A Robust Technique for Secure Routing Against Blackhole Attack in AODV Protocol for MANETs

Neelam Khemariya, Ajay Khunteta, Krishna Kumar Joshi

Abstract— Mobile Ad hoc networks are playing very important role in the present world. They are playing significant roles in real life applications such as military applications, home and emergency applications, automotive computing, personal area networks, wireless sensor applications, wireless mess networks etc. Ad hoc networks have very adaptive nature and thus they are attacked through various attacks such as Fabrication. Denial of Service, Grayhole attack, Black Hole attack etc. Black hole attack is one of the very dangerous active attacks in the mobile Ad hoc Networks (MANET). In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. Once the malicious node has been able to insert itself among the nodes which are using in the communication, it can drop all the packet which are passing through it or it can do many other things with the packets passing between them. In this research paper a robust secure efficient approach for the detection of the Black hole attack in the Mobile Ad Hoc Networks (MANET) is proposed. The algorithm is implemented on AODV protocol. In this proposed approach a solution is provided which is based on the Inspection of DSN and if it is more than the Threshold value than this node is consider as malicious node and after that next phase provides the confirmation of the Black hole nodes.

Index Terms— AODV, Blackhole Attack, DSN, Fresh Route, MANET, Reactive Routing Protocols, Selfish Node, SSN.

1 Introduction

Wireless network enables communication between computers using standard network protocols, without network cabling. These networks use radio waves or microwaves as a communication medium. Wireless Networks can be classified mainly into two categories: **Infrastructure Wireless networks and Infrastructure less Wireless Networks**

In Infrastructure Wireless Networks, communication takes place between the Wireless nodes through the Access Point (AP) and the wireless nodes cannot communicates directly [1]. The access point just not works as a control medium access, but acts as a bridge as well.

Infrastructure less wireless networks does not need any fix infrastructure for the communication and also there is no requirement of the access point. These networks are also called Ad Hoc Networks [1]. These networks don't have any fixed or static topology as shown in figure 1.

Mobile Ad hoc networks are the collection of mobile nodes that uses wireless transmission for communication. These networks have no fixed infrastructure, no fixed configuration and no other controlling device such as router etc. The setup or deployment of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology also they have a very less setup time [2]. . The routers are free to move randomly and organize themselves dynamically. It means, these networks don't have static topology, they form the topology dynamically. Such networks received considerable attention in recent years in both commercial and military applications, due to the attractive properties of building a network on the fly and not requiring any preplanned infrastructure such as a base station or central controller. These networks are mainly used in military, researchers, business, students, and emergency services [2].

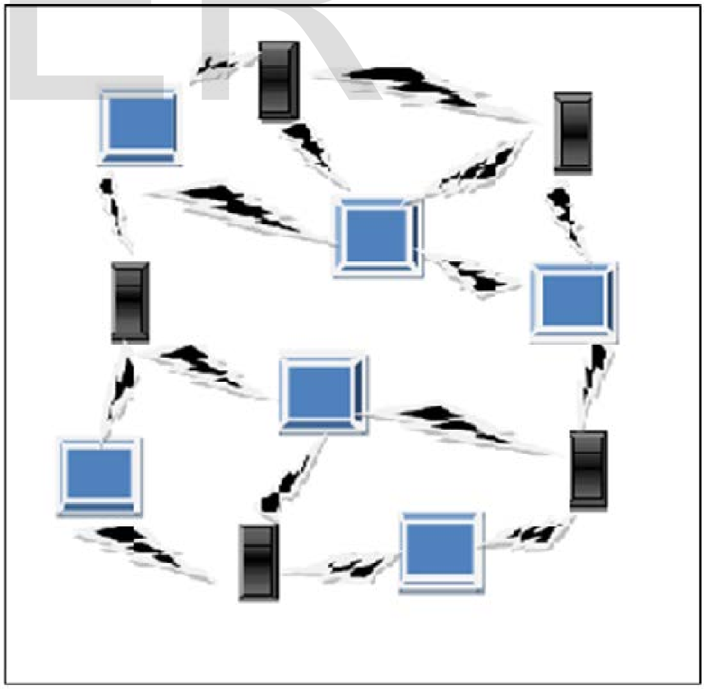

Fig. 1. Mobile Adhoc Networks

2 Routing in Mobile Ad hoc Networks

The routing in the Ad hoc networks is a very critical task because of the absence of any central coordinator or base station and the dynamic topology [2].

2.1 Issues in Designing a Routing for MANETs

In order to facilitate communication in these networks a routing protocol is used to discover the routes between nodes [3]. The greatest challenge for the Mobile Ad Hoc Networks (MANET) is to come with a robust security solution even in the presence of malicious nodes, so that MANET can be protected from various routing attacks. Mobile Ad Hoc Networks (MANET) has not got clear cut security provisions; it is accessible to any of the authorized network users and malicious attackers. Some important issues are given below:

- **Mobility:** In mobile AD-HOC network the nodes can move at any time so the network topologies highly dynamic in these types of networks so the routing is very tough in these networks because the node can change its position anytime therefore wired network routing protocols are not sufficient for routing in Mobile Ad Hoc Networks (MANET) because the routing protocols for Mobile Ad Hoc Networks (MANET) must be able to performed efficient mobility management [3].
- **Bandwidth Limitation:** In Mobile Ad Hoc Networks (MANET) the bandwidth is limited so the data rate is much less in comparison to a wired network so the routing protocols for Mobile Ad Hoc Networks (MANET) must use the bandwidth optimality and very low overhead [3].
- **Hidden and Exposed terminal problem:** For Mobile Ad Hoc Networks (MANET) we must need a specialized MAC because the MAC for wired network is not sufficient for Mobile Ad Hoc Networks (MANET). In Mobile Ad Hoc Networks (MANET) there is a problem called hidden and exposed terminal problem occur and simple MAC for wireless networks cannot handle this so we need a specialized MAC for these types of networks [3].
- **Resource Constraints:** two important resources for Mobile Ad Hoc Networks (MANET) are processing power and the battery life. And we know that these resources are limited so routing protocols used in mobile ad hoc networks must optimally manage resources.

2.2 Routing Protocols for MANETs

A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes. Many protocols have been suggested keeping applications and type of network in view.

Routing protocols can be classified by number of considerations.

2.2.1 Based on routing information update

Based on this category Mobile Ad Hoc Networks routing protocols can be classified into three categories, as shown in figure 2.

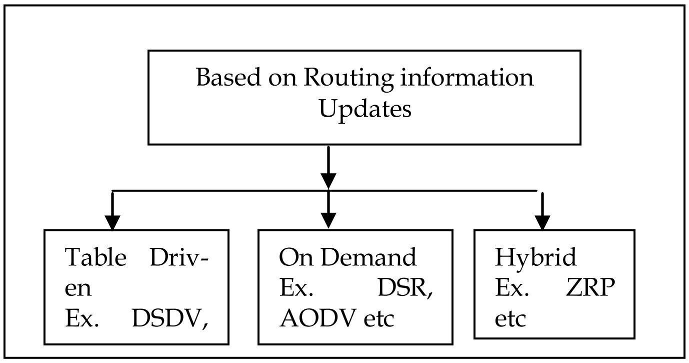
Based on Routing information Updates
Table Driven Ex. DSDV,
On Demand Ex. DSR, AODV etc
Hybrid Ex. ZRP etc

Fig. 2. Classification of Routing Protocols for MANETs

Table Driven Routing Protocols

In Table Driven routing protocols each node maintains one or more routing tables containing routing information about all other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some popular proactive protocols are: DSDV, WRP etc [4].

On Demand Routing Protocols

In On Demand routing protocols, the nodes don't maintain any routing table nut they have a route cache. Routes are find dynamically only when a node want to communicate with another node with the help of the route discovery procedure which is invoked by the source node. Some reactive routing protocols are: DSR, AODV etc [4].

Hybrid Routing Protocols

This type of protocols combines the best features of table driven and on demand routing protocols. In case of the intra-domain routing, these protocols uses the table driven approach, while in case of inter-domain routing these protocols uses the on demand approach[4]. Such as Zone Routing Protocol (ZRP) etc.

2.2.2 Based on topology information organization

Based on this category MANET routing protocols can be classified into two categories as shown in figure 3.

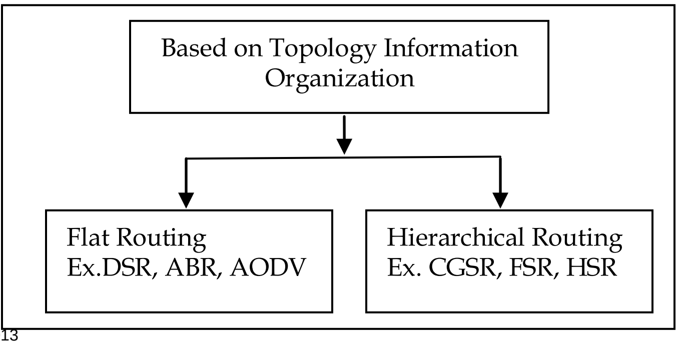
Based on Topology Information Organization
Flat Routing Ex.DSR, ABR, AODV
Hierarchical Routing Ex. CGSR, FSR, HSR

Fig. 3. Routing Protocols Based on Topology Information Organization

Flat routing Protocols

These protocols use a flat addressing scheme, which is a global addressing mechanism for nodes in a Mobile Ad Hoc Networks (MANET) Such as DSR [3].

Hierarchical routing Protocols

These protocols use a logical hierarchy of networks and an associated addressing scheme. The hierarchy could be based on geographical information or on hop distance Such as HSR, FSR [4].

3 ADHOC ON DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) routing protocol has certain beautiful features such as quickly adapt the new link in case of link failure, very low processing delay, small memory overhead, network utilization etc. It provides adaptive, source initiating, multihop routing between the mobile nodes.

AODV is loop free and it avoids the count to infinity problem occur in the Bellman-Ford algorithm and thus provides quick convergence in case of the dynamic network topology [5].

One important feature of AODV which differentiate it with the DSR is that it uses the destination sequence number for each route entry. This number is created by the destination node and it is included along with every route information it sends to the source nodes. For every route it sends to the source, there is a different unique destination sequence number. When a source has the choice between the two or more routes for the routing, it always prefers the route which has the greatest sequence number [6].

AODV has three types of messages:

Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs).

To find the route to the destination, the source node generates a RREQ and broadcasts it to its neighbors [6]. The Frame format for RREQ message is shown in the figure 4 below:

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Nu,ber							
Originator IP Address							
Originator Sequence Number							

Fig. 4. Frame format for RREQ message in AODV

When the destination get the RREQ packet it prepares a reply packet to the source, called route reply (RREP) packet and unicast it to the source node. All the intermediate nodes which receives the RREQ packet caches a route back to source node. Route Reply (RREP) Message Format shown in figure 5 below:

Type	R	A	Reserved	Prefix Size	Hop Count
Destination Ip Address					
Dsetinatiomn Sequence Number					
Originator IP Address					
Life Time					

Fig. 5. Frame format for RREP message in AODV

A RERR message is used to notify other nodes When a link break in an active route is detected. The RERR message contains the information about those destinations which are unreachable though any broken link. Route Error (RERR) Message Format is shown in figure 6 below:

Type	N	Reserved	DestCount
Unreachable destination IP Address(1)			
Unreachable destination sequence number(1)			
Additional Unreachable destination IP Address(if needed)			
Additional Unreachable destination sequence number(if needed)			

Fig. 6. Frame format for RERR message in AODV

The Route Reply Acknowledgment (RREP-ACK) message MUST be sent in response to a RREP message with the 'A' bit set [7]. This is typically done when there is danger of unidirectional links preventing the completion of a Route Discovery cycle. Route Reply Acknowledgment (RREP-ACK) Message Format is shown in figure 7 below:

Type	Reserved

Fig. 7. Frame format for RREP-ACK message in AODV

HELLO message is broadcasted to find the connectivity of a particular node in the network [7]. The important thing is that a node SHOULD only use HELLO messages if it is a part of active route. A node broadcast a HELLO message periodically on the HELLO_INTERVAL milliseconds.

4 Security Threats in MANETs

Mobile Ad Hoc Networks are unwired network with continuous changing topology (dynamic topology). So, they are very vulnerable to security threats.

4.1 Active Attacks

Active attacks are the kind of attack in which the attacker can see the information of a user and can modify it too. An active attack may be internal or external. In External attacks the attacker mainly aims to make congestion, send fake routing information or disturb the nodes so that they are not able to services in well manner [8]. An internal attack is an attack in which the opponent wants to gain the normal access to the network and participates the network activities by some malicious impersonation to get the access to the network.

Some most common active attacks are described below:

- **Modification**
  Modification of a message means that some portion of the original message is changed to make the message incorrect and to produce an unauthorized effect. A node may attack by altering the protocol fields in messages or injecting routing messages with false values [8]. A Denial of service attack may be done by modifying source routes as well.
- **Impersonation**
  This attack is also called spoofing attack. With the help of this attack, an attacker node cans cause lots of attacks in MANET. For example, traffic that belongs to the impersonated node may be redirected to the malicious node [8]. In this attack, the malicious node steals the identity of multiple nodes.
- **Fabrication**
  In fabrication attacks, false routing information is generated by an intruder such as false route error messages (RERR) .
- **Gray Hole attacks**: A gray hole may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes.
- **Eavesdropping:**
  Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. The main aim of this attack is to obtain some confidential information which should be kept secret during the communication [9].

4.2 Passive Attacks

In a passive attack (also called Selfish Node attack) the attacker can learn or use the information of a user but does not modify nor change it. In a passive attack, the attacker does not change or alter the operation of a routing protocol but only attempts to discover valuable information [9]. Defending against such attacks is very difficult. Two important passive attacks are the traffic analysis and the release of the message contents.

- Traffic analysis
- Release of the message contents

5 The Blackhole Attack

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created [10]. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

When a source node S needs to send packets to a destination node D to which it has no available route, it broadcasts a Route Request (RREQ) packet to its neighboring nodes. On receiving RREQ packets, the neighboring nodes update their Routing Tables (RTs) with an entry for the source node, and checks if it is the destination node or has a fresh enough routing to the destination node. If not, then the intermediate nodes receiving a RREQ packet broadcast the RREQ to its neighbors again [11]. The RREQ packet ultimately reaches the destination itself or at an intermediate node that has a fresh routing to the destination, which generates the Route Response (RREP) packet. The RREP packet is propagated along the reverse path to the source node. Suppose there is a malicious node in the path from source to destination. Whenever node B (Blackhole node) receives RREQ packets, it claims that it has the shortest route to the destination node and immediately sends a false RREP packet to the source node, even though it might not be having the route to the destination. The destination node may also send the reply but the reply from B could reach the source node first, if B is nearer to the source node. Moreover, B does not need to check its RT when sending a false message; hence its response is more likely to reach the source node firstly. This makes the source node thinks that the route discovery process is completed, ignores all other reply messages, and begins to send data packets through the path containing attacker node. Subsequently, all the packets through B are simply consumed or lost. B could be said to form a blackhole in the network and this type of attack is known as Blackhole Attack [12].

As shown in Figure 8 below, source node 1 broadcasts an RREQ message to discover a route for sending packets to destination node 3. An RREQ broadcast from node 1 is received by neighboring nodes 2, 4 and 5. However, malicious node 5 sends an RREP message immediately without even having a route to destination node 3. The RREP message sent by the malicious attacker node is the first message reaches to the source node .When the source node receive the message sent by the malicious attacker node, updates its routing table for the new route for the intended destination node and then also discards any RREP message from other neighboring nodes even from an actual destination node. When the Source node gets the route, it sends the data packets immediately from the route which is provided by the malicious attacker node. Nevertheless, a Black hole node drops all data packets rather than forwarding them on.

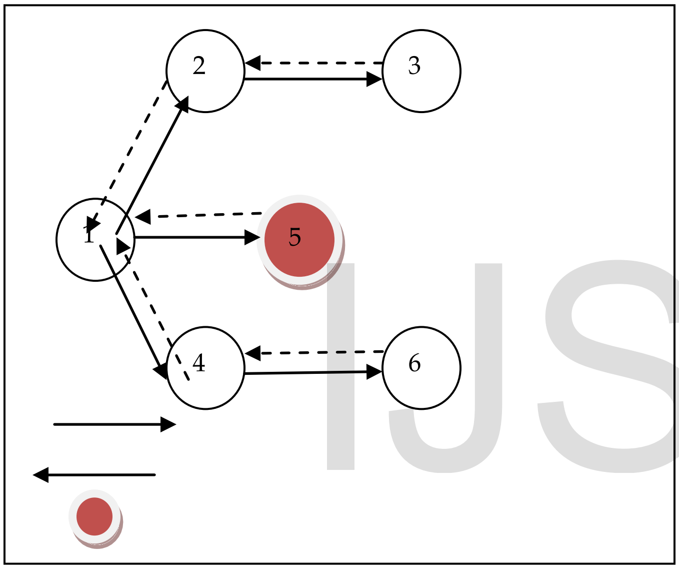

Fig. 8. Blackhole Attack in AODV

Blackhole attacks can be classified into two types: Single Blackhole Attack and Co-operative or Collaborative Blackhole Attack

Single Blackhole Attack

In the Single blackhole attack (shown in figure 9 below), there is a single malicious node which replies with the false information of the shortest path to the destination immediately when it gets a RREQ message for a particular destination [12]. Then this attacker node can drop all the traffic passing through it.

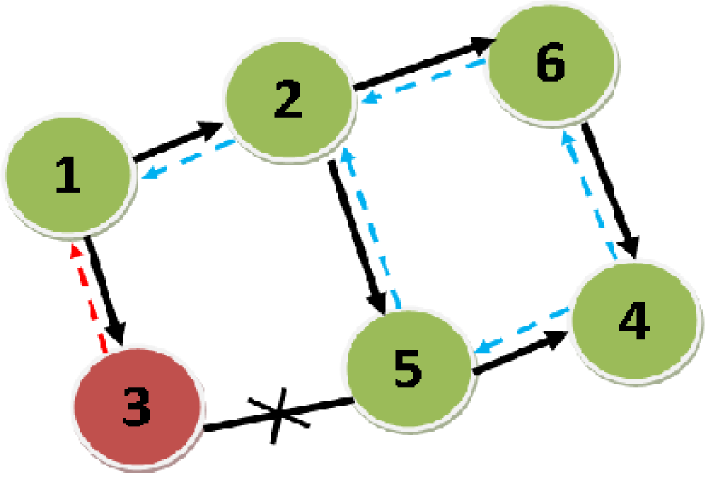

Fig. 9. Single Blackhole Attack in AODV

Collaborative or Co-operative Blackhole attack:

In collaborative or Co-operative Blackhole attack (shown in figure 10 below) multiple malicious nodes combined and coordinate malicious activities against some particular node. In this type of attack, the first blackhole node send the packet to another blackhole node and also every blackhole node have the complete information of every other blackhole node [12]. This type of attack is very tough to detect.

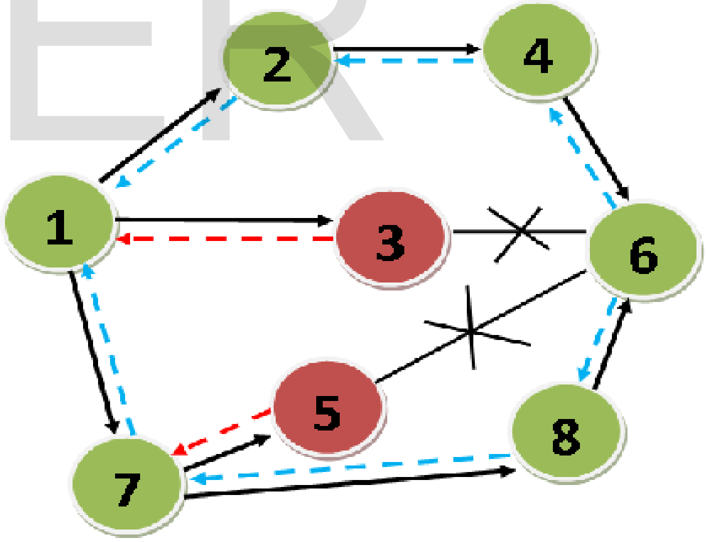

Fig. 10. Collaborative Single Blackhole Attack in AODV

6 Related Work

Raja Karpaga et.al. [13] Provided an efficient approach for the detection of the Blackhole attack on the DSR based Mobile Adhoc Networks, called BDSR (Black hole Detection in Dynamic Source Routing Protocol). In this approach, at initial state the Proactive detection approach is used while in the later stage the Reactive Detection mechanism is used. In Proactive Detection stage, this approach concentrates on the detection of the presence of any Blackhole node(s) initially.l while in the later stage it uses the Reactive approach which mainly concentrates on the reduction of the Overhead and the wastage of the resources.

Ekta Kamboj et.al [14] poposed an efficient approach for the detection of the Blackhole attack in AODV based Mobile ad hoc Networks. In this proposed approach, Intrusion Detection System based on the Fuzzy logic is used. In Fuzzy logic the correctness or the truthness of any statement is expressed or measured in terms of degree. In this approach, The Fuzzy parameter extraction module is used by a node to listens the traffic of its neighboring nodes and also chooses some parameters on which the fuzzy rules are to be implemented. Two parameters forward packet ratio and the average destination sequence number are used here. According to the fuzzy rules, If the forward packet ratio is low, average destination ratio is low then fidelity level is low. The fidelity level lies between 0 and 1.Minimum value for fidelity level can occur as a result of more malicious behavior than legitimate behavior of a neighboring node. This fidelity level is compared with the threshold value and model decides whether a node is black hole node or a normal node.

Maha Abdelhaq et.al [15] proposed a secure and efficient approach for the detection of the blackhole attack in the Mobile Ad hoc Networks based on AODV. The approach is known as Local Intrusion Detection Security Routing (LIDSR) mechanism. In the LIDSR mechanism, the detection of the blackhole node is performed locally with the help of the previous node just before the attacker node instead of detecting the attacker node with the help of the Source or the originator node.. So these things differentiate it with the previous approach known as the Source Intrusion Detection Security Routing (SIDSR) mechanism. This approach helps to reduce the security mechanism overhead.

Sowmya et. al. [16] proposed some modifications in ACO. The ACO algorithm provided an optimal path efficiently because it is fully distributed and thus, there is no single point of failure, also it is very simple to perform the operations on each and every node. The proposed algorithm is based on an asynchronous and autonomous interaction of agents. This algorithm is self organizing, robust and fault tolerant. In this proposed algorithm a threshold value is added with the ACO, to detect and prevent the blackhole attack in the MANET. The proposed scheme isolates these attacker nodes from the data forwarding or routing by reacting with the help of the ALARM packet to all its neighboring nodes.

Usha et.al.[17] proposed an algorithm for the detection of the Blackhole attack in AODV based MANET. In MANET world, when a node uses AODV protocol it can act as vulnerable by implementing following properties

- The node can set its hop count field to 1;
- The node can increase the sequence number by at least one when compared to other
  Nodes in the network;
- It can set the source IP address to a non existing IP address;
- It can unicast faked RREP message to the source node;

When a source node receives faked RREP message it updates its routing table towards nonexistent node. It can be achieved by an increasing destination sequence number and reducing hop count.

Shurman et.al.[18] proposed two attractive techniques to prevent the black hole attack in MANETs. In the first technique, at least two routes from the source to the destination node. First, the source node sends a ping packet (a RREQ packet) to the destination. The sender node will buffer at least three received RREP packets and after identifying a safe route it transmit the buffered packets. It represents that there are at least two routing paths existing at the same time. In this technique, two values are recorded in two additional tables which are last packet sequence numbers and the last packet received. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Second technique is good compared to first `original routing protocol. These both techniques fail to detect co operative black hole attacks.

Yibeltal Fantahum Alem et al. [19] proposed an approach for the detection of the black hole attack based on the Intrusion Detection Systems (IDS) .Intrusion detection can be done by two types: network based intrusion detection and host based intrusion detection. Basically network based intrusion detection works on switches, routers etc. In the mobile ad-hoc networks there is no central coordinator that monitors the traffic flow among the mobile nodes. They proposed the technique based on the anomaly detection by using host based Intrusion detection system. In this system every activity of a user is monitored and anomaly activities of an malicious node is identified from normal activities. To detect a black hole this system needs to be provided with a pre-collected set of anomaly activities called audit data. The system compares every activity with audit data. And if it found that any activity of a host is looking like out of the activity provided in the audit data, it isolates that particular node from the network.

Lalit Himral et al. [20] proposed an efficient and very simple approach for the detection of the black hole attack in the mobile ad hoc networks implemented on the AODV protocol. This method prevents from the black hole attack by the identifications of the nodes with their sequence number. The identification is made for whether there is large difference between the sequence number given by the source node and the sequence number given by the intermediate nodes who has sent back RREP message. In General RREP is sent by the malicious node with high destination sequence number than the other nodes and this entry is stored as the first entry in the Route Reply Table. It Then compare the first destination sequence number with the source node sequence number and if there exists much more differences between them, then that node definitely is the malicious node, and the source node immediately remove that entry from the Route Reply Table. When the malicious node is identified, the routing table information sent from the malicious node, are discarded from the network.

Deng et al. [21] proposed an approach to detect the individual black hole nodes. In this approach when any intermediate node replies for RREQ, it includes the next hop information to the destination in the RREP packet. When the source node receives this RREP packet, it sends a further request to the next hop of the replied node and asks them about the replied node and about the route to the destination. Thus we can easily identify trustworthiness of the replied node if the next hop is trusted otherwise not. Although this approach is very good for the detection of black hole- attack but it does not work in case of cooperative black hole attacks.

7 Proposed Work

In this paper, a robust secure efficient algorithm for the detection of the Black hole attack is described. This algorithm firstly identifies the black hole node in the given Mobile Ad hoc Network and then removes the entries for that node from the routing table. The algorithm is implemented in AODV (Ad hoc on demand Distance Vector) Routing Protocol. With the help of the proposed algorithm, both Single Blackhole attack and Co-operative Blackhole Attacks can be detected.

Source node S start the route discovery procedure for the destination D by preparing a Route Request packet, called RREQ packet and broadcast this RREQ packet to all its neighboring nodes. All the nodes getting this packet, forward to their neighboring node and the process continue until the packet reaches to the Destination node. When destination node get this RREQ packet, prepares a new packet for the reply, called RREP packet and unicast this packet to the source node S. The source node waits for all the replies and stores them into its own R-R (Route Record) table in terms of the decreasing Destination Sequence Numbers (DSNs). Means, a route which having highest DSN stored as the top entry in the R-R table. Now, the source node picks the first entry from the R-R table and compares its DSN with the Threshold value (Th). The threshold value is computed by averaging all the DSNs in the network. Now, If DSN is so much greater than Threshold (Th) then source node considers this node as the suspicious node and sits entry in the Suspicious Node Table (SNT) and then retrieve the second entry from the routing table and repeat the same procedure. This procedure is repeated until the DSN>>Th. After collecting all the suspicious nodes, the Source node again perform the Route Discovery procedure for the same Destination node D and for all the nodes retrieved in this time as the suspicious node, match them with the already stored in the Suspicious Node Table, stored them as the Malicious nodes in the Malicious Node Table(MNT). This phase is called the Malicious nodes detection phase. Now the Source node prepare a new RREQ packet for a new destination D1 and the same procedure is done for this new destination node and store all the nodes which have DSN>>Th as the new suspicious nodes and match them with the entries stored in the Malicious Node Table. All the nodes which have entry in both the tables are treated as the Black hole Node. This phase is called the confirmation of Black hole nodes phase. Now, source broadcast the information of these Black hole nodes to all nodes and when the other nodes get this information the remove all the entries of these Black hole nodes and now the normal process continues.

Algorithm

Step 1: Root Discovery Process

The source node S starts the route discovery phase for the Dest D (Destination 1) by preparing the RREQ packet and broadcast it to the neighboring node.

Step 2: Collecting Replies

The Source node store all the replies sent by the destination node or the intermediate nodes in terms of their DSN and NID and arrange them in terms of the decreasing DSNs in RR – Table

Step 3: Identification of Malicious Node

```
Retrieve the top entry from RR-Table.
If(DSN>>Th)
{
S [Node_id] =1;

Retrieve the next entry from the R-R table
}
After collecting all the Suspicious Node
Repeat step 1, 2 and 3 again
For Every node in the new R-R table
If (S [Node_id] = =1)
{
Malicious node= S [Node_id];
Store the Entry in Malicious Node Table
```

}
After collecting all the Malicious Nodes Go to step 4

Step 4: Confirmation of the Black hole Nodes
S Broadcasts a RREQ packet for destination D1 (Destination 2**)**. And collect all the replies in terms of their Decreasing DSNs in the R-R table.

```
For all Nodes
if (DSN>>Th)
{
Store in Suspicious Node Table
}
```

Match this new list with the Malicious Nodes List collected in step 3.
For all the nodes which appear in both of the list treated as the Black hole Nodes.

Step 5: Removal of Black hole Node
Remove the Entry of all the Black hole nodes detected in step 4 from the R-R table.

Step6: Node Selection Process for Secure Routing
Sort the contents of RR-Table entries according to the DSN in decreasing order and select the node which has highest DSN.

Step 7: Continue Default Routing Process
Continue with the normal procedure of AODV Protocol.

8 Implementations and Results

8.1 Parameters

The parameters are defined in the table 1 below:

TABLE 1
SIMULATION PARAMETERS FOR PROPSED WORK

Parameter	Value
Simulator	NS-2
Version	NS 2.34
Number of Nodes	10, 30, 40
Topography Dimension	670 m x 670 m
Traffic Type	CBR
Signal Prop. Model	Two Ray Ground model
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Antenna Type	Omni directional
Routing Protocol	AODV
Interface Queue	Drop Tail/Priority Queue
Max pkts in IFqueue	50
Channel	Wireless Channel
Max/Min Movement Speed	50 m/sec.
Min Movement Speed	10 m/sec
Pause Time	10 sec.
Simulation Time	120 sec.

8.2 Simulation Scenarios

Figure 11 below showing the simulation of 10 mobile nodes with one attacker node in NAM.

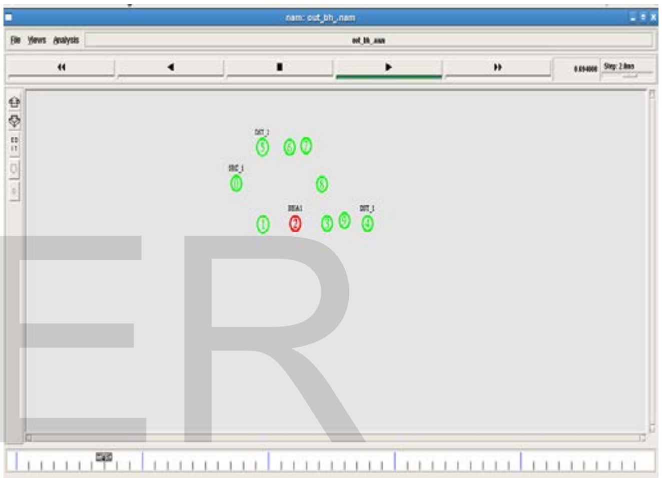

Fig. 11. Simulation of 10 mobile nodes with one attacker node in NAM

Figure 12 below showing the simulation of 10 mobile nodes with five attacker node in NAM.

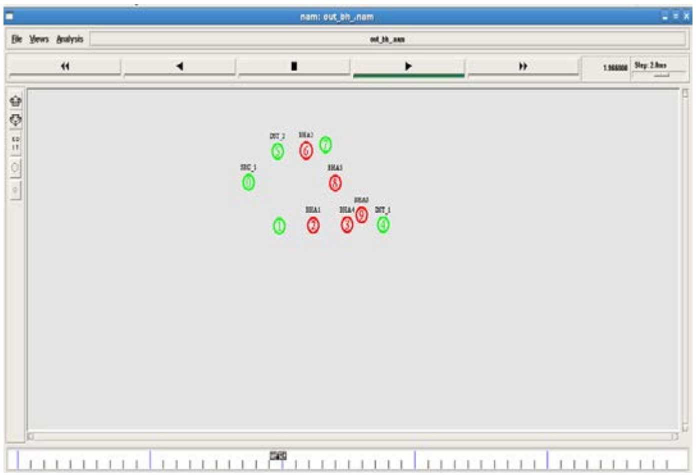

Fig. 12. Simulation of 10 mobile nodes with five attacker node in NAM

Figure 13 below showing the simulation of 30 mobile nodes with five attacker node in NAM.

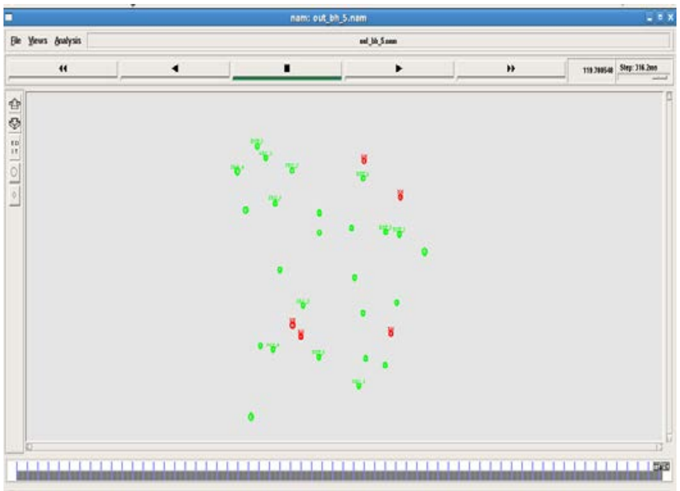

Fig. 13. Simulation of 30 mobile nodes with five attacker node in NAM

8.3 Simulation Graphs

We have shown three graphs to show the simulation results. Three Graphs are used to show the simulation results. These graphs are End to End Delay, Packet Delivery Ratio and Throughputs. Every graph contains two sub-graphs. The First Sub graph Shows AODV with attackers. This graph is shown by the red color. While the Second Sub-graph shows AODV with implemented algorithm. This graph is shown by the green color.

Case 1: When There is only one Attacker Node

Average End to End Delat Graph

This metric is basically used to describe the average time to send a packet from source to the destination. This Graph is drawn between Mobility (in m/sec) in X Axis and Throughput (in Kbps) in Y-Axis.

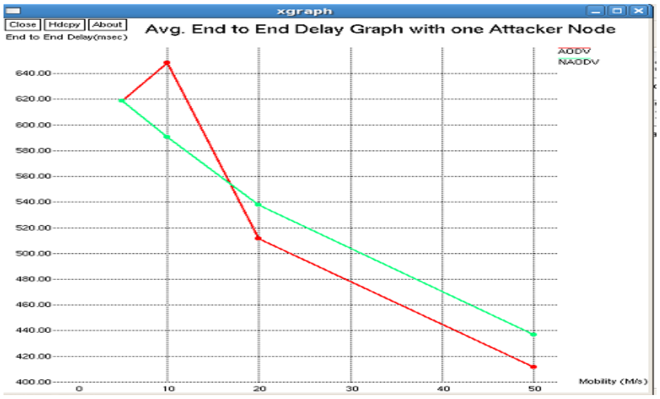

Fig. 14. Average end to end delay graph with one attacker nodes

Packet delivery Ratio Graph

This metric describes the ratio of total incoming packets and actual received packets by the destination. This Graph is drawn between Mobility (in m/sec) in X Axis and PDR in Y-Axis.

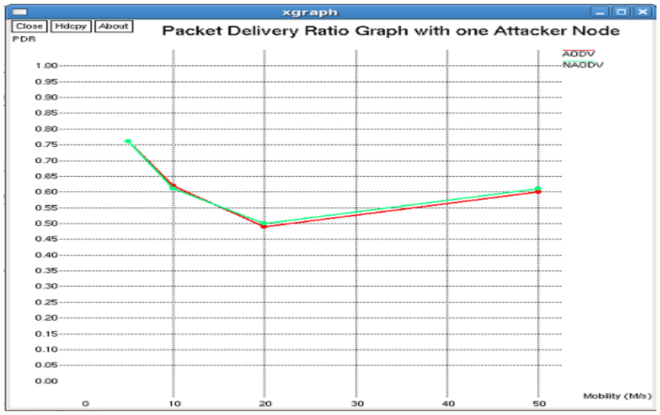

Fig. 15. Pacet delivery ratio graph with one attacker nodes

Throughput Graph

This metric describes the total number of bits send to the physical layer per second (Kbps). This Graph is drawn between Mobility (in m/sec) in X Axis and Throughput (in Kbps) in Y-Axis.

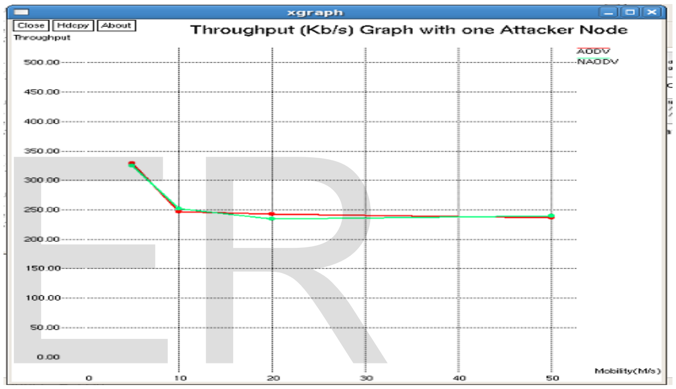

Fig. 16. Throughput graph with one attacker nodes

Case 2: When There are More than one Attacker Nodes (in our case 5)

Average End to End Delay Graph

This Graph is drawn between Number of Black hole Nodes in X Axis and Avg. End to end Delay (in milliseconds) in Y-Axis.

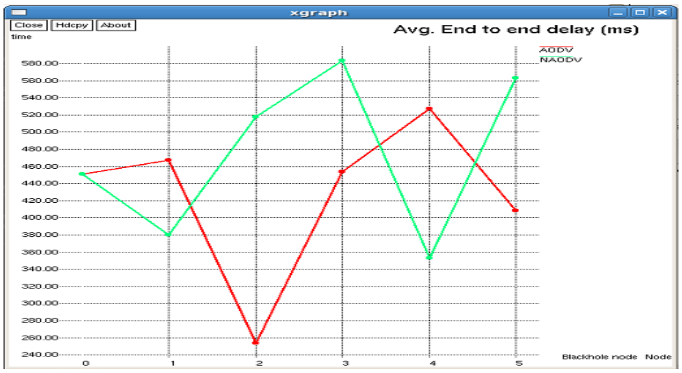

Fig. 17. Average end to end delay graph with 5 attacker nodes

Packet delivery Ratio Graph

This Graph is drawn between Number of Black hole Nodes in

X Axis and PDR in Y-Axis.

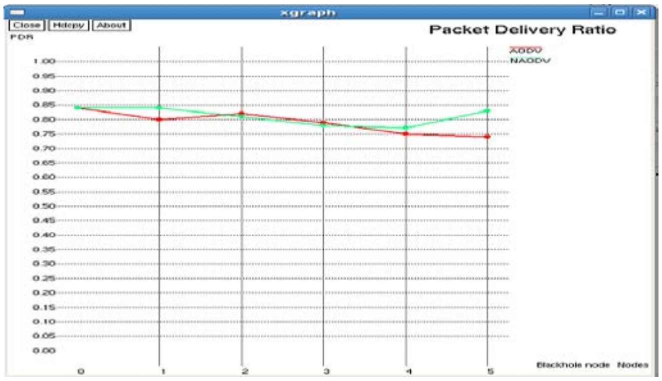

Fig. 18. Pacet delivery ratio graph with 5 attacker nodes

Throughput Graph

This Graph is drawn between Number of Black hole Nodes in X Axis and Throughput (in Kbps) in Y-Axis.

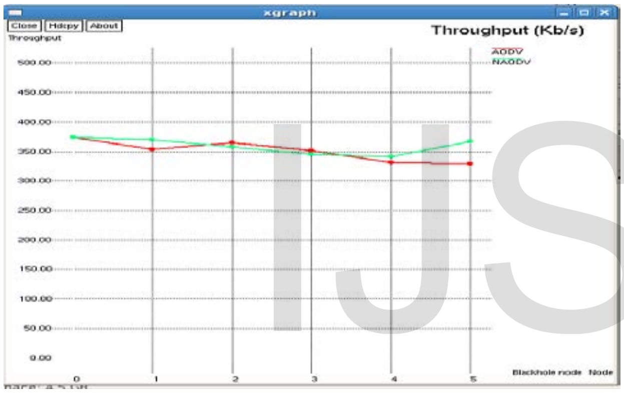

Fig. 19. Throughput graph with 5 attacker nodes

9 Conclusion and Future Scope

Mobile adhoc Networks due to their adaptive nature they are threatened by number of attacks such as Modification, Black Hole attack, Wormhole attack etc. Blackhole attack is one of the most dangerous active attacks in the mobile Ad hoc Networks (MANET). In this research paper a robust efficient approach for the detection of the Black hole attack in the Mobile Ad Hoc Networks on AODV routing protocol is proposed. In the proposed approach a solution is proposed which is based on the Inspection of DSN and if it is more than the Threshold value than this node is malicious node and after the detection of the malicious node a confirmation phase is provided for the confirmation of the Blackhole nodes.

As the future work, this algorithm can be implemented for some other dangerous network layer attacks such as Grey hole or Wormhole attack etc and also it can modify for providing the better resuly for the large MANETs and large number of Blackhole attacker nodes.

References

[1] Sunil Taneja and Ashwani Kush, “A Survey of Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248.

[2] “Ad Hoc Wireless networks” By Shivarammurthy, Pearson Education

[3]] T. Lin, S. Midkiff, and J. Park,”A framework for wireless ad hoc routing protocols”, in WCNC: Wireless Communications and Networking. IEEE Computer Society, 2003, pp. 1162.1167.

[4] Arun Kumar, lokantha Reddy and Prakash Hiremath, “Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008

[5] Anuj K. Gupta, Dr. Harsh Sadawarti, and Dr. Anil K. Verma, “Performance analysis of AODV, DSR & TORA Routing Protocols”. IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010 ISSN: 1793-8236

[6] S. R. Das, R. Castaneda, J. Yan, and R. Sengupta, “Comparative performance evaluation of routing protocols for mobile, ad hoc networks,” in Proceedings of 7th International Conference on Computer Communications and Networks (IC3N ’98) pp. 153 161, Lafayette, La, USA, October 1998

[7] RFC for AODV Protocol. http://www.ietf.org/rfc/rfc3561.txt

[8] G.S. Mamatha, Dr. S.C. Sharma, “Network Layer Attacks and Defense Mechanisms in MANETS- A Survey”, International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010

[9] N.Shanthi, Ganesan And Ramar, “Study of Different Attacks on Multicast Mobile Ad Hoc Networks”, Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT. All rights reserved.

[10] Sarita Choudhary, Kriti Sachdeva,”Discovering a Secure Path in MANET by Avoiding Black Holes”, International Journal of Recent Technology and Engineering (IJRTE) SSN: 2277-3878, Volume-1, Issue-3, August 2012.

[11] M. Umaparvathi, Dharmishtan K. Varughese, “Two Tier Secure AODV against Black Hole Attack in MANETs”, European Journal of Scientific Research ISSN 1450-216X Vol.72 No.3 (2012), pp. 369-382

[12] K. Lakshmi, S.Manju Priya, A. Jeevarathinam K.Rama, K.Thilagam, “Modified AODV Protocol against Blackhole Attacks in MANET“, International Journal of Engineering and Technology.

[13] Raja Karpaga Brinda.R1, Chandrasekar,”Defense Strategy for the detection of Black Hole Attack in Dsr”, Research Cell: An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Dec. 2011, Vol. 5

[14] Ekta Kamboj, Harish Rohil,” Detection of Black Hole Attack on AODV in MANET Using Fuzzy Logic “, Journal of Current Computer Science and Technology Vol. 1 Issue 6 [2011]316-318 Corresponding

[15] Maha Abdelhaq, Sami Serhan,3Raed Alsaqour and Anton Satria,” Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol”, Australian Journal of Basic and Applied Sciences, 5(10): 1137-1145, 2011 ISSN 1991-8178

[16] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi,”Detection and Prevention of Blackhole Attack in MANET Using ACO”, IJCSNS In-

ternational Journal of Computer Science and Network Security, VOL.12 No.5, May 2012

[17] Usha,Bose," Understanding Black Hole Attack in Manet", European Journal of Scientific Research ISSN 1450-216X Vol.83 No.3 (2012), pp.383-396

[18] Al-Shurman M, Yoo S-M, Park S, "Black Hole Attack in Mobile AdHoc Networks," 42nd Annual ACM Southeast Regional Conference (ACMSE"42), Huntsville, Alabama, 2-3 April 2004.

[19] Hongmei Deng, Wei Li, Dharma, P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[20] Yibeltal Fantahum Alem & Zhao Hheng Xaun, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection ", from Tainjin 300222, China 2010, IEEE Vol.2 (6), 2010.

[21] Lalit Himral, Vishal Vig, Nagesh Chand," Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST).

- *Ms. Neelam Khemariya is currently pursuing masters degree program in Software Engineering in Poornima College of Engineering, Jaipur, India. E-mail: neelam.khemariya@gmail.com*
- *Dr.Ajay Khunteta is currently working as Associate Professor in Computer Science Department in Poornima College of Engineering, Jaipur, India. E-mail: khutetaajay@poornima.org*
- *Mr. Krishna Kumar Joshi is currently working as Assistant Professor in Computer Science Department in Maharana Pratap College of Technology, Gwalior, India. E-mail: krishnakjoshi@gmail.com*