Mitigating Various Attacks in Mobile Ad-hoc Networks Using Trust Based Approach

Namratha Shetty[1], Deeksha Salian[2], Jahnavi S.[3], Jyothi N.[4]

Srinivas School of Engineering, Mukka, Mangaluru, Karnataka

***Abstract*: - A Mobile ad hoc network (MANET) is self-organizing, decentralized and infrastructure-less wireless network. The successful transmission of the data packet depends on the complete cooperation of each node in the network. These types of network don't have permanent base station, so each node in the network acts as a router. Due to openness, decentralized, self-organizing nature of MANET, it is vulnerable to various attacks. So security is the main concern in MANET.**

In this project, we have considered 2 attacks; Vampire attack and DDoS attacks. Vampire attack drains the energy of the nodes. DDoS attack exhausts the resources available to a network, such that the node cannot provide any services. Here, we discuss methods 2 methods as a solution to our problem; one is to prevent the attack from happening and other to detect and recover from the attacks.

***Keyword*: MANET, Vampire Attack, DDoS Attack**

I. INTRODUCTION

In mobile ad hoc network (MANET), the transmission of any data packets are totally dependent on the cooperation of each node in the network, since packets are transmitted from hop-to-hop. Also each node has their own transmission range, so if any source node wants to send the data packets to the final destination node, source node contacts to its neighbour; that neighbour node again contact to another neighbour and so on, so as to reach the final destination node. As we know the wired networks needs infrastructure and have central administration. But in remote locations such as mountains, valleys and some public locations wired networks are hard to setup. Since MANETs are infrastructure-less, open and no central administration required, it became popular. Today MANETs are widely used in every area where wired networks cannot reach. But due to the openness, infrastructure less and dynamic nature of MANET, it is highly sensible to various attacks. In MANET, routing is dependent on various factors such as topology, selection of route, route requests and responses, etc. In MANET, if any attack is occurred, it will affect the performance of the entire network and some secured information may get stolen.

1.1 Problem Definition

Protecting data transformation in mobile ad hoc networks is an important aspect to be seen. Parties within the network want their communication to be secure. At present MANET do not have any strict security policy. This could possibly lead active attackers to easily exploit or possibly disable mobile ad hoc network. Mobile ad-hoc networks are highly dynamic i.e. topology changes and link breakage happen quite frequently. Hence, needs a security solution which is dynamic too. Any malicious or misbehaving nodes can create hostile attacks.

These types of attack can seriously damage basic aspects of security, such as Confidentiality, Integrity, Availability, Non-Repudiation and Authentication, Authorization and Anonymity. Confidentiality ensures that Secret information or data is never disclosed to unauthorized devices. Integrity tells that a received message is not corrupted. Availability permits the survivability of network services despite Denial-of-Service attacks. Non-repudiation ensures that the sender of a message cannot deny having sent the message. Authentication enables a node to ensure the identity of the Peer node it is communicating with. Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Anonymity ensures that the information used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself.

1.2 Solution

To resolve this problem, hence proposed a more flexible trust based approach where at first it creates a cluster of nodes and then choose the node with the highest energy which is considered as trusted node. The communication is carried out through these trusted nodes. To find out the malicious nodes in the network, sent and received packets as well as the route response is calculated. This calculated value is compared with the threshold value and then malicious node is detected.

1.3 Objective of the Work

The primary objective of this project is to reduce the malicious behavior of mobiles nodes in MANET which is due to its openness, decentralized and self-organizing nature. This malicious behavior is due to various attacks which occur inside the network by intruders.

In this project, we consider 2 aspects; first we prevent attacks to occur in the network thereby allowing smooth transmission

of the data packets between trusted nodes; second is to detect and recover from an attack which occurred in the network.

1.4 Scope of the Work

It helps in creating a secured environment for the data to be outsourced with increased security and convenience.

We detect various untrusted attacks in the network thereby avoiding loss of data packets and providing data security.

II. LITERATURE SURVEY

1. Sandeep A. Throat and P. J. Kulkarni compared cryptographic and trust based approaches in MANET routing for implementing security. In this paper, author discussed the various design issues embedded in trust based routing protocol for MANET in detail. For future research in trust based routing protocol for MANET, author has also presented a survey on trust based routing protocol and provides the necessary direction.
2. Ramya S. Pure proposed a model which is designed over the Ad-hoc On-demand Distance Vector Routing Protocol (ADOV). The proposed routing algorithm adds a field to store the trust value or nodes trust on its neighbor, so that the computational overhead can be reduced and trustworthiness of routing procedure can be generated. Based on the trust value of node, the routing information will be forwarded to the next node having highest trust value. Authors also worked on some attacks such as Black hole attack, Gray hole attack and Worm hole attack. The proposed method helps to improve the throughput of the network.
3. Naveen Kumar Gupta and Kavita Pandey proposed an algorithm which is a Trust based AODV Routing Protocol for mobile ad-hoc network, and worked on the concept of honest value, which is calculated on the concept of hop and trust to protect the network from affected nodes (malicious nodes). In proposed HAODV routing protocol, before forwarding the data through various routes, the routing paths have been evaluated according to the trust metrics by the nodes. This method is based on honest mechanism to secure the AODV routing protocol. The performance of the HAODV has been analyzed using three parameters namely the number of drop packets, throughput and Packet Delivery Ratio. The HAODV performs well in terms of throughput and number of dropped packets. The future work of this method is to implement the proposed scheme with more number of parameters while evaluating the path.
4. Naveen Kumar Gupta and Amit Garg proposed a Trust based Management framework for securing AODV Routing Protocol. This worked on the concept of Trust factor and selection of most efficient route and using the Trust Value a routing path is evaluated, also during the route exchange process, the route gets updated. The performance of the proposed system is calculated based on the Packet Delivery Ratio (PDR), number of drop packets and throughput. The identity information (Internal Protocol address and Trust Factor Value) has been used to prevent the attack by the malicious node. This identity information has been assigned to each node in the initialized phase or when the node has been configured. In future works, to optimize above mentioned scheme in terms of number of nodes and building the fast mechanism to detect and prevent the attacker nodes even when large number of nodes.
5. Sumathy Subramaniam proposed a framework for Opportunistic Routing which help to improve the lifetime of network and a Trust model that helps to overcome the vulnerability due to attacks by malicious /selfish nodes, to provide reliable packet transmission. In Opportunistic Routing, one node is selected among the set of candidate nodes as a potential next-hop forwarder using metrics like number of transmission in the link, link error probability, cost, etc. for the packet transmission. This metrics helps in improving the network lifetime. Also, to prevent attack by malicious nodes, the Trust model is used which is based on direct and indirect Trust degree from similar trusted neighbors. On logical level, a proposed framework for Opportunistic Routing has the Two Modules: Routing Module and Trust Module. Routing module is mainly responsible for the selection and prioritization of candidate using the proposed metric, help to improve the residual battery power required for the packet transmission. Trust module is responsible for detection and prevention of malicious and selfish nodes. This Trust module is based on the direct and Indirect Trust degree. As an enhancement to the proposed work, further focus is to determine the delay incurred in transmission of packet from the source to the destination so as to better quality of service in MANET.
6. Issac Woungang proposed an Enhanced Trust Based Multi-path Dynamic Source Routing (ETBMDSR) protocol to securely transmit messages in MANETs. Authors proposed a method to improve the TB-MDSR scheme at least route selection time standpoint. The route selection time is the time taken by algorithm to find the suitable secured routing path to transmit the message from source to destination. In TB-MDSR scheme, a message between source to destination is first broken into four message parts. At the source node, the messages get encrypted using soft-encryption and similar XOR operation as in Step 1. The encrypted message parts are transmitted from source to destination through many trusted paths constructed using DSR and selected according to the Greedy approach on a path length basis (Step 2). At the destination node, the received encrypted messages are decrypted and the original messages is recovered (Step 3). The proposed ETB-MDSR scheme is implemented by following same steps as for the TD-MDSR scheme. However, in Step 2, a new Trust

management model is implemented. In ETB-MDSR scheme, History of Interaction (HI) modules stores the records on the interactions between nodes in suitable data structure. During trust computation, History Maintenance module is used to maintain and update the History of Interaction (HI) module, then calculate the Trust value which is based on the direct and indirect Trust values (using Direct Computation and Indirect Computation).

7. Ahmed M. Abd El-Haleem proposed a novel secure relative routing protocol for MANET, called TRIUMF for securing MANET against Packet Dropping Attack. It is hard to determine whether the node is malicious or selfish node. This proposed protocol first distinguishes the malicious and selfish nodes and then controls the degree of selfishness. The proposed monitoring tool first detects the malicious behavior and then the path searching tool identifies the attacker or compromised nodes in the network and isolated them, and then proposed routing protocol which selects the routes securely.
8. Zen Yan proposed a Trust Evolution based security solution to provide effective security decision on protection of data, safe routing and other network activities. The authors proposed two trust models based on the two ad-hoc system models. One is the independent model that represents independent ad-hoc networks, have not any connection to the predefined (fixed) networks. The second model is the cross model, that represents ad-hoc networks. This model has some few connections to the fixed networks. Personal Trusted Bubble (PTB) represents an ad-hoc node is the basic unit in both models. In PTB, the owner of the ad-hoc device has unreasonable full trust on the device, needed for the ad-hoc communication and organization. Trust relationship (logical and rational) should be evaluated computationally among bubbles, between bubbles and the fixed networks. The proposed trust evaluation is conducted digitally, ahead of any communication and for the better security decision; the result of this evaluation should be noticed.

III. ATTACKS

Security is the main concern of any MANET for secure transmission of any data. Due to the decentralized and open nature of wireless system, MANET is highly prone to various attacks. Attacks can be categorised as passive attacks and active attacks. Passive attacks only monitor the data traffic and looks for clear text password and other sensible information which may be used in other attacks. Active attacks try to break the security systems. Active attacks may include introducing malicious nodes, to steal or modify the sensitive information and break or bypass the security mechanism. Types of attacks are as follows:

- *Black hole attack*: In this type of attack, malicious nodes broadcast the message to all the nodes, that it has valid, shortest and fresh route to the destination. In this way such malicious nodes divert all the traffic toward itself and without forwarding the data packets to the neighboring nodes, all the data packets are dropped.
- *Gray hole attack*: this attack can be considered as a form of black hole attack. In this type of attack, the malicious nodes drop the data packets for particular nodes for particular period of time in the network. That is why grayhole attack is difficult to identify than black hole attack.
- *Wormhole attack*: In this type of attack, two malicious nodes form a tunnel and all the data packets received at one location of the network are tunneled at the other location in the network, in such way all the data are resent to the network. The tunnel between two malicious nodes is called as wormhole. Such attacks prevent any route other than any wormhole from being discovered.
- *Byzantine attack*: This type of attacks is carried out by intermediate nodes or group of intermediate nodes. Such malicious nodes provide the false routing information and create routing loop as well as forward the data packets to that path which is not optimal, which may be harmful to the routing system.
- *Denial of service attack*: it prevent the victim from being used all or part of the network connections. DOS attacks may have numerous forms and hard to detect. In this type of attack, attacker nodes sends the excessive amount of data packet or request to the server so that server get busy in testing illegal request and will not be available to others. This attack may degrade the performance of the network since it consumes the energy (battery power) of nodes.

In this scenario two attacks are considered: Vampire attack and DDoS attack.

Vampire attack: This is not protocol specific attack and hard to detect. This attack may exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic routing. It drains the power of the node which may result in network failure and data loss. The attacker packets (vampire attack) consumes more power of any nodes than the normal packets.

DDoS attack: This can be carried out from several layers, it is a distributed layer, large-scale attempt by malicious nodes to amass the victim network with enormous number of packets. This exhausts the resources of victim network such as bandwidth, computing power etc. in such case victim unable to provide the services to its client and network performance may degrade.

IV. PROPOSED DESIGN

The basic idea behind the trust based approach is to find out nodes having highest energy. In each cluster of network, maximum two nodes are identified having highest energy called trusted nodes. The communications are carried out

through these trusted nodes. That is trusted node in each cluster send the received packets to the destination or next trusted node in another cluster and so on. To find out the malicious nodes in the network, send and received packets as well as route response is calculated. Then the number of packets (send & received) compared to the threshold value, if it is less than the threshold value then particular node is considered as a malicious node.

- *Cluster based network formation:* The number of cluster depends on the total number of nodes in the network. Here maximum number of nodes in the cluster is considered as 10. To place the node in the cluster, the value of x and y coordinates of each cluster are determined to make sure that each x and y coordinates of each cluster to be within the specified range. For example, for a network of 300m x 300m, if the number of clusters are 3 then each node will be placed in 100m x 100x area.
- *Selection of Trusted nodes:* After formation of the network, the trusted nodes are determined (Nodes having highest energy). To choose the random energy of each node, rand () function is used. For example, expr rand ()*1000. We can also check the energy of each node by using, set e [$node (2) energy]; then print the value of e. After calculating the initial energy of each node in each cluster, nodes with highest and second highest energy have been chosen. These two are called as trusted nodes in each cluster. These nodes with highest and second highest energy are referred to as cluster head one and cluster head two respectively. All the communication will be carried out using these cluster heads.
- *Counting packets (send & received) along with Route responses:* The send and received packets are calculated for each node; also route response of each node is determined. This information is helpful to determine the malicious node in the network. Node having less route response and send packets may be considered as a malicious node.
- *Comparison of packets with threshold to get malicious nodes:* To get the malicious node, the number of packets (send & received) is compared with the threshold value to determine the malicious nature of any node. While calculating, the route response is also taken into consideration. The threshold value is set as 30. Here, we take into account the DDoS attack. This comparison is playing a vital role to determine the DDoS attacks.
- *Routing table update:* After determining the trusted nodes and malicious nodes in the network, the information is updated in the routing table. According to the routing table, most trusted path is selected for communication which helps to improve the network life as well as network performance.

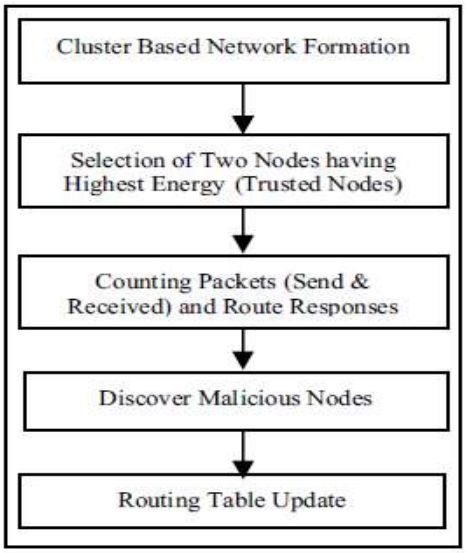

Figure 1: Work Flow

V. PROPOSED WORK

In the proposed work, the cluster based network is formed. Ten nodes are considered in each cluster. Total number of cluster is based on the total number of nodes in the network. Two nodes having maximum energy have been selected in each cluster.

Selection of each cluster:

Max_cluster=expr[val(nn)/Max_Node_in_Cluster]

Here, val (nn) is the total number of nodes in the network and maximum ten nodes are considered in each cluster. Also X and Y coordinates (Maximum values of X and Y) have been calculated for each cluster:

Set max_x[expr[expr $CURRENT_CLUSTER+1] $val (x)/$MAX_CLUSTERS]*

To calculate the energy of nodes, rand() function is used. The two nodes with highest energies in each cluster have been calculated. These two nodes are called Cluster Head 1 and Cluster Head 2. In between Cluster Head 1 and Cluster Head 2, node with highest energy is selected as CLUSTER HEAD in each cluster.

VI. SECURITY AND PERFORMANCE ANALYSIS

For the simulation purpose Network Simulator 2 (NS-2.35) has been used. Simulation parameter are as follows: The simulation area is 300 m by 300 m. AODV protocol has been used, since AODV protocol is loop free, avoid counting to infinity problem and does not need any central administration system to handle routing process. The UDP is used as application traffic. UDP has two advantages over TCP: First, the source code continuously sends UDP packets even if malicious nodes drop them, while node finishes the

connection if it is used TCP. Second, it is able to count sent and received packets separately even if the UDP connection is lost during simulation; but in case of TCP, node finishes the TCP connection after a while if it has not received the TCP acknowledgement packet.

Following are the simulation parameters:

Parameters	Value
Simulation Area	300*300
Number of Nodes	30
Routing Protocol	AODV
Application Traffic	CBR
Packet Size	1000 bytes
Simulation Time	(Total No. of Nodes +3) Sec
Packet Interval	0.07 Sec
Queue	50

Table1: Simulation Parameters

Figure 2 shows creation of normal scenarios. Here, we can see the communication is being carried out between node 4 and 15 and node 5 and 16.

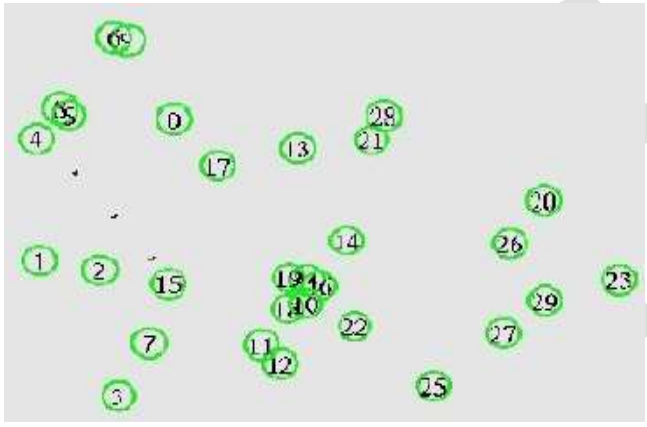

Figure 2: Normal Scenario Creation

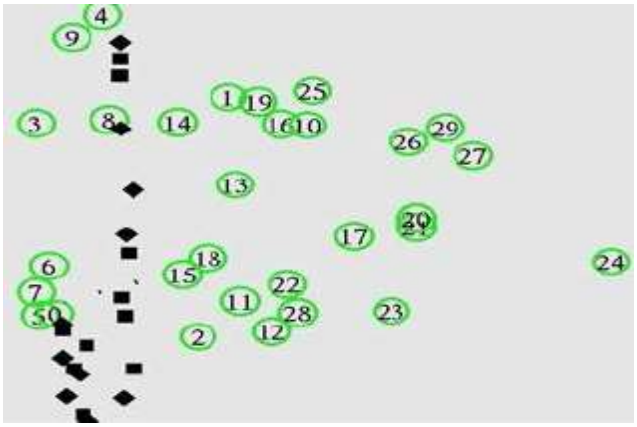

Figure 3: Scenario with DDoS Attack

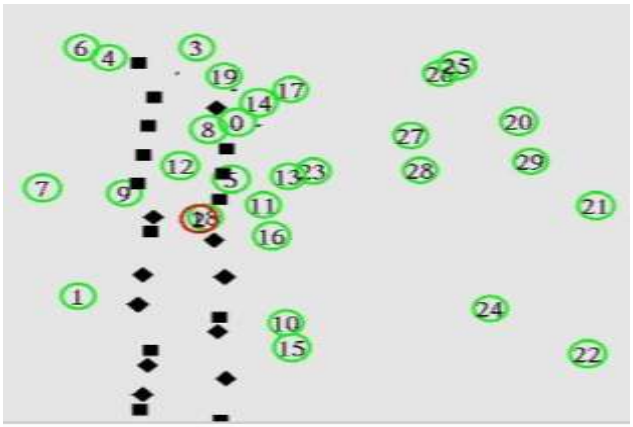

Figure 4: Scenario with Vampire and DDoS Attacks

Following Figure 5, Figure 6, Figure 7, Figure 8, Figure 9 and Figure 10 shows the PDR, Throughput, Delay, Jitter, Goodput and Energy respectively.

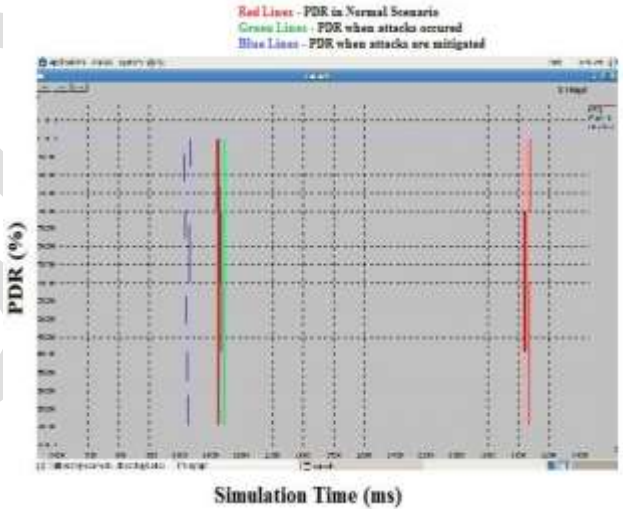

Figure 5: Packet Delivery Ratio

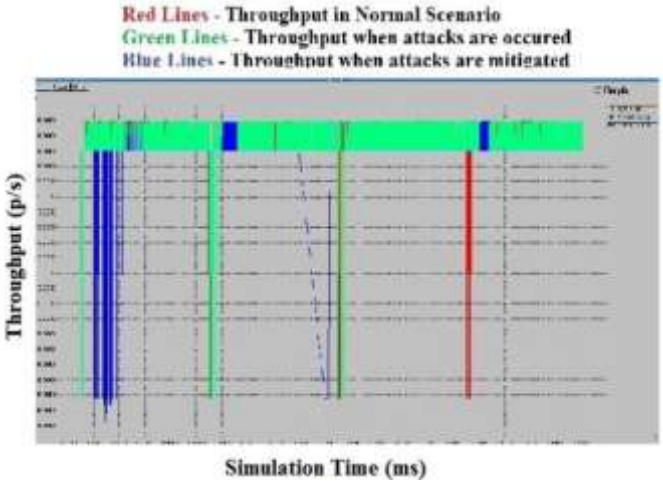

Figure 6: Throughput

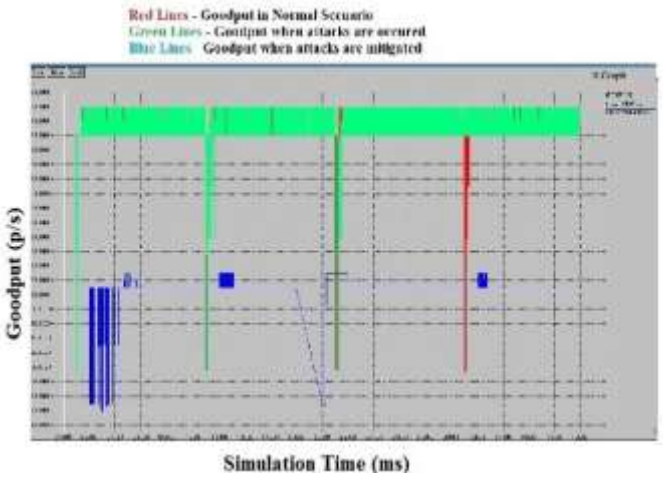

Figure 7: Goodput

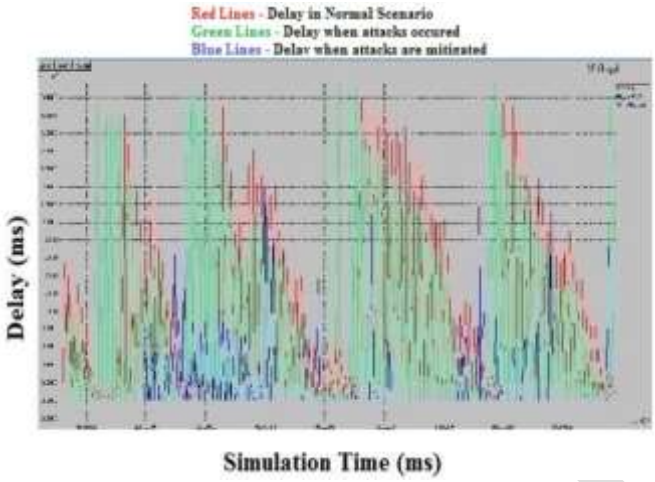

Figure 8: Delay

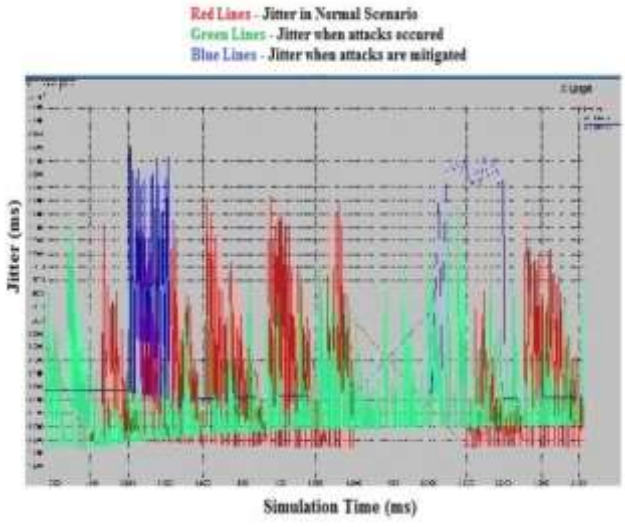

Figure 9: Jitter

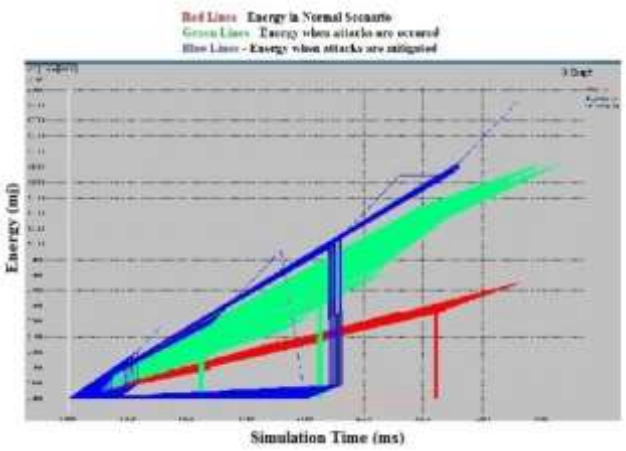

Figure 10: Energy

VIII. CONCLUSION AND FUTURE WORK

The Vampire and DDoS attacks are resources consumption attacks which drain the energy of node in the network. This draining of the energy of the nodes will affect the packet forwarding process which in turn might degrade the performance of the underlying network. Here we have considered small network of 30 nodes which are divided into three clusters; each cluster included ten nodes. Simulation have been performed and various parameters have been considered. From the result, we can conclude that the Vampire and DDoS attacks have been mitigated using trust based approach. The future work is to use the proposed technique to mitigate Vampire and DDoS attacks with more number of nodes and increasing the simulation area and also for other types of attacks.

REFERENCES

[1]. Pallavi Kharti. Using Identity and Trust with Key Management for achieving Security in Ad-hoc network; IEEE; 978-1-4799-2572-8/2014.
[2]. Sandeep A. Throat and P.J.Kulkarni. Design Issues in Trust Based Routing for MANET; IEEE; July 11-13, 2014.
[3]. Jenita T.and Jayshree P. Distributed Trust Node Selection for Secure Group Communication in MANET; IEEE; 978-1-4799-4363-0/2014.
[4]. H.Bharani , M.Kanchana, S,B.Dhivya , V.Kavitha and I.Vinnarasi Tharania . Vampire Attacks: Draining Life from Wireless Ad-Hoc Sensor Network; IJSTE; Vol. 1, Issue 1, July 2014.
[5]. Prof.Ramya S. Pure, Gauri Patil and Manzoor Hussaion Hussaion . Trust based solution using counter strategies for Routing attacks in MANET; IJISET; Vol. 1, Issue 1, July 2014.
[6]. G. Vijayanad and R. Muralidharan. Overcome Vampire Attacks Problem In Wireless Ad-Hoc Sensor Network By Using Distance Vector Protocols; IJCSMA; Vol. 2, Issue. 1, pg. 115-120, January-2014.
[7]. Naveen Kumar Gupta and Kavita Pandey. Trust Based Ad-hoc On Demand Routing Protocol for MANET; IEEE; 978-1-4799-0192-0/2013.
[8]. Naveen Kumar Gupta and Amit Garg. Trust and shortest path selection based routing protocol for mobile ad-hoc networks; IJCA; Vol. 76, No.12, August 2013.

[9]. Pallavi Kahtri and Aamir ohammed. TDSR: Trust Based DSR Routing Protocol for Securing MANET; International Journal of Networking and Parallel Computing. Vol. 1, Issue 3, January 2013.
[10]. Radha Krishna Bar, Jyotsna Kumar Mandal and Moirangthem Marjith Singh. Quality of Service of mobile ad-hoc network through Trust based AODV routing protocol by exclusion of Black-hole attack; Science Direct; CIMTA 2013.
[11]. Sumathy Subramaniam, R. Saravanan and Pooja K. Prakash. Trusted Based Routing to Improve Network Lifetime of Mobile Ad-hoc Networks: Journal of Computing and Information Technology; CIT 21, 2013.
[12]. Issac Woungang, Mohmmed S. Obaidat, Sanjay Kumar Dhurandher, Han-Chieh Chao and Chris Liu. Trust enhanced Message Security Protocol for Mobile Ad-hoc Networks; IEEE; ICC 2012.
[13]. Ahmed M. Abd El-Haleem and Ihab A. Al.TRIUMF: Trust-Based Routing Protocol with control degree of Selfishness for Securing MANET against Packet Dropping Attack; International Journal of Computer Science; Vol. 8, Issue 4, No. 1, July 2011.
[14]. N. Bhalaji and Dr. A. Shanmugam. Defence Strategy using Trust based model to mitigate active attacks in DSR based mobile ad-hoc network; Journal of Advances in Information Technology; Vol. 2, No. 2, May 2011.
[15]. Zhen Yan, Peng Zhang and Teemupekka Virtanen. Trust Evaluation Based Security Solution in Ad-hoc Networks; 2011.