Journal of Sustainable Development in Africa (Volume 10, No.2, 2008)

ISSN: 1520-5509

Clarion University of Pennsylvania, Clarion, Pennsylvania

FLOW RESERVATION STRATEGY FOR QOS IN MANETS

W. Munyoka
Bindura University of Science Education

C. Gombiro
Bindura University of Science Education

Abstract

Mobile ad hoc Networks research is gaining momentum of late. Mobile ad hoc networks (MANETs) are also gaining increased attention in the research community because of the great possibilities they provide in many applications such as conferences, disaster recovery, military systems, as well as other environments that require the establishment of dynamic networks between mobile devices without existing infrastructure

Mobile ad hoc networks (MANETs) provide a powerful and dynamic platform to enable mobile computers to establish communications without an existing infrastructure. In order to provide support for multimedia applications, Quality of Service (QoS) support becomes an important component in their design.

In this document we provide a detailed description of our theoretical proposed flow reservation strategy which we proposes to run in 802.11 ad hoc networks to provide some QoS guarantees to high priority traffic targeting Internet Service Provider,

Mobile phone services, Mines, mobile GIS computing and its application in emergency disaster notification information management system; with reference to Zimbabwean Telecommunications industry. We give brief link up on IEEE 802.11 and state hidden node problem found in IEEE 802.11. We also deal with the real impact of transmission in terms of used bandwidth and state how estimation of bandwidth should be handled. We further give details of our strategy and provide details of integration of our strategy with Ad-hoc On Demand Routing protocol.

Introduction

Networking and communication systems are rapidly growing in use world wide, and Africa is not an exception. Zimbabwe is on a verge of Telecommunications expansion and diversification, as the three major mobile operators Net*One, Econet

and Telecel transform into the GPRS and 3G platforms. Apart from offering more lines to consumers, there is a great need for coming-up with a QoS Flow Reservation Strategy. Increasingly, higher data throughput mobile networks (GPRS, EDGE, 3G and HSDPA) can support the rising demand for mobile data services. The telecommunications industry consist of a pool of different (heterogeneous) networks which include fixed ,wireless and mobile ad-hoc Networks(MANET)These network service indeed chew a lot of bandwidth hence requiring Quality of Service(QoS).

A mobile ad-hoc network (MANET) is a wireless network temporarily and spontaneously created by mobile stations without requiring any infrastructure or central control. Network managements and communications are typically performed in a distributed manner. Though ad-hoc networks are treated with little difference in IEEE standards for wireless networks as a whole, some unique features make ad-hoc networks distinct from other types of wireless networks such as wireless Local Area Networks (LANs). In a MANET, mobile nodes establish a network on the fly as they come within range of each other. Communication between two nodes is done either directly with 1-hop if they are within range of each other, or indirectly using multiple hops through intermediate nodes. Nodes are free to move around, join and leave the network as needed. As this happens, new links form as nodes come within range of each other, and existing links break as two nodes move out of range of each other.

Ad hoc network nodes operate in a very volatile environment where any connection could be dropped at any moment. Ad-hoc networks are a special class of wireless networks where there is no such fixed infrastructure as base stations for allocating channels, controlling usage, or provisioning of services. Rather, they need to be adaptively self-organizing. Any node in an ad-hoc network can transmit, receive, or relay signals.

A strategy is required to ensure predetermined service performance constraints. This strategy consists of avoiding the wastage of resources and interference with other on-going communications. Resource management in ad hoc networks has two main functionalities, which are: *admission control* and *resource reservation*. The source node investigates available resources on the path towards the destination node before admitting the flow (*admission control*). If there are enough resources to carry the flow without interfering with any ongoing communication, corresponding resources are reserved (*resource reservation*) and transmission begins.

In our approach we are utilizing HELLO messages from AODV routing protocol to send bandwidth information to neighbors, so that they can make necessary reservations based on the available bandwidth. Our approach tries to solve the problem of determining interference caused by transmission between two nodes in an 802.11 ad-hoc network in other nodes that are in their coverage area.

In this paper we are also highlighting the problems of differentiation mechanisms. In order to solve these issues we first carry out an evaluation of service differentiation mechanisms by way of simulations. On the issue of tackling the problem described in the problem statement there is a need for nodes (stations) to be equipped with the following:

1. Resource estimation (estimating available bandwidth).
2. Admission control based on available bandwidth.
3. Flow reservation after the admission control.

Model Classification

QoS in MANETs has been widely recognized as a challenging problem. Characteristics of MANETs such as mobility, the dynamics of the environment, and

the uncertainty of resource availability, make the provisioning of QoS guarantees difficult. In this paper we classify QoS models into the following four major groups:

- Models that are based on per-flow resource reservations (IntServ);
- Models that ensure per-class service differentiation (DiffServ);
- Hybrid models with both resource reservations and DiffServ;
- Models that consider QoS extensions to existing routing protocols.

An argument in favor of resource reservation solutions is that in MANETs, less traffic is expected than in the Internet. Therefore, the network can afford the added overhead of maintaining reservations on a per-flow basis. Since both approaches have their drawbacks, hybrid approaches are also of interest. In contrast to the first three types of models, QoS models can also be implemented as extensions to existing routing protocols.

Reservation-based models

INSIGNIA [23] is a QoS framework based on end-to-end per-flow resource reservations. In this framework, the reservation request for a flow specifies the maximum and minimum bandwidth requirements. A resource reservation for a flow is created during connection setup when a minimum bandwidth is negotiated. A route satisfying the request is provided by one of the existing MANET routing protocols. Reservations are soft-state: when a node has not received packets from a given flow for a certain period of time, the resources it has reserved for that flow are released. For the time the reservation exists, the destination monitors packet loss, delay, and throughput, and informs the source of possible deviations with respect to the negotiated bandwidth. When a deviation occurs, the reservation is adapted to offer a lower quality. INSIGNIA evaluates its model through simulations for various traffic, mobility, and channel conditions.

Similar to the work in INSIGNIA, in [12] QoS routing with per-flow end-to-end resource allocation is proposed. Unlike INSIGNIA, here message types of existing ad-hoc routing protocols like TORA query and reply and DSR/AODV route request and route reply are used, to identify nodes that fulfill the QoS requirements and to reserve resources. Again reservations are soft-state. Unlike INSIGNIA, this scheme does not consider adaptation, that is, it does not offer a lower QoS when the required QoS can no longer be guaranteed.

DiffServ-based models

SWAN [21][3] introduces a QoS model in which real-time traffic gets priority on a per-packet basis by means of controlling the amount of best-effort traffic accepted per node. In this sense SWAN is close to DiffServ. The amount of best-effort traffic that can be admitted is controlled by monitoring the delay suffered by real-time traffic. The evaluation of SWAN consists of simulations in terms of delay and throughput (for different mobility conditions) and measurements of a (very simple) wireless test bed in terms of delay (but the nodes do not move). In SWAN, each node monitors the delay suffered by the real-time traffic.

In [22], another DiffServ-like QoS solution is proposed. Different flows are assigned different priority classes and are given differential treatment. The idea is to define three queues per physical interface, each with two levels of precedence. Priority scheduling and round-robin scheduling are used to schedule the packets out of the queue. The performance analysis consists of simulations in terms of throughput and delay for different mobility scenarios and queuing schemes.

Hybrid models

A QoS model, coined the Flexible Quality of Service Model for MANET (FQMM) [26], proposes a combination of IntServ and DiffServ. Both IntServ and

DiffServ have their drawbacks: IntServ [9] has scalability problems and causes high processing overhead at the routers. DiffServ [8], in turn, does provide service differentiation among traffic aggregates over a long time scale, while for short time scales; it is difficult to provide QoS given the varying conditions in MANETs. Because of this limitation and assuming that MANETs have less traffic load than the backbone of the Internet, FQMM proposes a hybrid scheme with per-flow resource reservations for high-priority traffic and per-class service differentiation (DiffServ) for low-priority traffic. The performance analysis of FQMM is done via simulations in terms of throughput for different traffic scenarios.

QoS routing models

In this section we review models, which propose extensions for QoS to existing routing protocols such as Ad-hoc On-demand Distance Vector (AODV) routing and Dynamic Source Routing (DSR). Both AODV and DSR are on-demand routing protocols, which means that they can take QoS information into account during the route discovery process. The QoS model in [24] introduces extensions to AODV, which consist of additions to the route request and route response packets during the route discovery process. Moreover, the following QoS information is added to the routing table: the minimum available bandwidth, the maximum delay, and a list of sources, which have requested bandwidth or delay guarantees. A monitoring mechanism informs the source node that the required quality cannot be delivered anymore. In [25], QoS extensions to DSR are proposed, which consist of applying monitoring of the signal to noise ratio (SNR) to detect routes that, although in use, are likely to break soon. The model considers a threshold for the average SNR. Only when a node receives a route request and its average SNR is higher than the threshold, the node will take the request into consideration and forward it. This is to

avoid those nodes that accidentally receive a route request because their SNR is abnormally high, forward it and help to find a route that, in the end, will not have an acceptable

SNR.

The algorithm in [20], called Core-Extraction Distributed Ad-hoc Routing (CEDAR), considers a selected group of nodes, coined the core, which is responsible for performing routing computations taking into account QoS. The reason why this algorithm is mentioned here is because of the way in which links of different quality are treated. In CEDAR, the establishment of the core is a purely local computation (a node does not need to know the topology of the entire network). When a change in the topology occurs, the core recomputation will only occur in the vicinity of the topology change. Information about low bandwidth or unstable links is treated differently from information about relatively stable high-bandwidth links. Whereas the first is propagated throughout the core, the second stays local. Each core node maintains information about its local topology and link-state information of relatively stable high-bandwidth links further away (information about unstable or low-bandwidth links must not be propagated throughout the network; this is specified by a time-to-live field). For each link, nodes are responsible for monitoring the available bandwidth and informing the network. A core node will cache the available bandwidth of each link. The performance analysis of CEDAR is done through simulation using bandwidth as performance metric for different mobility scenarios. CEDAR is also implemented in a proof-of-concept demonstrator.

CEDAR (Core Extraction Distributed Ad Hoc Routing Algorithm)

CEDAR [19] aims at finding a route through the network that satisfies the minimum bandwidth requirements of an application with high probability. A set of

nodes is distributively and dynamically elected to form the core of the network by approximating a minimum dominating set of the ad hoc network using only local computation and local state. Each core node maintains the local topology of the nodes in its domain and also performs route computation on behalf of these nodes. QoS routing is achieved by propagating the bandwidth availability information of stable high bandwidth links to core nodes far away in the network, while information about dynamic links or low bandwidth links is kept local. Route computation first establishes a core path from the dominator of the source to the dominator of the destination. Using this directional information, CEDAR iteratively tries to find a partial route from the source to the domain of the furthest possible node in the core path that satisfies the requested bandwidth using only local information. Effectively, the computed route is a shortest-widest-furthest path (maximum bandwidth path) using the core path as a guideline.

Tools Used

Network Simulator (NS-2)

Simulator 2 (NS-2) [13] is a simulation tool and it is targeted at networking research based on discrete events simulations.

NS-2 provides substantial support for simulation of routing and multicast protocols over wired and wireless networks. NS-2 has an advanced 802.11 module, which is applied and verified extensively in the network community. Because simulation with 802.11 is essential in our research, NS-2 is an excellent simulation tool within this scope.

The idea of a discrete event scheduler is that actions may only be started as a result of an event. In NS-2 this is taken care of by a scheduler and a scheduling list.

Events are inserted into scheduling list upon request, together with their expiration time. The scheduler is responsible to go through the list and perform the necessary actions. Code written in c++ following the admission control algorithm will be imbedded in NS-2 simulator.

Xgraph and Gnuplot

Xgraph [18] and Gnuplot [10] are X-Window applications that include interactive plotting and graphing, and animation and derivatives. The programs are used to create graphic representations of simulation results. Output data from TCL scripts is used as data sets to Xgraph or Gnuplot. To use Xgraph in NS-2 the executable can be called within a TCL Script.

Other tools used

Other tools include AWK, *grep* and Perl scripts; these are mainly used to extract important statistics information from trace files. AWK utility allows us to do simple operations on data files such as averaging the values of a given column, summing or multiplying term by term between several columns. In our work we extensively used this utility to calculate and extract QoS metrics from trace files. The *grep* command in LINUX allows to “filter” a file. This is important because some generated trace files are enormous hence needs to be filtered.

4.1 Ad Hoc On-Demand Distance Vector (AODV)

AODV [15] is a method of routing messages between mobile computers. It allows these mobile computers, or nodes, to pass messages through their neighbors to nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can be passed. AODV makes sure these routes do not contain loops and tries to find the shortest route possible. AODV is also able to

handle changes in routes and can create new routes if there is an error. Figure 1 shows a set-up of four nodes on a wireless network. The circles illustrate the range of communication for each node. Because of the limited range, each node can only communicate with the nodes next to it.

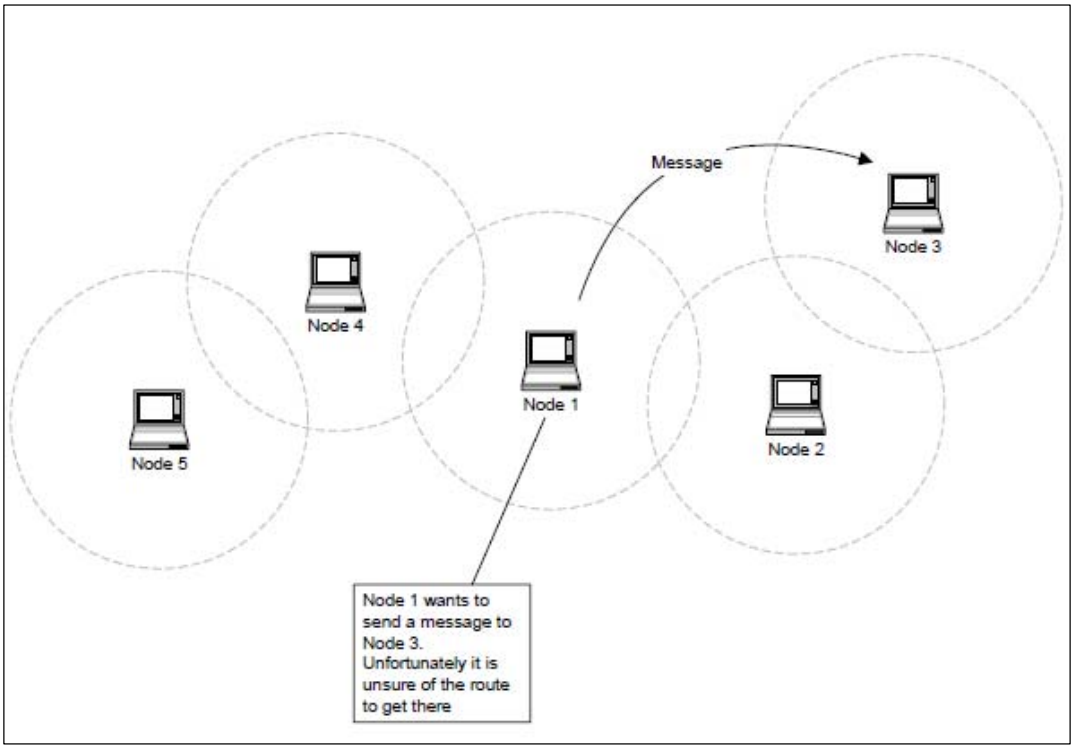

Figure 1. Sending RREQ in AODV

Nodes you can communicate with directly are considered to be Neighbors. A node keeps track of its Neighbors by listening for a HELLO message that each node broadcast at set intervals.

When one node needs to send a message to another node that is not its Neighbor, it broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message and a Sequence Number, which serves as a unique ID.

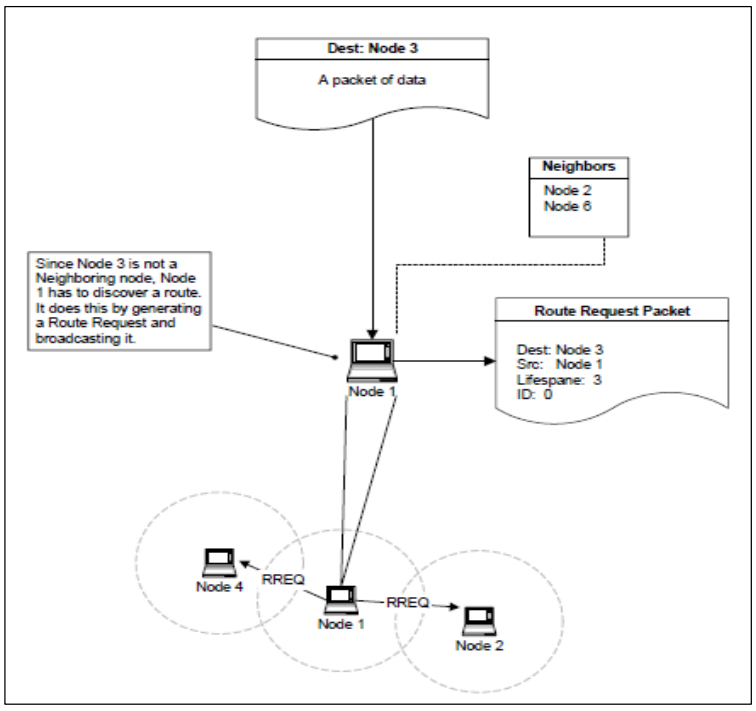

Figure 2. Node 1 wants to transmit to Node 3

In figure 2, Node 1 wishes to send a message to Node 3. Node 1's Neighbors are Nodes 2 and 4. Since Node 1 cannot directly communicate with Node 3, Node 1 sends out a RREQ. Node 4 and Node 2 hear the RREQ. When Node 1's Neighbors receive the RREQ message they have two choices; if they know a route to the destination or if they are the destination they can send a Route Reply (RREP) message back to Node 1, otherwise they will rebroadcast the RREQ to their set of Neighbors. The message keeps getting rebroadcast until its lifespan is up. If Node 1 does not receive a reply in a set amount of time, it will rebroadcast the request except this time the RREQ message will have a longer lifespan and a new ID number. All of the Nodes use the Sequence Number in the RREQ to insure that they do not rebroadcast a RREQ

In the Figure 3, Node 2 has a route to Node 3 and replies to the RREQ by sending out a RREP. Node 4 on the other hand does not have a route to Node 3 so it rebroadcasts the RREQ.

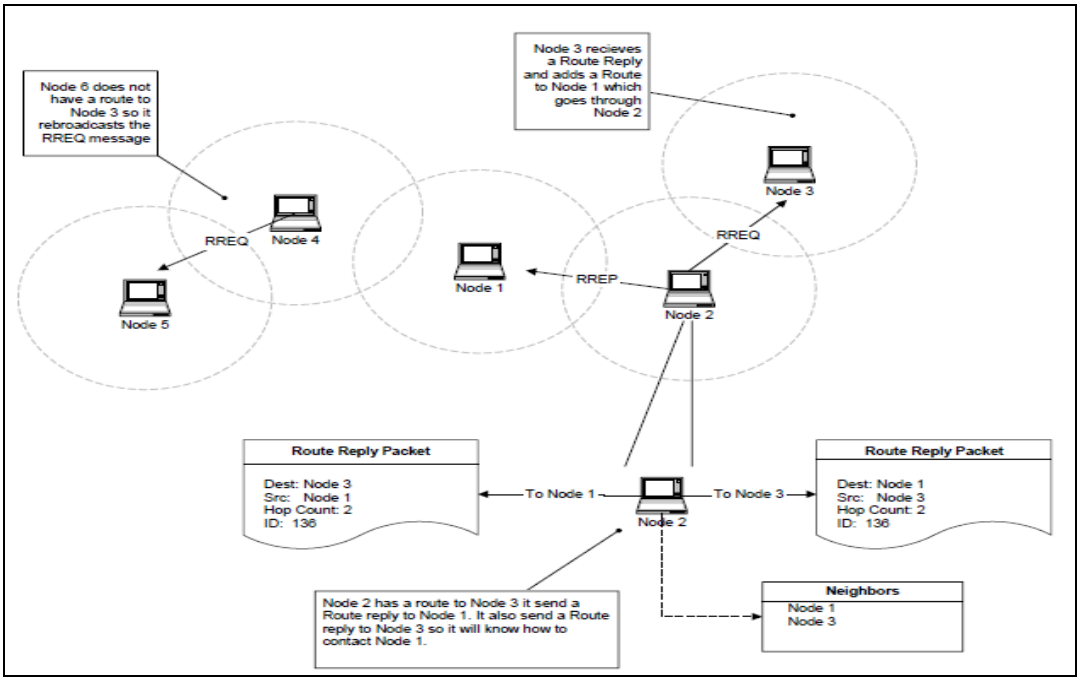

Figure 3. Node 2 Route Reply

4.1.1 Sequence Numbers

Sequence numbers serves as time stamps. They allow nodes to compare how "fresh" their information on other nodes is. Every time a node sends out any type of message, it increases its own Sequence number. Each node records the Sequence number of all the other nodes it talks to. A higher Sequence numbers signifies a fresher route. This makes it possible for other nodes to figure out which one has more accurate information.

In Figure 4, Node 1 is forwarding a RREP to Node 4. It notices that the route in the RREP has a better Sequence number than the route in its Routing List. Node 1 then replaces the route it currently has with the route in the Route Reply.

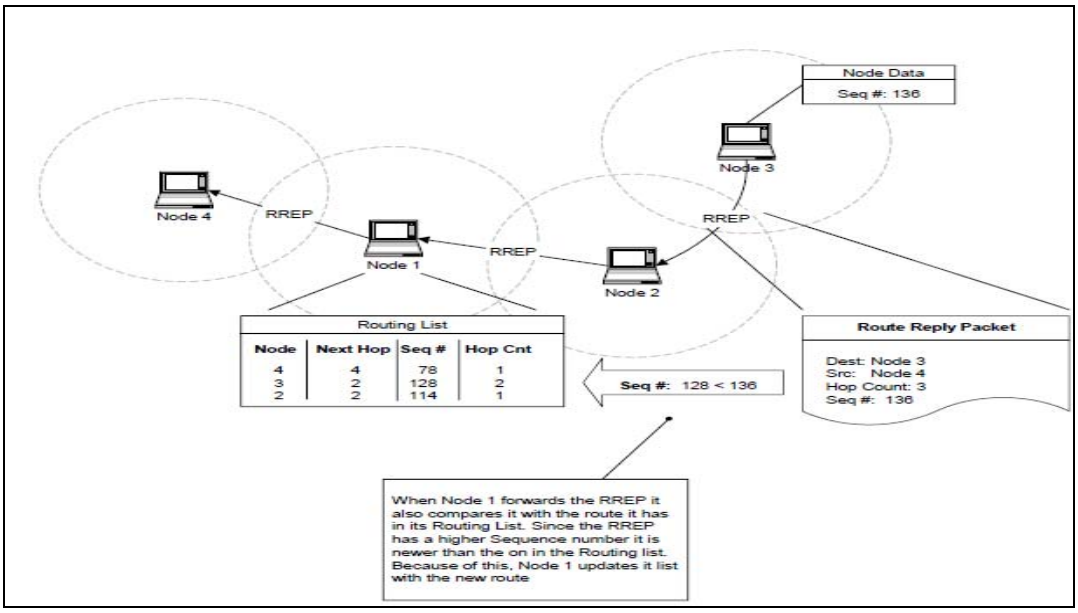

Figure 4. Sequence numbers in AODV

4.1.2 Error Messages

The Route Error Message (RERR) allows AODV to adjust routes when Nodes move around. Whenever a Node receives RERR it looks at the Routing Table and removes all the routes that contain the bad Nodes.

Figure 5 illustrates the three circumstances under which a Node can broadcast a RERR to its neighbors. In the first scenario the Node receives a Data packet that it is supposed to forward but it does not have a route to the destination. The real problem is not that the Node does not have a route; the problem is that some other node thinks that the correct Route to the Destination is through that Node.

In the second scenario the Node receives a RERR that cause at least one of its Routes to become invalidated. If it happens, the Node would then send out a RERR with all the new Nodes, which are now unreachable

In the third scenario the Node detects that it cannot communicate with one of its Neighbors. When this happens it looks at the route table for Route that uses the Neighbor for a next hop and marks them as invalid. Then it sends out a RERR with the Neighbor and the invalid routes.

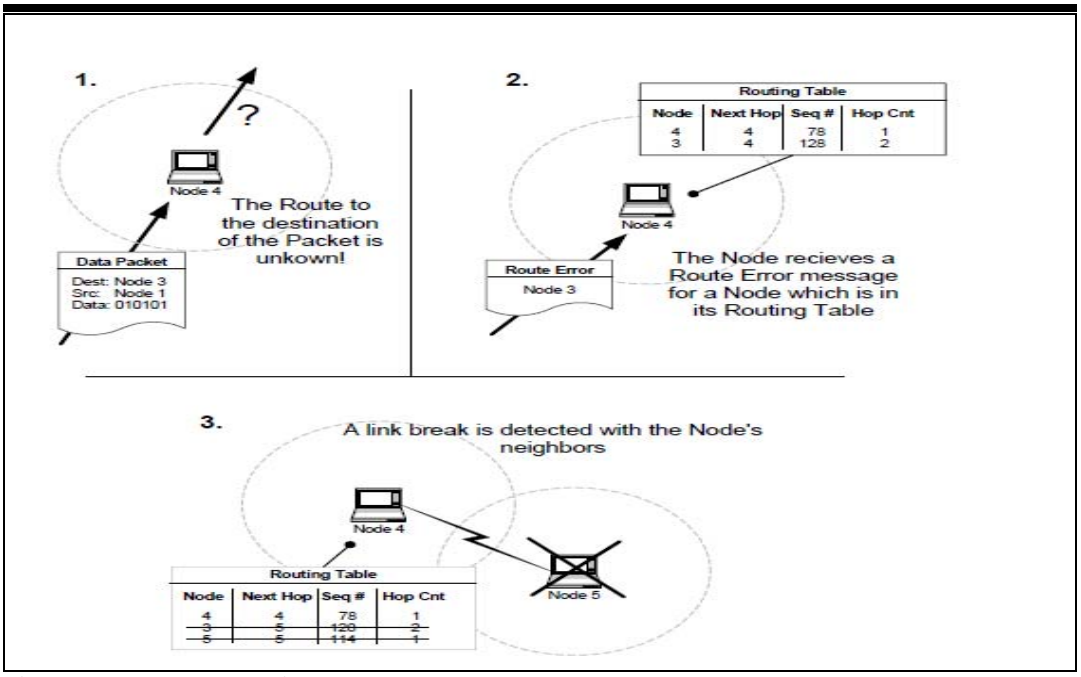

Figure 5. Error Messages in AODV

4.1.3 Hello Messages

An additional aspect of the AODV protocol is the use of HELLO messages, periodic local broadcasts by a node to inform each mobile node of other nodes in its neighborhood. Hello messages can be used to maintain the local connectivity of a node. Nodes listen for retransmissions of data packets to ensure the next hop is still within reach. If such a retransmission is not heard, the node may use any one of a number of techniques, including the reception of HELLO messages, to determine whether the next hop is within communication range. The HELLO messages may list

the other nodes from which a mobile has heard, thereby yielding a greater knowledge of the network connectivity

4.2 QoS extensions to AODV protocol

Several modifications have been carried out for the routing table structure, and RREQ and RREP messages in order to support QoS routing. Each routing table entry corresponds to a different destination node. The following fields are appended to each routing table entry:

- Maximum delay,
- Minimum available bandwidth,
- List of sources requesting delay guarantees,
- List of sources requesting bandwidth guarantees

4.3 Distributed Coordination Function (DCF)

The basic scheme for DCF is *Carrier Sense Multiple Access* (CSMA). This protocol has two variants: Collision Detection (CSMA/CD) and Collision Avoidance (CSMA/CA).

A collision can be caused by two or more stations using the same channel at the same time after waiting a channel idle period, or (in wireless networks) by two or more hidden terminals emitting at the same time.

CSMA/CD is used in Ethernet (IEEE 802.3) wired networks. Whenever a node detects that the transmitted signal is different from the one on the channel, it aborts transmission, saving useless collision time. This mechanism is not possible in wireless communications, as nodes cannot listen to the channel while transmitting, due to the big difference between transmitted and received power levels. In this case,

after each frame transmission the sender waits for an acknowledgment (ACK) from the receiver, as shown in figure 6:

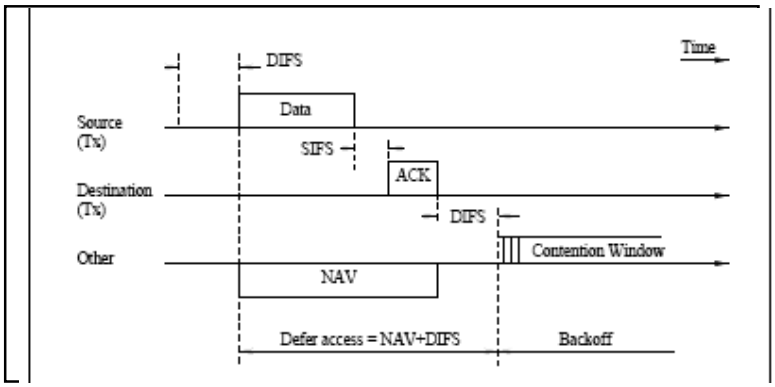

Figure 6. Basic Access Scheme

Source axis shows data transmitted by the source. The destination responds by an ACK, represented on the *Destination* axis. The third axis represents the network state, as seen by *other* nodes. Note that transmission delays are not shown. The Interframe Spacings DIFS and SIFS will be explained later in this Section.

If no ACK was returned, a collision must have occurred and the frame is retransmitted. But this technique may waste a lot of time in case of long frames, keeping transmission going on while congestion is taking place (caused by a hidden terminal for example). This can be solved by introducing an optional RTS/CTS scheme (Request to Send and Clear to Send respectively), in addition to the previous basic scheme.

In the *optional RTS/CTS scheme,* a station sends an RTS before each frame transmission for channel reservation. The destination responds with CTS if it is ready to receive and the channel is idle for the packet duration. When the source receives the CTS, it starts transmitting its frame, being sure that the channel is "reserved" for the frame duration. All other nodes update their *Network Allocation Vector* (NAV) at

each hearing of RTS, CTS and the data frames. NAV is used for *virtual carrier sensing*, detailed in the next paragraph.

This scheme is shown in figure 7. The overhead caused by the transmission of RTS/CTS frames becomes considerable when data frames sizes are small and sub-optimal channel usage takes place. Reference [6] discusses optimal data frame sizes (*RTS Threshold*) above which it is recommended to use the RTS/CTS scheme.

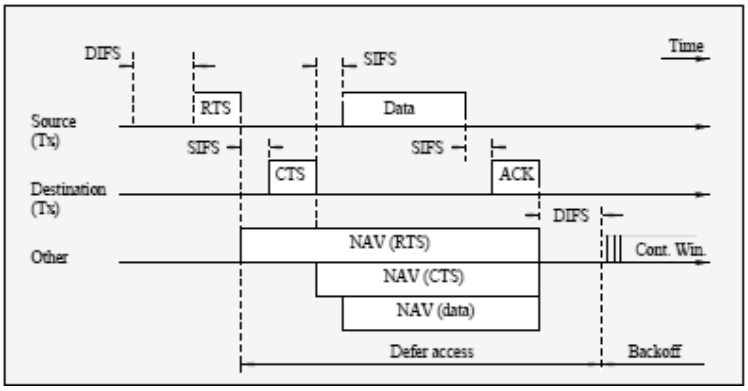

Figure 7 RTS/CTS Access Scheme

Not all packet types have the same priority. For example, ACK packets should have priority over RTS or data ones.

In DCF two Interframe Spacing IFSs are used: Short IFS (SIFS) and DCF IFS (DIFS), where SIFS is shorter than DIFS (See fig 6 and fig 7). As a result, if an ACK (affected with SIFS) and a new data packet (affected with DIFS) are waiting simultaneously for the channel to become idle, the ACK will be transmitted before the new data packet (the first has to wait SIFS whereas the data has to wait DIFS.)

Carrier sensing can be performed on both layers. On the physical layer *physical carrier sensing* is done by detecting any channel activity caused by other

sources. On the MAC sub-layer, *virtual carrier sensing* can be done by updating a local NAV with the value of other terminal's transmission duration. This duration is declared in data frames, RTS and CTS frames. Using the NAV, a node MAC knows when the current transmission will end. NAV is updated upon hearing an RTS from the sender and/or a CTS from the receiver, so the hidden node problem is avoided. In our work will use this mechanism to estimate the available bandwidth to be reserved.

The collision avoidance part of CSMA/CA consists of avoiding packet transmission right after the channel is sensed idle (+ DIFS time), so it won't collide with other "waiting" packets. Instead, a node with a packet ready to be transmitted waits a random time after the channel being idle for DIFS, backoff time, shown in fig 6 and fig 7. Backoff time of each node is decreased as long as the channel is sensed idle (during the called *contention window*). When the channel is busy, backoff time is frozen. When backoff time reaches zero, the node transmits its frame, but if the channel is sensed busy because of another "waiting" frame, the node computes a new random backoff time, with a new range. This range increases exponentially as 2^{2+i} where *i* (initially equal to 1) is the transmission attempt number. Therefore, the backoff time equation is:

$$Backoff\ time = [\ 2^{2+i} * \text{rand}\ ()] * Slot\_Time \quad \textbf{[0.1]}$$

Where Slot_time is function of some physical layer parameters, and rand () is a random function with a uniform distribution in [0, CW]. There is a higher limit for retransmission attempts *i*, above which the frame will be dropped. Collision avoidance is applied on data packets in the basic scheme, and on RTS packets in the RTS/CTS scheme. All nodes have equal probability to access the channel, thus share it equally.

4.4 IEEE 802.11

In general, the IEEE 802.11 [17] standard covers the MAC sub-layer and the physical (PHY) layer of the OSI (Open System Interconnection) network reference model. Logical Link Control (LLC) sub-layer is specified in the IEEE 802.2 standard. This architecture provides a transparent interface to the higher layer users: stations may move, roam through an 802.11 wireless network and still appear as stationary to 802.2 LLC sub-layer and above. . Figure 8 shows a snapshot of IEEE standardization activities done for 802.11 PHY and MAC layers. This allows existing network protocols (such as TCP/IP) to run over IEEE 802.11 wireless without any special considerations, just like if IEEE 802.3 wired Ethernet was deployed.

At PHY layer, first the IEEE provides three kinds of options in the 2.4 GHz band. The three PHY layers are an Infrared (IR) baseband PHY, a Frequency Hopping Spread Spectrum (FHSS) radio and a Direct Sequence Spread Spectrum (DSSS) radio. All three PHY layers support both 1 and 2Mbps operation. In 1999, the IEEE defined up to 11Mbps 802.11b in the 2.4 GHz free ISM (Industrial, Science, and Medical) band and up to 54Mbps 802.11a OFDM in 5GHz frequency. Ongoing 802.11g will extend 2.4GHz 802.11b PHY layer to support at least 20Mbps rate. Moreover, 802.11h will enhance 802.11a in the 5GHz band, adding indoor and outdoor channel selection for 5GHz license exempt bands in Europe. At MAC layer, ongoing 802.11e covers QoS support to the 802.11 wireless networks. 802.11i will enhance security and authentication mechanisms for 802.11 MAC.

The IEEE 802.11 MAC sub-layer defines two relative medium access coordination functions, the Distributed Coordination Function (DCF) and the optional Point Coordination Function (PCF). The transmission medium can operate both in

contention mode (DCF) and contention-free mode (PCF). The IEEE 802.11 MAC protocol provides two types of transmission: asynchronous and synchronous.

The asynchronous type of transmission is provided by DCF, which implements the basic access method of the 802.11 MAC protocol. DCF is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol, and should be implemented in all the stations. The synchronous service (also called contention free service) is provided by PCF, which basically implements a polling-based access method. In this paper will concentrate on DCF since it's the one that is used in ad-hoc networks.

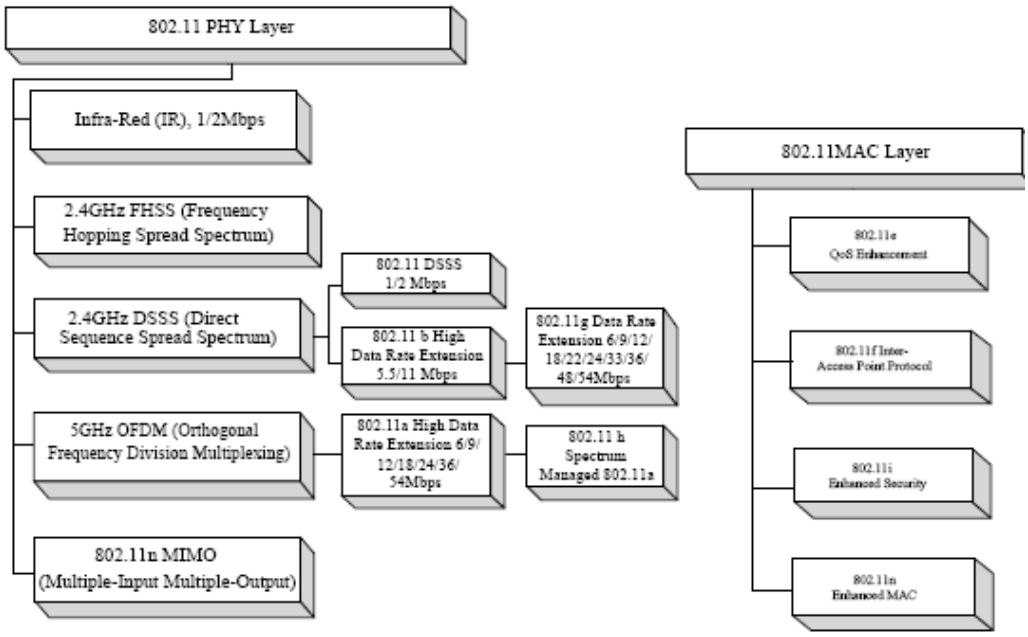

Figure 8. Snapshot of 802.11 PHY (left) and MAC (right) standardization activities

4.5 Estimating Bandwidth for Flow Reservation

Once the hidden node concept is introduced and its solution through the exchange of RTS/CTS messages is presented, we may start to design a QoS flow reservation based mechanism to these kinds of networks. The use of RTS/CTS will influence directly on our strategy, since plenty of nodes must remain frozen while a

transmission is taking place. This means that a transmission between two nodes may occupy media that was available also to other nodes, reducing their available bandwidth.

In order to know how much bandwidth is available for a node to use, we must take into consideration all transmissions that affect directly its opportunities to transmit.

In the case of 802.11, using RTS/CTS, a node is not allowed to transmit under the following cases:

1. It is receiving data;
2. One of its neighbors is receiving data (due to the reception of a CTS);
3. One of its neighbors is transmitting data to a node that is neither another neighbor nor the node itself (due to the reception of a RTS).

Representing this in an analytical way, we may state that the available bandwidth for a node *i* to transmit is given by:

$$Bi = TBi - \left(\mu i + \sum_{j \in Ni} \mu j + \sum_{j \in Ni, k \notin Ni+} \chi jk \right) \quad \textbf{[0.2]}$$

μi Represents case 1

$\sum_{j \in Ni} \mu j$ Represents case 2

$\sum_{j \in Ni, k \notin Ni+} \chi jk$ Represents case 3

Where:

- Bi is the available bandwidth (in bps) for node *i*;

- TBi is the total media bandwidth (in bps) for node *i*;
- μi is the total traffic (in bps) received by node *i* (either if node *i* is the destination of the traffic or if it just forwarding);
- χjk is the total traffic (in bps) being sent from node j to node k;
- Ni is the set of neighbors of node *i*;
- Ni+ is the set of neighbors of node *i* and the node *i* itself.

4.6 Proposed Flow Reservation Strategy

We propose flow reservation strategy based on the computation of the available bandwidth by each node of the network in a distributed way. We will analyze bandwidth using NS-2 simulation. Using simulation results, it is possible to determine how much available bandwidth is to be reserved for a node. This makes it possible to define a simple mechanism to allow per-flow Reservation. This strategy is intended to be used on ad-hoc networks based on 802.11, which should be capable of isolating QoS traffic from the ones with no QoS requirements.

4.6.1 Calculating Available Resource

Flow reservation strategy is based on the computation of the available bandwidth by each node of the network in a distributed way. By knowing its available bandwidth, a node is able to accept or reject a new reservation. So, the first step is to compute the B (*available bandwidth*) of each node.

As it may be noticed in the Section 4.5, there is no way to compute the B of a node using only local information. This means that a node must get information from its neighbors to compute this value correctly. This may be done by periodically announcing some key values to every neighbor (using broadcast frames). HELLO messages for neighbor discovery (such as AODV) we proposed to extend them in order to transmit these values.

According to formulae [0.2] in section 4.5, the following values should be broadcasted periodically to every neighbor:

- Total bandwidth reserved for traffic received by the node either as the final destination or as an intermediate node (μi);
- Bandwidth reserved for traffic generated or forwarded by a node to each of its neighbors (χjk)

[0.2] supposes that all the bandwidth of the wireless media is available for being reserved. This is a very optimistic view of the problem. In real systems, however, problems like the poor quality of the transmission media and the fact that the interference range of nodes is greater than their transmission nodes makes that only a portion Q of this bandwidth is really usable.

In order to take this into account (and also in the case that we want to reserve an amount of bandwidth for best-effort traffic), we may re-write [0.2] as:

$$Bi = Q - \left(\mu i + \sum_{j \in Ni} \mu j + \sum_{j \in Ni, k \notin Ni+} \chi jk \right) \qquad \textbf{[0.3]}$$

4.6.2 Admission Control

Knowing the available bandwidth of a node is not enough for building a QoS provisioning strategy. Besides this computation, it is also necessary to check if a given flow fits or not into the link. This means that for every new flow, we should check in each node of its candidate route if the traffic that will be generated locally by this new flow fits or not into the computed available bandwidth.

In fact, we may think of several cases in which the admission control may behave differently. We will analyze each one of them and finally propose an algorithm that serves as an admission control.

4.6.2.1 One Hop path

The first, and simplest, case that may happen is when we are trying to establish a new route composed of just one hop (Figure 9). In this case, data is sent directly from the source to the destination and it is not forwarded at any time. In this simple case, the admission may behave in the following manner:

Every node: Available bandwidth Bi *must be greater or equal to the amount of bandwidth r that is trying to be reserved (*$Bi \geq r$*)*

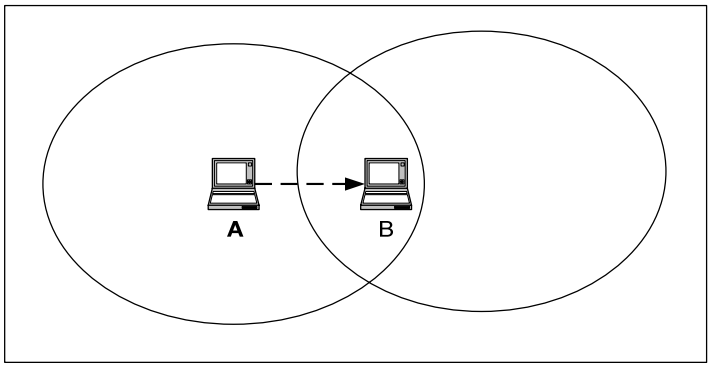

Figure 9. One hop path transmission

In the next cases, nodes should not only check for available bandwidth for transmitting or for receiving data. They should also consider the time that they must remain in frozen state due to the reception of an RTS or a CTS. Nodes that receive these packets are affected by the transmission and must be aware of this when checking if a transmission fits.

In the two-hop case (figure 10), for example, the source sends data and then, when the intermediate node forwards the packet to the destination, it receives an RTS and remains in silence (frozen). This means that although transmitting the information once, it should have the double available bandwidth so that this transmission may be successful.

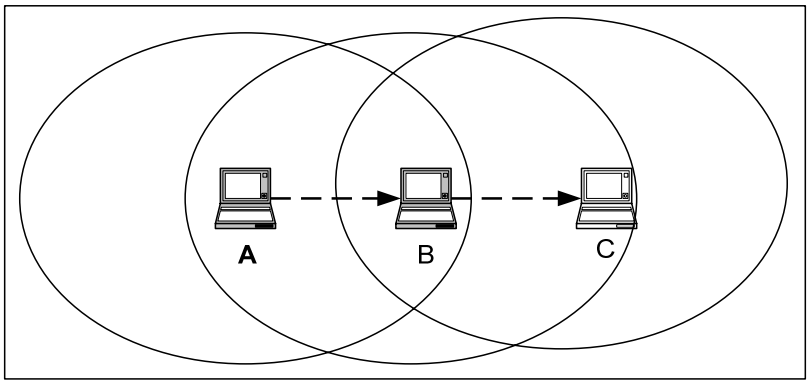

Figure 10. Transmission using two hop path

Below we present two-hop, three-hop and N-hop cases and tables that show the consequence of each transmission. Then, based on the information presented by the tables, we will build the necessary guidelines for each node in the path.

4.6.2.2 Two hop path

From Table 1 we may notice that every node is occupied twice the time of the transmission. Thus, we may state that the admission control may behave in the following way:

Source and destination nodes: $Bi \geq 2r$

Table 1. Effects of transmitting in each hop of a two-hop path

	A	B	C
Hop 1	Sender	Receiver	CTS
Hop 2	RTS	Sender	Receiver

4.6.2.3 Three Hop Path

From Table 2 we may notice that both the sender and the receiver are occupied twice the time of the transmission, while the intermediate node is occupied three times. Thus, we may state that the admission may behave in the following way:

Source and destination nodes: $Bi \geq 2r$

Intermediate nodes: $Bi \geq 3r$

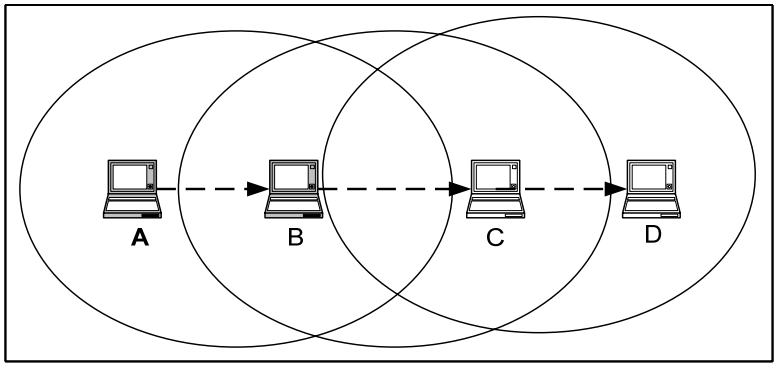

Figure 11. Transmission using three hop path

Table 2. Effects of transmissions in each hop of a three hop path

	A	B	C	D
Hop 1	Sender	Receiver	CTS	-
Hop 2	RTS	Sender	Receiver	CTS
Hop 3	-	RTS	Sender	Receiver

4.6.2.4 Any Hop path (N-hop)

From Table 3 we may notice that both the sender and the receiver are occupied twice the time of the transmission, while the second node and the one before the last are occupied three times.

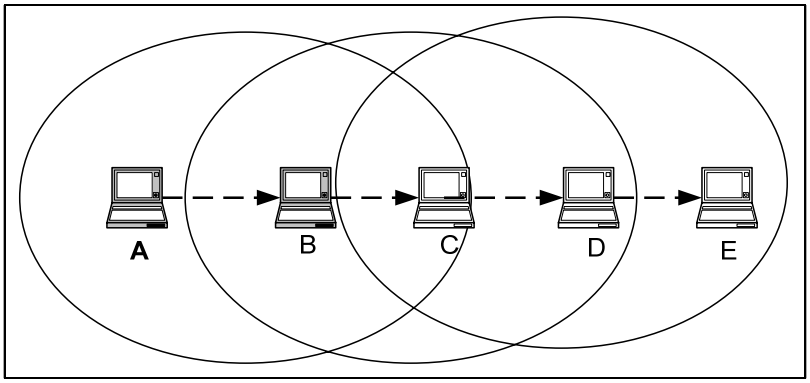

Figure 12. Transmitting using a four hop path

The one in the middle is occupied four times. This behavior will be the same for intermediate routes in any N-hop path ($N \geq 4$). Thus, we may state that the admission may behave in the following way:

Source and destination nodes: $Bi \geq 2r$

Second and *N-1* nodes: $Bi \geq 3r$

Intermediate nodes: $Bi \geq 4r$

To verify the validity of $Bi \geq 4r$ we simulated a group of eight mobile wireless hosts in chain topology (see Figure 14) within a multi-hop ad hoc network using the NS-2 network simulator. We sent CBR traffic from one host to the last host in the chain topology. The results in Figure 13 confirm that after the fourth host, the throughput normalizes for any node greater or equal to four in the topology.

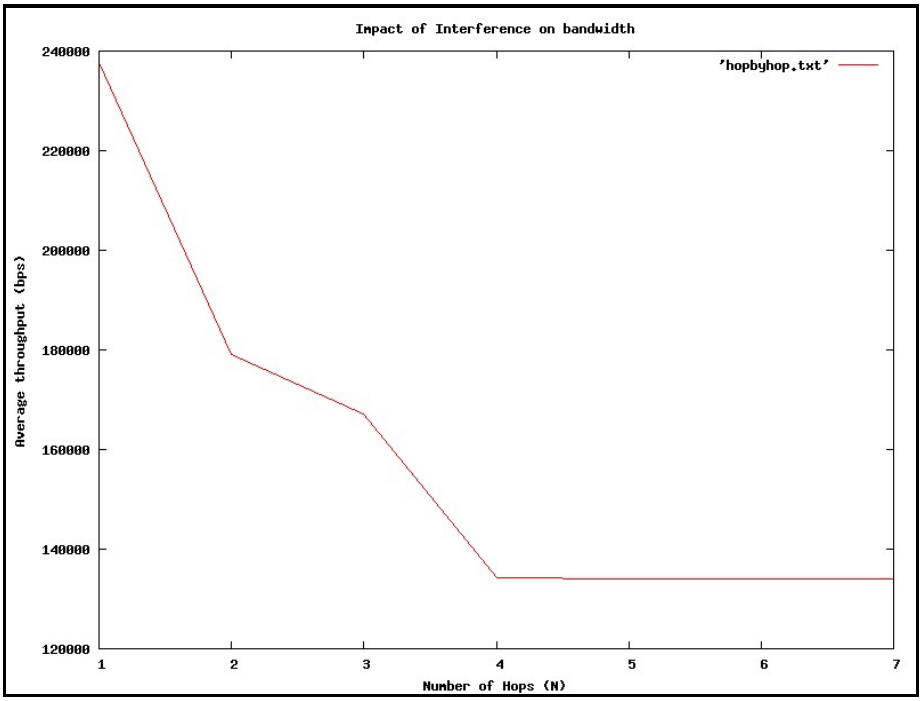

Figure13. Bandwidth normalize after 4th node on chain topology

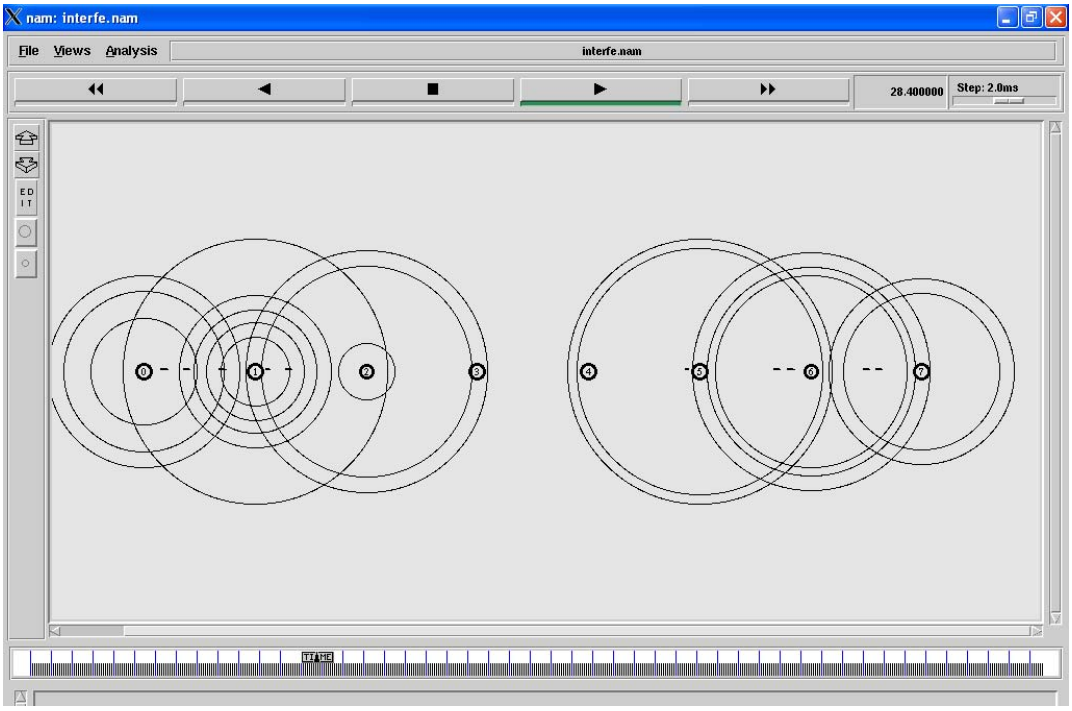

Figure 14. Chain topology simulation scenario for validating interference on available bandwidth

Table 3. Results of transmissions in each hop of a four hop path

	A	B	C	D	E
Hop 1	Sender	Receiver	CTS	-	-
Hop 2	RTS	Sender	Receiver	CTS	-
Hop 3	-	RTS	Sender	Receiver	CTS
Hop 4	-	-	RTS	Sender	Receiver

4.7 Evaluating the Impact of HELLO messages

In order to allow each node to have the complete set of information that is needed in order to compute its available bandwidth, some values must be piggybacked in HELLO messages. Figure 15 shows the impact of extending HELLO messages in the traffic seen by a single node. Although the growth is linear, HELLO packets of the node also see every neighbor, causing the overall traffic to grow exponentially. However, although the traffic growth is exponential, considering that AODV RFC [14] recommends a HELLO interval of 1 second, even when the

networks is dense (20 neighbors), the extensions in the HELLO messages causes traffic in one node to increase below 7Kbps.

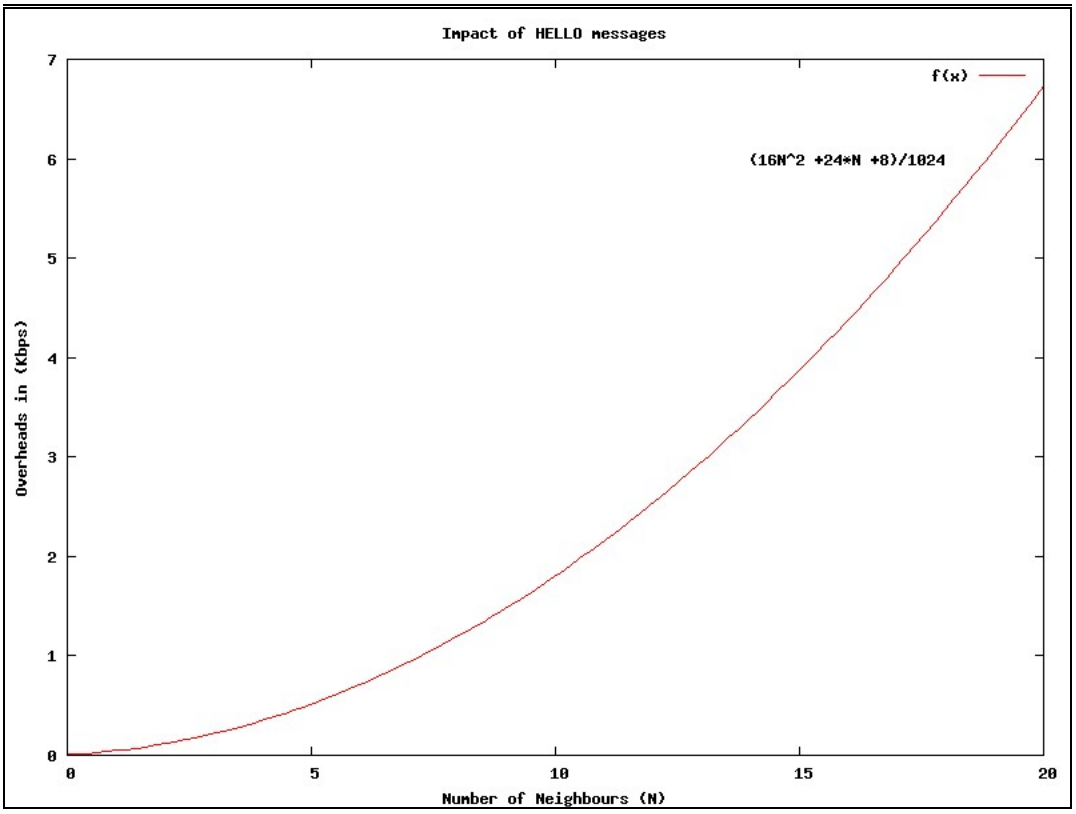

Figure 15. Impact of extra information being carried by HELLO messages

4.7.1 Admission Control Algorithm

An algorithm may be applied to accomplish every case presented in Section 4.6.2 above. In order to build this algorithm, a few characteristics may be noticed for all cases:

1. 1-hop routes may be easily identified and treated as an exception, since in this cases the destination is a neighbor (supposing neighbors are known);
2. In every other case, both in the source and in the destination $Bi \geq 2r$
3. In every other case, both in the second node and in the one before the last (when the destination is a neighbor of this node) $Bi \geq 3r$

4. In every other case, in every intermediate node $Bi \geq 4r$

Through these observations, the following algorithm may be implemented as an admission control algorithm (Figure 16) in every other node of the network:

```
if (current_node = source)
        if (destination in neighbors) {
                if ( B ≥ r ) accept new flow
                else reject new flow
        } else {
                if ( Bi ≥ 2r ) accept new flow
                else reject new flow
        }
} else if (current_node = destination) {
          if (source in neighbors) {
                if ( B ≥ r ) accept new flow
                else reject new flow
        } else {
              if ( B ≥ 2r ) accept new flow
                 else reject new flow
    }
} else if (source in neighbors OR destination in neighbors) {
          if ( B ≥ 3r ) accept new flow
          else reject new flow
} else {
        if ( B ≥ 4r ) accept new flow
        else reject new flow
}
```

Figure 16. Admission control Algorithm

4.7.2 Integrating Flow Reservation into Routing Protocol

Flow reservation strategy needs to be integrated into a routing protocol e.g. AODV [15]. The standard AODV discovers the path to the destination by broadcasting a Route Request (RREQ) message to all of its neighbors. They re-broadcast this message until it eventually reaches the destination. The destination, thus, replies the first RREQ it receives with a Route Reply (RREP) and this reply returns to the source, confirming the path that should be used to send data.

Since AODV floods RREQ to the entire network, reservations should not be done at this stage. This would cause many reservations to be done unnecessarily. The more reasonable approach is to make reservations in the way back to the source, when only one path was elected. However, although reservations are done backwards, the admission control may also function in the forward direction (when a node receives a RREQ), so that nodes that do not have enough resources to accept the new flow may be taken out from the possible routes, by not rebroadcasting RREQ messages.

Summarizing, AODV with our flow reservation strategy works in the following manner:

1. The source node applies the admission control algorithm to check if it has enough resources. If it doesn't, the flow is rejected. If it does, it broadcasts a RREQ informing the desired bandwidth.
2. Intermediate nodes that receive RREQ apply the admission control algorithm. They only re-broadcast RREQ if there are enough resources for the new flow.
3. When the message arrives at the destination, it applies the admission control algorithm and, if the new flow fits, it makes the reservation and sends a RREP back.
4. Each node that receives a RREP makes the reservation and forwards the RREP. If, for any reason there are no enough resources in the node, it does not forward the RREP back and may send a Release Reservation message to the destination (or we may just wait for the soft-state of these nodes to release already done reservations by their own).

5.0 Conclusion

We conclude by stating that our approach to provide QoS on top differentiated services in 802.11 networks is viable. If implemented, our approach will see a great

improvement in services, especially for Zimbabwe Telecommunications industry such as Internet service providers and Mobile phone services. We have presented QoS reservation strategy that takes into account the issues of interference from neighborhood traffic in order to compute its available bandwidth. We expect our admission control algorithm to block connections, which do not fit into the available bandwidth. We also believe that by being able to take into account the issues of neighborhood traffic, our approach should be able at least, to make realistic reservations.

References

Aad, I. and Casterlluccia, C. Remarks on per-flow differentiation in IEEE 802.11. In Proceedings of the European Wireless, Florence, Italy, February 2002.

Aad, I. and Casterlluccia, C. Differentiation mechanisms for IEEE 802.11. Infocom '2001, Anchorage, Alaska, April 2001.

Ahn, G.S., Campbell, A., Veres, A., and Sun, L.H., Supporting Service Differentiation for Real-Time and Best-Effort Traffic in Stateless Wireless Ad Hoc Networks (SWAN). IEEE Transactions on Mobile Computing, 1(3):192–207, July-September 2002.

Braden, R., Clark D., and Shenker, S. "Integrated services in the Internet architecture: an overview. Technical Report "1633, 1994.

Braden, R., et al. RFC 2205: Resource ReSerVation Protocol (RSVP), Sep 1997.

Chhaya, H. S., and Gupta, S. "Performance modeling of asynchronous data transfer methods of IEEE 802.11 MAC protocol". Wireless Networks, 3, 1997.

Corson, S., and Macker, "Mobile Ad-hoc Networks: Routing Protocol Performance Issues and Evaluation Considerations", IETF RFC-2501, January 1999

Differentiated Services (DiffServ) IETF Working Group. <URL:http://www.ietf.org/html.charters/diffserv-charter.html>

Integrated Services (IntServ) IETF Working Group. <URL:http://www.ietf.org/html.charters/intserv-charter.html>

Kelley Colin, Thomas Williams, and others, "Gnuplot Home page", <URL: http://www.gnuplot.info/faq/>, Accessed Nov 2005.

Kunz, T., Ge Y., and Lamont, L., "Quality of Service Routing in Ad-hoc Networks Using OLSR," in Proceeding of the 36th Hawaii International Conference on System Science, 2003.

Lee, S.B. and Campbell, A.T. "INSIGNIA: In-band signaling support for QoS in mobile ad-hoc networks". In 5th Int. Workshop on Mobile Multimedia Comm. (MoMuc'98), Berlin, Germany, October 1998.

Network Simulator 2 (NS-2) Homepage. <URL:http://www.isi.edu/nsnam/ns/ > Accessed September 2005.

Perkins, C. E. and Belding-Royer, E., Requests for Comments (RFC3461). <URL: http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt> Accessed November 2005.

Perkins, C. E. and Royer, E. M., Ad-hoc On-Demand Distance Vector Routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, New Orleans, LA, February 1999.

Sinha, P., Sivakumar, R. and Bharghavan, V., CEDAR: A Core-Extraction Distributed Ad Hoc Routing Algorithm. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), pages 202–209, 1999.

Society, I.C. IEEE standard for Wireless LAN-Medium Access Control and Physical Layer Specification, November 1999.

XGraph homepage <URL:http://www.isi.edu/nsnam/xgraph/ >, Accessed November 2005

R. Sivakumar, P. Sinha, and V. Bharghavan, "Cedar: A core-extraction distributed ad-hoc routing algorithm," IEEE Journal on Selected Areas in Communications, vol. 17,no. 8, pp. 1454–1465, August 1999

R. Sivakumar, P. Sinha, and V. Bharghavan. CEDAR: a Core-Extraction Distributed Ad-hoc Routing Algorithm. IEEE Journal on Selected Areas in Communications, 17:1454–1465, 1999.

G-S. Ahn, A.T. Campbell, A. Veres, and L-H. Sun. Supporting Service Differentiation for Real-Rime and Best-Effort Traffic in Stateless Wireless Ad Hoc Networks (SWAN). IEEE Trans. on Mobile Computing, 1(3):192–207, 2002.

H. Arora and H. Sethu. A Simulation Study of the Feasibility of Differentiated Services Framework for QoS in Mobile Ad Hoc Networks. In Proc. of Applied Telecommunication Symposium, April 2002.

S-B. Lee, G-S. Ahn, X. Zhang, and A.T. Campbell. INSIGNIA: An IP-Based Quality of ServiceFramework for Mobile ad Hoc Networks. J. of Parallel and Distributed Computing, 60:374–406, 2000.

Z.Y. Demetrios. A Glance at Quality of Services in Mobile Ad-Hoc Networks. Technical report, University of California-Riverside, 2001.

Y.-C. Hu and D.B. Johnson. Design and Demonstration of Live Audio and Video over Multi-hop Wireless Ad hoc Networks. In Proc. of the 2002 Military Communications Conference (MILCOM), pages 1211–1216, 2002.

H. Xiao, W.K.G. Seah, A. Lo, and K.C. Chua. A Flexible Quality of Service Model for Mobile Ad-Hoc Networks. In Proc. of the Vehicular Technology Conference 2000, pages 445–449, 2000.