Multi-Priority and Trusted Multi-Path Selection Algorithm for Ad-hoc Network

Fariha Afsana, Nusrat Z. Zenia, Nazia Islam, Farhana A. Sunny
Institute of Information Technology
Jahangirnagar University
Dhaka, Bangladesh
Email:{afsana.fariha, nusratzenia, naziasebelly, sun.iit.ju}@gmail.com

M. S. Kaiser and S. A. Mamun
Institute of Information Technology
Jahangirnagar University
Dhaka, Bangladesh
Email:{mskaiser, sam}@juniv.edu

***Abstract*—This paper presents a multi-priority and multi-path selection algorithm for heterogeneous traffic for wireless ad-hoc networks. The main objectives are achieving higher throughput, better resource utilization through load balancing and relinquish network congestion. The proposed algorithm has considered signal-to-interference plus noise ratio (SINR), available link bandwidth, link delay (transmission delay and queuing delay), trust value of a node and traffic class (such as real time and non-real time traffic) to select optimal path. The performance of the proposed Multi-Priority and Trusted Multi-Path Selection (MTMS) algorithm has been evaluated by OPNET Modeler 14.5 simulator. It is found that in terms of average throughput (bit/second) and link delay proposed MTMS algorithm outperforms ad-hoc on-demand distant vector (AODV) and dynamic source routing (DSR).**

***Keywords*—Wireless ad-hoc network, trust, traffic class, load balancing, outage probability.**

I. Introduction

Wireless ad-hoc is a decentralized self-configured system that communicates without relying on a predefined infrastructure to keep the network connected. There are a variety of applications of ad-hoc networks, such as disaster recovery, home security, machine diagnosis, military applications, vehicular movement, environmental monitoring, biological detections, soil makeup, noise levels, mechanical stress levels on attached objects and the current characteristics such as speed, direction and size of the objects [1].

Ad-hoc networks consist of multiple nodes which can move arbitrarily. When two communicating nodes are not in range of each other, multiple hops are needed to exchange data between them in the network. Major vital issues in this regard are to manage data efficiently to minimize interference, network congestion and utilize existing network resources. In multi-hop ad-hoc network different time varying paths exist between source and destination. Thus suitable link selection and establishment are prime concern.

Several researches have been done on route selection of ad-hoc network. Multi-priority Multi-path Selection for Video Streaming (MPMPS) has chosen the maximum number of disjoint paths for maximizing throughput of multimedia streaming and to reduce end to end transmission delay. Authors prioritized image and audio streams which are the parts of video stream based on application requirements [2]. Route Outage Probability (ROP) has been proposed as a metric to choose best route for minimizing packet loss due to multi-path fading. Based on current channel condition and estimated cost of route, multiple routes were cached and used later as alternate routes [3][4].

Another route selection approach has used packet drop probability (PDP) as route selection parameter. Authors proposed an optimal scheme for selecting disjoint path between two nodes to minimize concurrent PDP over all possible path pairs and to maximize average video quality [5]. PDP was estimated by taking the interference between different links into account. Because of the multi-hop nature of the ad-hoc network, multiple wireless nodes may exist between source/destination pair. These intermediate nodes may be subjected to different types of attack. The link performance will depend on the behavior of nodes. During the literature survey, a significant number of researches have also been reported on it. Path Selection for Multi-path Streaming is such an approach where some potential vulnerabilities of mobile ad-hoc along with proposed prevention, detection and reaction mechanisms have been overviewed [6][7][8].

It is worth noting that previous studies have indicated partial fulfillment of efficient ad-hoc routing requirements. In MPMPS, they have always considered shortest path with minimum hop count as best path to reduce delay [2]. However, always shortest path with minimum hop count may not be the best path because a path with better bandwidth and energy with minimum queue occupancy can transmit data more rapidly than shortest path. Again ROP based algorithm is not bandwidth efficient and it has not focused on delay [3]. To the best of our knowledge, no research paper has been reported on bandwidth utilization and load balancing for wireless ad-hoc. Our contribution is to propose an algorithm to select, multi-priority multi-path for load balancing with the concern of trust, heterogeneous traffic with delay optimization which will perform better resource utilization and relinquish congestion. Based on node's resources (power, queue occupancy rate) as well as link properties (available bandwidth, SINR, delay), Route Selection and Management Cost ($RSMC$) will be calculated to explore feasible paths. It is assumed that transmissions are burst in nature and the channel information is known to the receiving nodes.

The rest of this paper is organized as follows. Section II includes system model. Section III proposes routing algorithm. Section IV and V show simulation result and numerical analysis respectively. Conclusion is given in section VI.

II. System Model

A. Scenario

A possible ad-hoc network scenario is depicted at a particular time in Figure 1. Here, wireless nodes behave simultaneously as a host and a router. These wireless nodes form wireless mesh network like architecture resulting the existence of multiple links between source/destination pair.

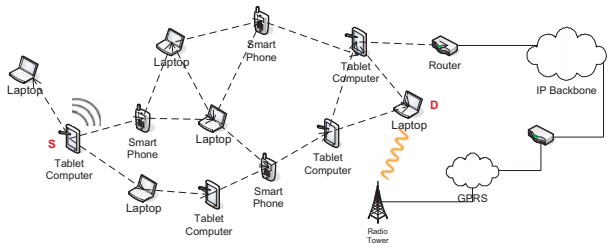

Fig. 1. A possible ad-hoc network

In Figure 1, a source, denoted by S, wants to transmit data to destination, denoted by D, which is situated outside of its transmission range. Other mobile nodes located between them can forward messages of S.

Figure 2 shows the collaboration of intermediate nodes between $S-D$ which results in multiple possible paths, denoted by $\{L_1, L_2, \cdots, L_n\}$. Based on $RSMC$ and trust value, the algorithm selects one or more possible paths.

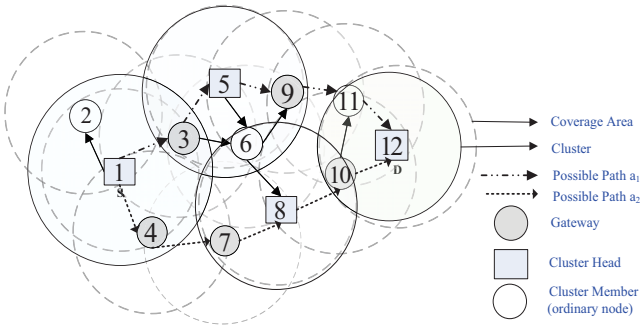

Fig. 2. Simplified network with possible paths between S and D

B. Performance metric

Due to resource limitation (e.g., bandwidth, power) and link instability, all these possible paths may not efficient. So an efficient route management process should be activated with this dynamic restructuring in a trust and delay tolerant way which will assure resource optimization. To select most favorable path, concentration should be given on real time and non-real time traffic to guarantee the use of limited bandwidth and energy. Non-real time traffic is delay tolerant but it is the crucial point in the case of real time traffic. Considering the mentioned criteria, $RSMC$ for link $i-j$ is counted based on trust value (τ_{ij}), available link bandwidth (BW_{ij}), link delay (Γ_{ij}) and link SINR (γ_{ij}).

The expression for Route selection metric can be expressed as

$$RSMC = \sum_{i=0}^{n} \beta_i \times \frac{\gamma_{ij}}{\gamma_{max}} + \beta_j \times \frac{BW_{ij}}{BW_{max}} + \beta_k \times \frac{\Gamma_{ij}}{\Gamma_{max}}. \quad (1)$$

Where $\beta_i,\ \beta_j,\ \beta_k$ refer to the weight metrics for γ_{ij}, BW_{ij} and Γij. The value of $\beta_i,\ \beta_j,\ \beta_k$ can be different for real and non-real time traffic. The maximum value of BW_{ij}, Γij and γ_{ij} are denoted by BW_{max}, Γ_{max} and γ_{max} respectively.

1) Trust Value: Trust value is calculated to select a trustable node for a next message among all encountered nodes. Depending on the number of forwarded packets ($F_{ij}(t-1)$) and received packets ($R_{ij}(t-1)$) of previous communication at time $(t-1)$, the trust value calculation, $\tau_{ij}(t)$ at time instant t can be expressed as,

$$\tau_{ij}(t) = \begin{cases} \tau_{ij}(t-1) + G \times \delta & if\ X > 0 \text{ and } Y > 0 \\ \tau_{ij}(t-1) - \delta & if\ X = 0 \text{ and } Y = 0. \end{cases} \quad (2)$$

Here G=$\frac{X}{Y}$, $X = F_{ij}(t-1)$, $Y = R_{ij}(t-1)$ and $\tau_{ij}(t-1)$ is trust value at time $(t-1)$. δ = 0.1 which is the reward or penalty value for trust calculation [11].

2) Available Link Bandwidth: Bandwidth constraint is one of the most important constraints for ad-hoc network. Thus it is considered as one of the performance metrics to select path and to detain load balancing. Let, at any time, link utilization for link $i-j$ is u_{ij}, where $0 \le u_{ij} \le 1$. Then, BW_{ij} can be defined as

$$BW_{ij} = \min_{i,j} BW^*_{ij}(1 - u_{ij}). \quad (3)$$

Where i, j=$0, \cdots, n$ and $i \neq j$.

Usually, the level of congestion of link $i-j$ can be determined by u_{ij}. If $\overline{BW}_{ij}$ is the current bandwidth usage of link $i-j$, then u_{ij} can be expressed as

$$u_{ij} = \frac{\overline{BW}_{ij}}{BW^*_{ij}} = \frac{BW^*_{ij} - BW_{ij}}{BW^*_{ij}}. \quad (4)$$

3) Link Delay: Link delay affects the performance of heterogeneous traffic. In our proposed algorithm, we have set different priority to delay for real and non-real traffic by multiplying weight metric with normalized delay. To calculate Γ_{ij}, equation (5) can be considered.

$$\Gamma_{ij} = \Upsilon_{ij} + \Psi_{ij}. \quad (5)$$

Here Υ_{ij} indicates transmission delay and and Ψ_{ij} indicates queuing delay.

Υ_{ij} is the time required to put an entire packet into the communication media and it can be determined by equation (6).

$$\Upsilon_{ij} = \frac{l}{T_r}, \quad (6)$$

where l and T_r denote the packet length and transmission rate respectively.

During the transmission of other packets a packet may have to wait for a specific time in a queue at a node which is referred to as Ψ_{ij} . If we consider $M/M/1/K$ queue model where K is the size of the buffer, Ψ_{ij} of a node can be computed by the equation (7).

$$\Psi_{ij} = \frac{1}{\mu}\left(\frac{\lambda}{\mu - \lambda}\right). \quad (7)$$

Where λ is average arrival rate (packets/sec) and μ is average service rate (packets/sec).Therefore,

$$\Gamma_{ij} = \frac{l}{T_r} + \frac{1}{\mu}\left(\frac{\lambda}{\mu - \lambda}\right). \quad (8)$$

4) Link SINR: In fading channel, γ_{ij} becomes random and it can be expressed as

$$\gamma_{ij} = \frac{P_i |h_{ij}|}{\sigma^2 + \sum I_{mj}}. \quad (9)$$

Here P_i is the transmit power, I_{mj} is the interference from node m to node j, where $m = 1, 2, 3, \cdots, n$ but $m \neq j$. total signal power received from all other transmitters, h_{ij} is distance independent fading co-efficient of receiver and $\sigma > 0$ is the variance of receiver noise.

An outage occurs when γ_{ij} drops below a certain threshold, γ_{th} or Γ_{ij} becomes larger than the maximum tolerable delay, Γ^*_{ij}. It follows that, if outage (P_{out}) occurs, then it may be expressed as

$$P_{out} = P(\gamma_{ij} < \gamma_{th}) \cup P(\Gamma_{ij} > \Gamma^*_{ij}). \quad (10)$$

Where γ_{th} can be found simply by using equation (11).

$$\gamma_{th} = 2^{2T_r} - 1. \quad (11)$$

In our system, we have aimed to select trusted multi-path to balance load in network which would reduce P_{out} as well. Emphasis has been given on Γ_{ij} reducing and γ_{ij} inclusion during $RSMC$ determination. However, estimating the cost of a route using $RSMC$ better represents route reliability by lowering P_{out}.

C. System Architecture:

The proposed route selection scheme is presented by the block diagram depicted in figure 3. We have divided our route

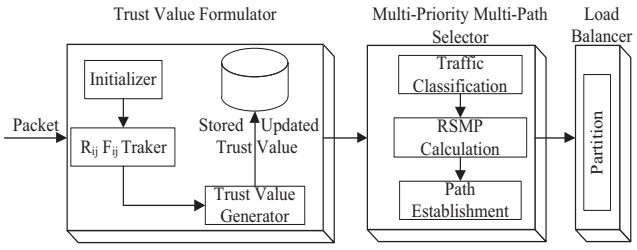

Fig. 3. Block Diagram of Multi-priority Multi-path Routing

selection and route management procedure into three portions:

1) Trust value formulation: Responsible for calculating τ_{ij} to ensure reliability. The task of trust value formulator is conducted by initializer, $R_{ij}F_{ij}$ Tracker and Trust value calculator.

Initializer module is used to assign an initial trust value to unknown mobile nodes in the network. If the initializer detects the entrance of a new node in the network it initiates its τ_{ij} to 0.5.

In $R_{ij}F_{ij}$ Tracker, neighbours are searched by sender broadcasting Node Discovery Packet (NDP). Depending on the responder node j with respect to i, R_{ij} and F_{ij} are tracked by $R_{ij}F_{ij}$ Tracker.

Trust value calculator calculates $\tau_{ij}(t)$ using equation (2). Trust value storage stores the updated value of trust. The work flow of trust value calculation is described in Figure 4, where, $\triangle E$ indicates battery life and E_{th} indicates a certain threshold.

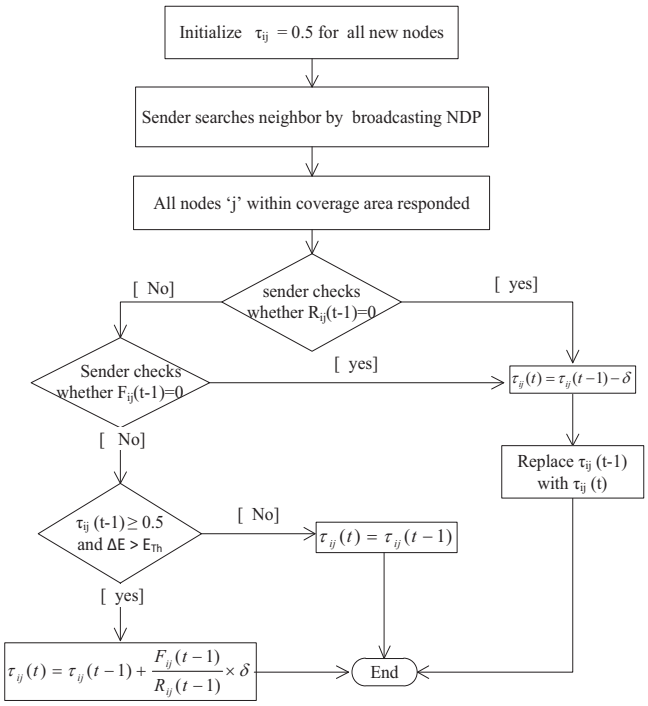

Fig. 4. Operation of Trust Formulation Section

2) Multi-Priority Multi-Path Selector: This portion comprises with traffic classification, $RSMC$ calculation and path establishment. Considering $\tau_{ij}(t-1)$, hello packets are multicast to other reliable nodes within coverage area. If receiver is intermediate node, $RSMC$ is calculated for both real and non-real time traffic. When destination receives packets, it prioritizes the paths based on $RSMC$. Considering the available resources of multiple possible paths, the load balancer partitions data packets and optimally maps them to those paths.

III. Multi-Priority and Trusted Multi-Path Selection Algorithm

Algorithm of our proposed scheme is presented in this section. The process of Multi-priority Multi-path Selection followed by trust value formulation is pointed out here.

A. Trust value formulation

Trust value formulation of any node at time t will use the packet forwarding and receiving ratio of previous communication at time $(t-1)$. Completion of trust value calculation is depicted in algorithm 1.

Algorithm 1: Algorithm for Trust Value Formulation

Data: $R_{ij}(t-1)$, $F_{ij}(t-1)$ and $\tau_{ij}(t-1)$
Result: updated $\tau_{ij}(t)$
initialization;
set $\tau_{ij} = 0.5$ to all new nodes in the topology;
S broadcasts NDP to all neighbor nodes;
for any responder node 'j',
if $R_{ij}(t-1) = 0$ **then**
  $\tau_{ij}(t) = \tau_{ij}(t-1) - 0.1$;
else
  if $F_{ij}(t-1) = 0$ **then**
    $\tau_{ij}(t) = \tau_{ij}(t-1) - 0.1$;
  else
    if $\tau_{ij}(t) \geq 0.5$ *and* $\triangle E > E_{th}$ **then**
      $\tau_{ij}(t) = \tau_{ij}(t-1) + \frac{F_{ij}(t-1)}{R_{ij}(t-1)} \times 0.1$;
    else
      $\tau_{ij}(t) = \tau_{ij}(t-1)$
    end
  end
end

B. Multi-priority Multi-path Selection

Algorithm 2 represents the final processing of multi-priority multi-path selection.

Algorithm 2: Algorithm for Multi-priority Multi-path Selection

Data: trust value of neighbour nodes $\tau_{ij}(t)$
Result: multiple possible paths with priority
initialization;
set $counter = 1$ and calculate τ_{ij} using algorithm 1;
while $counter = 1$ **do**
  if $\tau_{ij} \geq 0.5$ **then**
    Sender S multicasts "Hello packet" to neighbor nodes 'j' containing information of BW_{ij}, γ_{ij} *and* Γ_{ij} ;
    if *intermediate node* **then**
      set β_i, β_j, β_k for real and non-real time traffic;
      calculate path cost for real-time traffic ($RSMC_R$) and non-real time traffic ($RSMC_N$) using equation (1);
      forward "hello packet" to next node with updated $RSMC_R$ and $RSMC_N$;
    else
      D receives packet, prioritizes paths based on $RSMC_R$ and $RSMC_N$ and informs to S;
      S selects paths, partitions data packet and finally sends;
      set $counter = 0$;
    end
  else
    discard;
  end
end

Flow chart for path selection is shown in figure 5.

IV. Simulation Environment

In this section simulation results are given to verify the performance of MTMS algorithm. The performance has been examined with a simple twelve node network shown in Figure 6.

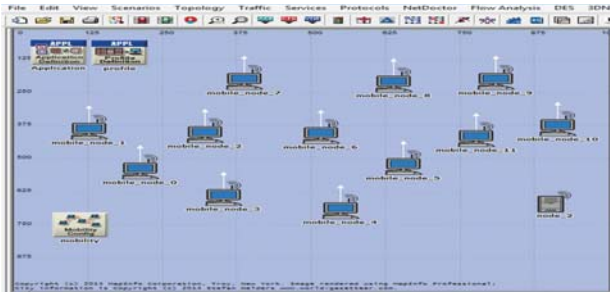

Fig. 6. Opnet simulation distribution of twelve nodes

A. Simulation Parameters

As simulation parameters, we have considered link throughput, end to end delay and network load.

Network throughput refers to average rate at which message is successfully carried between $S - D$ pair and end to end delay is time taken for a packet to be transmitted across a network from source to destination. Normalized routing load is the number of routing packets transmitted per data packet delivered at the destination. The Simulation Parameters are shown in the table I.

TABLE I. Simulation Parameters

Parameter	Value
Simulation Area	$100m \times 100m$
Number of Nodes	12
Data Rate	11 Mbps
Physical Characteristics	Direct Sequence
MAC Layer Protocol	802.11b
Transmit Power	0.005 watt
Packet Reception power threshold	-95 dB
Buffer Size(bits)	256000
Mobility Model	Random Waypoint

B. Simulation Results

This portion investigates the result of simulation using essential metrics that are used in this dissertation. We have created three different scenarios in OPNET to compare their results.

Figure 7 shows the effect of average time on average throughput for the AODV, DSR and MTMS. MTMS outperforms DSR and after a certain time it performs as efficiently as AODV while considering multiple paths. It is to notify that AODV performs well for single path routing but single path sometimes results in ultimate congestion. So, the simulation shows that our modified protocol significantly improves the network throughput. Figure 8 shows the comparison of delay

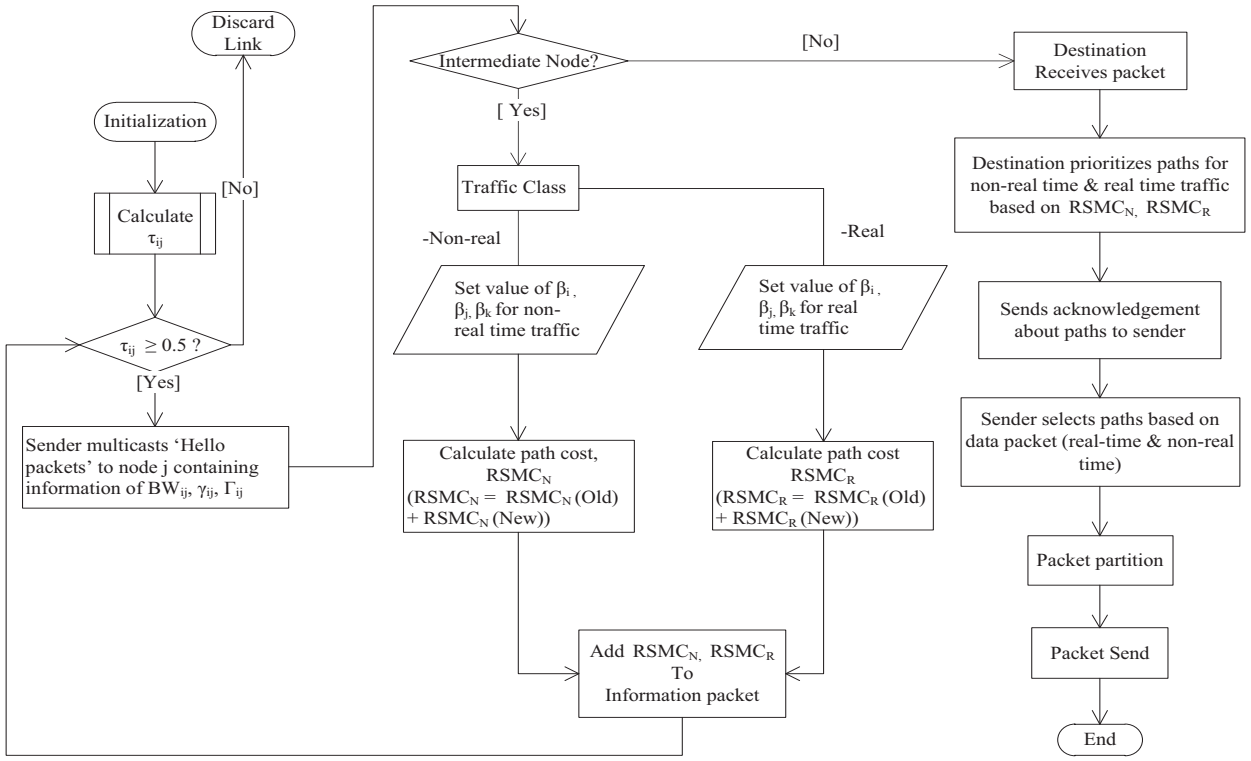

Fig. 5. Operation of Path Selection Section

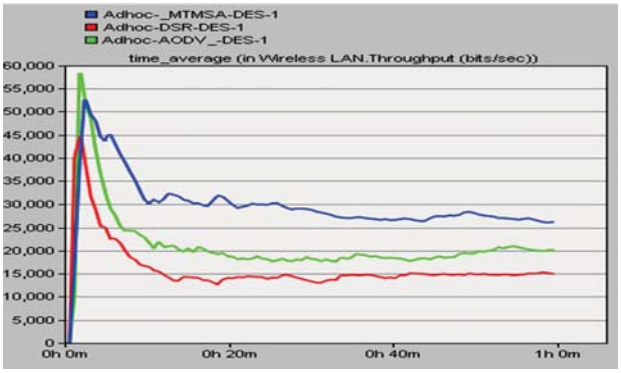

Fig. 7. Effect of time on average throughput

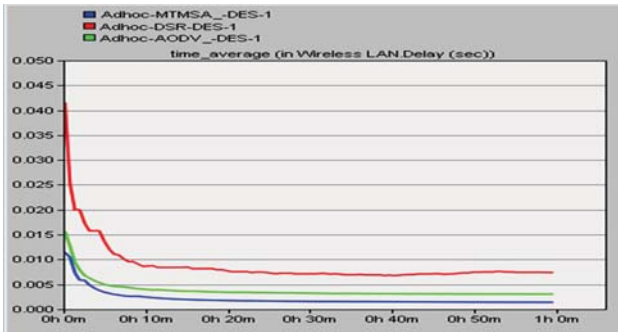

Fig. 8. Effect of time on average Delay

for AODV, DSR and MTMS. It is found that end to end delay is minimum for the proposed case.

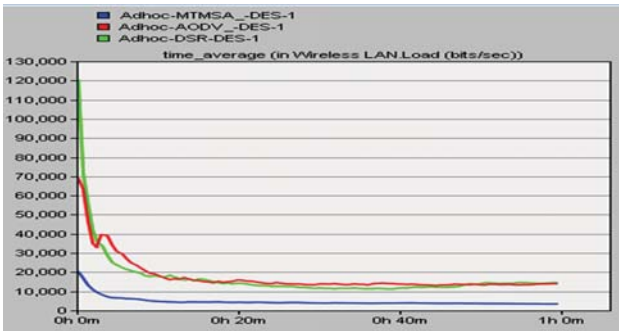

Fig. 9. Effect of time on average Load

Based on the results of buffer availability, exploited bandwidth and processing time at intermediate node, network load is calculated. Figure 9 shows that AODV and DSR perform approximately like each other however MTMS performs better than them in this regard.

AODV selects single path based on hop count. In the shortest path, node may have long queuing delay. We have calculated cost considering Ψ_{ij}, BW_{ij} and γ_{ij} to select multiple paths. Packets are partitioned and distributed over all selected paths. So load and delay is significantly reduced in our proposed algorithm. Because of delay tolerant nature, our proposed MTMS algorithm is better for real time traffic. But all multiple paths may not have high bandwidth. For this reason, throughput is average.

V. Numerical Analysis

This section illustrates τ_{ij} calculation and path selection procedure.

1) Trust Value Calculation: In Figure 2, nodes 2, 3 and 4 are the neighbour nodes of node 1. So, for τ_{ij} calculation, these nodes will be considered by node 1. Initially node 1 has $\tau_{12} = 0.35$ and $\tau_{14} = 0.6$.

When node 1 broadcasts NDP packet, it finds node 3 as a new node. According to the algorithm, node 1 will store $\tau_{13} = 0.5$. Then node 1 will examine the packet receiving and forwarding behavior of node 2, 3 and 4 which is shown in table II.

TABLE II. Packet receiving and forwarding information received by node 1

Node	Trust Value(τ_{ij})	$F_{ij}(t-1)$	$R_{ij}(t-1)$	ratio
2	0.35	0	0	0
3	0.5	8	6	0.633
4	0.6	8	7	0.714

Node 1 will calculate new trust value for all nodes using equation 2. For example, $\tau_{13} = 0.5 + 1.33 \times 0.1 = 0.633$. After calculating τ_{12}, τ_{13} and τ_{14}, the updated values will be stored at node 1 which is depicted in table III.

TABLE III. Updated trust value stored at node 1

Node	Trust Value(τ_{ij})
2	0.25
3	0.633
4	0.714

Node 1 will multi-cast packet to node 3 and 4. Node 2 will be discarded because it is not trustworthy ($\tau_{12} < 0.5$).

2) Path Selection: Assume that sender node (node 1) sends hello packet to node 3 and 4. These nodes will forward packet to their trustable neighbor nodes by following trust value formulation algorithm. Each intermediate node will calculate $RSMC$ using equation 1. Let, for path $L_1[1 \to 3 \to 5 \to 9 \to 11 \to 12]$, $L_2[1 \to 3 \to 6 \to 8 \to 10 \to 12]$, $L_3[1 \to 4 \to 7 \to 8 \to 10 \to 12]$, node D will get CR_1, CR_2, CR_3 respectively with $RSMC_R$. Where, $CR_1 > CR_2$ and $CR_3 > CR_1$. Destination node D (node 12) will prioritize L_3 as 1, L_1 as 2, L_2 as 3 for real time traffic. Again, node

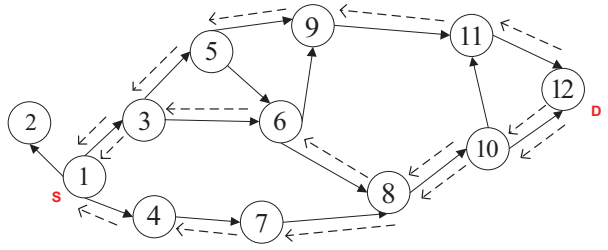

Fig. 10. Path selection and acknowledgement

D will get $RSMC_N$, CN_1, CN_2, CN_3 respectively for path L_1, L_2, L_3 where $CN_1 > CN_2$ and $CN_2 > CN_3$.

D (node 12) will prioritize L_1 as 1, L_2 as 2, L_3 as 3 for non-real time traffic.

VI. Conclusion

This work has proposed a new routing algorithm for ad-hoc network. It selects optimal path based on the trust value of neighbor nodes, link SINR, link delay and available link bandwidth. Intermediate nodes between $S - D$ pair calculates $RSMC$ based on the mentioned link attributes and forwards this information to the next intermediate nodes or an intended destination. The destination node prioritizes all the links for heterogeneous applications and sends this information to node S. Depending on the load, S prioritizes the packets and sends packet through one or multiple paths to minimize delay. The OPNET simulator results show that in terms of average throughput (bit/second) and link delay proposed MTMS algorithm outperforms adaptive on-demand distant vector (AODV) and dynamic source routing (DSR).

References

[1] S. Beura, G.k. Pallai, B. Majhi, "Strong Link Establishment in Wireless Ad-hoc Network using Position based Re-configuration", International Journal of Engineering Research and Development, 2(7), pp. 62-68, Aug. 2012.

[2] L. Zhang et al., "Multi priority Multi path Selection for Video Streaming in Wireless Multimedia Sensor Networks", Springer, vol. 5061, pp. 439-452, June 2008.

[3] M. Park et al., "Wireless Channel-Aware Ad-hoc Cross-Layer Protocol with Multi-Route Path Selection Diversity", in Proc. IEEE 58th Vehicular Conference, Oct. 2003, vol. 4, pp. 2197 - 2201.

[4] S. Kandukuri and S. Boyd, "Optimal Power Control in Interference-Limited Fading Wireless Channels With Outage-Probability Specifications", IEEE Transaction on Wireless Communications, 1(1), Jan. 2002.

[5] W. Wei and A. Zakhor, "Path Selection for Multi-path Streaming in Wireless Ad-hoc Networks", in Proc. Image Processing, 2006 IEEE International Conference, Atlanta, GA, Oct. 2006, pp. 3045-3048.

[6] N. Bhalaji et al.,"Trust Enhanced Dynamic Source Routing Protocol for Ad-hoc Networks", Proceedings of World Academy of Science, Engineering & Technology, vol. 49, pp. 1373-1378, Feb. 2009.

[7] L. Wang et al., "Adaptive multipath source routing in ad-hoc networks", IEEE International Conference, June 2001, vol. 3, pp. 867 - 871.

[8] Z. Yan et al., "Trust Evaluation Based Security Solution in Ad-hoc Networks", Proceedings of the Seventh Nordic Workshop on Secure IT Systems, vol. 14, 2003.

[9] H. Arslan, S. Reddy, "Noise Power and SNR Estimation for OFDM BasedWireless Communication Systems", Wireless Communication and Signal Processing Group, 2003.

[10] D. Torrieri and M. C. Valenti, "The Outage Probability of a Finite Ad Hoc Network in Nakagami Fading", IEEE Transactions on Communications focuses on all telecommunications including telephone, telegraphy, facsimile, and point-to-point television by electromagnetic propagation, 60(11), pp. 3509-3518, Nov. 2012.

[11] S. Aravindh et al., "A Trust Based Approach for Detection and Isolation of Malicious Nodes in Manet", International journal of Engineering and Technology, vol. 5, Feb. 2013.