A Time-based Admission Control Mechanism for IEEE 802.11 Ad Hoc Networks

Carlos Rodrigo Cerveira[1,2] and Luís Henrique M. K. Costa[2*]

[1] Diretoria de Telecomunicações da Marinha, Rio de Janeiro, Brasil.
[2] Grupo de Teleinformática e Automação PEE/COPPE - DEL/POLI,
Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil.
{rodrigo,luish}@gta.ufrj.br

Summary. This paper presents a time-based admission control mechanism (TAC) for IEEE 802.11 ad hoc networks. The proposed mechanism was adapted to the QoS AODV routing protocol, which takes the quality of service requirements of the data flow into account in the route discovery process. TAC-AODV estimates the idle time of the physical medium based on the frames listened. The incoming traffic is admitted according to the offered load as well as the intra-flow interference, calculated based on the number of hops in the forwarding chain. TAC-AODV is compared to AAC-AODV, another admission control mechanism found in the literature, and the simulation results show that TAC-AODV is in average 12.5% better in terms of the packet delivery rate.

1 Introduction

The use of multimedia applications on MANETs is becoming more and more desired; however, most of the routing strategies used in MANETs only provide best effort service. To overcome this problem a number of QoS (Quality of Service) techniques have been proposed.

These techniques spread different layers of the protocol stack, such as multiple queues at the MAC layer, routing protocols which search for QoS routes, and through signaling mechanisms for reservation, admission control, and packet scheduling.

QoS at the MAC layer can be implemented through IEEE 802.11e, which establishes different medium access categories, in order to prioritize certain types of traffic [7].

The purpose of the QoS routing [5] is to find a way to satisfy the users request in terms of available bandwidth, end to end delay, or jitter. On the other hand, QoS signaling protocols allocating resources along the chosen route. Signaling and routing are very coupled.

Additionaly, Admission control should be used together with signaling and routing. Its purpose is to assist the routing protocol in choosing a path for

the source node up to the destination node, with enough bandwidth for the transmission of flow and, without interfering with pre-existing traffic.

This paper proposes a new Time-based Admission Control Mechanism (TAC), which is based on a precise estimate of the available resources and on the intra-flow interference, taking into account the inherent characteristics of an ad hoc network. All nodes which take part in the route discovery process - from the source to the destination nodes - have their available resources checked and this new flow will be accepted, in case there is enough resources to fulfill the request and not to havoc the pre-existing flows.

This paper is organized as follows. Section 2 presents related work on AODV and QoS AODV. Sections 3 and 4 present the available resources and intra-flow interference estimations, respectively. Section 5 reviews AAC-AODV, an admission control mechanism proposed in [1]. Section 6 introduces the TAC-AODV protocol; Section 7 analyzes the performance of TAC-AODV through simulation and, finally, Section 8 concludes the paper.

2 Related Work

Ad hoc On demand Distance Vector (AODV) is a reactive routing protocol based on distance vectors [6]. AODV only triggers a route discovery procedure when there is a data transfer, using Route Request (RREQ) and Route Reply (RREP) messages. QoS AODV is an extension of AODV which takes QoS into account by adding extensions to the control messages and routing tables of AODV. The QoS AODV control messages carry the Maximum Delay and Minimum Bandwidth which are acceptable for the flow being started [3, 4, 5]. During route discovery, each intermediary node between the source and destination checks if the request can be fulfilled, otherwise, the route discovery is interrupted. QoS AODV finds a route that fulfills the QoS request, however, it does not take into account two factors: the impact on the ongoing traffic and the intra-flow interference. Two approaches are found in the literature which take these into account, Adaptive Admission Control (AAC) AODV [1] and Contention-Aware Admission Control Protocol (CACP) [9]. CACP supports only source routing protocols such as DSR, and does not propose any strategy to handle mobility and loss of QoS guarantees. AAC-AODV, on the other hand, is based on QoS AODV and introduces "lost QoS" messages to cope with changes in the QoS route. This work is based on AAC-AODV, which is described in more detail in Section 5.

3 Available Resources Estimate

In IEEE 802.11 networks, the medium is shared by the nodes located within the same carrier-sense region (CS nodes). The carrier sensing range is normally larger than the transmission range. Therefore, any transmission will have an

impact which is beyond the transmission range. Assuming that two nodes are within the transmission area of each other, the bandwidth available at the "link" connecting these two nodes is considered as the smallest of all available bandwidths, belonging to their sensing range. For example, consider that in
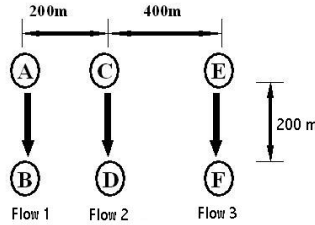

Fig. 1. Available resources estimate.

Figure 1 the flow AB is consuming 30% and the flow EF is taking 45% of the channel bandwidth. If we suppose a transmission range of 250 m and a carrier detection range of 550 m, the AB and EF flows do not interfere with each other. Now, suppose that node C wants to send traffic to D, and that the traffic load takes 40% of the channel bandwidth. Upon verification of the available resources, node C concludes that there is not enough bandwidth, as node C is within the interference area of both the AB and EF flows, which leave only 25% of the bandwidth available.

4 Intra-flow Interference

When a flow is transmitted using multiple hops, there will be interferences created by the traffic itself, because the carrier-sense range is larger than the transmission range. Suppose the scenario with five hops of Figure 2, where the full lines represent the transmission range area whereas the dotted lines represent the CS region. In that scenario, node 3 is in the interference range of five other nodes, which decreases its available bandwidth by five times. Therefore, another strategy is needed to accurately predict how much bandwidth is necessary in each node to accept a given traffic load. This phenomenon is called intra-flow interference. Now, suppose, a flow between node 1 and node 6 (destination) in Figure 2. Note that node 3 is in carrier-sense range of nodes 1 and 5. Therefore, node 3 not only suffers from the interference of nodes 2 and 4 transmissions, but also suffers from the interference of nodes 1 and 5, when they transmit. The intra-flow interference estimate is detailed in Section 5.2.
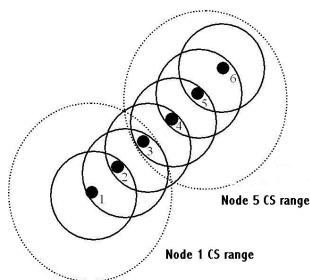
Fig. 2. Intra-flow interference.

5 Adaptive Admission Control (AAC) AODV

A straightforward way to guarantee that a flow is transmitted at the requested rate is to constantly calculate the available bandwidth and decide if a flow can be accepted based on an estimate of how much of the available bandwidth this flow will consume. The maximum available bandwidth can be computed from the IEEE 802.11 nominal transmission rate (11 Mbps for IEEE 802.11b), minus the overhead due to the time spent with the transmission of control bytes, i.e., the data frame preamble, RTS/CTS, and ACK frames, minus the time spent in the MAC operation, i.e., SIFS, DIFS, and backoff. The maximum available bandwidth depends on the packet size used by the application. Adaptive Admission Control (AAC) AODV [1] uses an approximation of this computation. AAC-AODV implements flow admission control based on two main mechanisms: Available Resources Estimate and Predictive Solution for Route Discovery.

5.1 Available Resources Estimate

To compute the maximum available bandwidth, AAC-AODV defines a "maximum bandwidth" of 5.1 Mbps experimentally obtained and considers a 40% reduction due to MAC overhead. That computation produces a maximum bandwidth of 3.6 Mbps for IEEE 802.11b [1]. The Bandwidth Estimate consumption at one node is the sum of the size of the packets sent, received, or detected during a predefined period of time. Assume that N is the number of packets sent, received, or detected by a node within a period of time T, and S is the packet size in bytes. Then, the average bandwidth used during T is:

$$BW(bps) = \frac{N*S*8}{T} \ . \tag{1}$$

5.2 Predictive Solution for Route Discovery

In [9], Kravets and Yang define the Contention Count (CC) at a node as the number of nodes on the multihop path that are located within carrier sensing range of a given node. In order to provide a good estimation of the expected

intra-flow contention, AAC-AODV uses CC to estimate the number of nodes which contend with each other for the medium access. Each node forwarding traffic has to calculate a CC variable in order to provide a good intra-flow interference estimate.

The CC variable can be obtained from the Hop Count field of the RREQ and RREP messages of AODV. The RREQ messages stores the number of hops between the source and the node forwarding the RREQ, while the RREP stores the number of hops from the destination to the forwarding the reply.

To compute CC, the authors [1] consider that the carrier-sense range is more than twice the size of the transmission range. Therefore, every node on the path generally interferes with, at most, two upstream and downstream nodes.

Let h_{req} and h_{rep} be the number of hops obtained from the RREQ and RREP messages, respectively. According to [1], the Contention Count (CC) of one node is defined as:

$$\begin{cases} \text{if } h_{req} > 2 \rightarrow h_{req} = 2 \\ \text{if } h_{rep} > 3 \rightarrow h_{rep} = 3 \\ \qquad CC = h_{req} + h_{rep} \end{cases} \qquad (2)$$

The estimate can only be made after the RREP reception as both h_{req} and
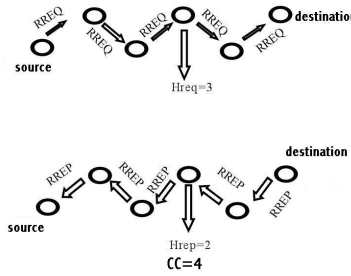

Fig. 3. Consider the nodes numbered from 1 to 6 beginning at the source node. By applying Equation 2 to the 4th node, we realize that the CC is equal to 4.

h_{rep} are needed. Thereafter, each node verifies if the bandwidth available is large enough to support a CC*Rate. If affirmative, the RREP is forwarded to the source.

6 Time-Based Admission Control (TAC)

The techniques presented in Section 5 are not sufficient to decide on the acceptance of a new traffic. It is still necessary to determine how much the new flow will take from the nominal bandwidth. Additionally, the intra-flow interference must be taken into account. AAC-AODV considers a maximum available

throughput of 3.6 Mbps [1]. That value actually corresponds to the network
saturation throughput using 1024-byte packets (see Table 1). Obviously, this
approximation reduces the protocol efficiency for packets smaller than 1024
bytes. In order to avoid this shortcoming, we measure the channel idle time as
an indication of the available bandwidth instead. In a saturated network, the
channel is occupied at all times.

6.1 Available Resources Estimate

The estimate of available resources is based on a variable called Busy Time
Estimate (T_b). A node can estimate the amount of time that the media is busy,
T_b, by summing up the times that the media is busy with routing messages,
RTS, CTS, ACK, and $DATA$ frames transmission, reception, and detection
during an interval of time. The accuracy of the busy time estimate depends
on the interval, t, between measurements. The larger t, the more accurate is
the estimate. Nevertheless, t should be small enough to be transparent to the
channel dynamics. Therefore, the choice of t is a tradeoff between accuracy and
transparency [1]. The transmission of an IEEE 802.11 data frame takes the
following amount of time, T:

$$
\begin{aligned}
T = DIFS + Backoff + RTS + SIFS+ \\
CTS + SIFS+ \\
Data + SIFS + ACK \ .
\end{aligned}
\tag{3}
$$

Consider that $DIFS$ is 50 μs, $3 \times SIFS$ is 30 μs, and that the backoff time is
the product of a time slot and a random number from 0 to 31. Then, the average
backoff is 15.5 μs, multiplied by the slot-time of 20 μs. The $RTS+CTS+ACK$
frames, including all the physical preambles have 120 bytes, or 960 bits, which
are transmitted at the basic rate of 1 Mbps, taking 960 μs. The 192-bit data
frame preamble is transmitted at the basic rate. $Data$ includes the payload
received by the routing layer, and the IP and MAC headers, which sum up
48 bytes. Therefore, the average time packet, T_{med}, in μs can be calculated as
follows:

$$
T_{med} = 50 + 30 + 310 + 960 + 192 + \tfrac{8*(psize+48)}{11} \ ,
\tag{4}
$$

where $psize$ is the payload received by routing layer. Then, the average through-
put, V, can be computed as:

$$
V(Mbps) = \tfrac{psize*8}{1542+\frac{8*(psize+48)}{11}} \ .
\tag{5}
$$

The total busy time (T_T) during the period of 1 second can be computed as the
fraction of the interval t where the medium is the busy, divided by the interval
t:

$$
T_T = \tfrac{T_b+(DIFS+3*SIFS+Backoff)*NPD}{t} \ ,
\tag{6}
$$

where NPD is the number of data packets transmitted, received, or detected, T_b
is the time during which the media is busy with the $RTS+CTS+ACK+Data$
frames and routing messages transmission.

A very important issue is the estimate of the backoff value when there are various stations contending for the medium. The stations will decrease their backoff simultaneously. When a station hears a transmission, the station will pause its backoff counter and re-start it when the media remains idle again for a DIFS period. Therefore, we can not use the average backoff value of Equation 4 for the calculation of the total packet transmission time. Bianchi [8] shows that the saturation throughput of an IEEE 802.11 network is defined by:

$$V(Mbps) = \frac{E[P]}{Ts + \tau \frac{1 - Ptr}{Ps Ptr} + Tc(\frac{1}{Ps} - 1)} \ , \tag{7}$$

where $E[P]$ is the data payload, in bits and transmitted in a slot-time, Ts is the time spent, in μs, for the successful packet transmission, the second and the third terms of the denominator are the amount of idle slot-time and slot-times spent with collisions, both in μs, for the successful packet transmission.

With the RTS/CTS mechanism, Bianchi [8] demonstrate that if we have 5 or more stations contending for the medium and the initial size of the backoff window equal to 31, the saturation throughput does not depend on the number of stations. This is because the number of idle slot-times and slot-times spent with collisions for successful transmission of a packet are constant and small in relation to Ts.

By examining Equations 5 and 7 we obtain the values in Table 1, where the network saturation throughput is given for different frame sizes, considering only one node accessing the medium and with 5 or more nodes trying to access the medium. In order to calculate the saturation throughput by using the Bianchi [8]

Table 1. Packet size and Throughput

Packet(bytes)	V(Mbps) 1 node	V(Mbps) 5 or more nodes	Difference (%)
64	0.31	0.34	9.0%
256	1.16	1.25	7.5%
512	2.10	2.25	6.5%
1024	3.52	3.74	5.8%
2300	5.66	5.90	4.0%

model, the number of idle slot-times and slot-times spent on collisions was set to 8, in accordance to the graphs presented in [8]. In our simulations, in order to estimate the backoff of Equations 6 and 9, we used the 160 μs value (8* 20 μs slot-times), reducing by 150 μs the average time spent to transmit a packet.

To calculate the Available Free Time (T_F) of a node in 1 second, we only have to subtract T_T:

$$T_F = 1 - T_T \ . \tag{8}$$

As described in Section 3, in order to precisely estimate the medium free time, the node needs to know the available free time of all of its neighbors. TAC-AODV uses the HELLO message to disseminate the available free time. The

available free time extension of the HELLO message is the free time measured by the node that issued the HELLO message. Upon reception of a HELLO, a node stores the available free time of its neighbors in a cache table. The node's decision on whether to forward the RREQ and RREP messages is based on the minimum available free time locally measured and measured by one-hop neighbors.

6.2 Resource availability verification

When receiving the packet at the routing layer, the node checks the transmission rate used and the size of the packet. Therefore, it is possible to estimate the amount of time needed to transmit this packet. The transmission time (T_{tx}) using IEEE 802.11b, considering an average backoff of 160 μs is calculated as:

$$T_{tx} = \frac{num}{1000000} * (1392 + \frac{8*(psize+48)}{11.0}) , \tag{9}$$

where num is the number of packets generated by the application in 1 second, calculated by the ratio between the transmission rate of the application and the size of the packet.

Then, the node checks if its available free time is enough to fulfill the application request. The RREQ message will only be forwarded if the node can fulfill the request. TAC-AODV adds two new fields to the RREQ and RREP messages, which contain the traffic rate and the size of the packet generated by the application.

When the intermediary nodes receive the RREQ and RREP messages, they also check whether they can fulfill the request from the source node. The intermediary nodes use Equation 9 with the information on rate and packet size contained in the RREQ and RREP messages. Note that the node intra-flow interference (Section 5.2) is accounted for and multiplied by T_{tx}. The flow is accepted only if:

$$T_F - CC * T_{tx} > 0 \tag{10}$$

In case the node can not fulfill the request, it drops the RREQ or RREP message interrupting route discovery.

6.3 Node mobility

All nodes continuously check if the Quality of Service (QoS) is being met. Suppose that a node is forwarding a QoS flow and the node moves and begins to suffer from the interference of other nodes. The available free time of the node will be reduced and it might not manage to route the previously accepted flow at the requested rate. In that case, the node will send an ICMP QoS Lost message [5] in the direction of the source node, reporting that it might not fulfill the QoS request. Upon reception of the QoS Lost message, the source node will interrupt the traffic and will generate a new RREQ for this flow, in order to discover a new path to fulfill the request.

7 Performance Evaluation

The simulations were performed using the 2.27 version of ns-2 [10]. We used the IEEE 802.11b with RTS/CTS. The scenario used in the simulations consists of a network of 50 nodes randomly positioned in an area of 900x600 m, moving according to the random waypoint model with a speed of 5 m/s and 10 s pause time. Four CBR sources are used, with size 512-byte packets. The CBR transmission rate varies from 100 to 900 kbps. We performed 30 simulation runs for each rate.

7.1 Metrics

Since the admission control is performed at the routing layer, the application does not receive any information of the lower layer regarding an unreachable destination. This is the case of the ns-2 implementation. Obviously, in the real world it is possible to have cross-layer optimisation in order to pause the application if no destination route is found. In case there is no feasible route due to the admission control action, the data packets are dropped at the routing layer. Nevertheless, we did not implement any routing layer signaling in ns-2. Thus, we define a metric called the Packet Delivery Ratio (PDR) which counts only the transmitted packets, in bytes, delivered by the MAC layer of the source node. The received packets, in bytes, are the ones received at the application layer of the destination node.

The second metric, the Overhead is defined as a the ratio between the number of control bytes produced by the routing protocol and by the number of data bytes received at the destination node.

The third metric is the end-to-end delay. It is defined as the difference between the arrival time of a packet at the destination node's application layer and the time by which the packet was generated at the source node's application layer.

The fourth metric is the Flow Rejection. It is defined as the ratio between the number of packets dropped at the routing layer, due to the admission control action, and the number of packets generated at the application layer.

The fifth metric is called the Overflow. It is defined as the ratio between the number of packets dropped at the MAC layer, due to queue overflow, and the number of packets generated at the application layer.

7.2 Simulation Results

Figure 4(a), shows the packet delivery rate (PDR) as the source transmission rate is varied. The AODV, AAC-AODV, and TAC-AODV behaviors are the same for the 100 kbps rate. Up to this point, the network is not saturated. Figure 4(e) points out that, no packets are dropped at the MAC Layer. AAC-AODV and TAC-AODV admit all offered traffic, and no packets are dropped at the routing layer (Figure 4(d)). Nevertheless, as the load increases, TAC-AODV
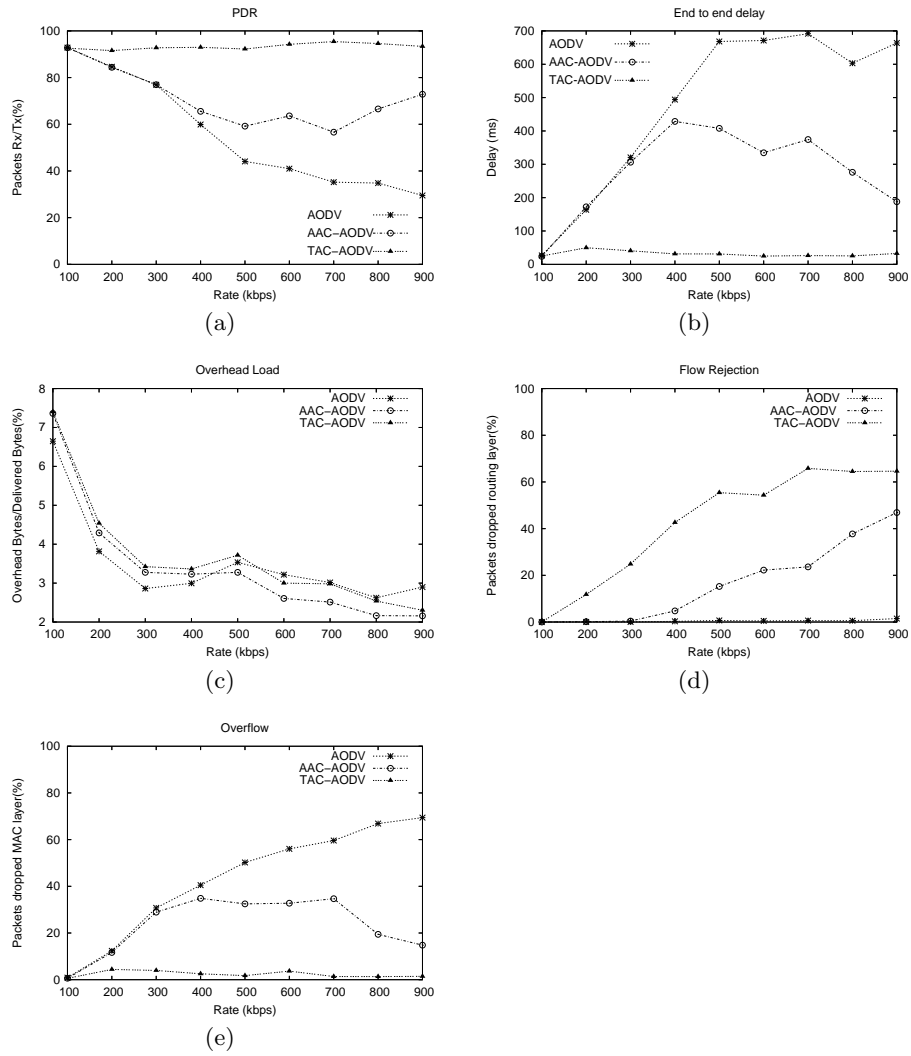
Fig. 4. Graphs for 512 byte packets.

rejects new traffic that would saturate the network, avoiding queue drops and sustaining the packet delivery rate above 90%. The delivery rate does not reach 100% because the mobility may cause route errors. With the increase of the network load the PDR of AAC-AODV starts to decrease. This happens because the network maximum throughput estimated by AAC-AODV for applications with 512-byte packets is not optimized and, therefore, the admission control accepts more traffic than the network could stand. AODV has the worst performance, as it has no admission control and accepts all of the traffic offered to the network.

Another important parameter is the packet average delay. Figure 4(b) shows that the TAC-AODV end-to-end delay remains below 50 ms, even with high rates causing the network to be saturated, which means that there is queuing in all nodes. AAC-AODV behaves similar to AODV for rates of up to 300 kbps. With higher rates, however, the admission control enters into action, since the traffic in the network reached the saturation value assumed by the protocol, reducing the delay, yet not reaching the delay obtained with TAC-AODV.

Figure 4(c) analyzes the protocol overhead. The AAC-AODV and TAC-AODV protocols employ HELLO, RREQ, and RREP messages which are longer than AODV. These messages carry additional fields used for admission control, as described in Section 6. The overhead of TAC-AODV is slightly larger than AAC-AODV due to the "packet size" field added in the RREQ and RREP messages. With increasing network load, AAC-AODV and TAC-AODV perform better than AODV. The admission control restricts the spread of RREQ and RREP messages, because they can be dropped if the available resources are not enough, reducing the number of routing control bytes. Figure 4(d) shows that only with a 400 kbps rate the AAC-AODV admission control is used, while TAC-AODV starts operating at the 200 kbps rates, restricting the admission of new flows. This means that, in the ns-2 simulator, packets are dropped at the routing layer. On the other hand, since AODV has no admission control, all packets are sent to the MAC layer. This causes an overflow in the MAC queue and, consequently, a high number of dropped packets (Figure 4(e)). Figure 4(e) shows the complementary behavior of Figure 4(d) and the efficiency of the TAC-AODV admission control, since TAC-AODV causes fewer packet drops at the MAC layer. AAC-AODV has a larger number of dropped packets due to an optimistic estimate of the available bandwidth, as previously mentioned. When
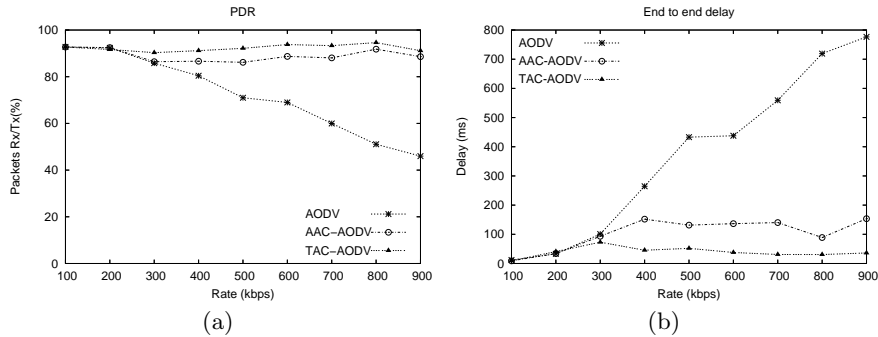

Fig. 5. PDR and end-to-end delay for 1024-byte packets.

the same experiments are repeated for 1024-byte packets, we note that the performance of AAC-AODV is closer to that of TAC-AODV. This is because with the 1024-byte packets the saturation throughput is closer to the maximum

bandwidth value, which is used by the protocol AAC-AODV. Therefore, the optimal bandwidth estimate used for admission control depends on the packet size.

8 Conclusion

Admission control is a key component to guarantee QoS in IEEE 802.11 ad hoc networks. In this paper, we proposed an admission control mechanism and combined it with the AODV routing protocol. The basic idea of TAC-AODV is to use the channel idle time as an indication of the bandwidth currently used in the network. Moreover, TAC-AODV takes into account the intra-flow interference effect and the influence of the nodes which are in the same carrier-sense region to provide an accurate estimate of the available resources. We have demonstrated through simulation that TAC-AODV provides more efficient QoS guarantees than other admission control mechanisms found in the literature.

References

1. R. de Renesse, M. Ghassemian, V. Friderikos, A.H.Aghvami, *Adaptive Admission Control for Ad Hoc and Sensor Networks Providing Quality of Service*, Technical Report, Center for Telecommunications Research, King's College London, UK, May 2005.
2. T. Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj and C. Siva Ram Murthy, *Quality of Service provisioning in Ad Hoc wireless networks: a survey of issues and solutions*, Elsevier Ad Hoc Networks, 1999.
3. Stéphane Lohier, Sidi-Mohamed Senouci, Yacine Ghamri Doudane, Guy Pujolle, *QoS routing in ad hoc networks*, Med-Hoc-Net, Sardegna, Italy, September 2002.
4. Stéphane Lohier and Sidi-Mohammed Senouci, *A Reactive Qos Routing Protocol for Ad Hoc Networks*, EUSAI, November 2003.
5. Charles Perkins, *Quality of Service for Ad Hoc On-Demand Distance Vector Routing.* Available at http://people.nokia.net/charliep/txt/aodvid/qos.txt
6. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das, *Ad Hoc On Demand Distance Vector (AODV) Routing.*, IETF RFC 3561.
7. S. Mangols, S. Choi, P. May, O. Klein, G. Hiertz, and L. Stibor, *IEEE 802.11e Wireless LAN for Quality of Service* , Proc. European Wireless, vol. 1, pages 32-39, Florence, Italy, February 2002.
8. Giuseppe Bianchi, *Performance analisys of the IEEE 802.11 Distributed Coordination Function.* IEEE Journal on Selected in Communications, vol. 18 no. 3, 2000.
9. Robin Kravets and Yaling Yang, *Contention-Aware Admission Control for Ad Hoc Networks.* IEEE Transactions on mobile computing, vol. 4, no. 4, 2005.
10. K. Fall and K. Varadhan, *NS Notes and Documentation*, The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC, 1997.
11. Villela, B. A. M. and Duarte, O. C. M. B. "Maximum Throughput Analysis in Ad Hoc Networks", Lecture Notes in Computer Science - Networking'2004, pp. 223-234, vol. 3042, Springer-Verlag, May 2004.