Malicious Node Detection against Attack using Trust Based Approach in MANET

[1]Anand Verma, [2]Prof. Sachin Mahajan

[1]Research Scholar, [2]Assistant Professor
Department of Computer Science and Engineering
Jawaharlal Institute of Technology,
Borawan, Khargone(M.P.), INDIA

Abstract – In ad hoc network security turn out to be all the more difficult issues because of its dynamic nature. The system permits any node to join and furthermore leave the framework without having a physical address or getting assent. Exceptionally designated frameworks are powerless to different sorts of attacks, for instance, refusal of organizations, emulate, and listening stealthily. The dynamic topology of MANETs licenses nodes to connect and vanishes from arrange anytime of time. This general normal for MANET has rendered it vulnerable to barrier attacks. The Malicious Node attack is one of such security peril. In this attack, a pernicious node inconsistently publicizes most limited way to the goal node with an intension to interfere with the correspondence. In this paper, we propose a strategy for distinguishing Malicious Node (s) in particular Malicious Node. We proposed to consider diverse parameters like support length, vitality and bundle drop mean whole recreation session. Consequently, we proposed a trade for steering that approach not just identifying the Malicious Node notwithstanding counteracting system. The investigational comes about demonstrates the adoptable execution of the count and recover the particular execution parameters i.e. throughput, end to end delay, packet delivery ratio, and vitality utilization

Keywords: MANET, AODV, NS2, Malicious Node, Routing Protocol, RREQ, RREP

I. INTRODUCTION

With the quick advancement and organization of cell phones, Mobile Ad Hoc Networks (MANETs) turn into a critical segment of present day appropriated frameworks. As a result of the framework less property, MANETs can be effectively conveyed. They are exceptionally alluring to applications, for example, military operations and first reaction to debacles. The capacity to set up correspondence without a framework and the ability to convey past the hub's remote transmission scope of board Mobile Ad hoc Networks (MANET) as the sending ground for different fields, for example, remote sensor systems, universal systems and shared systems. The multiplication of specialized gadgets and the advancement of innovation affirm that it is the apparatus, which can transform the current processing space into savvy space [1] [2].

A Mobile Ad hoc Network (MANET) is a course of action of remote versatile centers that continuously self-deal with in self-self-assured and temporary framework topologies. People and vehicles would in this manner have the capacity to be web worked in regions without an earlier correspondence system or when the usage of such establishment requires remote development [9]. In the adaptable offhand system, focus focuses can obviously converse with the distinctive focus focuses inside their radio degrees; while focus focuses that not in the incite correspondence go utilize generally engaging node(s) to chat with each other.

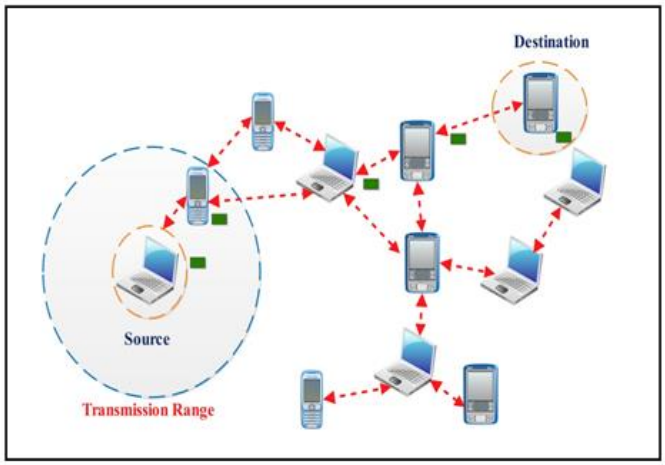

Figure 1: Mobile Ad-hoc Network

Figure 1 demonstrate the ad-hoc network structure comprise mobile and computer system device. In this each devices have a specific range for communication establishment. If most of the device, in this range all are communication to each other one device for one time. Mobile ad hoc network is a new technology [4].

II. MALICIOUS NODE ATTACK

From the investigation of fundamental on-request directing convention's operation, it is inalienably sensible that the arrangement acknowledge the individuals to forward others bundles, which is a unimaginable desire in a free framework like MANET[9,10,11]. The aftereffect of not sending others packages or dropping others bundles keeps any kind of correspondence to be developed in the framework. Consequently given a choice between the need to secure organizations or to ensure key working of the framework, actually the choice falls for the last said. Thusly, the need to address the package dropping event takes higher requirement for the versatile offhand frameworks to create and work successfully [5,12,13].

A bundle might be dropped under different reasons, which thusly can be gathered into the accompanying classifications [6,18]:

- Unsteadiness of the medium,
  - A packet may be dropped due to contention in the medium
  - A packet may be dropped due to congestion and corruption in the medium
  - A packet may be dropped due to broken link
- Genuineness of the node
  - A packet may be dropped due to overflow of the transmission queue
  - A packet may be dropped due to lack of energy resources
- Selfishness of the node
  - A bundle might be dropped because of the self-centeredness of a hub to spare its assets
- Maliciousness of the node
  - A bundle might be dropped because of the harmful demonstration of a malignant hub

Figure 2 shows the overview of the Malicious Nodeattack scenario. In a dark gap assault, a vindictive hub sends fake steering data, guaranteeing that it has an ideal course and makes other great hubs course information parcels through the malignant one.[10,11,13]

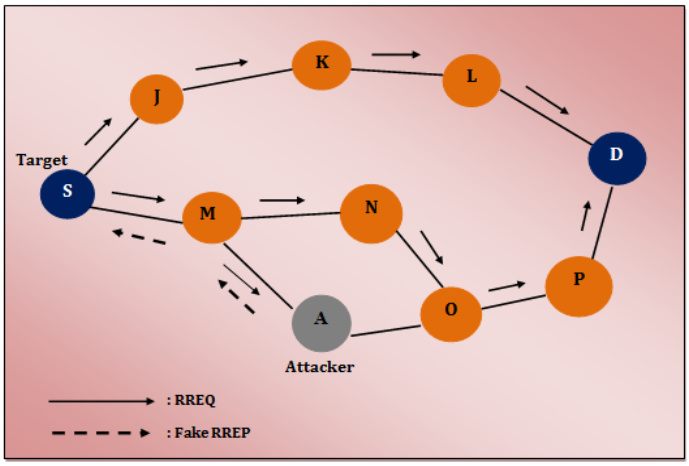

Figure 2: Malicious Node Attack

For instance, in AODV, the aggressor can send a fake RREP (counting a fake goal grouping number that is manufactured to be equivalent or higher than the one contained in the RREQ) to the source hub, asserting that it has an adequately crisp course to the goal hub. This makes the source hub select the course that goes through the aggressor. Along these lines, all activity will be directed through the aggressor, and accordingly [7, 14, 15].

III. PROPOSED SYSTEM

1. Methodology

A system of broad standards or principles by which particular techniques or strategies might be inferred to translate or take care of various issues inside the extent of specific orders. Unlike an algorithm, a methodology is not a formula but a set of practices.

1. **Initiate Route Discovery**
2. **Assigning Parameter**
3. **Formulate Algorithm**

1. Initiate Route Discovery:

For securing system, the proposed algorithm is creating utilizing diverse constraints. With the goal that we fundamentally we have to expect a few requirements to advance further. For this we have to set up a sit out of gear organize for showing the idea, right off the bat we make a typical system where with various number of system e.g. 20, 40, 60, 80, 100, 125 and 150.

Initialize the Network, with N nodes where$N = 1, 2, 3, \ldots . n$,, in ideal condition

S initiates a RREQ message with the subsequent components:

– The IP locations of S and D

– The present succession number of S and the last known arrangement number of D

– A communicate ID from S. This communicate ID is augmented each time S sends a RREQ message.

The couple of the source S forms a unique identifier for the RREQ.

For route discovery, we process a route request for RREQ to all other hub aside from the hub which is producing request. In this way, source hub sit tight for the course answer i.e. RREP which is originating from that hub to its match communicates ID and IP address.

Furthermore, to process proposed technique, we utilize some systems administration diverse components to process the calculation from this we get the productive yield that diagrams the secured organize. In next point we accept some checking requirements which are utilized to assemble calculation.[16]

2. Assigning Parameter

In this segment we portray relegated parameter need to process the proposed approach by we build the calculation

- ✓ **Node Energy:** Node energy of a node indicates how the network is efficient and long life of the node in entire working network session. Energy less than a predefined average can affect the normal functioning of network. Therefore in order to serve the network longer it is required the cluster head node has the sufficient energy level. According to the definition of energy consumption the difference of two time based energy level is used for computing the energy consumption rate which is used for cluster head selection. Thus suppose at time t_1 the node have the energy $E_i$and after a time difference Δt the new energy level becomesE_c at timet_2.
- ✓ **Buffer Length:** The buffer or queue length of a node demonstrates the amount of workload which is processed by any node. In this context the amount of buffer length is free to use indicate the node if free and can able to serve better the legitimate node. That is here for the length of buffer the letter B is used.
- ✓ **Packet Drop:** Packet drop is the failure of one or more transmitted packets to arrive at their destination. The total number of packets dropped during the simulation is termed as the packet drop ratio. It can be also termed as the difference between the total number of packets send and the total number of packets received. In this term we can calculate dropped packet when network performance degraded.

To solve the issue of the Malicious Nodebased attack in network. We enroll fundamental 3 modules of our technique that develop whole framework that demonstrating proficiency and adequacy of this work.

3. Formulate Algorithm

The proposed work is indented to secure the system, in this manner the AODV directing convention is altered to distinguish the malignant hub among the accessible courses amongst source and goal[17]. Table 1 and 2 demonstrate the entire process of algorithmic calculation in a short summary:

Table 1: Average calculation of different factors

Input: Number of Nodes; ***Output:*** Threshold Values for finding Malicious Nodes;
Process: **1:** Initialize the Network, with N nodes where $N = 1, 2, 3, \ldots .$,, in ideal condition. **2:** Initialize Route Discovery by Source Node N_s **3:**N_s sends RREQ Packets to Destination N_d

4: Wait Until all Route Replies not received

5: For each routing in routing table:

6: Consider for each node buffer length is $B_i where i = 1, 2, \ldots . n$

7: Find average buffer for all node

$$Avg_{buffer} = \frac{1}{N}\sum_{i=1}^{n} B_i$$

8: Count Number of Packet drop during simulation

$$PacketDrop = TotalSend - TotalReceived$$

9: Compute Average Packet Drops of all nodes

$$Avg_{Pd} = \frac{1}{N}\sum_{i=0}^{n} PacketDrop_i$$

10: Find Consume Energy for each node

$$ConsumedEnergy(E_c) = InitialEnergy - RemainEnergy$$

Where the E_c is the amount of energy dropped by a node i

10: Compute Average Threshold value for Energy

$$Avg_E = \frac{1}{N}\sum_{i=1}^{n} E_{C_i}$$

11: Broadcast the Avg_{buffer}, Avg_{Pd}, Avg_E to the entire network

Description: The proposed algorithm is demonstrated the Malicious Nodeattack detection and avoidance by their property. In this section we provide the detail description about formulated algorithm. Therefore, table 1 depicts the basic average calculation of factor assigning to finding Thresholding value of the node energy, buffer length and packet dropped during simulation process. Firstly, we have to discovered path between source nodes to destination node. Therefore, AODV protocol establish route by finding destination node. So that source node broadcast the RREQ packets to all nods. The RREQ packet contains different field like Source IP address, destination IP address, Broadcast ID, TTL values etc. On the basis of this field values destination node match all field values and unicast the RREP to source node. Whenever source node receive RREP reply it establish route between this two nodes. After the route is discovered source node able to communicate with destination via sending and receiving packets.

Now, we calculate different factor values, on which basis we initiate the process of finding malicious nodes. Networks have the property where every node join or leave the network frequently whenever the network topology is changed. We calculated the node energy, buffer length and dropped packet by putting the values in developed formula. After calculation of the factor values after we find out the average value of all nodes by summation of all node dividing by number of nodes. These average values are broadcast to entire network.

Table 2: Algorithm for Malicious Node Detection

Input: Number of Nodes, Packets;

Output: Suspected node List, Attacker Node;

Process:

1: Normalize values of each node in Network between 0 to 1

2:for each node in suspected list

3:*if* $(PacketDrop_i > Avg_{Pd} \&\& Avg_{buffer} < B_i \&\& Avg_E < E_c)$

List the Suspected Node

4:*endif*

5: Get Weight of all Suspected Node using normalize value

6: Assign weight to each node
W= 0.5*PacketDrop+0.25*Energy+0.25*Buffer

7: Compute Average weight of all Node

$$Avg_{weigt} = \frac{1}{N}\sum_{i=1}^{n} W_i$$

8: Compare weight of each node to average node weight

9:*if* $(\text{weightNode}_{[i]} < Avg_{weight})$

Malicious Node

else

Normal Node

10:*endif*

Table 2 show that the decision of factor on which we apply generated average values. For the deep security of the network, we check factors value of individual nodes to average values and make decision. Firstly we normalize the node values between 0 and 1 and if we get the factor value should be normalize in this range. To check the suspected list of the node we compare average value for buffer length, energy and dropped packet of the entire node to all individual nodes. If the individual node value is higher than the particular node value we list that entire node in suspected list. After get the list of suspected nodes we assign a weight value to each suspected nodes. Find out weight we use normalize values of all nodes. Hence, for making weight computation, we take 0.5, 0.25 and 0.25 for average packet drop, average energy and average buffer length respectively. After weight computation, we compute the average value of normalize weight. Finally for suspected list, compare the average value of the weight to individual node weight. If the average weight is high for a particular node list the malicious node. Thereafter avoid this node on communication route and start transmission of data through the legitimate nodes.

IV. IMPLEMENTATION

The simulation is being implemented in the Network simulator [8]. Protocol used here is AODV.

Table 3: Simulation Scenarios

Parameters	*Values*
Dimension	1000 X 1000
Antenna Model	Omni Antenna
Channel Type	Wireless Channel
Radio-Propagation	Two Ray Ground
Traffic Model	CBR
Number of Nodes	20, 40, 60, 80, 100,125,150
Routing Protocol	AOMDV

This section provides the understanding about the simulation scenarios under which the experiments are performed. To demonstrate the security technique their two key simulation scenarios are proposed in this section. Both the simulation scenarios are conducted with different number of nodes that are 20, 40, 60, 80, 100, 125 and 150 nodes for both attacks.

In order to perform the experiments here we show simulation scenario of 20 node script of proposed and normal approach with their description in given figure 3 and 4.

1. Simulation when Malicious Nodeis deployed: In this simulation, the network is configured when the attacker node is deployed with modification of AODV routing protocol. To comprise the network representation the vindictive hub is sent in organize and the system introduction is enlivened on the premise of the system follow document. The normal network nodes are illustrated using the green color and the malicious attacker is established shown ingiven in figure 3. In this arrangement an aggressor consistently drop the parcels as opposed to sending them to the following jump; subsequently significant measure of bundles is dropped amid assault conveyed. In this circumstance Communication is occurred between source hub 9 and goal hub 18.

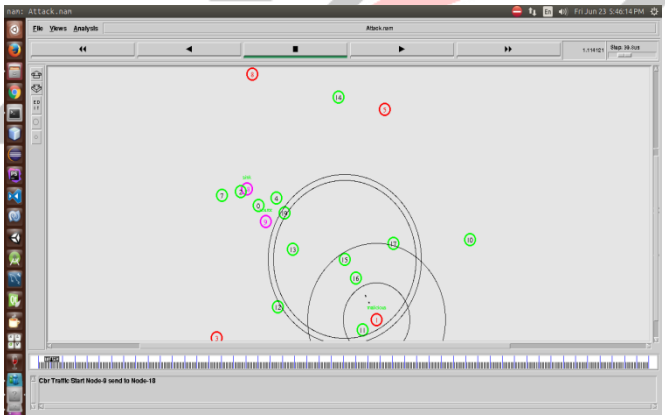

Figure 3: Simulation of Malicious NodeAttack under AODV Routing

2. Proposed Secure Routing Technique' simulation*:* In this scenario proposed routing method which is developed using AODV routing modifications are implemented using MANET environment. in this situation we can't remove attacker node because this node is also a part of our network configuration. Therefore our aims to ignore/avoid the entire attacker node which is drop packets. The conveyed aggressor is standardized utilizing the procedure and their execution is assessed on the premise of the system follow records. The figure 4 exhibits the reproduction screen of the proposed secure steering system for Black-gap Attack aversion.

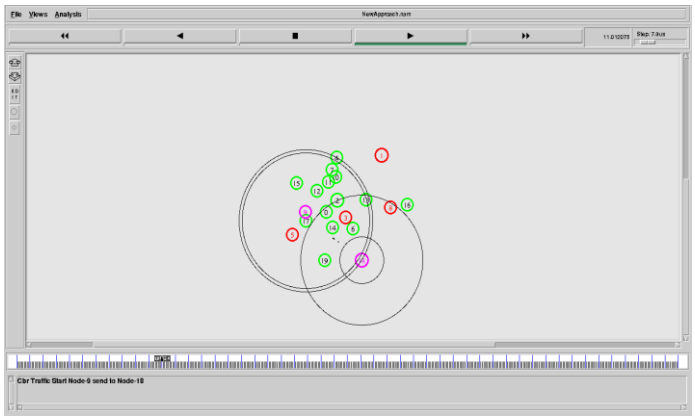

Figure 4: Simulation of Proposed Method under Modified AODV

V. RESULT ANALYSIS

1. End to End delay

End to end delay is the time taken by a parcel to go from source to goal. Deferral relies upon number of bounces and clog on the system. End-to-end defer of information parcels incorporates all conceivable deferrals caused by buffering amid course disclosure, lining at interface line, retransmission delays at MAC layer, engendering and exchange time:

$$\text{E2E Delay} = \text{Receiving Time } (R_t) - \text{ Sending Time}(S_t)$$

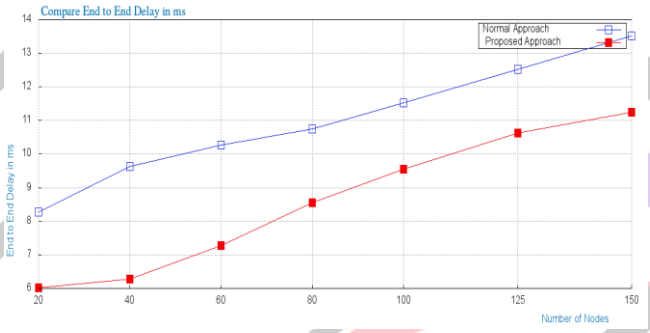

Figure 5: End to End Delays

Figure 5 demonstrates the relative End to End Delay in assault condition and the proposed secure directing procedure. In this figure the X hub exhibit the quantity of hubs in organize and the Y pivot demonstrates the execution of system regarding milliseconds. As indicated by the created comes about the proposed procedure is limited postpone time amid parcel transmission when contrasted with dark opening assault which increment defer time for bundle transmission. Frame this diagram we can close as though quantities of hubs are increments in a separate way at whatever point postpone time increment at the same time for the examination.

2. Packet Delivery Ratio

Packet delivery ratio is portrayed as the extent of data bundles got by the objectives to those created by the sources. Experimentally, it can be described as:

$$\text{Packet Delivery Ratio (PDR)} = \frac{\text{Total Received Packets}}{\text{Total Sent packets}} \text{X100}$$

Charts demonstrate the portion of information parcels that are effectively conveyed amid PDR versus the quantity of hubs.

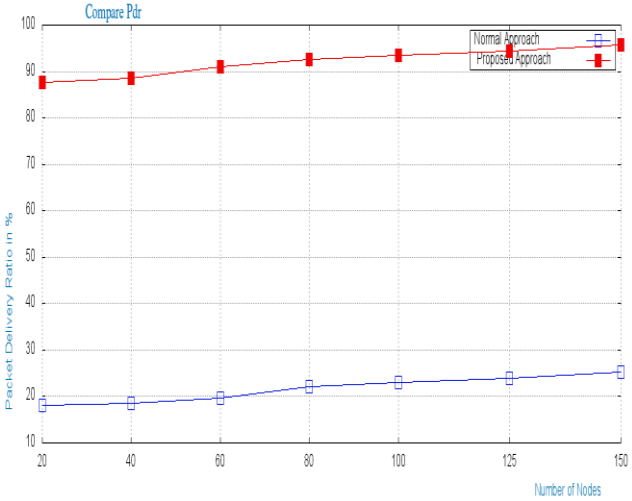

Figure 6: Packet Delivery Ratios

The similar bundle conveyance proportion of the frameworks is given using figure 6, in this figure the X center point exhibits the quantity of hubs for recreation in the system and the Y pivot demonstrates the measure of parcels effectively conveyed to the goal as far as the rate. Also, blue line demonstrates that assaulting execution and red line demonstrate that proposed approach execution. Proposed approach really conveyed high number of bundle by utilizing our proposed idea comparable that aggressor hub diminish the PDR execution that implies a large portion of the parcel devoured persistently.

3. *Throughput*

It is characterized as the aggregate number of bundles conveyed over the aggregate reenactment situation. This information might be conveyed over a physical or consistent connection, or go through persuaded organize hubs. The throughput is typically measured in bits every second (piece/s or bps), and at times in information bundles every second or information parcels per schedule opening.

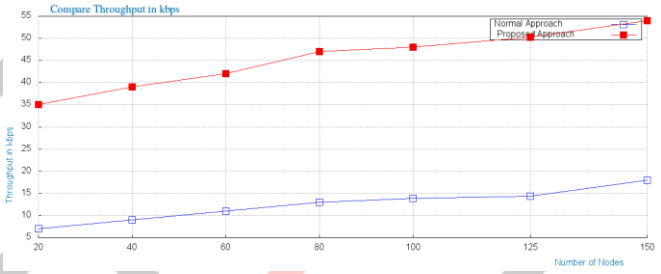

Figure 7: Compare Throughput

The relative throughput of the system is exhibited utilizing figure 7, in this chart divergent number of hub deploying in X-axis in network and the Y axis shows the throughput performance in KBPS. The red line in this graph demonstrates the execution of the proposed system and the blue line demonstrates the execution of the altered AODV based Malicious Nodeattack condition. According to achieved performance the proposed technique improve the throughput of the network during the attack conditions also therefore the technique is effectively avoid the attack effect as if there are number of attacker nodes are increased

4. *Routing Overhead*

Routing overhead is described as the amount of additional bundles infused in arrange for correspondence. The key purpose for to compute this parameter because the routing overhead reduces the parcel conveyance proportion and transmission rate of the information. The given figure 8 demonstrates the execution of system as far as steering overhead. The directing overhead builds the measure of transmission capacity utilization which diminishes arrange execution.

According to the above performance the network under the attack condition indicating blue line increases the routing overhead continuously while number of node increase

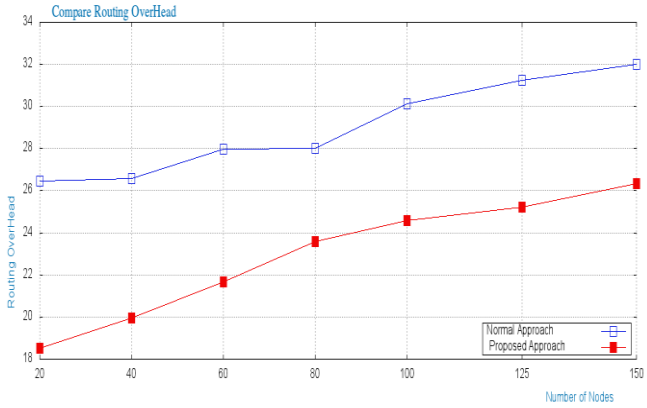

Figure 8: Compare Routing Overhead

Then again when the system is designed through the proposed directing idea the steering overhead progresses toward becoming constant after reach a specific pick point. Along these lines the proposed strategy can recuperate the system from the Black gap assault. Directing overhead is awesome effect on the system while malevolent hub is in greater part or number of hub is not performing legitimate working.

5. *Remain Energy*

The measure of vitality devoured amid the system occasions is named as the vitality utilization or the vitality drop of the system. In systems administration for every individual occasion a lot of vitality is devoured. The given figure 9 demonstrates the vitality

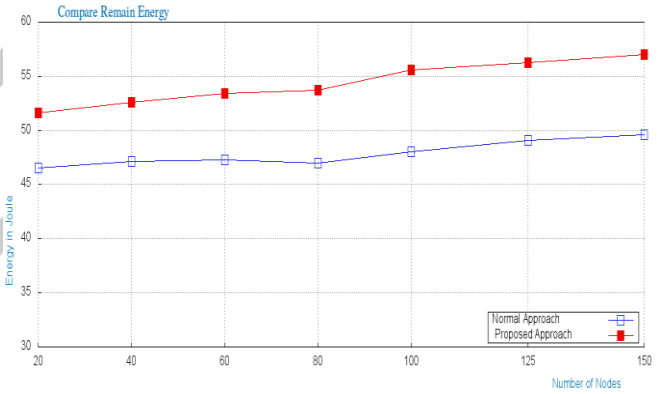

Figure 9: Energy preservation for Malicious NodeAttack

Figure 9 displays remain energy of network for both simulation scenarios. The blue line of the graph demonstrates the measure of vitality stays amid correspondence occasions for attacking condition under AODV routing protocol. Additionally the redline demonstrates the measure of vitality stays amid the proposed calculation based system. In the Attack condition the system vitality is much of the time expended when contrasted with the proposed steering convention on the grounds that the Black-gap assaults focusing on the system by dropping the honest to goodness bundles of the system. In this manner the proposed strategy is powerful and ready to recoup the system from the assault circumstances.

CONCLUSION

Our Experimental results are compared with the packet dropper attack that is implemented with AODV and TAODV. The proposed work is used to mitigate the malicious nodes by classifying the nodes in malicious or non-malicious. Proposed work is a trust based approach in which the train data is used. Proposed work used special function for the classification as per the behavior of the node. We tested out the proposed solution using the NS-2.34 simulator and compared the performance in terms of Packet Delivery Ratio(PDR), End to End Delay(E2ED), Normalized Routing Overhead and Average Throughput. The energy of each node is a big concern in the wireless network. In future, we can apply different proposed model for more accuracy and decrease the mathematical computation. We also have to concentrate on the different types of attacks like worm, whole, selfish, etc.

REFERENCES

[1] B.G.KIN, “The Quality of Service in the Internet”, IEEE, 0- 7803-7093-7/0.
[2] Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj, C. SivaRam Murthy, “Quality of Service Provisioning In Ad Hoc Wireless Networks: A Survey of Issues And Solutions. Ad Hoc Networks”, Ad Hoc NetworksVol.4, pp. 83–124

[3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999
[4] ZHOU, L., and HAAS, Z. J. Securing Ad Hoc Networks. IEEE Network 13, 6 (1999), 24–30.
[5] O. F. Gonzalez, G. Ansa, M. Howarth, and G. Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks", Journal of Internet Engineering, Vol. 2, No. 1, June 2008.
[6] V. L. L. Thing and H. C. J. Lee, "IP Traceback for Wireless Ad-hoc Networks", Available from: http://www.diadem-firewall.org/publications, Accessed on: 28th November 2016.
[7] Kannhavong, Bounpadith and Hidehisa Nakayama "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless communications 14.5 (2007).
[8] The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/
[9] Sushamasingh, Atishmishra , Upendrasingh," Detecting and [23] Avoiding of Collaborative Black hole attack on MANET using Trusted AODV Routing Algorithm " , 1st IEEE Symposium on Colossal Data Analysis and Networking'16, 18-19 March 2016,IEEE, page(s) 1-4
[10] Neeraj Arya ; Upendra Singh ; Sushma Singh," [23] Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm", Computer, [23] Communication and Control (IC4), 2015 International Conference on , 10-12 Sept. 2015, IEEE page(s) 1 – 5
[11] Upendra Singh; Makrand Samvatsar; Ashish Sharma; Ashish Kumar Jain, Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol, 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Pages: 1 - 6, DOI: 10.1109/CDAN.2016.7570908
[12] Ravi Parihar, Ashish Jain, Upendra singh "Support Vector Machine through Detecting Packet Dropping Misbehaving Nodes in MANET " International Conference on Electronics, Communication and [39] Aerospace Technology (ICECA 2017) 481-486 IEEE 21-22 April, 2017 Coimbatore

[13] Mukesh Muwel ,Prakash Mishra ,Makrand Samvatsar, Roopesh Sharma , Upendra Singh , "Efficient ECGDH Algorithm Through Protected Multicast Routing Protocol In Manets" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-7.
[14] Lokesh Baghel ,Prakash Mishra ,Makrand Samvatsar , Upendra Singh," Detection Of Black Hole Attack In Mobile Ad Hoc Network Using Adaptive Approach ", Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.
[15] Amar Singh Chouhan ,Vikrant Sharma ,Upendra Singh, "A Modified AODV Protocol To Detect And Prevent The Wormhole Using Hybrid Technique ", Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.
[16] Roshani Verma ,Roopesh Sharma ,Upendra Singh, "New Approach Through Detection And Prevention Of Wormhole Attack In MANET", Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.
[17] Vibhavarsha Prakaulya ,Neelu Pareek ,Upendra Singh, "Network Performance In IEEE 802.11 And IEEE 802.11p Cluster Based On VANET" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.
[18] Vidya Kumari Saurabh ,Roopesh Sharma ,Ravikant Itare , Upendra Singh , "Cluster-Based Technique For Detection And Prevention Of Black-Hole Attack In Manets" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.
[19] Divyanshu Wagh ,Neelu Pareek ,Upendra Singh, "Elimination Of Internal Attacks For PUMA In MANET" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.