A Cross Layer Approach for Intrusion Detection in MANETs

Sandeep Sharma, Rajesh Mishra
Gautam Buddha University
Greater Noida, India

ABSTRACT

In this paper, we propose a cross layer approach to detect the malicious node (Black hole attack) in MANET. In this approach, the malicious node is detected by the collaborative decision made by the network layer, MAC layer and physical layer on the basis of the parameters passed by the physical and the link layer to the network layer using cross layer design, and then the best path is selected among the various paths between the source node and the destination node. The routing protocol which is used in the simulation is AODV. The malicious node is then deleted from the routing table and the performance of our technique is proved by the simulation of our system model using the network simulator NS-2.

General Terms

Wireless Network, Mobile Ad-Hoc Networks, Attacks on MANETs..

Keywords

MANETs, AODV, Cross Layer, Intrusion Detection.

1. INTRODUCTION

1.1 MANET

An Adhoc network does not rely on the infrastructure, for connectivity with the neighboring nodes and forms the network with the end user nodes. All the required services like forwarding, routing, administration and maintenance are carried out by the node themselves. Nodes in the Adhoc network rely on the multi-hop relying to communicate with the node which is not in their coverage area. The adhoc network uses a unique technique known as the cooperative routing [3], due to the absence of any infrastructure and any centralized nodes for routing. In such type of the routing the source node depends upon the neighboring nodes for the forwarding of the packets and this in turn introduces some unpredicted vulnerabilities at the routing protocols. Since all nodes in the network take part in the routing, hence a malicious node can broadcast false routing information to its neighboring node, which could be readily accepted by the node without authentication Because of this problem any malicious node in MANET with malign intentions, can cause routes to be added, modified or deleted. Securing the routing protocol is an open research problem in the area of adhoc network and many of the current research problems focus on such issues [7].

1.2 Cross Layer Design

Traditionally, the complete networking task of the protocol is divided into independent layers. Each of these layers is designed separately with the services it is going to implement, with the help of the well defined interfaces through which these layers communicate with each other. In the layered architecture, UDP packets are sent to and fro from the network layer to the application layer via the transport layer. This communication causes some avoidable delay which degrades the overall performance of the network. If we can design a direct application layer- network layer interface bypassing the transport layer, we can save the end to end delay [6] and hence the overall network performance can be improved. Designing such interfaces which do not exist in the reference model is a cross-layer communication. Cross layer design refers to protocol design done by actively exploiting the dependence between the protocol layers to obtain better performance gain [5]. This is unlike the layered architecture where the protocols at the different layers are designed independently and do not depend on the other layer protocol. In the layered protocol stack each layer communicates only with the adjacent layers using well defined interfaces and hence there is no performance optimization. Performance optimization can be obtained with the help of adaptation and optimization using the available information across many protocol layers. One of the vital methods of cross layer design is sharing of the database between the different layers (fig.1) so that the parameters could be available at different layers of the protocol stack.

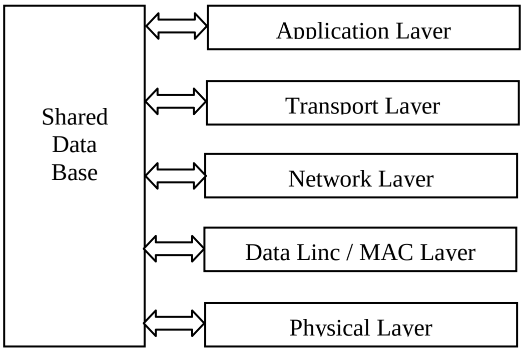

Fig. 1. Cross Layer Design with Shared Database

1.3 Paper organization

In this paper we propose a cross layer based technique for the detection of the malicious node for the MANET. Not only the malicious node is detected, it is also authenticated based on the physical, MAC and network layer metrics. We simulated a Black hole attack and investigate its effect on various parameters such as the throughput, packet delivery ration, routing overheads and end to end delay for one to five malicious nodes. AODV, the already existing routing protocol is used and modified for the purpose. The simulation is performed using the network simulator ns-2. The paper is arranged in the following way: we begin in Section 2, discussing the related work on intrusion detection techniques. In Section 3, we are providing an overview of the working of AODV protocol. We present our system model in Section 4 followed by the simulation results and discussions in Section 5 and then conclusions of the paper are briefed in section 6.

2. RELATED WORK

Security is a major concern whenever we are using wireless channel to communicate. As the channel is open to all any potential intruder can join our network and listen our communication. So we must have a strong scheme to detect any intrusion in the network. A number of intrusion detection schemes for intrusion detection system have been presented for ad-hoc networks. A classification and description of various techniques used for the intrusion detection is discussed in [13]. In [14], the authors proposed a cross layer based adaptive real time routing attack detection system (CARRADS) for the MANET, that has the ability to adapt at real-time to new network environments and attack patterns. The detection engine is prepared with the help of machine learning algorithm support vector machines (SVM). The author in [15], proposed a technique to detect based on dynamically updating learning data. This technique can adapt very easily, changes within the MANET. The authors in [16], proposed a node based anomaly intrusion detection system for ad hoc networks using unsupervised association rule mining technique which can effectively locate the attack source within one hop perimeter. In [17], the author has discussed single layer and cross layer approaches to detect the intrusion detection in MANETs, and proposed a cross layer approach as an effective remedy over single layer IDS. The authors in [18], proposed a cross layered based anomaly detection technique which is based on cluster data mining technique to detect the DoS attack and sink-hole attack at different layers of the protocol stack. In [19], the authors proposed a cross layer based routing mechanism and it is used only for establishing multiple paths rather than security. In their proposed work, the authors in [20] discussed a cross layer approach to reduce the link break in MANETs. This scheme offers low packet retransmission ratio by distribution information between PHY and MAC layer and identify the link failure instead of predicting received signal power.

3. THE AODV PROTOCOL

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, which means that, it builds routes between nodes only and when desired by the source nodes (originating nodes). It maintains these routes until they are needed by the sources and delete them when undesired. Additionally, for the multicast group members, AODV forms trees which connect them. The trees consist of the members of the group that needed to be connected. AODV uses sequence numbers to ensure the freshness of routes. A route with a large sequence number is most recent than the route having the lower sequence number. One characteristic feature of AODV is that it uses a destination sequence number for each route entry. The destination sequence number is created by the destination node to be included along with any the route information it sends, to the requesting (source) nodes. Using destination sequence numbers ensures loop freedom. Whenever the choice between two routes to a destination is given, the requesting node is required to select the route with the greatest sequence number. AODV offers loop-free, self-starting and scalable network routing for the adhoc networks. The AODV uses four types of messages to communicate between the nodes [4].

- The Route Request (RREQ) Message (Fig.2)
- The Route Reply (RREP) Message (Fig.3)
- The Route Error (RERR) Message (Fig.4)
- The Route Reply Ack.(RREP-ACK) Message (Fig.5)

Among these four messages, route request and route reply messages are used for the route discovery while the remaining two viz. route error and route reply acknowledgement messages are used for the maintenance purpose. AODV builds routes using the route request / route reply cycles. When a source node requests a route to a destination node, for which the route is not known, it broadcasts the route request (RREQ) message in the network. Nodes in the network having receiving this message, updates their source node information by setting up backwards pointers in the route tables. Apart from the IP address, current sequence number, broadcast ID of the source node, the RREQ also contains the most recent sequence number for the destination node of which the source node is aware of. A node receiving the RREQ may send a route reply (RREP) message if it is either the destination node or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ message. If this is the case, it unicasts and not broadcast a RREP back to the source node. Otherwise, it rebroadcasts the RREQ message in the network. Nodes keep a track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it to the next neighboring node. As in the AODV protocol the RREP message propagates back to the source, nodes get an opportunity to set up forward pointers to the destination node. Once the source node receives the RREP message, it may begin to forward data packets to the destination node, as the route has been discovered. If the source node later receives a RREP message that contains a greater sequence number than the previous one or contains the same sequence number but with a smaller hop-count, then it may revise its routing table for the routing information for that destination and start forwarding the data packets via the better route. AODV maintains the route until it is active and deletes the route from the routing table of the intermediate node when it becomes inactive. A route is considered to be active when there is periodic data traffic between the source and the destination along that route and becomes inactive once the source node stops sending the data packets through that route. In the case of a link break while the route is active, the node upstream of the link break and propagates a route error (RERR) message to the source node to inform it that it has now become the unreachable destination. After receiving the route error (RERR) message, if the source node still desires the route, it can reinitiate route discovery through RREQ/RREP cycle.

3.1 The Route Request Message format

The route request is broadcast by the source node when it desire a route for the destination for which no route exists in the routing table.

◄——— Bit Positions ———►

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

<table>
<tr><td>Type</td><td>J R G D U</td><td>Reserved</td><td>Hop Count</td></tr>
<tr><td colspan="4">RREQ ID</td></tr>
<tr><td colspan="4">Destination IP Address</td></tr>
<tr><td colspan="4">Destination Sequence No.</td></tr>
<tr><td colspan="4">Originator IP Address</td></tr>
<tr><td colspan="4">Originator Sequence Number</td></tr>
</table>

Fig 2. Route Request (RREQ) Message Format

Where type is 1, J is the join and R is the repair flag which are reserved for the multicast. G is the gratuitous RREP flag, when set, the RREP is unicast to the node specified by the destination IP address field. D is the destination only flag, when set, only the destination may respond this RREQ. U is the unknown sequence no. flag, when set, indicates that the destination sequence no. is not known. Hop count is the no. of hops between the originator node and the node handling the request. The RREQ ID is the sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address. The destination IP address is the IP address of the destination for which a route is desired. The destination sequence number is the latest sequence number received in the past by the originator for any route towards the desired destination. The originator IP address is the IP address of node originated the route request. The originator sequence number is the current sequence number to be used in the route entry pointing towards the originator (source node) of the route request.

3.2 The Route Reply Message Format

A node receiving the route request may respond RREP

← Bit Positions →

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

Type	R A	Reserved	Prefix Size	Hop Count
Destination IP Address				
Destination Sequence No.				
Originator IP Address				
Life Time				

Fig 3. Route Reply (RREP) Message Format

Where type is 2, R is the repair flag, A is the acknowledgement flag. The repair flag is for multicast and when an acknowledgement is required then the flag A is set. The prefix size is of 5 bit and when nonzero, specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination. Hop count specifies the no. of hops between the originator IP address to the destination IP address. The life time is the time in milliseconds for which nodes receiving the RREP consider the route to be valid.

3.3 The Route Error Message Format

The RERR message is sent whenever a link break causes one or more destinations to become unreachable from some of the node's neighbors.

← Bit Positions →

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

Type	N	Reserved	Dest.Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Dest. IP Addresses (if needed)			
Additional Unreachable Dest. Sequence No. (if needed)			

Fig 4. Route Error (RERR) Message Format

Where type is 3, N is "no delete flag" when it is set when a node has performed a local repair of a link, and upstream nodes should not delete the route. The Dest. Count in the message indicates the number of unreachable destinations included in the message and should be at least 1. The unreachable destination IP address specifies the IP address of the destination that has become unreachable due to a link break. The unreachable destination sequence number is the sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field.

3.4 The Route Reply Acknowledgement Format

The Route Reply Acknowledgment (RREP-ACK) message must be sent in response to a RREP message with the 'A' bit set. This is typically done when there is danger of unidirectional links preventing the completion of a Route Discovery cycle. The type here is 4.

← Bit Positions →

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

Type	Reserved

Fig 5. Route Reply Acknowledgement (RREP-ACK) Message

4. THE SYSTEM MODEL

Our proposed technique gathers information about various parameters of the three lower layers viz. the physical layer, data link layer and network layer. These parameters are then made available to different layers through the common shared database which is a vital cross layer design technique and used by many researchers. After the deployment of the nodes, each node calculates their link stability, residual energy, and node degree. Based upon these metrics an observer node is deployed who observes the trust value of the neighboring nodes by closely monitoring the data transmission going on within the network. At the start, the trust value equals to 1 for

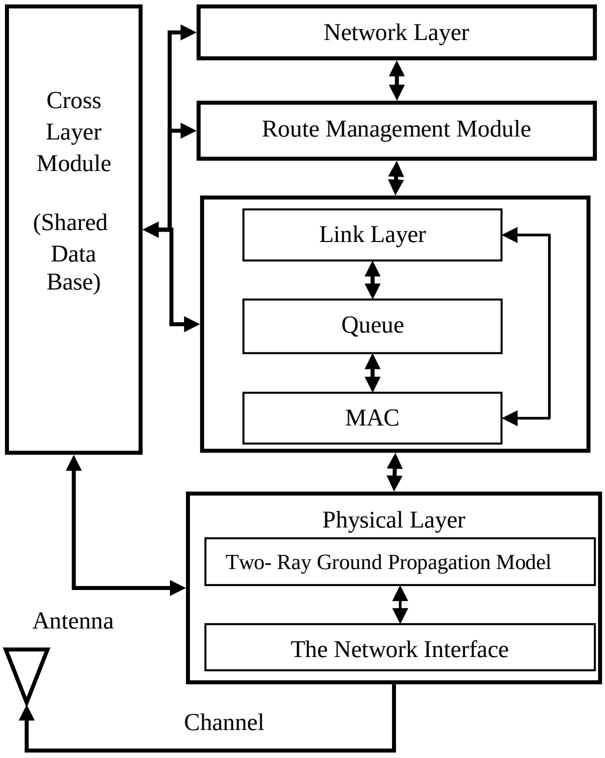

Fig 6. Cross Layer Scheme for our proposed work

each of the node and increments each time the data packet is received from an authenticated node. With each data packet transmitted on the network, the trust values of each node are updated in the AODV protocol running at the network layer. This trust value is then appended in the route request message which is further secured with the help of message authentication code (MAC) calculated at each node. When a destination receives the route request, it updates the trust value taking into consideration the success and failure of the authentication. The destination trust values are sent back to the source node through the route reply message, and the source obtains multiple routes for the desired destination but selects the route with high trust value. After this the source node supplies this path information to the MAC layer for the allocation of the access time as access control is the responsibility of MAC layer. A simple strategy adopted to allocate access time to different nodes depends upon the trust value and hence more access time is allocated to the nodes having high trust value and less access time is allocated to the nodes having small trust values.

4.1 The Channel Model

The received signal strength RSS value of the wireless channel is estimated at the physical layer which determines the link status for all the links and the link expire time is calculated with the RSS value. The link break predication is based on the RSS value which is calculated with the help of

$$P_r\,(d) = 10 \log_{10} [P_t\, G_t\, G_r\, (\lambda/4\pi d^2)\,]\ \text{dBm} \qquad \textbf{(1)}$$

where,

P_r = Received Signal Strength (function of distance d)

P_t = Transmitted Power

G_t = Gain of the Transmitting Antenna

G_r = Gain of the Receiving Antenna

d = Distance between Transmitter and Receiver

λ = Wavelength of the Radio Signal

Further, the antenna type used in our work is unidirectional whose radiation pattern is circular and radiates equally in all direction.

4.2 Estimation of the Residual Energy of a Node

In our work, all the nodes are initialized with 100 Joules of energy which will be consume in transmission, reception of the data packets and also utilized for control actions to be performed at the node level. The residual energy is the energy left out at the node after a finite time which is the difference of the initial energy and the consumed energy by the node. If there are n nodes in the network then the total energy consumed of node n^{th} node is given by

$$E_{CON} = \rho\, N_F\, E_b + \rho\, N_R\, E_b \qquad \textbf{(2)}$$

Where,

E_{CON} = Total energy consumed by the n^{th} node

N_F = No. of packets forwarded by the n^{th} node

N_R = No. of packets received by the n^{th} node

ρ = Packet size in bits

E_b = Energy per bit

The residual energy can be calculated by subtracting the consumed energy from the initial energy of the node.

$$E_{RES} = \text{Initial Energy} - E_{CON} \qquad \textbf{(3)}$$

4.3 Estimation of the Node Degree D_N

In a network like MANET, every node acts as a router to forward the packet to the next node and receives the packet from the previous node. While receiving the packet, the node must authenticate the source i.e. the previous node based on which it can judge whether the node is legitimate transmitter or a malicious node. Each node is surrounded by a number of nodes which is known as the degree of the node. For example (in Fig. 7) the node degree of node 4 is 5 as it is surrounded by 5 nodes.

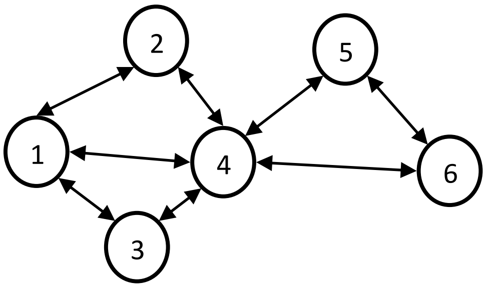

Fig 7. Node degree DN of a node in the network

$$D_N = \text{No. of the neighboring nodes} \qquad \textbf{(4)}$$

4.4 Estimation of the Link Stability

As the distance between the transmitter and receiver continuously changes in the mobility model, hence the received signal strength fluctuates and link is not stable in terms of RSS value. The consistency with which two nodes are connected with each other is known as the link stability. In MANET, the topology changes dynamically and hence the link stability is not the same always. The link stability between two nodes are given by

$$S_L = TR/d \qquad \textbf{(5)}$$

Where TR is the transmission range and d is the distance between the nodes.

4.5 Selection of the Observer Node

In the network there are n nodes deployed and to appoint an observer node among the nodes, each node broadcast a network discovery message to all the nodes in their transmission range. Each node then computes their residual energy using 2 and 3, node degree using equation 4, and link stability using equation 5. These calculated values are then feedback to each node through the network discovery message which contains the following information:

{Sending Node ID_Neighbor Node ID_Sequence Number of the Destination Node_Residual Energy of the Node E_{RES} _Node Degree D_N _Lilk Stability S_L}

Each node waits for a certain amount of time T_{wait} so that it receives all possible network discovery messages from entire network, and after which each node prepares a neighborhood table.

Table 1. Format of the Neighborhood Table which will be prepared at node 1 in which it prepare information of the neighboring node in the network.

Neighboring Node	Neighboring ID	Res. Energy E_{RES}	Node Degree N_D	Link Stability S_L
2				
3				
4				

When the neighborhood table is prepared, a node is appointed as an observer node. This appointment is based upon absolute value of residual energy, node degree and link stability calculated and entered in the neighboring table.

$$\text{Abs. Value of node A} = \alpha*TR + \beta*.D_N + \gamma*S_L \qquad \textbf{(6)}$$

Where TR is the transmission range, D_N is the node degree, S_L is the link stability, α, β, and γ are normalization constant. Such absolute values of each node are calculated and the node with the highest absolute value is selected as a observer node. So, an observer node is best in terms of the transmission range and link stability. The duty of the observer is to closely observe the network traffic and to identify any malicious behavior and also to authenticate legitimate node based on the trust values of the nodes .Any black hole attacker node will broadcast and claim that he is having the fresh route to destination ,hence can have all the data packets an retains them. The observer node will observe this activity and concludes that it is a malicious action and hence decrease the trust value of the node in the trust table. The trust table is prepared at the observer node in which all the trust values of the neighboring nodes are maintained. These trust values are broadcast periodically to all the neighboring nodes so that they can update their table of the trust values.

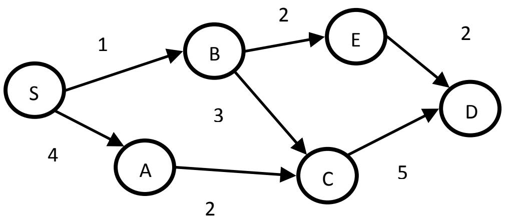

Fig 8. Figure showing the Route selection depending upon the trust values of the nodes in the network with source S and destination D. The trust values are mentioned with the link.

When the trust values are collected at the source node(s) then it calculate the trust values of all possible routes to destination and supplies to the network layer. The network layer when have multiple routes to destination, it select the one with highest trust value and in this way our communication becomes reliable. For example take the network shown in the Fig. 8 in which the source node is S and the destination node is D. There exist three routes from the source to destination. The first route is S,A,C,D with a trust value total of 11, the second route is S,B,C,D with a total trust value of 9 and the third route S,B,E,D with a total trust value of 5. The network layer must select the route S,A,C,D with the highest trust value 11 among the three available routes.

5. SIMULATION RESULTS

5.1 The performance Analysis and simulation environment

Table 2. Simulation Parameters

Simulator	NS-2 (Version 2.35)
Channel Type	Wireless Channel
Propagation Model	Two Ray Ground
Network Interface Type	Phy/WirelessPhy
MAC Type	IEEE 802.11
Interface Queue Type	Droptail Type
Link Layer Type	LL
Antenna Model	Omni directional
Energy Model	Energy Model
Routing Protocol	AODV
Topology Dimensions	1000 m×1000 m
Initial Energy in Joules	100 J
Simulation Time	20.0 s
No. of Malicious Node	5
Max. packets in the queue	50
No. of Mobile Nodes	30
Mobility Model	Random 0-20 m/sec
Network Traffic	Constant Bit Rate
Packet Size	512 bytes

The performance analysis of our proposed approach is carried out by using the network simulator NS (version 2.35) which is installed on a windows 7 operating system. The topology is made in 1000 m×1000 m area with a simulation time of 20 seconds. We have simulated the scenario with 30 nodes with random mobility model vary with 0-20m/sec with an initial energy of 100 joules. For the routing of the data packets generated at the rate of 1000 packets/sec CBR traffic, AODV routing algorithm is employed. Then we simulate a black hole attack with 1-5 malicious nodes and perform the attack. The following table summarizes our simulation parameters taken for the scenario.

5.2 The Blackhole Attack

In a black hole attack, a malicious node (attacker node) uses its routing protocol to broadcast itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of the most resent routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus have the capability to the data packet and retain it. There are two types of the black hole attack (Fig.9)

- Internal black hole attack.
- External black hole attack

In the internal type, we have an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element and is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node. In contrast, External attacker physically stays outside the network and denies the network access either by creating congestion in network or by distracting the entire network. External attack can become a kind of internal attack when it takes control over internal malicious node and control its behavior to attack other nodes in MANET network. In our work we simulate internal black hole attack as our malicious node resides inside the network and in the routes between the source and destination.

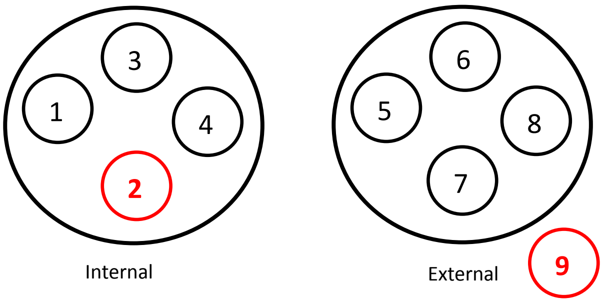

Fig 9. MANET Network in which node 2 is an internal and node 9 is an external black hole attacker.

5.3 Simulating Blackhole Attack

In our work first we simulate using ns-2.35, black hole attack in MANET. For this we modify and used AODV for the addition of the malicious node and behave like an attacker node with the help of the boolean value in our aodv.cc and aodv.h file. Further we named it as “malicious” that is used to attack on the .tcl file. If a black hole attack has to be simulated, a true malicious value in our .tcl file is to assign by using following command

```
$ns at 0.0 "[$node_(Node_ID) set ragent_] malicious"
```

This will activate black-hole in the network as we modify our aodv.cc file and due to which either all the data packets are captured by the malicious node as mentioned as “Node_ID” in the AODV or dropped.

5.4 Detecting Blackhole Attack

After the simulation of the black hole attack, next step is to detect the attack. For this we again need to add some functions in aodv.cc and aodv.h files of ns-2.35. This is done by checking each node and each data packet record which tells us the statistics about the no. of data packets received send and forward by the node, as AODV keeps this record using a vector of C++. A counter is initialized and incremented for every data packet. When a data packet is available on the network, MAC listens to the data packet and informs the network layer about the data packet for which the information in the AODV gets modified. The malicious node performing the black hole attack intercepts all the data packets and no packets are received by other nodes and this characteristic is reflected in the AODV statistics which can be used to detect the malicious behavior of the node. If any node is only receiving the data packets and not forwarding them then it may be attacker node and hence we decrease its trust value by one. At the starting point we have initialize the trust value of each node to be unity and at the end depending upon the trust value, a node having the least trust value is detected as an attacker node.

5.5 Removing the black hole attack

For removing the attacker node we again add some function into the aodv.cc and aodv.h files of AODV. By using the trust values of the nodes, we have found out attacker node and now we have to remove these nodes. For this we take use of the routing statistics available at the network layer and checks if its IP address is present in the current path. We pass a command to AODV to change the path after removing the malicious node(s). For secure AODV we again added a boolean value “remove” to update these information in the .tcl file using the command

```
$ns at 0.0 "[$node_($i) set ragent_] remove"
```

After removing the attacker node(s), our network is safe even in the presence of the internal black hole node (s).

5.6 Performance Metrics

In our work we have focused on the following performance parameters

- Throughput: It is the number of packets delivered successfully from the source to destination.
- End-to End Delay is the average time taken by the packet to be delivered from the source to destination.
- Routing Overheads is the numbers of extra bits required other than the data bits in each data packet for delivery to the destination.
- Packet Delivery Ratio is the parameter which tells how successfully the packets are delivered to the destination.

The performance metrics are calculated with our simulation and results are sketched and presented in Fig.10, 11, 12 and 13 for ready reference. The throughput delivered and packet delivery ratio of our proposed technique shows better than that of the standard AODV under attack. As per the end to end delay is concerned our proposed technique is inferior as it has to incorporate security features also for the detection of the blackhole attack and this discussion follows for the comparative high routing overheads as well. But overall our proposed technique serves with about 0.9788 detection probability to detect the blackhole attack in the MANETs.

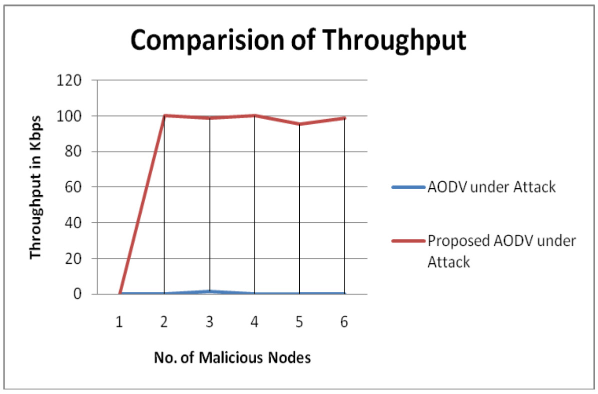

Fig 10. Compares the throughput of our proposed algorithm with the conventional AODV, under attack

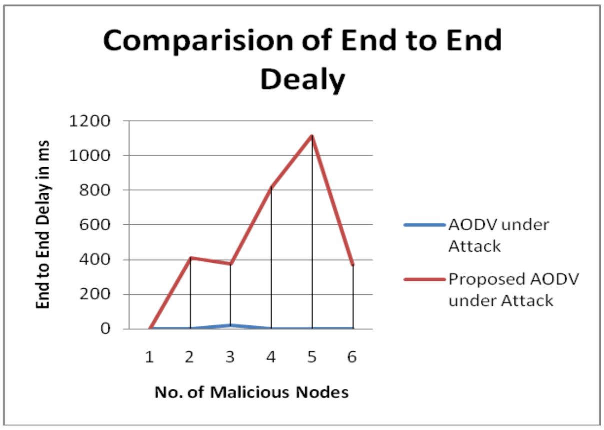

Fig 11. Compares the end to end delay our proposed algorithm with the conventional AODV, under attack

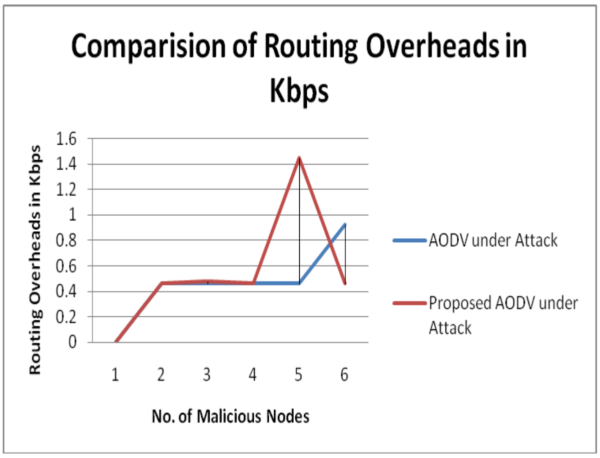

Fig. 12. Compares the routing overheads of our proposed algorithm with the conventional AODV, under attack

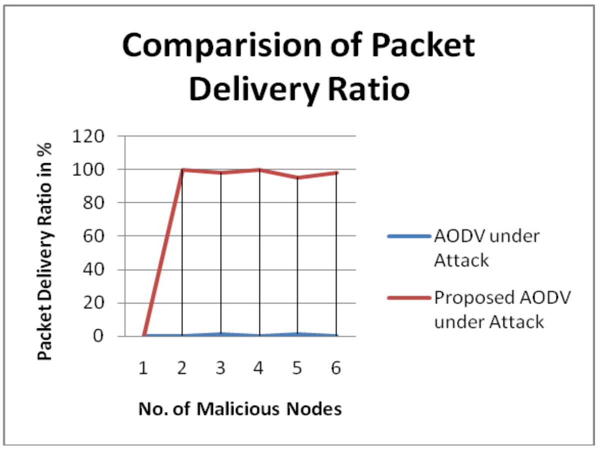

Fig. 13. Compares the routing overheads of our proposed algorithm with the conventional AODV, under attack

6. CONCLUSIONS

In this paper, we have proposed a cross layer based detection and authentication technique to detect the blackhole attack in MANETs. In our technique we have proposed an observer node that is responsible to monitor the transmission going on between the nodes and calculate the trust value of the neighboring nodes depending upon the no. of packets received and forwarded. If the rate at which the node is forwarding the data packets is much smaller than that of the rate of receiving the packets then it is a malicious behavior and detected by the observer node. For such behavior the trust value of the node is decremented every time. This trust values are informed to rest of the nodes and to protect the trust value message authentication message MAC is used. Among the different available routes to destination, the path with the highest trust value is selected. These trust values are updated at the MAC layer which then assigns the access time. More time is allotted to the node with high trust values and less time to the nodes having lower trust values. Our simulation results prove our technique to improve the security performance. .

7. REFERENCES

[1] V. Srivastava and M. Motani, “The Road Ahead for the Cross-Layer Design,” in Proc. of IEEE 2nd International Conf. on Broadband Networks, pp.551-560,vol.1, 2005.

[2] T. S. Rappaport et al., “Wireless Communications: Past Events and a Future Perspective,” IEEE Comm. Mag., vol. 40, May 2002, pp. 148–61.

[3] Min-Hua Shao ; Ji-Bin Lin ; Yi-Ping Lee, “Cluster-based Cooperative Back Proppagation Network Approach for Intrusion Detection in MANET”, IEEE10th International Conference on Computer and Information Technology (CIT), pp.1627-1632, July 2010.

[4] C. Perkins, E. Belding-Royer, S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Feb. 2003. http://www.ietf.org/internet-drafts/draftietf-manet-aodv-13.txt.

[5] V. Srivastava and M. Motani, “Cross-layer design: A survey and the road ahead,” in IEEE Communications Magazine, pp. 112-119, December 2005.

[6] R. Ludwig, A. Konrad, A.D. Joseph, and R.H. Katz. “Optimizing the End-to-End Performance of Reliable Flows over Wireless Link”. Wireless Networks,8(2/3):289–299, 2002.

[7] G. Thamilarasu, S. Mishra, and R. Sridhar, “A cross-layer approach to detect jamming attacks in wireless ad hoc net-works, in Military Communications Conference, MILCOM2006, Washington D.C, pp. 1–7, Oct 2006.

[8] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” IEEE Wireless Communications, vol.11, no.1, pp. 48–60, Feb. 2004.

[9] H. Yih-Chun, and A. Perrig, “A survey of secure wireless ad hoc routing,” IEEE Security & Privacy Magazine, vol.2, no.3, pp. 28–39, May/June 2004.

[10] C.E. Perkins, E.M. Royer, S.R. Das, and M.K.Marina, “Performance comparison of two ondemand routing protocols for ad hoc networks,” IEEE Personal Communications Magazine special issue on Ad hoc Networking, pp. 16–28, Feb. 2001.

[11] Hwee Xian TAN and Winston K. G. SEAH, “Dynamic Topology Control to Reduce Interference in MANETs” In proceedings of 2nd International Conference on Mobile Computing and Ubiquitous Networking, Osaka University Convention Centre, Osaka, Japan, 2005.

[12] A.Rajaram, Dr.S.Palaniswami, “A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks” International Journal of Computer Science and Information Security, (IJCSIS) Vol. 6, No. 1, 2009

[13] V. Kotov and V. Vasilev, “A survey of Modern Advances in Network Intrusion Detection,” in the proc. of 13th International Workshop on Computer Scince and Information Technology CSIT, pp. 18–21, 2011.

[14] John Felix Charles Joseph , Amitabha Das b, Bu-Sung Lee and Boon-Chong Seet , “CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS”, Elsevier Computer Networks, 2010.

[15] Santoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “A Self-Adaptive Intrusion Detection Method for AODV-based Mobile Ad Hoc Networks,”IEEE 2005.

[16] Yu Liu, Yang Li, and Hong Man, “Short Paper:A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks,”IEEE Computer Society ,2005.

[17] John Felix Charles Joseph , Amitabha Das, Boon-Chong Seet, and Bu-Sung Lee, “Cross layer versus Single Layer Approaches for Intrusion Detection in MANETs”, pp.194-199, IEEE 2007.

[18] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han, “A Novel Cross Layer Intrusion Detection System in MANET,” in the proc. of IEEE 14th International Conference on Advanced Information Networking and Applications, pp. 647-654, 2010.

[19] Arjun P. Athreya and Patrick Tague,” Towards Secure Multi-path Routing for Wireless Mobile Ad-Hoc Networks: A Cross-layer Strategy” 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Digital Object Identifier: 10.1109/SAHCN.2011.5984886 , pp- 146 – 148, 2011.

[20] R. Senthil Kumar and P Kamalakkannan, “A Review and Design Study of Cross Layer Scheme Based Algorithm to Reduce the Link Break in MANETs,” in the proc. of IEEE International Conference on Pattern Recognization, Informatics and Mobile Engineering, pp.139-143, 2013.

[21] G. Thamilarasu, S. Mishra, and R. Sridhar, “A cross-layer approach to detect jamming attacks in wireless ad hoc net-works, in Military Communications Conference, MILCOM2006, Washington D.C, pp. 1–7, Oct 2006.