Node Cooperation and Message Authentication in Trusted Mobile Ad Hoc Networks

Vijayakumar A [#1], Selvamani K [*2]
[# 1]Research Scholar, Department of Computer Science and Engineering, Anna University, Chennai-25 Tamil Nadu, India.
[1] kaniporiyalan@yahoo.co.in
[*2] Assistant Professor, Department of Computer Science and Engineering, Anna University, Chennai-25 Tamil Nadu, India.
[2] selvamani@annauniv.edu

***Abstract*— Mobile Ad hoc Networks (MANETs) are no infrastructure mobile network that relies on the cooperative route dissemination which forwards the packet in short transmission range. This research work involves in increasing the capabilities of node cooperation and message authentication by eliminating the selfish nodes because the selfish nodes are very harmful to mobile ad hoc networks while having communication. Hence, encouraging the reliable cooperation among nodes becomes a very important concern in mobile ad hoc networks. For this purpose, two hop communications are used in MANETs with cooperative communication, message integrity, hop-by-hop authentication. This research work proposes a high secured cooperative trusted communication using Object Link State Routing Protocol (OLSR) and Message Authentication among the nodes in mobile ad hoc network. This protocol establishes a verifiable impression of uniqueness for network traffic enabling hop-by-hop, secured and cooperative communications. The simulation results prove that the proposed scheme improves the throughput and decreasing the delay in packet delivery among trust based cooperative nodes in mobile ad hoc networks. To ensure secured message transmission and integrity of the messages that the Merkle Tree and Hash Chain based message authentication scheme is additionally incorporated for more security.**

Keywords - Authentication, Cooperative Communication, Packet Delivery, Routing, Transmission, Throughput.

I. INTRODUCTION

Mobile Ad hoc Network has the capability of organizing its own network whenever communication is required. Mobile nodes in MANETs have the property of moving freely in the absence of a fixed infrastructure. Hence, frequent changes in routes will happen due to unpredictable topology changes and link disconnections. Also MANETs are facing the pitfalls in energy, bandwidth computational power and in trusted centralized authority. Recent Investigations shows that node cooperation becomes an important issue and unsolvable problem in MANETs. Moreover providing proper co-operation is much complex in MANET than other network environment. In MANET nodes can arbitrarily join and leave the network and due to the lack of centralized control the detection of misbehaving nodes is difficult. In MANET non co-operative nodes or misbehaving nodes are broadly classified as malicious nodes and selfish nodes. Malicious nodes are the group of nodes that intentionally attacks and shut down the entire network. Selfish nodes are the group of nodes that gain the information from the network and they do not cooperate with the other nodes for future communication.

This research paper attempts in providing necessary cooperation among the nodes in MANETs. Node cooperation is performed by two important strategies namely reward and punishment. The cooperation properly for communication will be rewarded and misbehaving nodes are punished such that they will not be allowed to participate in communication because those are harmful in packet delivery among these networks. The message integrity is also achieved by applying Merkle hash tree algorithm.

The rest of the paper is organized as follows: Section II describes the background in node cooperation in MANETs. Section III explains the proposed architecture for cooperation and authentication. Section IV reveals the simulation results and discusses the results obtained. Section V concludes the proposed work and results obtained.

II. BACKGROUND WORK

There are many works pertaining to node cooperation mechanisms in mobile ad hoc networks namely reputation-based, credit-based approaches and etc.,

A. Reputation based Approaches

In reputation based approaches, the Watchdog mechanism is one of the promiscuous mode operations for detecting misbehavior nodes. It was used to observe neighbors and also aims in detecting and isolating the selfish nodes. The node reputation is heavily weighted towards the past reputation. In this, only positive indirect reputation is allowed to avoid false accusation and Denial of Service (DoS) attacks. The disadvantages of

Watchdog mechanisms are that they are not detect the misbehaving nodes in the presence of ambiguous, collisions, receiver collisions, limited transmission power, false misbehavior, collusion, and partial dropping[9]. The rating of other nodes which performs route selection using PATHRATOR technique and by choosing proper routes without selfish nodes, as well as that has high node rating. In this, the selfish nodes are not punished, but it is rewarded to a certain extent, as their packets continue to be forwarded by other nodes. The PATHRATOR alone cannot detect a path [7].

An extension to the DSR protocol called OCEAN, which also considers selfish behavior. All node maintains the ratings for neighbors and each node directly interact with it. By avoiding trust management complexity and also false accusation, these ratings are not propagated to the other nodes. The reputation value of neighbor node is less than the faulty threshold, then based on these faulty threshold in a faulty list, the traffic will be rejected.[6].The problem of selfish nodes were also addressed by SORI (Secured and Objective Reputation based Incentive) based on the ratio of the number of packets sent and number of packets forwarded. Also this reputation is updated periodically and is broadcast to neighbor nodes when significant changes occurs which is called the first hand reputation, similarly the second-hand reputation is based on the credibility and weight obtain on the first hand reputation by sender node. As a punishment to selfish nodes the packets originating from selfish nodes are periodically dropped. Also an alarm signal is sent to neighbor nodes about selfish nodes. The extension to the source routing protocol named CONFIDANT which represents the selfish and several types of misbehavior. The misbehaving nodes were found, the system sends alarm to other nodes in the network, defined as friends to isolate misbehaving nodes from the network .The CONFIDENT protocols are limited to one-to-one interaction and misbehavior results in a bad reputation propagating to more than one node and it addresses additional issues in network layer, such as traffic diversion. [3].

B. Credit based Approaches

'NUGLET' is one among the credit based model [2] which is the unit of credit gained by cooperative nodes. In this model source node includes necessary credit in its packet and each intermediate node takes its quota from packet. In Packet trade model, every intermediate node buys the packet from previous node in the path and sells it to the next node. This mechanism relies on a tamper-proof hardware at each node to ensure that the correct amount of credits are added or deducted [2,3]. 'Sprite' is a cheat-proof system which does not rely on any tamper-proof hardware. Credit Clearance Service (CCS) is a central entity which is responsible for balancing network nodes' credits. Sprite makes use of a digital signature for any single transaction. The author analyses the effectiveness of the mechanism using game theory [12]. The Cooperation was also achieved in MANETs through Priority forwarding which is providing incentive based packet forwarding among the mobile nodes. In this scheme, an ad-hoc network provides two types of traffic: best effort and priority. The source node pays for forwarding its packet to intermediate nodes and hence best-effort service is provided [11].The next incentive based cooperative scheme in which every node determines the price of providing service for other nodes to forward their packets. The pricing was based on delivery ratio of packets and available bandwidth. The system which focuses combination of reputation method and the price based method for cooperative communication in MANETs [5]. The various pros and cons of existing systems were analysed through previous backgrounds. Hence it is necessary to propose a scheme to resolve the problems in node cooperation and message authentication.

III. PROPOSED SYSTEM

A new model for cooperative communication and message authentication on mobile ad hoc networks is proposed in this research paper. The two most important operations at the network layer are data forwarding and routing. Data forwarding regulates how packets are taken from one link and forwarded to another link. Hence routing determines the data packets to choose the right path to move from the source node to destination node. this proposed scheme also aims to make the node to participate in routing. To achieve this, the general guiding principles are applied such that it rewards the well behaving nodes and penalize the misbehaving nodes. The well behaving node is a node that correctly generates routing protocol control traffic and correctly relays routing protocol traffic on behalf of other nodes for smooth cooperation among the mobile nodes. The proposed mechanism for node cooperation and messaged authentication for mobile ad hoc networks is shown in Figure.1. This proposed system concentrates various process namely neighbourhood detection, cooperative node selection based on primary rating and secondary rating calculation, forwarding node selection, topology diffusion and message authentication. The functionality of this proposed architecture is explained in the following chapters.

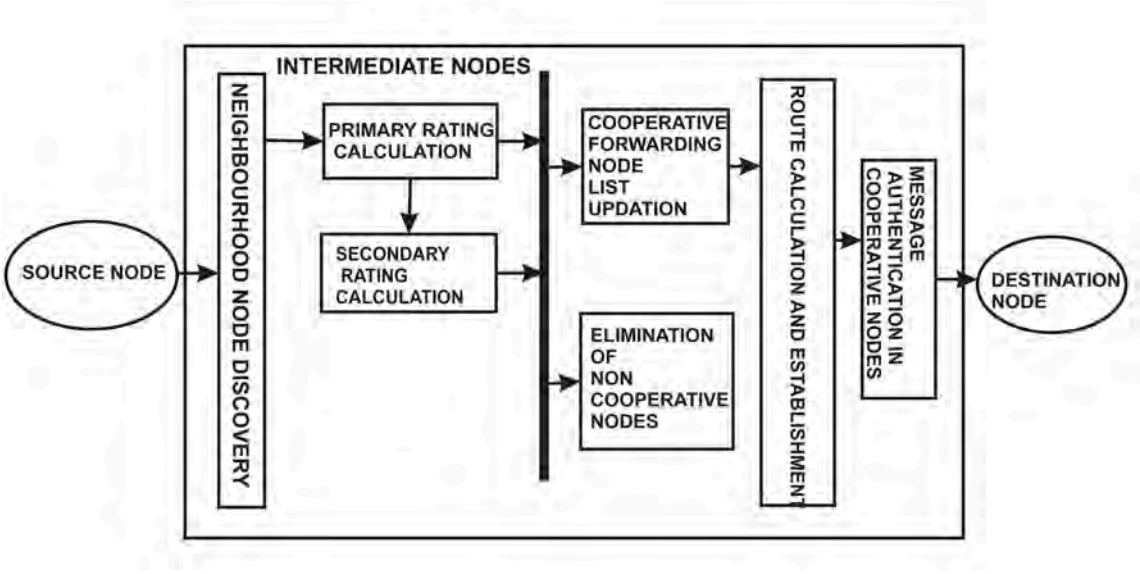

Fig. 1. System Architecture for Node Cooperation and Authentication

A. Neighbour Discovery

Each node finds out other nodes within the communication range in mobile ad hoc networks. A node will deliver the information through its neighbourhood node. The simple method for identifying the neighbour node in MANET is HELLO messages are broadcasted in a regular interval.

The symmetric nature of a link is determined by the publicity of neighbours from which a node has received a HELLO message in its own HELLO messages. The empty HELLO message is sent by node A. The node B receives this empty message and registers in it. But node B stores node A as an asymmetric neighbour and node B cannot finds its own address in this HELLO message. Node B sends a HELLO message to node A. Upon receiving this message by node A, it identifies its own address and also sets node B as symmetric neighbour. During the reception of HELLO message in node B, the Node A is register as a symmetric neighbour by node B. The HELLO messages are generated and it is transmitted to all one hop neighbour nodes and two-hop neighbour nodes for sensing links, neighbour nodes and MPR selectors. After transmitting this HELLO message to links and MPR nodes that the links and MPR nodes are grouped for the purpose of byte usage. The goal behind this method is mainly for link sensing in MANET and to identify if the mobile nodes are having non-main addresses. The typical neighbour discovery using HELLO messages is shown in figure.2.

The neighbour set of a node Nx that has Ns as a symmetric neighbour and Na as an asymmetric neighbour can be written down as a tuple of the asymmetric and the symmetric links: NSx=(Ax={Na},Sx={Ns}).The following expression represents the contents of a HELLO message from Nx:HELLOx=(Nx;Ax;Sx).

The operation of the HELLO messaging protocol between two nodes called N1 and N2 can then be explained as follows.

Step 1: Both N1 and N2 start out with empty neighbour sets: NS1= (Ø, Ø) and NS2= (Ø, Ø).

Step 2: N1 sends out a HELLO message which is received by N2. Since N1 does not know any neighbours, the neighbour list in the HELLO message is empty: (N1,Ø,Ø).

Step 3: n receiving this message N2 adds N1 to its neighbour set and marks the link to N1 as asymmetric. The Update neighbour set of N2 is then NS2=({N1},Ø).

Step 4: N2 broadcasts a hello message containing in the list of asymmetric neighbours (N2, {N1}, Ø).

Step 5: N1 receives the hello message and adds N2 to its neighbour set. Since N2 advertised an asymmetric link to N1, the latter realizes that N2 is receiving its HELLO messages. Thus it concludes that a symmetric link with N2 exists. This results is in the following neighbour set of N1 :(Ø, {N2}).

Step 6: N1 broadcasts a hello message and advertises N2 as a symmetric neighbour (N1, Ø, {N2}).

Step 7: On receiving this message N2 realizes that it has a symmetric link to N2: NS2 = (Ø, {N1}).

Step 8: Periodic broadcasting of the HELLO messages is used to keep the entry of the link between N1 and N2 alive, a link is only considered lost if its entry times out before another HELLO message was received.

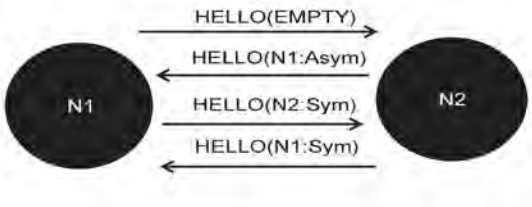

Fig. 2. Neighbour Node Discovery.

B. Cooperative Node Identification and Routing

In mobile ad hoc networks, each and every node contains the rating table which consists of neighbor node's behavior. In rating table each entry have a node ID, primary rating and secondary rating. the node ID in rating table which uniquely identifies each and individual node in MANETS. The secondary rating is which means packet delivery ratio of individual neighbor node based on the observation and its packet delivery ratio. The primary rating is a secondary rating based matured node classification. i.e., Node information is compared with critical path message information which enables the node to decide to identifying and handling the misbehaving nodes. The warning message is informed to neighbor nodes to establish the right routing path and eliminating the misbehaving nodes from the network.

Also in promiscuous mode of mobile ad hoc network, a node can have a capacity to overhear the transmissions of its neighbors. So the rating based packet delivery ratio is taken into the account of cooperative strategy among the mobile nodes. This kinds of rating categorization which helps to identify nodes as cooperative and as non-cooperative in the one hop and two hop neighbors. The Source Node is assigned as N and neighbor node is assigned as X. The Node N keeps the track of two numbers for each of its neighbors is as follows.

1) Request for forwarding Nodes (X) [RFN(X)] which represents the total number of packets transmitted from N to X for forwarding and

2) Has forwarded Node (X) [HFN(X)] which means the total number of packets that has been forwarded by node X and it is noticed by source node N.

Hence the secondary Rating of each neighbor node's packet delivery ratio is calculated as follows.

i.e., Packet Delivery Ratio = RFN (X) / HFN (X).

The basic concern about the cooperative secured communication using OLSR is assuring the nodes perfectly relay the messages and also provides traffic control. The detection of cooperative and non-cooperative nodes through OLSR is as follows. Each node are assumed as promiscuously to its multipoint relay transmissions during the direct observations based misbehavior node detection in networks. If the source node 'N' identifies that the MPR are not relay messages to its one hop neighbors, the source node 'N' decreases the MPR's secondary rating by α and its sends the misbehaving message about the MPR to all its one-hop neighbors and also consequently to its two hop neighbors. After reception of this message, each neighbor of '*N*' decrements the X's secondary rating by β, Otherwise, if the MPR is identified to relay the message, based on its secondary rating is increased by γ, Thus the misbehaving nodes are eliminated from the message transmission based on the source node 'N' observation about the decreased secondary rating MPR selectors. This leads the perfect classification among the mobile nodes as cooperative and misbehaving nodes in network to ensuring good reputation based message transmission in entire network.

C. Forwarding Node Selection

The forwarding node selection in cooperative communication is represented in figure3.in Object Link State Routing, the flooded information is used to calculate the next hop destinations and in this routing multipoint relay selection is to identify two hop neighbours to reach the desired destinations. i.e., The minimization of flooding can be achieved through Multipoint Relay (MPR) and disseminate its messages to network. The minimization of flooding leads reducing duplicate retransmissions of packets. The MPR is used for large and dense networks to optimize the message transmission in mobile ad hoc network. Each and every node selects a set of its neighbour. i..e., MPR node sets. These set of nodes are called the forwarding nodes of that node and they can change over periodically based upon the selector nodes in their HELLO messages. The forwarding node is chosen by the node and also it is inclusion of node list. The MPR set which consists of its neighbours and all two hop neighbours. The all two hop neighbours are having its bidirectional link to selected MPR.

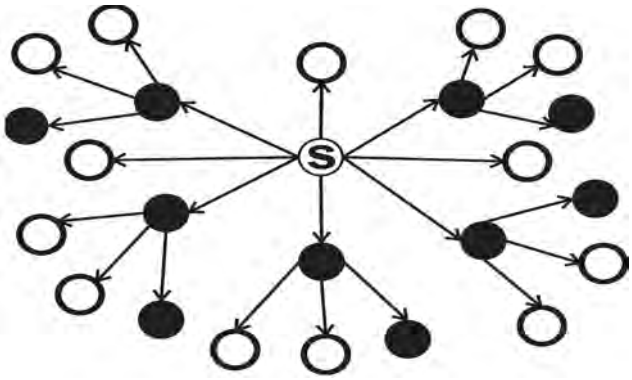

Fig. 3. Forwarding Node Selection

The selected MPR are acted as intermediate nodes in their traversal path, during each node broadcasts the control information. When the information are received by MPR selector each node justify and updates the desired route to each destination. The MPR selector nodes are the major role to multipoint relay in one hop and two hop neighbours through the MPR selector table for information dissemination in mobile ad hoc networks.

D. Topology Diffusion

The topology control can be achieved through the control of link status in mobile ad hoc networks. The cooperative level transmissions channel assignments (multi-hop and cooperative communications) may be the parameters of link status. To achieving cooperative transmissions the following transmissions are used i.e., direct transmission, multi-hop transmission and cooperative communications. In these above transmissions the direct transmissions having no relays and the multi-hop transmissions are not able to combine the signals at destination but the cooperative transmissions can combine the relay and source node signals to decode.

In cooperative transmissions, the selection of relay node can identify the network topology through the links. So the two neighbouring nodes can be functioning without any interruptions through this wireless links. While neighbouring links are divided into many hops that it leads duplication of packets in network and also decreases the capacity of entire network (14).

To achieve the best transmission among the cooperative communications the network topology control is essential for identifying neighbours by announcing the wireless links. In mobile networks, through identifying where and how deploys the wireless links that the NTC is providing good topology and topology diffusion. Figure 4. represents the topology control message diffusion of entire networks. This will optimize the entire networks and also resolve the issues in neighbouring node discovery in two hop and multi-hop communications. NTC messages diffusion provide sufficient information and enabling nodes to construct their own topology table for deduce neighbouring nodes in cooperative mobile ad hoc network.

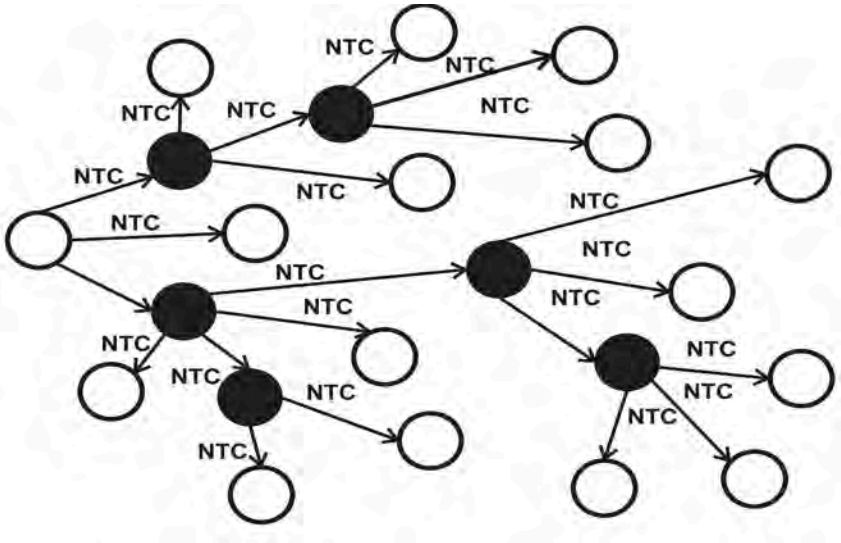

Fig. 4. Topology Diffusion

E. Authentication

To achieving the integrity verification for authenticating messages in each and every node the hash chains based signature verification mechanism and Merkle tree algorithm are proposed in this work.

A hash chain is a successive application of any cryptographic hash function H(x) by hashing a random seed variable x. It is recursively and sequentially calculated by hi = H(hi−1), where h1 = H(x). Thus, hi = Hi(x) in a hash chain of length i. The hash chain is usually applied in an opposite sequence since hi will not be revealed without hi−1. In the authentication protocol, the last element of the hash chain, that is the anchor hi, is initially provided by the owner to the verifier. The verifier can confirm the authenticity of the owner with hi−1 by subsequently hashing hi−1.

To independently authenticate each message, the message mj, the root r of the Merkle Tree, and a set of complementary branches {Bc} are required. Merkle Tree which represents message authentication is shown in figure 5. To authenticate m2, the sibling node of the nodes on the path from m2 to r should be included in {Bc}.

In this case, {Bc} = {b00}. The verifier recalculates r with {Bc} and mj . Message mj is authentic if and only if the recalculated value matches the root r. The functionality of the protocol initiates with handshake to exchange the anchors of hash chains. As represented in figure 5, the protocol includes a four-way packet exchange for each signed data message mj. The signer establishes a signature Merkle tree before the four-way exchange. Let Sig1, Auth1, Sig2, and Auth2 which denote the packets in the four-way exchange respectively.

The Sig1/Aug1 packet consists of the root of signature/acknowledgment of Merkle tree r and a fresh hash-chain element of the signer/verifier. The signer and verifier maintain their own signature and acknowledgment hash chains to identify themselves. .Message mj is disclosed in Sig2, along with a set of complementary branches {Bc}. On receiving Sig2, the verifier obtains messages mj and {Bc} and uses them to regenerate the Merkle tree root. Comparing this root with the received r in Sig1, message mj is authenticated, and its integrity is verified. An index xi and a secret si are contained in Auth2 to identify message mj.

In this, the set of complementary branches {Bc}, which logarithmically increases with the number of the signed data messages in a Merkle tree enables the verifier to independently authenticate each message. These functionalities are detailed in figure 6. The throughput and hash calculations are subject to based on the size of signed data blocks. Note that cooperative communication occupies two time slots in the transmissions. Each packet is attached with a signature hash chain to identify the sender. The first handshake exchanges the root r of the Merkle tree in Sig1/Auth1 packets. Messages and the corresponding complementary {Bc} are contained in Sig2 packets, whereas they are acknowledged by Auth2 packets. xi and si are used to identify the message.

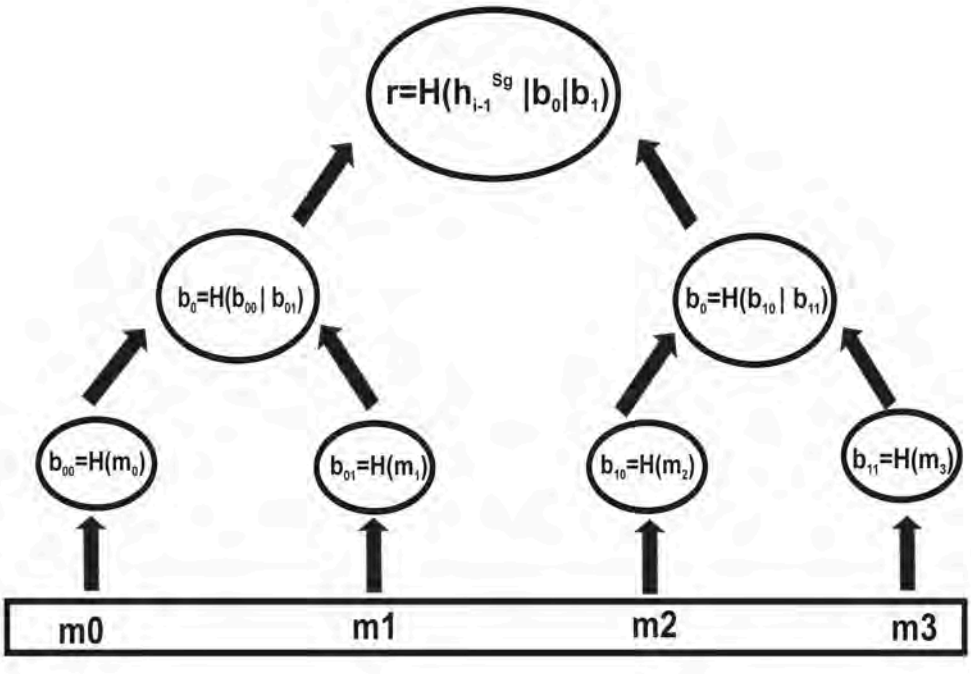

Fig. 5. Message Authentication using Merkle Tree

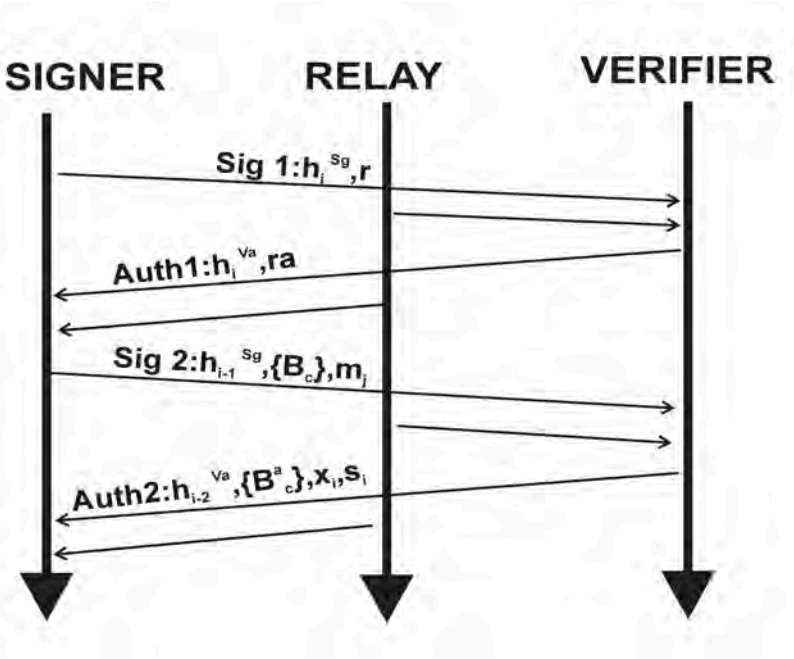

Fig. 6. Authentication for Cooperative Transmissions Model.

IV. SIMULATION RESULTS AND DISCUSSIONS

This proposed research work was implemented by NS2 Network Simulation Tool. The simulation was carried out with a field size of 1500m x 300m with 50 numbers of nodes. In this simulation, the nodes will move within the network space according to the random waypoint mobility model. In random waypoint mobility model and each node will moves to a random location within the specified network area. Once node arrives at the target location, it remains for a pause time before it is moving to another random location. The pause time will set to 0.5 second. The communication patterns will have Constant Bit Rate (CBR) connection with a data rate of 3 packets per second. 15 connections will establish at random. So each node would chance to connect to every other node.

The various parameters used in this simulation were shown the Table1. The performance of secured cooperative communication and message authentication simulated using Network Simulator NS2 and the experiments are carried out for the proposed scheme and the resultant values are compared with the existing systems. The obtained values are plotted as line and bar chart graphs for representing performance comparative analysis. These are detailed below.

The comparison of packet dropping ratio between the proposed and existing relative protocols was made through the network simulations. Figure 7 which prove that the proposed scheme to be more cooperative and minimization of the packet loss was achieved in the networks.

TABLE I. SIMULATION PARAMETER

Parameter	Value
Antenna	Omi antenna
MAC Protocol	802.11
Mobility Model	Random waypoint
Topology Area	1500mm×300mm
Number of Nodes	50
Transmission Range	250m
Packet Size	256b
Traffic Type	CBR
Simulation Duration	300s

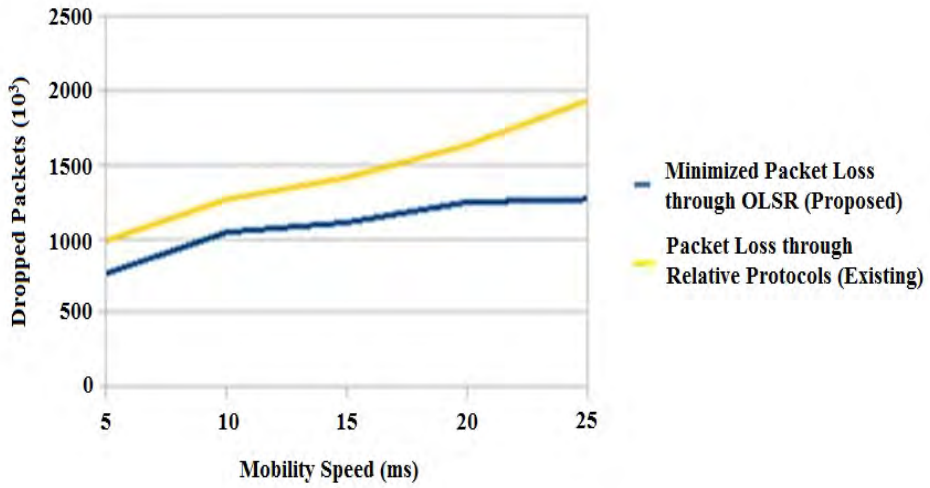

Fig. 7. Comparison of Node Mobility with Packet Dropping Ratio among Existing Relative Protocols and OLSR.

The performance analysis between node's mobility with packet delivery ratio of OLSR and existing relative protocols is shown in figure 8. i.e., the trust is achieved through higher PDR ratio and the relay nodes are identified their neighbour nodes. The proper routes are calculated and established based on the rewarding the mobile nodes in a network. The maximum throughput is achieved using OLSR and it leads cooperative transmission by elimination of node's lower rating ratio and the reputation among the network is also achieved.

The bar chart comparative analysis between delay and node mobility among OLSR, AODV and relative protocols is also shown in figure 9. It also ensuring the identification of malicious nodes in network, and also used to allow the message transmission through the proper cooperative nodes without any duplication of retransmission of packets. The Throughput analysis between the OLSR, AODV and existing relative protocols which ensures the good reputation, cooperation in message transmission is represented in figure 10. The misbehaving nodes are identified and neglected in time and route calculations, route establishments are achieved properly for secured cooperative communications in MANETs.

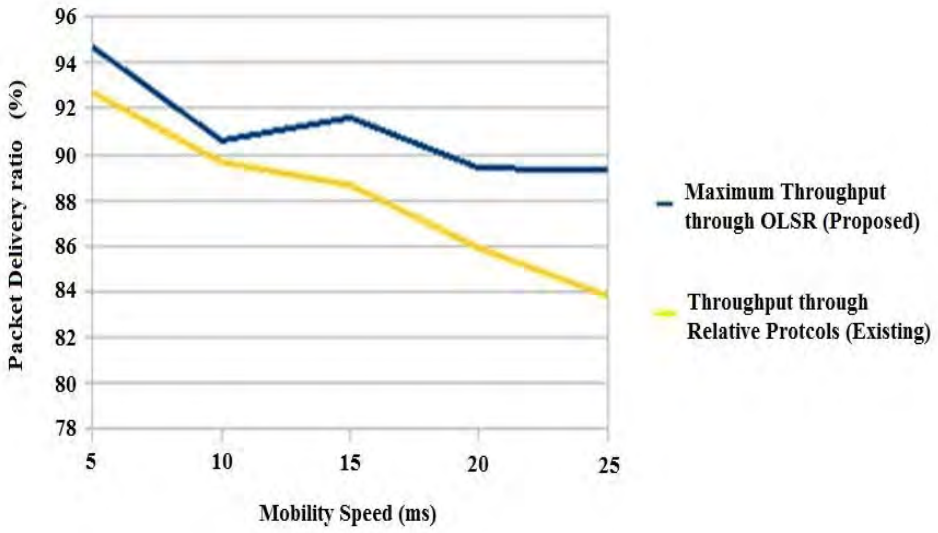

Fig. 8. Comparison between Node Mobility with Packet Delivery Ratio among Relative Protocols and OLSR

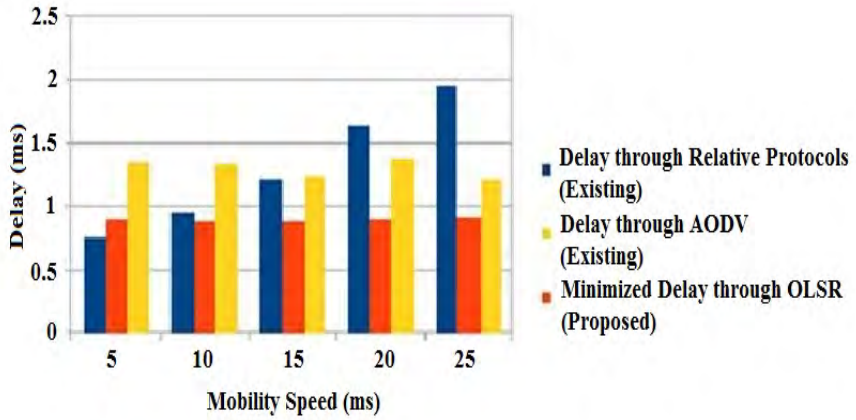

Fig. 9. Delay Comparison between Existing Relative Protocols and OLSR.

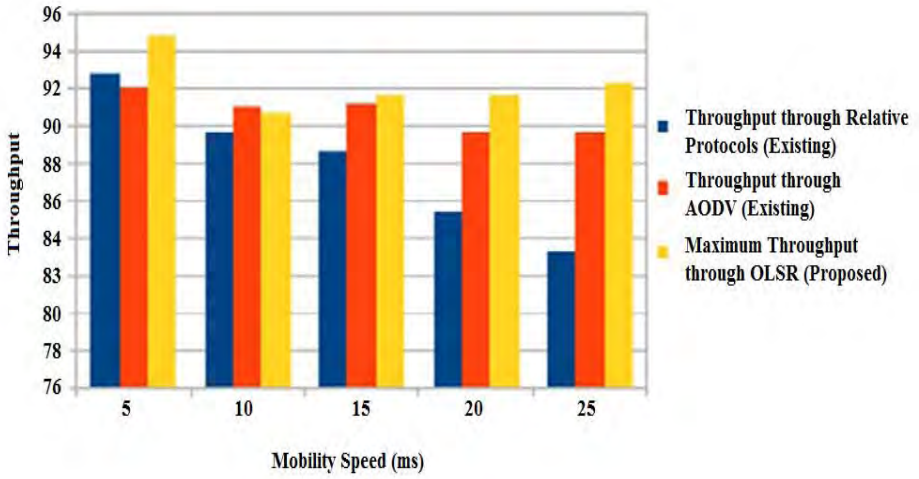

Fig. 10. Comparison of Throughput between Existing Relative Protocols and OLSR**.**

V. CONCLUSION FUTURE WORK

In this paper, the node cooperation and message authentication for trusted mobile ad hoc network are discussed in detail. The simulation work was carried out using NS2 network simulator and results were obtained for large scale network. This system mainly concentrates the node cooperation and message authentication for MANETs using OLSR protocol. The node reputation is calculated through its relay capacity by means of primary rating and secondary rating. The non-cooperative and misbehaving nodes are identified by the proper threshold value and trusted secured message transmissions are successfully simulated. The node cooperation and reputation in packet delivery is achieved in the specified network. In our future work that we are planning to ensure the message authentication based security using combination of Merkle tree signatures and hash chain to achieve more reputation in very large scale cooperative mobile ad hoc networks.

REFERENCES

[1] X.Bangnan, S.Hischke, B.Walke, "The Role of Ad hoc Networking in Future Wireless Communications", *International Conference on Communication Technology (ICCT)*, Volume.2, Pages: 1353-1358, 2003 .

[2] L. Bla_zevic', L. Buttyán, S. _Capkun, S. Giordano, J.-P. Hubaux, J.-Y. Le Boudec, Self-Organization in Mobile Ad hoc Networks: The Approach of Terminodes,*IEEE Communication Magazine 39*,pp - 166_174,2001.

[3] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes - Fairness in Dynamic Ad-hoc Networks," *Proceedings of MobiHoc*,2002.

[4] L. Buttyan, J. P. Hubaux, "Stimulating Cooperation in Self Organizing Mobile Ad hoc Networks", in *CM/Kluwer Mobile Networks and Applications (MONET)*, Volume.8, No. 5,2003.

[5] J.Crocraft, R.Gibbens,F.Kelly,S.Östring, " Modeling Incentives for Collaboration in Mobile Ad hoc Networks Performance Evaluation", pp 427_439. 2004.

[6] Q. He, D. Wu, and P.Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks," *Proceedings of WCNC 2004*, Atlanta, GA, 2004.

[7] S.Marti, T.J Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proceedings of MobiCom 2000*, Boston, MA, 2000.
[8] N.Meganathan et al "A Distributed Trust and Reputation Framework for Mobile Ad hoc Networks", *Springer CNSA*, 2010
[9] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Comm. and Multimedia Security Conf*, 2002.
[10] Quanshang Ghan, F.Richard Yu, Shengming Jinang, Victor C.M. Laung, Hamid Mehrvar, "Topology Control in Mobile Ad hoc Network with Cooperative Communications", *IEEE Wireless Communications*, pp-74 _79, 2012.
[11] B.Raghavan, A.C. Snoeren, "Priority Forwarding in Ad hoc Networks with Self Interested Parties", *in: Proc. 1st Workshop on Economics of Peer-to-Peer Networks*, Berkeley, CA, 2003
[12] S. Zhong, J. Chen, Y. R Yang, Sprite: A Simple, Cheat Proof Credit based System for Mobile Ad hoc Networks, in *Proc. IEEE INOCOM,2003*, San Francisco, CA, United States, pp. 1987_1997, 2003.
[13] Ze Li, Haiying Shen, "Game Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad hoc Networks", *IEEE on Transactions Mobile Computing*,Volume 11, No.8, 2012.
[14] Q.Guan,S.Jiang,Q-L Ding, and G.Weig, "Impact of Topology Control on Capacity of Wireless ad hoc Networks", in *Proc.* IEEE ICCS GuangZhou,China, pp.588-592, Nov.2008.
[15] A.Nosrattina, T.Hunter, and A.hedavat, "Cooperative Communication in Wireless Networks", IEEE Comm.., Mag., vol.42, No.10, pp.74-80, Oct.2004.