A TRUST BASED APPROACH FOR DETECTION AND ISOLATION OF MALICIOUS NODES IN MANET

Aravindh S[1], Vinoth R S [2] and Vijayan R[3]
[1,2] MS Software Engineering, School of Information Technology and Engineering,
VIT University ,Vellore, Tamil Nadu, India
aravindh.sp@gmail.com
vinoth9592@gmail.com
[3]Assistant Professor(SG),School of Information Technology and Engineering,
VIT University, Vellore, Tamil Nadu, India
rvijayan@vit.ac.in

Abstract— **A Mobile Adhoc Network (MANET) is a self-organized system comprised by multiple mobile wireless nodes. Due to the openness in network topology and the absence of centralized administration in management, MANET is vulnerable to attacks from malicious nodes. Nodes can change position quite frequently, which mean the mobility of the network. Node misbehaviours are serious attacks for routing protocols in MANET. Secure routing is the milestone in mobile Adhoc networks.**

The proposed trust management scheme gives an overview about trust in MANETs and current research in routing on the basis of trust. It uses trust values to favour packet forwarding by maintaining a trust counter for each node. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious and isolated from the Network, thus by increasing the performance of the network.

Keywords: **Trust Proctor, Trust Handler, Reputation Accumulator, Reputation Evaluator, DRUT, MANET**

I. INTRODUCTION

Wireless networks are defined as computer networks connected through wireless links, such as radio frequencies and infrared rays. Wireless local area networks (WLANs) have arisen with the main purpose of overcoming the limitations imposed by traditional wired networks, thus permitting faster network installations and mobility at lower costs. Ad hoc network consists of mobile nodes which communicate with each other through wireless medium without any fixed infrastructure. Mobile Ad hoc Network (MANET) do not have any fixed infrastructure and consists of wireless nodes that move dynamically without any boundary limitation. MANETs are advantageous because they are quick to install, provide fault tolerance, connectivity and mobility.

A. Security Issues in MANET

Various attacks exist in MANET. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

Gray Hole attack can advertise its route as a valid path with the motivation of intercepting the packets. The packets that pass through the attacked node are dropped with certain probability. Worm Hole Attack follows the tunnelling process. Group of nodes collaborate to encapsulate and exchange messages between them leading to short-circuit of normal flow of packets and consume energy. Black Hole Attack the node advertises as a valid path to the destination and intercepts every packet without forwarding and can generate fake information. Jellyfish Attack can enter into the forwarding group and can delay the packets unnecessarily for a specific time and then forwards the packet resulting in performance degradation. Denial of service attacks aim at the complete disruption of the routing function and the entire operation of the ad-hoc network. In a routing table overflow attack, the malicious node floods the network to consume the resources.

B. Design Challenges in MANET

MANET exhibits unique features like open medium, dynamic topologies, bandwidth constrained, variable capacity links, energy constrained operation, limited physical security MANETs hence attracted by the attackers. The nodes in the MANET are vulnerable to all kinds of attacks launched through compromised node. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application specific trade-offs between security and resource consumption of the device.

MANETs must provide various levels of security guarantees to different applications for their successful deployment and usage. However, due to their wireless links and lack of central administration, MANETs have far greater security concerns than conventional networks. It is easy for attackers to eavesdrop the messages since there is no physical connection. Without a security scheme in place, an intruder can easily participate in routing packets. Therefore, it can directly attack the network by dropping packets, tampering with packets, injecting false packets or flooding the network. As a result, it is possible to launch sophisticated wormhole, man-in-the-middle and Denial of Service (DoS) attacks with ease, or to impersonate another node. Security protocol designers for MANETs face technical challenges due to severe resource constraints like memory size, openness to eavesdropping, lack of specific ingress and exit points, high security threat, vulnerability, unreliable communication, and rapid changes in topologies or memberships because of user mobility or node failure.

II. SYSTEM ARCHITECTURE

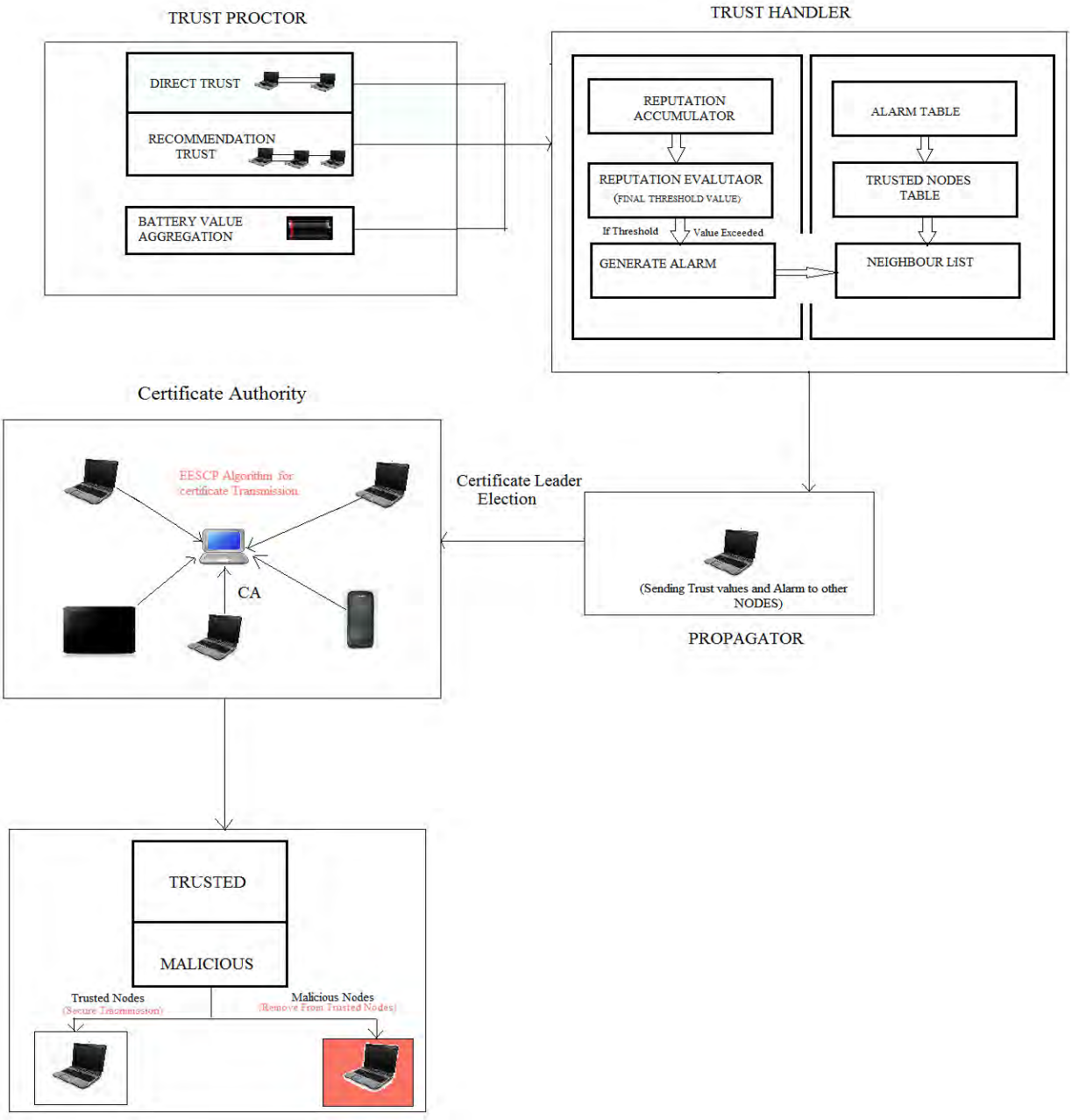

Fig. 1. Detection and Reaction Using TRUST (DRUT)

A. Direct Proctor

Direct trust calculation comes under direct observation of neighbors. In this proposed scheme, every node in the network monitors the behavior of its neighbors, and if any abnormal action is detected, it invokes an algorithm to determine direct trust value. This module monitors neighbour nodes by passively listening to their

communication for detecting dropped packet, delayed packet, forwarded packet. Every node in the network monitors the behavior of every other neighbors using watchdog mechanism to check whether neighbour really forwards the packet or drop them. By default all the nodes while communicating with other nodes the direct trust value of all the communicating nodes are calculated and stored in the trust table of corresponding node with field name like node index, direct trust value and one more total trust value of the corresponding node.

Otherwise by default all the nodes while communicating with other nodes, the direct trust value of all of the communicating nodes are calculated and stored in the trust table of corresponding node with field name like node index, direct trust value and one more total trust value of the corresponding node. After some time the neighbour nodes may move out of the range of a particular node due to their mobility and again they come back to the transmission range then again trust value is calculated and the corresponding entry in the table is updated .

1) *Direct Trust:* Direct trust agent performs the following tasks derivation of trust, quantification and trust computation. Node x want to calculate the trust value on node y termed as .

$$dt_{xy} = p_s / p_r \quad (1)$$

Where dt_{xy} is the final direct trust value of x and y.

p_s is the successful packet sent from the node x.

p_r is the successful packet receive from the node y.

To calculate the direct trust on node y, node x has to monitors the above statistics by using the following Table I

TABLE I
Direct Trust Table

Node ID	Packet Sent	Packet Received	Packet Dropped	Direct Trust

2) *Recommendation Trust*: The task of indirect trust monitor is to collect or request the trust related information of target node from the neighbouring nodes. The neighbour collecting the trust information is another issue. In other words, while requesting the trust information of the target node from neighbours, the direct trust value of that neighbour node should be considered. This is to avoid the security attacks like bad mouthing. This information generally called as Recommendation trust.

Obtaining Indirect Trust on Y from N

Step 1: Node X sends RTREQ to node(s) N.

Step 2: If node X has direct trust value on Y, then it will reply back with RTREP.

Step 3: Else If X does not have direct trust value record it will discard the RTREQ

Step 4: After receiving RTREP reply from neighbours consider the trust value of the node with maximum direct trust value by applying fuzzy logic.

Step 5: Integrate all the obtained RT value from neighbours to calculate the indirect trust value.

The task of recommendation agent is to collect or request the trust related information of target node from the neighbouring nodes. The source node will broadcast the recommendation request packet to all its neighbouring nodes. From the reply packets, fuzzy logic is applied to the direct trust value of all the replied neighbours. The node with maximum trust value is considered for evaluation of recommendation trust value.

3) *Battery Value Aggregation*: In Mobile Ad hoc network, the nodes are spending some energy for receiving data packets and some amount of energy for forwarding the packets to neighbour nodes. Initially they have maximum energy that means nodes with full battery capacity. After the communication starts energy consumption also starts. This consumption of energy is more for trusted nodes because, they have to receive as well as forward the packets to its neighbours. But is case of selfish nodes energy utilization is somewhat low, they only receive data packets, they won't forward packets to neighbors. Energy calculation requires initial node configuration. In node configuration initial energy, ideal power consumption, receiving power consumption, transmission power consumption all these details should be specified

B. Trust Handler(TH)

The trust handler handles all the incoming and outgoing ALARM messages. Incoming ALARMs can originate from any node. Therefore, the source of an ALARM has to be checked for trustworthiness before triggering a reaction. This decision is made by looking at the trust level of the reporting node. The proposed framework has provisions for several partially trusted nodes to send ALARMs which will be considered as an ALARM for a single fully trusted node. The outgoing ALARMs are generated by the node itself after having experienced, observed, or received a report of malicious behaviour. The recipients of these ALARM messages

are called friends, which are maintained in a friends list by each node. The ALARM should be generated even when the Final Trust value is low.

Reputation accumulator collects all the information from the Trust Monitor, which is essential to compute the Final Trust Value (FTV) for each node. After Finalizing the Final Trust Value, by holding this value, it could say that, the partial Identification of Malicious node. It was identified by using Trustworthy Mechanism. After identifying the trust, it generates the alarm to its neighbour nodes to avoid havoc in the network. The trust table maintains the trust records of each node to determine the trustworthiness of an incoming alarm. The friend list contains the list of all nodes to which the node has to send alarms when it detects any malicious activity. Trust evaluator generates a Trust Record Table (TRT) with Node id, trust type and Trust value of each node. Each node maintains a TRT table and every time trust is evaluated TRT table is updated.

$$FT_{value} = E_{value}+DT_{value}+IDT_{value}$$

Where

E_{value} = Energy value
DT_{value} = Direct trust value
IDT_{value} = Indirect trust value

Propagation or updating of the trust is done by either reactive manner. In this approach trust is updated only when demanded. So each node contains the direct trust value of all remaining nodes as well as the indirect trust or recommended trust value. Nodes with less trust values marked as MALICIOUS. An alarm is generated by the Trust Manager to indicate the node's malicious behaviour to other trusted nodes in its range thus isolating the less trusted nodes and building a secure system. No suspicious and misbehaving nodes can cause vulnerabilities and threats to the proposed scheme. Trust values of each node are calculated and packet transmission is done through nodes which has highest trust values. These trust values are calculated dynamically time to time and updated. Hence it ensures the secure transmission of packets.

C. Certificate Authority

Energy Efficiency and Secure Communication Protocol (EESCP) is used to divide the MANET into a set of 2-hop clusters where each node belongs to at least one cluster. The nodes in each cluster elect a leader node (cluster head) to serve as the IDS for the entire cluster. To balance the resource consumption weight based leader election model is used, which elected an optimal collection of leaders to minimize the overall resource consumption and obtaining secure communication using diffie-Hellman key exchange protocol.

III. RESULTS AND DISCUSSIONS

A. *NS-2 Scenario 1-60 Nodes*

A network model has been created as shown in the figure 2 with the help of NS-2. 25 nodes have been used in this scenario where Node ID 0, to Node ID 59, are connected to wireless network framing a MANET. The Soucrce Node ID is 2 and the Destination Node ID is 11, where the packets are pass between nodes using the AODV routing protocol.

Whenever the network Congestion has happened, the packet starts dropping the packets, either its because of a malicious activity of a node or a congestion occurs.

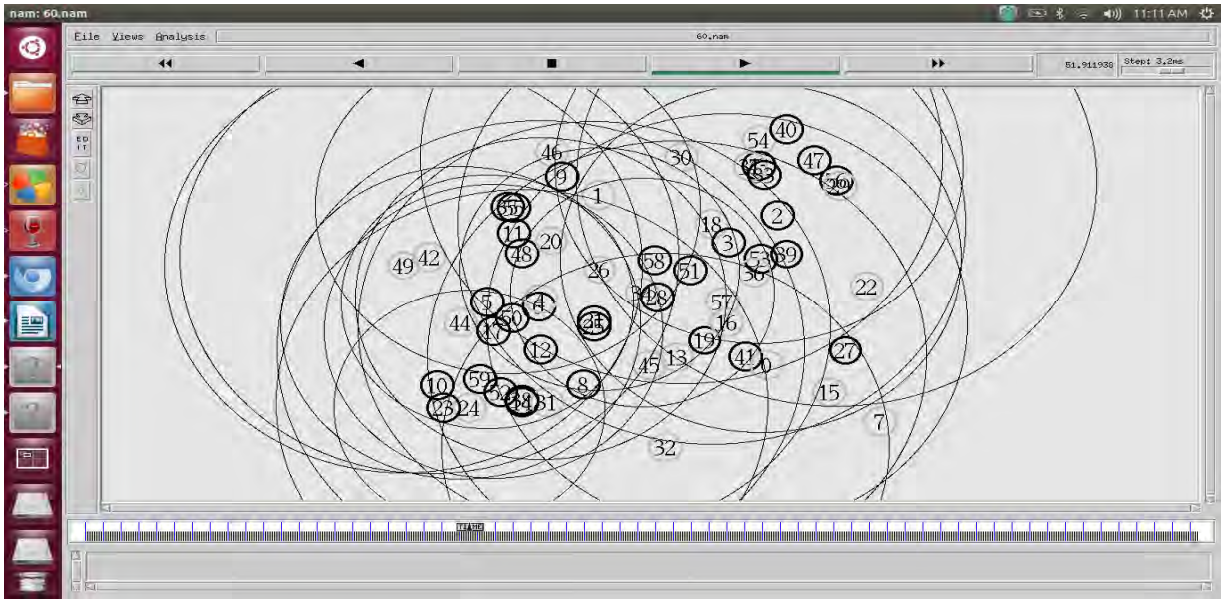

Fig. 2. Sample Model with 60 Nodes

B. *NS-2 Scenario 2-100 Nodes*

A network model has been created as shown in the figure 3 with the help of NS-2. 25 nodes have been used in this scenario where Node ID 0, to Node ID 100, are connected to wireless network framing a MANET. The Soucrce Node ID is 2 and the Destination Node ID is 11, where the packets are pass between nodes using the AODV routing protocol.

Here because of the high congestion of packets, which leads to the increase in the delay of packets to reach the destination and sometimes the packets are dropped, which leads to the destination node to probe once again to source node for requesting the dropped packets.

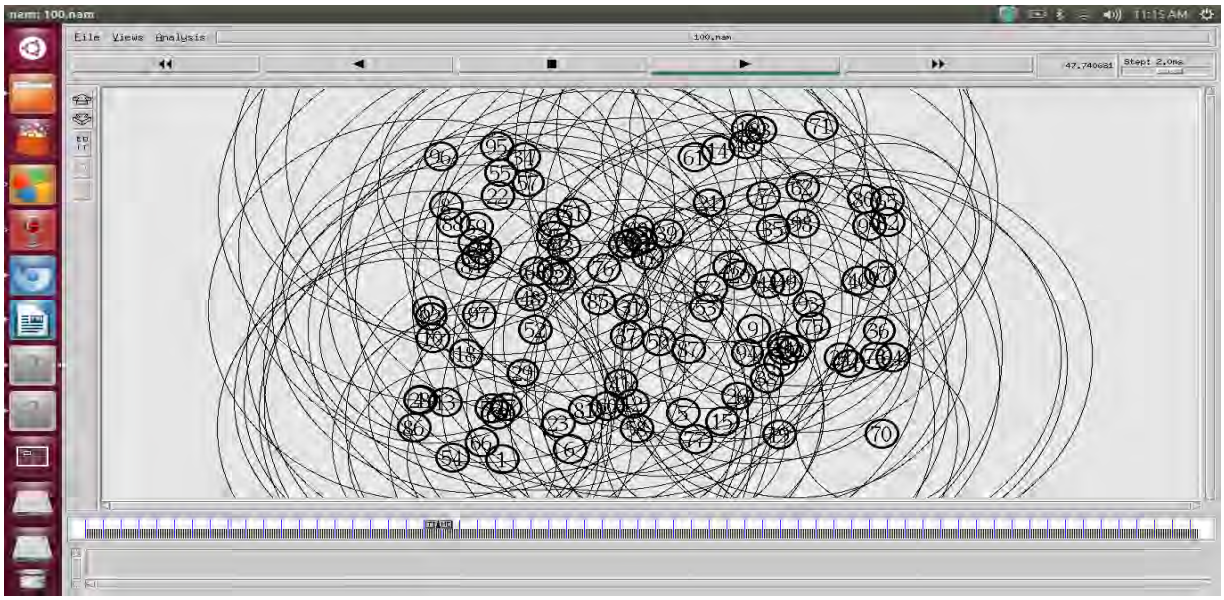

Fig. 3. Sample Model with 100 Nodes

C. *Throughput for 60 Nodes-Proposed and Existing*

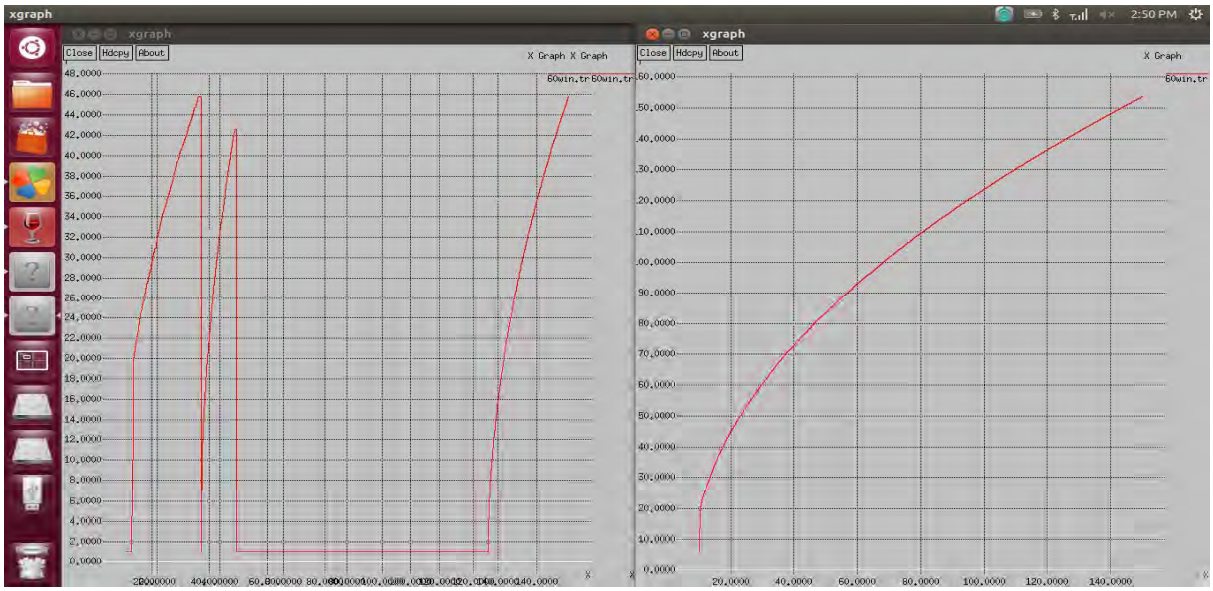

Fig 4 Throughput for the sample of 60 nodes for Existing and proposed

The graph is plotted with two different scenarios (60 and 100 nodes).With the effect to implementation of our framework. A comparative study is made with the existing system to the proposed framework. We have taken existing system that features Direct and Indirect Trust alone for detection of malicious node without Certificate Authority. Data are collected from the existing system node and the probability of detecting misbehaving nodes is compared with the probability rate of proposed system.

In the figure 4 and figure 5, it is concluded that the proposed system has higher and even consistent throughput. After the isolation of malicious nodes, the increase in the throughput and decrease in the end to end delay is observed. In the Existing system, the throughput has been varying at different timestamp, whereas in the proposed system,as the malicious nodes are identified in the first level of transmission and malicious nodes are isolated with increase in the level of throughput . The removal of malicious node ID in the trusted node table make the malicious nodes isolate. After the successful isolation, the trusted nodes are transferring the packets by having the certificates.

D. *Throughput for 60 Nodes-Proposed and Existing*

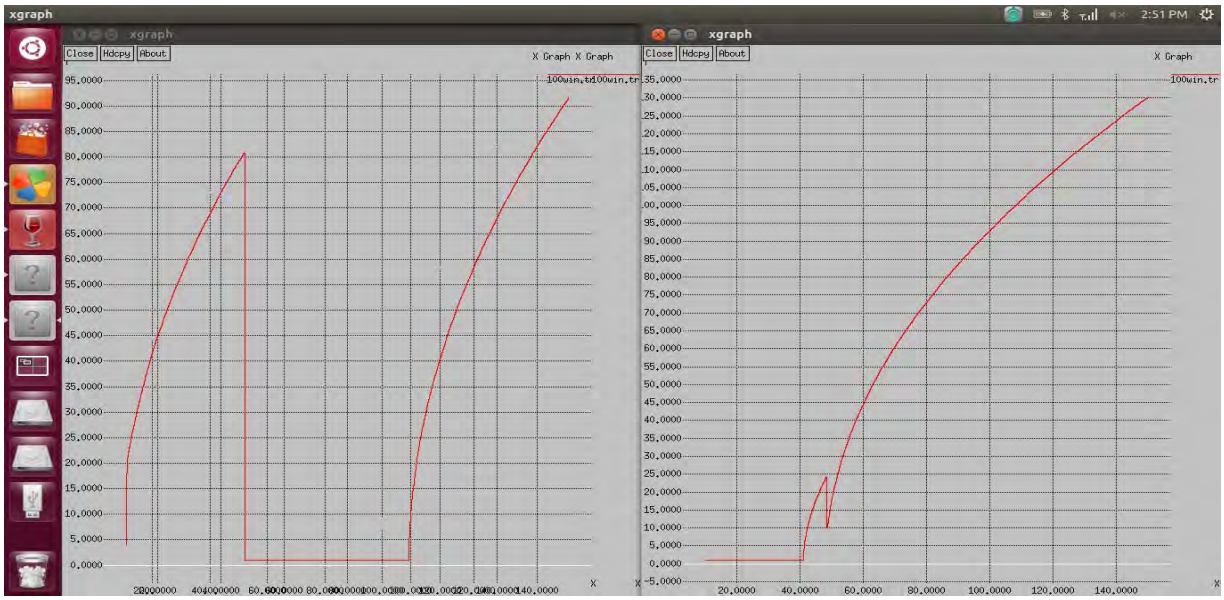

Fig 5 Throughput for the sample of 100 nodes for Existing and Proposed

IV. CONCLUSION

In this research work the solution to calculate the trust in mobile ad hoc network and to identify the malicious nodes taking energy utilization factor as an additional factor in calculating direct trust. Further performance evaluation by simulation and the investigation of additional elaborate adversary models, both for misbehaviour and for trustworthiness, are under way. Various important issues of design of such systems for wireless communication networks are also presented. In future the addition of some watchdog mechanisms for supervisor module will get more secured network. By considering some additional factors like wrong routing, replay packets generated, battery exhaustion, link broken will add more accuracy for the calculation of trust value. By considering the more reasons for packet dropping it will get more accurate trusted network. As a future enhancement this work can be extended to detect the selfish nodes which are malicious and malicious nodes which are acting as selfish nodes.

REFERENCES

[1] Ji Guo , Alan Marshall, Bosheng Zhou, "A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad hoc Networks", 2011 International Joint Conference of IEEE.

[2] Manoj V, Mohammed Aaqib ,Raghavendiran N and Vijayan R "A Novel Security Framework Using Trust and Fuzzy Logic in MANET", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[3] Jaydip Sen, "A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks", Computer Research Repository of IEEE 2010.

[4] Vijayan R, Mareeswari V and Ramakrishna K, "Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 3, June 2011 pp 647-652.

[5] Yacine Rebahi, Vicente .E Mujica-V and Dorgham Sisalem, "A Reputation-Based Trust Mechanism for Ad hoc Networks", proceedings of IEEE symposium on computers and communications 2005.

[6] Sonja Buchegger, Jean-Yves Le Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks", EPFL IC Technical report IC 2003.

[7] Ramprasad Kumawat and Vinay Somani "Comparative Study of On -demand Routing Protocols for Mobile Ad-hoc Network", International Journal of Computer Applications Volume 27– No.10, August 2011.

[8] Hui Xiaa, Zhiping Jiaa, Xin Lia, Lei Jua, Edwin H.-M. Shab, "Trust prediction and trust-based source routing in mobile ad hoc networks", ScienceDirect Ad hoc Networks 6 (2010).

[9] Pankaj Sharma and Yogendra Kumar Jain, " TRUST based Secure AODV in MANET", Journal of Global Research in Computer Science Volume 3, No. 6, June 2012.

[10] Rajan Shankaran, Vijay Varadharajan, Mehmet A. Orgun, and Michael Hitchens, "Critical Issues in Trust Management for Mobile Ad-Hoc Networks", Information Reuse and Integration,IEEE 2009.

[11] G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", International Journal of Computer Applications Volume 9– No.9, November 2010

[12] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", ScienceDirect Ad Hoc Networks 1 (2003) pp 13–64.