checked for authenticity by the receiving end before it is received. Once there is an exchange of the certificates the secret keys are also exchanges here that can further be utilized for encryption and decryption of the messages. The secure communication is provided through this method in the network along with the increment in throughput and packet ratio within the network.

**Pramod Kumar Singh et.al (2016),** proposed [30] a scheme in this paper that can prevent the network from the malicious nodes that can cause black hole attacks within mobile ad hoc networks. The malicious node is detected using the promiscuous mode within the proposed method. The information related to the malicious node is detected and propagated with the help of such modes. Within the network the RREQ packet is flooded within the source node. For establishing a new route RREP packet is required for which the node waits. Once the RREP is received from the intermediate node, the node moves to the promiscuous mode and sends a

hello message again to the destination node. The node is safe if the intermediate node forwards the message to the destination node. In other case, the node is malicious and there is no need of extra processing power or database within the network.

**Humaira Ehsan et.al (2012),** elaborated [31] the study related to different kinds of attacks present within MANET. NS2 tool was utilized for simulation of these attacks. The inferences of various attacks were generated on the basis of the impact that they leave on the network in terms of various parameters. Between the source and destination if the attacker node is present, the performance of the network can be degraded due to the malicious node present. There would be less impact of the malicious node on the network if the communication amongst source and destination is taking place on another part and the attacker is on the completely different part of the network.

**Fidel Thachil et.al (2012),** proposed [32] in this paper a novel technique for detecting and isolating the malicious nodes from MANETs. On the basis of trust factor that is computed for each node in perspective of the neighboring nodes, the recognition and isolation of the malicious nodes from the networks is done. Through the ratio calculated between the number of packets received by the node and the number of packets dropped by it, the trust value is computed. There is a trust value for each node. There is a fixed threshold value that is setup within the network. The node is considered to be malicious below this threshold value and is then removed from the reliable routes. The information related to malicious node is broadcasted in the rest of the network for taking security measures against it. As compared to the original AODV this method is much better. Even when the malicious node is present in the network, the packet is delivered in an efficient manner within the network through this method.

**Kundan Munjal et.al (2012),** proposed [33] in this paper a new method for detecting the black hole nodes within the network. The information related to the malicious nodes is to be displayed across the network. There are three different conditions presented within the network to run various tests and experiments. The first case has no malicious nodes involved in it and so the route is known to be reliable for exchange of data packets. There are two cooperating malicious nodes identified within the secondary case. Within the complete network this whole information is broadcasted. In the thirst case, if the node is reliable, the information related to its reliability if passed across the whole network. In all the situations the proposed network is beneficial and it helps in preventing the network from black hole attack. A reliable route is thus established from source to destination. There is a need to enhance the algorithm however in terms of end-to-end delay and routing overhead.

**Rutvij H. Jhaveri et.al (2012),** proposed [34] in this paper a new method that involves the utilization of intermediate nodes for detecting and isolating the malicious nodes on the basis of the sequence number. The RREP packets are sent back to the source node in the reverse path within the AODV. Through the destination node the RREQ packet is received. The packet is discarded if the sequence number is less that the table of the node and is accepted if it's higher. The calculation of PEAK value is done through the intermediate node with the help of various parameters such as routing table, sequence number, RREP sequence number and the number of replies at certain time interval. The PEAK value is the maximum possible value of sequence number. The packet is labeled as 'do not consider' if the sequence number is higher than the PEAK value in case of the RREP packet received. This packet is then forwarded in the reverse path. Thus, this method detects the malicious node within the network and notifies the rest of the nodes in the network. Thus, when a route

is to be selected from source to destination, this node is not involved.

**Nidhi Sharma et.al (2012),** presented [35] in this paper the various solutions that can be utilized for avoiding black hole attack in MANET. There is an initial solution proposed in this paper that has numerous routes to destination. With the help of numerous routes a unicast ping packet is also sent to the destination. Decision is made related to selection of route for communication when the replies are checked that are being received from the various routes. For verifying the legitimate node within the secondary approach, the sequence number is utilized. For the purpose of recording the sequence number of the forwarded packets there are two extra tables maintained which also keep track of the sequence number of the received packets. The route discovery process is initiated when there is a mismatch between the sequence between the sequence number of the received RREP and the sequence number of table. The whole network is informed regarding these nodes. The scheme does not add overhead as sequence number itself is included in every packet in base protocol.

**Gundeep Singh Bindra et.al (2012),** proposed [36] a new solution for maintaining the Extended Data Routing Information (EDRI) table at each node. This is done to detect the black hole and gray hole nodes present within the network. On the basis of the previous malicious examples the study is proposed in this paper and the new method is also based on those studies. The packet is further renewed and the requests and reply of the packets are utilized from the RREQ and RREP packets. The gray behavior of the nodes is considered within the EDRI table. A counter is placed for tracking the number of times a node has been found. The black hole as well as gray hole attacks are prevented to enter within the network. The only limitation is that only consecutive cooperating black hole nodes can be identified using this scheme.

**M. Jhansi et.al (2012),** proposed [37] in this paper a new method is proposed for detecting the cooperative black hole attack in the mobile ad hoc networks. Extra bits of information are utilized in this method for storing the information related to the numerous packets received by the node. The transmission of numerous packets is further done. There are two bits utilized here in which the initial bit presents the information on the routing data packet from the node. The secondary bit 'through' provides the information related to the routing data packet from the node. Across the intermediate node the cross check is provided that creates RREP by providing its next hop node and DRL table. With the help of source node the DRI entry is checked. On the basis of the positive match the data is routed. For the purpose of checking the reliability of the intermediate node, the FRq message is sent to the next hop node in the network in other.

## III. CONCLUSION

In this paper, it is concluded that mobile ad hoc networks is the decentralized type of network in which mobile nodes can join or leave the network when they want. Due to self configuring nature of the network various malicious nodes join the network which are responsible to trigger various type of active and passive attacks. In this paper, various techniques are reviewed to increase security of the network

## IV. REFERENCES

[1]. Taneja Sunil, Kush Ashwani,"End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011

[2]. MOHAMED ABDUL HAIMID BASHIR, thesis, "ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS"2004

[3]. Vigna Giovanni, Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool forOLSR-based Ad hocWireless Networks", 2004

[4]. Sen Sevil, Tapiador Juan , "Security Threats in Mobile Ad Hoc Networks", 2010

[5]. Nandy Rusha, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)

[6]. Wenjia Li and joshi Anupam , "Security Issues in Mobile Ad Hoc Networks- A Survey",2005

[7]. Tsudik Gene, "Anonymous Location-Aided Routing Protocols for Suspicious MANETs", 2010

[8]. Karim El Defrawy, and Tsudik Gene, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" , IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9, SEPTEMBER 2011

[9]. N. Purohit, R. Sinha and K. Maurya, "Simulation Study of Black Hole and JEllyfish Attack on MAnet using NS-3," IEEE, pp. 1-5, 2011.

[10]. H. L. Nguyen and U. T. Nguyen, "A Study of Different Types of Attacks in Mobile Adhoc Network," 25th IEEE Canadian Conference on Electrical and Computer Engineering, no. 2, pp. 1-6, 2012.

[11]. Tyagi s.s, R.K. Chauhan, "Performance analysis of Proactive and Reactive routing protocols for the ad hoc networks", International journal of computer applications, Vol. 1No.-14, 2010, pp. 27-30

[12]. Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., & Tolle, J. (2007). Detecting black hole attack in tactical MANETs using topology graph. In Proceeding of 32nd IEEE conference on local computer networks.

[13]. L. Zhou, and Z. Haas, "Securing ad hoc network," IEEE Network Magazine, Special issue on network security, Vol. 13,No. 6, November/December 1999, pp. 24-30.

[14]. X. Hong, K. Xu, M. Gerla, " Scalable routing protocols for mobile ad hic networks",Network IEEE, Vol. 16, Issue 4, july 2002, pp. 11-21.

[15]. S.A. Ade1& P.A. Tijare, "Performance Comparisons of the AODV, DSDV, OLSR and DSR Routing Protocols in MANET", International Journal of Information Technology and Knowledge Management, Vol. 2, No. 2,Dec. 2010, pp. 545-548

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

[17]. Gonzalez,Oscar God win Ansa, Michael Howarth andGeorge Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.

[18]. K. Weniger, M. Zitterbart, "Mobile adhoc networks – current approaches and future directions," Network, IEEE, vol 18, Issue 4, pp 6–11, July-Aug 2004.

[19]. opinder singh, Jatinder singh, Ravinder singh" An intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes", Volumne 10, Issue 14 April 2017.

[20]. Conti M, Giordano S, "Multihop Adhoc Networking: The Theory",IEEE Communications Magazine, Volume 45, Issue 4, pp 78 - 86,April 2007

[21]. Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks", 2002, 10 th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648

[22]. kyasanur Pradeep "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing,2005

[23]. Yixin Jiang Chuang Lin, Minghui Shi, Xuemin Shen "Multiple Key Sharing and Distribution Scheme With (n; t) Threshold for NEMO Group Communications", IEEE 2006

[24]. Rupinder singh, Jatinder simgh, Ravinder singh,"WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks" Mobile Information Systems Volume 2016 (2016).

[25]. Chen Tien- Chen and Shih Wei-KuanShih , "A Robust Mutual Authentication Protocol for Wireless Sensor Networks ETRI Journal, Volume 32, Number 5, October 2010

[26]. Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada "On Alarm Protocol in Wireless Sensor Networks", 2010

[27]. J. Sen, S. Koilakinda and A. Ukil, "A mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Network," International conference on Inteligent Systems, Modellingand Simulation, pp. 338-343, 2011.

[28]. Singh P. K and G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET," IEEE International conference on Trust, Security andPrivacy in Computing and Communcation, pp. 902-906, 2012.

[29]. F. Thachil and K. Shet, "A Trust Based Approach for AODV Protocol to mitigate Black Hole Attack in MANET," International conference on Computing Sciences ,pp. 281-285, 2012.

[30]. K. Munjal, S. Verma and A. Bakshi, "Cooperative Black Hole Node Detection by Modifying AODV," International Journal of Management, IT and Engineering, vol. 2, no. 8, pp. 484-501, 2012.