International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32175-32194

http://www.ripublication.com

Fuzzy Based Quality of Service Trust Model for Multicast Routing in Mobile Adhoc Networks

Nageswara Rao Sirisala and C.Shoba Bindu

CSE Dept, Vardhaman College of Engg, Hyderabad, India.
e-mail: nagsirisala@gmail.com
CSE Dept, JNTUACE, Anantapur, AP, India.
e-mail: shoba_bindhu@yahoo.co.in

Abstract

Mobile ad-hoc network (MANET) is a decentralized and infrastructure less network where a node enter and leave a network at any moment. Quality of Service (QoS) is the level of assurance given to the user about the service provision offered by the network. Due to node mobility, limited resources of mobile nodes and broadcast nature of wireless channels, the QoS provision is not trivial in MANETs. In multicast protocols, there is considerable amount of energy loss and lack of bandwidth since group of nodes are involving in a session. While maintaining multiple QoS parameters in MANET applications, achieving balance among them is a critical issue. Some articles addressed this issue using static methods by assigning fixed weightage to each parameter. The proposed QoS trust model (Fuzzy Based QoS Trust Model for Multicast routing in MANETs-FQTM) focuses on this issue by applying fuzzy inference mechanism. QoS metrics like Energy, Bandwidth, link expiry time and reliability are considered as input variables in the fuzzy inference system to evaluate node trust value. At the time of multicast tree formation, proposed scheme ensures that each path from source to destination includes high trusted intermediate nodes. The proposed method performance is analyzed theoretically and experimentally. In simulation results, the proposed method FQTM outperforms the MAODV and PMRP multicast protocols.

Keywords- Quality of Service, Fuzzy Logic, Trustworthiness, Multicast tree;

1. INTRODUCTION

Mobile ad hoc network are infrastructure less networks where each node can communicate with other nodes those are in its access region. In MANETs each node

can act as a router. Due to mobility the nodes can collectively form a network and dissolve dynamically based on their requirement without having any centralized administration. In multicast routing, a source node simultaneously sends the same message to a group of destinations. In multicast routing a multicast tree is formed by connecting source node with all the destination nodes.

QoS multicast routing [12,8]. is to form a multicast tree where source node positioned at root and each path from source to destination nodes must satisfies QoS parameters. In QoS multicasting, Energy efficiency [6,5] and bandwidth [10] are the significant QoS parameters to be addressed. Bandwidth calculation at a node is a typical task, which is evaluated as a set of free time slots in TDMA process[17,18]. Nodes in the multicast routing rapidly drain out their battery power as they involve in the construction of multicast tree followed by sending multiple copies of data to set of destination nodes [11].

Due to lack of administration and nodes mobility, MANETs are vulnerable to attacks. A malicious node can degrade the performance of efficient routing protocols with its non cooperative activities[4]. Evaluation of node's reliability value is certainly advantage in MANETs where the applications are run securely by involving reliable nodes only [9]. A node reliability can be evaluated by either direct or indirect observation of its activities [2].

In multicasting, due to node mobility the constructed tree is frequently getting disconnected which requires energy consumption to reformation of the tree. Estimation of the link expiry time (LET) [21] for a pair of nodes is really helpful in the construction of multicast tree with stable routes from source to destinations.

When a routing protocol is handling multiple QoS parameters it becomes a challenging issue to assign priorities to them at runtime, which is purely context based. In some papers [3] this issue is discussed by assigning static weights to the parameters, but which is not suitable for the applications with dynamic nature.

In this paper, the proposed QoS Trust model considering QoS metrics bandwidth, energy, link expiry time and reliability. We are using fuzzy logic[14] to evaluate node trust value based on the QoS metrics. The protocol constructs the multicast tree with high trusted nodes. A node trust value represents not only its level of belief but also its capability in all contexts of handling of applications[1].

The main advantages of the proposed QoS trust model are

1. The scheme can minimize the number of path failures by pre computing node's energy levels and their mobility as per application requirements.
2. The scheme can attain good throughput by allowing higher band width links in the multicast tree construction.
3. The scheme can run the data transfer in secure mode, since it includes the reliable nodes in tree construction.

The remaining sections in the paper are organized as follows. In section 2, short discussions on Related work is presented. Estimation of the QoS metrics in the proposed model (bandwidth, data transmission energy, Link expiry time and node reliability) are discussed, fuzzy logic theory to calculate the node trust value is discussed, FQTM multicast routing protocol and its time complexity is presented in

section 3. Simulation environment setup and results analysis are discussed in Section 4. Finally the paper concludes in Section 5.

2. RELATED WORK

Multicast routing protocols mainly classified [7] into mesh based routing and tree based routing protocols. Mesh based protocols [16] creates mesh structure topology where source node is having multiple paths to destination nodes. In case of link failure alternative paths are used instead of reconstruction of mesh. But control overhead is high in maintenance of mesh structure. In tree based routing[15], multicast tree is established connecting source with set of destination nodes, where source is at root position and having unique path to every destination node.

In multicasting, nodes usually have scarcity of energy and bandwidth, which leads to network partition, link failures and delay in data delivery. To avoid these problems a multicast routing protocol is capable of establishing a multicast tree, with nodes having sufficient energy and links with required level of bandwidth. This chapter discusses MAODV[20] and PMRP[13] multicast routing protocols.

2.1. Multicast Ad Hoc On-Demand distance Vector Protocol (MAODV)

MAODV is the extension of the AODV protocol and finds the unique routes to set of destinations on demand. It uses the same packet formats of RREQ(route request) and RREP(route reply)packets that are used in AODV. Whenever a new node wants to become a member of multicast group or having data to share to multicast group, broadcast the RREQ packet to next hop neighbours. If a node receiving RREQ, is not a multicast group member or not having route information to the multicast group, then it rebroadcast the RREQ. If a node receiving RREQ is a multicast group member and having route information to multicast group with higher sequence number than in RREQ, then it sends route reply packet to the source node. when the RREP packet is back to source node, all the intermediate nodes along the route to source node updates both routing and multicast routing tables by adding entry for its neighbour node from which they got RREP.

The source node waits for some time to collect all the RREPs and selects the route with minimum hop count and higher sequence number to the nearest multicast group member. Then it enables the next hop node in its multicast routing table and sends MACT (multicast activation) message to that node. On receiving MACT, the current node updates its entry for source node in its multicast routing table. The current node selects the best next hop node towards the multicast tree and sends the MACT. This procedure continues till the MACT reaches the nearest member of the multicast tree. The member nodes of a multicast tree forwards the data only along the activated routes.

2.2. Power-Aware Multicast Routing Protocol (PMRP) With Mobility Prediction

Route Discovery Process in PMRP: PMRP is the extension of the MAODV multicast protocol with node mobility prediction. It uses the GPS system to predict the node mobility. This protocol works based on three parameters termed as $P_{prediction}$, P_{remain} and LET. On receiving RREQ packet, each node calculates the three parameters

where $P_{prediction}$ is the power required in forwarding source data[19], P_{remain} is the node's current remaining power and LET is the link expiry Time which is calculated based on the two nodes velocity and their mobility directions.

Whenever a source node wants to send data, it broadcast the RREQ by adding its location information. After receiving RREQ an intermediate node will calculates the P_{remain} and $P_{prediction}$ parameters. If the calculated P_{remain} is less than $P_{prediction}$, then the node drops that RREQ packet. Otherwise it calculates the LET and places that information in RREQ packet before forwarding. Once RREQ packet reaches the destination node, it contains all the nodes information and LETs along the path to source node. Every destination node waits for some time to collect all the RREQ packets, then selects the RREQ packet with higher RET(Route Expiry Time) value and sends back RREP to the source node along the same route. RET value is equal to the minimum of all LETs along the route to source.

3. FUZZY BASED QoS TRUST MODEL (FQTM)

The proposed QoS trust model is a combination of the following components as shown in Figure 1.

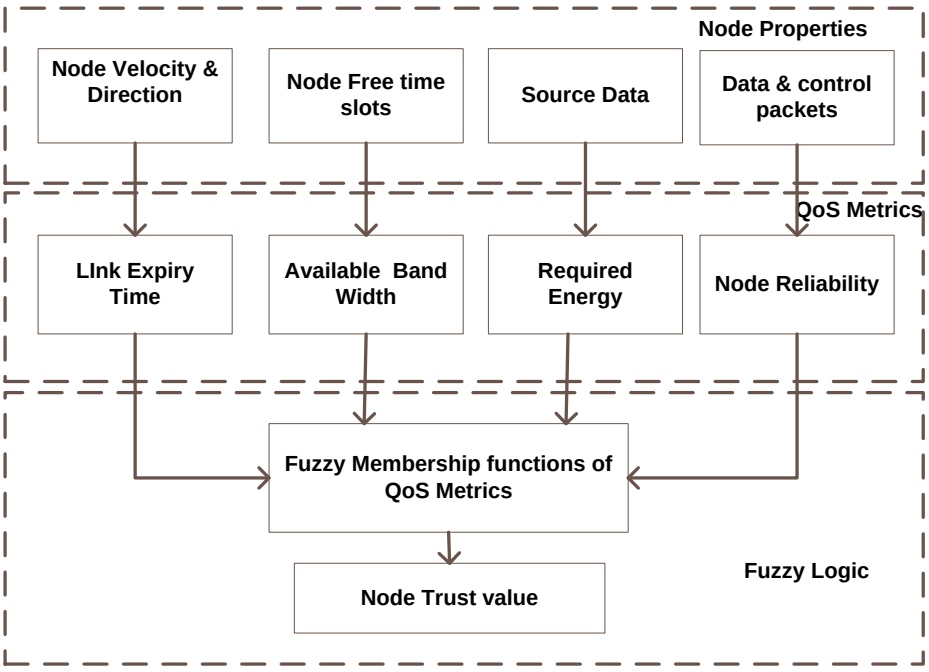


Figure 1: Fuzzy Inference QoS trust model

- Node properties
- Evaluation of QoS parameters
- Fuzzy logic inference of node trust value

The proposed method is the extension of MAODV, where a node can gather neighbour information by exchanging HELLO packets like node velocity, direction, free time slots, source data size. A node QoS metrics are computed using these metrics. In the fuzzy inference system, QoS parameters are considered as fuzzy input variables and using fuzzification and defuzzification methods a node trust value is evaluated which is in turn used in formation of multicast tree.

This section further describes the evaluation methods of each QoS parameters and fuzzy inference theory in calculating node trust value, finally presents the multicast route discovery mechanism and algorithm over a example network.

3.1Estimation of link Expire Time (LET)

Consider two nodes A and B within the same coverage area with the range of r. Let (x_1, y_1), (x_2, y_2) are the locations of the nodes A and B respectively, Assume v_1 and v_2 are the velocities, θ_1 and θ_2 $(0 \leq \theta_1, \theta_2 < 2\pi)$ are the directions of node A and B. In equation (1), the duration of link between A and B is estimated as,

$$LET = \frac{-(ab+cd)+\sqrt{(a^2+c^2)r^2-(ad-cb)^2}}{(a^2+c^2)} \quad (1)$$

where $a = v_1 cos\theta_1 - v_2 cos\theta_2$, $b = x_1 - x_2$, $c = v_1 sin\theta_1 - v_2 sin\theta_2$ and $d = y_1 - y_2$.

3.2.Node Energy Calculation

In MANETs every node has to spend some energy E_{ele} to enable the transmitter or receiver and E_{amp} is the amount of energy utilized by the amplifier in forwarding packets. A node has to spend $E_{Tx}(k, d)$ energy in transmitting a k-bit data over d distance.

$$E_{Tx}(k, d) = E_{amp} \times k \times d^2 + E_{elec} \times k$$

A node has to spend $E_{Rx}(k)$ energy in receiving k bit message

$$E_{Rx}(k) = (E_{ele} \times k)$$

Total energy consumed in forwarding k bit data over d distance d is

$$E_{total}(k) = E_{amp} \times k \times d^2 + 2 \times (E_{ele} \times k) \quad (2)$$

3.3.Band width Calculation using TDMA

In Graph Theory, a MANET is represented as a graph $G = (N, L)$, where N is the set of mobile nodes and L is the set of wireless links. For a mobile node n_i, the set of neighbours is represented as $NB_i = \{n_j \in N: (n_i, n_j) \in L\}$. In TDMA band width is represented in the form of time slots $S = \{s_1, s_2, s_3, \ldots . s_m\}$. For a node n_i, the

transmission schedule TS_i is the set of slots where node n_i can transmit, and RS_i is the set of slots where node n_i can receive from its neighbour.

A node n_i can transmit data to neighbour node n_j in time slot s_t, if the following conditions are satisfied.

1. Time slot s_t is not scheduled for either sending or receiving at nodes n_i or n_j.
2. For any 1-hop neighbour n_k of n_i, slot s_t is not scheduled for n_k as receiving slot $TS_i = \{s_t \in S:\ s_t \notin TS_i,\ s_t \notin RS_i, s_t \notin \cup_{n_k \in NB_i}\ RS_k\}$

A time slot $s_t$can be used by a host n_i to receive data from neighbour node n_j, if the below conditions are met

1. Time slot s_t is not scheduled for either sending or receiving at node n_i nor n_j.
2. For any 1-hop neighbour n_k of n_i, slot s_t is not scheduled for n_k as transmission slot. $RS_i = \{s_t \in S:\ s_t \notin TS_i,\ s_t \notin RS_i, s_t \notin \cup_{n_k \in NB_i}\ TS_k\}$

In the Figure 2, The multicast tree is created with the nodes S, A, B, C, D, E and F, where S is the source node and E,F and C are Destination nodes. In this tree the nodes C, D and F are the neighbours of B and during data communication the available bandwidth is shared among these nodes. According to TDMA, the shared bandwidth at node B is calculated as, the set of free slots between B and F is {5,7}, free slots between B and C is {5,6,7}, and free slots between B and D is {7}. Since 7th slot is the common slot in all neighbour nodes of B, it can send data in 7th slot.

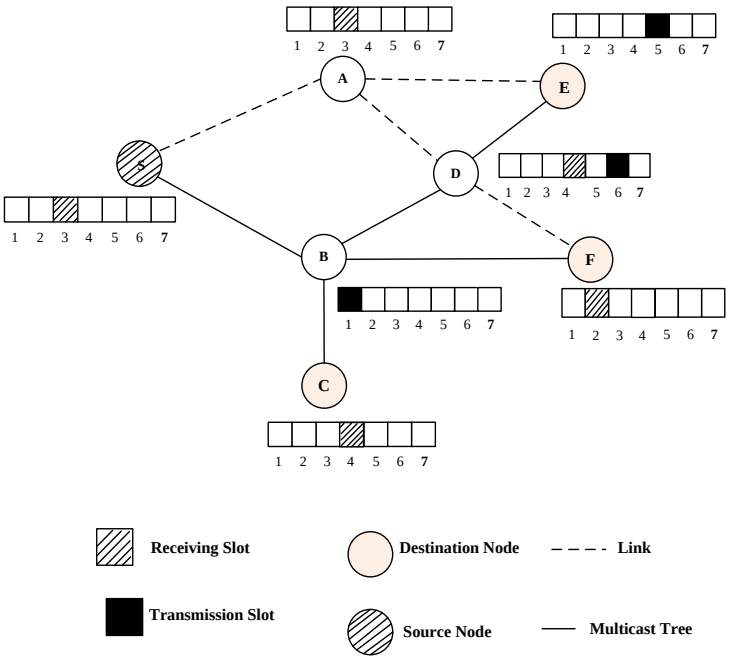


Figure 2: Bandwidth calculation using TDMA

3.4 Node reliability

We evaluate reliability *r* in the proposed scheme by a real number with a continuous value between 0 and 1. A Reliability value can be calculated from direct observation by using Bayesian inference.

In the direct observation, reliability values can be evaluated on two malicious behaviours: dropping packets and modifying packets, we assume that each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviours of the observed node. By applying the Bayesian inference, the observer node can estimate the reliability of its neighbours.

The reliability is a random variable as a degree of belief, which is represented as r, $0 \leq r \leq 1$. In Bayes' theorem, the node reliability r is estimated like:

$$f(r, y/x) = \frac{P(x/r\,, y) f(r, y)}{\int_0^1 P(x/r\,, y) f(r, y) dr}$$

Here y is the total number of packets reached the node, x is the number of packets transmitted correctly, and $P(x/r\,, y)$ can be represented as a binomial distribution:

$$P(x/r\,, y) = \binom{y}{x} r^x (1-r)^{y-x}$$

$f(r, y)$ can be described using Beta distribution as

$$Beta(r; \alpha, \beta) = \frac{r^{\alpha-1}(1-r)^{\beta-1}}{\int_0^1 r^{\alpha-1}(1-r)^{\beta-1} dr}$$

where $\alpha > 0, \beta > 0$. Then,

$$f(r, y|x) = \frac{\binom{y}{x} r^{\alpha+x-1}(1-r)^{\beta+y-x-1}}{\left(\int_0^1 P(x/r\,, y) f(r, y) dr\right)\left(\int_0^1 r^{\alpha-1}(1-r)^{\beta-1} dr\right)}$$

i.e $f(r, y|x) \cong \text{Beta}(\alpha + x, \beta + y - x)$

The expectation of node reliability is

$$E[r] = \frac{\alpha}{\alpha + \beta}$$

In the above beta function, the parameters can be represented iteratively as $\alpha_n = \alpha_{n-1} + x_{n-1}$ and $\beta_n = \beta_{n-1} + y_{n-1} - x_{n-1}$. Initially, there are no

observations i.e $\alpha_0 = \beta_0 = 1$, so the node reliability is 0.5. The node reliability is represented as a iterative function like.

$$E_n[r] = \frac{\alpha_n}{\alpha_n + \beta_n}$$

3.5Fuzzy inference system to evaluate node trust values

The node trust value is calculated using fuzzy inference mechanism, which considers the node residual energy, bandwidth, LET and reliability factors as input parameters.

3.5.1 Fuzzy logic system

Fuzzy logic is reasoning with qualitative information. The objective of the fuzzy control system is to replace a skilled human operator with a fuzzy inference rule-based system. In Figure 3, main phases of the fuzzy logic are described.

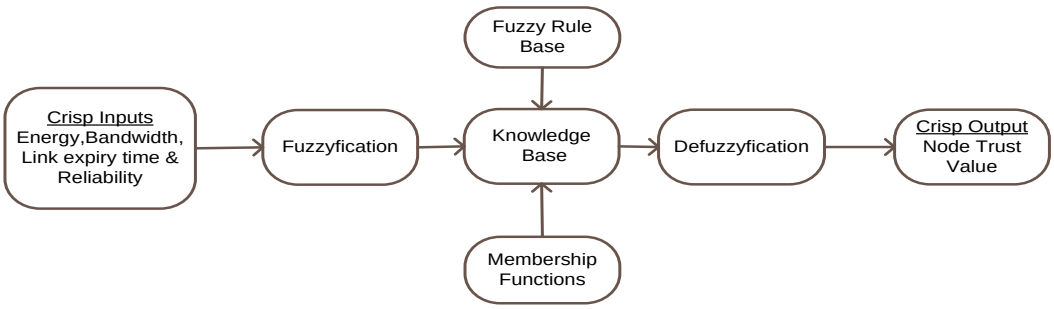


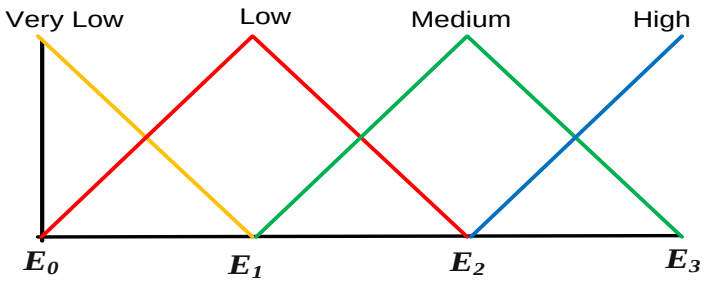
Figure 3: Fuzzy Logic in FQTM

3.5.2 Fuzzification

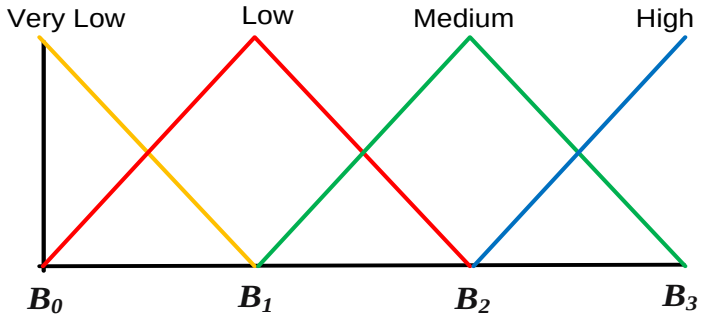
Fuzzification is the approach, which converts crisp input values into degree of membership value of linguistic terms for input variable. In the proposed method, we consider the QoS metrics Bandwidth, Energy, LET and reliability as fuzzy input variables, and the node trust value is the fuzzy output variable.

3.5.3 Fuzzy membership functions

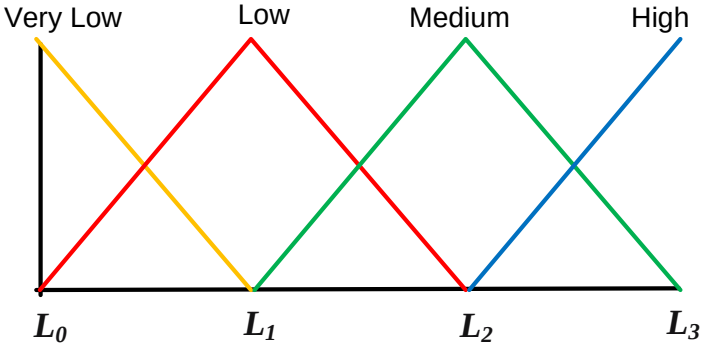
In Figure 4, the fuzzy input variables energy, bandwidth, LET and reliability are divided into four fuzzy sets like, very Low, Low, Medium and High. The fuzzy output variable ‘node trust’ is evaluated with the same fuzzy sets. Here the triangular membership function is used to measure the fuzzy sets of Input and output variables. The membership function of trust is similar to the reliability.



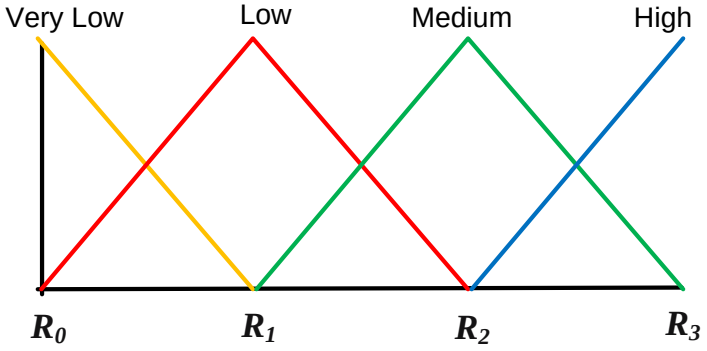
(a) Energy membership function



(b) Bandwidth membership function



(c) LET membership function



(d) Reliability membership function

Figure4: Triangular membership functions of fuzzy input variables

3.5.4Rule Base

Rule base is the repository of rules, those are framed on the combinations of fuzzy sets of input variables. Each rule appears in the format of ' IF-THEN'. Here each fuzzy input variable is having 4 fuzzy sets, so the fuzzy rule base can be defined with the maximum of 256($4 \times 4 \times 4 \times 4$) rules. For convenience in the below table 1, we are presenting 8 rules.

TABLE 1: Fuzzy Rule base

Energy	***LET***	***Bandwidth***	***Reliability***	***Trust***
High	*High*	*High*	*High*	*High*
High	*Medium*	*High*	*High*	*High*
Medium	*Low*	*Medium*	*High*	*Medium*
High	*Medium*	*Medium*	*High*	*Medium*
Medium	*Low*	*Medium*	*Very Low*	*Low*
Low	*Medium*	*Low*	*Low*	*Low*
Very Low	*Medium*	*Very Low*	*Medium*	*Very Low*
Very Low	*Very Low*	*Very Low*	*Very Low*	*Very Low*

3.5.5 Fuzzy Inference System

Fuzzy inference system is an intelligent component, which is having the decision making capability based on fuzzy rule base. In the below example, the Max-Min rule of composition is used to infer the result from the rule base.

In the Figure 5 with the help of an example scenario, evaluation of node trust is presented. Here the fuzzy sets of QoS parameters are defined as in table 2 (the values are taken from simulation environment).

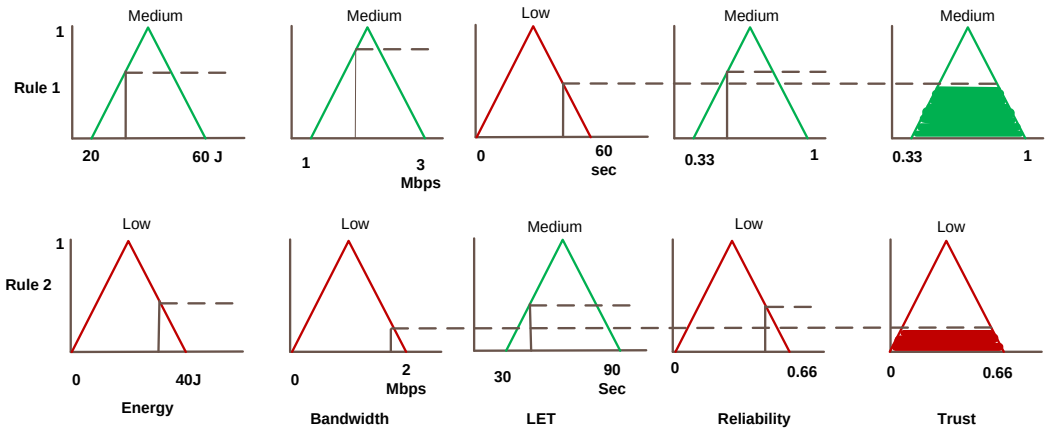


Figure 5: Example of node trust evaluation

TABLE 2: Fuzzy sets of QoS parameters

QoS Vs Fuzzy Sets	Very Low	Low	Medium	High
Energy (J)	0-20	0-40	20-60	40-60
Bandwidth (Mbps)	0-1	0-2	1-3	2-3
LET (Sec)	0-30	0-60	30-90	6-90
Reliability	0-.33	0-.66	.33-1	.66-1

The node trust value is evaluated over two rules from table 1.

1. *Rule 1: If(energy is Medium, Bandwidth is Medium, LET is Low and Reliability is Medium) then (Trust is Medium)*
2. *Rule 2: If(energy is Low, Bandwidth is Low, LET is Medium and Reliability is Low) then (Trust is Low)*

Let the crisp values for the fuzzy input variables are like Energy (32 J), Bandwidth (1.8 Mbps),LET(42 sec) and Reliability(0.528). For each crisp input value, degree of membership (μ) is evaluated. According to max-min rule of composition, shaded portions from two rules of the trust variable are combined and the maximum portion is considered as the fuzzy set of the trust variable as shown in Figure 6.

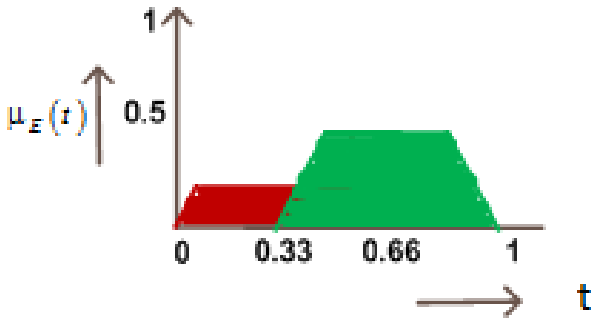


Figure 6: Defuzzificaion of node trust value

3.5.6 Defuzzification

Difuzzification is the process of converting a fuzzy set into crisp set. Here the centre of gravity (COG) method is used for converting fuzzy set value to crisp value for the trust fuzzy variable.

$$COG = \frac{\int_0^1 \mu_E(t)\, t\, dt}{\int_0^1 \mu_E(t)\, dt}$$

$$COG = \frac{(\int_0^{0.06}(.3t)\, t\, dt + \int_{0.06}^{0.39}(.2)\, t\, dt + \int_{0.39}^{0.52}.2 + 2.3(t-.39)tdt + \int_{0.52}^{0.64}(.5t)\, t\, dt + \int_{0.64}^{1}(1-t)\, t\, dt)}{(\int_0^{0.06}(.3t)\, dt + \int_{0.06}^{0.39}(.2)\, dt + \int_{0.39}^{0.52}.2 + 2.3(t-.39)dt + \int_{0.52}^{0.64}(.5t)\, dt + \int_{0.64}^{1}(1-t)\, dt)} \quad (3)$$

In Figure 6, the COG is calculated as in equation (3), and the Node trust value is estimated as 0.58.

3.6 Multicast routing in FQTM.

3.6.1 Route Discovery Process

1. Step 1: whenever a source node want to send data to group members, first it sets the RREQ packet with required QoS threshold values based on application requirements(using equation(2), energy threshold value is calculated). After a neighbour node receives a RREQ packet, it calculates the residual Energy, expiry time and bandwidth of the link to the upstream node from which it got the RREQ packet. It's reliability value computed by previous hop evaluator node. If the computed values are not greater than threshold values set by the source node, i.e it is not capable of handling the application so it drops the RREQ packet.
2. Step 2: If the computed QoS metrics are greater than threshold value, then intermediate node estimates its trust value using fuzzy inference system by considering estimated QoS values as fuzzy input variables. Node adds evaluated trust value and its ID to the RREQ packet and forwards to the next hop neighbours
3. Step 3: Each destination node waits for some time to receive all the RREQ packets. The destination node evaluates the Route Trust(RT) value, through which it got the packet. Route trust value is the product of all intermediate node's trust values except the destination node, since the destination node will not forward any packets further. Every destination node chooses the route with the maximum RT, and sends the RREP packet to the source node along the selected routing path. On receiving RREP packets, the intermediate nodes update their routing and Multicast tables.

3.6.2 Join process

Whenever a node is interested to share data or join a multicast group, it sends a join request packet to all the next hop neighbours. If the neighbour is an existing multicast member, then it responds by sending join reply. If a node is not a member and is not aware of a route to that group, it verifies whether its QoS metrics (energy, bandwidth, LET and reliability) are greater than the threshold values set by the initiator node. If the metrics are less than the threshold values then it discards the join request, otherwise estimates the trust value using fuzzy inference system. It adds the trust value to the join request packet and then broadcasts it to its neighbours. Each multicast tree member node waits for a time to receive the join request packet, selects the path with maximum route value from initiator node, and unicasts the join reply packet. On receiving all join reply packets, the initiator node will select the route with maximum trust value to the nearest multicast tree node.

3.7 Algorithm of multicast routing in FQTM

Algorithm 1: Route Discovery Process

Let assume a MANET with n number of nodes, where N represents the set of MANET node s like $N = \{N_1, N_2, N_3, \ldots, N_n\}$. N_s *is the source node,* N_d *is the destination node and* N_j *is an intermediate node. To form a multicast tree to all destination nodes* N_d, *Source node*

N_s sends RREQ to all next hop intermediate nodes N_j.
if (Node N_j is not the destination node N_d)

{

(1) Node N_j calculates the QoS metrics node energy(e), reliability(r), link Bandwidth (b) and expiry time(et). If the metrics are lower than the threshold values, it drops the RREQ packet.

(2) Otherwise Node N_j evaluates $\mu_{A_i}(e)$, $\mu_{B_i}(r)$, $\mu_{C_i}(b)$, $\mu_{D_i}(et)$ and the node trust value is

$$\mu_{E_i}(Trust) = min\left\{\mu_{A_i}(e), \mu_{B_i}(r), \mu_{C_i}(b), \mu_{D_i}(et)\right\}$$

$$\mu_E(Trust) = max\left\{\mu_{E_i}(Trust)\right\}$$

$$where\ 1 \leq i \leq (f1 \times f2 \times f3 \times f4)$$

Using defuzzification, trust value of N_j is evaluated, i.e TV_{N_j}.

(3) Node N_j adds its trust value (TV_{N_j}), ID to the RREQ packet and forwards to the neighbouring nodes.

}
else
{// *N_j is the one of destination nodes N_d*

(1) Node N_d waits for some time to receive RREQ packets. Based on intermediate node trust values, it finds the Route trust (RT) value.

$$RT = \prod_{N_j \in P,\ N_j \neq N_d} TV_{N_j}$$

(2) Node N_d chooses the route with the Maximum RT value and sends a RREP packet through that route to the source node. If two paths are identified with equal RT, then shortest path will be chosen.

(3) Each intermediate node N_j receives the relay packet, updates its routing and multicast tables.

(4) On receiving of RREP packets, source node N_s forms multicast tree to the destination nodes N_d

3.8 An example of FQTM multicast routing

In Figure 7, whenever the source node S wants to share data with the target nodes E, F and C. It sets the RREQ packet with threshold values of QoS metrics in the sequence of (Energy, Bandwidth, LET, Reliability) and send to next hop neighbours X, Y and

Z. Lets the threshold values are (20,1,30,0.6). On receiving of RREQ packet, the nodes X,Y and Z calculates their QoS metrics as (55,2,80,0.8),(50,2,70,0.7) and (15,1,25,0.5) respectively. But only X and Y are having enough QoS metrics, so the nodes X and Y updates RREQ packet with its ID and trust value (evaluated using fuzzy inference logic) and forwards to next hop neighbour. Since Z is not having enough QoS metrics, it drops the RREQ packet.

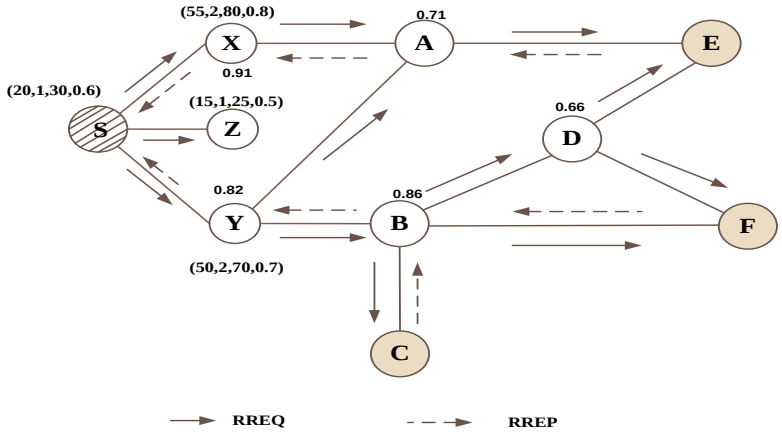


Figure 7: Route Discovery in FQTM

Every destination node receives the RREQ packet with node's ID and trust values through which it has come across. the destination node E receives RREQ packets through the routes (S,X,A,), (S,Y,A) and (S,Y,B,D) with trust values.64,.58 and.46 respectively, node E selects the (S,X,A) as a primary route and sends the RREP packet in that path to source. Likewise node F and C selects the route (S,Y,B) with trust value 0.7. Finally the source node constructs the multicast tree as shown in Figure-8. Table 3 describes the notations used in FQTM and algorithm.

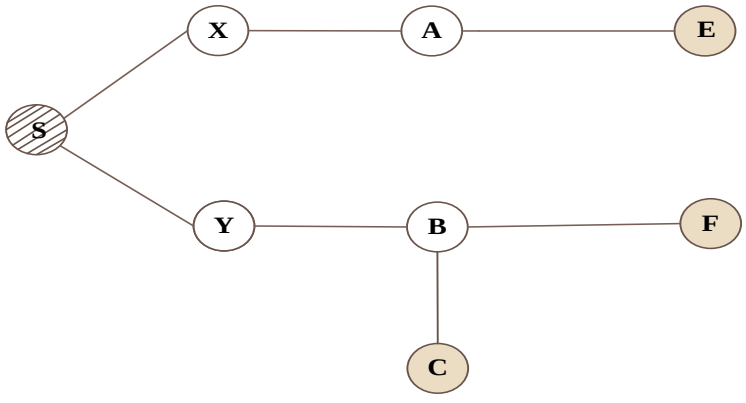


Figure 8: Multicast Tree in FQTM

TABLE 3: Notations used in FQTM

Notation	Meaning
n	*Number of nodes in the network*
m	*Avg number of neighbors*
p	*Number of packets forwarded through a node.*
f_1, f_2, f_3, f_4	*Number of fuzzy sets of energy, Reliability, bandwidth and LET*
$\mu_{A_i}(e)$,$\mu_{B_i}(r)$, $\mu_{C_i}(b)$, $\mu_{D_i}(et)$, $\mu_{E_i}(Trust)$	*Degree of membership of the energy, reliability, bandwidth, expiry time and trust respectively*

3.9 Theoretical analysis of FQTM

In Table 4, a node has to exchange Hello packets to get its m neighbours information, so it is the order of $O(m \times n)$ in the network. On sending P (data & control) number of packets to each of its m neighbours, a node can calculate the neighbour node reliability value as $O(p \times m \times n)$. After receiving RREQ packet, a node calculates the QoS metrics. In the network, every link carries unique RREQ packet, so the number of RREQ packets is the order of links in the network $O\left(\frac{n(n-1)}{2}\right)$ i.e $O(n^2)$. The proposed fuzzy Rule base is having maximum of f^q number of rules, where f is the number of fuzzy sets and q is the number of QoS parameters.

TABLE 4: Time and control overhead in FQTM

Event	Time complexity	Network control overhead
Neighbour monitoring	$O(m \times n)$	*Uses the hello messages*
Reliability Computation	$O(p \times m \times n)$ *// on sending every packet, a node monitors its neighbour node.*	$O(n^2)$ *// on receiving of RREQ packet, a node sends a message to evaluator for its reliability value*
QoS Metrics Estimation	$O(n^2)$ *// on receiving RREQ packet, a node estimates QoS metrics.*	*// Uses the existing Hello massages to get bandwidth and velocity of upstream node on receiving RREQ packet.*
Fuzzy Inference of trust value	$O(f_1 \times f_2 \times f_3 \times f_4)$ *//the rule base is having these many number of rules*	*//No messages required*

4. SIMULATION

This section describes the simulation environment in which results are taken and parameters are defined. The simulation runs on MAODV, PMRP protocols and proposed method FQTM. Performance of the protocols are analysed in the graphs.

4.1 ***Simulation Environment***

The simulation is run on ns2 (2.34) tool. The area of the simulation is 1400 X 1400, Network size that varies with 10 to 60 nodes, node velocity is considered from 0 to 40 m/sec, node transmission range is 250m, data packet size is 0.3MB, data transmission rate is maximum of 2 Mbps, node initial energy is set to 60J and the simulation is conducted for 600sec.

4.2 Simulation parameters

1 *Average packet delay:* The total time taken for all the data packet to reach at destination nodes divided by the number of packets delivered at the destination nodes.

2 *Throughput:* the number of data packets delivered at destination nodes per unit time

3 *Control overhead:* the ratio between the control packets transmitted and the data packets delivered

4.3 Simulation Results:

Impact of node velocity:

In simulation, the Average Packet delay, Throughput and Control overhead parameters are compared based on node velocities varying from 0-40 m/sec and the network size is fixed with 20 nodes.

In Figure 9, It is observed the average packet delay is increasing with the increasing node velocities. If the node velocity increases, then the number of link breaks also increases. In case of link failure packets are queued and forwarded after the path is re-established. The proposed method FQTM can construct the multicast tree with stable links by considering node energy levels and their location information, so it can reduce the number of link failures and hence can attain the minimum average packet delay comparatively with remaining two protocols.

Figure 10 describes the throughput (packets delivered in unit time) for three protocols. Throughput decreases with increasing node velocities. The proposed protocol FQTM improves the throughput by considering the band width in the estimation of node trust values.

Figure11 is showing comparison for control overhead parameter for three protocols. Control overhead increases with increasing node velocities.

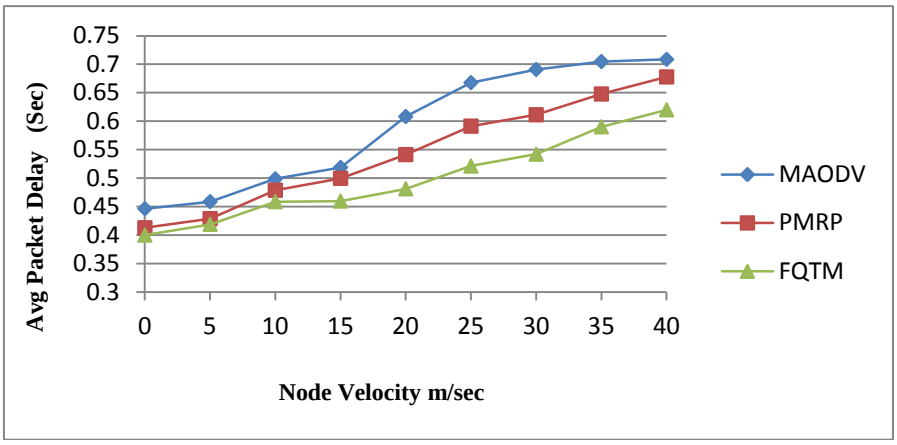


Figure 9. Avg packet delay verses node velocity

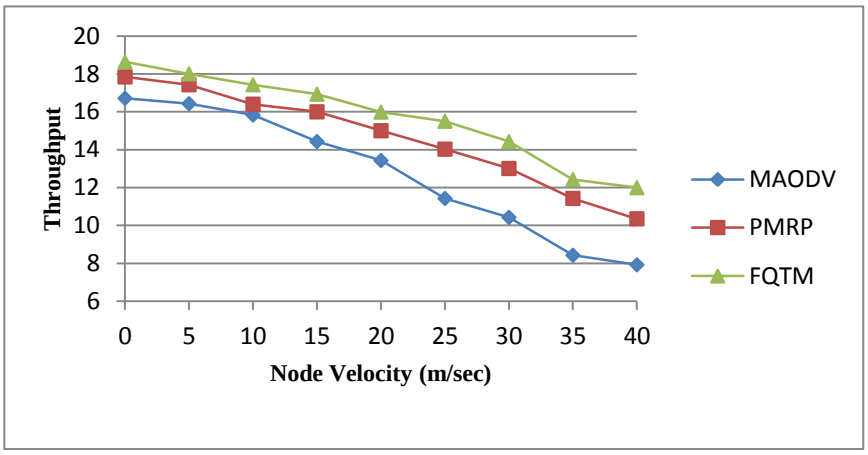


Figure10. Throughput verses node velocity

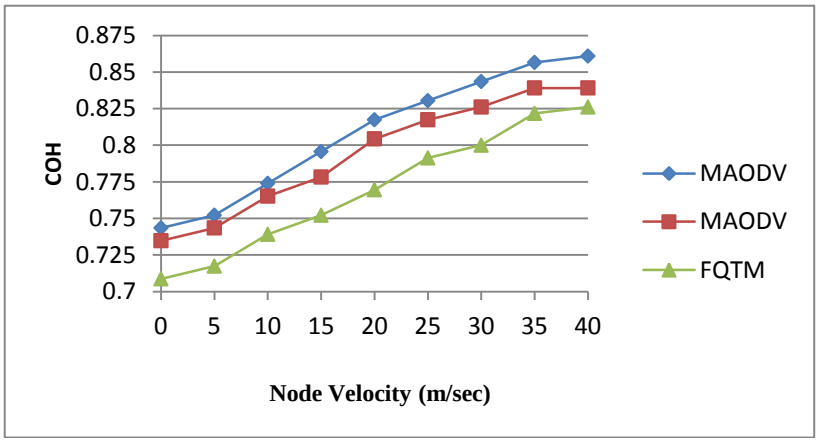


Figure11. Control overhead verses node velocity

When the route is disconnected, the nodes have to transmit the control packets for reestablishment of routes. The proposed protocol FQTM outperforms the remaining protocols by maintaining the minimum number of link failures.

Impact of network size:

In simulation, the Average Packet delay, Throughput and Control overhead parameters are compared based on network size varying from 10-60 mobile nodes and the node velocity is fixed with 10 m/sec.

Figure 12 depicts the performance comparison of three protocols for the parameter average packet delay with respect to network size. The average packet delay is increased with increasing network size. If the network size is increased, then the maintenance process time is increased for every node along the path. The FQTM some of the control packets (RREP) for even load balancing of nodes along the path, so it achieves the better performance than MAODV and PMRP.

In Figure 13, throughput parameter is evaluated. Throughput is decreasing with increasing network size, since route maintenance phase takes long time. The FQTM allowing only reliable nodes along the routes so it can reduce the packet drops and hence improves the throughput values comparatively.

In Figure 14, Control overhead is slightly decreasing with increasing network size. The FQTM gives better results by maintaining routes with stable links.

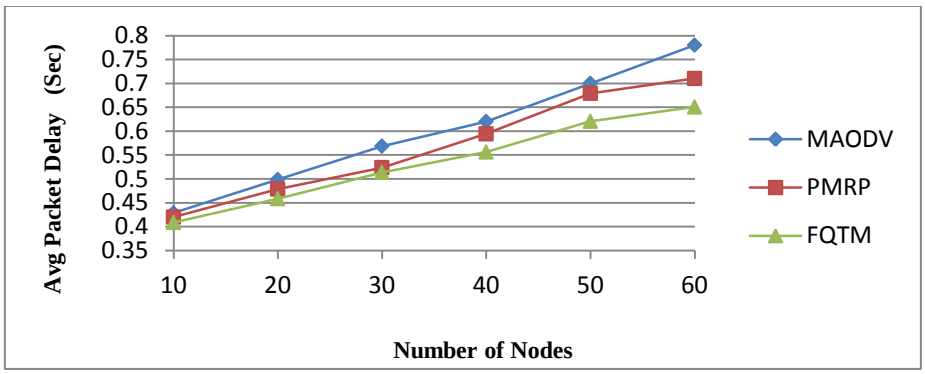


Figure 12. Average packet delay verses number of nodes

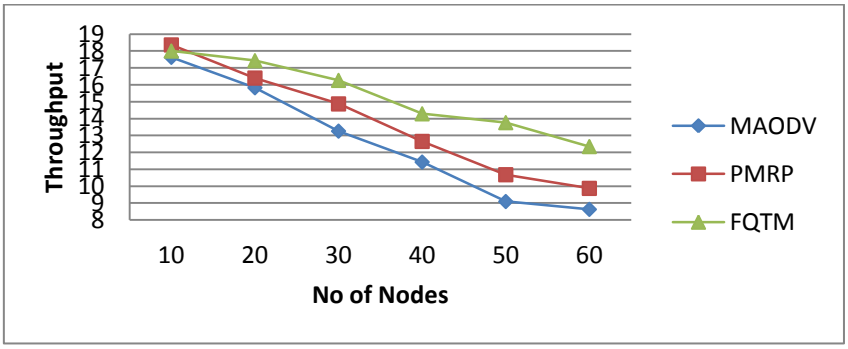


Figure 13.Throughput verses number of nodes

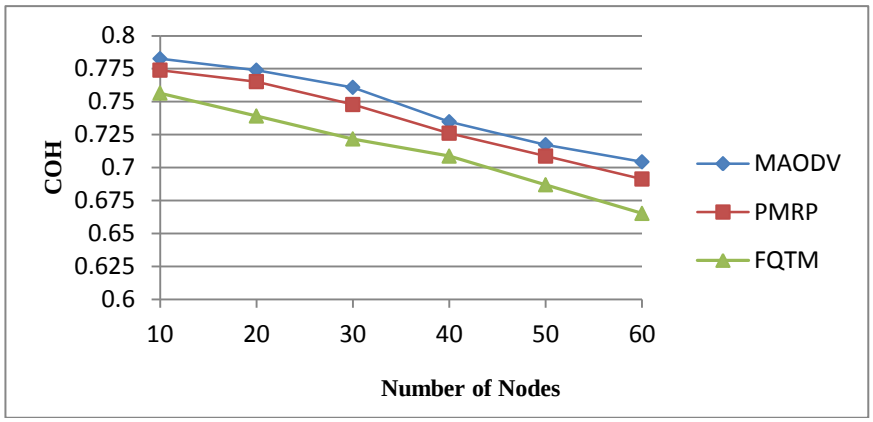


Figure 14. Control overhead verses number of nodes

5. CONCLUSION

The proposed model FQTM considers energy, link expiry time, bandwidth and reliability as QoS metrics for multicast routing in MANETs. Using fuzzy logic, the balance among the QoS parameters is achieved. The multicast protocol evaluates the node trust value by applying fuzzy inference rules over QoS parameters. The protocol constructs the multicast tree with high trusted nodes from source to set of destinations. So the routes from source to destination retain stable links and long life time, which can reduce the path breaks and hence control overhead. Since the node reliability is taken into consideration, a source node can do the data transmission in secure environment. The protocol performance is analysed theoretically and practically. The simulation results proved that the proposed method outperformed the MAODV and PMRP protocols.

REFERENCES

[1] Fei Hao; Geyong Min; Man Lin; Changqing Luo; Yang, L.T. 2014, "MobiFuzzyTrust: An Efficient Fuzzy Trust Inference Mechanism in Mobile Social Networks", IEEE Transactions on Parallel and Distributed Systems, vol.25, no.11, pp.2944-2955.

[2] Zhexiong Wei; Tang, H.; Yu, F.R.; Maoyu Wang; Mason, P., 2014 "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning," IEEE Transactions on Vehicular Technology, vol.63, no.9, pp.4647-4658.

[3] Sirisala, NageswaraRao.; C.Shoba Bindu. 2014 "Weightage based trusted QoS protocol in Mobile Adhoc Networks", IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp.283-287.

[4] Lei Ju, Edwin H. M. Sha, Hui Xia, Zhiping Jia, Xin Li, 2013 "Trust prediction and trust-based source routing in mobile ad hoc networks" Ad Hoc Networks Elsevier,Vol. 11, No. 7, pp. 2096-2114.

[5] Ruifeng Zhang, Olivier Berder, Jean-Marie Gorce, Olivier Sentieys 2012 "Energy–delay trade off in wireless multihop networks with unreliable links",,Ad Hoc Networks v10, pp1306–1321.

[6] Nicola Costagliola · Pedro Garçia López ·Francesco Oliviero · Simon Pietro Romano, 2012 "Energy- and Delay-Efficient Routing in Mobile Ad Hoc Networks". Mobile Network Applications v17 pp:281–297.

[7] Luo Junhai, Ye Danxia, Xue Liu, and Fan Mingyu, 2009 "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks". IEEE Communications Surveys & Tutorials, (Volume:11, Issue: 1), Page(s):78 – 91.

[8] Mina Masoudifar, 2009 "A review and performance comparison of QoS multicast routing protocols for MANETs" Ad Hoc Networks 7(6), pp:1150–1155.

[9] Ben-Jye Chang and Szu-Liang Kuo, 2009 "Markov Chain Trust Model for Trust-Value Analysis and Key Management in Distributed Multicast MANETs", IEEE Transactions on Vehicular Technology, vol.58, no.4, pp.1846-1863.

[10] Chia-Cheng Hu, Eric Hsiao-Kuang Wu, Gen-HueyChen, 2008 "bandwidth-Satisfied Multicast Trees in MANETs", IEEE Transactions On Mobile Computing, Vol. 7, No. 6,pp:712-723.

[11] Guo, S. 2007 "Energy-aware multicasting in wireless ad hoc networks: A survey and discussion', Computer Communications", Volume 30 Issue 9, Pages 2129-2148.

[12] Huayi Wu, Xiaohua Jia, 2007 "QoS multicast routing by using multiple paths/trees in wireless ad hoc networks", Ad Hoc Networks Volume 5 Issue 5, pages 600-612.

[13] Nen-Chung Wang, Yung-Fa Huang · Yu-Li Su 2007 "A Power-Aware Multicast Routing Protocol for Mobile AdHoc Networks With Mobility Predictio", Wireless Personal Communications, Vol 43:pp.1479–1497.

[14] Jing Nie, Jiangchua Wen, Ji Luo, Xin He, Zheng Zhou 2006 "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks", Fuzzy Sets and Systems, Volume 157, Issue 12, 16 Pages 1704-1712.

[15] Baolin, S. and Layuan, L. 2005 "On the reliability of MAODV in ad hoc networks", IEEE international symposium on microwave, antenna, propagation and EMC technologies for wireless communications, Vol. 2, pp. 1514–1517.

[16] Das, S. K., Manoj, B. S., & Murthy, C. S. R. 2002 "A dynamic core based multicast routing protocol for adhoc wireless network", In Proceedings of the third ACM international symposium on mobile ad hoc networking and computing, pp. 24–35.

[17] Kuei-Ping Shih. 2002 "A TDMA-based bandwidth reservation protocol for QoS routing in a wireless mobile ad hoc Network", IEEE International Conference on Communications Conference Proceedings ICC (Cat No 02CH37333) ICC-02.

[18] Zhu, C. and Corson, M. S. 2000, "Bandwidth Calculation in a TDMA-based Ad Hoc Network," Institute for Systems Research (ISR), Technical Reports: TR 2000-47, http://hdl.handle.net/1903/6173.

[19] Heinzelman, W. R., Chandrakasan, A., & Baladrishnan, H. 2000. "Energy-efficient routing protocols for microsensor networks". Proceedings of the 33rd Hawaii international conference on system sciences, Vol. 8, pp.1–10.

[20] Royer, E.M. & Perkins, C. E. 1999 "Multicast AODV". In Proceedings of the ACM MOBICOM, pp. 207–218,.

[21] Rappaport, T. S. 1996 "Wireless Communications: Principles and practice". Upper Saddle River, NJ: Prentice-Hall.