CHAPTER 7

AN INTEGRATED QoS ENHANCEMENT PROVISIONING MAC MODEL FOR MOBILE AD HOC NETWORKS

7.1 INTRODUCTION

Quality of Service of any network is directly dependent on the efficiency of the MAC protocol in handling channel contention. Performance of the MAC protocol may be reduced due to various reasons pertaining to the nodes, both intentional and unintentional. Intentional degradation of service can be caused by selfish nodes. In IEEE 802.11 DCF, the MAC protocol that is largely used in mobile ad hoc networks, the selfish nodes may skip adhering to the protocol, by repeatedly choosing a low backoff value for obtaining an unfair throughput share, for instance. Such misbehavior is of great concern in environments that provide differentiated services as high priority nodes will be deprived of their deserved higher throughput share. Unintentional degradation can be caused by the well known hidden and exposed terminal problems. In this chapter, a QoS model is proposed by integrating the mechanisms expounded in the preceding chapters. The model provides differentiated services through an adaptive AT-ST scheme, while taking care of selfish misbehavior mitigation and hidden/exposed terminal problem alleviation. It enhances network performance by reducing the number of retransmission attempts at the MAC layer and alleviates stale updates through cooperative caching.
To exploit the salient features of MANETs and to utilize them for real time applications, it is necessary to overcome the open issues and provide the services to each user or application. These open issues include limited battery power, network control difficulty, dynamic topology requiring frequent reconfiguration, and lack of reliability and security for transmissions. QoS is viewed as the performance level of the services offered by a service provider or a network to the user. QoS enhancement often requires negotiation between the host and the network, resource reservation schemes, priority scheduling, and call admission control.

7.2 QoS in MANETs

Applications like high quality multimedia services in wireless networks make it necessary to implement new techniques that can assure QoS. It should also account for the limited bandwidth, the delay and error characteristics of the wireless access network. This requires a differentiated services architecture that can offer multiple service levels, each with a different degree of QoS assurance (Sundaramoorthy Kannan et al 2005).

The goals of a misbehaving peer range from exploitation of available network resources for its own benefit to network disruption. The solution to this problem is the timely and reliable detection of such misbehavior instances, which would eventually lead to network defense and response mechanisms, and isolation of the misbehaving peer.

As discussed in the chapter 4, QoS of a wireless network that uses IEEE 802.11 MAC is also affected by packet dropping due to link layer contention caused by hidden terminals or buffer overflow (Hanal Abuzanat et al 2009). Such losses directly affect TCP window adaptation. The goal of MANET in providing effective operation over wide range of mobile networking context pose challenges in information management.
7.3 QoS ENHANCED MAC MODEL

The objective of the proposed 802.11 QoS Enhanced DCF MAC model is to improve the resource utilization with enhanced QoS by overcoming the challenges in a MANET. It incorporates the following enhancements to the MAC protocol.

- **Differentiated service provisioning**

  In order to ensure improved QoS for high quality demanding applications in wireless networks, it is necessary to prioritize hosts and provide differentiated services based on their bandwidth requirements. Such differentiated services are provided through an adaptive AT-ST scheme in this QoS model.

- **Selfish node avoidance**

  Selfish misbehavior becomes a critical issue in environments that provide differentiated services as high priority nodes are deprived of their deserved higher throughput share. Also there is a possibility that low priority nodes are eventually starved due to a large number of misbehaving high priority nodes. Amendments are made to the IEEE 802.11 DCF to simplify detection of such selfish hosts and to provide minimum guaranteed services based on the priority of the nodes. A penalty scheme is proposed for punishing selfish misbehavior of nodes.

- **Minimizing MAC level retransmission**

  TCP treats packet losses as a sign of congestion within the network. It, therefore, invokes congestion control algorithms using packet retransmission. SQB-RA resolves the retransmission problem. It is a cross-layer approach that helps in minimizing the number of retransmission attempts at the MAC layer to two.
- **Resolving the hidden terminal problem**

  The Guaranteed RTS/CTS Coverage algorithm aims at resolving the hidden terminal problem by ensuring that all the nodes including the nodes present in the interference range are aware of the ongoing transmissions. This algorithm is proposed as a centralized approach, wherein, the nodes that are present in the interference range are identified by the cluster head and this in turn identifies the set of Steiner nodes. The cluster head is elected using the modified KEL algorithm. Steiner nodes are subset of nodes present in the interference range, which broadcast the information to all the nodes in the interference range.

- **Cooperative caching to reduce bandwidth consumption**

  Maintaining cache nodes can reduce the multihop communication to get data from the data source which can save both battery power as well as bandwidth. But preserving consistency of data between the data source and the cache nodes is a serious issue to be considered. Stale updates have to be alleviated, and this is accomplished using the SPP approach.

### 7.3.1 Network Model

The network is modeled using a distributed ad hoc architecture where each node contends for channel access with a predefined priority. The nodes can detect and penalize selfish misbehavior in their neighborhood. Collisions due to nodes in interference range are avoided using a CH that creates a Collision Queue (CQ) of nodes whose AT packets undergo collision. The centralized approach continues till the collision queue maintained by CH is found to be empty while polling, thereafter, the distributed approach resumes.
Functions of the CH

- Time is slotted into sections and the duration of each section is equal to W, where W is the backoff window size determined by the CH for its cluster. The CH broadcasts Section Start (SS) and Section End (SE) messages at the beginning and end of every section.

- The CH maintains a Collision Queue and polls the nodes in the CQ at the end of every section. If the CQ is found to be null at the start of polling section, the CH broadcasts a cluster-dissolve message and the network reverts back to its distributed state.

- In order to tackle the hidden node problem, GRCC suggests that all nodes present in the interference range become aware of the ongoing transmissions. The CH is responsible for forming this Steiner nodes subset such that when information is passed on to this subset, it is certain that all the nodes in the interference range receive this information. Information in this context refers to the RTS/CTS and AT/ST signals. The Steiner nodes selection algorithm and other details are discussed in the earlier chapters.

Each node in the network maintains the following data structures:

- neighbor list table elements
  - Neighboring nodes – nodes in the immediate transmission range
  - Priority – Low Priority (LP) or High Priority (HP)
  - Egocentricity (\(i\)) of each node – degree of selfishness as perceived by the node.
• retry count (applicable only to low priority nodes)
• The expected backoff value (ExpBOV) for the transmission,
• Access values for sender(S) and receiver(R) (Sendacc for S,Recvacc for R)

- Count variables
  • HPsend – Total number of transmissions by a HP node
  • HPrecv – Total number of receptions by a HP node
  • LPsend – Total number of transmissions by a LP node
  • LPrecv – Total number of receptions by a LP nodes

Using these count variables, the Access ratios for the priority levels can be calculated separately as discussed in Chapter 4.4.

- Counters:
  • Backoff counter
    The backoff counter is a random number selected by each node from its contention window range \( W \), as in IEEE 802.11 DCF.
  • Section counter
    The section counter of a node comes into play once a CH is elected upon collision caused by hidden terminal problem. It spans the length of a section \( W \) which is determined by the CH. When the section counter reaches zero after waiting \( W \) idle slots, the CH broadcasts SE message which is followed by the polling session. Next section begins when the CH broadcasts a SS message.
7.3.1.1 Differentiated Service Provisioning and Avoiding Priority Reversal

Priority reversal occurs when a low priority node has its backoff at zero while nodes at a higher priority are in contention. This can lead to a situation with the lower priority node grabbing the channel before the higher priority nodes. When a sender’s backoff counter reaches zero, it broadcasts an Alert Transmission packet. Every other node receiving the AT packet will check the priority of the sender. If a node finds its priority to be higher, it sends a Suspend Transmission packet to the sender. This is represented by messages 10 and 11 in Figure 7.1. Node 8 initiates an AT packet and node 11 which has a higher priority cancels its transmission attempt by sending an ST packet.

The ST packet contains the current backoff value, $curr$ of the HP (high priority) node sending ST. After sending ST, the HP node waits for an SIFS period and then starts counting its backoff timer to zero. Once an LP node receives the ST packet, it resets it backoff value as stated in Equation (3.2).

However, the Initial Backoff value of the LP node remains the same. Additionally, the node maintains a $backpri$ variable which is initialized with the node’s Initial Backoff, and after each ST received, the $backpri$ is modified if necessary, as discussed in Chapter 3.3.1. The ST packets, thus, help to resolve the priority reversal issue.
1- AT from N1 to N3
2- RTS from N1 to N3 (Since no ST)
3- RTS from N5 (Steiner node) to N3 resulting in collision (Hidden terminal problem)
4- RTS from N1 to elected CH
5- RTS forwarded from CH to N3
6, 7- CTS issued to N1 forwarded via CH
8- CTS from CH to N5 (Steiner node)
9- CTS from CH to N6 (Steiner node)
10- AT from N8 to N9
11- ST from N11 to N8 (Avoiding priority reversal)
12- RTS from N11 to N10 (After backoff ticks 0) – No CTS issued due to identification of selfishness (ε > 10)

Figure 7.1 Schematic representation of Integrated QoS Enhanced MAC model

7.3.1.2 Starvation Avoidance

The excessive starvation of a low priority node is avoided using a retry count, based on the number of nodes in the network and network
characteristics. Once a node’s retry count reaches a threshold value, the initial backoff counter value is overwritten and a slot time is added to it and is used to overwrite the new backoff value which denotes the current or active backoff value of the low priority node. The backoff values of the nodes are reset as discussed in Chapter 3.3.2. This scheme thus avoids starvation of low priority nodes for the channel access. Even the low priority selfish nodes win the contention for channel in this scheme but they will be discerned in the next stage when they handshake with the receiver by exchanging RTS and CTS messages.

7.3.1.3 Selfish Misbehavior Detection

IEEE 802.11 DCF favours the node that selects the smallest backoff value among a set of contending nodes. Nodes may misbehave by manipulating their backoff value in order to gain an unfair advantage. In order to identify selfish misbehavior, each node calculates expected backoff value for every other node, i.e., the expected time interval the node has to wait before attempting the next transmission. This will allow the neighboring nodes to detect if the sender initiates its next AT packet without waiting for the stipulated backoff value. The RTS and ACK packets also include the backoff value and can be used to calculate expected backoff for subsequent transmissions. Thus, the egocentricity of the sender node is monitored by the other nodes and the misbehavior is detected.

The egocentricity of a node is calculated based on its medium access ratio over a period of time as discussed in Chapter 4.4. Table 7.1 shows an extended neighbor list table maintained by a node in a network with threshold value RC_MAX fixed at two.
Table 7.1 Extended Neighbor List table

<table>
<thead>
<tr>
<th>Neighbor nodes</th>
<th>Priority 0 – LP</th>
<th>Egocentricity (e)</th>
<th>Expected Backoff (ExpBOV)</th>
<th>Current Retry Count (RC value) RC_MAX=2</th>
<th>Access values as sender (SendAcc)</th>
<th>Access values as receiver (RecvAcc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>--</td>
<td>13</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>--</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>1</td>
<td>17</td>
<td>2</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>9</td>
<td>--</td>
<td>11</td>
<td>10</td>
</tr>
</tbody>
</table>

-- : Not applicable  Contention window, W = 20

All neighboring nodes can overhear AT and ST packets. On overhearing the AT packet, each node updates its table with the RC of the low priority sender node. Later, when a LP node temporarily becomes a HP node, its RC in all neighboring nodes’ tables would be maximum RC. Otherwise the LP node is detected as misbehaving by initiating a transmission without waiting for the stipulated backoff time and its egocentricity is incremented by one.

The LP sender calculates the Backoff value for its next transmission as described in Equations (4.4) and (4.5). The HP sender also takes a similar approach in calculating its BOV. The other nodes by overhearing the RTS and CTS frames can uniquely identify the sender (S), receiver (R) and its backoff values (SendBOV from S in RTS, RecvBOV from R in CTS). These nodes calculates the expected Backoff value (ExpBOV) and record it in the neighbor list table and increase the access value for sender and receiver after the DATA and ACK transmissions respectively.

Suppose the RTS is unsuccessful, the sender selects a new backoff using a deterministic function, as stated in Equations (4.6) and (4.7). The
receiver counts the number of idle slots during the interval between the sending of ACK, and the reception of the next RTS from the sender. The sender may misbehave by backing off for a lesser duration than the value assigned to it by the receiver. If the sender is observed to be manipulating the backoff value, it is marked as selfish and its egocentricity is increased. The misbehaving sender is penalized by assigning to it higher backoff values in subsequent transmissions. This backoff value is assigned to the sender depending on its egocentricity. If the sender is detected as misbehaving node, no other nodes send CTS to the sender. The transmission from the sender is blocked and it is, thus penalized.

There also exists a possibility that the receiver may misbehave in assigning backoff values. Receiver misbehavior is to assign small backoff values to a preferred sender to receive data from that sender at a rate higher than the fair rate. This type of attack is possible, when the receiver is expecting some data from a particular sender and seeks to obtain that data with minimal latency. This misbehavior can be detected using an approach similar to that used for detecting sender misbehavior. The neighboring nodes can monitor the backoff values assigned by the receiver R and decide if R is assigning small backoff values to any particular sender. Also by monitoring the sender S, they can verify if a receiver correctly penalizes a misbehaving sender.

7.3.1.4 Resolving Hidden Terminal problem

To address the hidden terminal problem caused by the Steiner nodes a CH is elected by using the modified KEL Algorithm. The CH is responsible for broadcasting AT/ST signals and guaranteeing that all the nodes in the interference range receive this information.
Cluster head election depends on the location and the egocentricity of nodes which are maintained in the neighbor list. If the egocentricity of a node transmitting the cluster head beacon is found to be greater than the threshold value indicating the selfishness degree of the node, the beacon is ignored and the node is permitted to be the cluster head. Finally, the node which successfully attains the channel will become the cluster head as stated in Chapter 5. The KEL algorithm stated in Chapter 5 is enhanced with the following steps appended to fix the cluster head, taken into consideration, the selfish behavior of nodes.

if egocentricity < 10
   other nodes accept it as the CH
else

   Nodes wait for the beacon from some other node which has the reference point similar to them with less egocentricity.

7.3.1.5 Consistent Information Management: Avoiding Stale Updates

The Data source is a centralized data store which provides consistent information to the nodes in the MANET. If all the nodes approach the data source alone, then it may lead to congestion and single point of failure. Caching helps in reducing communication which results in saving bandwidth as well as battery energy. In a stateful approach such as the SPP the data source node maintains the TTR value and the cache query rate associated with each cache copy. The cache updating algorithm proposed in Chapter 6 can reduce the number of hops the updates propagate through using bandwidth in an effective manner.

The data source node calculates the time span of the updating process and then sets the optimal TTR value to the nodes which receive the updates. It maintains a cache status table which has the entry for TTR value
and the Query rate. The data source node makes online decision on to, which node it should send update.

Conditions to remove the stale updates in the caches and providing omega consistency are applied. The traffic overhead and delay in receiving the update are very less in SPP approach when compared to other traditional approaches. Also the omega consistency achieved by this approach is handy in providing less query delay and traffic overhead.

7.4 SIMULATIONS

The proposed QoS model is validated using ns-2 advanced simulation platform. For the simulation, two different scenarios are considered with varying parameters as shown below in Table 7.2. The performance of the model is compared with the 802.11 DCF, which is extended to incorporate functionalities to alleviate the intensiveness of challenges such as priority reversal in services differentiation, selfish misbehavior, packet loss due to hidden terminal problem and stale updates by adopting AT-ST scheme, Persistent DCF model, Ren Wei’s algorithm and DynTTR mechanisms.

<table>
<thead>
<tr>
<th>Table 7.2 Simulation Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Percentage of selfish misbehaving nodes</td>
</tr>
<tr>
<td>Percentage of Steiner nodes</td>
</tr>
<tr>
<td>Percentage of low priority nodes</td>
</tr>
<tr>
<td>Number of nodes in the MANET</td>
</tr>
<tr>
<td>MAC Header</td>
</tr>
<tr>
<td>Data Rate</td>
</tr>
<tr>
<td>Number of cache nodes</td>
</tr>
<tr>
<td>Network Area</td>
</tr>
<tr>
<td>Mobility model</td>
</tr>
<tr>
<td>Propagation model</td>
</tr>
<tr>
<td>Traffic model</td>
</tr>
</tbody>
</table>
From the simulation study under these scenarios, four major performance metrics namely packet loss rate, traffic overhead, delay and average throughput are compared for the extended 802.11 DCF and the proposed Integrated QoS Enhanced MAC model.

Packet loss may be due to selfish nodes dropping packets wantedly to save their battery power, existence of hidden terminals, and packet forwarding in multihop communication. Simulation results in Figures 7.2 and 7.3 show that the packet loss is less in the proposed model than in extended 802.11 DCF.

![Figure 7.2 Comparative analysis on packet loss rate– Scenario 1](image)

![Figure 7.3 Comparative analysis on packet loss rate – Scenario 2](image)
Traffic overhead is typical in a network where there is much packet forwarding. In the extended 802.11 DCF using traditional Pull model, there is more traffic overhead due to frequent updates in the caches. Also, more number of retransmissions caused by loss of packets incurs additional traffic overhead. In the Integrated QoS Enhanced MAC model, though the above stated problems are eliminated, there is still considerable amount of traffic due to the forwarding of CTS to all the Steiner nodes by the cluster head. Comparative analysis on traffic overhead for period of time is validated by simulation. Figures 7.4 and 7.5 show that the traffic overhead in the proposed model is still lesser than the extended MAC model.

Figure 7.4 Comparative analysis on traffic overhead – Scenario 1

Figure 7.5 Comparative analysis on traffic overhead – Scenario 2
Comparative analysis on end-to-end delay for increase in period of time is validated by simulation. End-to-end delay is comparatively equal in both the models as shown in Figures 7.6 and 7.7. The delay incurred in the proposed model by forwarding the packets through the CH is compensated by the reduction in retransmissions at the MAC layer.

![Figure 7.6 Comparative analysis on end to end delay – Scenario 1](image1)

![Figure 7.7 Comparative analysis on end to end delay – Scenario 2](image2)

Finally, the average throughput of the models is compared under the two defined scenarios. Figures 7.8 and 7.9 show that the average throughput is almost stable in the proposed model when the number of nodes in the network increases as against the extended 802.11 DCF.
7.5 CONCLUSION

An Integrated QoS Enhanced MAC model has been designed to resolve diverse issues in a typical MANET. The model can be employed in applications requiring differentiated services. Fairness provisioning and misbehavior avoidance are handled effectively in a distributed manner. The proposed model also reduces bandwidth consumption through cooperative caching. Simulation results reveal that packet loss percentage and the traffic overhead have decreased when compared to the extended 802.11 DCF MAC. The end-to-end delay is almost the same in both the models but the average throughput which is the main determining factor in assessing the QoS is more efficient in the proposed Integrated QoS Enhanced MAC model.