Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 8 (2013) pp. 017-032

Trusted M-OLSR for Secure Routing in Wireless Mesh Networks

Amrita Bose Paul[1], Shantanu Konwar[2], Sukumar Nandi[1] and Santosh Biswas[1]

[1]Dept. of Computer Science and Engineering
IIT Guwahati, India
(a.paul,sukumar,santosh_biswas)@iitg.ernet.in

[2]Department of Computer Applications
AEC, Guwahati, India
shantanu.220984@gmail.com

Abstract: **Wireless Mesh Networks (WMNs) do not rely on any centralized administration and they are built by the connection of various static and mobile entities (i.e. nodes). The cooperation and coordination between these network entities are essential to establish a secure routing path. Presence of malicious or misbehaving nodes within a routing path may disrupt the network activities either by dropping or spoofing data packets. To ensure a secure route discovery and its maintenance, it is necessary to compute trustworthiness of individual nodes in a cooperative manner for discovering neighbors, selecting routers and announcing topology information in WMNs. In order to detect trustworthy nodes in the networks, we propose a model based on Multiple Criteria Decision Making (MCDM) which quantifies node behaviors into discrete quantities. The proposed scheme ensures detection of malicious and misbehaving nodes in the network. This proposed trust building process is then integrated with Modified Optimized Link State Routing (M-OLSR) for secure route calculation in WMNs. The newly developed protocol named as Trusted M-OLSR (TM-OLSR) allows only trusted and stable nodes to participate in route establishment and enhance security features of the corresponding protocol. To evaluate TM-OLSR's performance and suitability in WMNs, a comparison of the proposed protocol with M-OLSR is carried out using NS-2 simulator.**

Keywords: Wirelsess Mesh Network and Trust Model and OLSR

I. Introduction

The concept of Wireless Mesh Networks (WMNs) has evolved recently and several research groups are working on its various aspects [1]. By definition, WMNs is a multi-hop wireless access networks having a reliable static backbone where nodes can communicate forwarding each others packets. It is a type of radio based network systems which is self-organizing, self-configuring and requires minimal upfront investment in deployment [1]. WMNs has the capability to integrate into wired networks and can be easily extended at low cost without losing the mobility or flexibility provided by Mobile Ad-hoc Networks (MANETs). The unique characteristic of wireless mesh network is its fixed, and non-energy constrained wireless backbone, for which the topology does not have to cope with access point mobility. In WMNs, traffic flows from mobile clients to gateway nodes via static routers and vice-versa. The multi-hop wireless nature of WMNs needs special attention and demands a different approach for routing packets in the networks. However, though some progress have been made in routing and link layer protocols in WMNs, security issues are still in its infancy as very little attention has been devoted till date to this topic by the research community [1].

WMNs do not rely on any centralized administration and they are built by the connection of various static and mobile nodes. The cooperation and coordination between these nodes are very essential to establish a routing path [2]. The important factors influencing WMNs performance is the nature of underlying routing protocol used for data communication [3]. Since routing is one of the most important network services in data communications, it is one of the prime targets of the attackers. Presence of malicious or misbehaving nodes within the routing path may disrupt the network activities either by dropping or spoofing data packets. It is essential to design a routing protocol that associates misbehavior detection scheme (i.e., detection of malicious and compromised nodes) for secure route calculation in WMNs. Since WMNs rely on participation and cooperation of nodes within the network during the routing process, trusted routing is beneficial for discovering neighbors, selecting routers and announcing topology information for secure route discovery and its maintenance [4]. Hence, a cooperative mechanism is

required to built trust among the nodes to classify them as trustworthy (honest) / untrustworthy (selfish). This mechanism is to be integrated to a routing protocol for a reliable and secure route calculation in WMNs scenarios.

There is a traditional way of securing routing protocols by transmitting authenticated routing messages among the wireless network entities. However, this approach is insufficient as the key characteristics of WMNs make it possible for attackers, including malicious users, to add routers, establish links, and advertise routes. In addition, an attacker could steal the credentials of a legitimate user or a legitimate user could himself turn malicious, and thereby inject authenticated but incorrect routing information into the network. There are few research approaches on secure routing in WMNs and they are based on cryptographic computations. Most of them are adopted from existing solutions available for Mobile Ad-hoc Networks (MANETs). One such protocol called Ariande [5] is a secure on-demand source routing based on authentication of source node. Another such protocol SAODV [6] is a secure variant of AODV which uses cryptographic extensions to provide authenticity and integrity of routing messages. It uses hash chains in order to prevent manipulation of hop count field. The work in [7] presents a trusted routing named Trusted Computing Ad hoc On-demand Distance Vector (TCAODV), which extends the traditional Ad hoc On-demand Distance Vector (AODV) [8] routing protocol to ensure that only trustworthy nodes participate in route calculation and prevents selfish or malicious nodes from participating in the network. In TCAODV [7], a public key certificate as well as a per-route symmetric encryption key is established to ensure that only trusted nodes along the path can use the route. All these existing solutions imply a reduction of performance due to all additional cryptographic computations. Since, routing process in WMNs rely on participation and cooperation of nodes within the network, therefore, it is necessary to built a trust relationship between each pair of communicating nodes as well as between all nodes on the multiple routing paths in WMNs.

Therefore, it is essential to design a routing protocol that associates misbehavior detection scheme (i.e., detection of malicious and compromised nodes) for secure route calculation in WMNs with minimal computational overhead. The objective of this paper is to integrate the proposed trust building process as reported in [9] to M-OLSR [10], which has been developed for adaptability in WMNs. M-OLSR adaptively support static mesh routers and mobile mesh clients for communications. Simulation results of M-OLSR [11] demonstrates and established it as a suitable routing protocol with improved throughput, packet delivery ratio (PDR), and normalized routing overhead (NRO). This proposed integration will allow a self organized control to help the routing protocol for detecting misbehaving and malicious nodes while calculating secure and stable routing path for communication in WMNs. This trust based routing protocol named as Trusted Modified Optimized Link State Routing (TM-OLSR) allows only trusted and stable nodes to participate in route establishment and hence enhance security features and improve network performance because honest nodes can avoid working with less trustworthy nodes.

Trusted Modified Optimized Link State Routing (TM-OLSR) is a variant of M-OLSR (Modified Optimized Link State Routing) protocol, which has been developed for secure routing in WMNs scenarios. In TM-OLSR, each node detects its trusted static neighbor nodes through periodic exchange of HELLO messages. A HELLO message contains the emitting nodes own address, information about its neighbor, neighbor node type, neighbor trust value, trust status, link status, and willingness to carry traffic in the network. The trust value is maintained in the trust table of each individual node which is calculated through our proposed trust building model. So, during route calculation in TM-OLSR, paths that comprise trusted static routers are considered. To evaluate TM-OLSR's performance and suitability in WMNs due to its added security features, we compare the proposed protocol with M-OLSR [10], in terms of throughput, packet delivery ratio, normalized routing overhead and packet end-to-end delay.

In our proposed model of trust calculation, as reported in [9], trust is interpreted as a level of uncertainty as described in [12]. In the reported work [9], the Multiple Criteria Decision Making (MCDM) technique called TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) [13] [14] [15] is used for quantification of trust relationship. In the proposed model, each individual node effectively assigns a trust called individual trust to each of its neighboring nodes depending on node behavior. Again, depending on these assignments, each node selects its neighbors whose trust value is greater than a particular threshold value and subsequently advertises those trustworthy nodes in the network with their respective trust values. From these broadcasted trust information, recommended trust for neighboring nodes are calculated. Combination of both individual trust and recommendation trust give actual trust value. Trust value thus calculated is a continuous real number lying in the closed interval [-1,1]. Nodes with trust value above zero are considered as trustworthy and are included in the routing process whereas nodes having trust value lower than zero are recognized as misbehaving or malicious nodes and are excluded from routing. The proposed trust model is developed using C++ programming.

The rest of the paper is organized as follows. Section II provides a brief summary of different available approaches for trust calculation in MANETs, Wireless Sensor Networks (WSNs) as well as in WMNs. Section III gives a brief overview of M-OLSR [10] protocol for WMNs. For completeness of the work, we include our

trust evaluation model as reported in [9] in Section IV. Our proposed secure routing protocol called TM-OLSR is described in Section V. Performance evaluation of TM-OLSR is detailed and analyzed in section VI. Finally Section VII concludes the paper.

II. Related Work

Trust based routing approach available in MANETs , WSNs, and WMNs are reported here.

George et al. [16] interpreted trust as a relation among entities that participate in various protocols. They evaluated trust evidence in Ad-hoc networks without considering pre-established infrastructure. Using the concept of directed graphs, they distinguished entities as nodes and trust relation between nodes as edges to model the trust evaluation process. Again they emphasized on design issues related to trust evaluation algorithms and provided intuitive requirements for it. Applying theory of semirings they showed that two nodes having no previous direct interaction are able to establish indirect trust.

Huanzhao et al. [17] designed a trust routing protocol framework in WSNs. They analyzed the security framework theoretically for assessment of involved cost in their model. Validation of framework was done by various routing protocols and provided experimental evidence to defend various attacks in WSNs.

Yanli Yu et al. [18] proposed a service trust model, based on the subjective trust model. In their design they involve passive trust of objects and combine direct trust and recommended trust. They also presented passive trust feedback method which avoids forbids malicious nodes' deception. Extensive simulation experiments are provided to prove the feasibility and rationality of their trust model.

RLM, a general trust model designed by Xiaofeng Wang et al. [19] provides a comprehensive and robust reputation evaluation. Reputation value evaluation on the basis of aggregation of feedbacks provides quality measurements for reputation prediction variance. They proposed Kalman aggregation method for feedback aggregation. Also to mitigate malicious feedback aggregation, they designed Expectation Maximization algorithm. They provided a theoretical analysis for demonstrating the robustness of their RLM model.

Yan Lindsay Sun et al. [12] presented an information theoretic framework for quantitative trust measurement. They modeled trust propagation in ad hoc networks. According to them trust is a measurement of uncertainty with its value represented as entropy. For basic understanding of trust and propagation of trust they developed four axioms. On the basis of these axioms they presented two trust models: entropy-based model and probability based model. For secure as hoc routing and malicious node detection they employed the proposed trust evaluation method and trust models in ad hoc networks. Furthermore, simulation results show that their trust evaluation system can significantly improve network throughput as well as effectively detect malicious behaviors in ad hoc networks.

Although a variety of trust models have been proposed and developed by research community for ad hoc and sensor networks, but to the best of our knowledge, these schemes have not yet been extended for WMNs. The architectures and routing nature of WMNs are different from that of ad hoc and sensor networks. WMNs follows multihop as well as multipath routing where multiple alternative routers route the traffic between the source destination pair. Unlike peer-to-peer communications, client-gateway pair act as a source destination pair in WMNs. Therefore, the methods used for quantification of node behavior in ad hoc and sensor networks are not applicable for WMNs.

A trust measurement scheme for WMNs has been reported in [9]. The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [13] [14] [15] approach is being used for quantification of trust relationship. The scheme only derives the trust for each individual nodes that is maintained by each node, but no implementation and evaluation is carried out to test its effectiveness . In order to evaluate, we require to integrate the trust model to a protocol. In this paper, an extension of that work is reported which considers a mesh routing protocol called M-OLSR [10] and integrate the proposed trust measurement scheme as reported in [9] for secure route calculation in WMNs. The proposed integration facilitates a self organized control to help the routing protocol for detecting misbehaving and malicious nodes in WMNs. The newly developed routing protocol termed as Trusted M-OLSR allows only trusted and stable nodes to participate in route establishment and hence enhance security features of the corresponding protocol.

III. M-OLSR for WMNs

Modified Optimized Link State Routing (M-OLSR) [10] is a variant of OLSR (Optimized Link State Routing) [20] protocol, and has been developed for adaptability in wireless mesh networking (WMNs) scenarios [10]. Conceptually, OLSR [20] is an optimized version of a pure link state protocol developed by IETF group for MANETs and uses the concepts of Multipoint Relays (MPR) [21]. MPRs are selected nodes that cover all two hop neighbors and reduce flooding of broadcast packets by shrinking the number of nodes that retransmit the packets. OLSR contains three elements: i) Neighbor Sensing mechanisms for neighbor detection through periodic exchange of HELLO messages. ii) Generic Message Flooding for an efficient flooding of control traffic into the network employing the concept of MPRs for a significant reduction of duplicate retransmissions during the flooding process. iii) Topology Control Message Diffusion for providing each node with sufficient topological information so that each

node is able to compute an optimal route to each destination in the network using any shortest-path algorithm. In traditional OLSR for WMNs [20], a route is constructed only through selected MPRs which consider mobile clients and as well as static routers. In the protocol, there are no provisions for considering only static routers to be selected as MPRs. A detailed study of OLSR [20] for WMNs revealed the fact that, performance degrades with increase in traffic load as well as increase in number of mobile clients. The reason for this degradation is due to presence of mobile clients in route calculation process, while in WMNs, clients can not be a relay node. So, chances of packet drops increases because of non availability of routes. Based on these observations, the authors in [10], proposed a modification to the original OLSR protocol for its adaptability in WMNs and named it as M-OLSR. In M-OLSR, each node detects its static neighbor nodes through periodic exchange of HELLO messages. A HELLO message contains the emitting nodes own address, information about its neighbor, neighbor node type, their link status, and willingness to carry traffic in the network. The willingness of all static router and gateway nodes are set to WILL ALWAYS and specifies that these nodes can be selected for carrying traffic on behalf of other nodes and selected as MPRs, whereas all mobile clients have their willingness field set to WILL DEFAULT or WILL NEVER. The first modification is introduction of a new field called Node Type which is added in HELLO message to generate information about gateway, router and client nodes. Whereas in traditional OLSR, all nodes have same characteristics and capabilities and Willingness set to WILL DEFAULT. The HELLO message is transmitted in broadcast mode once per refreshing period of the protocol to all one-hop neighbors but not relayed further. The outcome of HELLO exchange is neighbor table for each node in M-OLSR. This table records information about its one hop neighbors, link status with these neighbors, neighbor type, and a list of two-hop neighbors. Such information has an associated holding time, and will be refreshed periodically to remain valid. Two new Selector Sets, called Gateway Selector Set and Router Selector Set are created along with the modifications in neighbor set, and 2-hop neighbor set of traditional OLSR. Using these modified data structure, M-OLSR protocol generates its routing table. The M-OLSR takes advantage of static router backbone of WMNs to calculate a more stable and optimal route with minimum hop count. Simulation results demonstrate and establish M-OLSR as a suitable routing protocol for WMNs with improved throughput, packet delivery ratio (PDR) and normalized routing overhead (NRO) in a dense and dynamic networks [11]. It is loop-free, simple, and robust in nature and provides instant availability of route whenever required. Though M-OLSR calculates a static route for packet forwarding, but the security issues were not considered which is very essential in WMNs.

IV. Modeling Trust in Wireless Mesh Networks

Trust has no clear definition but many described it as reputation, opinion, probability or uncertainty [12] [22]. In the proposed scheme of trust evaluation [9], trust is considered as a measure of uncertainty as defined by Yan Lindsay Sun et al. [12] and the Multiple Criteria Decision Making (MCDM) technique called TOPSIS [13][14][15] for trust derivation. This section describes the definition of trust and its four axioms that are used for establishment of trust relationship in [12] and the technique called TOPSIS [13][14][15] which is used for trust evaluation.

A. Understanding Trust

Trust can be described as a relationship established between two entities (i.e. nodes) for a specific action. In particular one entity trust the other entity to perform an action. Here, the first entity is referred as subject and the second entity is called an agent and both of them are neighbors to each other. Four axioms developed by Yan Lindsay Sun et al. [12] for defining trust relationship are listed below. These axioms are considered for trust calculation in the proposed model.

Axiom 1: *Uncertainty is a measure of trust.* From a subjects point of view certainty of performing of an action by an agent can be described as a trust. Trust value between these two entities is given by T(*subject : agent, action*) and is defined as

$$T\{subject : agent, action\} = \begin{cases} 1 - H(p), & for\ 0.5 \leq p < 1 \\ H(p) - 1, & for\ 0 \leq p < 0.5 \end{cases} \quad (1)$$

where $H(p) = -plog_2(p) - (1-p)log_2(1-p)$ and p = P(*subject : agent, action*). Here subject is the entity assigning trust and agent is the entity whose trustworthiness of doing an action is assigned. P(*subject : agent, action*) denotes the probability that agent will perform an action in the subject's point of view. When $p = 1$, subject trust the agent most and the trust value is 1. When $p = 0$, the subject distrust the agent most and the trust value is -1. When $p = 0.5$, the subject has no trust for the agent and the trust value is 0. Trust value is an increasing function with p.

Axiom 2:*Concatenation Propagation of Trust Does Not Increase Trust.* It states that when a subject establishes a trust relationship with an agent through recommendation, the trust value between subject and agent should not be more than the trust value between the subject and the recommender as well as the trust value between the recommender and the agent. Say, A, B, C are three different entities, where A is the subject, B is the recommender, and C is the agent. Let us consider A has trust relationship with B which is represented as T_{AB} and B's recommendation for C to A is represented as R_{BC}. Then if A wants to establish trust relation with C through recommendation then according to axiom 2,

its mathematical representation is as given below:

$$T_{AC} \leq min\left(T_{AB}, R_{BC}\right) \tag{2}$$

Axiom 3: *Multipath Propagation of Trust Does Not Reduce Trust.* It states that if a subject receives the same recommendations for the agents from multiple sources, the trust value should be no less than in the case where the subject receives less number of recommendations.

Axiom 4: *Trust Based on Multiple Recommendations from a Single Source Should Not Be Higher Than That From Independent Sources.* It is possible to have multiple recommendations from a single sources if the trust relationship is established jointly through concatenation and multipath trust propagation. Since the recommendation from a single source are highly correlated, the trust built on these correlated recommendations should not be higher than the trust built upon recommendations from independent sources.

B. Technique for Ordered Priority with Similarity to Ideal Solution (TOPSIS)

A variety of multiple criteria decision making (MCDM) techniques are available which help in ranking alternatives with respect to the different attributes and selection of the best alternative. TOPSIS is abbreviated for Technique for Order Preference by Similarity to the Ideal Solution. TOPSIS was developed by Hwang and Yoon [13], based on the concept that the chosen alternative should have the shortest distance from the positive ideal solution (PIS) and the farthest from the negative ideal solution (NIS) for solving a multiple criteria decision making problem. Briefly, the PIS is made up of all best values attainable for a criteria, whereas the NIS is composed of all worst values attainable for a criteria. The TOPSIS method involves following seven different steps for selection of best alternative among all available alternatives depending upon multiple criteria. The variations required to fit this model in the proposed trust building process is also described.

1. Construction of the decision matrix: The decision matrix is the relational matrix between the attributes and the alternatives.

2. Construction of the normalized decision matrix: The normalized value in the normalized decision matrix can be any transformation of the column of the decision matrix with the value being in between 0 and 1.

3. Assignment of weights to the criteria: Assign a weight vector w_j to each criterion. The weight to criteria can be obtained from various techniques, e.g., analytic hierarchy process [14]. In our work we considered each of the criteria having similar priority, so assigned weights are equal for each of the criteria.

4. Construction of the weighted normalized decision matrix: Each column of the normalized decision matrix is multiplied by its associated weight and a new matrix is obtained, the new matrix thus formed is called the weighted normalized decision matrix.

5. Determination of the ideal and non-ideal solution: The ideal (A*) and the non-ideal A^- solutions are defined as follows:

   $A^* = (v_0^*, ..., v_m^*)$,where

   $$v_j^* = \left\{max\left(v_{ij}\right),\ if\ j > J;\ min\left(v_{ij}\right),\ if\ j < J^{'}\right\} \tag{3}$$

   $A^- = \left(v_0^{'}, ..., v_m^{'}\right)$,where

   $$v_j^{'} = \left\{min\left(v_{ij}\right),\ if\ j > J;\ max\left(v_{ij}\right),\ if\ j < J^{'}\right\} \tag{4}$$

6. Calculation of the separation measures for each alternative: The separation from the ideal alternative is:

   $$S_i^* = \left[\left(v_j^* - v_{ij}\right)^2\right]^{1/2},\ where\ i = 1, ..., m \tag{5}$$

   Similarly, the separation from the negative ideal alternative is:

   $$S_i^- = \left[\left(v_j^{'} - v_{ij}\right)^2\right]^{1/2},\ where\ i = 1, ..., m \tag{6}$$

7. Calculation of the relative closeness to the ideal solution is:

   $$C_i^* = \frac{S_i^-}{\left(S_i^* + S_i^-\right)} \tag{7}$$

C. Assigning Trust in WMNs Nodes

To design a trust model among the WMNs entities (i.e., nodes), it is essential to specify the criteria for trust evaluation. Based on these criteria and interaction between nodes, a behavioral relationship is established among the network entities. This behavioral relationship is then transformed into discrete quantity. This transformation process is known as the quantification of trust relationship. In WMNs, there exists multiple alternative routes between a client-gateway pair. Therefore, the process of trust quantification in WMNs can be compared to a multiple criteria decision making (MCDM) problem where the objective of the technique is to select best source-destination path among the available choices depending on some criteria. They are *i*) probability (*p*) that an agent will perform a particular action, *ii*) number of packets to be forwarded on behalf of a Subject, *iii*) number of packets successfully forwarded by the agent, and *iv*) Delivery Ratio Efficiency (DRE). The proposed trust building process as

appeared in [9] assign trust to each individual nodes in WMNs. The steps required to calculate and assign trust to each node are detailed below. The proposed framework considers the following assumptions.

D. Assumptions

- Heterogeneity of nodes is being considered for WMNs.
- Every node in the network authenticates each other before any interactions.

E. Trust Model

- Defining Action: Packet Forwarding and Recommendation Exchange are considered as actions depending upon which the trust relationship will be established.
- Trust values are considered to be of two different types as described:
  - *Individual Trust:* It is the value which is assigned by the subject depending upon the behavioral activity of the agent. This value is specifically allotted depending upon the performance of an agent on a particular task that a subject assigns it. This value is independent from the influence of any third party.
  - *Recommended Trust:* This value is provided by a third party (recommender) who trusts or distrusts an agent. The subject considers this value and builds up a recommended trust value of an agent. This process of trust building is governed by the axioms as described in [12].

  The above mentioned two trust values are taken into account while computing the total trust value of a particular agent.

$$T_x = T_{Individual} + T_{Recommended} \quad (8)$$

Considering the above factors the trust building system is divided into two disjoint sub-systems. They are Individual Trust Building System and Recommended Trust Building System. A Subject (initially a client and subsequently intermediate routers in WMNs) uses combination of these two sub-systems to derive the trust of each nodes which is depicted in Fig. 1 and its each component is described below.

- **Behavior Monitor:** This component collects the information about the agents (i.e. neighbor nodes). These information are precisely the facts which are related with subject and agent relationship (i.e., action). The four criteria that are being considered for deriving individual trust are:

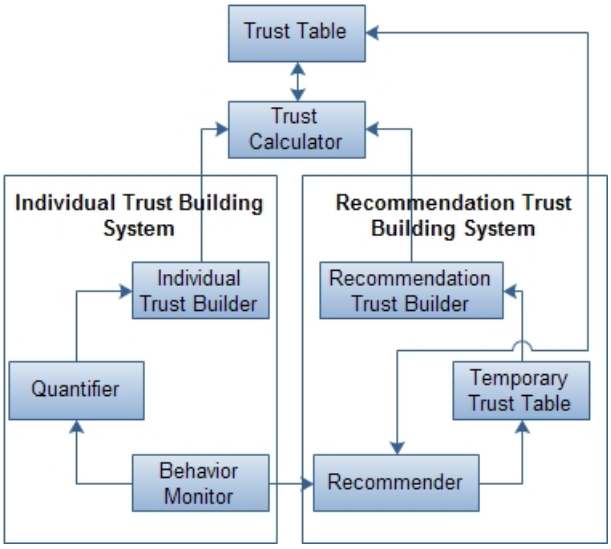

Figure. 1: Trust Derivation System

1. Probability (p) that an agent will perform a particular action. This value is calculated from equation 1. T and p have one to one relation.
2. Number of packets to forward on behalf of a Subject.
3. Number of packets successfully forwarded by the agent.
4. Delivery Ratio Efficiency (DRE).

A default trust value is assigned to every agent when they are going to start working for the subject for the first time. So, it is assigned a value which signifies that the node neither trusts nor distrusts the agent. So maximum uncertainty is observed when such condition arises.

$$T_x(a_i) = 0, \ where \ a_i = Set \ of \ 1 \ and \ 2 \ Hop \ Neighbors. \quad (9)$$

- **Quantifier:** It actually works with Behavior Monitor. This helps in quantifying the observation into discrete value. Say, an agent performs k number of events either successfully or unsuccessfully out of n trials. Then its DRE is calculated with the following formula:

$$DRE = \frac{k+1}{n+2} \quad (10)$$

where k = no. of packets delivered successfully and n = no. of packets required to deliver.

- **Individual Trust Builder:** This component is MCDM machine residing in every subject which actually uses the information provided by the *Quantifier* to calculate the individual trust of an agent. The MCDM machine is explained with the help of control flow charts depicted in Fig 2 and its different phases are subsequently elaborated

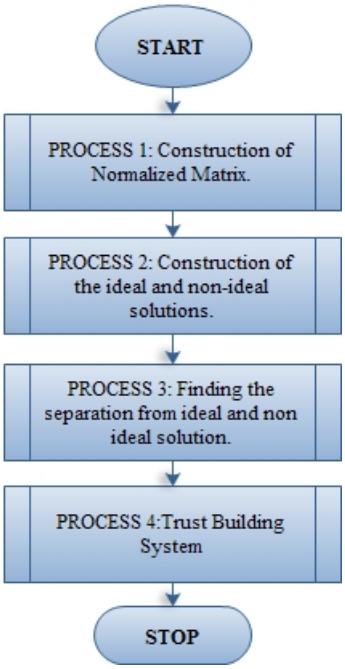

Figure. 2: MCDM Machine

in Algorithm 1, Algorithm 2, Algorithm 3, and Algorithm 4 respectively.

It is to be noted although the technique of TOPSIS is used in the proposed MCDM machine, but the first two steps of TOPSIS [13] are not present in the proposed MCDM machine as depicted in Fig 2, for these two steps are assigned to the *Quantifier*.

Algorithm 1: Normalized Matrix Construction

1. $j \leftarrow 0$ (Initializing counter to 0).
2. If $j <$ No. of Criteria
   (a) $i \leftarrow 0$
   (b) If $i <$ No. of Alternatives
   Input for each node w.r.t. criteria a[i][j]
   $i++$, Goto Step (a)
   (c) Else
   $j++$, Goto Step 2
3. Else
   (a) $x[j] \leftarrow$ Column wise square root of the sum of square of the scores
   (b) $j \leftarrow 0$
   (c) If $j <$ No. of Criteria
   i. $i \leftarrow 0$
   ii. If $i <$ No. of Alternatives
   a[i][j] $\leftarrow$ a[i][j] $\div$ x[j]
   $i++$, Goto Step (ii)
   iii. Else
   $j++$, Goto Step (c)
   (d) Else End

Algorithm 2: Construction of Ideal and Negative-Ideal Solutions

1. $i,j \leftarrow 0$ (Initialize Counters)
2. If $j <$ No. of Criteria
   (a) pos_ideal[j]$\leftarrow$Max(a[i][j]) and neg_ideal[j]$\leftarrow$Min(a[i][j]) where $0<i<$Number of Alternatives (nodes)
   (b) $j++$, Goto Step 2
3. Else End

Algorithm 3: Separation from Ideal Solution

1. $i,j \leftarrow 0$ (Initialization)
2. If $i <$ No. of Alternatives
   (a) $b[i][j] \leftarrow (pos\_ideal[j] - a[i][j])^2$ and $c[i][j] \leftarrow (a[i][j] - neg\_ideal[j])^2$ where $0 < j <$ No. of Criteria
   (b) $i++$, Goto Step 2
3. tempB[i], tempC[i], $i \leftarrow 0$
4. If $i <$ No. of Alternatives and $0 < j <$ No. of Criteria
   (a) $j \leftarrow 0$
   (b) tempB[i]$\leftarrow$tempB[i]+b[i][j]
   tempC[i]$\leftarrow$tempC[i]+c[i][j]
5. while $i <$ No. of Alternative do
   (a) tempB[i]$\leftarrow (tempB[i])^{1/2}$
   (b) tempC[i]$\leftarrow (tempC[i])^{1/2}$
   (c) $i++$
6. end while
7. End

Algorithm 4: Trust Building System

1. $i \leftarrow 0$
2. while $i <$ No. of Alternative do
   (a) rank[i]=$\frac{tempC[i]}{(tempB[i]+tempC[i])}$
   (b) $i++$
3. $i \leftarrow 0$
4. while $i <$ No. of Alternative do

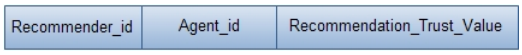

Figure. 3: Temporary Trust Table

(a) If rank[i] $\geq$ 0.5 and rank[i] $<$ 1 then
rank[i]=1 $-$ H(rank[i])
(b) Else
rank[i]=H(rank[i]) $-$ 1

5. end while
6. End

- **Temporary Trust Table:**

  This temporary trust table stores the information regarding each of the agent which exchanges recommendation with the subject. This trust table format is shown in Fig. 3 and its components are described below.

  1. $Recommender\_id$ is the field which shows the id of the node which sends the recommendation message.
  2. $Agent\_id$ field denotes the identification of node whose recommendation is provided by a node with $Node\_id$ = $Recommender\_id$
  3. $Recommendation\_Trust\_Value$ field stores the trust value of an agent which is obtained by the subject by considering .

  $$R_{a_i} = \{RecommenderNode : AgentNode, Action\} \quad (11)$$

- **Recommender:** This component is responsible for broadcast of recommendation message. The recommendations are for those nodes whose trust value is greater than threshold at present as well as in past. The threshold value is to be considered as 0. So any agent having history of trust value greater than 0 will be considered for recommendation as trustworthy node with a certain trust value that subject assigns to that agent. This is to guarantee the fact that a trustworthy agent must not have a past of being malicious and misbehaving. Malicious and misbehaving in the sense of negative trust value.

- **Recommendation Trust Builder:** This helps in processing the temporary trust table to assign a recommendation trust value. Subject activates this component while assessing an agent to find whether the agent is recommended by any other node and if recommended then by whom and with what trust level. On getting these information Recommendation Trust Builder than searches the Trust Table of the subject to find out the trust level of the recommender node. If the Trust value is Positive then new recommended value is derived out by considering the trust of recommender and recommended trust value as considered in axiom 2 [12]. In this case there exists no possibility of negative trust value or unavailable trust value because Recommendation Message only from trustworthy nodes is accepted, others are discarded.

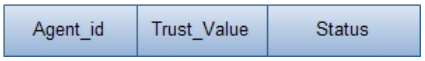

Figure. 4: Trust Table Format in a Node

- **Trust Calculator**: This is the simplest of all modules and it only add the value supplied by the Individual Trust Building and Recommendation Trust Building subsystems and prepares a list to be supplied to the Trust Table component.

- **Trust Table:** It contains the information regarding the trust value assigned to different agent by the subject. The format of this trust table is depicted in Fig. 4 and described subsequently.
  Here $agent\_id$ and $Trust\_value$ are the agent's id and subject's trust on the agent respectively. But the status field is set to 1 when the node is trustworthy and is behaving normally. But whenever agent's behavior becomes suspicious and trust value becomes negative this field value becomes 0. It is to be noted that this status field once changed to 0 can never be changed to 1 irrespective of the fact that the agent stops misbehaving. The status field play an important role for recommendation decision process because the ultimate objective is to avoid an agent having misbehaving and malicious history.

The proposed trust evaluation model is summarized in an algorithmic format named as Trust Building Process, Trust Calculator and Recommendation Broadcast process which are described next.

Algorithm 5: Trust Building Process

1. Subject considers each neighbor from neighbor list as an agent
2. While every agent is not processed
3. Subject select each agent
4. If Agent not perform action for Subject then
   T(a_i)=0
5. Else
   Call to Trust Calculator and Recommendation Broadcast Processing
6. End

Algorithm 6: Trust Calculator

- Module 1: Individual Trust Building
  Input:
  - Agent List a_i, where 1<*i*<*n* and *n* is the number of agents
  - No. of packets needed to be delivered for each a_i
  - No. of packets successfully delivered for each a_i
  - Initial Trust Value
  - Delivery Ratio Efficiency (DRE)

  1. Prepare above information in form of a decision matrix
  2. Apply the MCDM strategy to recalculate individual trust value
- Module 2: Recommendation Trust Building
  1. Search the Temporary Trust Table for a_i
  2. Get the T Recommended for a_i
  3. T(a_i)=$T_{Individual}$+$T_{Recommended}$
  4. Update the Trust Table against each agent with new calculated value
  5. If T(a_i) > Threshold then Broadcast this T(a_i) with the $Agent_{id}$

Algorithm 7: Recommendation Broadcast Processing

1. Collect each Recommendation Message if the recommender is trusty otherwise discard message
2. Extract $recommender_{id}$, $agent_{id}$ and $trust_{value}$ from Recommended Messages and transform it into a tuple r_i,a_i,R(a_i)
3. $T_{Recommended}$ = min (T_{ai},R_{ai}) , where T_{ai} is the calculated trust of the agent
4. If a_i is present in Temporary Trust Table then
   Update the $T_{Recommended}$ Field
5. Else
   Insert r_i,a_i,$T_{Recommended}$ tuple into Temporary Trust Table
6. Repeat 1-5 for all Different Recommendation Messages

F. An Illustrative Example

The proposed MCDM based trust calculation model is validated using C++ code simulation [9]. The example given below illustrate the same [9]. A subject say S is considered which has five neighbors called agents (a_i) say (*a1*,*a2*,*a3*,*a4*,*a5*). It is required to construct the trust table of the subject (S).

1. If there is no information about agents with the subject it indicates there is no previous interactions between the subject and agents. And also there is no recommendation from any other nodes. At this time an intermediate trust value ($T_{val} = 0$) will be assigned to the agents. So the trust table of subject S is as follows.

$S_{TrustTableEntries=}$

Agt_{id}	T_{Val}	$Status$
$a1$	0	1
$a2$	0	1
$a3$	0	1
$a4$	0	1
$a5$	0	1

2. Let after an interval of *x* time the trust building process is again invoked. At that time the subject S will collect all information regarding the its agents like no. of packets needed to be forwarded, packets actually delivered successfully, delivery ratio efficiency (DRE) and probability of successful completion of an action by the agent as desired. These values are then fed into the MCDM machine.
   The agents are considered as the different alternatives and information regarding agents are considered as criteria. They are represented in matrix form as follows:

$Agnts$	"p"	$Pck_{toDeliver}$	$Pck_{Delivered}$	DRE
$a1$	0.5	120	110	0.92
$a2$	0.5	150	140	0.96
$a3$	0.5	100	25	0.25
$a4$	0.5	80	15	0.19
$a5$	0.5	120	50	0.41

3. When above values are given to the MCDM machine, a new probability value *(p)* for each agent is calculated following TOPSIS method as described in the proposed model.

$Agents$	"p"
$a1$	0.78704
$a2$	1
$a3$	0.111999
$a4$	0
$a5$	0.314025

4. From equation 1, T value is calculated for each agent. From that relation the calculated trust values are as follows.

$Agents$	"T"	$Remarks$
$a1$	0.25	$(TrustworthyNode)$
$a2$	1	$(MostTrustworthyNode)$
$a3$	-0.49	$(UntrustworthyNode)$
$a4$	-1	$(MostUntrustworthyNode)$
$a5$	-0.10	$(UntrustworthyNode)$

5. Recommendation will be advertised for *a1*, *a2* agents.
   The process will be executed whenever the subject invokes it.

V. The Trusted Modified Optimized Link State Routing (TM-OLSR) Protocol

In this section, we describe the details of our proposed mesh routing scheme called TM-OLSR which integrates the proposed MCDM based trust model. First of all, each individual node in WMNs maintains a temporary trust table and a permanent trust table. Temporary trust table contains Recommender-id, Node-id and recommendation-trust-value, whereas permanent trust table contains Node-id, Trust-value and Status and is calculated from temporary trust table as described in Section IV-C. The permanent trust table is refreshed periodically to remain valid in the network. The status field is set to 1 when the node's trust value is positive and greater than 0. But whenever node's behavior becomes suspicious and trust value becomes negative, this field value becomes 0. It is to be noted that this status field once changed to 0 can never be changed to 1 irrespective of the fact that the node stops misbehaving. The status field play an important role for routing table calculation in TM-OLSR because the ultimate objective is to avoid a node having misbehaving and malicious history. The three main functionalities of the TM-OLSR protocol are HELLO Exchange, Topology Dissemination, Routing Table Calculation, they are detailed as follows.

A. HELLO Exchange

Each node in TM-OLSR detects its trustworthy, static, and symmetric neighbor nodes with which it has a direct link through periodic exchange of HELLO messages. A HELLO message contains the emitting nodes own address, information about its one hop neighbor, neighbor node type, their link status, trust value, status and willingness to carry traffic in the network. The willingness of all static router and gateway nodes are set to WILL ALWAYS and specifies that these nodes can be selected for carrying traffic on behalf of other nodes and may be selected as MPRs whereas all mobile clients have their willingness field set to WILL DEFAULT or WILL NEVER. The link status can be symmetric, asymmetric, multipoint relay, or lost. New fields called Trust Value and status are added in HELLO message to generate information about trustworthy and untrustworthy nodes. Trust value is a real number lying in the closed interval [-1,1]. Nodes with trust value above zero are considered as trustworthy and may selected as MPRs if its willingness field is set to WILL ALWAYS. The HELLO message is transmitted in broadcast mode once per refreshing period of the protocol to all one-hop neighbors but not relayed further. HELLO message serves three independent tasks: *i)* Link sensing, *ii)* Neighbor detection, *iii)* MPR Selection signaling. The outcome of link sensing is a link Set and is used when declaring neighbor information in HELLO messages. The set contains originator nodes own ID, neighboring nodes IDs, and time information to decide link type described in neighbor interface. The outcome of HELLO exchange is neighbor table for each node in TM-OLSR. The table records information about its one hop neighbors, link status with these neighbors, neighbor type, neighbor trust value, neighbor status and a list of two-hop neighbors. Such information has an associated holding time, and will be refreshed periodically to remain valid. Now, on the basis of collected information, each node selects its MPRs from one-hop neighbor set in such a way that, MPR nodes are trustworthy, static and cover all its two-hop neighbor set. The MPR set is recomputed if there is a change in appearance of one-hop or two-hop neighborhood set or a loss is detected. Each node also maintains a MPR selector set indicating those nodes which have selected it as a MPR. Using this modified data structure, TM-OLSR protocol generates its routing table.

B. Topology Dissemination

Through link sensing and neighbor detection functionality, each node gets knowledge of its static, trustworthy, and symmetric neighbor nodes as well as MPRs for optimized flooding. Based on this, all nodes with a non-empty MPR selector set periodically generate a Topology Control (TC) messages that are diffused in the network through generic message flooding for providing each node with sufficient information to allow route calculation. A TC-message contains address of a node generating TC-message, as well as addresses of all MPR selectors of that node. Thus through a TC-message, each node in the network maintains topology information about the network in Topology Tuples called Topology Set. Topology Set describes destination address of the node, which may be reached in one hop from the node described as next node address, a sequence number for recent information and a validity time. The node described as next is a MPR for destination node. This information is acquired from TC-messages and is used for routing table calculation. For each destination, a node maintains at least one Topology Tuple. In this process all nodes receive a partial topology graph of the network. Using this partial topology graph, optimal routes from a node to any reachable destination in the network is computed. The topological information in each node is valid for a limited period of time, and refreshed periodically to remain valid.

C. Routing Table Calculation

Each node in TM-OLSR maintains a routing table describing destination node address, Next-hop node address and hop required to reach the destination, which allows it to route data to destination node in the network. Route is through its MPR nodes and every node periodically broadcasts list of its MPR Selectors. Upon receipt of MPR information each node recalculates and updates routes to each known destination.

VI. Performance Evaluation

The performance evaluation of TM-OLSR and its comparative analysis with M-OLSR have been studied in this section. The protocol available in [10] is re-simulated in this paper to enable comparisons in the same scenarios with ns-2 [23] simulator and a comparative results have been illustrated. Extensive simulations are being carried out to evaluate performance and scalability of TM-OLSR under various networking scenarios with varying node density, node speed, and traffic load.

A. Assumptions

Our simulation model is based on a network architecture where three types of nodes exists, viz., gateways , routers, and clients. Routers are static forming a infrastructure backbone and clients has the mobility. Routers provide the coverage to the clients for communications. Some of the routers having Internet connections are named as gateway routers. All mesh routers and gateways are installed at certain strategic locations. The traffic flows between mobile clients and gateway nodes via static routers, and vice-versa. Client to client communication is through gateway routers. Clients of WMN has got a spontaneous and dynamic character. In the simulation model of trust calculations 25% of total nodes are considered as malicious. For simplicity we assume that malicious nodes drop the packets they receive.

B. Simulation Environment

We first investigate the establishment of trust table in each individual node of WMNs through proposed trust building model. Initially the Trust value of each nodes is 0. TM-OLSR routing protocol and the trust model works in association to each other. Trust is calculated in each time interval and remain valid for a small time duration.
Our TM-OLSR and M-OLSR routing models are built on the top of IEEE 802.11 MAC model of ns-2.35 and random waypoint model is adopted for driving mobile clients. A node in motion updates its position after every fixed interval of time. In order to gain good confidence in the measurement results, we run simulations 10 times with different seed values to obtain mean value of different matrices. Table-1 depicts the parameters set for simulation model that is common for all our simulation scenarios. The other attributes of our simulations viz., number of nodes, mobility, and traffic load are varied from scenario to scenario.

Table 1: **Parameters for Simulation Model**

Simulation Parameters	Value
Simulator	ns-2 (version 2.35)
Operating System	Linux (Ubuntu 10.04)
Simulation Time	100 sec
Simulation Area	1000m X 1000m
Number of Nodes	30 for sparse and 50 for dense
Transmission Range	250 meters/sec
Interference Range	550 meters
Node Placement Distance	200 meters
Movement Mode	Random-Waypoint
Speed of Mobile Nodes	1 meter/sec-5 meter/sec
Pause Time	5 sec
Traffic Type	CBR
Total CBR Flows	14 for sparse and 25 for dense
Data Payload	512 bytes
Packet Rate	20p/sec-60p/sec
Mac Layer	802.11 DCF with RTS/CTS
Radio Frequency	2.4 GHz
Radio Channel Rate	2Mbps
RF Propagation Model	Two-RayGround
Antenna	Omni-directional

We have measured the performance of TM-OLSR and M-OLSR in a sparse as well as a dense networking scenarios for WMNs. The topology of a sparse network is generated by placing 16 static router nodes at 200 meters distance to form a rectangular grid, and 14 mobile clients move within the area. There are 4 gateway nodes that are selected among the static routers placed at the border positions of the grid. A dense network scenario consists of 25 static routers, 25 mobile clients and 8 gateway nodes selected among static routers.

C. Performance Metrics

The protocols performance have been measured in terms of throughput, PDR, NRO and End to End delay. The protocols scalability is also investigated with varying node density.

- *Throughput*: Throughput is computed as the amount of data transferred (in bytes) divided by the simulated data transfer time (the time interval from sending the first CBR packet to receiving the last CBR packet).
- *Packet Delivery Ratio* (PDR): PDR is the ratio of the number of packets delivered and the number of packets generated by CBR sources.
- *Normalized Routing Overhead* (NRO): NRO is defined as the ratio of number of control packets propagated in the network to the number of data packets received by destination nodes.
- *End to End Delay* : End to End delay is defined as the average transit time of a packet, i.e.,the time

taken for a packet to reach destination from the source.

D. Results and Analysis

We simulated TM-OLSR and M-OLSR protocols in different scenarios whose results along with discussions are presented below.

1) Scenario I

In this scenario, we evaluate the protocols performance (i.e throughput, PDR , NRO and End-to-End Delay) in a sparse network. Simulation is carried out with different traffic load condition i.e. varying number of data packets sent per seconds while keeping the number of flows constant. Simulation parameters are same as referred in the Table-1.

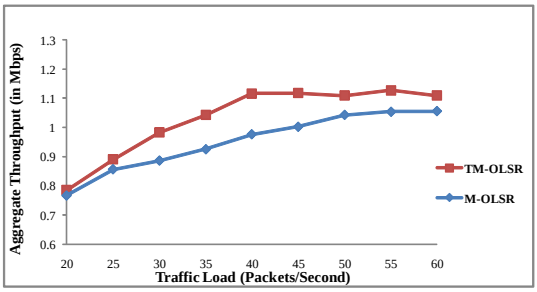

Figure. 5: **Aggregate Throughput vs. Traffic Load**

From Figure-5, it has been observed that the aggregate throughput of TM-OLSR and M-OLSR confirm resilience to increasing traffic load. In fact, TM-OLSR outperforms M-OLSR. It is noticeable that, aggregate throughput of both the protocols increases with increasing traffic load and then tends to reach a saturation point according to the network conditions, e.g. 40 packets/flow for TM-OLSR and 50 packets/flow for M-OLSR. But TM-OLSR performs better at M-OLSR's saturation point too. Number of connections/flow remains constant in the simulation. The simulation results consistently proved that when compared with M-OLSR, TM-OLSR exhibits a much better scalability of traffic loads.

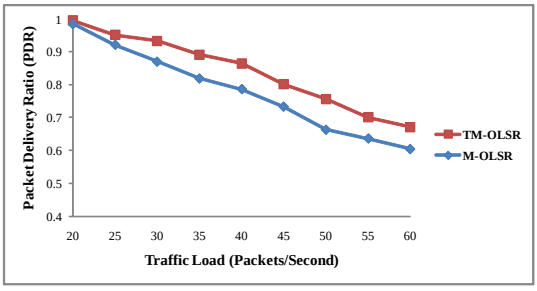

Figure. 6: **Packet Delivery Ratio vs. Traffic Load**

Figure-6, shows that as offered traffic load intensifies, aggregate PDR decreases for both the protocols because of increased intra-flow and inter-flow interference and contention. But performance of TM-OLSR degrades gracefully than M-OLSR. The degradation in M-OLSR is almost 25% higher than TM-OLSR. Although, both the protocols calculate best available routes using stationary nodes, but TM-OLSR also consider the trustworthy nodes for route calculation and hence chances of packet drops due to misbehaving and malicious nodes are minimized.

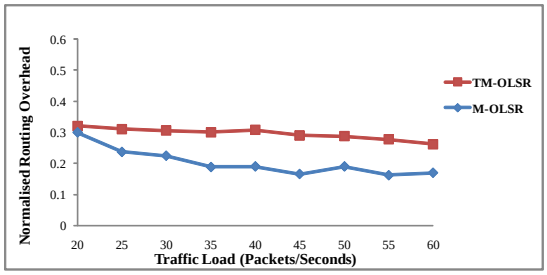

Figure. 7: **Normalized Routing Overhead vs. Traffic Load**

Figure-7 depicts NRO as a function of offered traffic load, where M-OLSR performs slightly better than TM-OLSR. Being proactive protocols, TM-OLSR as well as M-OLSR shows overhead immunity to traffic load. Once route is available to a source node, data packets follow the same route to reach a destination. As traffic load increases, aggregate throughput also increases, whereas overhead of control packets is almost constant because of proactive routings. But, the reason for higher routing overhead (which is insignificant as compared to M-OLSR) in TM-OLSR is due to the added security features. The rise in NRO of TM-OLSR is by .05% as compared to M-OLSR.

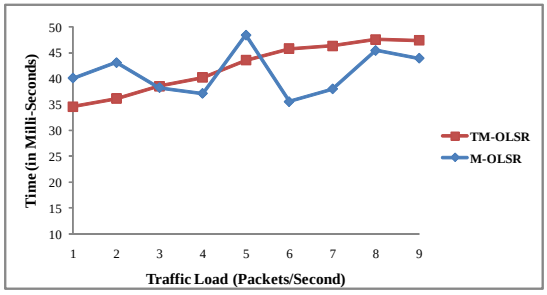

Figure. 8: **End to End Delay vs. Traffic Load**

The average end-to-end delay increase in a linear fashion for TM-OLSR which is evident from Figure-8. This is due to the larger queuing delays resulting from the increase in offered traffic load. End-to-end delay of TM-OLSR is slightly higher than M-OLSR. This is due to large size of TM-OLSR HELLO packets when compared to M-OLSR. This large routing over head packets causes the delay and latency of the pay load packets in TM-OLSR when compared M-OLSR.

2) Scenario II

To analyze TM-OLSR's scalability with network dynamics in a sparse network, we performed simulations by varying the speed of mobile clients from 1meter/sec to 5meter/sec., and comparison is being carried out with M-OLSR.
Table-2 depicts the aggregate CBR throughput, PDR, NRO and End-to-End Delay versus client mobility under different load condition for both TM-OLSR and M-OLSR protocol. As the speed increases, throughput and PDR drops for both protocols because mobile nodes lose connectivity with its next hop more often leading more route breaks and data loss. However, with increased mobility, as compared to M-OLSR, TM-OLSR's throughput and PDR degrades gracefully because of the fact that, routes are calculated via trusted routers. So chances of packets drop is minimized.

3) Scenario III

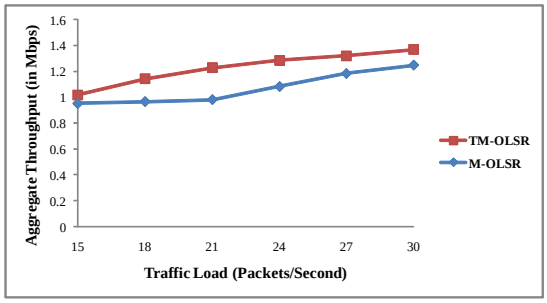

Figure. 9: **Aggregate Throughput vs. Traffic Load**

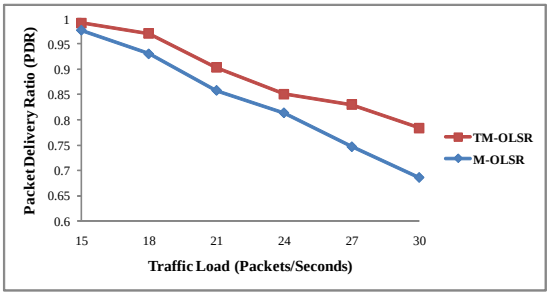

Figure. 10: **Packet Delivery Ratio Vs Traffic Load**

In this scenario, we vary average node degree to see how TM-OLSR scale with node density. We obtain different node densities by varying total number of nodes by keeping simulation area constant. To evaluate performance of TM-OLSR and M-OLSR, we vary offered traffic load from 15packets/sec to 30packets/sec, while keeping the number of CBR flows as 25. Other simulation parameters are same as referred in Table-1. We observed increased throughput for all protocols as node density increases. This is due to closer association and availability of nodes in the network causing minimal chances of link breakages. The decrease in PDR for both the protocols with increase in node density is due to increase in number of hops which in turn increases the routing over head for route discovery and latency which ultimately results in dropping of the payload packets. The PDR for TM-OLSR and M-OLSR are all most same in a high density scenario but M-OLSR performs worse in this case due to presence of untrustworthy nodes. Throughput is better for TM-OLSR as compared to M-OLSR.

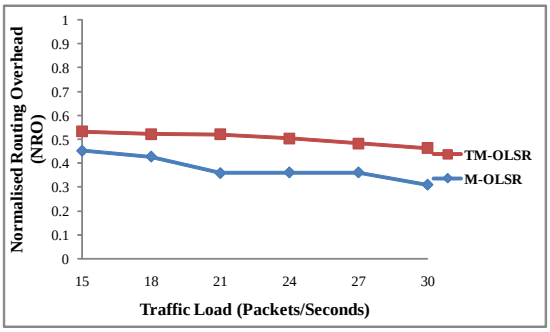

Figure. 11: **Normalized Routing Overhead Vs Traffic Load**

Figure-11 exibits NRO for both protocols in a dense network condition. NRO of M-OLSR is almost static because proactive protocol has lowest routing load and it marginally changes with the network size. The reason for higher NRO in TM-OLSR is that, as number of hops increases, the problem of congestion and drops, both in queues and in the medium also rises, which in turn requires generation of more number of routing messages for route establishment and maintenance.

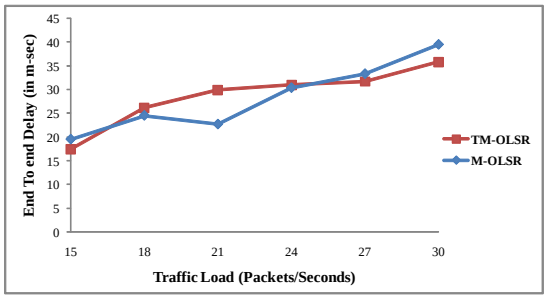

Figure. 12: **End-to-End Delay Vs Traffic Load**

From figure-12, we observed End-to-End Delay in a dense network. The delay rises in a linear fashion for both the protocols. And the amount of delay incurred in TM-OLSR is almost same as M-OLSR.

4) Scenario IV

To compare and analyze the performance of TM-OLSR and M-OLSR in a dense network with varying node mobility, we varied mobility of client nodes from 1 meter/sec to 5 meter/sec under different load condition. The network size remains constant as Scenario III. The

Table 2: Comparative Performance of TM-OLSR and M-OLSR in a Dynamic and Sparse Network

Data Sheet									
		Throughput		PDR		NRO		End-to-End Delay	
Traffic Load	Mobility	TM-OLSR	M-OLSR	TM-OLSR	M-OLSR	TM-OLSR	M-OLSR	TM-OLSR	M-OLSR
20 packets/sec	1meter/sec	0.796	0.785	0.995	0.984	0.331	0.299	34.562	40.109
	3meter/sec	0.779	0.764	0.978	0.967	0.437	0.398	30.813	41.150
	5meter/sec	0.763	0.743	0.951	0.945	0.491	0.456	28.562	35.977
25 packets/sec	1meter/sec	0.908	0.890	0.974	0.920	0.391	0.237	36.135	43.138
	3meter/sec	0.862	0.779	0.910	0.831	0.485	0.390	32.561	47.136
	5meter/sec	0.845	0.749	0.903	0.781	0.495	0.437	29.657	36.771
30 packets/sec	1meter/sec	0.986	0.882	0.901	0.870	0.356	0.224	38.539	38.203
	3meter/sec	0.965	0.796	0.858	0.753	0.519	0.459	36.256	48.116
	5meter/sec	0.953	0.752	0.841	0.740	0.549	0.514	31.567	42.362
35 packets/sec	1meter/sec	1.048	0.804	0.819	0.769	0.365	0.349	17.767	37.103
	3meter/sec	0.978	0.850	0.780	0.725	0.435	0.309	26.138	49.973
	5meter/sec	0.950	0.845	0.772	0.715	0.426	0.415	18.823	31.362
40 packets/sec	1meter/sec	1.188	0.886	0.780	0.716	0.360	0.295	31.523	48.387
	3meter/sec	0.988	0.898	0.757	0.692	0.383	0.336	24.279	57.519
	5meter/sec	0.975	0.878	0.712	0.650	0.445	0.407	21.747	45.533
45 packets/sec	1meter/sec	1.140	0.948	0.755	0.633	0.335	0.266	32.862	35.567
	3meter/sec	1.196	0.891	0.706	0.611	0.425	0.373	21.813	59.086
	5meter/sec	0.988	0.882	0.685	0.602	0.444	0.381	17.340	44.971
50 packets/sec	1meter/sec	1.173	1.979	0.663	0.633	0.288	0.189	34.781	37.965
	3meter/sec	0.987	0.966	0.624	0.599	0.391	0.357	27.010	58.374
	5meter/sec	0.976	0.956	0.603	0.569	0.437	0.394	21.345	45.264
55 packets/sec	1meter/sec	1.152	0.957	0.675	0.616	0.250	0.162	29.192	45.475
	3meter/sec	0.987	0.930	0.597	0.538	0.430	0.302	18.646	57.280
	5meter/sec	0.976	0.920	0.587	0.516	0.396	0.380	17.273	46.589
60 packets/sec	1meter/sec	1.185	0.989	0.646	0.595	0.262	0.169	18.483	43.899
	3meter/sec	0.975	0.944	0.568	0.512	0.344	0.283	21.519	60.110
	5meter/sec	0.969	0.929	0.525	0.481	0.366	0.362	20.252	43.080

other parameters considered for the simulation are remain same as Table-1. It has been observed that as traffic load increases along with increased speed, TM-OLSR outperform M-OLSR. PDR of both the protocols decreases with increased traffic load and mobility due to increased collision, and reduced channel access, but TM-OLSR exhibits better performance than M-OLSR. It has been observed that NRO of TM-OLSR rises insignificantly as compared to M-OLSR in dense and dynamic network. As density increases, End-to-End delay of both the protocols increases in a linear fashion with increase in load and speed, because larger number of nodes in the topology take part in route calculation. The data sheet for this scenario is provided in Table 3.

VII. Conclusion

In this paper we presented a trust based secure routing protocol called TM-OLSR for Wireless Mesh Networks. The protocol integrates MCDM based trust model with M-OLSR, for detection of malicious and misbehaving nodes which helps in determining the nodes trustworthiness. Thus the routing path generated through TM-OLSR only consider trusted nodes for packet forwarding. The Performance of TM-OLSR is evaluated through extensive simulations and a comparative analysis is being carried out with M-OLSR under various networking scenarios with varying node density, node speed, and traffic load. The results justify that the performance of TM-OLSR is much better than M-OLSR in terms of throughput, PDR and end-to-end delay in dense as well as in dynamic networks. But its NRO is slightly higher as compared to M-OLSR. We will explore this issue in our future work.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, 2005.

[2] M. Sichitiu, "Wireless Mesh Networks: Oppurtunities and Challenges," in *Proc. of Wireless World Congress*, 2005, pp. 1–6.

[3] A. B. Paul, S. Konwar, U. Gogoi, A. Chakraborty, N. Yeshmin, and S. Nandi, "Implementation and performance evaluation of AODV in wireless mesh networks using ns-3," in *Proc. of International Conference on Education Technology and Computer*, vol. 5, 2010, pp. 298–303.

[4] A. Naveed, S. S. Kanhere, and S. K. Jha, "Attacks and security mechanisms," Tech. Rep., 2008.

[5] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proc. of MOBICOM*, 2002.

[6] M. G. Zapata and N. Asokan, "SAODV : Securing ad-hoc routing protocols," in *Proc. of ACM Workshop on Wireless Security*, 2002, pp. 1–10.

Table 3: Comparative Performance of TM-OLSR and M-OLSR in a Dynamic and Dense Network

Data Sheet									
		Throughput		PDR		NRO		End-to-End Delay	
Traffic Load	Mobility	TM-OLSR	M-OLSR	TM-OLSR	M-OLSR	TM-OLSR	M-OLSR	TM-OLSR	M-OLSR
15 packets/sec	1meter/sec	0.953	0.912	1.161	0.997	0.581	0.452	17.186	19.539
	3meter/sec	0.894	0.887	0.998	0.976	0.768	0.742	23.289	30.836
	5meter/sec	0.878	0.854	0.976	0.948	0.782	0.759	30.313	33.782
18 packets/sec	1meter/sec	1.143	0.956	0.719	0.631	0.622	0.426	21.816	24.543
	3meter/sec	0.947	0.934	0.969	0.910	0.715	0.683	26.315	30.709
	5meter/sec	0.900	0.896	0.942	0.894	0.748	0.663	33.342	35.539
21 packets/sec	1meter/sec	1.227	0.998	0.877	0.858	0.453	0.359	22.710	27.717
	3meter/sec	0.991	0.985	0.846	0.834	0.682	0.588	27.583	31.038
	5meter/sec	0.977	0.936	0.899	0.837	0.757	0.623	39.222	44.067
24 packets/sec	1meter/sec	1.285	1.125	0.851	0.813	0.568	0.361	27.944	30.390
	3meter/sec	1.175	1.079	0.887	0.777	0.763	0.676	22.757	34.839
	5meter/sec	0.988	0.976	0.824	0.760	0.782	0.639	21.605	34.343
27 packets/sec	1meter/sec	1.322	1.165	0.776	0.747	0.503	0.360	32.266	33.343
	3meter/sec	1.343	1.086	0.771	0.736	0.738	0.699	38.093	43.407
	5meter/sec	1.012	0.993	0.890	0.729	0.745	0.665	24.953	36.932
30 packets/sec	1meter/sec	1.369	1.203	0.698	0.685	0.522	0.309	33.890	39.512
	3meter/sec	1.137	1.092	0.663	0.651	0.672	0.456	32.285	45.919
	5meter/sec	1.309	0.998	0.660	0.627	0.701	0.674	47.276	60.797

[7] M. Jarrett and P. Ward, "Trusted computing for protecting ad-hoc routing," in *Communication Networks and Services Research Conference, 2006. CNSR 2006. Proceedings of the 4th Annual*, may 2006, pp. 8 pp. –68.

[8] E. Charles, Perkins, M. Elizabeth, and Royer, "Ad hoc On-Demand Distance Vector Routing." in *Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, February 1999.

[9] S. Konwar, A. Paul, S. Nandi, and S. Biswas, "MCDM based trust model for secure routing in wireless mesh networks," in *Information and Communication Technologies (WICT), 2011 World Congress on*, dec. 2011, pp. 910 –915.

[10] A. B. Paul and S. Nandi, "Modified Optimized Link State Routing (M-OLSR) for Wireless Mesh Networks," in *Proc. of the 11th International Conference on Information Technology (ICIT 2008)*, 2008, pp. 147–152.

[11] A. B. Paul, S. Konwar, U. Gogoi, S. Nandi, and S. Biswas, "E-AODV for wireless mesh networks and its performance evaluation," 2011, pp. 26–33.

[12] Y. L. Sun, W. Yu, Z. Han, and K. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, 2006.

[13] C. Hwang and K. Yoon, "Multiple attribute decision making methods and applications." Springer-Verlag, New York, 1981.

[14] O. Jadidi, T. Hong, F. Firouzi, R. Yusuff, and N. Zulkifli, "TOPSIS and fuzzy multiobjective model integration for supplier selection problem," *International OCSCO World Press*, 2008.

[15] P. Das, "In search of best alternatives: a TOPSIS driven MCDM procedure for neural network modeling," *Neural Computing and Applications*, vol. 19, no. 1, 2010.

[16] T. George and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, 2006.

[17] H. Wang, X. Zhai, and P. Chen, "Trust Routing Protocol Framework Based on Bahavior Assessment for Wireless Sensor Networks," in *Proc. of IEEE International Conference on e-Business Engineering*, 2008, pp. 487–492.

[18] Y. Yu, K. Li, Y.Zhang, and L. Xu, "A service trust model with passive trust," in *Proc. of IFIP International Conference on Network and Parallel Computing*, 2008.

[19] X. Wang, L. Liu, and J. Su, "RLM: A General Model for Trust Representation and Aggregation," *IEEE Transactions on Services Computing*, vol. PP, no. 99, pp. 1–14, 2010.

[20] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol (OLSR)." *IETF Experimental RFC 3626*, October 2003.

[21] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying: An efficient technique for flooding in mobile wireless networks," Tech. Rep., 2000.

[22] D. Gambetta, "Can we trust trust?" in *Trust: Making and Breaking Cooperative Relations*. University of Oxford, 2000, pp. 213–237.

[23] "NS-2," http://www.isi.edu/nsnam/ns/.

Author Biographies

Amrita Bose Paul graduated in Science from Gauhati University, India, in the year 1987 and then obtained her Master of Computer Applications (MCA) degree from Jorhat Engineering College (Dibrugar University), India in 1991 followed by Masters in Computer Science and Engineering from Indian Institute of Technology (IIT) Guwahati, India in the year 2008. She is an Associate Professor at Assam Engineering College, Guwahati, India since March, 1992 and also pursuing her PhD in Computer Science and Engineering in IIT Guwahati. Her research area includes security issues in wireless mesh networks and intrusion detection in wireless network.

Shantanu Konwar received his Master of Computer Applications (MCA) degree from Assam Engineering College (Gauhati University), India in the year 2010. He worked as a Student trainee for one year (Aug 2009 to July 2010)in the research project entitled "Investigation of Security Issues in Wireless Mesh Networks and Development of a Secure Routing and Authentication Protocol" and subsequently as a Junior Research Fellow in the same project for another year (Aug 2010 to Aug 2011) at Assam Engineering College, India. Currently he is working as a Software Engineer in Kodiak Networks, Bangalore, India. His research interests include Network Security and Routing in Wireless Mesh Networks.

Santosh Biswas received B.E degree from NIT, Durgapur, India, in 2001. He has completed his MS and PhD from IIT Kharagpur, India, in the year 2004 and 2008, respectively. At present he is an assistant professor in the department of CSE, IIT Guwahati, India. His research interests include networking, VLSI testing and discrete event systems.

Sukumar Nandi received BSc (Physics), BTech and MTech from Calcutta University in 1984, 1987 and 1989 respectively. He received the PhD degree in Computer Science and Engineering from Indian Institute of Technology Kharagpur in 1995. In 1989-1990 he was a faculty in Birla Institute of Technology, Mesra, Ranchi, India. During 1991-1995, he was a scientific officer in Computer Science and Engineering, Indian Institute of Technology Kharagpur. In 1995 he joined Indian Institute of Technology Guwahati as an Assistant Professor in Computer Science and Engineering. Subsequently, he became Associate Professor in 1998 and Professor in 2002. He was in School of Computer Engineering, Nanyang Technological University, Singapore as Visiting Senior Fellow for one year (2002-2003). He was member of Board of Governor, Indian Institute of Technology Guwahati for 2005 and 2006. He was General Vice-Chair of 8th International Conference on Distributed Computing and Networking 2006. He was General Co-Chair of the 15th International Conference on Advance Computing and Communication 2007. He is also involved in several international conferences as member of advisory board/ Technical Programme Committee. He is reviewer of several international journals and conferences. He is coauthor of a book titled "Theory and Application of Cellular Automata" published by IEEE Computer Society. He has published more than 150 Journals/Conferences papers. His research interests are Computer Networks (Traffic Engineering, Wireless Networks), Computer and Network security and Data mining. He is Senior Member of IEEE and Fellow of the Institution of Engineers (India)