CLDASR: Cross Layer Based Detection and Authentication in Secure Routing in MANET

K.Suresh Babu
Research Scholar
School of IT
JNT University Hyderabad, India.
Kare_suresh@yahoo.co.in

K.Chandra Sekharaiah
Professor in CSE
School of IT
JNT University Hyderabad, India
chandra_sekharaiah@yahoo.com

Abstract - In MANETs, providing the security to the network from the routing attacks like black hole and gray hole is a big challenge. To resolve the above issues, in this paper we implement a cross layer based detection and authentication technique for secure multi-path routing (CLDASR). In the authentication method, when a source wants to send a data packet or a RREQ packet, it generates a hash value also encrypts the hash with the path using the shared symmetric key with the destination. In the black hole or gray hole detection method, every node observes the next hop in current route path. The proposed method helps in detecting the malicious node caused due to the packet drop and link failure in the network. By simulation results we show that the proposed approach reduces the packet drop due to the attack and increases the packet delivery ratio in malicious environment.

Keywords: MANET, Black hole, Gray hole, Hash value, Multi-path

I. INTRODUCTION

A. MANET

MANET stands for “Mobile Ad hoc Network”. It is a temporary infrastructure less multi-hop wireless network in which the nodes can move randomly. [1]. In MANET, nodes can directly communicate with all other nodes within their radio ranges. If the nodes are not in the communication range then the nodes use the intermediates nodes to communicate with each other. [2].It is a network in which a set of mobile nodes communicate directly with one another without using an Access Point (AP) or any connection to a wired network. Here the nodes are free to move randomly and they organize themselves arbitrarily. [3]. A MANET has applications in emergency search-and-rescue operations, in decision making in the battlefield, in data acquisition operations in hostile terrain, etc. [4]. The dependent nature of nodes in MANET over the cooperative behavior of its neighbor nodes has raised security concerns. In an ad hoc network attackers can attack the network from any direction at any node that is different from the fixed hardwired networks with physical protection at firewall gateways. It means that every node should be equipped to meet an attacker directly or indirectly [3].

B. Cross layer based Security in MANET

Due to the unique nature of MANET such as signal strength, higher bit error rates, dynamic variation in channel quality, fading effects, interference problems, mobility, shared and contention based MAC, multi-hop transmission and path selection at network layer needs some degree of interaction among different layers to optimize the overall network performance. To overcome the above mentioned problem a cross layer based information exchange method is proposed to improve the overall network performance. [6].The purpose of cross-layer cooperation is adaption to channel conditions. To detect multi-layer security attacks, the only option is to consider cross layer design. [6,7]. The two approaches that can be adapted to design a cross layer security mechanism for MANET are as follows: Multiple-Inputs Single Analysis (MISA): In this method the system gathers multiple inputs from different sources (layers) and analyzes these inputs from different sources (layers) and analyzes these inputs in a single analysis engine to make a decision. Multiple- Input Multiple Analysis (MIMA): In this method, the system obtains multiple inputs from different layers and these inputs are analyzed separately in different analysis engines. The importance of cross layer design to provide security in MANET are as follows:

- A security mechanism for one layer cannot protect the other layer and hence cross layer security mechanisms are necessary to protect the multihop networks from different types of attacks.

- The basic purpose of cross layer design is to use multi layer parameters from OSI stack to increase the efficiency and performance of MANET. [6].

C. Organization of the Paper

In this paper we propose and implement a novel cross layer based detection and authentication technique for secure multi-path routing(CLDASR) in MANETs by using the various metrics form physical layer, data link layer and network layer. We investigate the mechanism by implementing the required changes on the existing routing protocol AODV. The simulation is performed using the NS-2 simulator. The rest of the paper is structured as follows. In section 2, a brief literature survey is being provided. In section 3, the cross layer based detection and authentication technique for secure multi-path routing(CLDASR) is proposed. In section 4, the results of the simulation are discussed. In section 5 and section 6, the conclusion and references are presented respectively.

II. LITERATURE REVIEW

Abderrezak Rachedi et al in paper [4] have proposed new cross-layer approach based on physical, MAC, and routing layers for a monitoring mechanism[14]. A new analytical model is proposed to illustrate the parameters' effect on these different layers. The impact of the signal to noise ratio (SNR) and the distance between monitor and monitored nodes are clearly introduced. Arjun P. Athreya et al in paper [8] have proposed the cross-layer strategy to use RSSI measurements in the physical layer to define node neighborhood, ETX measurement from the link layer and node forwarding behavior from network layer to study path reliability via a utility function. Rakesh Shrestha et al in paper [9] have proposed a novel cross layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. Leovigildo Sánchez-Casado et al in paper [10] have proposed an intrusion detection system for detecting malicious packet dropping in mobile ad hoc networks, by collecting features from the MAC and network layers[15]. The cross-layer approach uses a heuristic to detect packet dropping attacks under several circumstances which are not usually taken into account in previous works and which can cause a high number of false positives in detection. Ping YI et al in paper [11] have presented a path based method to detect black and gray hole attack.

In these previous works it is learnt that, the techniques have not implemented any features like route changes to the IDS in order to provide accuracy for the detailed information about attack detection. There is no mechanism which has considered the routing attacks like black hole and gray hole. There is no authentication for nodes and packets. They have used an isolated approach for detection method that is not suitable for the mobile networks.

III. CLDASR: Cross Layer Based Detection and Authentication in Secure Routing in MANET

A. Overview:

In our proposed solution we implement a cross layer based detection and authentication technique for secure multi-path routing(CLDASR). In CLDASR, the Cross-Layer Approach for Malicious Packet Dropping [12] is enhanced by including an authentication and routing attack detection modules. To detect the packet dropping attack, the RTS, CTS and RREQ counts are checked as per the packet dropping detection algorithm. In the authentication method [13], when a source wants to send a data packet or a RREQ packet, it generates a hash value also encrypts the hash with the path using the shared symmetric key with the destination. The intermediate nodes on receiving packets encrypt the hash and append their ID with encrypted payload from previous node and encrypt this whole message with the share symmetric key. On receiving this message, the destination decrypt the packet in the reverse order of the ID's recorded in clear text and verifies the hash sent by S. In the black or gray hole detection method, every node observes the next hop in current route path. The forwarding rate of the node is determined by the ratio of successfully forwarded packets to total number of packets routed through that node. The forwarding rate is compared against a dynamic threshold value, which is determined based on MAC layer collision report and overhearing rate. If the forwarding rate is lower than the threshold, the next hop node will be considered as a black or gray hole by the detecting node.

B. Packet Dropping Detection Method:

Assume Node S want to send the packets to the node D. Node S will send the RTS (request to send) packet to the node D, when the medium is free.In the figure (1), source sending the RTS packets to the destination and destination is not communicating with any other node, so it is free. The Source send RTS packets to its neighboring nodes and the

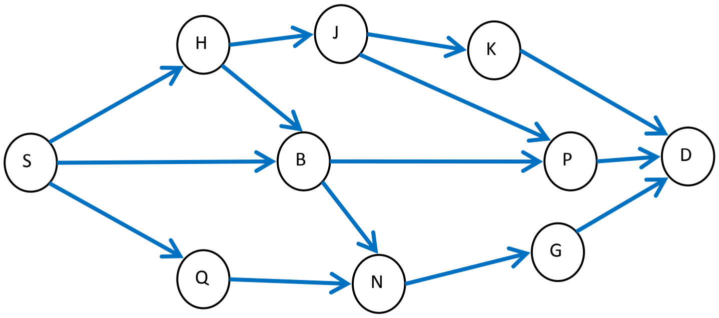

Figure 1: Source Sending RTS packet to Destination

neighboring node send it to their neighboring nodes. Like this it send up to the destination. T_m is the monitoring time and it is divided into number of slots, so that we can observe the packet dropping for every small amount of time (slot). In a single slot of time, detection will be done for each number of nodes in the network.

Node S sends a RTS message to the node D and another node also trying to send the RTS message to node D. So the messages probably suffer from collision (P_c). If there is no collision, node S replies with a CTS message. The CTS messages also suffer from collision (P_c). If node D sends the CTS message to another node, then there is a chance CTS collision. Then the probability of CTS collision is 1- P_c. Before the RTS or CTS collision node S has accessed the medium, it will transmit the desired data to D. The data is transmitted unless a channel error happens and probability for error is P_r. The node D will receive the packet, if there is no RTS/CTS collision and probability of receiving the packet is

$$P_R = (1-P_C)[1-(1-P_C).P_C](1-P_E) \qquad (1)$$

The packet is finally reached at node D and it may be dropped or forwarded to other neighboring nodes. If the packet is forwarded it may not be dropped, so the forwarded probability is

$$P_F = P_R(1-P_D) \qquad (2)$$

If the packet is dropped, then the probability of packet dropping is

$$P_D = 1-P_F/P_R \qquad (3)$$

If this effect is related to the traffic load, then we will take amount of packets that are sent in a slot of time. Consider the unanswered RTS packets, which are sent in a certain amount of time and there is a chance of collision. The probability of collision is

$$P_C^{'} = (1-P_C)[1-(1-P_C).P_C] = \frac{NR_U}{NR_T} \qquad (4)$$

I

n equation (4), NR_U , NR_T are the number of unanswered RTS messages and total sent RTS messages. P_F is obtained by the following equation

$$P_F = \frac{D_F}{D_R} \qquad (5)$$

In the equation (5), D_F is the data packets forwarded by a given node and D_R is data packets received by a given node. Calculate the P_D from the equation (3) and compare the value with TH. TH is the predefined threshold value. If the probability value is greater than the TH, then we will drop the packet, otherwise:

$$P_F = \begin{cases} \text{Drop} & \text{If } P_D \geq TH \\ 0 & \text{Otherwise} \end{cases} \qquad (6)$$

All the steps in packet dropping detection method is depicted in the following algorithm

```
Start
Define S = Time slot,
      NS = Number of time slots.
Divide the monitoring time into the number of
time slots (NS).
For S =1 to NS
For all the nodes in the network
Obtain the $NR_I(S)$, $NC_I(S)$ and $RREQ_I(S)$
Calculate the $P_C^{'}$ with the equation (4)
Calculate the $P_F$ using the equation (5)
Calculate the $P_D$ using the equation (3)
Compare the $P_A$ with TH using the equation (6)
for time slot S.
End for
End for
```

Figure 2 : Algorithm for Packet Dropping Detection

Table 1: Description of the notations

Notations	Description
T_m	Monitoring Time
S	Time Slot
NS	No. of Time slots
$NR_I(S)$	Total number of RTS messages sent by the node i to any other node in the neighborhood.
$NC_I(S)$	Total number of CTS messages replied by the neighboring node towards the node i.
$RREQ_I(S)$	Boolean Value

C. Source (S) and Destination (D) Authentication Procedure

When S wants to send a packet to D, the authentication is provided between the S and D by verifying the Hash value (HV). Assume S wants to send the data packets to the D. To construct the path between the source and destination, the source (s) will send a route request packet (RREQ) to the destination.

The source will encrypt with the Hash value (HV) with shared symmetric key with the destination and sends the encrypted Hash value (HV) to the D. The neighbouring nodes append their ID with encrypted payload from previous node and encrypt this whole message with the share symmetric key between them and D. Like this all the nodes will append their ID to encrypted payload from pervious nodes and send to the other nodes up to the D.

```
Start
Define  S = source,
            D = destination,
            $N_j$ = Neighbouring nodes
            $TS_s$ = Time Stamp of source
            $ATS_s$ = Active time stamp of source
            HV = Hash Value
            $K_{sd}$ = Key shared between the source and destination
            $K_{jd}$ = Key shared between the neighbouring node and destination ;
S wants to send data to D
S will send an encrypted data packet to the neighbouring node ($N_j$)
S encrypted message format → [$S_j$, D, HV{ HV, $TS_s$, Data}$_{Ksd}$]
The neighbouring node gets the encrypted message and appends their ID to that message
Neighbouring node message format → [$S_j$, D{j, HV,{S, D, $TS_s$, HV }$_{Ksd}$ }$_{Kjd}$]
If ($TS_s$ > $ATS_s$ )
      Drop the request.
Else if
      Neighbouring node send to its neighbouring node;
 Else if
 {
                  Neighbouring node = D;
                  D will decrypts the encrypted message and compare the HV
                  If (S. HV = D. HV )
                              Then D sends a replay packet to the S.
}
End
```

Figure 3: Algorithm for Authentication procedure for S and D

Finally the D receives the message and decrypts the packet. The decryption will be in the reverse order and the order is already noted in a clear text. After decrypting the message, D will verify the Hash value (HV) and if it matches then the D believes that packet has arrived from S.

Example for Authentication Procedure:

In the figure (1), S wants to send the data to the D. To make the path between the S and D, S sends a RREQ packet to the D. S send an encrypted data packet to the neighbouring node. Here in the example, S neighboring nodes are H, B and Q. S sends an encrypted data packet to the three neighboring nodes.

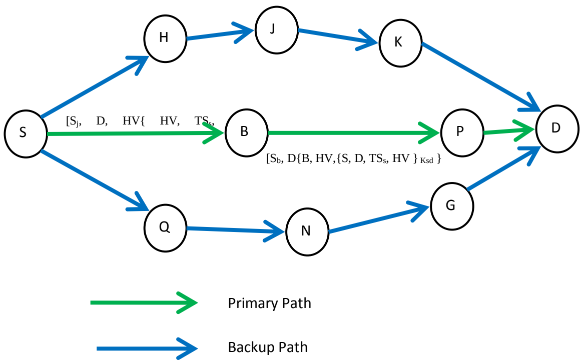

Figure 4: Example for Authentication

The neighboring node B gets the encrypted message. The neighboring node appends their ID with encrypted payload from S node and encrypts this whole message with the share symmetric key between them and D. Now it will send it to the next neighbouring node P. Now the neighboring node P will appends their ID with encrypted payload from B node and encrypts this whole message with the share symmetric key between them and D. It will send it to the next node that is the destination node (D).

D. Black Hole Detection Method

Black hole attack causes a serious damage to the network and authentication. When the source wants to communicate with destination, it will send a RREQ messages. Before getting the RREP from original destination, the attacker will send the duplicate RREP packet. Now the source node sends data packets to the black hole instead of original destination node.

In the black or gray hole detection method, every node observes the next hop in current route path. The forwarding rate of the node is determined by the ratio of successfully forwarded packets to total number of packets routed through that node [11].

$$\text{Forwarding Rate}\,(Fr) = \frac{Fs}{Tn} \qquad (7)$$

In the equation (7), Fs is the successfully forwarded packets and T_n is the total number of packets routed through that node. The forwarding rate is compared against a dynamic threshold value. We will determine the dynamic threshold based on MAC layer collision report and overhearing rate.

Dynamic Threshold Value:

The dynamic threshold is calculated based on MAC layer collision report and overhearing rate. Let P_c be the actual collision probability in the N^{th} time period. P_f be the actual forward probability of a node and P_o is the probability of a node overhearing the next hop's forward action.

$$P_o = (1-P_c)*P_f \quad (8)$$

We will calculate the P_o based on the Overhearing Rate (OVR (N)) and accumulated collision rate AR (N). We will calculate the Overheating Rate using the following equation

OVR (N) = total overhear packet number/total forward packet number

$$OVR\,(N) = \frac{T_o}{T_f} \quad (9)$$

In the equation (9), T_o is the total overhear packet number and T_f is the total forward packet number. We will calculate the Accumulated collision rate (AR) [11] using the following the equation

$$AR\,(N) = \sum_{i=1}^{N}(0.5^{N-i}) + CR\,(N) \quad (10)$$

In MAC layer collision report, we will take two integers to count the collisions. One is NC_p and second one is C_p. NC_p is the non-collision integer and it will increment by one, when a packet being received successfully. C_p is the collision integer and it will increment by one, when collision occurs. We will calculate the Collision report using the following equation

$$\text{Collision Report}\,(CR) = \frac{C_p}{C_p + NC_p} \quad (11)$$

We will calculate the P_o based on the Overheating Rate (OVR (N)) and accumulated collision rate AR (N).

$$P_f = \frac{OVR\,(N)}{1-AR(N)} < (1-T_f) \quad (12)$$

In the equation (12), T_f is the total forward packet number. If a node drops packets in a probability higher than T_f , the detecting node can accuse it as a gray hole attack.

Total Work Flow

When S wants to transmit the data to node D. S will send the data using the Authentication procedure. S will encrypt with the Hash value (HV) with shared symmetric key with the destination and sends the encrypted Hash value (HV) to the D. The neighbouring nodes append their ID with encrypted payload from previous node and encrypt this whole message with the share symmetric key between them and D. The node D gets the encrypted message from the neighbouring nodes and decrypts the message, the way it gets. Node D will compare the hash value with source hash value. If both matches, D trusts it has come from original S and start sending the RREP packets to S. If the hash value does not match, node D won't give any replay to the source. When the authentication is successfully checked, the node D will send RREP to the S. A path is established between S and D. Now every node checks for black hole attack, by using the black or gray hole detection method. Every node will calculate the forwarding rate of the neighboring node and compare the forwarding rate with threshold value. If the forwarding rate is lower than the threshold, the next hop node will be considered as a black or gray hole by the detecting node. The advantages with this method are:

- The proposed method helps in detecting the malicious node caused due to the packet drop and link failure in the network.
- It avoids any kind of collision and overhead in the network.

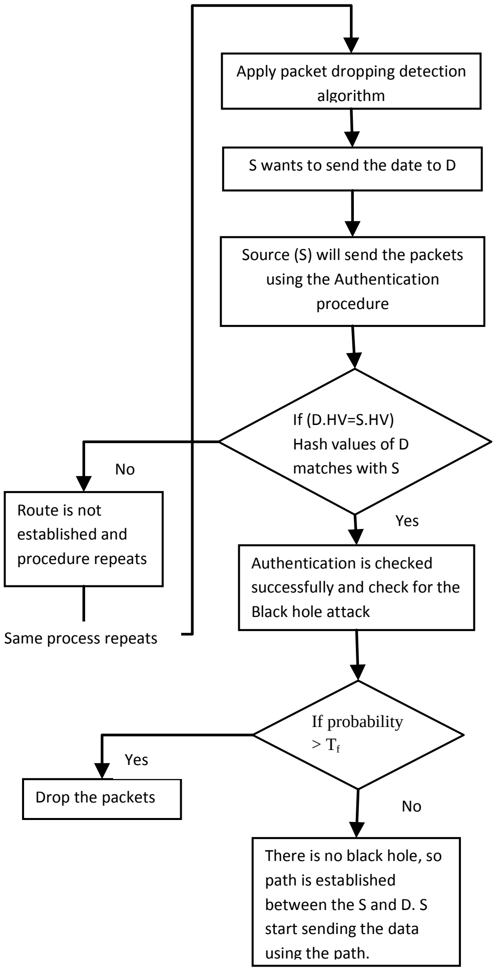
Apply packet dropping detection algorithm
S wants to send the date to D
Source (S) will send the packets using the Authentication procedure
If (D.HV=S.HV) Hash values of D matches with S
No
Yes
Route is not established and procedure repeats
Same process repeats
Authentication is checked successfully and check for the Black hole attack
If probability > T_f
Yes
Drop the packets
No
There is no black hole, so path is established between the S and D. S start sending the data using the path.

Figure 5: Work Flow

IV. SIMULATION RESULTS

A. Simulation Model and Parameters

The Network Simulator (NS2) , is used to simulate the proposed architecture. In the simulation, the mobile nodes move in a 750 meter x 750 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in table.

No. of Nodes	20,60 and 100
Area Size	750 X 750
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Sources	4
Attackers	2,4,6,8 and 10

B. Performance Metrics

The proposed Cross Layer Based Detection and Authentication in Secure Routing (CLDASR) is compared with the PDD technique. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio:** It is the ratio between the number of packets received and the number of packets sent.
- **Packet Drop**: It refers the average number of packets dropped during the transmission
- **Received Throughput**: It is the number of packets received by the receiver.

C. Results

4.3.1 Case-1 (20 node scenario)

In our experiment we vary the number of attackers as 2,4,6,8 and 10.

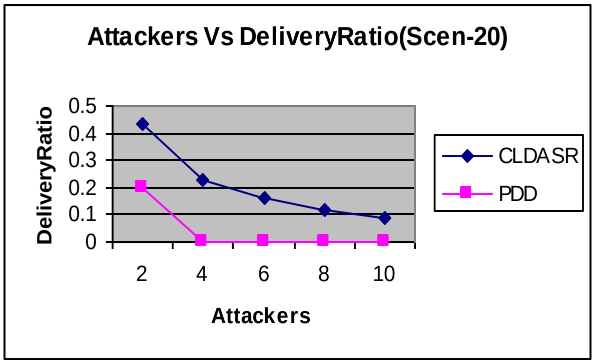

Figure 6: Attackers Vs Delivery Ratio

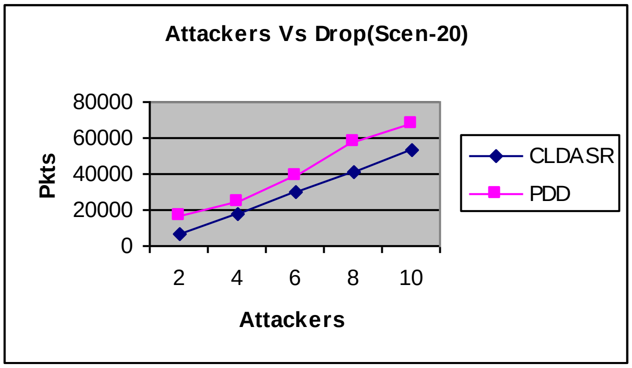

Figure 7: Attackers Vs Drop

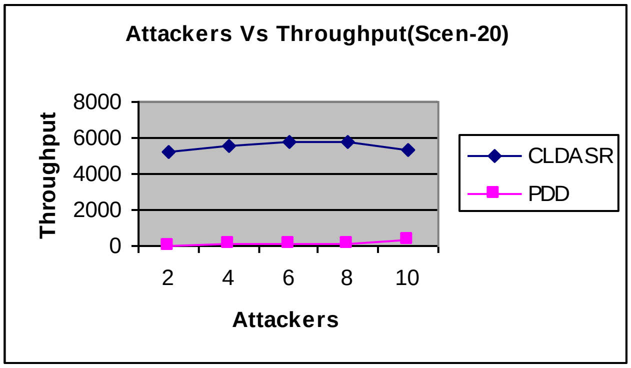

Figure 8: Attackers Vs Throughput

Figure 6 shows the delivery ratio of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the delivery ratio of our proposed CLDASR approach has 91% of higher than PDD approach.

Figure 7 shows the Packet drop of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the drop of our proposed CLDASR approach has 33% of less than PDD approach.

Figure 8 shows the received throughput of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the throughput of our proposed CLDASR approach has 97% of higher than PDD approach.

4.3.2 Case-2 (60 node scenario)

In our experiment we vary the number of attackers as 2,4,6,8 and 10.

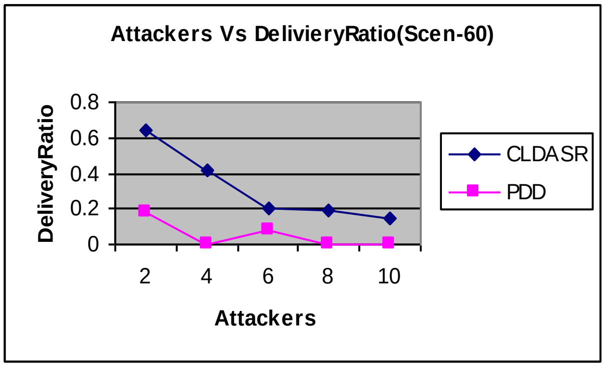

Figure 9: Attackers Vs Delivery Ratio

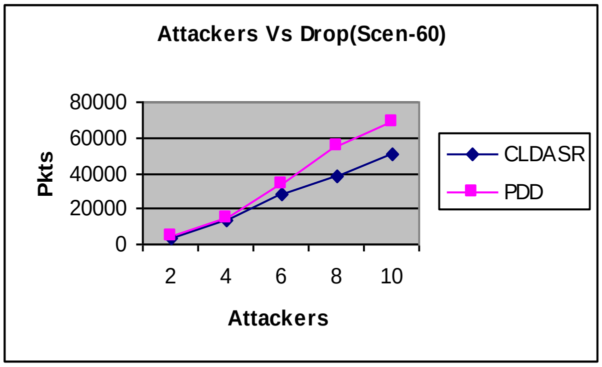

Figure 10: Attackers Vs Drop

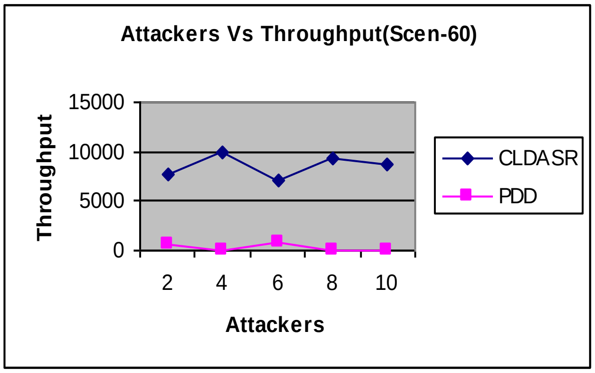

Figure 11: Attackers Vs Throughput

Figure 9 shows the delivery ratio of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the delivery ratio of our proposed CLDASR approach has 85% of higher than PDD approach.

Figure 10 shows the Packet drop of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the drop of our proposed CLDASR approach has 20% of less than PDD approach.

Figure 11 shows the received throughput of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the throughput of our proposed CLDASR approach has 96% of higher than PDD approach.

4.3.3 Case-3 (100 node scenario)

In our experiment we vary the number of attackers as 2,4,6,8 and 10.

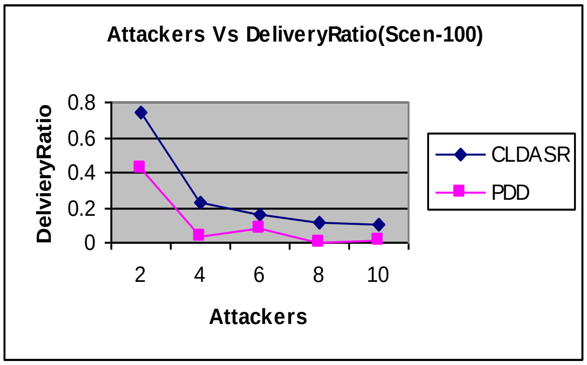

Figure 12: Attackers Vs Delivery Ratio

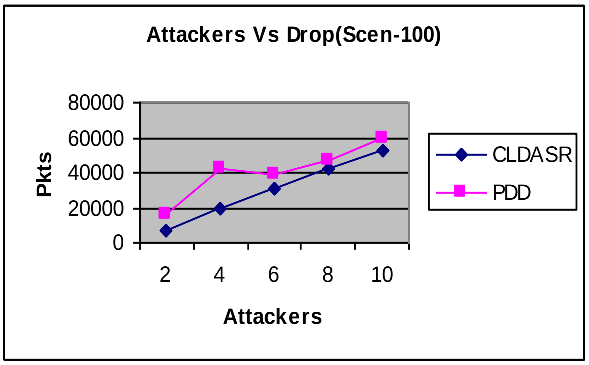

Figure 13: Attackers Vs Drop

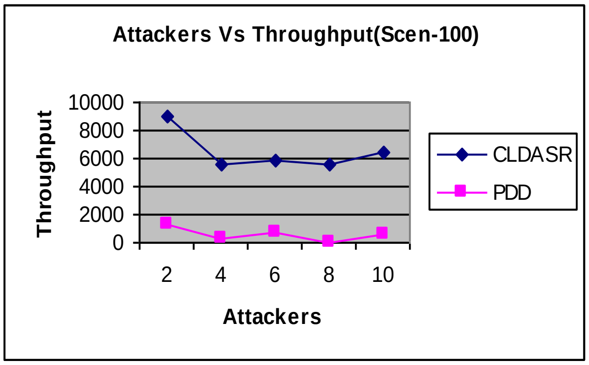

Figure 14: Attackers Vs Throughput

Figure 12 shows the delivery ratio of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the delivery ratio of our proposed CLDASR approach has 73% of higher than PDD approach.

Figure 13 shows the Packet drop of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the drop of our proposed CLDASR approach has 30% of less than PDD approach.

Figure 14 shows the received throughput of CLDASR and PDD techniques for different number of attacker scenario. We can conclude that the throughput of our proposed CLDASR approach has 92% of higher than PDD approach.

V. CONCLUSION

In this paper, we have implemented a cross layer based detection and authentication technique for secure multi-path routing. In the proposed solution, the Efficient Cross-Layer Approach for Malicious Packet Dropping is enhanced by including an authentication and routing attack detection modules. To detect the packet dropping attack, the RTS, CTS and RREQ counts are checked as per the packet dropping detection algorithm. In the authentication method, when a source wants to send a data packet or a RREQ packet, it generates a hash value also encrypts the hash with the path using the shared symmetric key with the destination. In the black or gray hole detection method, every node observes the next hop in current route path. The proposed method helps in detecting the malicious node caused due to the packet drop and link failure in the network. By simulation results we have shown that the proposed approach reduces the packet drop due to the attack and increases the packet delivery ratio in malicious environment.

VI. REFERENCES

1. Rajaram, A., and Dr S. Palaniswami. "A trust based cross layer security protocol for mobile ad hoc networks." arXiv preprint arXiv:0911.0503 (2009).

2. Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2008): 1-23.

3. Gopinath, S., S. Nirmala, and N. Sureshkumar. "Misbehavior Detection: A New Approach for MANET."

4. Rachedi, Abderrezak, and Abderrahim Benslimane. "Toward a cross-layer monitoring process for mobile ad hoc networks." Security and Communication Networks 2.4 (2009): 351-368.

5. Joseph, John Felix Charles, et al. "CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS." Computer Networks 54.7 (2010): 1126-1141.

6. Amardeep Singh, and Gurjeet Singh, “Security in Multi-hop Wireless Networks”, IJCST Vol. , Iss ue 2, June 2011.

7. Manikandan, K. P., and Satyaprasad2 K. Rajasekhararao. "A Cross Layered Architecture and Its Proposed Security Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks."

8. Athreya, Arjun P., and Patrick Tague. "Towards secure multi-path routing for wireless mobile ad-hoc networks: A cross-layer strategy." Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference on. IEEE, 2011.

9. Shrestha, Rakesh, et al. "A novel cross layer intrusion detection system in MANET." Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, 2010.

10 S'nchez-Casado, Leovigildo, Gabriel Maci'-Fern'ndez, and Pedro Garcia-Teodoro. "An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.

11. Cai, Jiwen, et al. "An adaptive approach to detecting black and gray hole attacks in ad hoc network." Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, 2010.

12. K. Suresh Babu, K.Chandra Sekhariah. “Security in MANETs Using Cross Layer Design (CLD)”, Proc of 2nd International Conference on Advanced Computing Methodologies (ICACM – 2013), ELSEVIER Publications, pp 448 – 452, August 2013.

13. K.Suresh Babu, K.Chandra Sekhariah, “*Securing AODV With Authentication Mechanism Using Cryptographic Pair Of Keys”, International Journal of Computer Science and Information Security (IJCSIS)*, USA, Vol 11 No. 2, pp 42-45, February 2013.

14. K.Suresh Babu, K.Chandra Sekhariah, B.Sasidhar, “Issues Related to Routing and Security in Mobile Adhoc Networks”, CI-4.7, *International Conference Systemics, Cybernetics and Informatics ICSCI-2009, January 07-10 2009*

15. K.Suresh Babu, K.Chandra Sekhariah, “Cross Layer Based Security in Manets”, *International Journal of Advanced Research in Computer Science(IJARCS), INDIA*, page 57-60, Vol. 4, No.4, May 2013.

AUTHORS PROFILE

K.Suresh Babu has done his M. Tech (Computer Science) from Central University, Hyderabad and presently pursuing Ph. D. from JNT University in the field of Network Security in MANETs. He has a teaching experience of 12years.His subjects of interests are Computer Networks, Network Security, Wireless Networks and Mobile Computing, Security in Mobile Computing. He published several papers in international journals and national journals, also participated and presented papers in International and National Conferences. He is presently course coordinator for M.Tech(Computer Science). He is also Program Officer for Nation Service Scheme(NSS) Unit at School of IT. He is also Cisco Certified Academy Instructor(CCAI).

K.Chandra Sekharaiah has done his M.Tech.(Computer Science) from JNTU Hyderabad and Ph.D. from IIT Madras. He is currently working as professor of CSE in School of Information Technology, JNT University Hyderabad, Hyderabad.