Recommendations Based QoS Trust Aggregation and Routing in Mobile Adhoc Networks

Nageswararao Sirisala[1] and C.Shoba Bindu[2]

[1]CSE Dept, Vardhaman College of Engg, Hyderabad, India
[2]CSE Dept, JNTUACE, Anantapur, India

Abstract: In mobile adhoc netwotk (MANET), a node's quality of service (QoS) trust represents how much it is reliable in quality. QoS trust of a node is computed based on its multiple quality parameters and it is an interesting and challenging area in MANETs. In this work, QoS trust is evaluated by taking into consideration quality parameters like node residual energy, bandwidth and mobility. The proposed method "Recommendations Based QoS Trust Aggregation and Routing in Mobile Adhoc Networks-QTAR" is a frame work. Where the trust is established through four phases like QoS trust computation, aggregation, propagation and routing. The Dempster Shafer Theory (DST) is used for aggregation of trust recommendations. In the network, trust information is propagated through HELLO packets. Each node stores the QoS trust information of other nodes in the form of trust matrices. We applied matrix algebra operations on trust matrices for route establishment from source to destination. The time and space complexity of proposed method is discussed theoretically. The simulation is conducted for the varying of node velocity and network size, where the proposed method shown considerable improvement over existing protocols.

Keywords: Quality of Service, Trust, Aggregation, Mobile Adhoc Networks.

1. Introduction

A group of wireless mobile nodes form a temporary network called a mobile Adhoc network (MANET), where a node can communicate with other nodes those are in its access region. Due to MANETs can be deployed quickly and easily, it became as a suitable communication network for the applications like battle fields, emergency and rescue operations.

Provisioning of QoS in mobile adhoc networks is a complicated task when compared with wired networks, the reason is node mobility, lack of administration and limited available resources. In QoS routing protocol, the intermediate nodes should have the minimum required energy, bandwidth and stability to transfer the source data efficiently to destination node. By considering these constraints, a node's QoS trust is computed in this work.

A node computes the direct QoS trust for its 1-hop neighbours by estimating their available resources like residual energy [5,28], bandwidth [20] and stability [6,21], through the interactions. If the resources are more than threshold level, then QoS trust is incremented, otherwise decremented. By aggregating 1-hop neighbour's trust recommendations, the indirect trust of 2-hop neighbours is computed. Here the Dempster Shafer Theory (DST)[8,24] is used for aggregation of trust recommendations. DST can reduce the impact of biased recommendations in indirect trust computation.

A node maintains trust information in the form of $n \times n$ trust matrix, where n is size of the network (number of nodes). Computed trust values should be propagated through the network, so that other nodes can avoid their risk in recomputation of trust for multihop away nodes. The computed trust values get propagated through the HELLO packets in the network.

In routing, the intermediate node's QoS trust values from source to destination are computed based on trust transitive rule(If A trusts B and B trusts C ; then A trusts C) . Using this rule ,we applied matrix algebra operations over trust matrices for route establishment.

In this paper, we did proper literature survey of different QoS trust parameters and their computation methods in MANETs perspective. In our proposed trust system, we evaluated node's trust value based on its Quality resources like bandwidth, energy and bandwidth. We applied dempster Shafer method in MANETs for combining trust recommendations. In unicast routing, we introduced iterative based trust matrix operations to compute trusted route from source to destination node.

The further sections in the paper are organised as follows. In section2, the existing methods of trust computation are presented. In section 3, the dempster safer method of trust combination is discussed and trust matrix operations are described. In section 4, the proposed method QTAR is presented as a combination of trust computation, aggregation, propagation and routing. Performance of proposed method is analysed theoretically. In section 5, simulation results of QTAR are explained. In section 6, the work is concluded.

In this work, the term Trust refers QoS Trust.

2. Related Work

In this section, we are discussing different author's trust handling methods that are proposed in MANETs.

Trust computation methods: The trust value of a neighbour node is evaluated based on packet forwarding ratio in [13,22], The misbehaviour factor of a neighbour node is evaluated for route request R_q, route reply R_p, route error R_e and data packets R_d. Each factor is computed based on number of such packets that are forwarded successfully and dropped. In [19] , trust value is evaluated as a combination of 3-parameters i.e (b, d, u). Here b, d and u refers belief, disbelief and uncertainty respectively. Every successful interaction with the neighbour node increments it's belief $(b = b + 1)$ and unsuccessful interaction increments the disbelief $(d = d + 1)$, where $b + d + u = 1$. In [27], beta distribution is used for trust computation based on number of packets, a node forwarded correctly among the total number of packets it received. Here α and β parameters are treated as good and bad experiences with that node. Some authors in

[7,9,10,15], used fuzzy logic for measuring node trust value. The trust management in MANETs is explained in [11]. In the paper [1], a node trust value is estimated using dynamic grey-markov chain model, which works based on nodes historical behaviour patterns. In [4] , the computed node trust value is validated by taking second hand information from trustable nodes usually called watchdogs . The second hand trust information , which is less than threshold deviation is used in final trust computation. In paper [2], a node's final trust value (FTV) is evaluated based on direct trust value (DTV) and indirect trust value (IDTV). DTV is computed based on packet forwarding ration, data consistency and time frequency. IDTV is computed based on recommendations of a node behaviour at particular time. In paper[3], trust is calculated based on similarity and time aging factors. Similarity factor between two nodes represents the relationship/similarity of their owning attributes. Aging factor represents the trust attenuation rate in successive time intervals.

Trust Aggregation methods: The work in [16] aggregated the gossips about a target node for deriving its trust value. Here, once the trustor node receives gossips/rumours from different nodes, it applies the push-sum operation as gossip average function. In [17], author used probability based methods for trust aggregation. Here two approaches are used i.e sequential and parallel aggregation methods. In sequential aggregation, the nodes trust values are aggregated from trust node to trustee node. In parallel method, trust values are gathered from different paths, these trust values are aggregated by assigning different weights to the paths.

Trust propagation methods: Social neighbourhood concept is used in[14] for trust propagation. Here the trustor node propagates trust value of trustee to 1-hop neighbour nodes, and then to 2-hop neighbours. Trust value is getting deducted by d-factor (based on forwarding nodes trust value) in every hop-by-hop propagation and this process continues till the propagated trust value reaches the threshold level. Graph theory based trust propagation method is used in [25]. Here the trust is propagated through transitive graphs using small world concept. In [12], the trust information is exchanged in the form of trust tickets. A node sends the trust request ticket and the provider replies through computed trust ticket. Both will meet at some common node (rendezvous) and from there, the trust value passed to the requester node.

Trust routing: TAODV [18], is a trust routing protocol, which establishes the trust worthy route to destination. It is a extension of AODV protocol, which uses the modified control packets TREQ(Trust request) and TREP(Trust reply). Source node sends the TREQ towards the destination, TREQ packets gather the trust information of intermediate nodes along the journey to destination. Once the destination receives the TREQ packets, it selects the TREQ with higher trust value and gives reply (TREP) to source node. Trusted-DSR[23] is the trust extension of DSR routing protocol. In which the source node's trust value gets incremented for every acknowledged packet and gets decremented for every retransmission of data. In [26], DyTR(Dynamic Trust) is proposed in terms of access control over the network .

3. System Model

In this section, some techniques are discussed like Dempster Shafer Theory (DST) and matrix algebra operations to make proposed method much clear in the next section.

3.1 Dempster shafer theory (DST)

DST works based on three metrics namely mass function (basic probability function-m), belief function (Bel) and plausibility function (Pl). Let $E = \{e_1, e_2, e_3\}$ be the set of all possible evidences under some consideration, then the power set of E ($i.e\ P(E)$) is the set of all sub sets of E, also referred as frame of discernment of E. i.e $\{\emptyset, \{e_1\}, \{e_2\}, \{e_3\}\{e_1, e_2\}, \{e_2, e_3\}, \{e_1, e_3\}, \{e_1, e_2, e_3\}\}$.

The mass function (m) maps every subset in frame of discernment to the range of values[0 1], i.e $m: P(E) \rightarrow$ [0 1]. Where it follows two conditions: $m(\emptyset) = 0$ and sum of mass functions of all subsets is 1 ($\sum_{B \in P(E)} m(B) = 1$).

If X is a set in the power set, then belief function of X is defined as $bel(X) = \sum_{C \subseteq X} m(C)$ and the plausibility of the set X in power set is defined as the sum of all the masses of the sets that intersect with the set$X$: $pl(X) = \sum_{C \cap X \neq \emptyset} m(C)$

3.1.1 Dempster's rule for combination

Let X is an element in frame of discernment, and $m_A(X)$, $m_B(X)$ are probability function values of two observer nodes A and B respectively. The combination of these two mass values $m_{A,B}(X)$ is calculated in eq(1).

$$m_{A,B}(X) = \frac{\sum_{P \cap Q = X} m_A(P) m_B(Q)}{1 - K} \qquad (1)$$

Here the constant K is defined as $K = \sum_{P \cap Q = \emptyset} m_A(P) m_B(Q)$

3.2 Trust matrix operations

In the network, each node maintains the trust information in the form of matrix (N^T) with order $n \times n$ where n is the number of nodes in the network,

$$N^T = \begin{pmatrix} t_{11} & \dots & t_{k1} & \dots & t_{n1} \\ \dots & & & & \dots \\ t_{1k} & \dots & t_{kk} & \dots & t_{nk} \\ \dots & & & & \dots \\ t_{1n} & \dots & t_{kn} & \dots & t_{nn} \end{pmatrix}$$

Here t_{ij} represents the trust value that node i has on node j. A node calculates the multi hop distance node's trust value by applying transitive rule (*transitive rule:* if node-i trust value of node-j is t_{ij} , node-j trust value of node-k is t_{jk} then node-i trust value of node-k is t_{ik}) towards that target node iteratively . t_i is the trust vector, having trust values of other nodes. i.e $t_i = [t_{i1} \dots t_{ik} \dots t_{in}]$. Calculation of t_i is represented as matrix operations in eq (2).

$$\begin{pmatrix} t_{i1} \\ \dots \\ t_{ik} \\ \dots \\ t_{in} \end{pmatrix}_{NEXT} = \begin{pmatrix} t_{11} & \dots & t_{k1} & \dots & t_{N1} \\ \dots & & & & \dots \\ t_{1k} & \dots & t_{kk} & \dots & t_{Nk} \\ \dots & & & & \dots \\ t_{1n} & \dots & t_{kn} & \dots & t_{nn} \end{pmatrix} \otimes \begin{pmatrix} t_{i1} \\ \dots \\ t_{ik} \\ \dots \\ t_{in} \end{pmatrix}_{CURRENT} \qquad (2)$$

In the above matrix operation $\otimes$, an element t_{ik} is calculated as $t_{ik} = max_{1 \le j \le n}\{t_{ij} \times t_{jk}\}$. Node i , iteratively executes the eq(2) for calculation of multi hop distance node trust values

$$t_i = (N^T) t_i$$
$$t_i = (N^T)^2 t_i$$
$$\vdots$$
$$t_i = (N^T)^n t_i$$

3.3 Advantages of QTAR

In the proposed method (QTAR), node trust value is evaluated in two phases. In first phase direct trust is evaluated using dempster shafer theory, in second phase indirect trust is evaluated using trust matrix operations.
The proposed method is having the following advantages over existing methods

1 The method can reduce the path breaks in routing process, since it selects the nodes with threshold level of energy and bandwidth.
2 The method can improve the packet delivery time by deploying stable nodes along the route to destination
3 The method is capable of finding alternate trust route, in case of route failure.

4. Recommendations Based QoS Trust Aggregation and Routing in Mobile Adhoc network

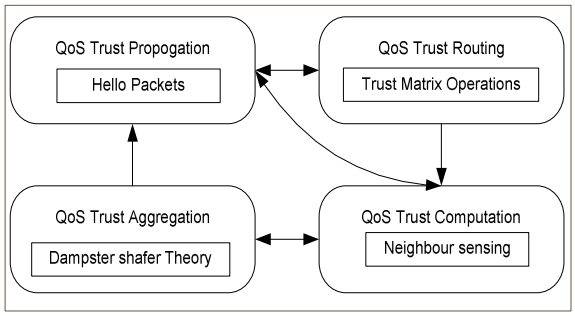

Figure 1: QoS Trust frame work in MANETs

In the figure 1, the QoS trust is managed through the following interrelated phases in proposed method (QTAR),

- QoS Trust Computation
- QoS Trust Aggregation
- QoS Trust Propagation
- QoS Trust Routing

4.1 QoS trust computation

Due to broadcast nature of MANETs, a node can observe and estimates the neighbour node's resources in their direct interactions. For a node, QoS trust value is computed based on their available QoS resources like residual energy, available bandwidth and node stability.

4.1.1 Residual energy

In path establishment to a destination node, a source node defines the threshold energy (Th_E) that an intermediate node should have for forwarding a packet. A node increments it's neighbour node's trust value if it is having residual energy greater than the threshold energy ($QTV \rightarrow QTV + 1$) otherwise it decreases($QTV \rightarrow QTV - 1$). Threshold energy is evaluated using equation (3).

$$Th_E = (E_{frw} \times m \times r^2) + (2 \times E_{act} \times m) \quad (3)$$

Here E_{frw} is a node forwarding energy, m is a size of data packet in bits, r is a node transmission range and E_{act} is the node's amplifier activation energy.

4.1.2 Available bandwidth

Source node calculates the threshold bandwidth (Th_{bw}) for an intermediate node for successful data transmission to the destination. A node increments neighbour node trust value ($QTV \rightarrow QTV + 1$) if it has bandwidth more than threshold level, otherwise decrements ($QTV \rightarrow QTV - 1$). The threshold bandwidth is evaluated using TDMA method, where the bandwidth of a node is computed based on the number of free transmission/ receiving slots it has with its neighbour node.

4.1.3 Node stability

In MANETs, node mobility has significant impact on application's performance. A routing protocol prefers stable nodes along the path to destination. A node estimates neighbour node stability in the form of link expiry time with that node. If a neighbour node has threshold level of link expiry time, then its trust value is increased($QTV \rightarrow QTV + 1$) otherwise decreased ($QTV \rightarrow QTV - 1$). The link expiry time for a pair of nodes is evaluated based on their current location, velocities and direction of movement.

4.2 QoS Trust aggregation.

The Dempster's rule of combination, combines the 1-hop neighbours trust recommendations to derive the indirect trust for 2-hop neighbours. In MANET context, a node can have three possible trust evidences like trust $\{T\}$, distrust $\{\bar{T}\}$ and uncertainty (trust/distrust) $U = \{T, \bar{T}\}$.

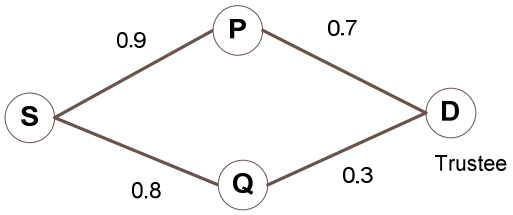

Figure 2: Aggregation of QoS trust recommendations

In figure 2, Let's assume P, Q nodes trust evidences $(T, \bar{T}, U)$ on node-D are $\{0.7,0.2,0.1\}$ and $\{0.3,0.5,0.2\}$ respectively. Node S trust values of P, Q nodes are $T_P = 0.9$ and $T_q = 0.8$. Then node P, Q trust evidences are recomputed like

$$m_P(T) = T_P \times 0.7 = 0.63$$
$$m_P(\bar{T}) = T_P \times 0.2 = 0.18$$
$$m_P(U) = T_P \times 0.1 = 0.09$$
$$m_Q(T) = T_Q \times 0.3 = 0.24$$
$$m_Q(\bar{T}) = T_Q \times 0.5 = 0.40$$
$$m_Q(U) = T_Q \times 0.2 = 0.16$$

The aggregation of P,Q nodes recommendations on node-D is evaluated as in eq(1).

$$m_{P,Q}(T) = \frac{m_P(T)m_Q(T) + m_P(T)m_Q(U) + m_P(U)m_Q(T)}{1 - [m_P(T)m_Q(\bar{T}) + m_P(\bar{T})m_Q(T)]} = \frac{0.05}{0.09} = 0.55$$

The above equation can be extended for combining of *n* nodes recommendations on node-D. i.e $m_{1\ldots n}(T)$.

4.3 QoS trust propagation

In the network, the trust values are propagated through the HELLO packets. Every node periodically sends the HELLO packets, which contains the 1-hop and 2-hop neighbours trust values. Additionally a node can send trust request (TREQ) to its neighbour nodes for remote node trust value. The proposed method uses the AODV routing principles for route discovery.

4.4 QoS trust routing

Whenever a source node wants to send data to destination node, it sends the RREQ packets to neighbour nodes with pre calculated QoS threshold values.

1) On receiving RREQ packet, an intermediate node adds its ID and forwards to the next hop neighbours.
2) RREQ packet collects the trust values of the intermediate nodes in its journey to destination node.
3) After receiving RREQ packets, the destination node updates its trust matrix.
4) Destination node applies the transitive operations iteratively over it's trust matrix to find out the trust worthy route from the source node (sec 3.2). Then it sends the RREP packet to source node through the computed route.
5) On receiving RREP packet, source node establishes the route and starts the data transmission.

4.4.1 QoS routing example.

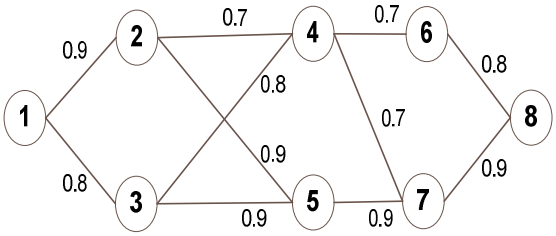

Figure 3: QoS trust routing in MANETs

In figure 3, source node-1, wants to establish the path to destination node-8. Source node sends the RREQ packet to the neighbour nodes. The RREQ packets collect the intermediate nodes trust values and reach the destination node. Destination node-8 prepares the trust matrix (N^T) and applies the matrix operations to find out the trust worthy path from node-1 to node-8 iteratively.

Iteration 1:

Initially source node -1 contains the trust values of 1-hop neighbours, i.e nodes 2,3.

$$\begin{bmatrix} t_{11} \\ t_{12} \\ t_{13} \\ t_{14} \\ t_{15} \\ t_{16} \\ t_{17} \\ t_{18} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.7 & 0.8 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.9 & 0.9 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.7 & 0.9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.8 & 0.9 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0.9 \\ 0.8 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

After the first iteration, source node's 2-hop neighbours (node 4,5) trust values are evaluated

Iteration 2:

After the second iteration, source node's 3-hop neighbours (node 6,7) trust values are evaluated

$$\begin{bmatrix} t_{11} \\ t_{12} \\ t_{13} \\ t_{14} \\ t_{15} \\ t_{16} \\ t_{17} \\ t_{18} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.64 & 0.7 & 0.8 & 0 & 0 & 0 & 0 & 0 \\ 0.81 & 0.9 & 0.9 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.7 & 0.9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.8 & 0.9 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0.9 \\ 0.8 \\ 0.64 \\ 0.81 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Iteration 3:

After third iteration, source node's 4-hop neighbour (node 8) i.e destination node trust value is evaluated.

$$\begin{bmatrix} t_{11} \\ t_{12} \\ t_{13} \\ t_{14} \\ t_{15} \\ t_{16} \\ t_{17} \\ t_{18} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.64 & 0.7 & 0.8 & 0 & 0 & 0 & 0 & 0 \\ 0.81 & 0.9 & 0.9 & 0 & 0 & 0 & 0 & 0 \\ 0.51 & 0 & 0 & 0.8 & 0 & 0 & 0 & 0 \\ 0.73 & 0 & 0 & 0.7 & 0.9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.8 & 0.9 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0.9 \\ 0.8 \\ 0.64 \\ 0.81 \\ 0.51 \\ 0.73 \\ 0.66 \end{bmatrix}$$

Iteration4:

This process ends, after finding destination node's trust value. Here the destination node trust value from source node is 0.66.

$$\begin{bmatrix} t_{11} \\ t_{12} \\ t_{13} \\ t_{14} \\ t_{15} \\ t_{16} \\ t_{17} \\ t_{18} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.64 & 0.7 & 0.8 & 0 & 0 & 0 & 0 & 0 \\ 0.81 & 0.9 & 0.9 & 0 & 0 & 0 & 0 & 0 \\ 0.51 & 0 & 0 & 0.8 & 0 & 0 & 0 & 0 \\ 0.73 & 0 & 0 & 0.7 & 0.9 & 0 & 0 & 0 \\ 0.66 & 0 & 0 & 0 & 0 & 0.8 & 0.9 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0.9 \\ 0.8 \\ 0.64 \\ 0.81 \\ 0.51 \\ 0.73 \\ 0.66 \end{bmatrix}$$

4.4.2 Trace out the route

In the trust matrix(N^T) of last iteration, identify the node (j) such that from which the destination node got the maximum trust value. By the backtracking through previous iteration's trust matrices, identify the node through which node-j got maximum trust value. This procedure is continued till the source node reached. Here the trust worthy path from source to destination is 1-2-5-7-8.

4.5 Theoretical analysis of proposed method

The frame work in the proposed method follows four phases. In table1, the time and space complexity of each phase is discussed. In trust computation, each node has to compute direct trust value for its q-number of neighbours, so it is $O(n \times q)$. A node uses $n \times n$ matrix for trust maintenance, so it is $O(n^2)$. In trust aggregation, for combining n-recommendations a node has to spend $O(m^n)$ time, where m is the number of elements in the frame of discernments. Trust propagates through HELLO packets, so it is $O(n \times f_h)$, where $O(f_h)$ is the frequency of hello packets. For route identification, destination node performs k iterations of matrix operations, so it is$O(kn^2)$.

Table 1: Time and Space complexities of QTAR

Method	Time complexity	Space complexity
QoS Trust computation	$O(n \times q)$	$O(n^2)$
QoS Trust aggregation	$O(m^n)$	no additional space required
QoS Trust propogation	$O(n \times f_h)$.	$O(f_h)$
QoS Trust routing	$O(kn^2)$	no additional space required

5. Results

The simulation results are taken in the network simulator (ns2). The proposed method(QTAR) performance is compared with existing protocols AODV and AQOR for the parameters bandwidth, energy consumption, delay and packet delivery ratio(PDR).

5.1 Experiment setup

The simulation is run for 600 sec where the network size is increased from 10 to 50 nodes and node velocity is increased from 12 to 60 m/sec. We adopted the random way point mobility model. A node's transmission range is 250 m

5.2 Simulation parameters

1) *Packet delivery time:* it is calculated as the faction of total time taken by data packets to reach the

destination to the number of data packets received at destination node.

2) *Throughput*: The amount of data transferred from source to destination in unit time.
3) *Routing energy*: total energy consumed by the nodes along the route in data transmission from source to destination.
4) *packet delivery ratio:* it is the ratio of number of data packets are delivered to the number of total packet generated.

5.3 Simulation results

In figure 4, the packet delivery time (sec) is increased when the nodes velocity is increased. While the nodes are moving at higher velocity, the links get broken frequently. The proposed method allows only stable nodes in its data transmission, there by reduces the packet delivery time.

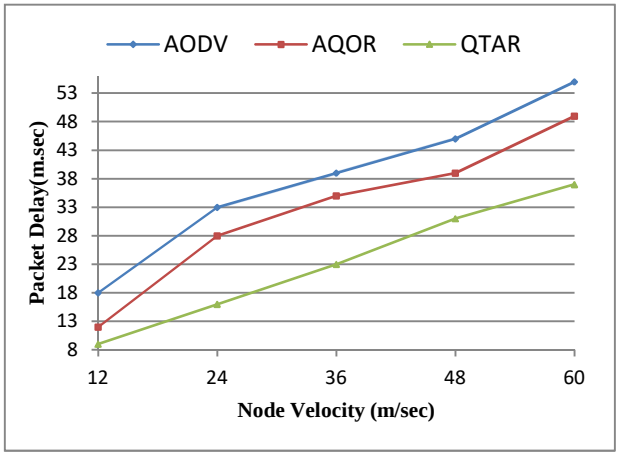

Figure 4: node velocity Vs packet Delay

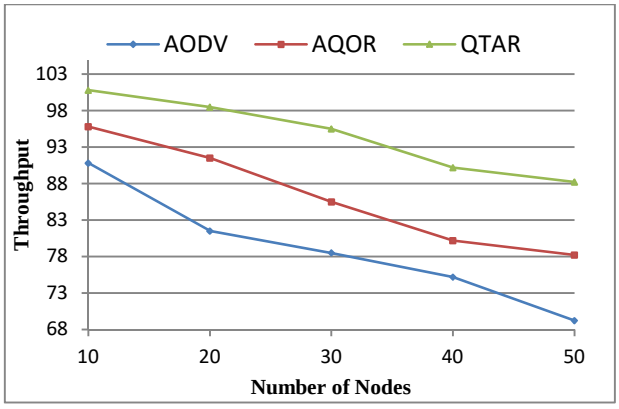

Figure 5: number of nodes Vs throughput

In figure5, the throughput is decreased with increased network size. When an intermediate node is having more neighbour nodes, then its bandwidth is reduced. QTAR considers bandwidth as a QoS metric in path construction. Hence the proposed method results in good throughput.

In figure 6, the routing energy (total energy of intermediate nodes along the path) is increased with increased network size. QTAR selects the nodes with sufficient energy, so that the number of re transmissions is reduced. Hence the routing energy consumption in QTAR is less than others.

In figure 7, Packet delivery Ratio (PDR) decreases for higher node velocities. If the path is disconnected, the routing protocol has to deploy alternate path, so it reduces the PDR. By selecting stable nodes, the proposed method reduces the path breaks and increases the PDR value.

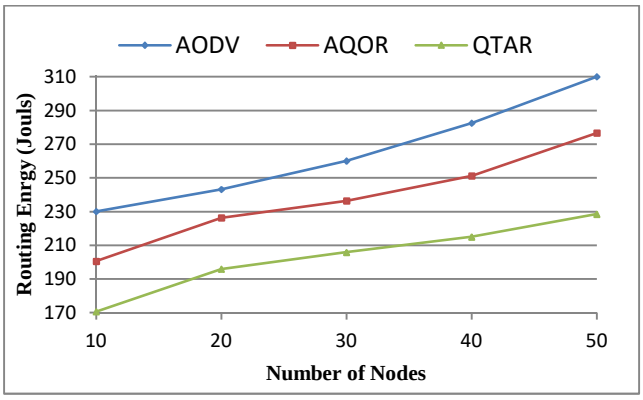

Figure 6: number of nodes Vs routing energy

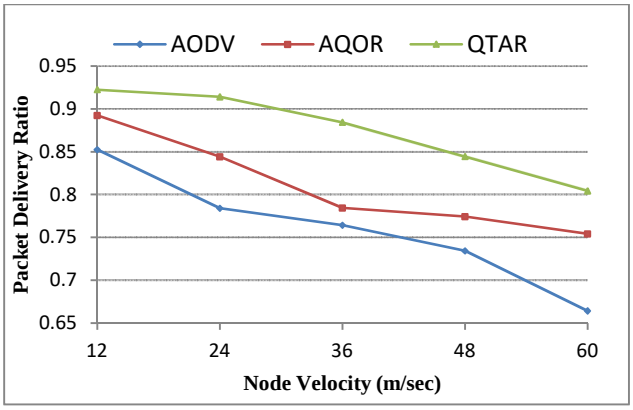

Figure 7: node velocity Vs PDR

6. Conclusion

In this frame work, the QoS trust is established in four phases i.e computation, aggregation, propagation and routing. Direct trust of a node is evaluated based on its quality of available resources. In indirect trust computation, we used the dempster shafer combination rule for reducing the impact of biased recommendations. Trust information is maintained in the form of trust matrices at every node. We applied matrix operations for finding trustworthy route from source to destination. The performance of the proposed method is analysed theoretically in terms of time and space complexities. In simulation results, the QTAR outperformed the existing protocols.

References

[1] Hui Xia and Jia Yu "Applying trust enhancements to reactive routing protocols in mobile ad hoc networks" journal of Wireless Networks, vol 22, pp 2239–2257, 2016.

[2] Priya Sethuraman and N. Kannan , "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET" journal of wireless networks. Vol 22, pp1-11,2016

[3] V. Jayalakshmi and T. Abdul Razak "Trust Based Power Aware Secure Source Routing Protocol using Fuzzy Logic for Mobile Adhoc Networks", IAENG International Journal of Computer Science, vol 43, pp98-107, 2016.

[4] Muhammad Saleem Khan and Majid Iqbal Khan,"MATF: a multi-attribute trust frameworkfor MANETs", EURASIP Journal on Wireless Communications and Networking , vol 2016,pp1-17, 2016.

[5] Moussa Ali cherif and Sofiane Boukli Hacene "A energy-conserving predictive preemptive multipath routing protocol for adhoc networks: a lifetime improvement", International Journal

of Communication Networks and Information Security (IJCNIS), vol -8, issue 1, pp31-39. 2016

[6] Maryam el Azhari, Ahmed Toumanari, Rachid Latif, Nadya el Moussaid, "Relay based thermal aware and mobility support routing protocol for wireless body sensor networks", International Journal of Communication Networks and Information Security (IJCNIS), vol -8, issue 2, pp 64-73, 2016.

[7] Fei Hao, Geyong Min, Man Lin, Changqing Luo, Yang, L.T. "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, 2014.

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

[9] Hu-Chen Liu, Long Liu, Qing-Lian Lin, and Nan Liu "Knowledge Acquisition and Representation Using Fuzzy Evidential Reasoning and Dynamic Adaptive Fuzzy Petri Nets", IEEE Transactions On Cybernetics, Vol. 43, No. 3. Pp1059-1072, 2013.

[10] Sirisala, NageswaraRao.; C.Shoba Bindu." Uncertain Rule Based Fuzzy Logic QoS Trust Model in MANETs" 21st International Conference on Advanced Computing and Communications-ADCOM, IIT madras, pp55-60,2015.

[11] Kannan Govindan, Member IEEE and Prasant Mohapatra, Fellow IEEE "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, 2012.

[12] N. Cheng, K. Govindan and P. Mohapatra, "Rendezvous based trust propagation to enhance distributed network security," in Proceedings of IEEE *INFOCOM Workshop* on Security in Computers, Networking and Communications, china, pp 112-122, 2011.

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

[14] S. Trifunovic, F. Legendre and C. Anastasiades, "Social trust in opportunistic networks", IEEE Conference on Computer Communications Workshops, San Diego, pp. 1–6, 2010.

[15] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks", The International Journal of Computer and Telecommunications Networking, vol. 53, no. 14, pp. 2396–2407, 2009.

[16] Y. Bachrach, A. Parnes, A. D. Procaccia, and J. S. Rosenschein, "Gossip-based aggregation of trust in decentralized reputation systems,", Journal of Autonomous Agents and Multi-Agent Systems, vol. 19, no. 2, pp. 153–172, 2009.

[17] J. Huang and D. Nicol, "A calculus of trust and its application to PKI and identity management," in The 8th ACM Symposium on Identity and Trust on the Internet, Gaithersburg, pp. 23–37, 2009.

[18] A.Menaka and M.E Pushpa"TAODV: A Trusted AODV Routing protocol for Mobile ad hoc networks" IEEE international conference on Internet multimedia services architecture and applications. Pp268-273,2009

[19] G. Lenzini, M. S. Bargh and B. Hulsebosch, "Trust-enhanced security in location-based adaptive authentication," Journal of Electronic Notes in Theoretical Computer Science, no. 197, pp. 105–119, 2008.

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

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

[22] A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks," International Journal of Wireless Personal Communications, vol. 37(1-2), pp.139–168, 2006.

[23] C.D. Jensen, P.O. Connell, "Trust-based route selection in dynamic source routing", Proceedings of International Conference on Trust Management, Italy, pp150–163, 2006.

[24] T. M. Chen and V. Venkataramanan, "Dempster–Shafer theory for intrusion detection in ad hoc networks," IEEE journal of Internet Computing, vol. 9, no. 6, pp. 35–41, Nov./Dec. 2005

[25] E. Gray, J. marc Seigneur, Y. Chen, and C. Jensen, "Trust propagation in small worlds," 1st International. Conference on Trust Management, Greece, pp. 239–254, 2003.

[26] T. Hughes, J. Denny, P.A. Muckelbauer, J. Etzl, "Dynamic trust applied to ad hoc network resources", in Proceedings of the Autonomous Agents and Multi-Agent Systems Conference, Melbourne, pp. 273–280, 2003

[27] A.Jøsang and R. Ismail, "The Beta Reputation System," in proceedings of Bled Electronic Commerce Conference , Slovenia, pp. 324–337, 2002.

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