AN ENHANCED AD HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL FOR MANET'S

[1]C.Siva Krishnaiah, [2]Prof.N.Geethanjali, [3]Dr.T.Harikrishna
[1] Research Scholar, [2] Professor, [3]Assistant Professor
[1]Computer Science,
[1]Rayalaseema University, Kurnool, India

Abstract: Mobile Ad hoc Network is a recurrently self-configuring network possessed of a standard set of mobile devices which can converse between them without infrastructure attached wirelessly. This paper make available a flexible model that support end-to-end optimized QoS support in ad hoc networks that is both competent and easily deployable. This architecture uses agent based QoS administration and route decisions are made after calculation of available local and flow bandwidths under the consideration of link availability. This end-to-end admission control or signaling eliminates the rerouting of route request and route replies and packets transmission thus increase the bandwidth consumption and limits the nodes in transmission. This includes an admission control system that comprises an end-to-end Route Requests to avoid making stringent bandwidth reservations, so present soft QoS guarantees to real-time flows.

***IndexTerms* - manet, QoS, network agent, opmaodv.**

I. INTRODUCTION

Mobile Ad hoc Network is a recurrently self-configuring network made of a standard set of mobile devices which can converse between them without infrastructure attached wirelessly. Each device organized in a MANET remains unrestricted to be in motion alone in any route, and so change its associations to other devices often. Quality of Service is the overall performance realized by the users of the network. QoS in a network is measured quantitatively using several parameters such as error rates, bit rate, throughput, availability, transmission delay and jitter etc., Quality of service is principally significant for the conveyance of traffic with special necessities supporting new applications with even stringent service demands.

II. PROPOSED SYSTEM ARCHITECTURE

The suggested QoS architecture gives support to real-time applications in MANET. The goal of proposed method is to provide a sustainable framework that offer end-to-end QoS support to ad hoc networks and that is both capable and easily deployable using present technology. Georgiadis et al. [1] have presented that making resource reservations in multi-hop wireless environments for admission control is an NP-hard problem that is even under streamlined rules for bandwidth arrangement. This expresses that the per-node local quantities do not contain abundant data for end-to-end bandwidth reservation. This makes putting into practice of bandwidth reservation schemes for MANETs as difficult (e.g., the one proposed in the INSIGNIA [2] framework). So, we considers a QoS framework by comprising a unique admission control system based on end-to-end Route Requests that skips making stern bandwidth reservations, thus contributes soft QoS guarantees to real-time flows. The diverse architectural components, shown in Fig.1, fit in to an integrated QoS architecture described by numerous cross-layer optimizations among its components.

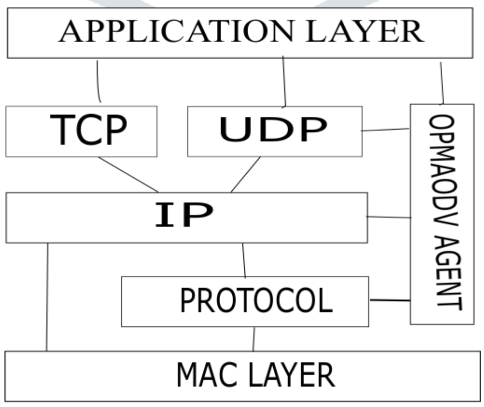

Figure 1: System Architecture

The core element of the proposed QoS architecture is OPMAODV agent. This realizes a Request -based admission control mechanism that achieves end-to-end QoS measurements according to the applications QoS requirements. On the other hand, this is not a firm requirement since OPMAODV agent will still operate independently of the MAC layer used. In terms of the software required for MANET nodes, the sources and destinations of QoS flows must have an OPMAODV agent running. The remaining nodes will simply treat forwarded packets as regular data packets, being ignorant of the mechanism itself.

Regarding OPMAODV agent modules, Fig. 2 shows the designed block diagram of an OPMAODV agent. The main component of OPMAODV agent is QoS module. The QoS module is accountable for evaluating QoS parameters on an end-to-end path. Another component is the packet filter, which blocks all network traffic that is not acceptable into the MANET agreeing to these end-to-end measurements.

Service Registration: An application that desires to use OPMAODV agent need register itself with the OPMAODV agent.

Connector: It is indicating the destination IP address and the source and destination ports, along with a QoS specification (QSPEC) that states the wished bandwidth, delay, and jitter: If any amidst the accessible bandwidth, the end-to-end delay, or the jitter values does not meet the application's requests, OPMAODV agent will advise this event to the application. Once application registration is successfully completed, the QoS module is activated.

Destination details: The agent, upon in receipt of Route Request Packets, will update the destination particulars where it keeps per-source statistics of the packets received during the current probing period. After receiving the last packet of a Route Request (or if a timeout is triggered), the destination agent will send a route reply back to the source OPMAODV agent.

Connection Status Table: Describing a connection status flag as adequate or not. For the choice of a single terminal, if only part of the registered connections can be allowed, priority is given to those that have registered first.

Synchronizer: It imposes a timer related constraints on QoS Module.

QoS Module: This is the module responsible for QoS optimization. It contains the components QoS Policies and QoS Optimizer.

QoS Policies: These are QoS policy requirements (QPSPEC) mentioned by the applications at the time of registration. The QoS Module other component ensures that these specifications are met the allowed connections.

QoS Optimizer: This component performs QoS optimization tasks. Upon receiving each Route reply, it will update the state of the path using per-connection bandwidth, jitter and delay flags. Once enough data is gathered, it checks all the associated connections headed for that destination, and then chooses whether a connection should be accepted, preserved, or rejected according to the QoS Strategies locally preserved and then update the connection status table accordingly. It will intermittently accomplish path probing between the source and destination. The purpose is to evaluate if the path can meet the QoS policy necessities (QPSPEC) available.

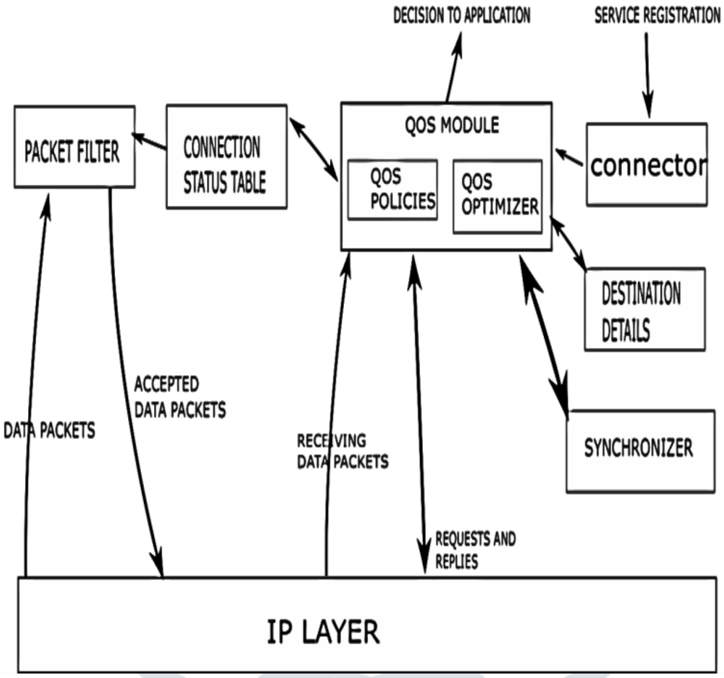

Figure 2: Working Model

III. Interaction between the routing protocol and OPMAODV agent

The OPMAODV agent can use routing layer data to assess the current state of end-to-end paths, evading probe packets when no path is available. It can also quantity the QoS of new paths as soon as they become accessible through route discovery processes. The valuation of routing states can be completed by interacting directly with the routing agent, or by intercepting routing packets incoming through the wireless interface. Regarding the interface between OPMAODV agent and reactive AODV [3], we attain optimal performance by re-assessing the end-to-end QoS conditions as soon as a routing RREP message from a destination of a QoS flow is received. Such a message specifies that a new path to that destination is obtainable, and so the admission control mechanism is able to respond formerly if the new path cannot meet the QoS necessities. Still, other cross-layer optimizations between OPMAODV agent and protocol are necessary to achieve optimum performance; as an example, the measurement of optimal timeout values at the receiver OPMAODV agent must take into account that traffic is incoming through various paths. The source OPMAODV agent must also take multipath routing into interpretation when assessing end-to-end delay. As a final observation, we wish to emphasize that the routing protocol remains agnostic about the functioning of OPMAODV agent and, in the case of AODV and non-QoS-aware routing protocols.

IV. QoS aware routing

The different nature of wireless medium in ad hoc networks demands the design of new solutions to provide QoS. As the nodes in ad hoc networks cooperate with each other for routing, they must cooperate with each other for QoS support also. This needs an admission control along the routes to prevent new flows from consuming too many resources and disrupting the guarantees made to existing flows. Hence it is necessary to provide effective admission control protocol for MANETs so that end-to-end connections with QoS requirements can be maintained.

It includes the tasks such as route request packet construction, available bandwidth estimation and link selection. Source node is responsible for the construction of route request packet in the desired manner. It computes the application's flow bandwidth requirement and identifies whether the link matches with the requirements of the transmission initiated by the sender. Intermediate node is responsible for available bandwidth estimation and decision of link used to forward. While receiving the route request packet, it computes both these values and then enters into the assessment admission control check. In the assessment of admission control, intermediate node mainly checks whether its own available bandwidth and its contention neighbor's available bandwidth are greater than the requested bandwidth

On success of the assessment admission control the received route request packet is broadcast otherwise it is discarded. The intended destination node on receiving the route request packet constructs the corresponding route reply packet and sends it back to the source on the same reverse route. While receiving the route reply packet the intermediate node performs the final full-fledged admission control. The intermediate node with the help of path information available in the route reply packet derives its contention count value. Using this contention count value, the application's actual flow bandwidth requirement at this node is computed. Based on this value admission control is done. On success of the admission control, the requested bandwidth reservation is made and the route reply is sent on reverse route. On failure of the admission control, route reply is discarded and steps are initiated to cancel the bandwidth reservation made in the successor nodes along the path.

V. ESTIMATION OF BANDWIDTH AVAILABLE

Each node in the MANETs can determine it's $Bandwidth_{local}$ by passively listening network activities. This approach proposes to use the fraction of channel idle time based on the past history as an indication of local available bandwidth at a node. A node can perceive the channel as either idle or busy.

The channel is idle if the node is not in any of the following three states: First, the node is transmitting or receiving a packet. Second, the node receives a Request To Send (RTS) or a Clear To Send (CTS) message from another node, which reserves channel for a period of time specified in the message. Third, the node senses a busy carrier with signal strength larger than a certain threshold, called the carrier sensing threshold, but the node cannot interpret the contents of the message. Idle time calculation requires estimation of Channel Busy Time (T_{busy}) within the stipulated time period (T_p). Normally the medium is busy with the control messages like RTS, CTS, ACK and the transmission, reception, detection of data frames. Hence the amount of time required for single data packet transmission (Cerveira-2006) at the network layer is computed as given in Equation 3.1.

$$T = T_{c\_msg} + T_{mac} + T_{frame} \qquad (3.1)$$

Where,

T_{c_msg} - Time consumed by the routing control messages like RTS, CTS, ACK.

T_{mac} - Time consumed by DIFS, SIFS, and back off intervals (MAC layer overhead).

T_{frame} - Time needed for single data frame transmission.

The Channel Busy Time (T_{busy}) estimation, when 'L' number of packets are transmitted, received or detected for the duration of T_p is given in Equation 3.2.

$$T_{busy} = T_{c\_msg} + L * (T_{mac} + T_{frame}) \qquad (3.2)$$

If contention occurs, nodes involved in it are entering into the back off state. Nodes are also start decreasing their chosen back off counter value. When the node hears a next transmission, its back off counter is paused and restarts when the medium remains idle again for DIFS duration.

Channel idle time (T_{idle}) within the period T_p is comprehended as shown in Equation 3.3.

$$T_{idle} = T_p - T_{busy} \qquad (3.3)$$

By monitoring the amount of T_{idle}, during every period of time T_p, the $Bandwidth_{local}$ of a node is computed using a weighted moving average (Yang 2005) as specified in Equation 3.4.

$$Bandwidth_{local} = \Phi\ Bandwidth_{local} + (1 - \Phi)\ (T_{idle}/T_p)\ Bandwidth_{channel} \qquad (3.4)$$

Where,

$Bandwidth_{channel}$ is the capacity of the channel and Φ the weight factor, $0 < \Phi < 1$.

The amount of time that the channel is in this idle state, denoted as $T_{contentionidle}$ for every period of time T_p, contention neighborhood available bandwidth ($Bandwidth_{neighbor}$) is calculated (Yang 2005) using the weighted moving average given in Equation 3.5.

$$Bandwidth_{neighbor} = \Phi\ Bandwidth_{neighbor} + (1 - \Phi)\ (T_{cidle}/T_p)\ Bandwidth_{channel} \qquad (3.5)$$

Where,

$Bandwidth_{channel}$ is the capacity of the channel and is the weight factor, $0 < \Phi < 1$.

Each data packet's transmission time is calculated as per Equation 3.6.

$$T_{data} = T_{rts} + T_{cts} + T_{ack} + T_{difs} + 3T_{sifs} + (P+Q)/Bandwidth_{channel} \qquad (3.6)$$

Where,

T_{data} - Time of Each data packet Transmission
T_{rts} - Time for RTS Transmission
T_{cts} - Time for CTS Transmission
T_{ack} - Time for ACK Transmission
T_{difs} - Inter frame space defined for DCF in the IEEE 802.11 protocol standard
T_{sifs} - IEEE 802.11 protocol standard specified short inter frame space
P - Data packet size
Q - Header length of IP and MAC packet
$Bandwidth_{channel}$ - Channel capacity

If, at every second the application produces ‘R’ packets with an average packet size 'P', the corresponding flow bandwidth condition ($Bandwidth_{flow}$) is calculated as given in Equation 3.7.

$$Bandwidth_{flow} = R \times T_{data} \times Bandwidth_{channel} \qquad (3.7)$$

The Throughput $T_{throughput}$ can be calculated by

$$T_{throughput} = P / (T_{data+ack} - T_{stateready}) \qquad (3.8)$$

Where,

$T_{data+ack}$ - It is total time of data packets and acknowledgement transmission.
$T_{stateready}$-It is packets ready state for broadcast.

VI. ROUTE DISCOVERY AND MAINTENANCE

The proposed route discovery and process can be considered in QoS feasibility of link between the nodes. The QoS decision factor uses 0 for unreliable/not feasible link and 1 for QoS feasible link based on these QoS factor the path discover is made by the process. When a node detects 0 as QoS decision factor for node path then that is discarded for RREQ and RREP packets transmission. Whenever the node recovered from failure or obtained necessary resources as per the QoS Policy specifications (QPSPEC) then its link decision factor is modified by receiving a probe request to neighbors. The QoS decision factors are updated by QoS Optimizer component of OPMAODV agent. The Figure 3 (I) indicates that all routes are QoS feasible and Figure 3(II) indicates that root A->C and B->G are in failure/Not feasible state so such routes are not selected by the route discovery process.

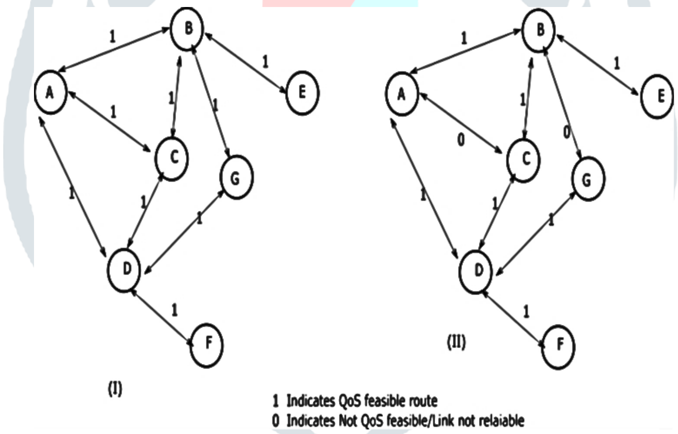

Figure 3: Route Discovery and maintenance

When a node receives RREQ first it is processed by QoS optimizer and then forwarded to next neighbor node that is selected only when that has path with sufficient bandwidth and feasible state. The objective of route discovery is minimizing the RREQ and RREP messages and provides sufficient resources to the other transmissions.

Pseudocode for Route Discovery

1. Determine the source and end nodes of the network.
2. Source Construct the RREQ with expected QoS Specification (bandwidth, delay etc.,) and submit to QoS agent.
3. Now such RREQ is forwarded to neighbors till end node as follows
    a. At each intermediate node neighbors local bandwidth is calculated.
    b. Now arrived RREQ is compared and if satisfies the RREQ specifications then such neighbor is selected for RREQ forward.
    c. Route information is recorded in packet header.
4. After RREQs reached to end node now the end node agent construct RREP and forward to best shortest path.
5. In any case such shortest path is failed to transmit the RREP then send a control message to end node by the agent at path failure node.
6. In such case the end node choose alternate path from the RREQ information and forward RREP.
7. Each intermediate node reserves the resources of the route and forward to upward until it reaches to the source.

In the Figure 3 (I) if the transmission is expected between A to G nodes and the RREQ/RREP are forwarded between the nodes possibly A->D->G or A->B->G with selection criteria. There are possible paths between A to G are A->C->D->G and A->B->C->D->G.

In the Figure 3 (II) if the transmission is expected between A to G nodes and the RREQ/RREP are forwarded between the nodes possibly A->D->G and A->B->C->D->G with selection criteria. There are no other possible paths between A to G since A->C and B->G routes are unreliable.

VII. SIMULATION AND PERFORMANCE EVALUATION

Simulation can be carried out by using NS-2 simulator. It can be carried out using Parameters mentioned in Table 1. In Figure 4 we observed that throughput increases in the presence of fixed packet size and variable number of nodes. It indicates that the growth of network size will increase load on network and in the presence of efficient QoS strategy throughput will increase.

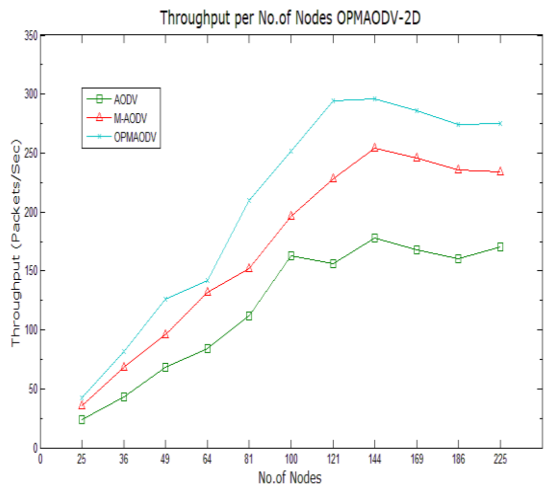

Figure 4: Throughput

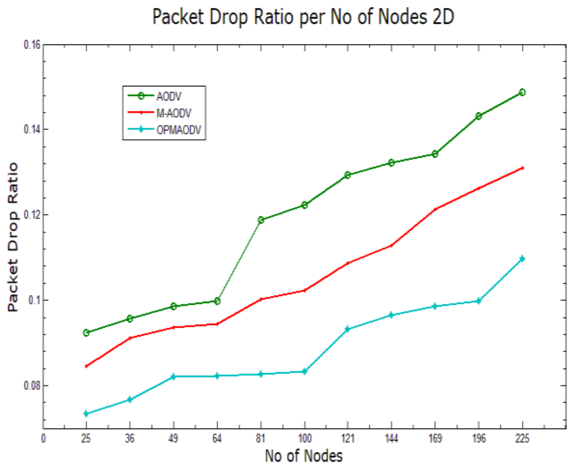

Figure 5: packet drop ratio

The simulation can be carried out to identify packet drop ratio (shown in Figure.5) using the variable no of nodes with fixed packet size of 512 kb. When no of nodes increase the channel load will increase and it leads to drop of packets but the drop of packets is optimal in the increased network situation.

Table 1: Simulation Parameters

Parameter (units)	Value
Simulation area (m X m)	1000 x 1000
Simulation time (s)	100
Number of nodes	5X5 to 15X15
Node pause time (s)	10, 20
Propagation model	Two-ray ground
Transmission range (m)	250
Data packet size (B)	512 KB
Session duration (s)	40 – 120
Session start time (s)	0 – 150
Simulation tool	NS-2
Bandwidth	2 Mbps
CBR data rate (Packet/sec)	5

VIII. CONCLUSION

The projected QoS system is based on AOMDV protocol and it is greatly operational in the situation of unbalanced network. Since its evaluations uses the local channel bandwidth and required flow bandwidth dynamically and route the packets based on bandwidth obtainability by considering the feasible routes only. It has the scheme of link failure identity and management hence there is almost no rerouting of packets hence it will increase the throughput.

REFERENCES

[1] L.Georgads,P.Jacquet, and B.Mans,Mar-2004, “Bandwidth reservation in multi hop wireless networks: complexity and mechanisms” in ICDCSW’04, Hachoj-Tokyo,Japan,pp 762-767.

[2] Lee.S.B, a.Gahng-Seop,X.Zhang, and A.T.Campbell,Apr-2000, “INSIGNA- An IP-based quality of service framework for mobile ad hoc networks”, JPDCSWMCC, vol.60,pp.374-406.

[3] C.E.Perkins, E.M.Belding-Royer and Das.S.R,rc-3561,”Adhoc on demand distance vector routing”,MANET workgroup.

[4] Kalpana V and Dr.S.Karthik,2018, “Bandwidth Constrained Priority Based Routing Algorithm for Improving the Quality of Service in Mobile Ad hoc Networks”, International Conference on Soft-Computing and Network Security(ICSNS),IEEE.

[5] Calafate.C.T, Malumbres.M.P and others, May-2009, “Qualit of Service support in MANETS: A Modular Architecture based on the IEEE 802.11e Technology”, IEEE Transactions on circuits and systems for video technology, Vol.19, No.5.

[6] Thenmozhi, D. S. and R.Lakshmipathi, 2010, “Quality of Service Enhanced Routing in Mobile Ad hoc Networks”, International Journal of Computer Science and Information Security, Vol. 8, No. 5, pp. 34–40.

[7] Cerveira,C.R and Costa,2006, “A Time based Admission control Mechanism for IEEE 802.11 Adhoc networks “ mobile and wireless communication networks, Vol. 211 of IFIP(International Federation for Information Processing), pp.217-228,springer.

[8] Y.Yang and R.Kravets, 2005, ‘Contention Aware Admission Control for Ad hoc Networks’, IEEE Transactions Mobile Computing, Vol.4,pp.363-377.