Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security in MANET: Effective value Based Malicious Node Detection and Removal Scheme

Priyanka
Master of Technology (Deptt. Of Computer Science And Engineering) MITM, Hisar Haryana, India

Mukesh Dalal
Assistant Professor (Deptt. Of Computer Science And Engineering) MITM, Hisar, Haryana, India

Abstract— Mobile Ad-hoc Network (MANET) is self configured network that consists of mobile nodes which communicate with each other to forward packets. MANET is vulnerable to various types of attacks like black hole, grey hole, worm hole etc due to its open medium, limited power, lack of clear lines of defence. The security of AODV routing protocol used in ad-hoc network is influenced by these attacks. In black hole attack, attacker claims to have shortest route to destination by injecting a fake reply message. This document introduces an effective value based technique to detect and remove black hole malicious nodes from network by using effective values derived from the detection results.

Keywords— Mobile Ad-hoc Networks (MANET), Ad-hoc On Demand Distance Vector (AODV), Denial of Service (DoS), Black hole attack, Malicious node, security, compromised node

I. INTRODUCTION

A MANET [1] is self configured network that can be easily deployed, needs no infrastructure and centralised administration. It consists of mobile nodes which communicate with each other to forward packets from source to destination. It is widely applicable [7] in many areas such as in military and battlefield applications, disaster area networks etc. MANET posses many characteristics [4] such as mobility, multi hop communication, dynamic topology, bandwidth constraint and variable link capacity etc. It is vulnerable to various types of attacks due to many security issues such as dynamic nature, limited computation, and lack of clear lines of defence. It is mainly influenced by Denial Of Service (DoS) [2] attacks such as black hole, grey hole, worm hole, impersonation, eavesdropping and replay attacks.

A malicious node can easily join the network and starts its malicious behaviour by dropping packets, advertising wrong routing information. A malicious node can silently drops all or some of the packets even when no congestion occurs. This situation becomes more sever when a group of malicious nodes co-operate each other. So, Security in MANET is an essential component for basic network functionalities like packet forwarding, routing and network management performed by all nodes instead of dedicated ones. Network operation can be easily jeopardized if security countermeasures are not embedded into basic network functions at the early stages of their design.

The advantages [4] of MANET are as follows:

- Fast Installation
- Dynamic Topologies
- Fault Tolerance and mobility
- Spectrum Reuse Possibility

In order to prevent the adverse effects of routing misbehaviour, the malicious nodes must be detected and removed from the network. In this paper we will discuss the technique for the same but before that we will discuss various security issues and attacks that can occur in MANET and disrupt its normal working operation.

A. Security Issues

There are many security issues that need to be resolved in the MANETs. The main issues [3] are as follow:

1) Open medium: Ad-hoc networks are by nature very open to everyone. This is also one of their biggest disadvantages: basically anyone with the proper hardware and knowledge of the network topology and protocols can connect the network and steal or alter information.

2) Threats from compromised node inside the network: A compromised node may also have access to encryption keys and authentication information. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by modifying routing information.

3) Lack of clear line of defence: In ad-hoc networks, attacks can come from any directions. The boundary that separate inside network with outside world is not very clear. It is not clear from where to deploy traffic monitoring and from where the access mechanism.

4) Dynamic topology: Direct links between nodes can be broken and reformed rapidly due to mobility. It is very hard to differentiate between normal behaviour and anomaly behaviour in dynamic environment.

5) Limited Resources: There are different varieties of devices in MANET ranges from laptops to handheld devices. These devices rely on battery power so many attacks like sleep deprivation torture can be done easily.

B. Classification of Attacks In MANET

Security of communication in MANET is important for secure transmission of information. Attacks on networks come in many varieties and they can be grouped based on different characteristics. There are many ways to diversify attacks:

- Location or source based attacks
- Behavior based attacks
- Malicious and selfish node attacks

*1) Location based attacks***:** Based on location of attacker, attacks can be categorized into two types:

*External attacks***:** External attacks are mainly carried out by node that does not belong or outside the network. They get access to the network by some means and once they get access to the network they start sending bogus packets, wrong routing information and cause denial of service in order to disrupt the performance of the whole network.

Internal attacks: In internal attack [5], the attacker has normal access to the network as well as participates in the normal activities of the network. The attacker enters in the network as new node either by compromising a current node in the network or by malicious impersonation and starts its malicious behavior.

Internal attacks are more dangerous than the external attacks: because the compromised nodes are originally the benign users of the ad-hoc network, they pass the authentication mechanism easily and get protection from the security mechanisms.

2) Behaviour based Attacks: Based on behaviour of the node, attacks are classified further into two types:

*Active attacks***:** In active attack the attacker disrupts the performance of the network by stealing important information and destroying the data during the exchange in the network [1] [6]. Active attacks can be an internal or an external attack. The active attacks destroy the performance of network in such case the active attack act as internal node in the network.

*Passive attacks***:** In passive attacks [1], attackers do not disrupt the normal operations of the network but listen to network in order to get important information, what is happening in the network, how the nodes are communicating with each other and how they are located in the network.

3) Malicious and Selfish Node attacks: Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes.

On the other side, **selfish nodes** can severely degrade network performances and eventually partition the network by simply not participating in the network operation [1] [14]. These nodes do not participate in network activities to save their battery power.

C. Attacks Types

Among numerous possible threats and attacks, MANETs are particularly susceptible to DoS attacks. Some known DoS attacks particularly developed against MANETs are examined.

1) Denial of Service (DoS) attack: The first type of attack is denial of service, in which the attacker aims to crab the availability of certain node or even the services of the entire ad-hoc networks. However, as seen so far, they are basically the results of most of the kinds of tampering with network integrity, redundancy and availability. In the traditional wired networks, the DoS attacks are mainly caused by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable.

2) Black hole Attack: Black hole attack is **D**enial **of S**ervice (DoS) attack on routing traffic. Black hole attack has two properties: First, the node advertises itself as having a shortest and fresh route containing larger sequence number and smallest hop count number to a destination node and exploits the mobile ad hoc routing protocol such as AODV, even though the route is not valid, with the intention of intercepting or dropping packets. Second, the attacker drops most of the packets without any forwarding.

A black hole can be caused either by a single node or by several nodes in collusion.

In case of a **single node black hole attack**, the node drops the entire packet instead of forwarding to destination as shown in figure 1.

In case of **multi-node collusion [8] or cooperative black hole attack**, BH forwards all the data to BH' and BH' drops them instead of forwarding to the destination. Black hole attacks have serious impact on routing algorithms.

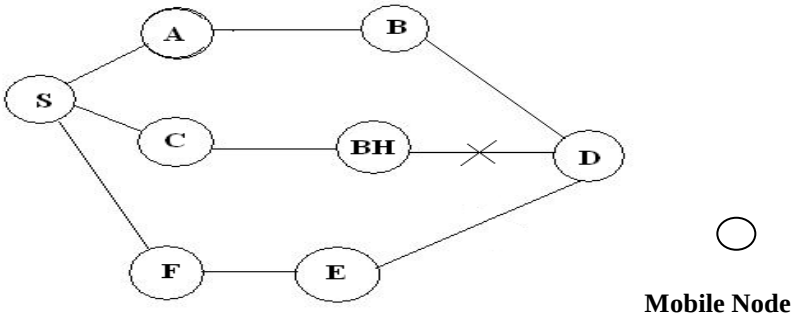

Figure 1 Single Black hole Attack

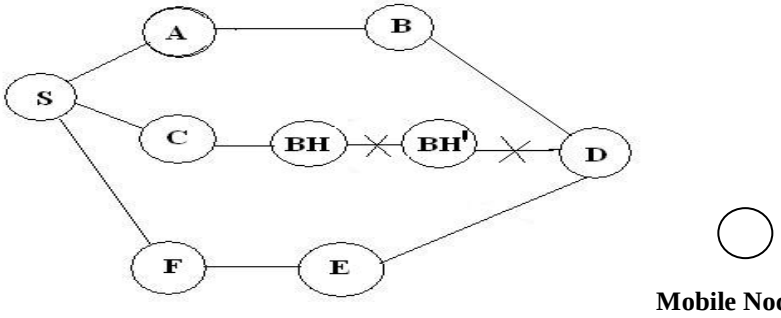

Figure 2 Cooperative Black hole Attack

3) Gray hole Attack: A Gray hole attack [5] is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later.

*4) Wormhole Attack***:** In a wormhole attack, a malicious node uses a path which is outside the network to route messages to another compromised node at some other location in the network. This attack is hard to detect because the path that is used to pass on information is usually not part of the actual network.

5) Eavesdropping attack [9]: This is a passive attack. The malicious node simply listens to the network and observes the confidential information. Later, it uses this information to carry out attacks.

*6) Impersonation attack***:** The attacker assumes the identity of another node in the network and receives messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the attacker is able to reconfigure the network so that other attackers can (more) easily join or he could remove security measures to allow subsequent attempts of invasion.

*7) Sleep deprivation torture***:** The idea behind this attack as described in [10] is to request the services a certain node offers, over and over again, so it cannot go into an idle or power preserving state, thus depriving it of its sleep.

The rest of the paper is organised as follows: Section II discusses some related work carried out earlier by researchers. Section III discusses overview of AODV protocol. Section IV describes the proposed scheme and its related algorithms. Section V gives the simulation results and finally Section VI concludes the paper.

II. RELATED WORK

Many secure routing protocols have been proposed by researchers that defend against malicious nodes' attacks that MANETs face. Some of the contributions are described here:

In [11], Bansal and Baker proposed a scheme for malicious node detection that is based on direct observations. The rating of a node is increased if the observed behaviour is positive whereas if the observed behaviour is negative the rating is decreased by more value than that is used for increment. If the rating of a node decreases beyond faulty threshold then it is added in faulty list. This faulty list is appended in route request by each node broadcasting it to be used as the list of nodes to be avoided. A route is rated good or bad depending on whether the next hop is on faulty list or not. It is rated bad if next hop is in faulty list and traffic from that route is rejected. A second chance mechanism employs timeout after an idle period. After a timeout, the node is removed from the faulty list with its rating remaining unchanged.

In [8] a protocol BAAP is described by Saurabh Gupta et. al. for avoiding malicious nodes in the routing path by using legitimacy table which is maintained by each node in the network. **A**d-hoc **O**n-demand **M**ultipath **D**istance **V**ector (AOMDV) is used to form link disjoint multi-path during path discovery. When intermediate node replies to source node, few nodes in the routing path may have more than one path to the destination but it chooses only one path to destination node. In BAAP, a legitimacy table is maintained by each node to choose the most legitimate node to source node and next hop to destination node while sending RREP back to source node. The fields contained by legitimacy table are: Node ID, Path count and Sent count. Node ID field stores the IP address of the node whose legitimacy value is being recorded. Path count field indicates the number of times the node has been chosen in the path and the Sent count field describes the number of times connections have been successful through the Node ID to destination node. These two count fields are used to define the Legitimacy Ratio (Sent count/ (Path count +1)) of a Node ID which indicates the confidence of node in performing its function of correct routing. A higher legitimacy ratio has higher possibility of a node being non-malicious.

In [12], Vishnu K et al. presents a scheme based on backbone network to detect and remove black hole nodes from network. Backbone network consists of group of nodes those are powerful in terms of battery power and range and are permitted to allocate the Restricted IP address to the newly arrived nodes. When a source node wants to initiate route discovery it asks the backbone network to allocate any unused RIP address. After the backbone network assigns the RIP address, the source node sends RREQ not only to search for destination but also for allocated RIP. If the RREP for the RREQ comes from the destination then network is safe but if RREP comes from RIP then it is assumed that there is black hole node in the network. The source node sends a monitor message to neighbour nodes to go into promiscuous mode and listen to the network. If the neighbour nodes monitors that the node drops the packet more than normal case it sends reply message to source node that there is black hole node in the network.

SAODV (Secure Ad-hoc On Demand Distance Vector) [13] is a security extension to the AODV routing protocol. This protocol provides security features like data integrity, non-repudiation and authentication. It uses two concepts: digital signature and hash functions. Digital signatures are used to protect non mutable fields of messages and hash

functions are used to protect hop count information. It uses extension messages. In these extension messages there is digital signature of AODV packet signed with private key of sender. The source node sends this packet, all the intermediate node verifies the signature and makes the route if the signatures are verified. The same also happens in the reverse direction.

III. AODV OVERVIEW

The Ad-hoc On Demand Distance Vector (AODV) [15] is on demand reactive routing protocol that does not maintain routes all the time but establish them when needed by source to send packets to destination. In ad-hoc networks each node maintains a routing table which consists of information about next hop for a route. When a source wants to send data packets to destination it first checks in its routing table whether a route to destination is present or not. If such a route is not available, it searches for the route and initiates a route discovery by broadcasting a route request message RREQ to its neighbour. The node receiving the RREQ checks whether it is the destination for the packet or not, if so then it sends the route reply RREP message back to the source. If it is not the destination then it checks whether it has fresh enough route to destination or not. If so it sends RREP message to source. But if it is neither the destination nor it has fresh enough route to destination it forwards the RREQ to its next neighbour. Before forwarding the RREQ, a node maintains or updates its routing table for the reverse route which is needed to send the reply message back to the source. It also updates information about destination in its routing table. It compares the destination sequence number contained in the packet with the destination sequence number present it its table and updates its routing table with the larger sequence number of the two.

All the nodes follow this procedure and go on forwarding the packet to next nodes. When the packet reaches to the destination or the node which has fresh enough route to the destination, a reply message is sent back to source. This reply message reaches to source through the reverse route maintained by intermediate nodes. The source node updates its routing table with this route information and starts sending data packets to destination on this route.

During the operation if any node detects a link failure it sends a route error RERR message to alert the nodes which use this route about the failure. Since there is no security mechanism in AODV many types of attacks can be easily performed on it. This paper provides security to AODV by eliminating threats of Black hole attack.

IV. THE PROPOSED SCHEME

Effective value based malicious node detection and removal scheme is proposed which consists of two components: detection and removal. The detection component is responsible for monitoring and detecting malicious nodes in the network and the removal component takes corresponding actions to punish misbehaving nodes and exclude or remove these nodes from the network. The removal component is based on effective information derived from the detection results therefore; effective value is the basis of proposed solution and needs to be considered comprehensively.

A. Assumptions For The Solution

1) MANET is assumed to be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue, which is generally called cluster head.

2) Here, the primary concern of secure data forwarding is to guarantee that a packet could reach its destination correctly. The only consideration is packet dropping problem, because other security problems such as confidentiality could be implemented by upper layers.

3) Each node in the network supports promiscuous mode, which is necessary for the detection part of the solution.

B. Formation of Cluster and its Working

A cluster is a group of nodes which are within the same radio range. For the proposed scheme, a deployment agency works for the cluster formation. From the cluster, a cluster head is selected in such a way that all of the other nodes in the cluster should be within one-hop vicinity. The Work done by Cluster Heads is as follows:

1) When any new node wants to join the cluster then new node sends the join request to the nearest cluster head.

2) If new node within range of two cluster head nodes then this node sends join request to both of the cluster heads.

3) Here timeout scheme is used for the joining of new nodes that is only new node join request in predefined time period is considered.

C. Tables used by Cluster Head for Proposed Scheme

In the proposed scheme different data structures are required at each Cluster Head in order to keep history of neighbour nodes, to calculate their legitimacy values and effective values. Detailed introduction and format for these tables are discussed below.

*1) Node Table***:** Each cluster head maintains a node table which is used to keep information about all the nodes. Node table contains two fields Node ID and Cluster Head Node ID. Each node in the network has a node ID that is any real number and this ID must not be changed.

TABLE 1 Node Table

Node ID	Cluster Head Node ID

2) Legitimacy Value Table: This table is maintained by the Cluster Head in order to keep history of all successful transmission paths through it. The information of this table is used in calculating the legitimacy value of a particular node. Legitimacy value table contains four different fields, Node ID, Successful connections, Total connections chosen and Legitimacy value. Node ID represents a node's identity as discussed above. Successful Connections represents how many times connection to destination have been

successful through the Node ID. Total Connections chosen represents how many times the Node ID has been chosen in the route. Legitimacy value is the ratio of successful connections to the total connections chosen. A higher legitimacy value means higher possibility of a node being non-malicious.

Legitimacy value is the proportion of how many times connection to destination have been successful through the Node ID to the how many times the node ID has been chosen in the route.

Legitimacy value=Successful Connections/Total connections chosen (I)

TABLE 2 Legitimacy Value Table

Node ID	Successful connections	Total Connection chosen	Legitimacy Value

*3) Effective Level Table***:** When Cluster Head node enters into promiscuous mode, it calculates the effective value of the node which replied the RREP (N_{RREP}) and next node of N_{RREP} (if next node is in the same cluster) to check that they forwards the packet correctly. In this effectivity model, effective values are limited in a continuous range from 0 to 1. The effective value of 0 signifies complete distrust whereas the value of 1 implies absolute trust. An example of trust levels of nodes are listed in Table 3. The initial effective value of all the nodes is set to 0.75 (less trustworthy node). A threshold t, termed as the malicious-list trust threshold, is used to detect malicious nodes. In other words, if the effective value of a node is smaller than t, it will be regarded as a malicious node. Effective value is calculated by the cluster head node to check that whether nodes are forwarding packets correctly or not.

Table 3 Effective Level Table

Level	**Effective Value**	**Meaning**
1	[0,t)	Malicious
2	[t,0.75)	Suspect
3	[0.75.0.9)	Less trustworthy
4	[0.9,1)	Trustworthy

Effective value is calculated as follow:

$$\text{Effective Value} = \frac{\left(\frac{TDP - DP}{DP}\right) + M\,(LV)}{M} \quad \text{(II)}$$

Where
TDP= Total number of dummy packets sent to N_{RREP} for forwarding.
DP = Total number of packets forwarded by N_{RREP} to next node.
LV = Legitimacy value of a particular node.
M = Weight of the effective value based on its observation and its make the solution more resistant to malicious node attack. The value of M should be larger than 2.

D. RREQ and RREP Packets Format and Processing:

Compared to AODV, the proposed scheme has the following differences in message format and type.

1) RREQ Packet: In the proposed scheme RREQ has additional cluster head node ID of originator field shown in Figure 3. This field is used to store the node ID address of the cluster head after it left the originator. Intermediate nodes would not process the RREQs which has the same cluster head node ID of source field value. Protocol creates link disjoint multiple paths in path discovery phase using cluster head node ID of source field but during path setup (RREP) it chooses only single link which has the higher legitimacy ratio among multiple links towards source and destination.

When a node originates some data and wants to send it to another node. It will follow the same actions as what AODV defines. Figure 4 shows the propagation of RREQ packet. The route discovery source 1 creates a route request packet. When a node receives the route request packet, it first checks whether it is the target of the route discovery. If it is not the target, the node should process the packet according to the following sequence of steps:

1) The node checks whether it has processed the packet from the same source with the same request identification and target address before. (For AODV, source address, request identification and target address are used to identify a route request packet.) If this is the case, the packet should be dropped silently.

Types	J	R	D	G	U	Reserved	Hop Count
Cluster Head Node ID of Source						RREQ ID	
Source IP Address							
Source Sequence Number							
Destination IP Address							
Destination Sequence Number							

Figure 3 RREQ Packet for proposed Scheme

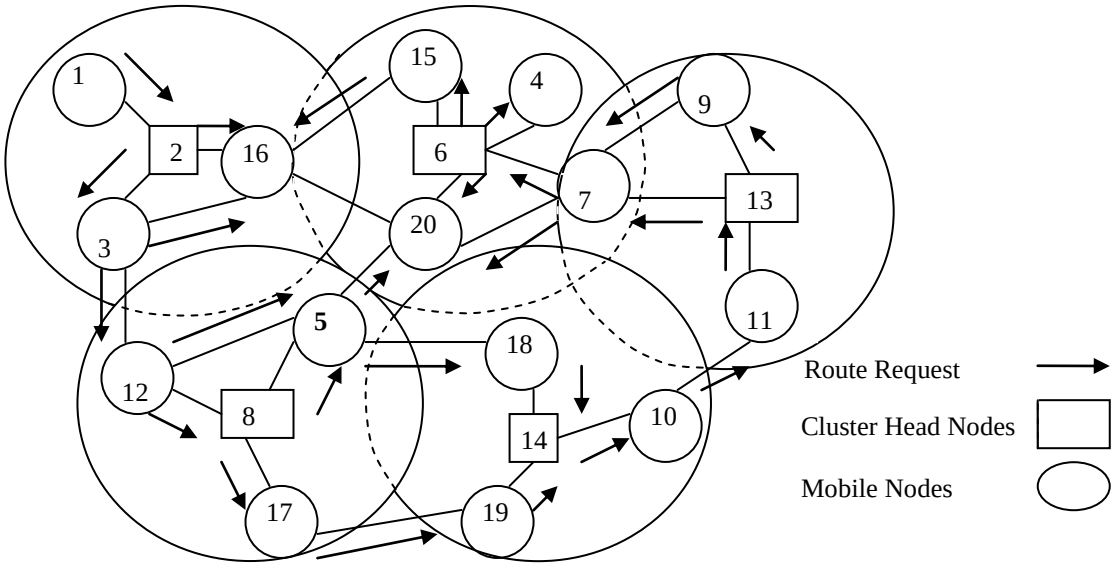

Figure 4 Propagation of RREQ message

2) If the node has never seen this request packet before and is allowed to forward the packet, it appends its own address to the route record of the packet, which is the requirement of AODV. Therefore, all intermediate nodes on the path can be accumulated in the request packet.

2) RREP Packet: In the proposed scheme RREP has additional Node ID, N_{RREP}'s Next Node and Cluster Head Node ID of N_{RREP} fields shown in Figure 5. Node ID field is used to store ID of N_{RREP} , N_{RREP}'s next node field contains the next node of N_{RREP} and cluster head node ID of N_{RREP} field contains the cluster head Node ID of the node which originates the RREP..

If the target address field in the route request packet matches with node's own IP address or any intermediate node has fresh enough routes to the destination then the node returns a route reply to the initiator for the request packet. If the target node itself send route reply packet then following sequence of steps takes place:

1) The sequence of hop addresses source, Address [1], Address [2], Address[n], target accumulated in the route record is put into the route reply packet. Source is the address of the originator of this route request packet, each Address[i] represents each intermediate node on the path.

2) Cluster head Node ID, Node ID of destination are also accumulated into the route reply packet.

In case any intermediate node has fresh enough route to the destination then N_{RREP} has to reply with its cluster head node ID and its Node ID and node ID of next hop node. RREP having Large Sequence Number & Minimum Hop Count will be chosen among various replies and all of other RREP buffered at Originating Node.

Figure 6 shows the propagation of RREP message from destination node 18 to source node 3

E. Explanation of Proposed Scheme

With the help of a clustered network, a scheme is proposed which requires a real number that acts as node ID associated with each node of the network. The key idea in the algorithm is that after finding the route, the source node sends encrypted message to the cluster head of N_{RREP} through a trusted path. The encrypted message contains the following information:

$$E\ [\text{Number of dummy packets, SN, DN, } LV_{1\ldots\ldots i}, \text{ Nonce}]$$

Where

SN and DN are source node and destination node respectively and

$LV_{1\ldots\ldots i}$ are legitimacy values of the nodes.

On receiving and decrypting this message cluster head goes into promiscuous mode and starts monitoring N_{RREP} and its next hop node if next hop node belongs to same cluster of N_{RREP}. Now source node sends some dummy packets to the N_{RREP} node then the cluster head node starts listening in the cluster for all the packets destined to that particular (N_{RREP}) node and next node of the N_{RREP}. Following this the cluster head node initiates the detection and removal of the chain of malicious nodes that are cooperating together to dump the packets. It counts packets forwarded by N_{RREP} and its next hop and based on this count value and legitimacy value calculated by equation (I), it calculate the effective value of a N_{RREP} and its next hop node by formula given in equation (II). If the effective value falls below threshold effective level (t) then it detects N_{RREP} and its next hop node as malicious and calls for removal process.

If the NRREP belongs to same cluster as that of source node, the cluster head node itself enters into promiscuous mode and starts monitoring NRREP and its next hop node if both belong to the same cluster, counts packets forwarded by these nodes and finally calculates effective value by equation (II). It detects the next hop node if only if it belongs to same cluster as that of NRREP.

.

Types	R	A	Reserved	Prefix Size	Hop Count
Source IP Address					
Destination IP Address					
Destination Sequence Number					
Nrrep's Next Node				Lifetime	
Node ID				Cluster Head Node ID of Nrrep	

Figure 5 RREP Packet for proposed scheme

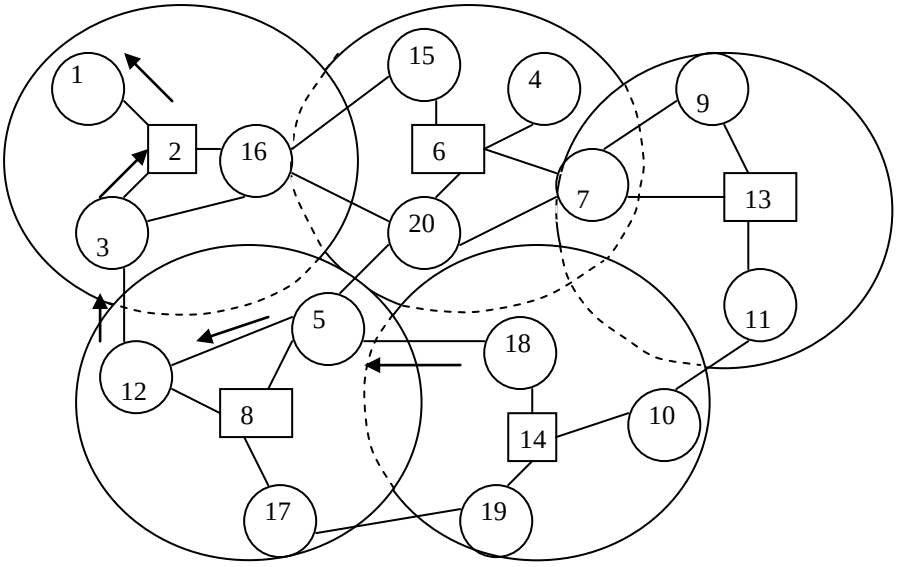

Figure 6 Propagation of RREP message

In removal process the following step should be followed:

- CH adds malicious node(s) to the malicious list.
- Now CH broadcast the malicious list to the whole network.
- After getting the list all nodes of the network find the Node IDs of the malicious nodes in their tables.
- Each node deletes all the entries related to these Node IDs from the respective tables

V. SIMULATION RESULTS

In this Section, the proposed scheme will be evaluated on the basis of simulation results. The experiments for the proposed scheme have been carried out by using the MATLAB (Matrix Laboratory) package. For simulation purpose a total of 40 nodes were taken. Numbers of malicious nodes were varied from 2 to 5 through the simulation. The graph of packet delivery rate (Figure 7 and 8) represents the throughput of AODV under two malicious nodes attack and AODV with extension of proposed scheme. The X-axis of the graph represents Number of nodes and Y-axis represents the Network Throughput. The graphs shown here demonstrate that AODV with the extension of proposed scheme always perform better than standard AODV. Mobile nodes are distributed over average density area. The input parameters used for simulation are summarized in table 4.

Using these parameters performance for different scenarios is carried out.

- AODV under two malicious nodes cooperating in black hole attack
- AODV with extension of proposed scheme

The throughput percentage for these experiments is calculated by taking average of network throughput for number of nodes 20, 40, 60, 80 and 100. This is in line with our expectation since the malicious nodes which failed in forwarding packets are removed from the routing cache. The result is that good paths are used for transmitting packets.

In figure 7, the effects of two malicious nodes on AODV are shown. The graph of network throughput against number of nodes for AODV under two malicious nodes is plotted. From the figure 7 we see that the throughput for AODV decreases as the number of nodes increases. There are several reasons for this decrease as follows:

1) As we increase the number of nodes in the network the problem of congestion increases in the cluster as a result packet drop ratio increases due to collision between packets.

2) Resources such as bandwidth become limited, as load on cluster head increases because it has to manage more number of nodes and due to which more energy consumption takes place.

3) One another reason is malicious nodes cooperating in black hole attack. These nodes capture the packets and do not forward them to next node and drop them.

The average throughput for AODV under the effect of two malicious nodes comes out to be 32% approx. From this result, it is shown that the effects of malicious nodes cannot be neglected.

Table 4 Input Parameters used for simulation

Parameters	**Values**
Simulator	MATLAB
Protocol	AODV
Number of nodes	40
Number of malicious nodes	2-5
Packet size	512 bytes

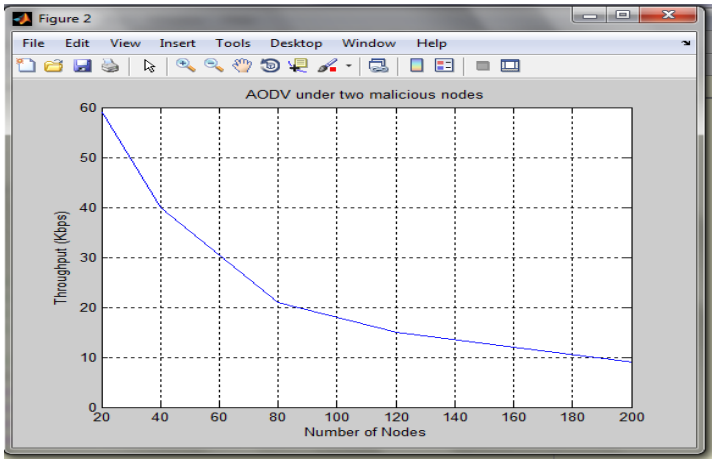

Figure 7 Network throughput of AODV under two malicious nodes

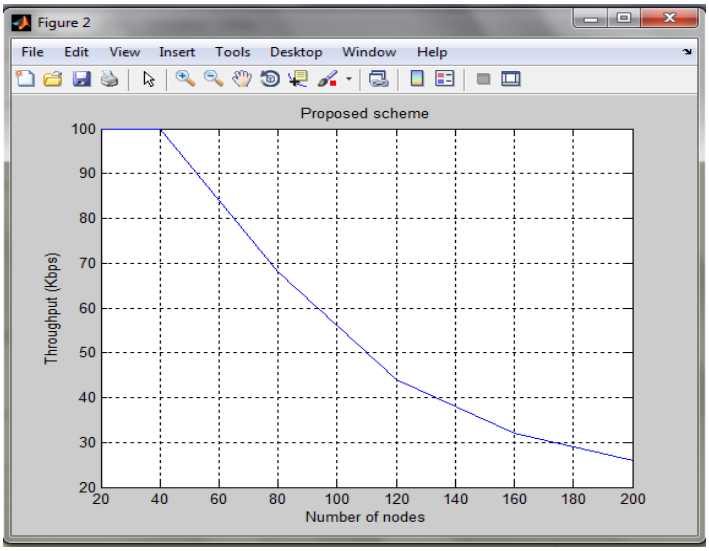

Figure 8 Network throughputs Of AODV with the extension of proposed scheme

In figure 8, graph of throughput of AODV with extension of proposed scheme is shown against number of nodes. The proposed scheme finds out the effective values of node given the legitimacy values and based on the effective value it is decided whether the node is malicious or not. If node is found malicious it calls for removal phase and removes malicious nodes. The simulation results show that in case of AODV with the extension of proposed scheme the throughput is increased around 11% from standard AODV which comes out to be 71%. The throughput in this case comes out to be about 82%.

VI. CONCLUSIONS

During the research work, effective value based scheme is presented to detect and mitigate the malicious nodes attack in MANETs. The detection mechanism and the removal approach in this solution are specially introduced. The detection mechanism could be used to effectively detect malicious nodes by performing neighbour monitoring and information exchange between cluster heads. Depending on cooperation of all well-behaving nodes in the network, malicious nodes could be excluded from the discovered routes. And route selection is based on hop count as well as path quality to select the most reliable route to a specific destination.The proposed scheme is implemented in MATLAB. The results of the experiments showed that even in the presence of malicious nodes, the newly proposed scheme improves network throughput to about 82%, from 71% network throughput provided by AODV, 32% network throughput provided by AODV under two malicious nodes. A conclusion is made from the simulation results that malicious nodes degrade the network performance considerably and increase other nodes' burdens.

Moreover, if data packets are used instead of dummy packets to check the node's effective value more improved performance results can be obtained. The next step is to simulate more scenarios in which more complicated misbehaviour exists such as detecting the malicious nodes which belongs to two different clusters, and to analyze the network for these scenarios.

REFERENCES

[1] Joseph Macker and Scott Corson Mobile ad-hoc networks (MANET) http://www.ietf.org/proceedings/01dec/183.htm

[2] A. D. Wood and J. A. Stankovic, " Denial of service in sensor networks", Computer, vol. 35, no. 10, pp. 54-62, 2002.

[3] G. M. Ignas, M. Niemegeers, Sonia M. Heemstra de Groot, "Research issues in adhoc distributed personal networking", wireless personal communications : An international journal, vol.26, Issue 2-3, pp.149-167, Kluwer Academic Publishers August 2003

[4] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Peit Demeester, "An overview of mobile ad hoc networks: applications and challenges", MAGNET project.

[5] Irshad Ullah, " Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis, Blekinge Institute of Technology ,June, 2010.

[6] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Low price Edition, Pearson Education, 2007.

[7] Humayun Bakht, "Application of mobile ad hoc networks", http://www.computingunplugged.com /issues/issue200409/00001371001.html.

[8] Saurabh Gupta, Subrat Kar, S Dharmaraja , "BAAP: Black hole Attack Avoidance Protocol for Wireless Network", IEEE proceedings of the International Conference on Computer & Communication Technology (ICCCT),2011.

[9] K. SIVAKUMAR et.al. 1366 www.ijcsmr.org. Overview of Various Attacks in Manet And Countermeasures For Attacks.

[10] F. Stajano, F. and R. Anderson, "The Resurrecting Duckling : Security Issues For Ad-hoc Wireless Networks In Security Protocols", 7th International Workshop Proceedings, 1999

[11] S. Bansal and M. Baker, "OCEAN: Observation based cooperation enforcement in ad hoc networks", *Technical Report*, Stanford University,

12] Amos J Paul ,Vishnu K "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks", International Journal of Computer Applications (ISSN NO. 0975 - 8887), vol. 1, no. 22, 2010.

[13] Manel Guerrero Zapata, " Secure ad hoc on-demand distance vector (SAODV) routing", draft-querrero manet-saodv-03, Mobile Ad Hoc Networking Working Group, 17 March 2005.

[14] A. James , "Computer security threat monitoring and surveillance ", James P. Anderson Co.Tech. Rep., April 1980

[15] C. Perkins, E. Belding - Royer, S. Das,"Ad hoc On-Demand Distance Vector Routing", RFC 3561. July 2003.

