UNIVERSITY CARLOS III OF MADRID

Department of Telematics Engineering

Master of Science Thesis

Control Theoretic Optimization of 802.11 WLANs: Implementation and Experimental Evaluation

Author: **Andrea Mannocci**
M.Sc. in Computer Science Engineering

Supervisors: **Albert Banchs Roca, Ph.D.**
Vincenzo Mancuso, Ph.D.

Leganés, July 2011

Abstract

In 802.11 WLANs, the dynamic adaptation of the contention parameters along network conditions results in relevant performance improvements. Despite the ability to change these parameters has been available in standard devices for years, no adaptive mechanism using this functionality has been validated in a realistic deployment so far.

In our work, we report our experiences related to the implementation and evaluation of two adaptive algorithms based on control theory, one centralized and one distributed, in a large-scale testbed consisting of eighteen commercial off-the-shelf devices. We conduct extensive measurements under non-ideal channel condition, considering the impact of different network scenarios in terms of number of active nodes and traffic generated. We show that both algorithms significantly outperform the standard configuration in terms of total throughput. We also expose the limitations inherent to distributed schemes, and demonstrate that the centralized approach substantially improves performance under a broad variety of scenarios, which confirms its suitability for real deployments.

Table of Contents

1 Introduction **1**

2 Background **3**
- 2.1 IEEE 802.11 EDCA . . . 3
- 2.2 Optimal Point of Operation of the WLAN . . . 4
- 2.3 Centralized Adaptive Control Algorithm . . . 4
- 2.4 Distributed Adaptive Control Algorithm . . . 6

3 Implementation Details **9**
- 3.1 Implementation Overview . . . 9
- 3.2 Estimation of p_{obs} . . . 10
- 3.3 Estimation of p_{own} . . . 10
- 3.4 Contention Window Update . . . 11

4 Testbed Description and Validation of the Implementation **13**
- 4.1 Testbed Description . . . 13
- 4.2 Validation of the Algorithms . . . 16

5 Performance Evaluation **18**
- 5.1 UDP Throughput . . . 18
- 5.2 Impact of SNR on Throughput . . . 20
- 5.3 Hidden Nodes Scenario . . . 21
- 5.4 Impact Network Size . . . 21
- 5.5 TCP Throughput . . . 22
- 5.6 TCP Transfer Delay . . . 25

6 Related Work **28**

7 Conclusions **29**

References **30**

List of Figures

2.1 Retry flag marking upon collisions. 3
2.2 CAC algorithm. 5
2.3 DAC algorithm. 7

3.1 CAC and DAC implementations. 10

4.1 Deployed testbed. 14
4.2 SNR of the links between each node and the Access Point. 14
4.3 CW_{min} used by four selected nodes and the estimated p_{obs} and p_{own} with DAC. . 15
4.4 Announced CW_{min} and observed collision probability with CAC. 15

5.1 Total throughput with UDP traffic. 19
5.2 Throughput per station with UDP traffic. 19
5.3 Throughput obtained vs. SNR. 20
5.4 Performance with hidden nodes. 21
5.5 Total throughput for different number of stations. 23
5.6 Fairness for different number of stations. 23
5.7 Total throughput of FTP-like traffic. 24
5.8 Throughput per station with FTP-like traffic. 24
5.9 TCP delay performances. 26
5.10 Upload tranfers duration for the three mechanisms ($\lambda = 1/30\ s$). 27

Chapter 1

Introduction

The IEEE 802.11 standard for Wireless LANs [14] has become one of the most commonly used technologies to provide broadband connectivity to the Internet. The default channel access mechanism employed in IEEE 802.11 networks is based on a CSMA/CA scheme, regulated by a set of parameters that determines the aggressiveness of the stations when trying to access the channel. In particular, the contention window (CW) parameter controls the probability that a station defers or transmits a frame once the medium has become idle, and therefore has a key impact on the WLAN performance.

Commercial devices implement a fixed CW configuration, which is known to yield suboptimal performance. Indeed, for a fixed CW, if too many stations contend the collision rate will be very high, while if few stations are backlogged the channel will be underutilized most of the time. This behavior has been analyzed by several works in the literature, e.g. [3], which have shown that adapting the CW to the number of backlogged stations significantly improves performance.

Following the above result, an overwhelming number of solutions have proposed to adapt the 802.11 MAC behavior to the observed network conditions with the goal of maximizing the WLAN performance [8, 20, 12, 16, 24, 23, 17, 22, 2, 6, 7]. However, as we detail in the related work chapter, these previous works suffer from at least one of these two limitations: (i) their performance has not been assessed with real deployments, and therefore lack experimental evidences gathered from scenarios with non-ideal channel effects and implementation constraints [8, 20, 16, 24, 23, 17, 6, 7]; or (ii) they rely on non-standard capabilities, or functionality that is not supported by existing wireless devices, and therefore would require complex modifications to be implemented [8, 12, 16, 22, 2, 6, 7]. Furthermore, most of them are based on heuristics and lack the mathematical foundations to guarantee optimal performance [8, 20, 12, 16, 2].

In this thesis we present our experiences with the implementation of two adaptive algorithms, namely the *Centralized Adaptive Control* (CAC) [18] and the *Distributed Adaptive Control* (DAC) [19], both based on a Proportional Integrator (PI) controller that dynamically tunes the CW configuration to optimize performance. In contrast to previous proposals, both algorithms are supported by solid theoretical foundations from control theory and can be easily implemented with unmodified existing devices.

We first provide a detailed description of the implementation of our adaptive mechanisms, which run as user space applications and rely on standardized system calls to estimate the contention level in the WLAN and adjust the CW configuration of 802.11 stations. We also provide insights into the differences between the theoretical design and the practical implementation of the

algorithms, caused by the inherent limitations of the real devices. Furthermore, we demonstrate the feasibility of utilizing these algorithms with commercial off-the-shelf (COTS) hardware and open-source device drivers.

By conducting exhaustive experiments in a large-scale testbed consisting of 18 devices, we evaluate the performance of our proposals under non-ideal channel effects and different traffic conditions. Additionally, we compare the performance of our algorithms against the default IEEE 802.11 configuration, and identify those scenarios where a network deployment can benefit from using such adaptive algorithms.

Our results confirm that both approaches outperform the standard's default scheme, improving the performance by up to 50%. Our experiments also reveal that the distributed algorithm suffers from a number of problems with heterogeneous radio links, which are inherent to its distributed nature and the limitations of the wireless interfaces. In contrast, the centralized scheme exhibits remarkable performances under a wide spectrum of network conditions. The conclusions drawn from our analysis prove the feasibility of using adaptive MAC mechanisms in realistic scenarios and provide valuable insights for their design.

The remainder of the thesis is organized as follows. Chapter 2 summarizes the IEEE 802.11 EDCA protocol and the underlying principles of CAC and DAC. In Chapter 3 we report details about the implementation of the functionality comprised by the proposed schemes. Chapter 4 describes our testbed and the validation of the implementation of the algorithms. Chapter 5 presents a thorough experimental study of the algorithms in a broad set of network conditions. Finally, Chapter 6 summarizes the related work and Chapter 7 concludes the work.

Chapter 2

Background

This chapter briefly summarizes the behavior of IEEE 802.11 EDCA mechanisms and the ideas on which the two adaptive protocols implemented and assessed here are based on.

2.1 IEEE 802.11 EDCA

The IEEE 802.11 Enhanced Distributed Channel Access (EDCA) mechanism is a CSMA/CA-based protocol that operates as follows. As depicted in Fig. 2.1, upon the availability of a frame to be transmitted, a station is allowed to send it on air only after having sensed the channel idle for a period of time equal to the arbitration interframe space parameter ($AIFS$). Otherwise, if the channel is found busy (either immediately or during the $AIFS$ period), the station continues to monitor the medium until it is sensed idle for an $AIFS$ interval, and then enters in a backoff process.

Upon starting the backoff process, a station computes a random integer uniformly distributed in the range $[0, CW - 1]$, and initializes its backoff time counter with this value. The CW value is called the contention window, and depends on the number of failed transmission attempts. For the first transmission attempt the minimum contention window (CW_{min}) is used. In case of a collision, its value doubles, up to a maximum value CW_{max}. The backoff time counter is decremented once every time slot if the channel is sensed idle and frozen when an ongoing transmission is de-

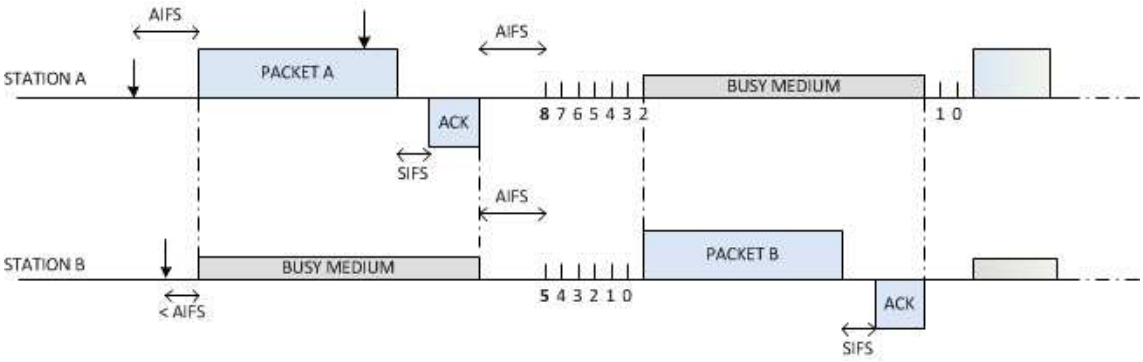


Figure 2.1: Retry flag marking upon collisions.

tected on the channel. Finally, when the backoff time counter reaches zero, the station transmits its frame in the next time slot.

When two or more stations start transmitting simultaneously, a collision occurs. Acknowledgment (ACK) frames are used to notify a transmitting station of successfully received frames. In the case of a failed transmission, the station doubles its CW and executes the backoff process again. Once a frame has been successfully transmitted or the retry limit has been exceeded, CW is set again to CW_{min}. To prevent duplicates, the standard provides a retry flag R in order to mark those frames that are being retransmitted, i.e., the flag is set to 0 on the first transmission attempt, and set to 1 on every subsequent retransmission (see Fig. 2.1). As we discuss later, our algorithms exploit this functionality to infer the network conditions and adapt the CW of the stations accordingly.

To support service differentiation, EDCA implements different access categories (ACs) at every station, each having a different backoff configuration. The parameters of each AC are announced by the Access Point using the Beacon Frames. In the rest of the tractation we do not consider service differentiation and assume that all stations only execute the Best Effort AC.

2.2 Optimal Point of Operation of the WLAN

Both CAC and DAC share the goal of adjusting the CW to drive the WLAN to the optimal point of operation that maximizes the total throughput given the observed network conditions. Let p denote the probability that a transmission attempt collides. Following [3], we have shown in [18, 19] that the optimal collision probability in the WLAN p_{opt} can be approximated by

$$p_{opt} \approx 1 - e^{-\sqrt{\frac{2T_e}{T_c}}}, \tag{2.1}$$

where T_e is the duration of an idle slot (a PHY layer constant) and T_c is the average duration of a collision. Therefore, p_{opt} does not depend on the number of stations, but only on the average duration of a collision T_c. Given the average length $E[L]$ of the longest packet involved in a collisions, T_c can be computed using

$$T_c = T_{PLCP} + \frac{E[L]}{C} + EIFS.$$

where T_{PLCP} is the duration of the Physical Layer Convergence Protocol (PLCP) preamble and header, C is the modulation rate and $EIFS$ is a PHY layer constant.

2.3 Centralized Adaptive Control Algorithm

The *Centralized Adaptive Control* (CAC) algorithm [18], illustrated in Fig. 2.2, is based on a PI controller located at the Access Point (AP). This controller computes the configuration of the CW_{min} parameter, while CW_{max} is set as $CW_{max} = 2^m CW_{min}$ in order to benefit from the features of the binary exponential backoff algorithm (with m being set as in the default configuration, which is $m = 6$ for IEEE 802.11a).

Following the above, the controller performs two tasks every beacon interval (approx. 100 ms): (i) it estimates the current point of operation of the WLAN as given by the observed collision probability p_{obs}, and (ii) based on this estimation and p_{opt}, it computes the CW configuration to be used during the next beacon interval and sends it to the stations in a beacon frame.

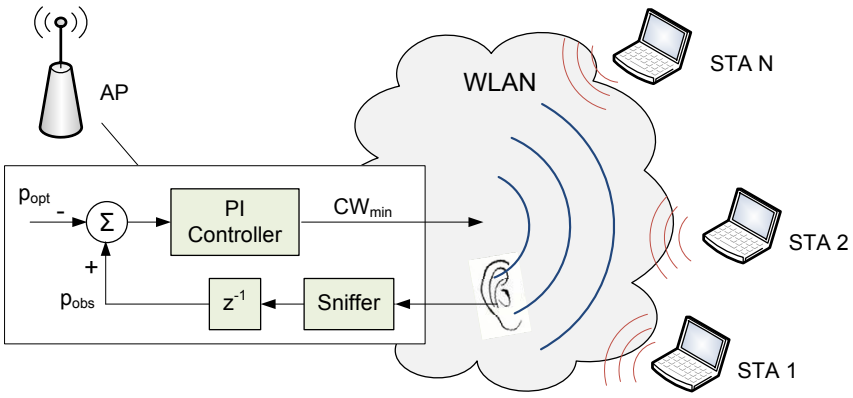


Figure 2.2: CAC algorithm.

The computation of p_{obs} is based on the observation of the retry flag of successful frames. Let us denote by R_1 (R_0) the number of observed frames with the retry bit set (unset) during a beacon interval. Assuming that no frames exceed the retry limit given by the MAX_RETRY parameter,[1] and that transmissions attempts collide with a constant and independent probability,[2] the observed probability of a collision in the WLAN can be estimated with (see [18]):

$$p_{obs} = \frac{R_1}{R_0 + R_1}. \tag{2.2}$$

The error signal e fed into the PI controller to calculate the new CW_{min} is computed as the difference between the observed collision probability p_{obs} and the target value p_{opt}:

$$e = p_{obs} - p_{opt}. \tag{2.3}$$

In this way, when the observed collision probability is above the target value, the error signal will be positive and trigger an increase of the CW_{min}, and consequently a decrease of the collision rate in the next beacon interval. Similarly, when the collision probability is below the target value, CW_{min} is decreased in order to increase the activity on the channel.

The $\{K_P, K_I\}$ parameters of the PI controller are obtained using the Ziegler-Nichols rules, to achieve a proper trade-off between stability and speed of reaction to changes, and are given by (see [18] for the details):

$$\begin{cases} K_P = \frac{0.8}{p_{opt}^2(1+p_{opt}\sum_{k=0}^{m-1}(2p_{opt})^k)}; \\ \\ K_I = \frac{0.4}{0.85 \cdot p_{opt}^2(1+p_{opt}\sum_{k=0}^{m-1}(2p_{opt})^k)}. \end{cases} \tag{2.4}$$

The operation of CAC is summarized in Algorithm 1.

[1] Note that this assumption is accurate as in an optimally configured WLAN the collision probability is very low.
[2] This assumption has been widely used and shown to be accurate, see e.g. [3].

Algorithm 1 Centralized Adaptive Control algorithm.

```
1: while true do
2:     repeat
3:         if new frame sniffed then
4:             retrieve retry flag
5:             if retry flag is set then
6:                 Increment R_1
7:             else
8:                 Increment R_0
9:             end if
10:        end if
11:    until new beacon interval
12:    compute p_obs[t] using (2.2)
13:    e[t] = p_obs[t] − p_opt
14:    CW_min[t] = CW_min[t − 1] + K_P · e[t]+
15:                +(K_I − K_P) · e[t − 1]
16:    send beacon with new CW configuration
17: end while
```

2.4 Distributed Adaptive Control Algorithm

The *Distributed Adaptive Control* (DAC) algorithm [19] employs an independent PI controller at each station to compute its CW configuration, to drive the overall collision probability to the target value p_{opt}. As illustrated in Fig. 2.3, each controller computes the CW_{min} value employed by its Network Interface Card (NIC), based on the locally observed network conditions. Similarly to CAC, CW_{max} is set as $CW_{max} = 2^m CW_{min}$.

While with centralized approaches all stations use the same configuration provided by a single entity, and therefore fairly share the channel, with distributed approaches this is not necessarily the case. To guarantee a fair throughput distribution, the error signal utilized in DAC consists of two terms: one to drive the WLAN to the desired point of operation, and another one to achieve fairness between stations. More specifically, the error signal at station i is given by

$$e_i = e_{collision,i} + e_{fairness,i}. \tag{2.5}$$

The first term of (2.5) ensures that the collision probability in the network is driven to the target value:

$$e_{collision,i} = p_{obs,i} - p_{opt}, \tag{2.6}$$

where $p_{obs,i}$ denotes the collision probability as measured by station i. When the collision probability observed by station i is larger than the target value, the above term yields a positive error that increases the CW of station i, thereby reducing the collision probability.

The second term of (2.5) is computed as

$$e_{fairness,i} = p_{obs,i} - p_{own,i}, \tag{2.7}$$

where $p_{own,i}$ is the collision probability experienced by station i. The purpose of this second component of e_i is to drive the CW of all stations to the same value. Indeed, the higher the

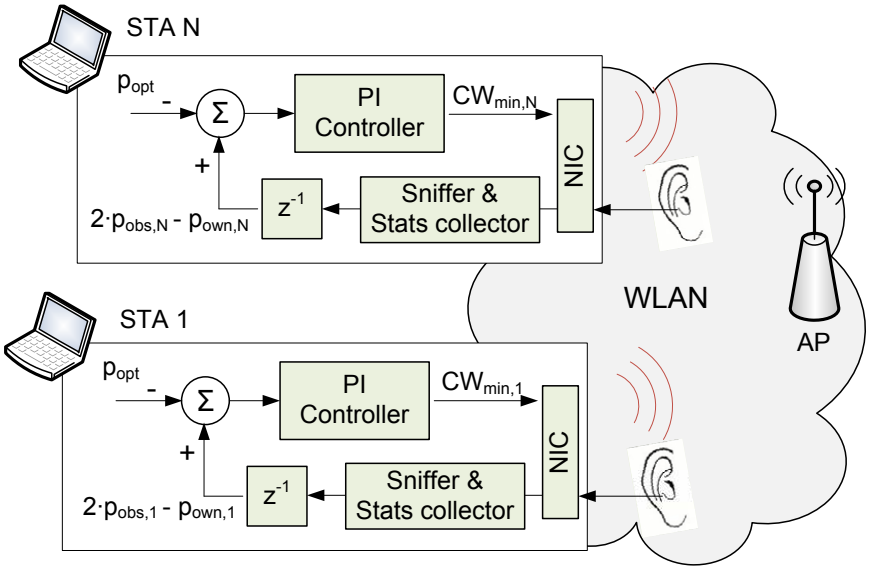


Figure 2.3: DAC algorithm.

CW_{min}, the lower the number of collisions caused, and thereby, the lower the observed collision probability $p_{obs,i}$ is. Therefore, a station will increase its CW_{min} if it experiences less collisions than the others.

To compute the error signal, each station needs to measure $p_{obs,i}$ and $p_{own,i}$. The former is computed as p_{obs} in CAC. For the computation of $p_{own,i}$, we rely on the following statistics which are readily available from wireless cards: the number of successful transmission attempts T and the number of failed attempts F. With these statistics, $p_{own,i}$ is computed as:

$$p_{own,i} = \frac{F}{F+T}. \tag{2.8}$$

Each station will estimate $p_{obs,i}$ and $p_{own,i}$ and compute the error signal e_i, which is provided to the PI controller for the computation of the new $CW_{min,i}$. Like in CAC, we choose to trigger an update of the $CW_{min,i}$ every beacon interval, as this is compatible with existing 802.11 hardware, which is able to update the EDCA configuration at the beacon frequency.

Although the analysis of DAC, based on multivariable control theory, significantly differs from the analysis of CAC, based on standard control theory, the $\{K_P, K_I\}$ parameters that each station uses are the same ones of (2.4), as proved in [19]. The DAC operation is summarized in Algorithm 2.

Algorithm 2 Distributed Adaptive Control algorithm.

while true **do**
  repeat
    if new frame sniffed **then**
      retrieve retry flag and
      increment R_0 or R_1 accordingly
    end if
  until beacon received
  compute $p_{obs,i}$ using (2.2)
  fetch T and F from driver stats
  compute $p_{own,i}$ using (2.8)
  $e[t] = 2 \cdot p_{obs,i}[t] - p_{own,i}[t] - p_{opt}$
  $CW_{min}[t] = CW_{min}[t-1] + K_P \cdot e[t] +$
    $+(K_I - K_P) \cdot e[t-1]$
  update the local CW configuration
end while

Chapter 3

Implementation Details

A major advantage of CAC and DAC is that they are based on functionalities already available in IEEE 802.11 devices, and therefore can be implemented with COTS hardware. In this chapter, we describe the hardware used in our deployment and the implementation of the functionality required by CAC and DAC.

3.1 Implementation Overview

We have implemented our algorithms using Soekris net4826-48 devices.[1] These are low-power, low-costs computers equipped with 233MHz AMD Geode SC1100 CPUs, 2 Mini-PCI sockets, 128 Mbyte SDRAM and 256 Mbyte compact flash circuits for data storage. To accommodate the installation of current Linux distributions, we have extended the storage capacity of the boards with 2 GB USB drives. As wireless interfaces, we used Atheros AR5414-based 802.11a/b/g devices.

As software platform we installed Gentoo Linux OS (kernel 2.6.24) and the popular MadWifi open-source WLAN driver[2] (version v0.9.4), which we modified as follows: (i) we enabled the dynamic setting of the EDCA parameters for the best effort access category, which is in line with the standard specifications but disabled by default in the driver, (ii) we overwrote the drivers' EDCA values for the best-effort traffic with the standard recommended ones [14], and (iii) for the case of DAC we modified the driver to enable the stations to employ the locally computed EDCA configuration using standardized system calls (as described in Section 3.4). The source code of the modified drivers and our implemented prototypes is available online.[3]

Fig. 3.1 illustrates the main modules of our implementation of CAC and DAC. The algorithms do not require introducing modifications to the hardware/firmware nor have tight timing constraints, and therefore they can run as user-space applications that communicate with the driver by means of `IOCTL` calls. We also take advantage of the ability of the MadWifi driver to support multiple virtual devices using different operation modes (master/managed/monitor) with a single physical interface. In the following we detail the implementation of the different modules.

[1] `http://www.soekris.com/`
[2] `http://madwifi-project.org/`
[3] `http://www.hamilton.ie/ppatras/\#code`

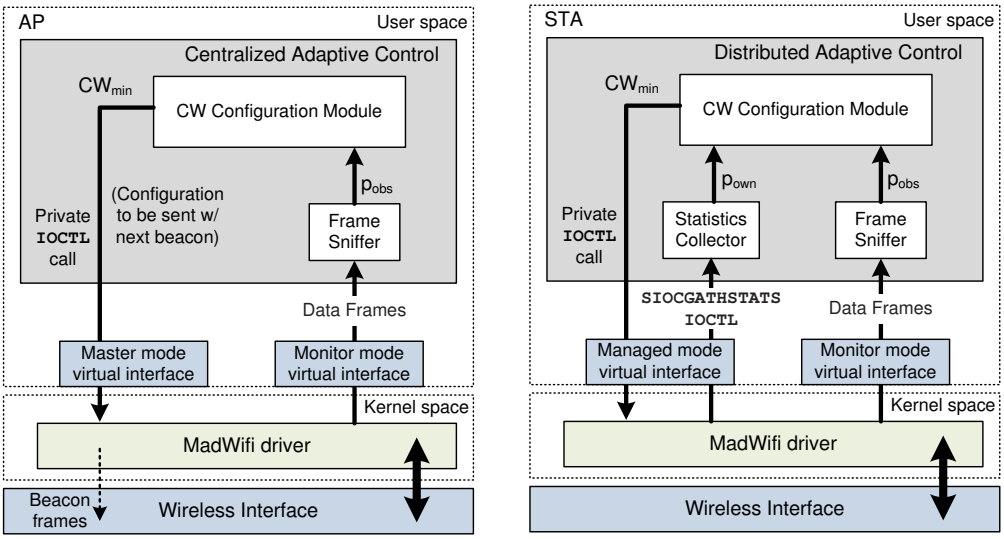


Figure 3.1: CAC and DAC implementations.

3.2 Estimation of p_{obs}

Both algorithms require to estimate the collision probability observed in the WLAN. For the case of CAC this is performed only at the AP and results in p_{obs}, while for the case of DAC this is performed independently at each station i and results in $p_{obs,i}$. The estimators are computed with (2.2), which relies on observing the retry flag of the overheard frames. We next explain how these values are obtained from a practical perspective.

To overhear frames, we utilize a virtual device operating in the so called `monitor` mode with promiscuous configuration. With this configuration, the device passes all traffic to user-space applications, including frames not addressed to the station. We also configure the device to pass the received frames with full IEEE 802.11 link layer headers, such that the Frame Control field of the frames (where the retry flag resides) can be examined.

With this set-up, the algorithms open a `raw` socket to the driver, which enables the reception of Layer 2 frames. Through this socket the algorithms listen for transmitted frames and process their headers in an independent thread (the "Frame Sniffer" module of Fig. 3.1). For every observed frame, one of the counters used in the estimation of the collision probability is incremented: R_0 if the retry flag was unset, R_1 if the retry flag was set. Every beacon interval the computation of p_{obs} or $p_{obs,i}$ using (2.2) is triggered, and then the counters are reset to zero.

3.3 Estimation of p_{own}

In addition to the observed collision probability $p_{obs,i}$, the DAC algorithm requires to estimate the experienced collision probability $p_{own,i}$. We perform this computation in the "Statistics Collector" module of Fig. 3.1 using information recorded by the wireless driver. More specifically, at the end of a beacon interval we open a communication channel with the driver instance, config-

ured in `managed` mode, and perform a `SIOCGATHSTATS IOCTL` request. Upon this request, the driver populates an `ath_stats` data structure, which contains detailed information about the transmitted and received frames since the Linux kernel has loaded the driver module. Out of the statistics retrieved, the records that are of particular interest for our implementation are:

- `ast_tx_packets`: number of unique frames sent to the transmission interface.
- `ast_tx_noack`: number of transmitted frames that do not require ACK.
- `ast_tx_longretry`: number of transmission retries of frames larger than the RTS threshold. As we do not use the RTS/CTS mechanisms, this is the total number of retransmissions.
- `ast_tx_xretries`: number of frames not transmitted due to exceeding the retry limit, which is set by the `MAX_RETRY` parameter.

To compute $p_{own,i}$ we need to count the number of successful transmissions and the number of failed attempts. To compute the former, we subtract from the number of unique frames those that are not acknowledged (e.g., management frames) and those that were not delivered,

$$\textit{Successes} = \texttt{ast\_tx\_packets} - \texttt{ast\_tx\_xretries} - \texttt{ast\_tx\_noack}.$$

Similarly, to compute the number of failed attempts, out of the total number of retransmissions we do not count those retransmissions caused by frames that were eventually discarded because the `MAX_RETRY` limit was reached, therefore,

$$\textit{Failures} = \texttt{ast\_tx\_longretry} - \texttt{ast\_tx\_xretries} \cdot \texttt{MAX\_RETRY}.$$

With the above, the terms F and T of (2.8) used to estimate $p_{own,i}$ are computed as

$$\textit{F[t] = Failures[t] - Failures[t-1],}$$
$$\textit{T[t] = Successes[t]- Successes[t-1],}$$

where t denotes the time of the current beacon interval and $t-1$ the previous one.

3.4 Contention Window Update

With the estimated collision probabilities, CAC and DAC compute the error signal at the end of a beacon interval according to (2.3) and (2.5), respectively. Depending on this value, the PI controller triggers an update of the CW_{min} to be used in the next beacon interval t, according to the following expression:

$$CW_{min}[t] = CW_{min}[t-1] + K_P \cdot e[t] + (K_I - K_P) \cdot e[t-1].$$

To ensure a safeguard against too large and too small CW_{min} values we impose lower and upper bounds for the CW_{min}. We set these bounds to the default CW_{min}^{DCF} and CW_{max}^{DCF} values specified by the standard, which are 16 and 1024, respectively, for IEEE 802.11a [13].

The algorithms assume that the CW_{min} can take any integer value in the $[16, 1024]$ range. However, with our devices only integer powers of 2 are supported (i.e., $CW_{min} \in \{16, 32, \ldots, 1024\}$). Therefore, the value actually used is obtained as:

$$CW[t] = 2^{rint(\log_2(CW_{min}[t]))}.$$

where `rint(x)` is a function that returns the integer value nearest to `x`.

To commit the computed `CW` configuration, first we retrieve the list of private `IOCTL`s supported by the device to search for the call that sets the CW_{min}. Once this call has been identified, we prepare an `iwreq` data structure with the following information: the interface name, the base-2 exponent of the `CW` computed as above, the access category index as defined by the standard (`0` for Best Effort) and an additional parameter that identifies if the value is intended to be used locally or propagated. For the case of DAC this value is set to 0, as the `CW` is only intended to the local card, while for the case of CAC is set to 1, thereby requesting the driver to broadcast the new `CW` within the EDCA Parameter Set element of the next scheduled beacon frame.

Chapter 4

Testbed Description and Validation of the Implementation

In this chapter we first describe our testbed. Then we analyze the link qualities between each node and the AP and show that our set-up is able to mimic a realistic deployment with significant differences in terms of SNR. Finally, we confirm that, despite the constrains imposed by the devices and the realistic radio conditions, both CAC and DAC are able to drive the WLAN to a stable point of operation.

4.1 Testbed Description

Our testbed is located in the Torres Quevedo building at University Carlos III de Madrid. It consists of 18 devices deployed under the raised floor, a placement that provides physical protection as well as radio shielding to some extent (see [21]).

Fig. 4.1 illustrates the location of the nodes. We placed one node (denoted as AP) towards the center of the testbed, thus following the placement of an Access Point in a realistic deployment, while the other stations (numbered from 1 to 17 in no particular order) are distributed at different distances from this node. All nodes are equipped with 5 dBi omnidirectional antennas and are configured to operate on channel 64 (5.32 GHz) of IEEE 802.11a standard [13], where no other WLANs were detected. All nodes use the 16-QAM modulation and coding scheme, which provides 24 Mbps channel bit rate, as calibration measurements showed that this was the highest rate achievable by the node with the worst link to the AP (node 15). Additionally, we disabled the RTS/CTS, rate adaptation, turbo, fast frame, bursting and unscheduled automatic power save delivery functionality, as well as the antenna diversity scheme for transmission/reception.

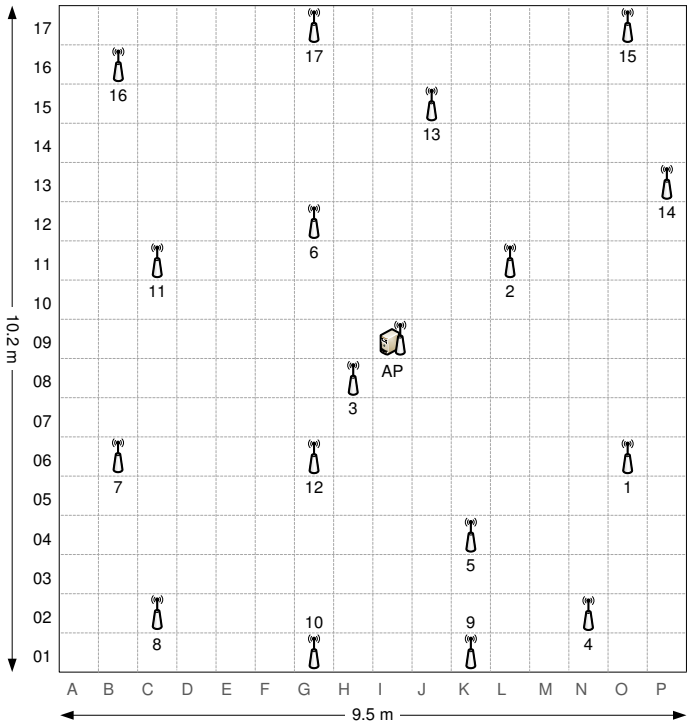


Figure 4.1: Deployed testbed.

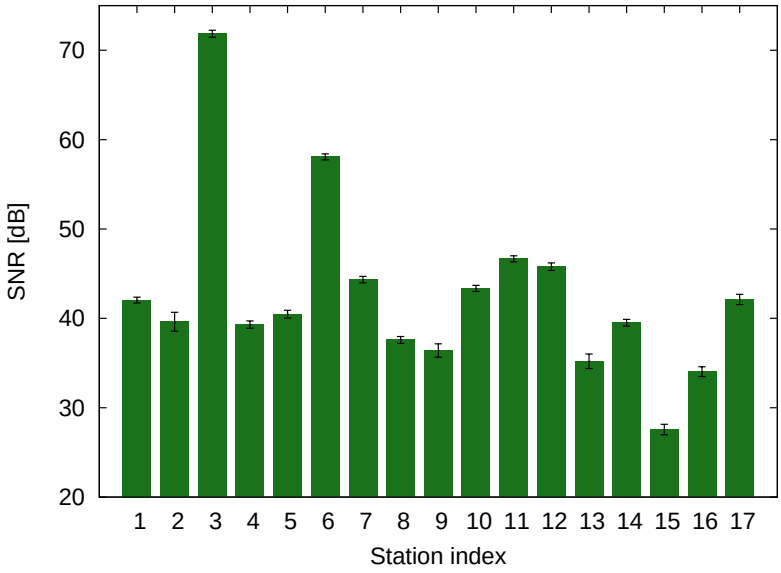


Figure 4.2: SNR of the links between each node and the Access Point.

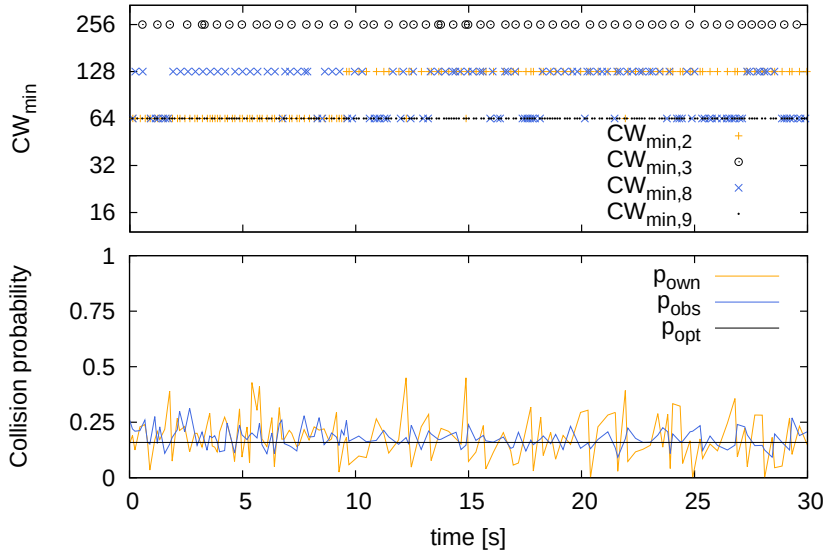


Figure 4.3: CW_{min} used by four selected nodes and the estimated p_{obs} and p_{own} with DAC.

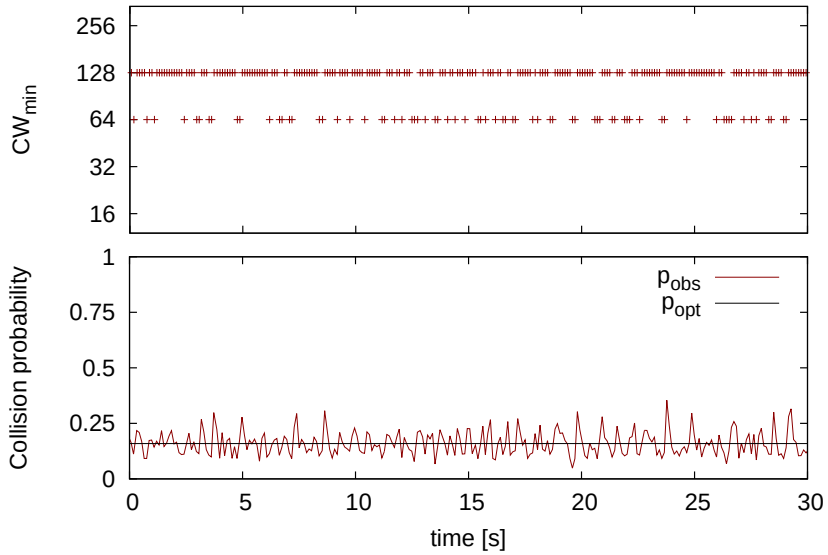


Figure 4.4: Announced CW_{min} and observed collision probability with CAC.

Unless otherwise specified, all nodes use the same transmission power level of 17 dBm. Given the node placement of Fig. 4.1, this setting results in very dissimilar link qualities between each station and the AP (e.g., node 3 is extremely close). To confirm this link heterogeneity, we designed the following experiment. For a given node, we ran a 10-second `ping` test between the station and the AP, recording the SNR values of the received frames as obtained by the `wireshark` packet analyzer[1] from the `radiotap` header.[2] This test was performed on a node-by-node basis, and repeated for 18 hours. The average and standard deviation of the SNR for each link are shown in Fig. 4.2.

From the figure we confirm that the use of a fixed power setting in the considered deployment results in very diverse radio links between the AP and the stations. Note that, throughout the reported experiments, we periodically repeated the above measurement in order to confirm that the radio conditions did not change.

4.2 Validation of the Algorithms

Our first set of experiments aims at confirming that the good operation properties of CAC and DAC, obtained analytically and via simulations in [18, 19], are also achieved in a real testbed. Specifically, we want to confirm that the use of the algorithms results in stable behavior despite the described hardware/software limitations and the impairments introduced by the channel conditions, and also assess their resource consumption in terms of CPU and memory usage.

Point of operation. We consider a scenario with $N = 10$ stations, constantly backlogged with 1500 B UDP frames, that send data to the AP utilizing `iperf`.[3] For the case of the centralized algorithm (CAC) we log its key variables, namely, the `CW` announced in beacon frames and the observed collision probability p_{obs}. Both are obtained every 100 ms and depicted in Fig. 4.4.

As the figure shows, CAC drives the WLAN to the desired point of operation. Indeed, the announced `CW` oscillates between the two allowed values closest to the optimal CW_{min}, while p_{obs} fluctuates stably around the desired p_{opt} given by (2.1). We conclude that, despite the hardware limitations imposed on the values of `CW` and the channel impairments, CAC is able to drive the WLAN to the desired point of operation.

Next we validate the operation of the distributed algorithm (DAC). We consider the same scenario as before, logging the key parameters of the algorithm at each station, namely $CW_{min,i}$, $p_{own,i}$ and $p_{obs,i}$. In Fig. 4.3 we depict in the upper subplot the evolution of the CW_{min} used by four representative nodes (namely 2, 3, 8 and 9), while in the lower subplot we show the collision probabilities estimated by node 2 ($p_{obs,2}$ and $p_{own,2}$).

From the two subplots we see that DAC also drives the average collision probability in the WLAN to the desired value. However, there is a key difference as compared to the previous case: while with CAC all stations use the same CW_{min} value, with DAC they operate at different average CW_{min}. Indeed, the four stations considered in the experiment use average CW_{min} values of 92, 300, 92 and 64, respectively. As we will explain in Section 5.2, this behavior is caused by the relative differences in link qualities, already identified above, combined with the inability of the wireless interface to identify the reasons for a packet loss.

[1] `http://wireshark.org`

[2] With the `radiotap` option, the driver provides additional information about received frames to user-space applications, including the signal-to-noise ratio.

[3] `http://sourceforge.net/projects/iperf/`

Resource consumption. In addition to analyzing the performance of CAC and DAC, it is also important to asses their resource consumption. For this purpose, we analyzed the CPU and memory usage of the algorithms utilizing the `top` Linux application, which provides a dynamic real-time view of a running system. With this tool, we recorded the used shares of the CPU time and available physical memory with a frequency of 1 sample per second and computed the average usage. CAC, which runs exclusively at the AP, demands on average 39% of the CPU time and only 1.6% of the physical memory. For the case of DAC, which runs at every station, the average CPU time consumption is 28%, while the physical memory consumption is 4.3%. Given the low speed of the nodes' CPU (233 MHz) and their reduced physical memory (128 MB), these results show that both CAC and DAC are suitable for commercial deployments.

Chapter 5

Performance Evaluation

We next assess the performance of the algorithms under a large number of different scenarios and compare their performance against the default EDCA configuration, which we use as a benchmark. Each considered experiment runs for 2 minutes and is repeated 10 times to obtain average values of the measured metrics with good statistical significance.

5.1 UDP Throughput

We first measure the achievable throughput between the nodes and the AP when all the stations are transmitting UDP traffic at the same time. Fig. 5.1 plots the average and standard deviation of the total throughput obtained with each mechanism. We observe that the EDCA default configuration achieves around 11 Mbps, while the use of DAC and CAC results in a performance gain of approximately 45%. Therefore, we confirm that both approaches, by properly adapting the CW configuration to the number of contending stations, achieve a much higher efficiency.

To further examine the performance of the algorithms, we plot the per-station throughput in Fig. 5.2. According to the figure, the use of the EDCA recommended values not only provides the lowest overall throughput figures, but also fails to provide a fair sharing of the available bandwidth. Indeed, it can be seen that, e.g., the node with the best link quality to the AP (node 3) achieves more than three times the throughput obtained by the station with the poorest link (node 15).

While DAC provides a larger total throughput than EDCA, it does not improve the level of fairness. Actually, it results in a somehow *opposite* performance as the one obtained with EDCA: stations that obtained a relatively large bandwidth with EDCA (e.g., nodes 3, 6) now obtain a relatively small bandwidth with DAC. The use of CAC, on the other hand, provides the best performance both in terms of total throughput and fairness, as it provides all stations with very similar throughput values.

To quantify the throughput fairness achieved by the considered mechanisms we compute the Jain's fairness index (JFI) [15]. The resulting JFI values are 0.865, 0.997 and 0.817 for the case of EDCA, CAC and DAC, respectively. These figures confirm the good fairness properties of CAC, and shows that DAC and EDCA suffer from a higher level of unfairness, a result that we analyze next.

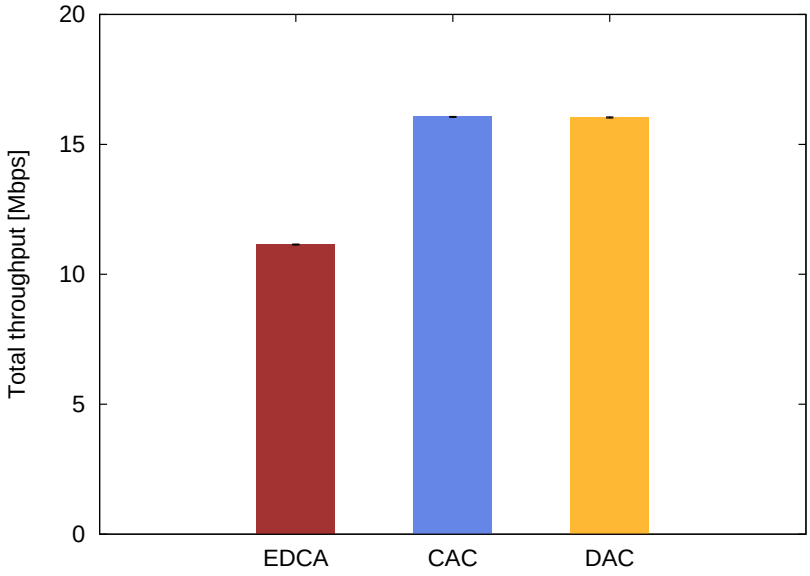


Figure 5.1: Total throughput with UDP traffic.

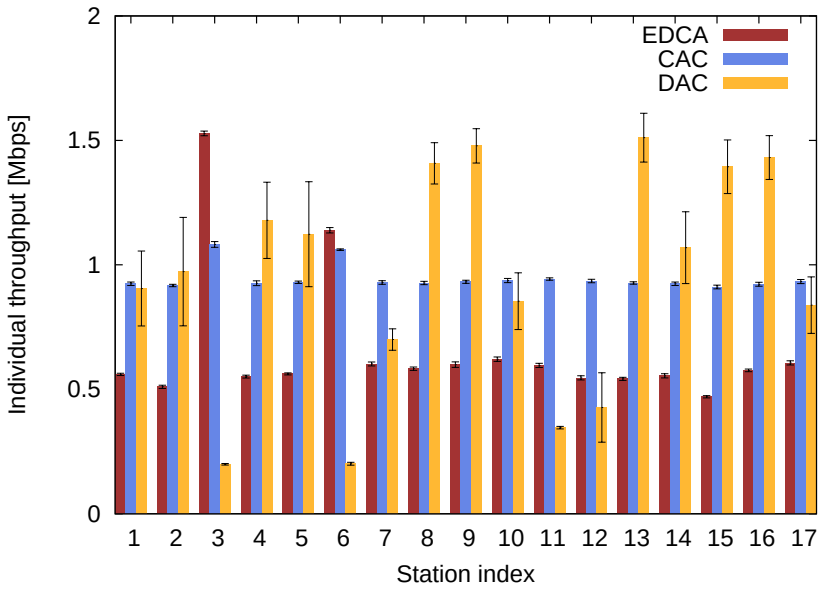


Figure 5.2: Throughput per station with UDP traffic.

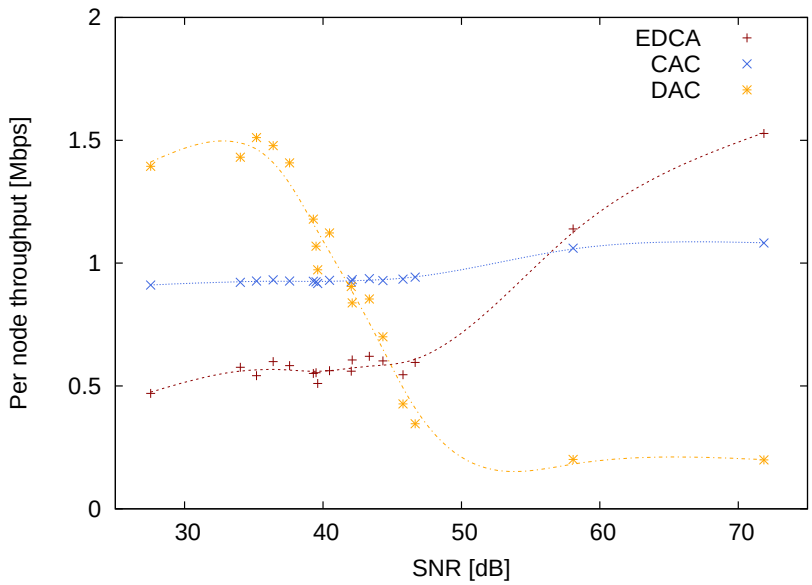


Figure 5.3: Throughput obtained vs. SNR.

5.2 Impact of SNR on Throughput

We have seen that link quality impacts the obtained throughput distribution, in particular for EDCA and DAC. To analyze this impact, we plot in Fig. 5.3 the average UDP throughput per station vs. the SNR of the link between the station and the AP. Note that for ease of visualization we also plot *natural smoothing splines* over the data points.

From the figure we observe that: (i) for EDCA there is a noticeable and positive correlation between SNR and throughput; (ii) for CAC, performance is not much affected by SNR dissimilarities, as significantly better link qualities result in very small throughput improvements; (iii) for DAC there is a large and negative correlation between SNR and throughput, with small differences in terms of SNR causing large differences in terms of throughput.

For the case of EDCA, the positive correlation is caused by the *capture effect*. With this effect, in case of a collision the receiver can decode the packet with the higher SNR. As a result, stations with better link quality obtain higher throughput. In contrast, the use of CAC reduces the number of collisions in the WLAN, and therefore the impact of the capture effect is significantly reduced.

For the case of DAC, the negative correlation is also driven by the capture effect as follows. Nodes with high capture probability will experience smaller collision rates than the others, and therefore will have $p_{own,i}$ smaller than $p_{obs,i}$. This will cause a positive error signal according to the $e_{fairness,i}$ term in (2.7), which will result in large CW_{min} values. Conversely, nodes with low capture probability will experience larger $p_{own,i}$ values and smaller $p_{obs,i}$ ones, and therefore will have smaller CW_{min} configurations. In this way, capturing nodes will transmit less often and therefore will obtain low throughput figures, while the other nodes will transmit more often and experience a higher throughput. Additional experiments with different transmission power settings, not reported due to space constrains, confirmed that a careful *equalization* of the link qualities is able to restore fairness in all cases.

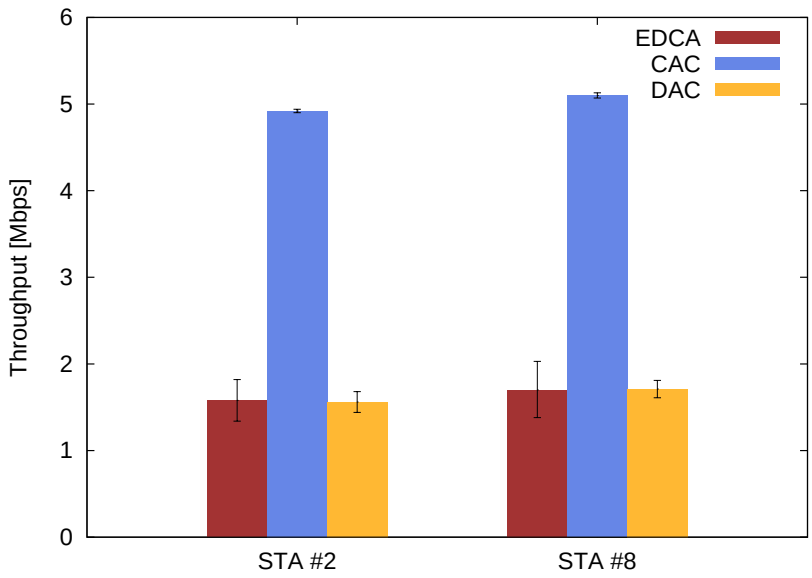


Figure 5.4: Performance with hidden nodes.

5.3 Hidden Nodes Scenario

Our adaptive algorithms have been designed for scenarios where all stations are in radio range of each other and coordinate their transmissions by means of carrier sensing. However, in real deployments hidden nodes may be present, and therefore we want to investigate their behavior under such circumstances.

To this aim, we ran extensive measurements, selecting different topologies and different transmission power settings, to determine the most pathological scenario. This is obtained when node 3 acts as AP, and nodes 2 and 8 act as stations, using a transmission power level of 5 dBm. With this setting, each EDCA station transmitting in isolation (i.e., with the other station silent) obtains about 16.3 Mbps of UDP throughput, while if both stations transmit simultaneously the throughput of each one drops to 1.6 Mbps. Thereby we managed to reproduce a hidden node scenario.

We then repeated the experiment with CAC and DAC, and obtained the results depicted in Fig. 5.4. We observe that the use of DAC does not improve performance over EDCA. In contrast, CAC provides a dramatic throughput increase, i.e., more than three times the throughput attained with the other mechanisms. We conclude that CAC detects the large collision rate and commands hidden nodes to be less aggressive by announcing a higher CW_{min}, which lessens (but does not eliminate) the hidden node problem. On the other hand, a station running DAC is not able to overhear MAC (re-)transmissions from hidden nodes, and hence cannot correctly estimate the collision probability in the network.

5.4 Impact Network Size

We next evaluate the performance of the algorithms as a function of the number of stations. To this aim, we measure the total throughput and JFI for an increasing number of contending nodes,

adding new stations in ascending order of their link quality. We plot the throughput and fairness results in Fig. 5.5 and Fig. 5.6 respectively.

We observe that for both DAC and CAC the total throughput performance is substantially flat, regardless of the number of stations. This result confirms that both approaches are able to adapt the CW to the number of stations present in the WLAN.

For the case of EDCA, performance degrades with the number of stations, which is the expected result from the use of a fixed set of (relatively small) contention parameters. However, for $N > 15$ the total throughput performance slightly grows again, a behavior caused by the capture effect as the last nodes to be added in our experiments are the ones experiencing better link qualities (nodes 3 and 6). This is confirmed by the fairness values, as for $N > 15$ there is a drop in the JFI for the case of EDCA. JFI values also confirm that DAC is more sensitive to heterogeneous link conditions, as its performance noticeably degrades with N. In contrast, with CAC the fairness index is practically constant for all N values.

5.5 TCP Throughput

We next evaluate performance in a scenarios in which stations use TCP. We start by evaluating the throughput and fairness performance when all stations are constantly backlogged sending TCP traffic to the AP, replicating *bulky* FTP transfers. Note that this scenario is substantially different from the ones considered in the previous sections, as TCP congestion control[1] introduces a "closed loop" that can lead to extreme unfairness conditions and even starvation [10].

We plot in Fig. 5.7 the total throughput values for the three mechanisms. According to the results, both CAC and DAC significantly outperform EDCA, improving throughput by 50% and 40%, respectively.

The per-station throughput distribution is depicted in Fig. 5.8. With EDCA, the node with the poorest link quality (node 15) suffers from a large performance degradation, this being worse than in the UDP case (see Fig. 5.1). The use of DAC with TCP traffic also exacerbates the unevenness in the traffic distribution, with node 15 clearly outstanding among the other nodes. DAC results also present a large deviation, caused by relatively frequent TCP timeouts from nodes with weak radio link (e.g., node 15). Conversely, CAC yields a remarkable fair and stable throughput distribution.

Like in the UDP case, we compute the JFI values for the resulting throughput distributions. In this case, the values for EDCA, CAC and DAC are 0.787, 0.996 and 0.692, respectively. We conclude that, as expected, the performance of EDCA and DAC worsens with TCP, while CAC preserves its good properties in this scenario.

[1]The Linux distribution used in our deployment executes the TCP CUBIC variant [11].

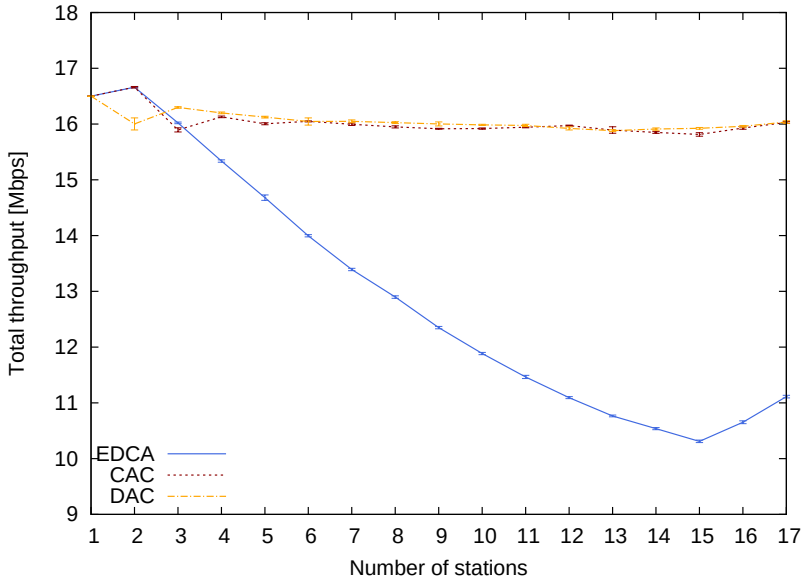


Figure 5.5: Total throughput for different number of stations.

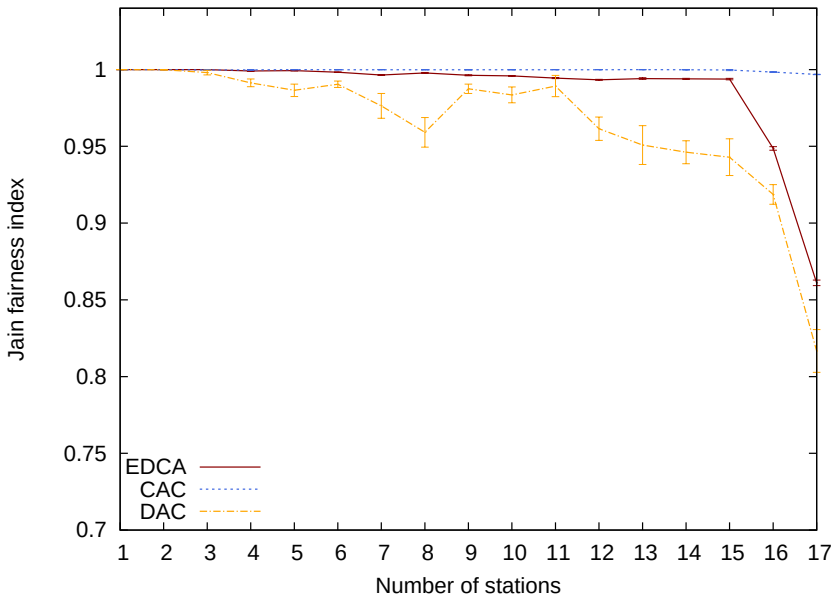


Figure 5.6: Fairness for different number of stations.

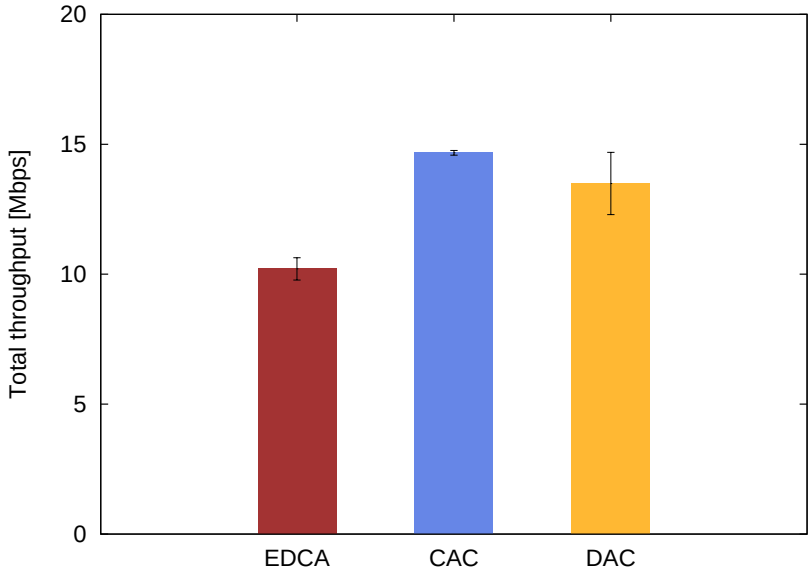


Figure 5.7: Total throughput of FTP-like traffic.

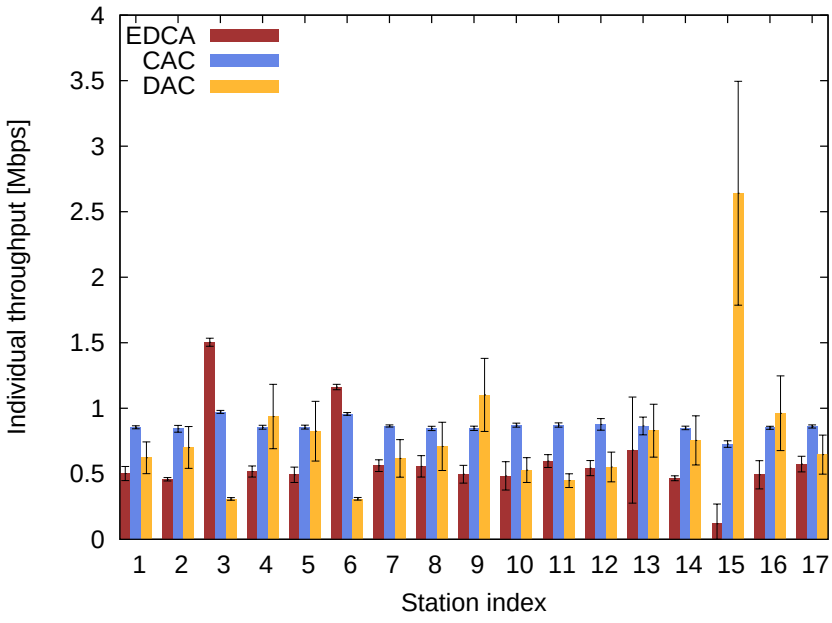


Figure 5.8: Throughput per station with FTP-like traffic.

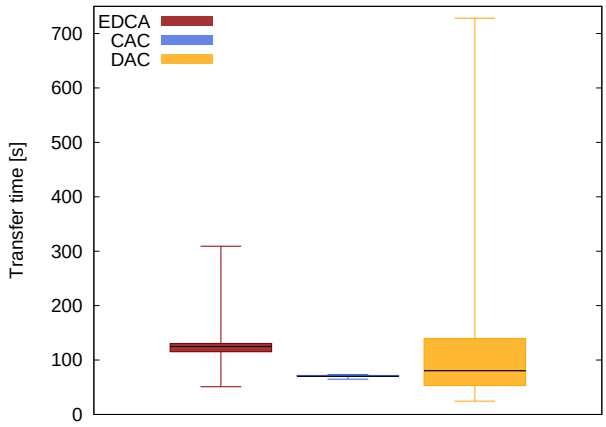
5.6 TCP Transfer Delay

We finally consider a scenario involving finite-size TCP connections. More specifically, all stations alternate periods of activity—during which a transmission of 10 MB occurs—with silent periods exponentially distributed with mean $1/\lambda$ [1]. We consider three different values for λ, corresponding to three different levels of activity, namely high, moderate and low. For each case we ran 1-hour experiments, logging all transfer durations and computing the per-station average delay. We use a *box-and-whisker* diagram to illustrate the distribution of the average delay among nodes: we provide the median, first and third quartiles of the average delay, as well as its maximum and minimum values.

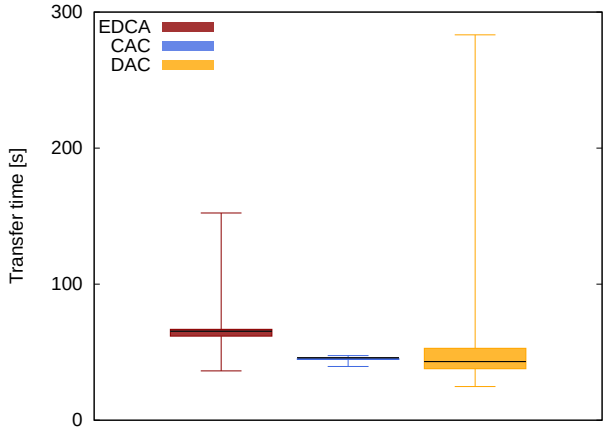
Results are depicted in Fig. 5.9. As shown in Fig. 5.9(a), with $\lambda = 1/30\ s$, which corresponds to high activity, we see that CAC provides the smallest and most uniform distribution of transfer delay among nodes, with practically no difference between the best and worst performing node. In case of EDCA, the delay shows a larger median and higher variability. However, the small distance between the first and third quartiles shows that most of the stations experience similar performance. Finally, for the case of DAC, despite the median is similar to the one of CAC, results show a much larger dispersion.

As can be seen in Fig 5.9(b), when the traffic activity is moderate ($\lambda = 1/60\ s$), the absolute values decrease, but the relative results are similar, i.e., CAC provides again the smallest and most uniform delays among nodes. Finally, as depicted in Fig 5.9(c), when the activity of the nodes is low ($\lambda = 1/90\ s$), medians are very similar, but CAC still provides the most fair distribution of the transfer delays. From these experiments, we conclude that CAC also provides the best performance under dynamic traffic scenarios.

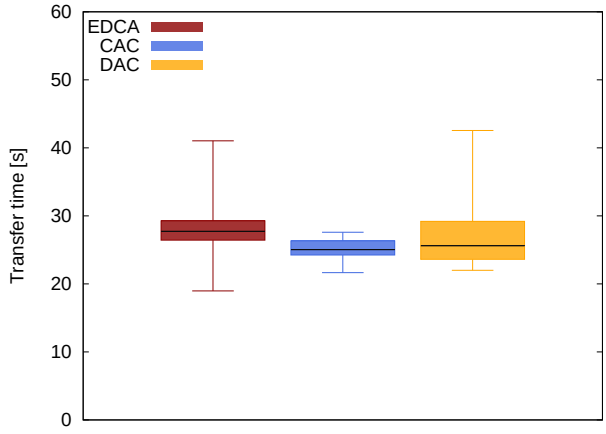
In order to provide a better and more intuitive feeling of what is going on within the testbed during these measurements, we report in Fig. 5.10 the duration of each file transfer for all the three mechanisms (reported only for the case of $\lambda = 1/30\ s$ without loss of generality). Specifically, in Fig. 5.10(a) we can observe that EDCA, as expected, favors the transfers of those nodes which experience better channel conditions (i.e., node 3, 6), whereas penalizes those initiated from nodes experiencing poor link qualities (e.g., node 15). In Fig. 5.10(b) instead, we can graphically appreciate how CAC equally shortens the transfer time without any remarkable distinction among nodes. Finally, in Fig. 5.10(c) we can observe how DAC favors nodes with relatively low SNR (e.g., nodes 15, 16), while nodes with good channel conditions almost starve, being able to complete only a few transfers (i.e., node 3, 6). Moreover, given a fixed node, the large variability of file transfer duration reflects a higher level of unpredictability which was absent with the other mechanisms. In fact, results obtained with DAC suffer from a larger dispersion, as enlightened by the broad standard deviations shown in Fig. 5.9. In our experiments we observed that this highly variable file transfer duration, as well as the TCP throughput, is due to the frequent occurrence of TCP timeouts at nodes with weak connectivity, which are also the nodes using the most aggressive $CWmin$ when DAC is adopted.



(a) $\lambda = 1/30\ s$

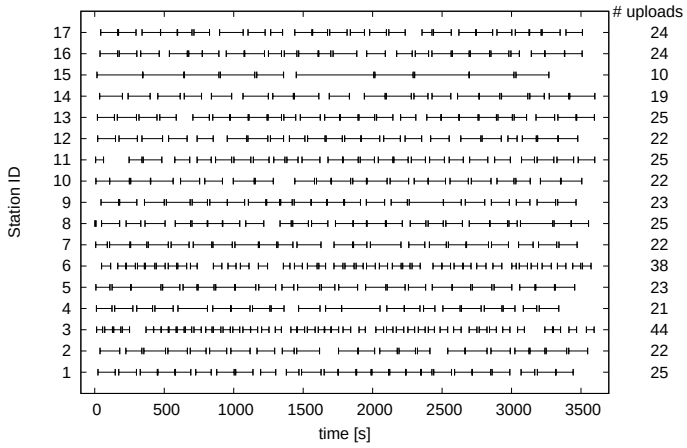


(b) $\lambda = 1/60\ s$

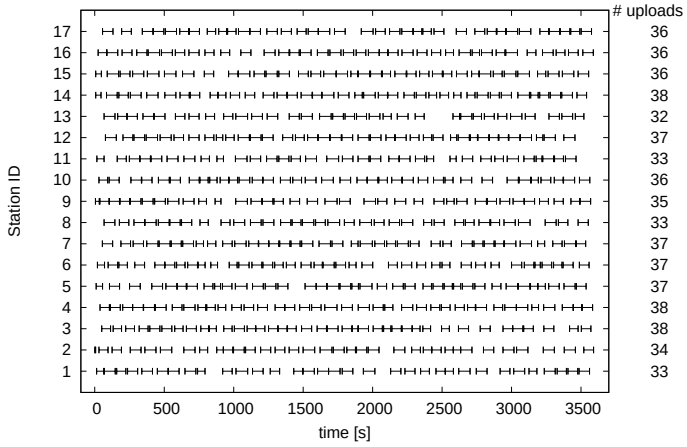


(c) $\lambda = 1/90\ s$

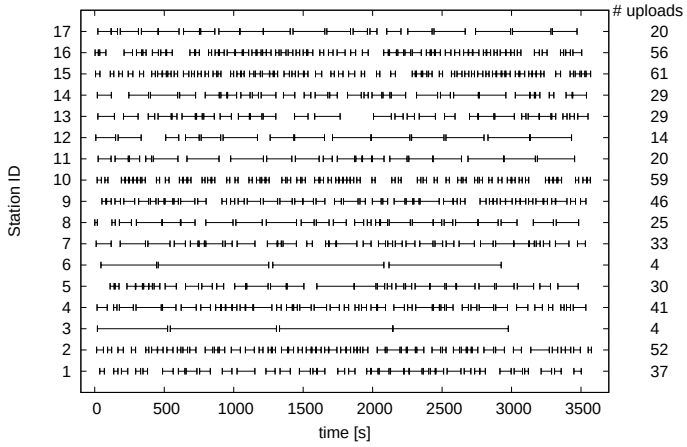
Figure 5.9: TCP delay performances.



(a) EDCA



(b) CAC



(c) DAC

Figure 5.10: Upload tranfers duration for the three mechanisms ($\lambda = 1/30\ s$).

Chapter 6

Related Work

The scientific literature offers many examples of MAC optimization approaches. Many of them are based on a centralized entity, responsible for monitoring system performance and adapting the system parameters to current conditions. Other works focus on distributed approaches to adapt MAC parameters. Very little experimental work is available, and it is based on complex algorithms, non-standard functionality and small-sized networks. In the following we review the most significant contributions in each of these areas and describe the novelty of our work.

Centralized approaches. A significant number of approaches exists in the literature [16, 8, 18, 22] that use a single node to compute the set of MAC parameters to be used in the WLAN. With the exception of our CAC algorithm [18], the main drawbacks of these approaches are that they are either based on heuristics, thereby lacking analytical support for providing performance guarantees [16, 8], or they do not consider the dynamics of the WLAN under realistic scenarios [22].

Distributed approaches. Several works [24, 17, 4, 5, 12] have proposed mechanisms that independently adjust the backoff operation of each stations in the WLAN. The main disadvantages of these approaches are that they change the rules of the IEEE 802.11 standard and therefore require introducing significant hardware or firm-ware modifications.

Implementation experiences. Very few schemes to optimize WLAN performance have been developed in practice [22, 9, 2]. While the idea behind Idle Sense [12] is fairly simple, its implementation [9] entails a significant level of complexity, introducing tight timing constrains that require programming at the firmware level. The same limitation holds for the approach of [2], which introduces changes to the MAC protocol that require redesigning of the whole NIC implementation. Finally, the work of [22] does not propose or evaluate any adaptive algorithm to adapt the CW but just evaluates the performance of static configurations. Additionally, all of these works rely on testbeds substantially smaller than ours.

Chapter 7

Conclusions

In this thesis, we prototyped two adaptive mechanisms capable of tuning the contention window along the network conditions. In contrast to other proposals which require complex modifications, these mechanisms rely on standard functionalities already supported by COTS hardware/firmware, and do not introduce any extension to the IEEE 802.11 MAC. We extensively evaluated the performances of the two mechanisms in a 18-nodes testbed, considering a wide spectrum of network conditions. With our experimental study we identified the key limitations of the distributed scheme, inherent to realistic scenarios, and we confirmed that the centralized mechanism significantly improves network throughput, transfer delay and fairness under a broad variety of circumstances, including the pathological case of hidden nodes.

A major conclusion from our work is that, by simply adding a few lines of code at the AP to exploit the functionality readily available, we can achieve performance improvements of up to 50%. We do believe that the results drawn herein advocate a widespread adoption of the centralized mechanism. Finally, we also think that a centralized scheme should be adopted for future proposals design, while a distributed approach is nothing but a necessary fallback for those cases in which any node has a centralized and complete view of the network.

References

[1] P. Barford and M. E. Crovella. Generating representative web workloads for network and server performance evaluation. In *Proceedings of ACM SIGMETRICS*, pages 151–169, 1998.

[2] R. Bernasconi, S. Giordano, A. Puiatti, R. Bruno, and E. Gregori. Design and Implementation of an Enhanced 802.11 MAC Architecture for Single-Hop Wireless Networks. *EURASIP Journal on Wireless Communications and Networking*, 2007.

[3] G. Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, Mar 2000.

[4] L. Bononi, M. Conti, and E. Gregori. Runtime optimization of ieee 802.11 wireless lans performance. *IEEE Transactions on Parallel and Distributed Systems*, 15(1):66–80, Jan. 2004.

[5] F. Cali, M. Conti, and E. Gregori. IEEE 802.11 protocol: design and performance evaluation of an adaptive backoff mechanism. *IEEE Journal on Selected Areas in Communications*, 18(9):1774–1786, Sept. 2000.

[6] L. Chen, S. H. Low, and J. C. Doyle. Joint congestion control and media access control design for wireless ad hoc networks. In *Proc. IEEE INFOCOM*, Miami, Florida, march 2005.

[7] L. Chen, S. H. Low, and J. C. Doyle. Random access game and medium access control desig. *IEEE Transactions on Networking*, 18(4):1063–6692, dec. 2010.

[8] J. Freitag, N. L. S. da Fonseca, and J. F. de Rezende. Tuning of 802.11e Network Parameters. *IEEE Communications Letters*, 10(8):611–613, 2006.

[9] Y. Grunenberger, M. Heusse, F. Rousseau, and A. Duda. Experience with an implementation of the Idle Sense wireless access method. In *Proceedings of the ACM CoNEXT conference*, pages 1–12, New York, New York, 2007.

[10] O. Gurewitz, V. Mancuso, J. Shi, and E. Knightly. Measurement and modeling of the origins of starvation of congestion-controlled flows in wireless mesh networks. *IEEE Transactions on Networking*, 17(6), dec. 2009.

[11] S. Ha, I. Rhee, and L. Xu. CUBIC: a new TCP-friendly high-speed TCP variant. *ACM SIGOPS Operating Systems Review*, 42:64–74, July 2008.

[12] M. Heusse, F. Rousseau, R. Guillier, and A. Duda. Idle sense: an optimal access method for high throughput and fairness in rate diverse wireless LANs. In *Proc. ACM SIGCOMM*, pages 121–132, Philadelphia, PA, USA, 2005.

[13] IEEE 802.11. *Supplement to Wireless LAN Medium Access Control and Physical Layer specifications: high-speed physical layer in the 5 GHz band*. IEEE Std 802.11a, 1999.

[14] IEEE 802.11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Revision of IEEE Std 802.11-1999, 2007.

[15] R. Jain, Chiu, D.M., and W. Hawe. A Quantitative Measure of Fairness and Discrimination for Resource Allocation in Shared Systems. *DEC Research Report TR-301*, 1984.

[16] A. Nafaa, A. Ksentini, A. A. Mehaoua, B. Ishibashi, Y. Iraqi, and R. Boutaba. Sliding Contention Window (SCW): Towards Backoff Range-Based Service Differentiation over IEEE 802.11 Wireless LAN Networks. *IEEE Network*, 19(4):45–51, Jul 2005.

[17] Q. Ni, I. Aad, C. Barakat, and T. Turletti. Modeling and Analysis of Slow CW Decrease for IEEE 802.11 WLAN. In *Proc. IEEE Personal, Indoor, and Mobile Radio Communications Conference (PIMRC)*, Beijing, 2003.

[18] P. Patras, A. Banchs, and P. Serrano. A Control Theoretic Approach for Throughput Optimization in IEEE 802.11e EDCA WLANs. *Mobile Networks and Applications (MONET)*, 14(6):697–708, Dec 2009.

[19] P. Patras, A. Banchs, P. Serrano, and A. Azcorra. A Control Theoretic Approach to Distributed Optimal Configuration of 802.11 WLANs. *IEEE Transactions on Mobile Computing*, 10(6):897–910, Jun 2011.

[20] L. Scalia, I. Tinnirello, J. Tantra, and C. H. Foh. Dynamic MAC Parameters Configuration for Performance Optimization in 802.11e Networks. In *Proc. GLOBECOM*, pages 1–6, San Francisco, CA, USA, Dec 2006.

[21] P. Serrano, C. J. Bernardos, A. de la Oliva, A. Banchs, I. Soto, and M. Zink. FloorNet: Deployment and Evaluation of a Multihop Wireless 802.11 Testbed. *EURASIP Journal on Wireless Communications and Networking*, 2010.

[22] V. A. Siris and G. Stamatakis. Optimal CWmin selection for achieving proportional fairness in multi-rate 802.11e WLANs: test-bed implementation and evaluation. In *Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization*, pages 41–48, Los Angeles, CA, USA, 2006.

[23] Q. Xia and M. Hamdi. Contention Window Adjustment for IEEE 802.11 WLANs: A Control-Theoretic Approach. In *Proc. International Conference on Computer Communications (ICC)*, Istanbul, Turkey, Jun 2006.

[24] Y. Yang, J. J. Wang, and R. Kravets. Distributed Optimal Contention Window Control for Elastic Traffic in Single-Cell Wireless LANs . *IEEE Transactions on Networking*, 15(6):1373–1386, Dec 2007.