International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Detection and Prevention of Misbehaving Node using PDA and Enhanced 2ACK Scheme

Anil Rathod[1], Sherly Noel[2]

[1]M.Tech in Computer Networks, CMR Institute of Technology, Bangalore, India

[2]Assistant Professor, MR Institute of Technology, Bangalore, India

Abstract: ***A mobile ad-hoc network is an autonomous collection of the mobile nodes communicating each other with the help of wireless links either a direct or indirect manner. In a MANET (Mobile Ad-Hoc Network) we assume that all the nodes which are transmitting data are fully cooperative in nature. Due to the availability of low cost devices, open medium, wide distribution of nodes, changing topology, no centralized monitoring and its ability to provide instant wireless networking capabilities MANET is vulnerable to malicious attacks and it's a topic worth research. So security of data and identifying the misbehaving node is indeed. To overcome we propose a technique which is combination of two PDA (Prevention and detection of algorithm) and Enhanced 2ACK scheme. The nodes are cooperative in nature to forward the packets to destination in a MANET network. Selfish node will not forward the packet to neighboring nodes so it will reduce the performance of a network and loss of data. In a PDA algorithm we use a trust function which collects the trust function from the neighboring node when it detects dropping of packets. After collecting trust function we will call Enhanced 2ACK scheme which will send 2hop acknowledgement to other sender node. Based on both the techniques cluster head will decide the behavior of a node and will generate the global alarm. For routing we use an AODV (Ad-hoc on demand protocol) protocol.***

Keywords: Mobile ad hoc network (MANET), Misbehaving Node, Prevention and detection algorithm (PDA), Enhanced 2ACK, Ad hoc on demand protocol (AODV)**.**

1. Introduction

AN Ad Hoc Network is defined as a collection of nodes dynamically forming a network without any preexisting infrastructure or centralized administration. Each node participates in routing by forwarding data to other nodes. The determination of which nodes forward data is done dynamically based on the network connectivity. Ad hoc networks can use flooding for forwarding the data. It is the auto-configurable network and Self organizing network [1]. Nodes are mobile and hence have a dynamic network topology. Nodes in ad-hoc networks play both the roles of Routers and terminals. Mobile ad hoc network contains the collection of mobile nodes with each of these nodes having their movement throughout the network. The communication between these mobile nodes is via the wireless links by directly or intermediate nodes and there is no fixed infrastructure because of their mobility.

This type of network is even referred as an "ad hoc" network meaning "for this purpose". Hence, ad hoc network is used for connecting the wireless clients together without the aid of any wireless access point or a connection to any existing wired network [3].

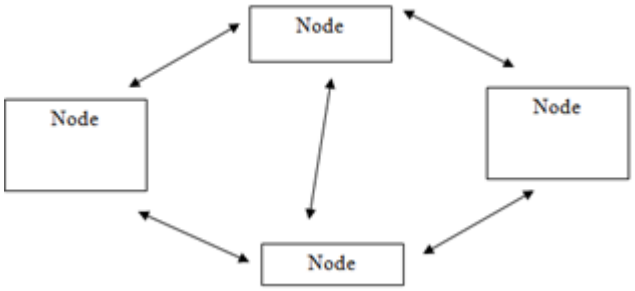

Figure 1: Mobile ad hoc network

In mobile ad hoc wireless networks as shown in Fig. 1, there is no Access Point (AP) and each node communicates directly with each other and does not need any infrastructure [3]. Each node in the MANET needs to implement the medium access mechanism, mechanism for hidden 1 terminal problem, priority mechanisms, providing QOS, forwarding data. The Mobile Ad hoc Network is the complex distributed system with dynamic wireless mobile nodes. The mobile nodes within the radio coverage range can communicate directly with each other. If the mobile nodes are out of the radio range means that the communication and the transmission of packets are made by the cooperation of the intermediate mobile nods throughout the entire network. The network topology of the MANET may change rapidly, dynamically and unpredictably based on the own parameters.

According to IETF RFC 2501, MANET has following characteristics [11][12]:

- As the nodes can move freely, hence there is spontaneous formation and deformation of the mobile network with symmetric or asymmetric links.
- The nodes in MANET are resource constrained in terms of battery power, bandwidth and energy consumption.
- Nodes share the same media (radio, infrared) and communicate wirelessly.
- Each mobile node acts as an independent router and hence supports a distributed peer-to-peer mode. Thus, it results in the formation of multi-hop network also.
- The capacity of the wireless link in MANET is small, bandwidth constrained and variable in nature with susceptibility to interference, external noise and signal attenuation effects.

Typical features of MANET contributing to the vulnerabilities :

- **Wireless link unreliability between the mobile nodes**
  Due to the continuous mobility of the wireless nodes and limited energy supply to them, the links between mobile nodes are not consistent.
- **Changing topology**
  The nodes can freely move into and out of the other node's radio range in the ad hoc network. Therefore, the routing information will be changing at any time.
- **Lack of security feature incorporation**
  As the topology of the mobile ad hoc networks is changing constantly, it is important for each and every pair of the adjacent nodes to incorporate in the routing issue for preventing from the potential attacks.

Despite of these applications, mobile nodes in the MANET have their own merits such as, small storage requirement, utilization of low bandwidth, low error rate in packet transmission, limited battery power usage, easy and quick deployment, no planning required (created at the time it is needed), no need of infrastructure, no need of a central controlling. There are many network actions are performed by the mobile nodes in MANET they are authentication, routing, packet discovery, packet transmission, packet forwarding, network management, discovering topology, delivery of packets [4]. The MANET having the characteristics of the open distributed medium, wide distribution of nodes in the network with the changing (dynamic) topology and there is no requirement of centralized monitoring or administration. For the mobile ad hoc networks, Intrusion Detection System (IDS) aims to provide solutions being self-organized, collaborative and without centralized entity. Due to the Limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, the IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. This paper addresses the security issues in the mobile ad hoc networks and proposes a secure misbehaving node detection & prevention system which detects, prevents and blocks the misbehaving nodes by using the Packet Dropping detection Algorithm (PDA) and 2ACK scheme.

The design of the proposed system includes Cluster head election algorithm to elect the cluster head form the clusters in the MANET and to maintain cluster members, Monitoring Neighbor Nodes to record the nodes activity in the MANET, Trust Collector Function to record the nodes trustworthiness in network and to inform about this to the cluster head node, 2ACK scheme it will send 2hop acknowledgement , Raising Global Alarm, it is generated by the cluster head node and it notifies about the existence of the malicious/misbehaving node in the MANET.

2. Related Work

Many researchers have devoted their work to the development of intrusion detection in the dynamically changing environment such as mobile ad hoc networks. In line with these developments in this section it is detailed about recent developments of the intrusion detection or the misbehaving node detection techniques for the MANETs. A node may become selfish or misbehaving due to honest as well as malicious reasons. Honest reasons involve collisions, channel error, buffer overflow etc. Malicious reasons could be due to attacks (black hole attack or wormhole attack) on the node, congestion etc [15]. Hence, a selfish node tries to save its own energy and bandwidth, minimizes the packet transfer rate and maximizes the packet delivery time.
The selfish behavior of a node is considered when it [10][45]

- Simply drops the packets
- Does not co-operate in route establishment
- Blocks all the types of packet/traffic
- Refuses to forward the packet
- Advertises to the sender as the shortest route to the destination node.

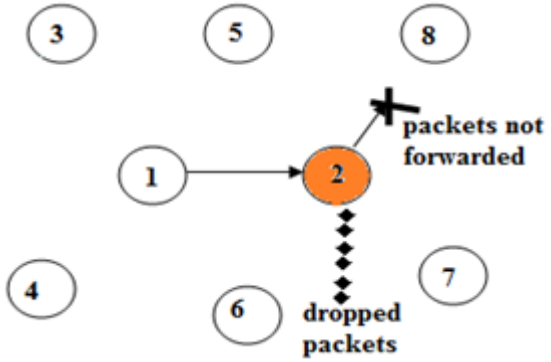

Figure 2: Selfish node behavior

Marti et , (2000) proposed [5] a scheme named Watchdog mainly to improve the overall throughput of the network with the presence of malicious nodes. This scheme has two parts, watchdog and path rater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by listening to its next hop's transmission as shown in Fig. 2. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. When the node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many research studies and implementations have proved that the Watchdog scheme is efficient. In the Fig. 2, Watchdog node (A) listens, next hop's (B) transmission, to find any malicious misbehaviors activity in the network. If a Watchdog node (A) overhears that its next node fails to forward the packet within a certain period of time. Then, Watchdog node reports it as misbehaving. Many MANET IDSs are developed as an improvement to the Watchdog scheme. The Watchdog scheme also fails to detect malicious misbehaviors with the presence receiver collisions, limited transmission power, false misbehavior report and partial dropping.

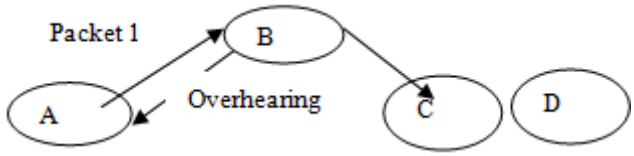

Figure 3: Watchdog Scheme

TWOACK algorithm was proposed [6] by Liu et al., (2007) it is one of the most important approaches because of; many weaknesses of the Watchdog scheme were solved. TWOACK algorithm is aimed to resolve the receiver collision and limited transmission power problems of Watchdog. TWOACK detects misbehaving nodes by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. That is each node required to send back an acknowledgment (ACK) packet to the node that is two hops away from it. The TWOACK scheme is shown in fig 4

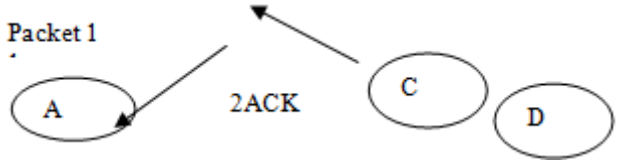

Figure 4 2: ACK

In this fig 4 Node A forwards Packet 1 to node B, node B forwards the same to node C. When node C receives Packet 1, as it is two hops away from node A, node C is required to generate a TWOACK packet. The retrieval of this TWOACK packet at node A shows the successful transmission of a Packet 1, from node A to node C. When TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process continued to every three consecutive nodes along the rest of the route. This scheme successfully solves the receiver collision and limited transmission power problems. However, the ACK process in every packet transmission process adds a significant amount of network overhead and also easily degrades the life span of the entire network.

3. Proposed System

A.AODV (Ad hoc on Demand Vector) Routing Protocol:

The main aim of this routing protocol is to identify the most recent routes it employs with the destination sequence numbers. The main difference between the AODV and Dynamic source routing protocol is the in DSR only source node knows the routing information but in AODV the source node as well as the intermediate node knows the next hop information. It's also reactive on-demand protocol for the routing the information.

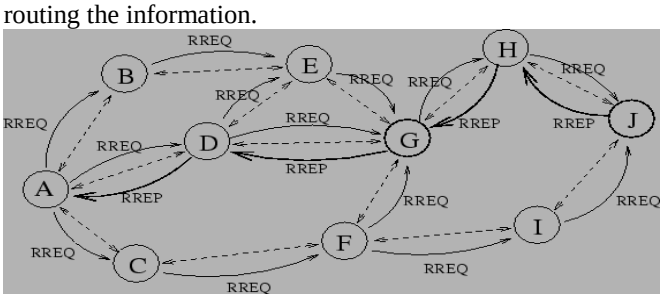

Figure 5: AODV

In the above figure 4.1 source generates the route request packet will be sent to all the near neighboring nodes until it reaches to its destination .It uses the destination sequence number to determine the up-to-date path to the destination. In AODV protocol it uses two request packets

RREQ: This route request packet will be broadcasted to all the neighboring nodes with the sequence no of the destination.
RREP: This route reply packet is Unicast to the source node from the destination node.

B.PDA Algorithm

The proposed system uses Packet dropping Detection Algorithm (PDA) for the discovery of misbehaving node in the MANET. It incorporates an assurance plan against an data packet dropping attack based on the cooperative participation of nodes. This scheme requires each node in the system to monitor the behavior of its neighbors; when it recognizes packet dropping it invokes a distributed approach to deal the attack. After detecting a node that is dropping packets the scheme then uses a trust collector function to gather trust values from the neighbors of the suspicious node. If a majority of the nodes has a low trust value for the suspicious node, they then inform all the nodes about the attacker by raising a global alarm.

Proposed algorithm ensures that nodes in the network are aware of the misbehaving nodes and informs to the cluster head immediately if they are found in the MANET. The important components/ algorithm/technologies of the proposed system for the MANET to detect the misbehaving node are, Packet dropping Detection Algorithm (PDA), Trust collector function, The Connectivity, Energy and Mobility driven weighted Clustering (CEMCA) Algorithm. The Fig 5 shows the architecture of the proposed system for the misbehaving node detection in the MANET.

PDA Algorithm

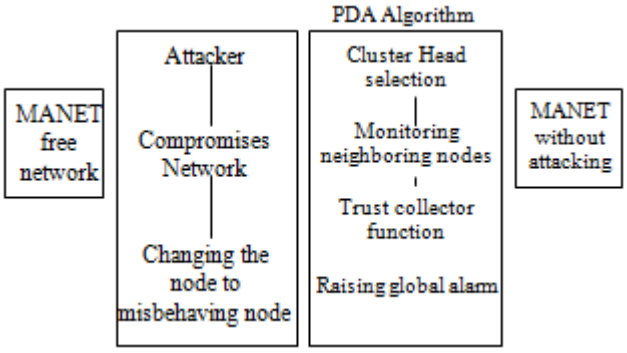

Figure 5: System Architecture

In this design it is first taken, MANET with attack free network and the nodes in the network are properly working without any malicious / misbehaving activity. Then the attacker compromises the network by introducing or changing some nodes in the network into misbehaving nodes and those misbehaving nodes does not forward the packet to the destination. These misbehaving nodes drop the packet totally or partially when they routed via this malicious node. The PDA algorithm is used to detect those misbehaving nodes and alerts the malicious activity throughout the

network by using the algorithms. In the subsequent sections It is detailed about main steps involved in the PDA algorithm for the detection of the malicious node such as, Cluster head election algorithm, Monitoring neighbor nodes, Trust collector function, Global Alarm.

Cluster Head Election Algorithm

The Connectivity, Energy and Mobility driven weighted Clustering Algorithm (CEMCA) is used for the election of the cluster head. The cluster head for MANET elected by considering following parameters of a node: lowest node mobility, highest node degree, and highest energy level, best transmission range. Normalized value of mobility, degree and energy level is calculated and is used to find the weight for each node. This algorithm is completely distributed and all nodes have the equal chance to be a cluster head. In the Fig. 6, it is shown about the flow of cluster head selection. Here, in first step ach node co operatively participates in the cluster election algorithm. Then the nodes collect the mobility value and the energy value each of the other nodes. If the node's energy value and node's mobility value low then elects that node as the cluster head. These steps repeated until new cluster head is to be chosen.

Monitoring Neighbor Nodes

Each node in the MANET passively listens to the communication to and from each of its neighbors. For, detecting packet drops and modifications by the neighboring nodes, each node checks whether the neighbors really forward the packets with contents unchanged, or drop them, or modify the contents before forwarding them. If any of the nodes in the MANET detects some of the nodes are dropping or partially dropping the packets that they received. Then the neighbor nodes informs about it, by using the trust collector function to the cluster head.

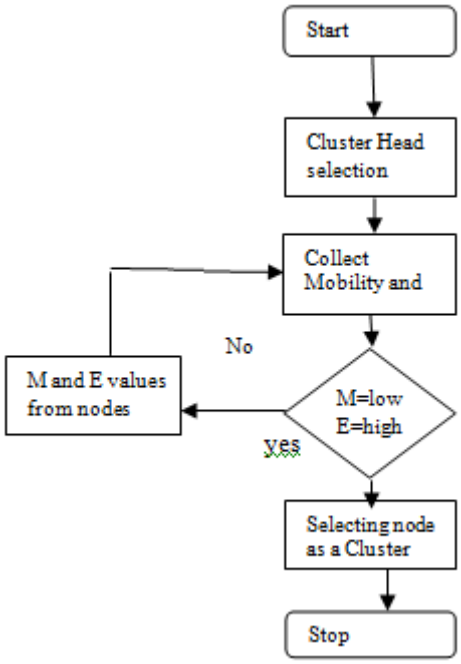

Figure 6: Cluster head selection

Trust Collector Function

The Trust collector function of a node invokes a majority consensus algorithm among the neighbors of a node that has been suspected to be malicious. On being activated by their neighbor node that has suspected some malicious activity by one of its neighbors, the cluster head node is to verify its behavior as observed by all of its neighbors. The cluster head node forces the neighbor nodes, to get the information about trustworthiness of the suspected node. The trustworthiness of the neighbor node means that, the information about suspected malicious node whether it drops or forwards the received packet to its neighbor. The cluster head node receives the challenging responds by all of its neighbors. The neighbors respond by sending the observed value of the degree of maliciousness of the suspected malicious node. The cluster head node calculates the neighbor's trust about the suspected malicious node by using the received values. It is calculated by, if all neighbors of the suspected malicious nodes having the negative trustworthiness, then the suspected node is declared as the malicious node and the malicious node information is flooded throughout the network.

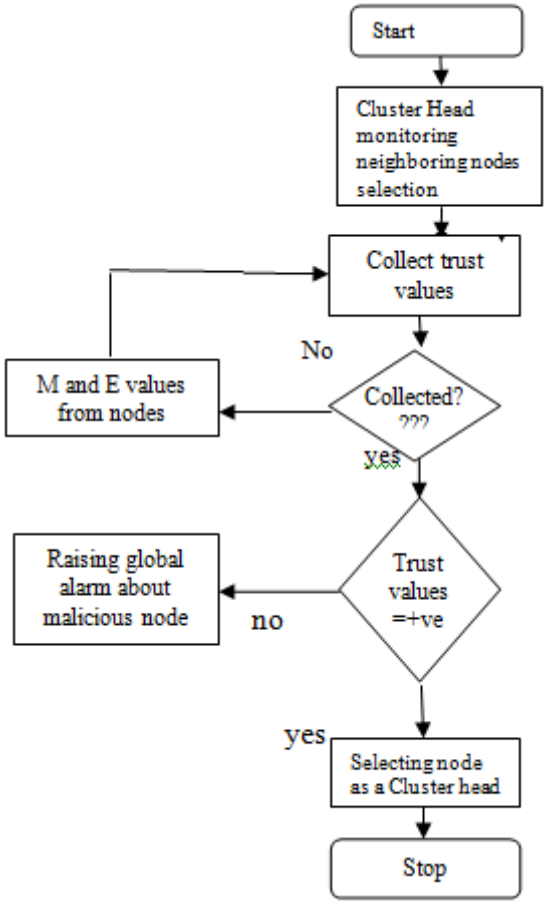

Figure 6: PDA algorithm

Global Alarm

The cluster head node initiates a response action of the detection of malicious node as the global alarm. When a global alarm is raised by the cluster head node, the al message is flooded across the entire network with the information about malicious node. The Fig.6 shows overall flow of the PDA algorithm. In that the cluster head monitors the each node in the network within the coverage area and maintains the cluster member information. If any packet drop

occurs by the node in the MANET, Then the cluster head collects the trust values from all other neighbor nodes about the particular packet dropping node. If all of the neighbor nodes gives the trust values about dropping node, then the cluster head raises the global alarm about that the particular node is malicious node by broadcasting packet to all cluster members. The proposed algorithm includes several advantages such that reliability of the network, reliable packet transmission, provides enhanced intrusion prevention system to MANET, detecting misbehaving node early as possible.

C. Enhanced 2ACK Scheme

In Enhanced 2ACK scheme is used as an approach to inform the sender of the data packet about the successful arrival of the packet by destination. It tries to reduce the overhead by sending genuine and authenticated 2ACK packets only for the certain fraction of data packets received. But it adds routing overhead and end-to-end delay because of the authentication process carried out.

Figure 7: Enhanced 2ack

Considering the three consecutive nodes N1, N2, and N3 as absent of triplet along the routing path .In the route discovery phase of the AODV protocol, the route from the source node 'S' to the destination node 'D' is generated. When the node N1 sends the data packet to other node N2 which it later forwards to the next node N3, it remains unclear to the node N1 whether the data packet has been successfully received at the node N3 or not. When the data packet has been successfully received at this node N3, it sends out an acknowledgement packet- 2ACK packet over the two hops to the node N1 bearing the ID of the corresponding data packet.

The node N1 acts as the 2ACK packet receiver or the observing node and the node N3 as the 2ACK packet sender. To detect the selfish behavior, the sender of the 2ACK packet maintains a table or list of IDs of sent data packets but not acknowledged. After the node N1 has sent the data packet on a particular path, it will add the data ID to the data structure maintained by the observing node i.e. LIST. The counter 'Cpkts' (no. of forwarded data packets) is then incremented simultaneously.

At the node N1 for 'λ' seconds (the timeout for 2ACK reception), each ID will stay on the list. If the acknowledgement packet '2ACK' corresponding to this ID arrives within the time limit, then this ID will be removed from that list. Otherwise, the counter 'Cmis' will be incremented by one. When the node N3 will receive a data packet, it will first determine whether there is a need of sending the 2ACK packet to the observing node 'N1'. For reducing the additional routing overhead, only a certain fraction of the data packets will be acknowledged with this 2ACK scheme. This fraction is referred as the acknowledgment ratio, Rack [16]. For a certain time period i.e. Tobs, node N1 will keep on observing the link behavior N2-> N3. At the end of this observation time, ratio of missing 2ACK packets as Cmis/Cpkts is calculated by the observing node N1 which is then compared with 'Rmis'. Here 'Rmis' is referred as the threshold value for determining the allowable ratio of the total number of missed 2ACK packets to the total number of sent data packets. If this ratio turns out to be greater than Rmis, then the N2-> N3 link is declared as misbehaving link and the node N1 sends out the route error message- 'RERR' packet. As the certain fraction of received data packets are acknowledged, the term 'Rmis' must stand satisfactory for the following equation

Rmis>1- Rack

This scheme overcomes the drawbacks of watch dog mechanism, i.e. the problem of limited transmission power, receiver collisions, ambiguous collisions and limited overhearing range. The major drawback of this scheme is that routing overhead is affected by the authentication of 2ACK packets. Increase in the ratio of 2ACK packets and data transmissions results in increase of routing overhead. Also, 2ACK scheme is less resistant to the collusion attacks and malicious alarms.

4. Simulation Results

We have evaluated the performance of the network by means of simulation using NS-2.34. The simulation includes 50 nodes, with AODV as routing protocol.

Scenario 1:

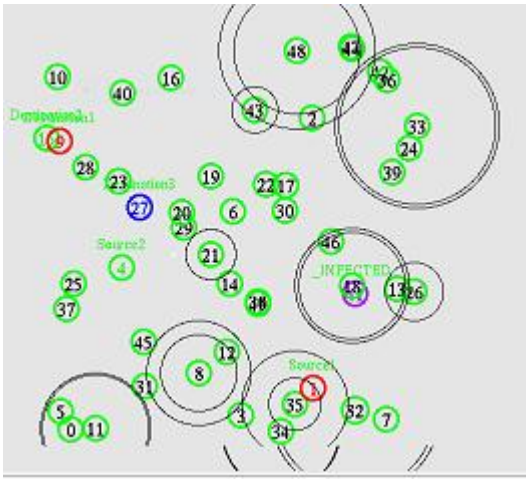

Figure 8: Nodes

In above figure we have 50 nodes each labeled with a unique no from 0-50.In above figure red color nodes are the senders and green color nodes as destination. The circle in the above figure indicates the range of the node.

Scenario 2:

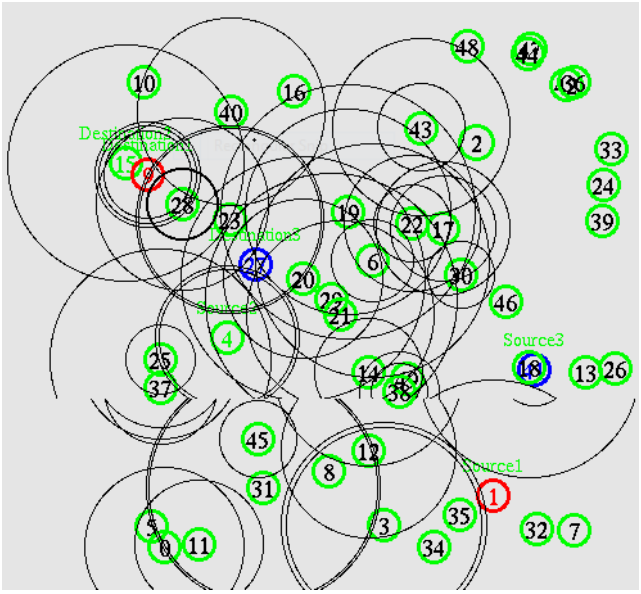

Figure 9: Misbehavior node

Sender transmits the data through the intermediate nodes, by using the PDA and Enhanced 2ACK we can identify the exact misbehaving node, misbehaving node are identified by purple color in above diagram.

Scenario 3:

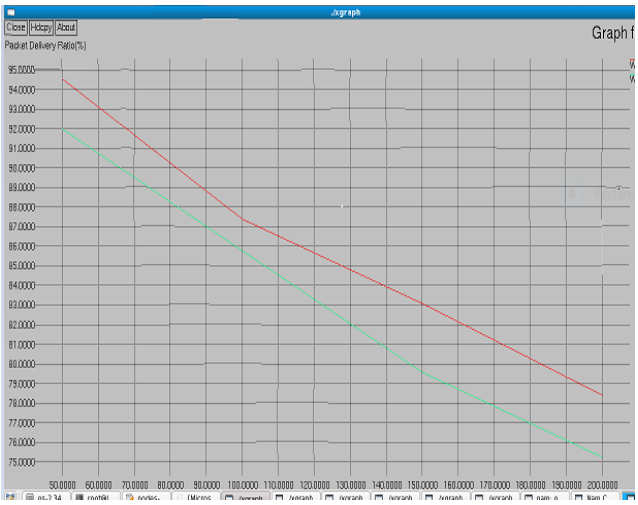

Figure 10: Graph of packet dropping

In above figure graph indicates that PDA and Enhanced 2ACK can decrease the packet dropping as compared to the 2ACK scheme.

5. Conclusion and Future Work

Dropping of packets by a node is always a major threat to the security of MANETs. The work mainly focuses on dropping of packets, misbehaving node and overall effect the network performance. In this paper we use CEMCA algorithm for cluster head selection based on energy of the nodes whenever there is dropping of packets cluster head calls for a trust function from all neighboring nodes. Some nodes may send the false trust value about the neighboring node, If cluster head decides that node as a selfish node then there will be loss of data. So we use 2ack scheme to identify the exact misbehaving node later cluster head decides the selfish behavior of a node. In future work we need some different clustering algorithm for cluster head selection. We need to avoid overhead on the cluster head. Simulation results enhanced 2ACK is better than 2ACK.

6. Acknowledgment

Anil Rathod, thanks to Mrs. Sherly Noel, who is always encouraging and motivating me to do research activities. I am also very thankful my families and friends.

References

[1] M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK - A Secure IDS for MANETs", IEEE Trans. on Indus. Elec, pp.l089-1098, 2013.
[2] H. Deng, w. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communications, October 2002.
[3] J.H. Schiller, "Mobile Communications," second Edition, Pearson Education Ltd, 2003.
[4] Y. Yoo And D. P. Agrawal, "Why Does It Pay To Be Selfish In A MANET", IEEE Wireless Communications, Dec. 2006.
[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, pp. 255-265, 2000
[6] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536-550, May 2007.
[7] T. Sheltami, A. AJ-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Int. 1. Multim. Syst., vol. 15, no. 5, pp. 273-282, Oct. 2009.
[8] J. Sen, M. Chandra, P. Balamurlidhar, S.G. Harihara and H.Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad hoc Networks", Proc. IEEE Conference on Telecommunication and Malaysian International Conference on Communication, 2007.
[9] F.D.Tolba, D. Magoni and P. Lorenz "Connectivity, energy & mobility driven weighted clustering algorithm" in proceedings of IEEE 2007.
[10] Adnan Nadeem and P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," IEEE Communications Surveys, 2013.
[11] S. Basagni, M. Conti, S. Giordano & I. Stojmenovic, "Mobile Adhoc Networking," John Wiley & Sons, 2004.
[12] S. K. Sarkar, T. Basavaraju and C. Puttamadappa, "Adhoc Mobile Wireless Networks: Principles, Protocols and Applications," CRC Press, 2007.
[13] P. Goyal, V. Parmar and R. Rishi, "MANET: vulnerabilities, challenges, attacks, application," International Journal of Computational Engineering & Management, 11, pp. 32-37, 2011.
[14] P. Mohapatra and S. Krishnamurthy, Ad Hoc Networks: technologies and protocols: Springer, 2005.

[15] P. Mohapatra and S. Krishnamurthy, Ad Hoc Networks: technologies and protocols: Springer, 2005. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless communications, vol. 14, no. 5, pp. 85-91, 2007.
[16] H. Liu., J. G. Delgado-Frias and S. Medidi, "Using a cache scheme to detect selfish nodes in mobile ad hoc networks," Communications, Internet, and Information Technology, 2007.

Author Profile

Anil Rathod received B.E. degree in Bsaveshwar engineering college Bagalkot and Perceiving M.TECH. Degree in Computer Engineering from CMR institute of technology.

Mrs. Sherly Noel, she completed her B.E and M.tech from satyabama university Chennai. She is presently is an assistant professor at CMR Institute technology Banglore.