Cluster based Authentication Scheme (CBAS) for Secure Routing in MANET

C. Sivaranjani Devi
M.E, Communication Systems,
Saranathan College of Engineering,
Trichy, India

S.A. Arunmozhi
Associate Professor, ECE,
Saranathan College of Engineering,
Trichy, India

ABSTRACT

MANET consists of a collection of independent mobile nodes connected by wireless links, where they can join or leave the network at any time. Due to infrastructure-less and mobility in nature, secure routing is essential in MANET to transmit packets from source to the destination. There are different types of routing attacks which causes disruption of the whole network. In our proposed method called CBAS, provides secure routing in MANET against wormhole attack. Hence the nodes are grouped into cluster and each cluster is governed by the cluster head and cluster heads are controlled by the master head node. Zero Knowledge Protocol (ZKP) is used to apply authenticity among the nodes. Communication starts between the source node and the destination node after ensuring that the network contains only the true nodes.

Keywords

Manet, Clustering, Authentication, Security.

1. INTRODUCTION

MANET is a self-organizing network without relying on any predefined infrastructure [1]. The nodes may either perform as host or a router. Nowadays MANET is most popular with users and it is widely used in many applications [2] like military, conferences, search and rescue, emergency operations etc. Hence they do not pretend on any centralized entity to monitor the network. MANET is subjected to many security issues due to the nature of mobility, infrastructure-less and lack of centralized agent. In order to perform the delivery of messages from one point of location to another point of location in the network, routing is essential. Routing can be performed either by single hop or multi hop. If source and destination are in direct contact, there is no need of intermediate nodes and if it is not in the line of sight, routing occurs through intermediate nodes. Routing protocols are a principal standard to route the data packets from one node to another. There are different types of routing protocols [3] to establish a routing mechanism in MANET. They are proactive, reactive and hybrid protocols. Proactive routing protocol is a table driven routing protocol, where each node maintains table. Reactive protocol, on the other hand, establishes route, whenever there is a route demand by the user. Hence the maintenance of topology is not required. Hybrid routing protocol is the combination of both proactive and reactive routing protocol. Hence communication occurs at network layer and therefore there are different types of routing attacks which causes routing disruption like packet dropping, selective forwarding and modification of packets etc.

Security in the network is said to be achieved only when it satisfies the security goals like confidentiality, authentication, integrity, availability and authorization. Authentication is a process carried out by two parties in order to identify one another. Without authentication, an unauthorized node can enter into the network and use the available resources within the network. This unauthorized node may behave as malicious user and do malicious activities, which degrades the performance of the network. Therefore necessary preventing mechanism would be taken for unauthorized nodes entering into the network.

2. RELATED WORK

Sweety Goyal and Harish Rohil [4] developed a neighbor node analysis approach to identify the attack and removes the attacker node from MANET. In neighbor node analysis approach, they analyzed the neighbor nodes to check the authenticity of nodes for secure transmission of data among networks. According to this approach, a node will request to its neighboring nodes and perform a request and response mechanism. Therefore if the reply time is not accurate, then there is an attack in the network. As the transmission starts source node search for a neighbor list and the source encrypt the RREQ packet with the public key of neighboring node and distribute it to all around. If the neighboring node receives RREQ packet, decrypt using by its own private key, then if the node get authenticated it will send RREP packet to source node otherwise it is removed from the neighbor list.

Kamini Singh, Gyan Singh and Arpit Agarwal [3] designed a cluster based approach to mitigate the wormhole attack based on a trust value and the network has a number of clusters, where each cluster consists of a number of nodes and a cluster head. Node nearer to the cluster head acts as a server node. This server node is responsible for the authentication. If a node is authenticated by the server node, then it included in the network or else excluded i.e. that node ID is deleted and are not added in the transmission path.

Mohit Kumar and Nidhi Shalya [5] proposed a token based approach to secure AODV. In this approach, once a route is established between source and destination, authentication to be performed for the source and destination. Hence a double encryption algorithm is used to increase the security level. This method reduces the packet loss due to malicious node to a considerable extend and hence enhance the performance.

Nidhi Nigam, Vishal Sharma and Mahesh Malviya [6] present the concept based on the principle of RBS (Reference Broadcasting System). Hence the relative velocity between the sender and the receiver were calculated by using the concept of RBS. By this RBS theory, a node which is nearer to the sender node will be chosen as a reference node. According to this approach, if the threshold value of the malicious node does not match with the defined threshold, it cannot impersonate.

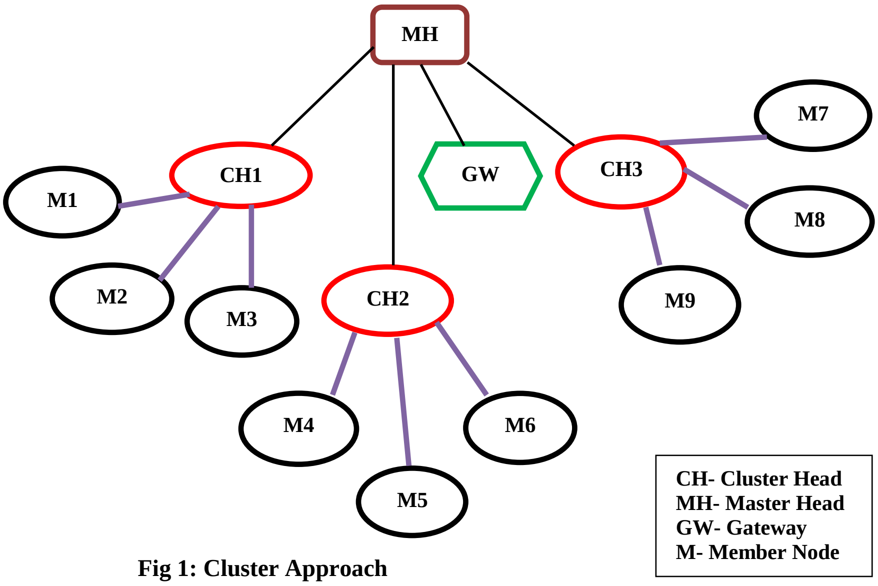


Fig 1: Cluster Approach

This process is continued until the packet reaches the destination. Whenever the packet reaches the destination, the processing approach is started to determine whether the node is trusted or not. A node that takes place in data transmission will move from its position and informs about the change to all other nodes, which are taking place in data transmission. If the above circumstances are satisfied, then the authentication of the node is confirmed and the packet is sent otherwise the next neighbor is selected for data transmission.

Mohini Gupta and Amit Kanungo [7] proposes a routing entry base detection technique and neighbor trustworthy base technique to provide secure and as well as reliable communication. The research in this paper establishes the foundation work to design IPS mechanism to identify the nodes and the links which are actively involved in the network.

3. SECURITY THREATS IN MANET

MANETs are widely used in many applications, security challenges have become a major concern to provide secure communication. Absence of centralized entity makes MANETs vulnerable to various types of security attacks [8]. Attacks are broadly classified into two categories as active and passive attacks. Passive attacks simply eavesdrops the packet transmission and do not make any malicious activities like packet dropping and packet modification. Active attacks are different from passive attacks and thus alter the data packets that are being exchanged in the network. Some of the attacks launched in MANET routing protocols, causes serious disruption in routing. These attacks are listed below.

3.1 Black Hole Attack

In black hole attack [9], a malicious node advertises itself that it has a valid route to the destination. With this intension, the attacker consumes or intercepts the packet without any forwarding. The attacker will then receive the network traffic of other nodes and do packet dropping.

3.2 Gray Hole Attack

Gray hole attack [10] is an extension of black hole attack in which malicious node behaviors and activities are unpredictable. In this, malicious node advertise a same behavior as a true node during route discovery process and silently drops some packets or also forward packets even when no congestion occurs.

3.3 Rushing Attack

In rushing attack [9], all nodes send the routing packets towards the destination, where an attacker node can rush the routing packets towards the destination quickly by saying that it has the shortest path to the destination than the all other normal nodes, leading to problems with routing.

3.4 Byzantine Attack

In byzantine attack [12], a single intermediate or a group of intermediate nodes behaves as a malicious node, either create a routing loop or direct the data packets to non-optimal path or selectively drop the packets.

3.5 Wormhole Attack

Wormhole attack [11] is a type of routing attack which leads to the disruption of communication. Among all the attacks, wormhole attack is the most serious one, because two colluding nodes act as attacker and they tunnels packet from one point of location to another point of location in network via wireless link. Hence the attackers locate a powerful position in MANET and it degrades the network performance.

4. PROPOSED METHODOLOGY

MANET is highly susceptible to many attacks, specifically the routing attacks. The objective is to provide secure routing against the wormhole attack using CBAS and to ensure that only true nodes are present in the network. The proposed methodology addresses the verification of nodes ensuring that the network containing true nodes. The zero knowledge protocol (ZKP) authentication scheme is used to authenticate all the nodes present in the network. By this way all the nodes present within the network will be true nodes and secure communication can takes place.

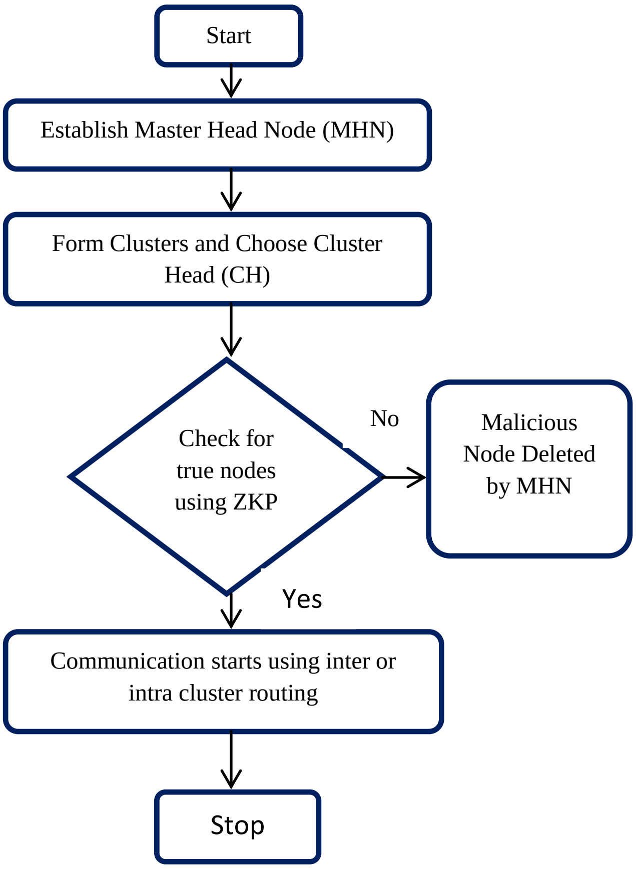

Start
Establish Master Head Node (MHN)
Form Clusters and Choose Cluster Head (CH)
Check for true nodes using ZKP
No
Malicious Node Deleted by MHN
Yes
Communication starts using inter or intra cluster routing
Stop

Fig 2: Flow Diagram

4.1 Algorithm

1. Master Head node and gateway node are established.
2. Clusters are formed and elect cluster head for every cluster.
3. Zero knowledge protocol (ZKP) is used for verifying authentication.
4. The authenticity of cluster heads is verified by the master head node and member nodes authenticity is verified by the respective cluster head.
5. If any node in the network identified as wormhole node during authentication process, that node ID will be deleted by the master head node, else step (6) is followed.
6. The intra or inter cluster routing is established to start communication.
7. Packets are forwarded from source node to the destination node using the established routes.

The network contains master head node, gateway node, cluster head and the member nodes. The master head node is powerful and has all information about the total network. The network is divided into clusters with minimum number of nodes. The node with maximum neighbor in a cluster is elected as a cluster head. The cluster based approach of network is used as shown in Figure 1. The need for clustering is to achieve scalability in presence of large networks and high mobility. This clustering technique is used to reduce traffic during routing process and it helps to reduce signaling messages. Therefore in every cluster, the header receives frequent signaling message to have necessary information about other clusters and it provides these information to the nodes in the cluster when needed. Thus clusters are formed and the nodes in the network are authenticated using Zero Knowledge Protocol (ZKP) to ensure that all the nodes present in the network are not malicious. The authentication level includes as the cluster heads are verified by the master head node and the member nodes are verified by the respective cluster head. Hacking such a network is not possible due to the nature of very strict in proving the nodes as true nodes. If the authentication scheme detects any node as wormhole node during authentication process, that node id would be removed by the master head node from the network. After ensuring that the true nodes present in the network, communication starts between the source node and the destination node using intra or inter cluster routing. If source and destination node are present in same cluster, then it corresponds to intra cluster routing, where communication takes place via cluster head. If source node present in one cluster and the destination node in another cluster, therefore it refers to inter cluster routing and the communication takes place via cluster head and gateway node. Finally the packets are forwarded from source node to the destination node using the established routes.

4.2 Zero Knowledge Protocol (ZKP)

This algorithm performs the verification of nodes in the network. A zero knowledge authentication is a protocol which takes place between two parties called the prover and the verifier. In ZKP [13], prover has to prove the verifier, without revealing any secret. The member head node acts as a trusted third party (T). The master head node has information about the whole network. Master Head node maintains n as public key, which is a prime number which will be shared among nodes during communication. The algorithmic process of Zero knowledge protocol is as discussed below.

a. T is a trusted third party and n is a prime number
b. Prover selects the value of s and computes $v = s^2 \bmod n$.
c. Prover registers v with T as his public key where s is kept secret.
d. Prover → Verifier: $p = r^2 \bmod n$
e. Verifier → Prover: $e \in \{0, 1\}$
f. Prover → Verifier: $y = r\, s^e \bmod n$
   If $e = 0$, $y = r$
   or
   If $e = 1$, $y = r\, s \bmod n$
g. Verifier calculates
   $y^2 \bmod N = ((r\, s \bmod N)^2 \bmod N)$
   $y^2 = (r^2 \bmod N) * (s^2 \bmod N)$
   $y^2 = p * v$

Thus the Verifier got both p and v from the above steps. Therefore it compares with y^2 and confirms authenticity of prover node. The algorithm never directly passes the secret key. Instead the key is enclosed in some operations. This kind of authenticity makes the attacker, difficult to enter into the network.

5. IMPLEMENTATION

5.1 Simulation Parameters

The cluster based approach is simulated using network simulator version 2.35. The proposed approach is simulated using a rectangular scenario of 802*521 square areas. CBR (Constant Bit Rate) traffic is used to generate UDP packets for the simulation. The total simulation time to analyze the proposed work performance is 90 seconds. There are different types of packet sizes used in NS-2.

Table 1. Simulation Parameters

PARAMETER	VALUE
Area	802*521
Simulation Time	90 seconds
Number of Nodes	22
Mobility Model	Random way point
Traffic Model	CBR(UDP)
Number of Wormhole Tunnel	1
Mac Protocol	802.11
Transmission Range	250m

5.2 CBAS Scheme

The cluster based scenario as shown figure 3 is simulated using network simulator-2 [14]. The network topology consists of 22 nodes. It has 1 master head node, 4 gateway nodes which perform inter cluster routing and it is common to all clusters. 4 clusters are formed and each cluster consists of 4 nodes each. Cluster head is elected for each cluster based on maximum neighbors.

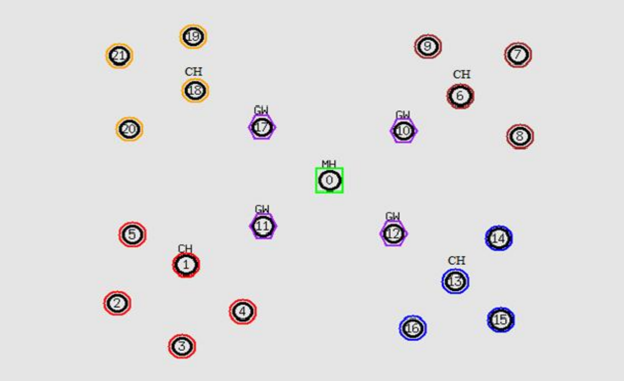
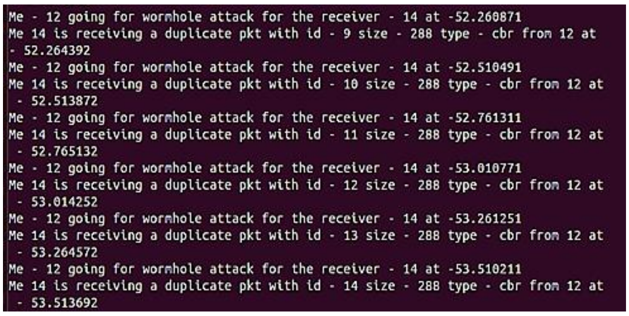


Fig 3: Cluster Scenario

Hence node 12 is positioned as wormhole attack, where it tunnels packet to the node 14. The wormhole attack will be included in the network for 10 seconds. Thus the wormhole attacker node tunnels packet to the node 14 is shown in figure 4.



```
Me - 12 going for wormhole attack for the receiver - 14 at -52.260871
Me 14 is receiving a duplicate pkt with id - 9 size - 288 type - cbr from 12 at
- 52.264392
Me - 12 going for wormhole attack for the receiver - 14 at -52.510491
Me 14 is receiving a duplicate pkt with id - 10 size - 288 type - cbr from 12 at
 - 52.513872
Me - 12 going for wormhole attack for the receiver - 14 at -52.761311
Me 14 is receiving a duplicate pkt with id - 11 size - 288 type - cbr from 12 at
 - 52.765132
Me - 12 going for wormhole attack for the receiver - 14 at -53.010771
Me 14 is receiving a duplicate pkt with id - 12 size - 288 type - cbr from 12 at
 - 53.014252
Me - 12 going for wormhole attack for the receiver - 14 at -53.261251
Me 14 is receiving a duplicate pkt with id - 13 size - 288 type - cbr from 12 at
 - 53.264572
Me - 12 going for wormhole attack for the receiver - 14 at -53.510211
Me 14 is receiving a duplicate pkt with id - 14 size - 288 type - cbr from 12 at
 - 53.513692
```

Fig 4: Node12 Tunnels Packet to Node 14

In figure 5, node 12 is identified as a wormhole attacker during the authentication process using ZKP and that node will be deleted by the master head node.

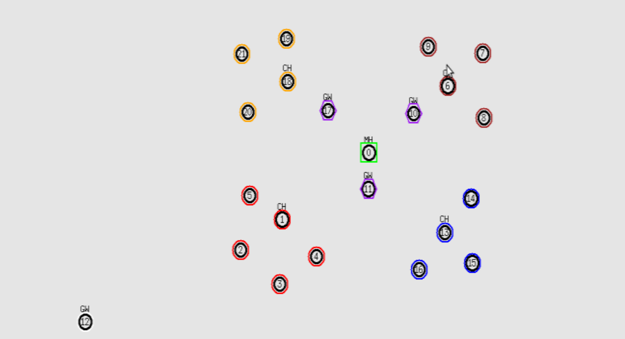


Fig 5: Node12 Wormhole Attack Node Deleted by MH

Thus the wormhole attacker node is deleted from the network and the routing process will be performed. In figure 6, node 3 acts as source node and the node 15 acts as destination node. The node 3 belongs to cluster 1 and node 15 belongs to cluster 3. Hence the source node and the destination node are present in different clusters, inter cluster routing is enabled to transfer the packet from source to destination. The communication in inter cluster routing occurs via the source nodes cluster head and gateway node and destination nodes cluster head and gateway node. As in figure 6, the estimated route by inter cluster routing to transfer the packet is 3-1-11-10-13-15.

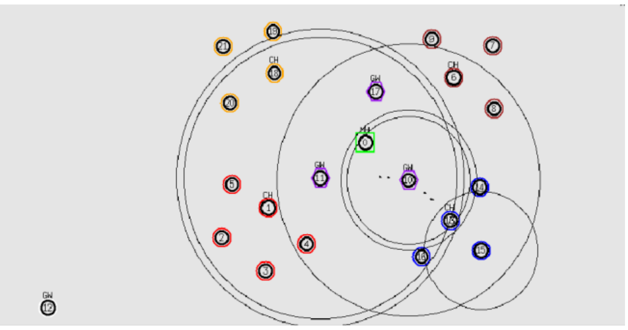
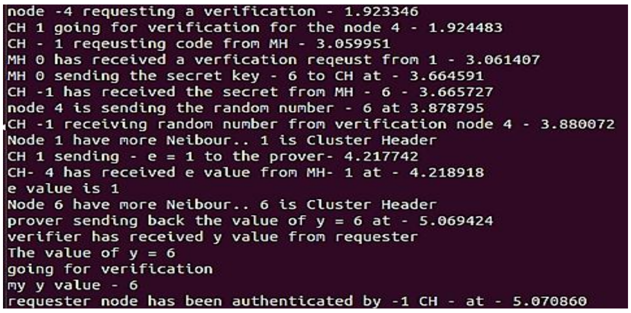


Fig 6: Communication by Inter Cluster Routing

5.3 Authentication of Nodes

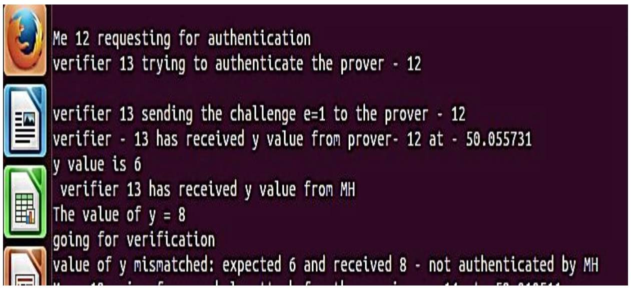
The nodes present in the network are authenticated using zero knowledge protocol (ZKP). The ZKP uses a challenge and response mechanism to authenticate the nodes. The ZKP is used to ensure the network contains only the true nodes. A sample of single node from each cluster is verified using Zero knowledge protocol and confirms the authenticity of true nodes. In figure 7, node 4 belongs to cluster 1 gets authenticated by the respective cluster head ID 1. Similarly all the nodes present in the network are authenticated using ZKP.



```
node -4 requesting a verification - 1.923346
CH 1 going for verification for the node 4 - 1.924483
CH - 1 reqeusting code from MH - 3.059951
MH 0 has received a verfication reqeust from 1 - 3.061407
MH 0 sending the secret key - 6 to CH at - 3.664591
CH -1 has received the secret from MH - 6 - 3.665727
node 4 is sending the random number - 6 at 3.878795
CH -1 receiving random number from verification node 4 - 3.880072
Node 1 have more Neibour.. 1 is Cluster Header
CH 1 sending - e = 1 to the prover- 4.217742
CH- 4 has received e value from MH- 1 at - 4.218918
e value is 1
Node 6 have more Neibour.. 6 is Cluster Header
prover sending back the value of y = 6 at - 5.069424
verifier has received y value from requester
The value of y = 6
going for verification
my y value - 6
requester node has been authenticated by -1 CH - at - 5.070860
```

Fig 7: Node 4 gets authenticated by CH Node 1

In figure 8, node 12 belongs to cluster 2 gets authenticated by the respective cluster head ID 13. During authentication process the information between the prover and the verifier gets mismatched. Therefore node 12 is not authenticated by its cluster head.



```
Me 12 requesting for authentication
verifier 13 trying to authenticate the prover - 12

verifier 13 sending the challenge e=1 to the prover - 12
verifier - 13 has received y value from prover- 12 at - 50.055731
y value is 6
 verifier 13 has received y value from MH
The value of y = 8
going for verification
value of y mismatched: expected 6 and received 8 - not authenticated by MH
```

Fig 8: Node 12 not authenticated by its CH Node 13

6. PERFORMANCE ANALYSIS

6.1 Throughput

Throughput is the rate of successful message delivery over a communication channel. In figure 9, the throughput has been noted for different packet sizes. The x-axis denotes the packet size and the y-axis denotes the throughput value in kbps.

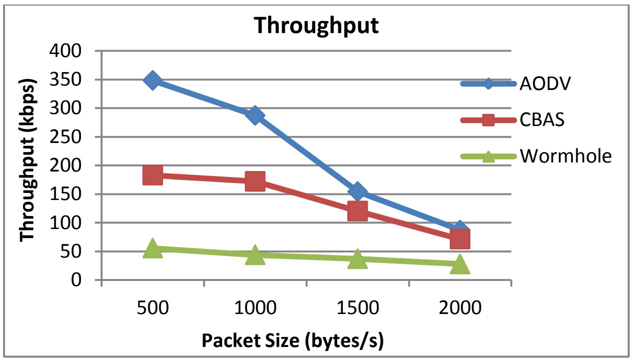


Fig 9: Throughput vs. Packet Sizes

It is inferred from the figure that, when the packet sizes are increased, the throughput value get decreased. The throughput value of the CBAS approach is high as compared to the presence of wormhole attack network because it prevents the wormhole attack using a CBAS scheme and low when it is compared to the normal AODV routing network.

6.2 Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of total number of packets received to the total number of packets sent.

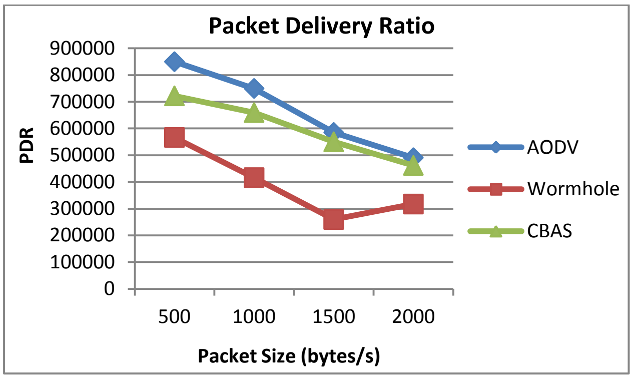


Fig 10: PDR vs. Packet Sizes

The wormhole included network has a least PDR value when it compared to the CBAS and the normal AODV routing network.

6.3 Average End to End Delay

Average end to end delay is the total time taken for a packet to reach from source to destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and the propagation and transfer times.

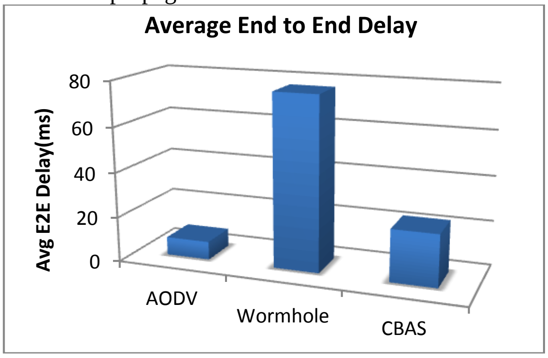


Fig 11: Average End to End Delay

Therefore the average end to end delay increases drastically as 76.852ms, when the wormhole attack included in the network, leading to more time consumption.

6.4 Normalized Routing Load

Normalized routing load is defined as the total number of routing packets transmitted per data packet. In figure 12, the normalized routing load is calculated for the three different networks as proposed method, with the presence of wormhole attack and the normal AODV routing network and it is compared for different packet sizes. Thus the routing load will always be high for the wormhole included network.

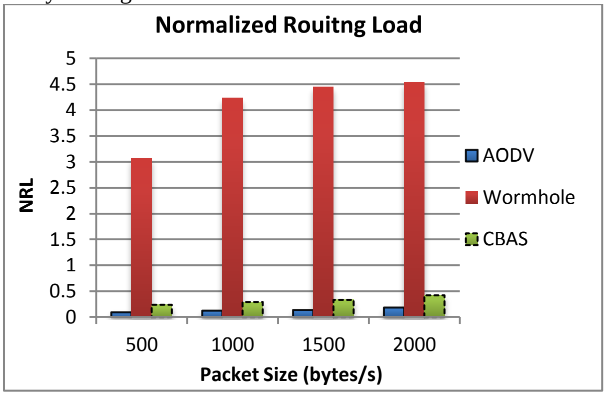


Fig 12: NRL vs. Packet Sizes

7. CONCLUSION

In this paper, we proposed a CBAS scheme to provide secure routing against wormhole attack in MANET. Authentication is one of the best security solutions which protect the whole network. Therefore the packets from source to destination are forwarded in secure manner by employing an authentication scheme called zero knowledge protocol (ZKP). The wormhole node will be deleted by the master head node during the authentication process and then the communication starts between the source node and the destination node. Therefore the performance characteristics have been improved by proposed approach in the presence of wormhole attack. The implementation and simulations were carried out using the network simulator-2. Future work includes an indent to work on energy consumption.

8. REFERENCES

[1] Ramandeep Kaur and Jaswinder Singh “Towards Security against Malicious Node Attack in Mobile Ad Hoc Network” in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[2] Samiksha Suri “Different Methods and Approaches for the Detection and Removal of Wormhole Attack in MANETS” in International Journal of Engineering and Technical Research, volume 1, No.5, July 2013.

[3] Kamini Singh, Gyan Singh and Arpit Agarwal “A Trust based Approach for Detection and Prevention of Wormhole Attack in MANET’ in International Journal of Computer Applications, Volume 94, No.20, May-2014.

[4] Sweety Goyal and Harish Rohil “Securing MANET against Wormhole Attack using Neighbor Node Analysis” in International Journal of Computer Applications, Volume 81, No 18, November 2013.

[5] Mohit Kumar and Nidhi Shalya “Securing AODV against Wormhole Attack using Token based Approach” in International Journal of Applied Information Systems, Volume 4, No.10, December 2012.

[6] Nidhi Nigam, Vishal Sharma and Mahesh Malviya “A Novel Approach for Wormhole Detection in MANET” in International Journal of Computer Applications, Volume 63, No.7, February 2013.

[7] Mohini Gupta and Amit Kanungo “A Novel Defense IPS Scheme against Wormhole Attack in MANET” in International Journal of Computer Applications, Volume 79, No. 17, October 2013.

[8] Aarf Khan, shweta shrivastava and Vineet Richariya “Normalized Wormhole Local Detection Algorithm (NWLIDA)” in International Journal of Modern Engineering & Management Research, Volume 1, Issue 3, October 2013.

[9] Bipin N.Patel and Tushar S.Patel “A Survey of Detecting Wormhole Attack in Manet” in International Journal of Engineering Research and Applications, Volume 4, Issue 3, March 2014.

[10] Mahesh Kumar Kumawat and Jitendra Singh Yadav “A Survey of Detection and Prevention Techniques for Gray-Hole Attack in MANET” in International Journal of Computer Science and Applications, Volume 5, 2014.

[11] Yih-Chun Hu, Adrian Perrig and David B. Johnson “ Wormhole Attacks in Wireless Networks” in IEEE Journal on Selected Areas in Communications, Volume 24, No. 2, February 2006.

[12] Neha Shrivastava and Anand Motwani “Survey of Malicious Attacks in MANET” in International Journal of Computer Applications, Volume 80, No. 14, October 2013.

[13] Bill Ewanick “ Zero Knowledge Proof” March 31, 2011.

[14] Univ. de Los Andes, Merida, Venezeula and ESSI, Sophia – Antipolis, France. “NS Simulator for Beginners”, Dec 2003.