Cognitive Wireless Local Area Networks

vorgelegt von

Murad Abusubaih
(Msc. in Electrical Engineering)

von der Fakultät IV – Elektrotechnik und Informatik –
der Technischen Universität Berlin
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
– Dr.-Ing. –

Dissertation

Promotionsausschuss:

Vorsitzender: Prof. Dr. Dr. Holger Boche

Berichter: Prof. Dr.-Ing. Adam Wolisz

Berichter: Prof. Dr. rer. nat. Jens-Peter Redlich

Tag der wissenschaftlichen Aussprache: 24.8.2009

Berlin 2009
D 83

To My Lovely Wife ALAA

Abstract

The last few years have seen a tremendous increase in the deployment of 802.11 Wireless Local Area Networks (WLANs). The proliferation of wireless users and the promise of converged voice, data and video technology is expected to open new numerous opportunities for 802.11 - based WLANs in the networking market.

When the WLAN design was first developed in 1990, the model assumes that a WLAN deployment comprises one stand alone Access Point (AP). In fact, such a system provides satisfactory user experience as long as there is few users with relatively light traffic load and one AP. Due to rapid increase of wireless users and the requirement for continuous coverage, multi-AP WLANs nowadays span buildings or floors. Some neighboring APs have to be configured on the same channel due to the limited number of channels the 802.11 standard supports. This leads to mutual interference among WLAN nodes, increasing contention and back-off intervals. Inevitably, the capacity of the WLAN and the performance that wireless users experience precipitously drop due to interference. A consequence of dense WLAN deployments coupled with the limited number of channels, is that interference is the main serious and challenging problem and methods to mitigate it are essential.

As a matter of fact, the reason for the interference problem stems from the static configuration of today's WLANs. On the positive side, better performance can be achieved by integrating dynamic and adaptive management schemes in today's WLANs. Efficient WLAN management and better Quality of Service (QoS) can be achieved if APs and WLAN cards actively negotiate and agree on their configurations. We call such WLANs "Cognitive WLANs". **A cognitive WLAN is a self-reconfigurable WLAN that is aware of the dynamical changes in the radio environment and users dynamics. It listens, learns, shares information and adapts its parameters dynamically as necessary.**

This thesis contributes to the development of a cognitive WLAN by suggesting a framework for interference mitigation. Within this framework, the Terminal-AP selection policy currently implemented in WLAN adapters is firstly improved. The goal is to reduce the impact of interference at the selection phase. A terminal is informed by APs about the interference conditions before joining a Basic Service Set (BSS). With this policy, a user is not only enabled to join a BSS within which it has a strong signal to the AP, but also one which measures less interference from nodes belonging to neighboring BSSs.

While the network is operational, nodes monitor the QoS in the WLAN. If QoS is observed to be degraded, diagnostic algorithms are used to infer probable cause. Methods for interference estimation are developed. Interference estimation is achieved through packet loss discrimination and passive channel monitoring. The network first tries to tune the Request to Send/Clear to Receive (RTS/CTS) mechanism if the cause is interference resulted from hidden nodes. New criterion for tuning the RTS/CTS in multi-rate multi-BSS deployments is developed. The criterion instructs a usage of RTS/CTS by detected active hidden node pairs, if these handshake packets are expected to improve the communication quality across the WLAN. However, if the RTS/CTS is expected to be not sufficient, interfering BSSs negotiate and change the channel access scheme. They coordinate their transmissions by switching from the Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) to a time slotted access scheme if the switching is found to be feasible and expected to be useful. A hybrid channel access scheme is developed to achieve the later goal. For the operation in the time slotted modus, a scheduling algorithm has been developed.

Zusammenfassung

In den letzten Jahren hat IEEE-802.11-basierte WLAN-Technologie (Wireless Local Area Networks) immer weitere Verbreitung gefunden. Die gestiegenen Benutzerzahlen und die Möglichkeit, Sprach-, Daten- und Videodienste auf der gleichen Kommunikationsplattform anzubieten, eröffnen neue Möglichkeiten für WLAN-Technologien am Markt.

Die im Jahre 1990 begonnen Arbeiten am 802.11 WLAN-Standard sind davon ausgegangen, dass es in typischen WLAN-Installationen nur einen einzigen Access Point (AP) gibt. Wenn die Benutzerzahl nicht zu gross ist, lässt sich mit einem solchen Aufbau für die einzelnen Benutzer eine befriedigende Dienstqualität erreichen. Durch die rapide gestiegenen Benutzerzahlen und den Wunsch nach kontinuierlicher WLAN-Abdeckung werden heutzutage WLANs mit mehreren APs realisiert, die einzelne Etagen oder sogar komplette Gebäude abdecken. Es ist mitunter notwendig, benachbarte APs auf dem gleichen Frequenzkanal zu betreiben, weil der Standard nur wenige nicht-ueberlappende Kanäle vorsieht. Dies führt zu gegenseitiger Interferenz zwischen WLAN-Knoten, erhöhter Konkurrenz beim Zugriff auf den Kanal und vergrösserten Backoff-Intervallen. Es ist nicht zu vermeiden, dass die Kapazität des WLANs und die für einzelne Benutzer erreichbaren Dienstqualitäten unter der erhöhten Interferenz leiden. Für dichte WLAN-Installationen und bedingt durch die geringe verfügbare Anzahl an Frequenzkanälen ist Interferenz zu einem wesentlichen Problem geworden und dementsprechend gibt es grosses Interesse an Methoden, mit deren Hilfe die Interferenzsituation verbessert werden kann.

Es kann davon ausgegangen werden, dass der wesentliche Grund für das Interferenzproblem in der statischen Konfiguration heutiger WLANs liegt. Eine verbesserte Leistung kann durch die Integration dynamischer und adaptiver Management-Verfahren in heute WLANs erreicht werden. Um ein effizientes WLAN-Management und bessere Dienstgüten zu erreichen, können APs und Terminals ihre Konfigurationsparameter dynamisch untereinander aushandeln. Wir bezeichnen solche WLANs als "kognitive WLANs“. Ein kognitives WLAN ist ein selbstkonfigurierendes WLAN welches Veränderungen in der Radio-Umgebung und der Benutzerpopulation erkennt und sich daran anpassen kann. Ein kognitives WLAN lauscht auf dem Kanal, lernt den derzeitigen Zustand, tauscht Informationen mit anderen kognitiven WLANs aus und passt seine Parameter und Konfigurationsdaten dynamisch an.

Diese Arbeit leistet einen Beitrag zur Entwicklung kognitiver WLANs. Es wird ein Framework zur Verringerung der Interferenz in 802.11-basierten Infrastruktur-WLANs vorgeschlagen. Im Rahmen dieses Frameworks wird zunächst die Auswahlregel für die Zuordnung von Terminals zu APs verbessert. Das Ziel ist Interferenzen bereits in Phase des Auswahl des AP zu reduzieren. Bevor ein Terminal sich an ein Basic Service Set (BSS) assoziiert, wird es von APs über Interferenzen informiert. Mit dieser Strategie, wählt ein Terminal nicht nur ein BSS mit dem stärksten Signal aus, sondern berücksichtig Interferenz von Knoten der benachbarten BSSs.

Während das Netzwerk aktive ist, beobachten alle Knoten die Dienstgüte in ihrem WLAN. Wenn die beobachtete Dienstgüte nicht mehr ausreichend ist, werden zunächst die Ursachen dafür mittels spezieller Diagnosealgorithmen ermittelt. Methoden zur Abschätzung der Interferenz wurden entwickelt, die die Ursache eine Verluste bestimmen und den Kanal passive beobachten. Wenn festgestellt wird, dass die Interferenz vor allem aus Hidden-Terminal-Problemen resultiert, werden die Parameter des Request to Send/Clear to Send (RTS/CTS)-Handshakes angepasst. Ein neues Kriterium zu Feinabstimmung des RTS/CTS Mechanismus für multi-rate multi-BSS Installationen wurde entwickelt. Dieses Kriterium basiert darauf der RTS/CTS Mechanismus bei aktiven verdeckten Knoten einzuschalten. Wenn das RTS/CTS nicht ausreicht, wird für das betrachtete BSS ein neues Mediumzugriffsverfahren vereinbart, insbesondere wird von Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) zu einem Zugriffsverfahren auf der Basis fest zugewiesener Zeitslots gewechselt wenn dies eine Verbesserung verspricht. Ein hybrider Medienzugriffs Mechanismus und ein Scheduling Algorithmus für den Betrieb in einem System mit zeitgesteuerten Zugriff wurde etwickelt.

Acknowledgments

I would like to thank Professor Adam Wolisz for his guidance and support during my doctoral study. His motivation and encouragement caused me to work hard during the last years and enjoy my work at the same time. His inspiring ideas, suggestions enriched and improved the quality of this work. I learned a lot from him.

Also, I would like to thank my colleagues Dr. James Gross, Mr. Berthold Rathke, Sven Wiethoelter, and Daniel Hollos. for the valuable discussions, fruitful collaboration, and input in the course of the work. It is a pleasure to work with you! Thanks also to all the TKN-group members, for their cooperation and help.

Special thanks goes to my parents for their constant support and encouragement throughout my study. Especially, I would like to express my love to my wife ALAA who has always been besides me. Her unabated support helps me a lot to progress.

Last but not least, I would like to express my gratitude to the German Academic Exchange Service (DAAD) for the grant to pursue my doctoral study in Germany.

Contents

List of Tables

List of Figures

List of Acronyms

ACK Acknowledgment

AP Access Point

BER Bit Error Rate

BSS Basic Service Set

CBR Constant Bit Rate

CCA Clear Channel Assessment

CCI Co-Channel Interference

CCK Complementary Code Keying

CTS Clear to Send

CSMA Carrier Sense Multiple Access

CSMA/CA Carrier Sense Multiple Access / Collision Avoidance

CSMA/CD Carrier Sense Multiple Access / Collision Detection

CW Contention Window

DCF Distributed Coordination Function

DFS Dynamic Frequency Selection

DIFS Distributed Inter-Frame Space

DS Distribution System

DSSS Direct Sequence Spread Spectrum

EDCA Enhanced Distributed Channel Access

ESS Extended Service Set

FDMA Frequency Division Multiple Access

FHSS Frequency Hopping Spread Spectrum

GIS Geographic Information System

GPS Global Positioning System

HCF Hybrid Coordination Function

HCCA Hybrid Coordination Function-Controlled Channel Access

IBSS Independent Basic Service Set

IAPP Inter-Access-Point Protocol

IP Internet Protocol

ISM Industrial, Scientific and Medical

IEEE Institute of Electrical and Electronics Engineers

MAC Medium Access Control

Mbps Mega Bit Per Second

MIB Management Information Base

MIMO Multiple Input - Multiple Output

MSDU Medium Access Control Service Data Unit

MPDU Medium Access Control Protocol Data Unit

NAV Network Allocation Vector

OFDM Orthogonal Frequency Devision Multiplexing

OSI Open System Interconnection

PCF Point Coordination Function

PDA Personal Digital Assistant

PHY Physical Layer

QoS Quality of Service

RCPI Received Channel Power Indicator

RRM Radio Resource Measurements

RSSI Received Signal Strength Indicator

RTS Request To Send

RTS/CTS Request To Send / Clear to Send

SIFS Short Inter-Frame Space

SIR Signal-to-Interference Ratio

SINR Signal-to-Interference and Noise Ratio

SSID Service Set Identity

STA Station

TG Task Group

TDMA Time Division Multiple Access

TPC Transmit Power Control

VoIP Voice over Internet Protocol

WAN Wide Area Network

WLAN Wireless Local Area Network

Chapter 1

Introduction

It was not difficult for WLANs to penetrate all homes, small offices, large companies and public hot-spots. This has been fueled by three trends: the decreasing cost of wireless networking equipments like Access Points (APs) and WLAN cards; the fast advances in WLAN data rates; and the growing use of laptops and personal digital assistants (PDAs). Nowadays, WLAN is the preferred access technology for an increasing number of users. In alignment with the growth of WLANs, users demands are also becoming more and their satisfaction becomes a challenging task for both network designers and administrators.

Although originally several solutions for WLANs have been competing, today virtually all WLANs are based on the IEEE 802.11 standard. The IEEE 802.11 standard defines two modes of WLAN operation: the Ad hoc and the Infrastructure modes. In the former, wireless stations (STAs) communicate directly with each other without involving any intermediate central point while in the later STAs communicate with each other and with the wired network via a central device called the Access Point (AP). The IEEE 802.11 utilizes the license free band. The 802.11b/g operate in the Industrial, Scientific and Medical (ISM) 2.4GHz band while 802.11a operates in the National Information Infrastructure 5GHz band. As in all communication systems, the 802.11 spectrum is a scare resource. The number of supported channels by any IEEE 802.11 standard is limited and among all channels only few of them do not overlap.

In infrastructure WLANs, each AP is usually assigned a fixed channel. STAs connected to an AP over the same channel share the limited channel bandwidth. High physical rates are offten employed if a STA is close to its AP. A low rate STA tends to degrade the performance of high rate STAs if they are associated with the same AP. WLAN administrators try to improve users' connectivity with the network by deploying a high density of APs. However, the dense deployment of APs can introduce mutual interference, high collision rates, and long back-off intervals unless the network is carefully planned and tuned. This is due to the limited number of orthogonal channels that the 802.11 standard supports which requires the assignment of same channel to multiple APs that are close to each other.

Generally, interference can be defined as the overlapping of two signals in the same frequency band. Interference is the main challenging problem that limits the performance of wireless networks. In 802.11 WLANs, it may prohibit two nodes from sending packets, despite non of the signals interfering the receiver of the other. On the other hand, an interfering signal may damage a packet being received, if its power is strong enough relative to the desired signal power at its receiver.

As a consequence to the aforementioned facts, even efficient network planning strategies, usually carried out before network deployment, will not be good enough to provide WLAN users an acceptable QoS due to the dynamic nature and randomness of network events. This motivates the requirement for dynamic cognitive self-managed WLANs. Such a network will be able to listen, learn, share information and adapt its parameters dynamically as necessary. The aim of this thesis is to contribute to the development of such WLANs.

Despite that WLANs are nowadays so popular, their performance is rather far from being satisfactory. Huge research activities have been lunched in recent years in academia, industry and within standardization bodies to solve the problems of current WLANs and enhance users' QoS. Nonetheless, there is a rather large space for improvement and many serious challenges are still open.

This thesis contributes to the development of a cognitive WLAN by proposing a framework to alleviate the interference problem in such a network. It provides innovative concepts that can influence the design of future WLANs and complement other existing solutions. Figure 1.1 shows the main active research directions and the location of the thesis work in this research area. Due to the large amount of research efforts devoted to network planning, channel selection and power control approaches, the thesis suggests a new methodology for interference mitigation that focuses specially on the

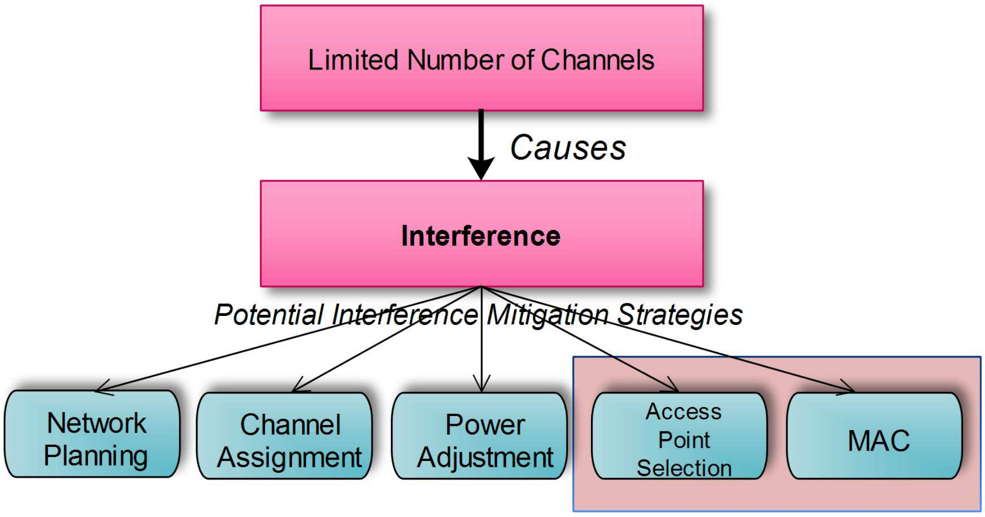


Figure 1.1: Thesis Scope

AP selection policy and the MAC protocol. The objective is to reduce performance limitations due to interference. For the evaluation of the suggested methods, the measure of success will be the improvement of users' QoS as well as fairness among them. The proposed framework aims to achieve the interference mitigation goal by first reducing the interference impact at the AP selection phase. Then it tunes the MAC operation, while the network is operational, based on interference conditions. These are assessed through measurement-based interference estimation approaches we develop for this purpose.

Thesis contributions are summarized as follows: first the thesis develops a new decentralized AP selection policy. The goal of this policy is to reduce the impact of interference on a STA at the selection phase. With this selection policy, a STA is guided by its potential AP about the interference conditions before joining the BSS. Interference information is provided in beacon and probe response frames. By this, a STA is not only enabled to join a BSS within which it has a strong signal to the AP, but also one which measures less interference from nodes belonging to neighboring BSSs.

While the network is operational, APs use interference estimation methods and monitor the communication quality within their BSSs. They accomplish this with the help of the STAs they accommodate. If the communication is observed to be degraded and diagnoses conclude that the cause is high interference resulted from hidden nodes, interfering BSSs first consider the tuning of RTS/CTS in order to reduce interference. As second contribution, new criterion for tuning the RTS/CTS in multi-rate multi-BSS deployments is developed. The criterion instructs a usage of RTS/CTS by detected active hidden node pairs, if these handshake packets are expected to improve the communication quality across the WLAN.

However, if the RTS/CTS signaling is assessed to be unhelpful or insufficient, interfering BSSs consider a change of the channel access scheme. They negotiate and switch from the 802.11 CSMA/CA to a time slotted mechanism if the switch to the time slotted modus is expected to be useful and feasible. As third contribution, a hybrid channel access scheme is developed to achieve the later goal. The challenging and crucial aspects of this phase are:

- The estimation of interference and determination of interfering links.
- The decision when to select which access scheme.
- The determination of the scope of BSSs that shall employ a certain access scheme.
- The design of a scheduling algorithm that assigns time slots to wireless links.

The rest of the thesis is organized as follows: Chapter two presents general relevant background. Chapter three describes the system under consideration in this thesis. System entities, load and metrics are presented. In chapter four, methods for interference estimation are proposed. In chapter five, the interference-aware STA-AP selection policy is proposed. In Chapter six, the efficiency of using RTS/CTS for mitigating interference resulted from hidden nodes is studied. New criterion for controlling the RTS/CTS signaling is proposed. Chapter seven proposes and discusses a coordination-based channel access scheme for further mitigation of interference under high load conditions. Chapter eight evaluates the proposed interference mitigation solution proposed throughout this thesis, considering a case study of a real scenario and traffic. Chapter nine draws the main conclusions of this work and discusses some future research issues.

Chapter 2

Wireless Local Area Networks

2.1 Introduction

Recently, IEEE 802.11 Wireless Local Area Networks (WLANs) [1] are being rapidly deployed around the world. Because of the continuously dropping price of WLAN devices, WLAN is now the preferred access technology for families, small offices and enterprises. This chapter briefly describes the WLAN technology.

2.2 The 802.11 Standard

IEEE has approved the first 802.11 standard in June 1997. Like any 802 protocol, the standard defines a set of Medium Access Control (MAC) and Physical Layer (PHY) Specifications for local wireless networking as illustrated in figure 2.1. Figure 2.2 shows the relation between the IEEE 802.11 standards and the Open System Interconnection (OSI) reference model. The first 802.11 supports two transmission rates: 1Mbps and 2Mbps. In 1999, the IEEE 802.11a standard was released. It utilizes the 5GHz band and advances the data rate up to 54Mbps. Then, later that year, the IEEE ratified the 802.11b standard which operates in the 2.4 GHz band and allows a row transmission rate up to 11Mbps. In 2003, the 802.11g is standardized. Other enhancements of the original 802.11 standard are provided in section 2.8.

2.2.1 Physical Layer Standard

The physical layer mainly defines the frequencies, physical rates and encoding technique. Figure 2.3 provides some details about each standard. The original 802.11 standard defined three physical media:

- **Direct Sequence Spread Spectrum (DSSS):** This technology uses a single wide channel. The spreading is achieved by multiplying the data with a pseudo-random numerical sequence (called PN). The IEEE defines this standard to be used in the unlicensed 2.4GHz ISM band. The number of available channels depends on the amount of bandwidth allocated by the national regulatory agencies in country.

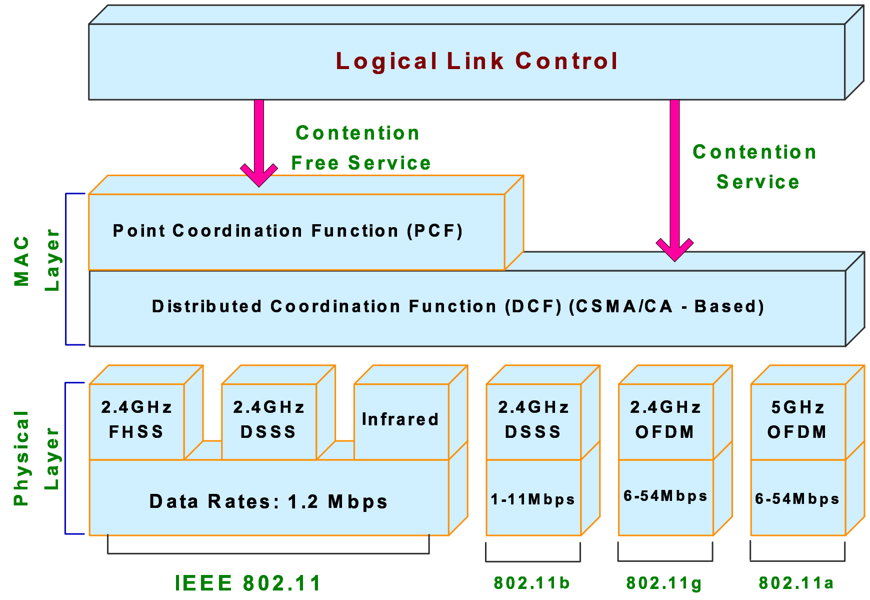


Figure 2.1: IEEE 802.11 Standards

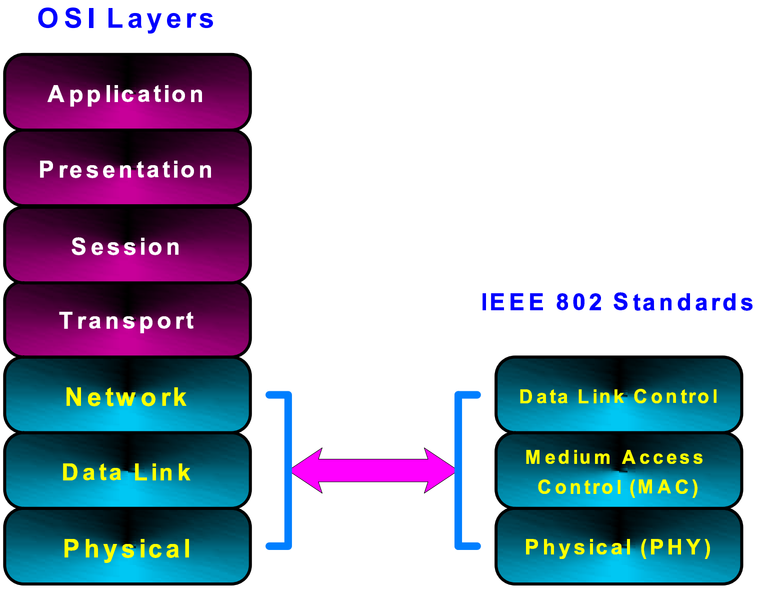
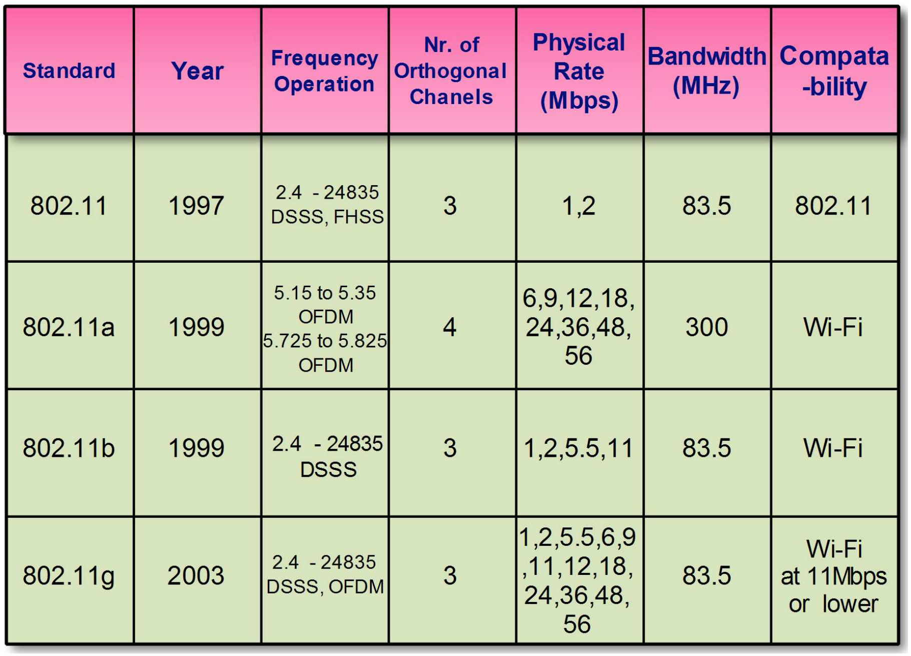


Figure 2.2: 802.11 and the OSI model



Standard	Year	Frequency Operation	Nr. of Orthogonal Chanels	Physical Rate (Mbps)	Bandwidth (MHz)	Compata -bility
802.11	1997	2.4 - 24835 DSSS, FHSS	3	1,2	83.5	802.11
802.11a	1999	5.15 to 5.35 OFDM 5.725 to 5.825 OFDM	4	6,9,12,18, 24,36,48, 56	300	Wi-Fi
802.11b	1999	2.4 - 24835 DSSS	3	1,2,5.5,11	83.5	Wi-Fi
802.11g	2003	2.4 - 24835 DSSS, OFDM	3	1,2,5.5,6,9 ,11,12,18, 24,36,48, 56	83.5	Wi-Fi at 11Mbps or lower

Figure 2.3: Physical Layer Standard

- **Frequency Hopping Spread Spectrum (FHSS):** With this technology, the system pseudo-randomly hops between a number of narrowband channels in relatively short time. The number of available channels ranges from 23 in Japan to 70 channels in the United States [2].

- **Infrared:** This technology uses Infrared at a wavelength between 850 and 950nm. Due to the limited supported data rates and the line of sight requirements, this option was not preferable and did not gain market support.

The 802.11b has been widely adopted in the networks market. It is now a default component of many laptops, personal computers and Personal Digital Assistants (PDAs). At the physical layer, the 802.11b uses an extension of the default IEEE 802.11 DSSS technology. The 802.11b achieves its maximum 11Mbps data rate by employing a modulation technique called Complementary Code Keying (CCK). However, some other technologies share its allocated spectrum like microwave ovens and cordless phones.

Unlike 802.11b, the 802.11a employs Orthogonal Frequency Devision Multiplexing (OFDM) technology at the physical layer rather than spread spectrum. OFDM uses multiple carrier signals at different frequencies and sends some of the bits on each frequency. Unfortunately, 802.11a suffers problems with coverage. Due to the well known basic rule of physics: the higher the radio frequency, the shorter the range, for the same transmission power level, an 802.11a device covers less area that an 802.11b can cover. As a result, more APs are required to cover a given area. In addition to the coverage problems, some countries prohibit the usage of the 802.11a products without dynamic frequency selection (DFS) and transmit power control (TPC). This is because the 802.11a devices share the same spectrum allocated to Radar and Satellite communication systems. Hence, the standard is not widely adopted.

802.11a is prohibited in some countries due to conflicting spectrum use

The 802.11g operates in the 2.4GHz band supporting a data rate of 54Mbps. The 802.11g devices employ DSSS and OFDM at the physical layer. They are backword compatible with 802.11b devices. Hence, 802.11b clients are able to connect to an 802.11g AP and 802.11g clients can connect to an 802.11b AP. However, like 802.11b devices, the 802.11g faces the interference problems from other devices running in the 2.4GHz band as well as 802.11b devices.

2.3 Types of 802.11 WLANs

The IEEE 802.11 defines two basic WLAN architectures, the Ad hoc and Infrastructure. The Ad hoc mode (shown in figure 2.4), also called Independent Basic Service Set (IBSS) or peer to peer, allows two or more STAs/clients to establish connectivity between them and the wireline network without the involvement of any central point. It is commonly used to form small networks set up for a specific purpose (for example a single meeting in a conference room). The Infrastructure mode (shown in figure 2.5), also called the Basic Service Set (BSS), relies on a central point called the Access Point (AP) through which the 802.11 STAs communicate with each other and the wireline network. The most important function of the AP is bridging. It converts the 802.11 frames to another type for delivery to the Wide Area Network (WAN). To cover a large area, two or more APs (BSSs) normally connected through a wired backbone are deployed. The connected BSSs are called Extended Service Set (ESS) and the wired backbone is called the Distribution System (DS). The DS is a logical component of the 802.11. It's main function is to relay frames among APs. The IEEE 802.11, however, does not define a specific technology for the DS. In almost all commercial products, Ethernet is used as the backbone technology. A configuration option at the STA that lets the user to choose between BSSs is called Service Set Identifier (SSID). It is a friendly name that identifies a particular BSS. Multiple access points can share the same SSID if they are part of an ESS and provide access to the same network.

The Infrastructure architecture has two major advantages:

- Unlike Ad hoc mode, the Infrastructure mode places no restrictions on the distance between two communicating STAs. The only requirement is that STAs should be within the coverage range of APs that form the ESS.

- APs assist STAs attempting to save power. When an AP notes that a STA enters a power saving mode, it buffers all frames distined to the STA. Hence, STAs can power up their wireless transceivers only to transmit or receive buffered frames from the AP.

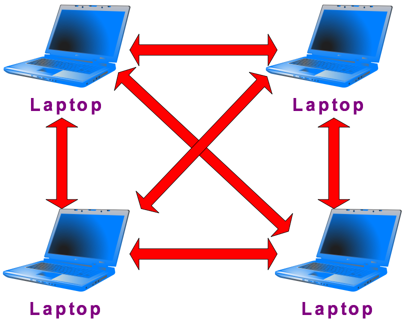


Figure 2.4: Ad hoc WLAN

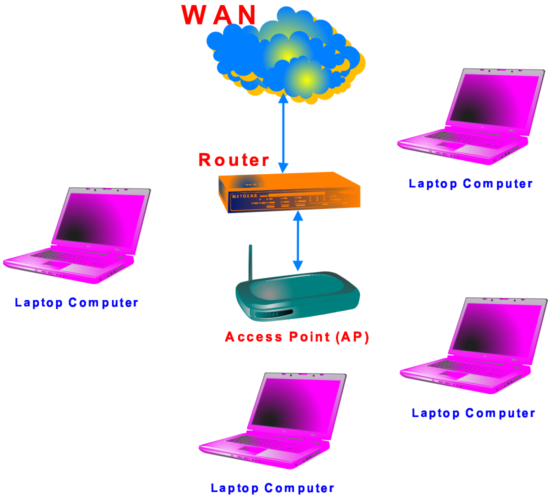


Figure 2.5: Infrastructure WLAN

2.4 Network Services

The major services the IEEE 802.11 provides are:

1. **Distribution:** In an infrastructure network, the AP uses this service to deliver a frame to its destination. Note that any communication in an infrastructure network goes through the distribution service.

2. **Association:** This is a management service. It facilitates the delivery of frames to STAs. Each STA has to register or associate to an AP to obtain network services. The DS can then use the registration information to determine the AP to which each STA belongs. The IEEE 802.11 does not mandate any particular implementation of the usage of the association information, except the functions that the DS must provide.

3. **Reassociation:** A management service that is initiated by a STA whenever the

signal level indicates that a different association with another AP is beneficial. After the completion of the reassociation, the DS updates its records to reflect the reachability of the STA via its new AP.

4. **Disassociation:** A management service used by STAs to terminate their associations. When a STA invokes this service, any data in the DS regarding this STA is removed.

2.5 Scanning and Joining a WLAN

Before it can join a network and access data transmission services, a STA has first to discover the networks in its vicinity. This process is called scanning. A set of parameters are used in the scanning process. Some of them are pre-configured by the user or the network administrator, some others have default values in the driver. The major parameters are:

1. **BSSType:** Determines wether a STA is part of an IBSS or BSS (Ad hoc or Infrastructure). This parameter is pre-configured by the user.

2. **SSID:** Normally, each network has a human-readable name (SSID) assigned by the administrator. Users are able to select the SSID the adapter has to search for.

3. **Scan Type:** This parameter determines whether the scanning process should be performed actively or passively.

4. **Channel List:** It is the list of the channels over which the scanning should be performed. Some 802.11 products allow the user to configure the channel list using specific commands.

5. **Min Channel Time and Max Channel Time:** These two parameters specify the maximum and minimum time periods that the scan procedure should work for each particular channel in the channel list.

2.5.1 Scanning Modes

The 802.11 supports two types of scanning:

- **Passive Scanning:** This mode, illustrated in figure 2.6, intends to save battery as it does not involve transmission. A STA simply hops over each channel on the channel list and listens for beacon frames. Beacon frames are transmitted periodically by APs to enable STAs finging them. A beacon basically includes the information a STA has to know before selecting a network and starting transmission such as: the SSID, channel, and supported physical rates. Beacons are also used to synchronize STAs and APs clocks

- **Active Scanning:** In this mode, illustrated in figure 2.7, a STA itself tries to find the BSSs in its vicinity rather than waiting BSSs to announce themselves. A STA transmits a frame called Probe Request frame on each channel on the channel list. APs respond to Probe Requests by sending Probe Response frames, providing same information as beacons.

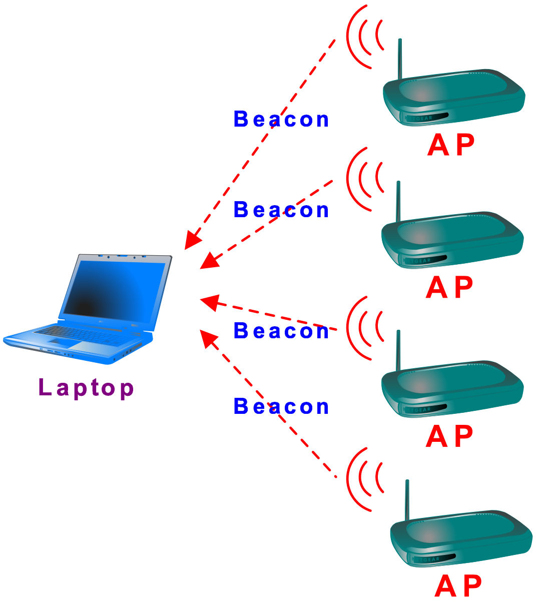


Figure 2.6: Passive Scanning

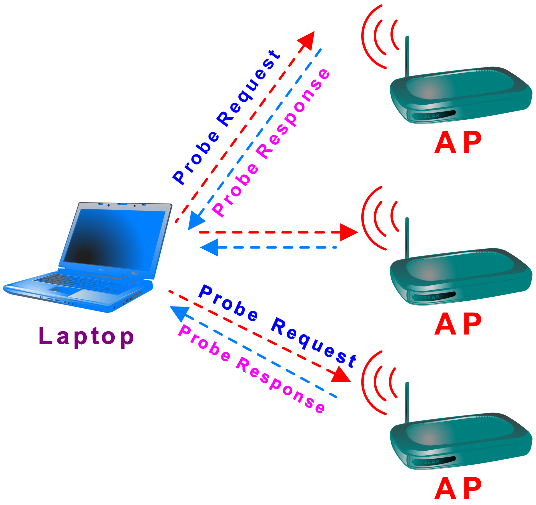


Figure 2.7: Active Scanning

2.5.2 Network Selection

After scanning, either passively or actively, a STA generates a scan report. The scan report includes all BSSs and their parameters collected during scanning. Joining occurs before association. In selection, a STA joins the BSS it wishes to associate with, matches its local parameters with the parameters received from the selected BSS. In current implementations of the 802.11 devices, the selection decision is based on the power level, also called Received Signal Strength Indication (RSSI). The STA simply selects the AP from which it has received the strongest signal during the scanning process.

2.6 The 802.11 Medium Access Control (MAC) Protocol

This section elaborates the 802.11 MAC protocol.

2.6.1 Protocol Functionalities

The MAC layer protocol maintains and manages communications between WLAN nodes (APs and STAs) by coordinating the access to the shared wireless channel. Basically, the protocol has the following functionalities:

- Accepting MAC Service Data Unit (MSDU) from upper layers and adding headers and tailers to create MAC Protocol Data Unit (MPDU).
- Fragmentation of MPDU into several frames to increase the probability of successfull delivery.
- Providing access control functions such as address coordination and frame check sequence generation and checking.
- Regulating the usage of the shared radio channel.
- Being transparent to different Physical Layer (PHY) technologies.
- Assuring equal access opportunities for all nodes sharing the wireless channel.
- Managing the battery of wireless devices.
- Maintaining acceptable security level.

The IEEE 802.11 MAC successfully adapts Ethernet-style protocol for the radio links. It uses a distributed Carrier Sense Multiple Access Scheme (CSMA) for controlling the access of the wireless channel. Unlike Ethernet, a wireless device can not transmit and listen at the same time to detect collisions. Therefore, the 802.11 utilizes a collision avoidance (CSMA/CA) rather than a collision detection (CSMA/CD) algorithm. Each node employs the same algorithm to gain access to the physical medium.

Ideally, the CSMA/CA works as follows: A node wishing to transmit a frame has first to sense the medium, and, if no activity is detected, the node waits a randomly selected additional period of time before it transmits if the medium is still free. If the receiving node receives the frame intact, it issues an Acknowledgment frame (ACK) to confirm the reception of the frame. The ACK frame completes the process if successfully received by the sender. The sender assumes a collision to have occurred if the ACK frame is not successfully received. The reason could be either the ACK was not correctly received or the frame was not received intact. In this case, the frame is transmitted again after deferring another random amount of time.

2.6.2 MAC Modes

The IEEE 802.11 MAC employs three coordination functions:

- **Distributed Coordination Function (DCF):** It is the mandatory and fundamental access scheme supports asynchronous frame passing. The mode is used in both IBSS and BSS architectures and enables wireless nodes to interact without a central controller. A node shall first check the medium and only transmits if the medium has been sensed to be free for some time period. The RTS/CTS protocol can be optionally used to reduce the probable collisions as will be explained in section 4.2.

- **Point Coordination Function (PCF):** An optional mode restricted to infrastructure BSS. It provides contention free services or priority based access. The mode aims to support time-bound delivery of data frames. The point coordinator resides in the AP and grants access to the shared channel by polling clients according a prioritized polling list during the contention free period. Then, the coordinator switches back to the normal DCF mode.

- **Hybrid Coordination Function (HCF):** A medium access protocol proposed to enhance the original DCF and PCF coordination functions. It is standardized in IEEE 802.11e. The enhancements intend to provide the quality necessary for delay sensitive services such as IP telephony and video streaming. The HCF consists of enhanced distributed channel access (EDCA) and HCF-controlled channel access (HCCA). The EDCA enhances the legacy DCF mechanism by introducing different priority levels for different traffic types. It uses four queues for background traffic, best effort traffic, video traffic and voice traffic with increasing priority. Low priority traffic will back-off whenever a higher priority queue has data. EDCA defines different medium access parameters (CW, Inter-Frame Spaces) for each traffic type to ensure that high priority traffic grabs the channel more. HCCA enhances PCF operation by distinguishing the traffic in a similar way as EDCA. STAs include their requests in data frames sent to APs. A scheduling policy running at an AP prioritizes STAs for polling based on the received requests. The IEEE 802.11e does not standardize the scheduler and left its implementation to vendors.

In this thesis we focus on the DCF mode since it is being used for channel access in most of todays' WLANs.

2.6.3 Carrier Sensing

Carrier Sensing is the technique used for checking the availability of the wireless medium. The 802.11 MAC defines two types of sensing: The physical carrier sensing and the virtual carrier sensing. If either process indicates a busy medium, the MAC refrains from sending and and informs higher layers. The physical layer provides the physical sensing function. Due to the hidden node problem (will be discussed in section 4.2), the physical sensing does not provide all necessary information. Therefore, a second type of sensing called Virtual Sensing has been used. The Virtual Sensing is attained using the Network Allocation Vector (NAV). The NAV is a local timer that indicates how long the medium will be reserved for transmission. A transmitting node provides the NAV value to other nodes in a duration field part of most 802.11 frames including the RTS/CTS frames. The NAV timer is set at receiving nodes using the provided NAV value. Receiving nodes start counting down from the NAV value to zero. They do not attempt transmission unless the NAV is zero.

2.6.4 Interframe Spacing

An Interframe Space is a fixed amount of time that is independent from the physical transmission rate. Like Ethernet, the 802.11 uses interframe spacing to coordinate medium access and create different priority levels for different frame types. The idea behind this is that a node does not need to wait long time to transmit a high priority frame after detecting an idle medium. The 802.11 specifies the following Interframe spacing periods:

- **SIFS:** A short period used with high priority frames like ACKs and RTS/CTS. A STA wishes to send an RTS frame, for example, waits a SIFS period after the sensing functions indicate an idle medium.
- **PIFS:** It is the period of time that must elapse before a node transmits a frame in the contention free mode.
- **DIFS:** It is the minimum period of time that must elapse before a node starts transmitting a data frame after sensing an idle medium. It is used for contention-based services.

2.6.5 Backoff with DCF

Once a node completes transmission of a frame, it waits a DIFS period. Then, it must wait a new period so called contention window or backoff window before attempting to transmit the next frame (See figure 2.8). The length of the backoff window is a randomly selected multiple integer of time slots. The random integer number is selected from a uniform distribution between 0 and contention window (CW). Hence, the random integers are equally likely to be selected. CW is set to a value called CWmin at the first transmission attempt and is doubled each time a transmission fails up to a value called CWmax. CW is reset to CWmin after a successful transmission. The value of CWmin is 32 and 16 for 802.11b and 802.11a respectively. The value of CWmax is 1024 in both.

Although the original contention window adjustment algorithm is found to be robust both in simulations and practical implementations, some enhancements have been proposed to this algorithm. Reference [3], for example, proposes to base the minimum contention window CWmin on the number of active STAs which is dynamically changing. The intuition behind this proposal is that a too small CWmin may considerably increase the collision rate in the network if the number of active STAs in high. Similarly, a too high CWmin may waste the wireless bandwidth if the number of active STAs is small. Other algorithms can be found in [4, 5].

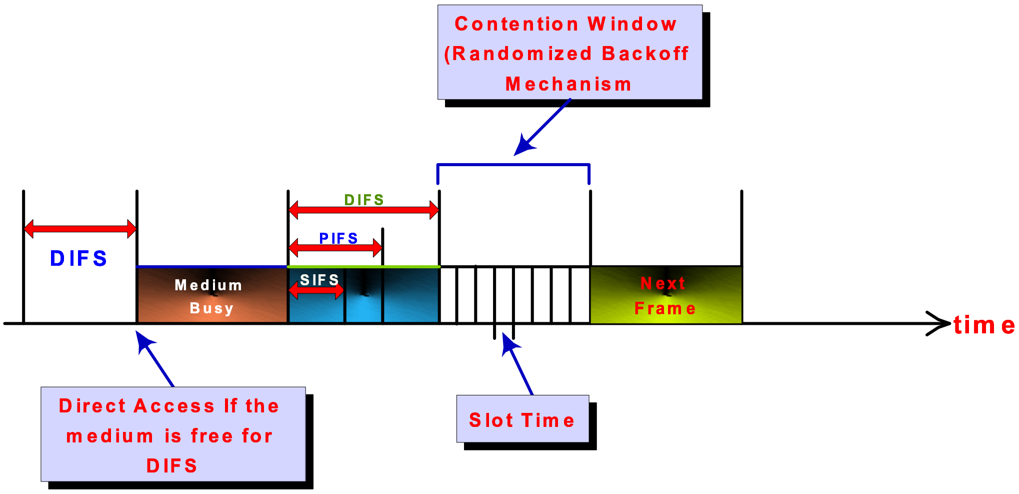

Contention Window (Randomized Backoff Mechanism
DIFS
PIFS
DIFS
Medium Busy
SIFS
Next Frame
time
Direct Access If the medium is free for DIFS
Slot Time

Figure 2.8: IEEE 802.11 Medium Access and Inter-Frame Spaces

2.7 Limitations of 802.11 MAC

The primary aim of the 802.11 MAC is to provide access functions to the wireless medium. Nevertheless, the basic concepts of 802.11 MAC described before present several limitations. Among these limitations are:

- The DCF mode does not meet the requirements of QoS applications within a single STA, e.g. Multimedia. Data traffic is treated equally in a first come first serve, best effort way. Typically, applications such as voice over IP and video conferencing can tolerate some losses, but require low delay and jitter.

- The PCF which was designed to support time-bounded applications, has some problems which make it unfavorable and not widely implemented. Among these problems, the polling scheme itself introduces overhead. Effective and efficient management of the polling list is complex. Additionally, the transmission time of a frame depends on the frame length and the employed physical rate which changes dynamically. Hence, the AP is not able to precisely predict the frame transmission time, preventing it to provide guaranteed delay and jitter performance [6].

- In the infrastructure mode, APs contend for the wireless channel like STAs without any priority, causing asymmetric throughput between downlink and uplink traffic [7].
- Throughput unfairness. This is known as the *Anomaly problem* [8]. Accordingly, a node transmitting at low rate occupies the medium for a long time, penalizing all other nodes contending for the medium. Chapter 5 elaborates more on this problem.
- The 802.11 was originally designed for non-overlapped BSSs configuration scenario. The increased deployment of wireless APs and the evolving number of wireless users, increases the load volume a WLAN has to handle. As load increases, interference increases, leading to more collisions and retransmissions, which in turn add to the load and consequently to still more collisions.
- Asymmetric Interaction. Due to the asymmetry in radio propagation, one transmitter may sense the signal of another transmitter, but not vice versa. This can starve the first transmitter [9]. Additionally, the hidden node problem (will be discussed in the next section) can completely shut-off some flows in the network, especially if some other flows are active but do not experience similar problem. The former is called asymmetric transmitter interaction while the latter is called asymmetric receiver interaction.

A plethora of ideas have been proposed within industry, academia and standardizations bodies to alleviate the above limitations in the 802.11 MAC. Within the standardizations groups, the 802.11e was developed to support time-sensitive applications in a BSS. However, it does not address multi-AP deployments. Some other solutions try to improve the MAC performance through sophisticated back-off algorithms, but achieved limited success.

2.8 Some Enhancements of the basic IEEE 802.11 Standard

2.8.1 IEEE802.11h

The IEEE 802.11h standard aims at facilitating the deployment of 802.11a products in Europe. Most of European countries utilize part of the 5GHz band for radar and satellite communications. This prohibits the deployment of 802.11a devices. The 802.11h addresses this problem by introducing two additional mechanisms, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). The DFS mechanism selects the frequency channels avoiding active channels occupied by Radars and satellites which requires efficient sensing technology. On the other hand, the TPC mechanism ensures that 802.11h devices emit power levels according the European Regulations for the operation in the 5GHz band.

2.8.2 IEEE802.11k

Within IEEE802.11, the only measured value available to APs and STAs is the RSSI. This value is related to the power level measured during packet reception. RSSI is used internally in WLAN card to determine when the energy in the channel is below a certain threshold at which the WLAN card is clear to send. At this point, a packet can be sent. In order to better manage and utilize radio resources, the IEEE has formed a task group, referred to as 802.11k [11], for Radio Resource Measurements (RRM). The task group has defined a set of measurements and reports to be exchanged between STAs and their APs for WLAN management. The way in which those reports could be used for radio resource management has not been specified and left to vendors' implementations. In the 802.11k standard, a STA can do measurements and report the results to the AP or another STA upon request. A STA can request another STA to perform measurements on its behalf. The procedures that handle the exchange of reports have been defined in the standard. In most cases, APs request STAs to report measurement reports, but in some cases STAs might request some data from the APs. To acquire some measurements, a STA might need to switch to other channel(s) for some time period. This can result in service disruption during this period and consequently affect active applications. The set of supported reports include:

- **The Beacon Report:** The AP can request a STA(s) to monitor the RF environment and respond with a summarized information about the detected beacons from a BSS(s) that uses some channel(s) specified in the request. The response is standardized in a report called the beacon report. It includes information regarding the services that observed APs support as well as the connection qualities to those APs.

- **Frame Report:** This report is requested by APs. It includes information about all the frames a STA has received from other STAs during the measurement period. The information includes the average received power as well as the number of frames received from each address.

- **Channel Load Report:** The channel load report is built by STAs and requested by APs. It mainly includes the fraction of time a specified channel has been sensed to be busy during the measurement period.

- **Noise Histogram Report:** This report is requested by APs. It includes all non 802.11 energy received on the channel when CCA indicates that no 802.11 signal is present.

- **Hidden Station Report:** The hidden station report is generated by a STA and requested by APs. It includes the number of frames and the address of the hidden STA. The measuring STA tracks a hidden STA if it receives initial transmissions

(Not retransmissions) of frames that must be acknowledged but does not receive the corresponding acknowledgments (ACKs).

- **Medium Sensing Time Histogram Report:** This report is generated by STAs and provides the AP with a statistical distribution of the medium idle and busy duration during the measurement interval as observed by the STA.
- **STA Statistics report:** Through this report, a STA informs the AP about its connection quality and network performance during the measurement period.
- **Neighbor report:** This report is requested by STAs and might be used to optimize the aspects of roaming across WLAN cells. The report includes an ordered list of APs that the STAs may use as candidates for BSS roaming. APs can generate the neighbor report utilizing the information received in the beacon reports from all STAs. It enables the AP to collect load characteristics information from the neighboring BSSs.

2.8.3 IEEE802.11v

Currently, WLAN network control is limited to the APs. Network administrators have little control over the WLAN STAs. The IEEE 802.11v standard aims at providing efficient mechanisms that simplify WLAN deployment and management. The standard provides functionalities to control the STA's Management Information Base (MIB) over the air. The work on this standard began in 2005 and approved in 2008. Specifically, the Task Group wants to define the procedures to:

- Enable AP to automatically inform the STA which network it should connect to without the need to manually set the Service Set Identifier (SSID).
- Enable AP to control the STA's parameters like the operational channel and data rate.
- Allow an AP to request a STA to connect to another AP to facilitate efficient load balancing solutions.

2.8.4 IEEE802.11f

The IEEE802.11f, also known as Inter-AP Protocol (IAPP), has standardized a set of messages to be communicated over the Distribution System (DS) to support mobility among APs from different vendors ensuring transmission continuity. The purpose of these messages is to:

- Enable the new AP and the old AP to exchange STA context information such as security information that speeds up the re-authentication procedure of a STA on re-association.
- Cause layer 2 devices to update any forwarding information they may hold regarding the roaming STA so that frames destined for it are delivered to a point in the DS where the new AP can forward those frames to this STA.

2.8.5 IEEE802.11r

The IEEE 802.11r [12] intends to speed up the STAs roaming among APs. With the current implementation of WLAN devices, a mobile STA does not know if necessary QoS resources are available in a neighboring cell before joining the new cell (or BSS). Thus, a blind transition may lead to inadequate application performance. The idea behind the 802.11r standard is to use the current AP to which a STA is associated as a pipe to communicate all security and QoS information with candidate APs before making a transition. This enables a STA to minimize disruptions while switching channels. The IEEE 802.11r protocol is still under development.

There is a trade-off among the certainty of communication with an AP, the speed of a handoff and disruption of current communications. While a STA can minimize the disruption of it's data stream by staying on its current channel and communicating with other candidate APs via its AP, it can not determine anything regarding its ability of communication with other APs over the wireless channels they use. On the other hand, by changing the operational channel, a STA can be certain about the quality of communication with the candidate APs but insert some disruption to ongoing communications.

With the rapid increase of WLAN users and density APs to fullfill their capacity requirements, more frequent handoffs are expected. The capabilities provided by the 802.11r protocol will be very usefull for such environment. The protocol is expected to be a major milestone for millions of WLAN users that require video, voice and data service over the WLAN.

2.8.6 IEEE802.11n

The IEEE802.11n standard defines a new physical layer for increasing the throughput of WLANs by utilizing Multiple Input - Multiple Output (MIMO) technology. MIMO utilizes multiple antennas which allow multiple streams to be transmitted simultaneously over the same channel, multiplying the capacity of each channel. The 802.11n amended standard specifies methods of increasing the transmission speed of WLANs up to 600 Mbps which is more than 40 times faster than 802.11b and near 10 times faster than 802.11a or 802.11g. It is projected that 802.11n will also offer a better operating distance than current networks. The 802.11n is backward compatible with 802.11b/g. Although the standard still under development, some products based on pre-draft versions are now available in the market.

2.9 Summary

In this chapter, we give an overview of WLAN technology emphasizing the aspects which are relevant to the work in this thesis. Particularly, the operation modes of WLANs are discussed. Then, we identify the limitations of current 802.11 MAC protocol and elaborate the notion of interference and its types. Finally, the chapter provides a brief overview of 802.11 standards.

Chapter 3

System Description

3.1 Introduction

As pointed out earlier, the demand for WLANs has grown immensely nearly everywhere-from the home to the office to public hotspots in restaurants, cafes, and universities. Due to the numerous advantages they have, infrastructure based 802.11 WLANs are dominating. Their central architecture makes the management of the wireless resources (e.g. time, power, and channels) according to the user needs or fairness rules and the extension of the WLAN coverage easier. Therefore, the infrastructure-based 802.11 WLAN is considered in this work. A special focus is given to the challenges this network faces in order to improve its performance.

3.2 Assumed Scenario

In this thesis, we consider an ESS infrastructure-based 802.11 WLAN (see figure 3.1) deployed in a large area like a campus, a departure hall in an airport or a conference room as basic setting. Due to a potentially high number of users, multi 802.11 APs are deployed within this area. APs are assumed to operate on non-overlapping channels. Due to the lack of such non-interfered channels the 802.11 standard supports, some APs are assigned the same channel. APs provide communication services to the users that reside within their coverage area, which is as shown in figure 3.1 assumed to be irregular due to fading. The coverage area of APs may overlap. Neither the location of an AP nor its operational channel is known to the other APs. Users appear in the coverage area at different points in time and at different places. Users have nomadic mobility degree, i.e., they start their devices and stay at constant positions during their active sessions. At any time instant, a user is associated to a single AP.

3.2.1 System Entities

Access Point (AP):

It is the central controller of a BSS connected to the infrastructure network. An AP provides communication services to an associated user by delivering his/her packets to other users within the same BSS or to the infrastructure network. APs also deliver the

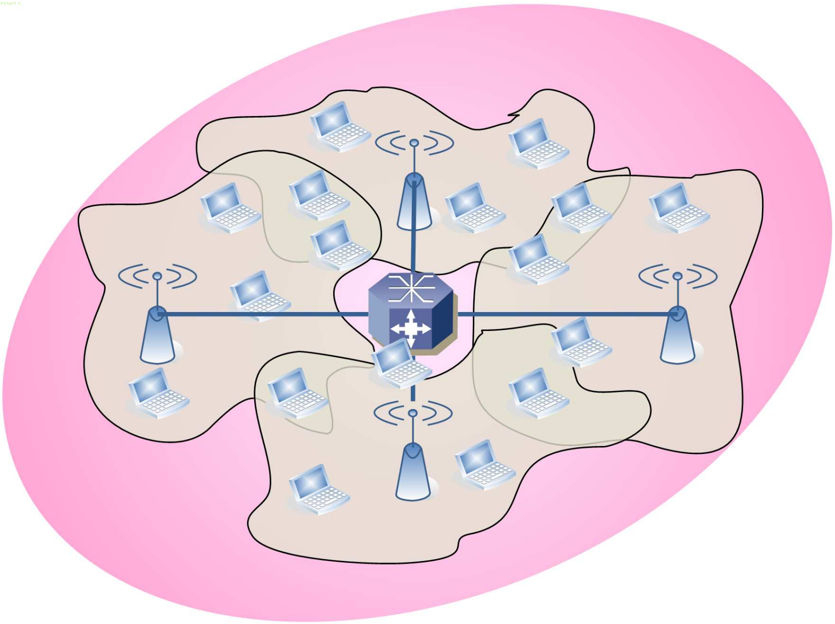


Figure 3.1: Network Model

traffic coming from the infrastructure network to the destined users. An AP is assumed here to be compliant to the IEEE 802.11k and to have an omni-directional antenna which contributes constant loss or gain when communicating with every user within its BSS.

Station (STA):

A STA is assumed here to be some stationary computer with a wireless network interface card (NIC) compliant to IEEE 802.11k standard. Every STA has to associate itself with an AP in order to be allowed to communicate with other STAs and/or the infrastructure network. Typically, a user runs applications (assumed to be non-real time data applications) which trigger or respond to communications with other WLAN users or the infrastructure network. All STA's communications is relayed through one AP to which it is attached.

Basic Service Set (BSS):

It is the AP and the set of STAs it accommodates. A pair of STAs may not hear each other despite associating to the same AP.

Extended Service Set (ESS):

A set of BSSs which APs are coupled via the distribution system (DS).

3.3 Problem Formulation

In current 802.11 WLANs, channel access is governed by the DCF access mode. Despite that this mechanism is robust and efficient within a single BSS, it fails to provide acceptable service for many WLAN users in multi-BSS deployments when the traffic load gets high. The main reason is the interference among the BSSs.It is known that the ability of a receiver to correctly decode a transmitted packet highly depends on the amount of total interference power measured at the receiver from concurrent transmitter(s). Therefore, interference may cause packet corruptions, leading to errors which will cause discards and retransmissions. Retransmissions are overhead that add to the load and consequently might result in more collisions. Generally, collisions among nodes (STAs and APs) influence and degrade the performance of all nodes. This is because the average time required to transmit a frame successfully by any node increases gradually as the number of collisions in the BSS increases. Additionally, interference may prevent some nodes from accessing the channel despite their transmissions do not interfere.

Absolute elimination of interference may not be possible. Hence, the fundamental question is: ***how can we reduce its impact and consequently improve the QoS users experience in the WLAN.***

3.4 Proposed Solution Approach

In this thesis, we propose the following approach (illustrated in figure 3.2) for interference mitigation. We first try to reduce interference at the selection phase by developing an interference-aware STA-AP selection policy. The new AP selection policy considers both intra-BSS and inter-BSS interference. Intra-BSS interference is resulted among nodes that access the channel within the same BSS, while inter-BSS interference is caused by nodes that belong to neighboring BSSs configured on same channel. Since more than one channel is used in the network and BSSs may experience different interference conditions, a careful selection of the AP is expected to improve the performance of WLAN users. Additionally, the proposed AP selection policy reduces the anomaly problem which arises due to heterogeneous physical transmission rates used by wireless nodes. Therefore, we improve the AP selection via some guidance information about BSS status. APs include this information in beacon and probe response frames.

After selecting their APs and while the network is operating, WLAN nodes monitor the operational conditions. If the QoS is found to be degraded, the WLAN uses diagnostic and interference estimation methods to determine the cause of performance degradation. If the interference is found to be the cause, the WLAN checks wether the situation can be improved by tuning the RTS/CTS as first option. Indeed, this depends on the network topology and wether this interference is due to hidden nodes. If the RTS/CTS is insufficient or does not help, then the system considers, as second option, a change of the channel access scheme from the CSMA/CA to a time slotted access scheme. The change takes place if it is found to be useful and feasible.

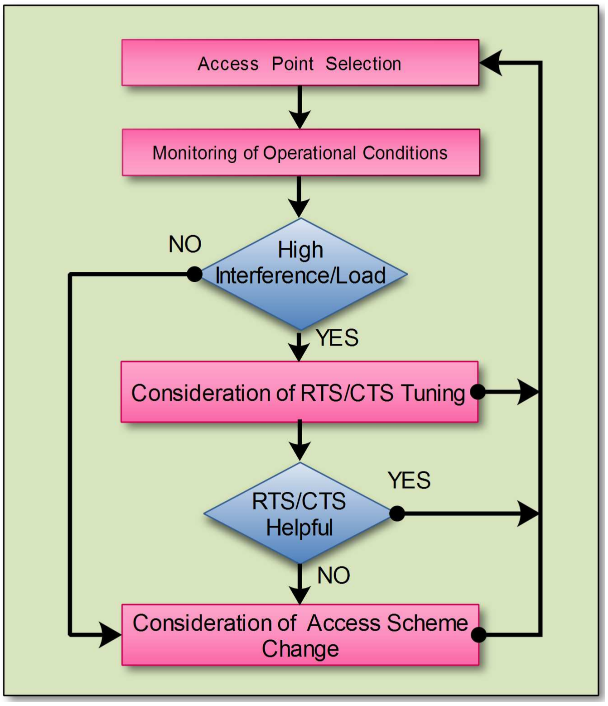

Access Point Selection
Monitoring of Operational Conditions
NO
High Interference/Load
YES
Consideration of RTS/CTS Tuning
YES
RTS/CTS Helpful
NO
Consideration of Access Scheme Change

Figure 3.2: The proposed System

The proposed solution is comprised of:

- Methods for diagnosing performance degradation and interference estimation.(Chapter 4)
- An Interference-Aware STA-AP selection policy.(Chapter 5)
- Criteria for tuning RTS/CTS.(Chapter 6)
- A hybrid access scheme.(Chapters 7 and 8)

3.5 AP Deployment

We consider two types of AP deployments in evaluation experiments. We call the first type the *planned deployment*, wherein APs are equally spaced as shown in figure 3.3. This type of deployment can be seen in scenarios, where APs are owned by same organization like university campuses, airports, offices, hotels, etc. It is assumed here that APs are able to communicate through the distribution system. In the last part of this work, we consider a second type of deployment referred to as the *chaotic deployment*, whereby channels and distances among APs are random. This type of deployment can be seen in residential areas, where APs are owned by different providers in the same region. It is also assumed here that APs are able to communicate via the infrastructure network, though, belonging to different administrative parties. Figure 3.4 is an example

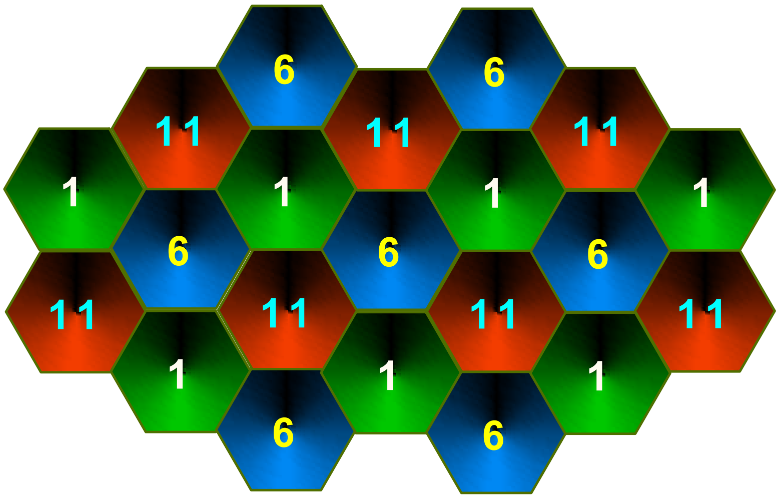


Figure 3.3: A Planned deployment of a WLAN

network in San Diego (USA). This data was obtained from the WifiMaps.com website which provides a GIS visualization tool, to map wardriving results that cover a few densely populated residential areas in USA. For each AP, the database provides the AP's geographic coordinates, its wireless network ID (ESSID), channel employed, and the MAC address.

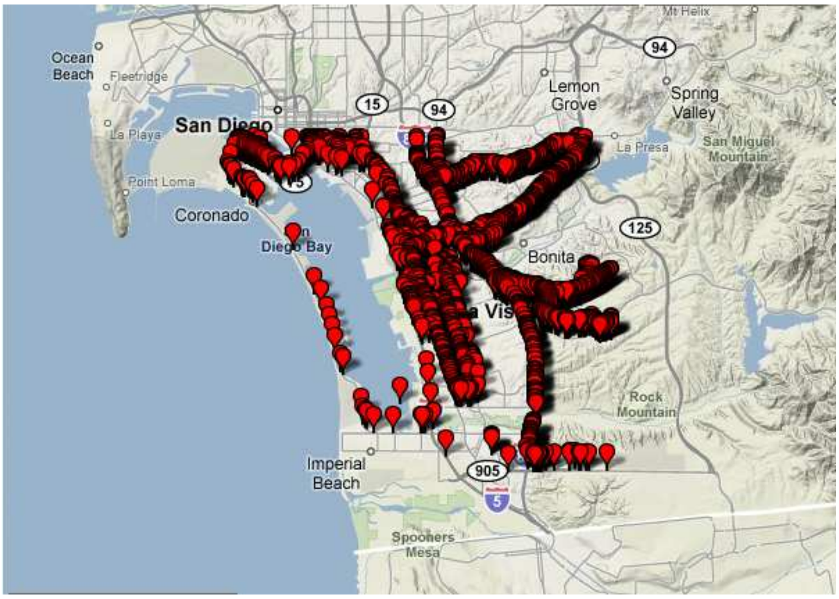


Figure 3.4: A Chaotic deployment of a WLAN

3.6 Load Model

Mainly, two types of load models will be considered in this thesis:

- A constant bit rate (CBR) traffic load. Each STA is assumed to have a CBR traffic from an infinite source.
- A realistic traffic load obtained from real WLAN traces.

3.7 System Metrics

In the considered infrastructure WLAN with STAs carrying non-real time traffic, the interference will influence the amount of successful data packets the network delivers during a period of time and the fairness level among the users the network accommodates. Interference mitigation is expected to improve these two quantities. Therefore, the evaluation of the ideas proposed throughout this thesis will be mainly based on the following:

- Goodput: This is the first metric of interest. It is the amount of data bits transferred successfully in the network during a second time interval.
- Fairness among STAs. The well-known Jain fairness index [10] will be used. This metric is computed as follows:

$$FairnessIndex(FI) = \frac{1}{M}\frac{\left(\sum_{m=1}^{M} G_m\right)^2}{\sum_{m=1}^{M} G_m^2} \tag{3.1}$$

  where G_m is the goodput of STA m and M is the total number of STAs. Note that the fairness index approaches 1 as the STAs achieve equal goodput.

As evaluation strategy, the proposed ideas throughout this thesis will be decoupled and compared against relevant algorithms/schemes currently implemented in WLANs as well as some other relevant ones in the literature.

3.8 Summary

This chapter describes the system under consideration in this thesis. It first presents the assumed WLAN scenario and identifies the system entities. Relevant terms are also defined. The challenging problem under study is then formulated. Finally, we discuss the traffic model as well as evaluation metrics which will be used throughout this work.

Chapter 4

Interference Measurement

4.1 Introduction

Interference can be generally defined as the overlapping of signals in the same frequency band. It is an important factor that determines wether a collision or a correct reception occurs. In wireless communication, the signal attenuates with distance as it propagates from the transmitter over the channel. The signal also undergoes other different attenuations while travelling in the wireless environment (e.g. passing through different types of obstacles). At the receiver side, the receiver attempts to decode the attenuated signal. The ability of a receiver to correctly receive the transmitted signal depends on the sum of the noise and the total interfering power measured at the receiver (during the reception of the desired signal) relative to the power level of the desired signal being received. The Signal to Interference and Noise Ratio (SINR) is a commonly used value that determines whether a wireless node can correctly decode a transmitted signal in presence of noise and some other concurrent interfering ones. The transmission can be successfully received only if this ratio is sufficiently high.

Estimating interference conditions at a receiving node and determining interference relations among different wireless nodes is a challenging problem. Interference relations provide the information of which wireless links do interfere if activated concurrently. This information will be needed later for the determination of which wireless links can be allowed to access the channel concurrently in a time slot, if the WLAN changes to the time slotted modus as will be explained in chapter 7. Estimate of interference conditions at a WLAN node characterizes the impact of interference on the ability of this node to correctly receive packets. This will be needed for the diagnosis of the cause of performance degradation. This chapter proposes two methods to achieve the aforementioned goals. Diagnosis of performance degradation will be accomplished through a method for discriminating the cause of packet loss at a receiver side, while the determination of interference relations will be accomplished through passive observation of the wireless channel.

4.2 Interference in 802.11 WLANs

Actually, the coverage area of a WLAN node highly depends on the objects, structures in the propagation environment, the used modulation type, and the power level a node employs. Moreover, the coverage varies in time even when nodes are fixed depending on the movements in the area.

Two different ranges are of significant importance for the coverage of a wireless node:

- **Communication Range:** Is the range within which a receiver is able to receive and decode a transmitted packet with small error rates.
- **Sensing Range (CCA Range):** Is the range within which a receiver's CCA mechanism is able to detect a busy channel.

Generally, interference in WLANs is grouped into two types:

- **802.11 Interference:** Also called self-interference, it is generated by 802.11 WLAN sources like APs and WLAN adapters.
- **Non-802.11 Interference:** This type of interference is generated by nearby non-802.11 devices that operate in the same frequency band allocated to 802.11 WLANs.

In this work, we only consider the 802.11 interference (self-interference). In infrastructure-based 802.11 WLANs, self-interference can be further classified in two categories:

- Intra-BSS or intra-cell interference.
- Inter-BSS or inter-cell interference.

Intra-BSS interference is resulted from the simultaneous access of the wireless channel by nodes that belong to the same BSS. A node wishes to send a data frame and was not able to detect or sense an ongoing transmission in the BSS will interfere/collide with the ongoing transmission. Both nodes are called hidden nodes and the problem is referred to as the hidden node problem.

Hidden nodes lie outside the CCA area of each other. Current WLANs rely on the MAC protocol to resolve this type of interference via the optional Request to Send/-Clear to Send (RTS/CTS) protocol. Figure 4.1 illustrates this protocols. The RTS and CTS frames are small frames exchanged prior to transmission of data frames. To illustrate how these handshake packets mitigate the hidden node problem, let us consider uplink transmissions in an infrastructure WLANs. A sending STA transmits an RTS frame to the AP. The RTS reserves the medium and silences any node that has received it. The AP replies with a CTS frame. As all BSS STAs hear the AP, they refrain from sending for a time period included in the duration field of the CTS frame. Theoretically, this allows the sending node to transmit and receive a frame without any chance of collision. The main drawback of the RTS/CTS protocol is the additional overhead

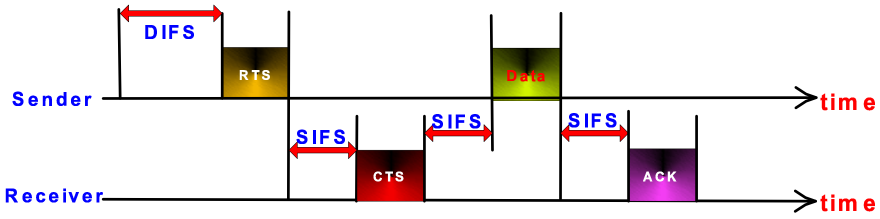


Figure 4.1: IEEE 802.11 Hidden-Terminal Provision for Collision Free Access

to the WLAN due to the temporary reservation of the wireless channel. Therefore, the 802.11 standard recommends it to be used just for large packets which consume large bandwidth if retransmitted.

Nowadays, WLAN administrators deploy many APs to better cover a given area and improve users connectivity with APs. The closer the user to an AP, the larger the physical transmission rate the WLAN adapter is expected to employ. Due to the lack of non-interfered channels the 802.11 standard supports, this kind of dense deployment will likely result in the *Inter-BSS interference* unless the network is carefully planned and tuned. *Inter-BSS interference is a phenomenon where signals transmitted from one BSS spread to a neighboring BSS that operate over the same channel. Such a coincident in time signal may corrupt the frame under reception if its strength is comparable relative to the signal strength of the frame being received.* Similarly, signals from neighboring BSSs on the same channel can prevent local nodes from transmitting their frames, even if intended receivers might not interfere. This is known as *Exposed Node Problem.* This problem stems from the fact that the CSMA/CA provides information about potential collisions at the transmitter side and not at the receiver.

In fact, the real impact of interference depends both on the interference signal level and the frequency of the interference event. The later is strongly dependent on the traffic profile. In this work, two complementary approaches will be developed for the estimation of interference conditions as well as determination of interfering links, **Packet Loss Discrimination and Passive Observation of Interference through Packet Decoding**. The approaches are measurement-based, where the measurements are to be conducted while the network is operating. This trend is in line with 802.11 standards which develop mechanisms to facilitate measurements during network operation (e.g. the 802.11k standard).

While we confine our attention to the Received Channel Power Indicator (RCPI), recently standardized in 802.11k, other signal level indicators such as RSSI can be used if the RCPI measure is not supported. As an 802.11 standard feature, the RSSI value is defined in the standard as a measure of the power level observed at the receiver antenna, measured during the PCLP (Physical Layer Convergence Protocol) of an arriving packet [14]. Note that the specific details of implementation for acquiring this value (e.g. # of samples, a method to compute a final value from numerous samples) is not explicitly provided by the standard and left to manufactureres. In contrast, the RCPI value is measured over the entire frame at the antenna connector used to receive that frame. This is illustrated in figure 4.2. Hence, the RCPI value seems to be a better metric to represent the signal power level of a received packet. Again, the standard does not explicitly specify the details for acquiring the RCPI value and leaves that to manufacturers.

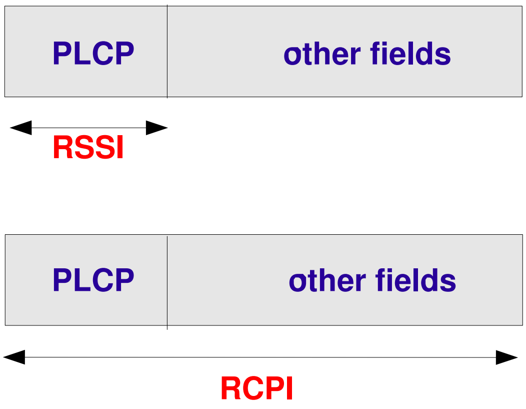


Figure 4.2: RSSI and RCPI Measurement

4.3 Packet Loss Discrimination

4.3.1 Introduction

Packet loss in 802.11 WLANs can occur either due to collision or a weak signal that arrives at the receiver antenna. A challenging issue is the determination of packet loss cause once it occurs, which is a key for improving the performance of 802.11 WLANs.

With current 802.11 products, the only feedback to the sender is the ACK packet, which indicates successful packet reception. If ACKs do not arrive, the sender does not know the reason. In this case: backoff, rate selection, power, or channel selection are candidate actions to be taken. Obviously, only based on lack of ACKs, it is quite hard for the sender to decide on the right action to be executed. Different strategies have been proposed for reaction to the absence of ACKs. In most implementations, the cause of failure is firstly attributed to collisions, thereby the contention window is doubled and the sender enters the backoff state. Depending on the used strategy, after some number of unsuccessful transmission trials, a failure is then attributed to weak signals, triggering the rate selection algorithm. Clearly, if a frame is dropped due to a weak signal, doubling the contention window will waste the airtime, leading to serious performance degradation. Also, when collisions occur often, the rate selection will unnecessarily reduce the transmission rate.

This blind reaction can be overcome if communicating nodes are able to diagnose the cause of failure and invoke the proper adaptation algorithm. In this case, if insufficiently strong signal arrives at the receiver, the proper action would be a tune of transmit power level, transmission rate, or perhaps invoke of handoff procedure. On the other hand, if packets are not ACKed due to collisions, it would be better for the sender to tune backoff, the operational channel, or even negotiate a change of the access scheme in case of high interference.

As a result of the above discussion, a method to diagnose the cause of packet losses is a key for effective WLAN management algorithms. In this section, a new packet loss discrimination method for estimating interference conditions in multi-BSS WLANs will be developed. It will be used for interference recognition at receiving nodes.

4.3.2 Review of Existing Approaches

Witehouse et. al. [15] have shown that if two frames arrive at the receiver of a node with certain timing and power levels characteristics (the second frame arrives after the preamble and header of the first frame and the power level of the second frame is significantly higher than that of the first frame), then it is possible for the node to conclude that a collision had definitely occurred. The receiver synchronizes and receives the new frame. The authors propose a mechanism by which a node detects the new frame. A node achieves this by observing a significant jump of received power and searching for headers while decoding the first frame. The proposed approach was implemented for sensor networks, on a platform that allows at any time low-level access to timing and power parameters. This is not the case with 802.11 implementations, which provides power level indication (RSSI) at the MAC for each frame. The algorithm may not detect all collisions since a collision is assumed only if significant power levels between the first frame and a new coming one is observed.

Another attempt was done by Yun and Seo [16]. They proposed a mechanism for collision detection in 802.11 links based on RF energy measurements. The authors assume that a WLAN adapter (at the receiver) can measure the duration of RF energy pulse (the time span a receiver detects energy above the sensitivity threshold) on a channel during packet reception. The physical layer reports the measurement result to the MAC layer. As the packet duration is known to the sender (from the Length and Rate information), the sender deduces a collision to have occurred if the duration of energy measured at the receiver and sent back to the sender is larger than the packet duration. Obviously, this approach only works with some configurations of packet length and their relative phase shift. The approach introduces overhead due to the backward transmission of measurements from receivers to senders. Moreover, experimental evaluations conducted in [17] concluded that the efficiency of the proposed mechanism might be poor in practice.

Pang et. al. [18] have modified the 802.11 MAC and used explicit negative acknowledgment (NAK) for the purpose of differentiating frame losses due to intra-BSS collisions and weak signal. The authors assume that if all STAs in a WLAN BSS are close enough and can hear one another, a collision occurs only when more than one STA sends data frame in the same time slot. In this case, collision on initial bits may happen and both the header and body will be corrupted (i.e. the receiver can neither receive the header nor the payload of the collided packet). Based on this observation, the authors propose that a receiver sends back a NAK if the MAC header is correctly received but the MAC body of the frame is wrong. Upon receiving the NAK, the sender concludes that a link error has occurred. If neither ACK nor NAK arrives at the sender, collision is assumed to have occurred. It is clear that the algorithm fails if a sent NAK frame does not arrive at the sender for some reason or if STAs are not within the range of each other.

In [19, 20], collision detection has been used to improve rate adaptation algorithms. The authors assume that RTS/CTS is always signaled before data packets. Assuming negligible transmission error probability of an RTS frames, a loss after the exchange of RTS/CTS is attributed to channel errors since RTS/CTS reserve the medium for the next packet. In addition to the overhead imposed by the exchange of RTS/CTS, this differentiation mechanism may fail in the presence of hidden nodes across multiple Basic Service Sets (BSSs).

Recently, Sharvan et. al. [17] proposed a new measurement-based approach for discriminating packet collisions and losses due to bad channel conditions in 802.11 systems. Their approach is based on explicit sending back of complete frames in error along with the Received Signal Strength Indicator (RSSI) values to the sender. The authors rely on their observations indicated that data bits which follow the preamble is seldom found in error, due to receiver synchronization using the physical layer preamble. This includes source and destination MAC addresses. In the 802.11 standard, the RSSI is defined as a measure of the power level observed at the receiver antenna, measured during the PCLP (Physical Layer Convergence Protocol) of an arriving packet [14]. The intuition behind using RSSI is experimental observations that the RSSI of packets suffering from signal attenuations is usually lower than that of packets suffering from collisions. It has been observed that the RSSI of 98% of packets received in error was below -73dBm. Similarly, the authors observed that 98% of packets in error due to fading have a BER of 12% or less, while only 24% of packets in error due to collision have BERs of 12% or less. This means that about 75% of packets corrupted due to collisions have BER greater than 12%. The sender then uses the RSSI value (sent back from the receiver) and a BER value (computed at the sender as the ratio of incorrect bits in the packet sent back from the receiver) for the discrimination of packet loss. It employs some empirical rules to identify the cause of error assuming that the receiver was able at least to decode the MAC header of the frame in error. Particularly, if any metric (RSSI, or computed BER) indicates a collision, the algorithm outputs collision as result. The main drawback of this approach is that the RSSI value can not capture collisions unless the PLCPs of colliding packets overlap. This is due to the fact that the RSSI is measured during the reception of PLCP. Another drawback is the dependency of the decision rule on a fixed cut-off RSSI value (-73dBm), where the used value may not apply to any deployment scenario in general. The associated overhead with this approach is rather high due to packets relay-back between senders and receivers.

Another recent algorithm has been proposed by Malone et al. in [21]. The proposed algorithm differentiates between two types of packet losses. The first is losses due to intra-BSS collisions and the second is losses due to weak signals or hidden nodes. The algorithm is executed at the sender side utilizing MAC sensing statistics of busy and idle periods. The collision probability is estimated as the proportion of busy slots due to transmissions by other STAs(i.e # of Busy Slots/(# of Idle Slots + # of Busy Slots)). A busy slot is defined as the event that a node has detected the medium as busy due to transmissions of one or more other nodes, and has suspended its backoff until NAV, DIFS/EIFS indicate that the backoff can resume. An idle slot is defined as the event that a node has seen the medium as idle and, if backoff is in progress, has decremented its backoff counter. The probability of success is computed as the ratio of successful transmits to attempted transmits. Knowing the probability of successful transmission and the probability of collisions, the authors compute the probability of channel error. The authors extend their work in [22] to discriminate between losses due to noise/weak signal and hidden node (interference). They do that by sending a packet as a sequence of fragments. The authors assume that the first fragment is the only one subject to collisions while subsequent fragments are subject to noise. One concern about this discrimination method is that not all 802.11 packets are normally fragmented. Also, in a wireless environment, sensing results at the sender side is usually not enough to infer collisions at the receiver. Moreover, excessive fragmentation introduces additional overhead.

4.3.3 Receiver-Oriented Packet Loss Discrimination

In 802.11 there are two types of collisions. The first type occurs when a new packet arrives while the radio of the receiving node is already synchronized and receiving a packet (may be during header reception). If the stronger packet arrives while the receiver radio is synchronized and receiving a packet of weaker signal, the new packet will corrupt the tail of the first packet, thereby leading to corruption of both packets. However, if the first packet is strong enough relative to the new packet arrived (Capture works), the first (stronger) packet will be correctly received, i.e. the interfering new packet will not impact the first stronger packet. We call this interference *tolerated interference.*

In [17], the authors have experimentally observed a relation between the RSSI value of received packets and interference. Particularly, it has been shown that the RSSI value at a receiver increases when an interfering node is active. However, from the definition of RSSI, it turns out that an interfering signal contributes to the RSSI of a packet only if it arrives during the reception of the PLCP of this packet, i.e the RSSI value is the sum of the desired signal and interfering signal(s) only if interfering signal(s) arrive during the reception of the PLCP as illustrated in figure 4.3. Although the two packets in figure 4.3(a) overlap, the signal power of the new packet will not influence the RSSI of frame F1. This occurs when the transmitting nodes of the two frames are hidden from each other. In contrast, frame F2 in figure 4.3(b) will increase the RSSI of frame F1 as it arrives during the reception of PLCP of frame F1.

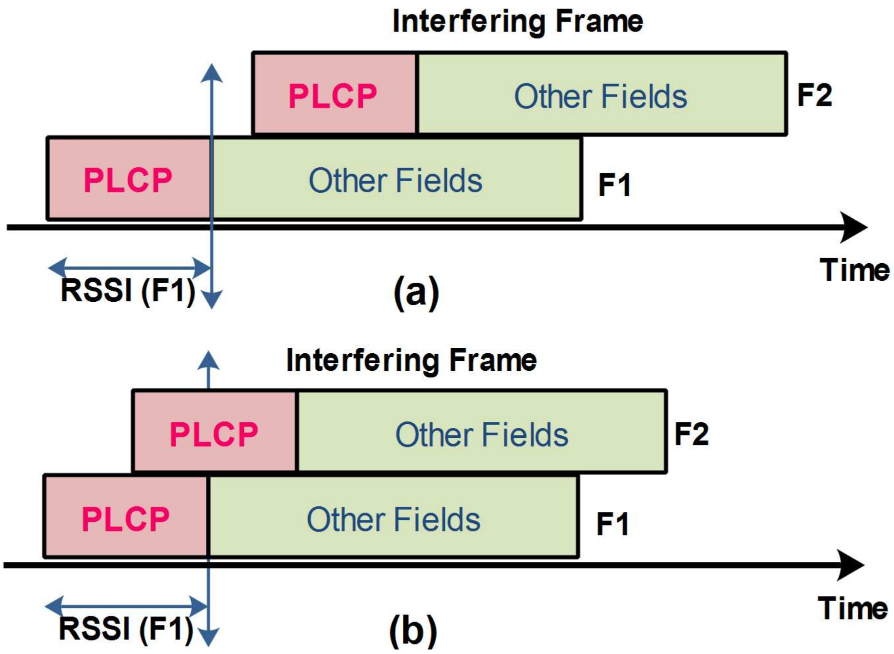


Figure 4.3: Impact of Interfering Signal on RSSI

As the RSSI value does not always provide complete information about potential interfering signal(s) during a reception of a packet, we would like to follow the above observations while suggesting the usage of the Received Channel Power Indicator (RCPI) [23] as a measure of the channel power (signal, noise, and interference) of a received IEEE 802.11 frame. The RCPI shall be measured over the entire frame on the channel and at the antenna connector used to receive that frame [23]. We assume hereafter that the RCPI value is an average power level measured over the entire frame.

In further considerations, we assume that the receiver is able to correctly decode the MAC header of a packet that arrives first. Observations in [17] indicated that this assumption is reasonable due to receiver synchronization using the physical layer preamble. Further we assume that the RCPI values of both correct and corrupted packets are available at the MAC layer.

Generally, the received instantaneous power of packet k at node i, $Px_{ik}(t)$ can be expressed as:

$$Px_{ik}(t) = S_{ik}(t) + I_{ik}(t) + n_{ik}(t) \tag{4.1}$$

where $S_{ik}(t)$ is the instantaneous received power of the actual/desired signal of packet k at node i, $I_{ik}(t)$ is the instantaneous power received from one or more interferers at node i during the reception of packet k, and $n_{ik}(t)$ is the instantaneous thermal noise power.

Assuming that $n_{ik}(t)$ is constant and an $RCPI_{ik}$ value is obtained by sampling and averaging the received instantaneous power $Px_{ik}(t)$ at node i over the whole length of packet k, then we have:

$$RCPI_{ik} = S_{ik} + I_{ik} + n_{ik} \tag{4.2}$$

where S_{ik}, I_{ik} , and n_{ik} are the contributions of the desired signal, interference signals, and the thermal noise to the $RCPI_{ik}$ value, respectively.

The probability that node i receives packet k incorrectly is then given as:

$$P_{ik}[Failure] = P\left[\frac{S_{ik}}{I_{ik} + n_{ik}} < \delta\right] \tag{4.3}$$

where δ is the minimum signal to interference and noise ratio (SINR) for a correct reception of a packet.

From equation 4.3, it is clear that:

- It is possible for the receiver of node i to correctly decode a packet k even in the presence of some interference I_{ik} (Capture effect).
- If I_{ik} exceeds some threshold I_{th}, the received packet will contain errors. **An increase in I_{ik} will result in an increase in the corresponding $RCPI_{ik}$, which value depends on the duration and strength of I_{ik}.**
- **If I_{ik} is below or equal I_{th}, then packet failure has to be attributed to a decrease in S_{ik} (i.e weak signal).**

A receiver discriminates between packet losses as follows:

Algorithm 1 Receiver-Oriented Loss Discrimination Algorithm

```
$Q_i(x)$ = The x % quantile RCPI value of a training sample of correctly received packets at node $i$.
$RCPI_{ik}$ = RCPI of packet $k$ received by node $i$.
for every packet $k$ received in error
        if ($RCPI_{ik} > Q_i(x)$)
                Cause = Collision.
        else
                Cause = Channel error.
```

Due the fact that a packet may still be captured and successfuly received in the presence of some interference (i.e tolerated interference), the algorithm uses a quantile RCPI value $Q_i(x)$ of correctly received packets as a threshold with which the $RCPI_{ik}$ of a corrupted received packet is compared for the sake of discrimination. Specifically, $Q_i(x)$ is the RCPI value below which fall $x\%$ of RCPI values of correctly received packets at node i. In our evaluations, $Q_i(x) = 70\%$ was found to achieve a good estimation accuracy. Note that in the case of multiple senders to a single receiver like STAs to an AP, the AP has to have a quantile value for each sender.

Obviously, using these statistics (power of correct and corrupted packets), it is also possible to estimate the amount of untolerated interference at the receiver of node i, i.e. the amount of interference from neighboring nodes that really causes packet loss at node i. This can be estimated over a period of time T as follows:

$$\hat{I}_i = RCPIFailed_i - Q_i(x) \tag{4.4}$$

where $RCPIFailed_i$ is the average RCPI value of incorrectly received packets due to interference at node i during T. *The main advantage of this estimation is that it can be performed on-the-fly. Nodes are not required to cease their transmitters and sense the medium for potential interferers.*

4.3.4 Performance Evaluation of the proposed Loss Discrimination Approach

In this section, we assess the performance of the proposed approach for diagnosing the cause of packet loss in 802.11 WLANs through detailed simulation experiments. The experiments have been conducted using the NCTUns simulation package [24]. The MAC protocol of NCTUns is ported from NS-2 network simulator [25]; which indeed implements the complete IEEE 802.11 standard MAC protocol to model accurately the contention of users for the wireless channel.

Evaluation Metric

For the evaluation of the proposed algorithm, we look at the estimated collisions and the actual/true collisions. Specifically, during each second of the simulation time, we sum the number of collisions as estimated by the packet loss discrimination algorithm proposed in this chapter and the total number of actual collisions (number of times the receive module of the simulator at the receiving node decides a collision to have occurred and drops the packet under reception as a result of this decision). The two values will be compared.

In order to incorporate different wireless conditions and assess the ability of the algorithm to capture the dynamical changes: First, we use different traffic patterns. Second, we increase the collision rate in the network by tuning the maximum contention window CW_{max}. Third, we increase the BER by randomly decreasing the SNR (per packet). The performance of proposed algorithm will be compared with recently proposed and relevant algorithms by Rayanchu et. al [17] and Malone et.al [21], which also have been implemented in the simulation tools.

Simulation Setup

The scenario is comprised of 10 BSSs and 100 STAs. The APs are deployed and configured over the same channel. The STAs are randomly distributed in the coverage area of the APs. APs are connected to a server (via an 802.3 switch) through cables of 100 Mbit/s bandwidth. The latency for packets between APs and the server was set to $10\mu s$. APs and STAs implement the 802.11b technology and use the DCF MAC protocol.

Depending on the distance between AP and STA, the wireless channel is attenuated more ore less severely. However, we assume that radio signals are not only attenuated by path loss, but are also affected by fading due to multi-path propagation. In order to accurately model these effects, a path loss component as well as a Rayleigh-distributed fading component is considered. For the path loss, a two-ray ground reflection model has been used with the received power P_{rx} given as:

$$P_{rx} = \frac{P_{tx} G_{tx} G_{rx} h_{tx} h_{rx}}{d^2} \tag{4.5}$$

where P_{tx} is the transmit power (in mW), G_{tx},G_{rx} denote the transmitter and receiver antenna gains respectively, h_{tx} and h_{rx} are the antenna heights of transmitter and receiver, and d is the distance between them. A Rayleigh fading model provided by the NCTUns simulator is used. It takes as parameters the received power P_{rx} and a fading variance set to its default value of 10dB. The received power level of a packet (with respect to both path loss and fading attenuations) is computed at the beginning of the packet and assumed to be constant over the whole packet length. It is passed to an error module provided by the simulator along with packet length and modulation type. This module determines whether a received packet is correct or corrupted due to fading and path loss attenuation.

The aggregated combined power level (our RCPI) of two packets if one arrives while the other is being received is computed at the receiver as follows:

$$P_{total} = \frac{P_f T_f + P_n T_{overlap}}{T_f} \tag{4.6}$$

where P_f is the received power level of the first packet, T_f is the duration time of the first packet, P_n is the received power level of the new incoming packet and $T_{overlap}$ is the time it overlaps with the first packet.

Wireless nodes choose their transmission rates depending on the perceived, average SNR (i.e. without the fading impact) and try to assure a bit error rate (BER) less than 10^{-5}. This rate remains constant during the simulation, i.e, no rate adaptation mechanism has been implemented. For IEEE 802.11b the possible rates actually are 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s and 11 Mbit/s. Table 4.1 lists the values of the parameters as used in simulations.

Packet capturing is modeled in the simulator as follows: While simulating packet reception time (a function of physical rate, packet size), if a new packet arrives and the power level of the first packet is greater than the power level of the new packet by at least the Capture Threshold, then the first packet is assumed to be received and the new packet is ignored.

Table 4.1: Constant Parameters

Parameter	**Value**	**Parameter**	**Value**
PLCP header T_{H}	48 μs	T_{SIFS}	10 μs
PLCP preamble T_{P}	144 μs	T_{DIFS}	50 μs
Receive Power Threshold	-100dBm	T_{Slot}	20 μs
Fading Variance	10 dB	T_{CWmin}	31
APs/STAs Tx Power	100 mW	T_{CWmax}	1023
RXThreshold (11Mbps)	-82dBm	G_{tx} , G_{rx}	0 dBi
RXThreshold (5.5Mbps)	-87dBm	h_{tx} and h_{rx}	1 m
RXThreshold (2Mbps)	-91dBm	RXThreshold (1Mbps)	-94dBm

Experiment Description

All STAs download UDP traffic from the server via their APs. Traffic was generated with the stg traffic tools that come with the NCTUns simulator. The traffic profile is provided in table 4.2. APs transmit data packets to the STAs. For every received packet, if the MAC at a receiving node has decided to drop a packet, a STA uses the proposed algorithm to determine the cause of packet drop. Whenever the algorithm guesses a collision as the reason of a dropped packet, a corresponding counter is incremented. Another counter is incremented whenever the receive module of simulator decides a collision. The values of both counters are logged every second. The RCPI quantile point $Q_i(x)$ was selected by each node i using a 70% (i.e. x=70) quantile of correctly received packets.

Simulation Time	Offered Load (Pkt/s)	Packet Size (B)
0 - 120	100	Randomly between 200 and 1500

Table 4.2: Traffic Profile

Experiment Results

Figures 4.4 plots the actual number of collisions and that estimated by the proposed algorithm and the algorithms of Rayanchu et. al [17] and Malone et.al [21] with the traffic profile of table 4.2. The figure shows that the proposed approach outperforms the other two approaches. The difference between the actual/true number of collisions and the one estimated by the proposed algorithm observed at the beginning of the simulation time is due to the algorithm learning phase (i.e. time until enough number of correctly received packets is used for the computation of a good quantile point, Quantile Learning Phase). As the approach of [17] does not capture the interference of packets that arrive after the preamble of the packet being received (the power of those packets do not contribute to the RSSI value of the packet being received), it was found to estimate less number of collisions.

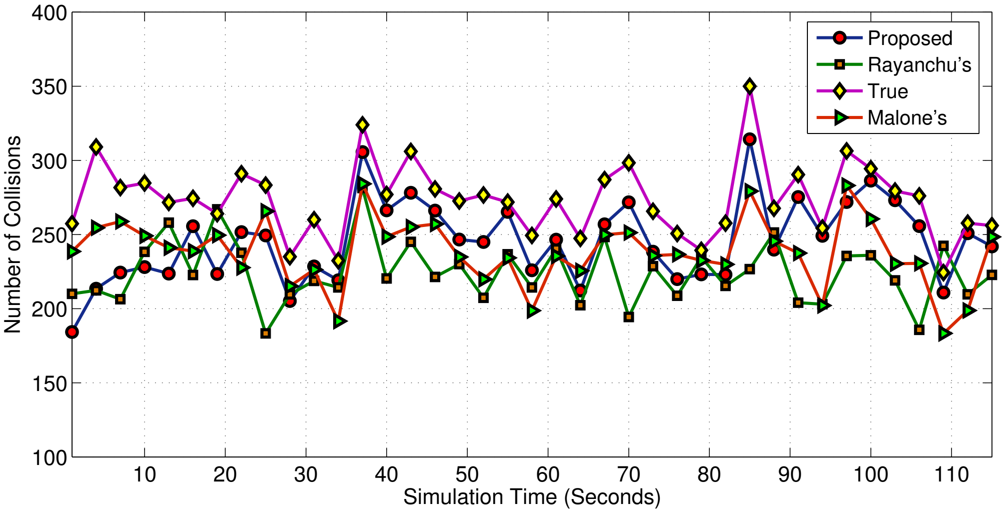


Figure 4.4: True and Estimated number of collisions.

Now, we increase the collision probability by decreasing the maximum size of the contention window CW_{max}. The results are plotted in figure 4.5. The figure shows that the proposed approach better tracks the increased number of collisions due to the decrease in the size of maximum contention window. Although the approaches of Rayanchu and Malone show an increase in estimated collisions as the CW_{max} decreases, their estimations are not accurate enough specially for small CW_{max}.

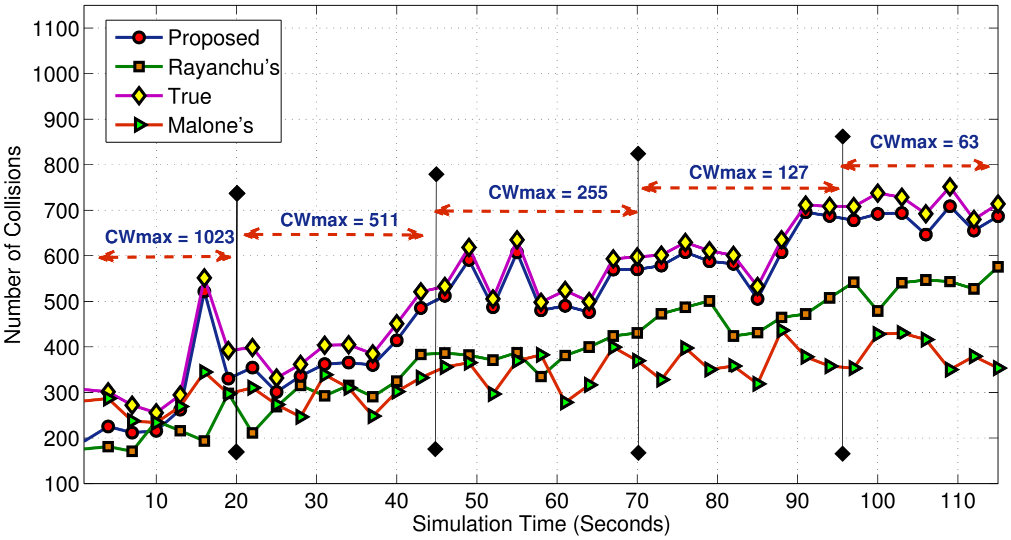


Figure 4.5: True and Estimated number of collisions for different CW_{max} values.

Then, we increase the BER by decreasing the SNR (i.e. in fact we want to increase the number of dropped packets due to weak signal). We plot the results in figure 4.6.

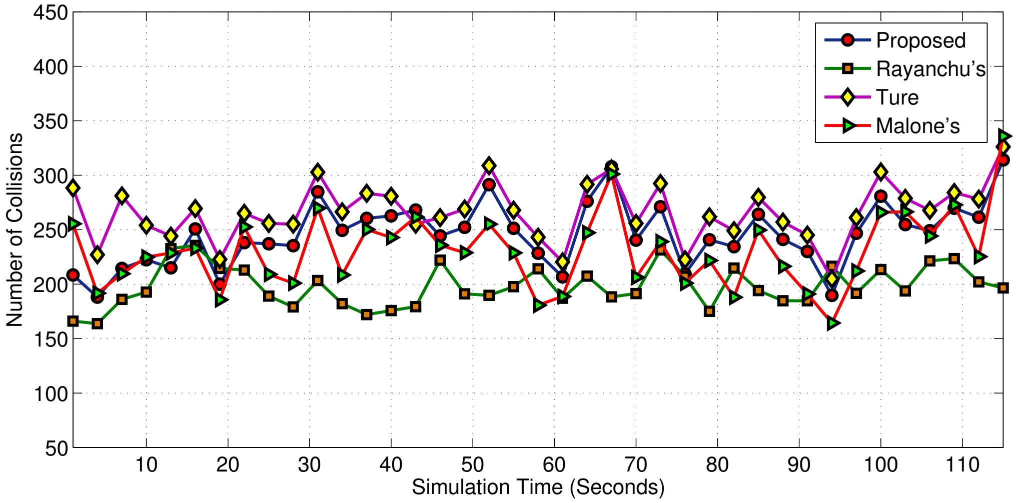


Figure 4.6: True and Estimated number of collisions with random per packet decrease of SNR.

Since the approach of Rayanchu bases the diagnosis on a fixed cut-off value of the RSSI, collision estimations with this approach are not close to the actual number of collisions. In contrast, our approach which learns from the history of correctly received packets, the fluctuations in the received signal power do not impact its ability of discriminating the cause of errors. It was found to outperform the other two approaches in this scenario.

The three approaches has been used for estimation of collision rate under different traffic conditions. The collision rate is computed as the ratio of the number of times the MAC decides a collision to the total number of received packets. Figure 4.7 reports the results of this test. The offered load is a CBR UDP traffic with a random uniform packet size between 200 - 1500 Bytes. The results show that the proposed loss discrimination approach provides better estimations than the others, especially when the collision rate is high. Nonetheless, under low load conditions, the three approaches provide comparable accuracy.

Finally, we have used equation 4.4 for estimating interference conditions. Every second, we compare the total amount of estimated interference with the total number of actual collisions. Since both parameters have different units, we normalized both values by the maximum of each and plot the curves together in figure 4.8. The figure shows a good correlation between the two curves, i.e., the estimated interference tracks the actual collisions in the network.

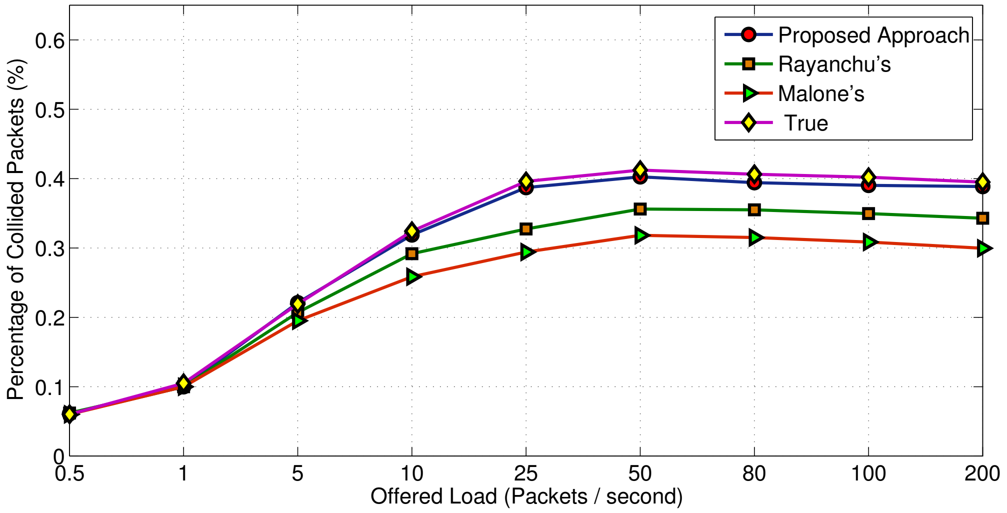


Figure 4.7: Estimation of Collision Rate with different Loss Discrimination Approaches.

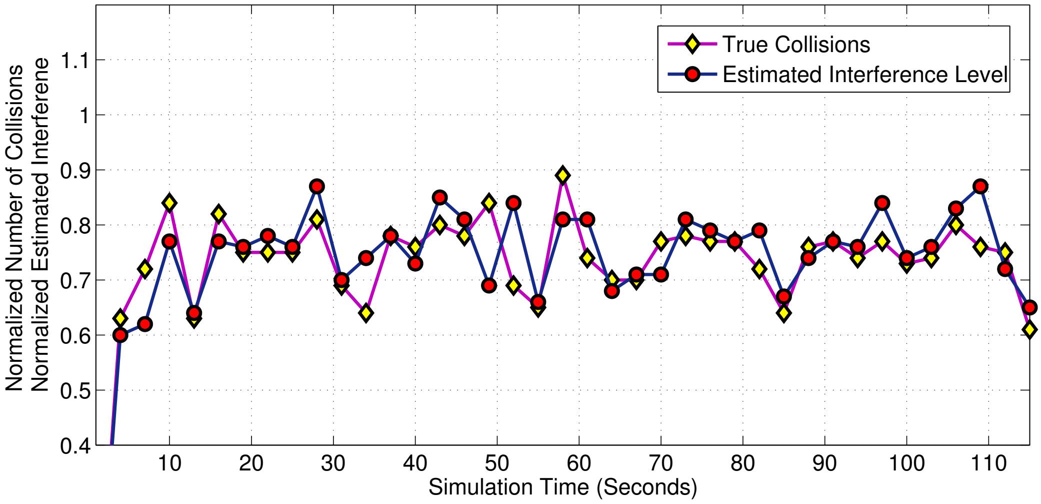


Figure 4.8: Comparison between true number of collisions and amount of Interference estimated by equation 4.4.

4.4 Methods for Determining Interference Relations

In fact, there is no way for measuring the amount of interference while a node is receiving a signal. Therefore, studies in the literature follow two different approaches to infer the effect of interference while assessing the performance of wireless communication systems:

- Using simplified models for interference approximation.
- Performing active interference measurements that are shifted in time.

Two models proposed by Gupta and Kumar [95] are being widely used:

1. **The Simple Interference Model:**
   With this model, the euclidean distance between wireless nodes is used to infer wether a transmission can be correctly received or not. Particularly, a receiver N_j is assumed to successfully receive a frame from a transmitter N_i , if and only if there is no other simultaneous sender within a guard zone, determined by a factor d, from the receiver N_j. In equation form, a transmission from node N_i to node N_j is successful if, for every other node N_k,

   $$|N_k - N_j| > (1 + d)|N_i - N_j| \tag{4.7}$$

   The factor d models the radius of the guard zone and specified by a protocol. Hence, the model is referred to as the *protocol interference model.* The main characteristic of the model is that it only accounts for the path loss as the source of signal attenuation and applies under same transmit power levels. Additionally, the selection of the factor d on which the protocol depends is a challenging open issue.

2. **The Physical Interference Model:**
   This model predicts that a transmission can be successful if the signal to interference ratio SINR exceeds some threshold. Specifically, a sender N_i transmits a frame successfully to receiver N_j in presence of K other concurrent transmissions, if and only if:

   $$\frac{\frac{P_i}{|N_i - N_j|^\alpha}}{\sum_{k=1}^{K} \frac{P_k}{|N_k - N_j|^\alpha} + P_n} > SINR_{TH} \tag{4.8}$$

   where P_i is the power level used by any sender N_i, $|N_k - N_j|$ is the distance between any nodes N_k, N_j, α is the path loss exponent which is usually supposed to be greater than 2, and P_n is the noise power level. $SINR_{TH}$ is the threshold value necessary for a successful decoding of N_i's transmission at receiver N_j.

Obviously, the physical interference model is less restrictive than the simple model. With this model, it may happen that a packet is successfully received by a receiver, even if there is another node located within the interference range of this receiver is simultaneously transmitting. Additionally, the model is more related to physical layer effects, as it considers attenuation sources like fading other than the path loss.

While the above interference models simplify the calculation of interference, their use in realistic networks has been shown to be erroneous [96]. This is due to the fact that the singnal strength is not a simple function of distance and the coverage of a node is irregular.

A second alternative approach for determining interference relations among links is through measurements that are shifted in time.Interference measurement can be performed actively during the network deployment phase, or passively while the network is operating. The core of active interference measurement approaches is the measurement of throughput or signal strength [13]. With the throughput-based approach, two links i and j are assumed to interfere if and only if the throughput of one degrades when the other is active. This is referred to as pairwise interference. The determination of interfering links takes place in the dedicated configuration phase and the start of network operation. With the signal strength based approach, each node sends in turn a series of broadcast packets. All other nodes measure the signal level of the received packets. The signal strength is used to indicate the potential interference level from the transmitting node to each other node. This measurements deliver, however, only an estimate of the real interference. This is due to the followings:

1. The signal strength varies in time, dependent on environmental changes of the wireless channel. Hence, initial measurements are not valid all the time.

2. The estimated interference is usually valid in the scenario used to estimate it. Due to the variable nature of traffic, the potential interference is not observed all the time. Additionally, protocol based dependencies on the node state (transmitting, receiving) change the dynamic pattern of the real interference.

4.5 Passive Interference Estimation

The packet loss discrimination method proposed in section 4.3 produces an estimate of the impact of interference at the node side. Particularly, it provides the knowledge of packet loss cause at a receiving node. Despite that a receiving node would be able to identify potential interferers through decoding of the MAC header of received collided packets, the method may not be sufficient. This is due to the fact that the observation of the MAC header of collided packets will help in recognizing the identity of hidden nodes, but not the identity of all potential interferers. Therefore, a node needs to observe all transmissions in order to identify which nodes from the neighborhood may damage its packets, including those visible to its sender. Additionally, as stated previously in this chapter, an important factor that determines the impact of an interferer on a receiving node is the frequency of the interference event. To achieve this goal, a passive observation of interference approach will be used. In this section, such approach is proposed. The approach does not only rely on whether some power is measured from an interfering node, but also on the time span an interferer occupies the medium. The approach works as follow:

- An AP requests the STAs it accommodates to monitor the wireless medium for a period of time T. The STA can do this by setting its radio interface in the promiscuous mode of the 802.11 standard during the monitoring period. This mode allows it to capture and pass to the MAC all packets on the medium, whether they are addressed to it or not.

- During the measurement period, a measuring STA monitors all transmitted frames over the medium and records the following information elements: The number of transmitted frames from each source address, the length of each frame, the rate at which each frame was transmitted, and the power level at which each frame is received.

- Since frames have different lengths and can be transmitted using different physical rates, an interference metric has to account for these facts. A STA k captures the interference level from a source address l as follows:

$$InterferenceLevel_{kl} = \frac{1}{T}\sum_{i=1}^{N}\frac{L_{li}P_{li}}{R_{li}} \tag{4.9}$$

  where L_{li} and P_{li} denote the length in bits and power level in dBm of frame i received from interferer l, respectively. P_{li} is captured from RCPI or RSSI. R_{li} denotes the physical rate in bits/second at which frame i is received from interferer l, and T denotes the length of the measurement period.

- Each measuring STA k sends the measurement information to its AP. ***From this report, the set of potential interferers for each STA can be identified as well as the impact of each interferer on this STA.***

- The duration of the measurement is fundamental. This period should be small in order to reduce the time a STA spends operating in the promiscuous mode but large enough to assure that transmissions from interferers fall within the measurement time and consequently produce accurate estimations. Note that the promiscuous mode of operation introduces processing overhead at the MAC for the extraction of information elements a measuring STA is collecting (i.e power level, physical transmission rate, and packet length). In order to produce accurate estimation and avoid continuous operation in the promiscuous mode for a long period, the observation period T can take place over short non-contiguous observation slots.

- The measurements are periodically conducted and reported to the AP. In order to reduce the measurement overhead, the time between successive measurements shall be adaptively set based on differences between measurement results which obviously depends on traffic patterns.

- Similarly, an AP measures interference level comming from nodes that belong to neighboring BSSs.

We make the following notes on the above interference estimation approach:

1. As pointed out, the approach considers the power levels of transmissions from interfering nodes jointly with the duration of these transmissions. This is important since the probability of collision due to interfering transmissions and the collision cost depend on the time period collided packets occupy the medium.

2. By considering the time of each frame and dividing over the whole measurement duration, we capture the activity level of an interferer and hence differentiate between interferers that permanently or transitory transmitting.

4.5.1 Evaluation of the Proposed Passive Measurement Approach

Experiment Objective

In this experiment, we would like to see how the interference level estimated using equation 4.9 characterizes interference impact captured by observation of the number of corrupted packets. The experiment is performed with real equipments as well as through simulation.

Experiment Setup

The real measurements were carried on a soccer field of 100m x 80m dimensions. Two APs are deployed as shown figure 4.9. They are configured on the same channel. 10 STAs are distributed across the coverage area of both APs at the distances shown the figure. APs and STAs use the 802.11b technology. The RTS/CTS mechanism was turned off. STAs were equipped with Atheros (5006x) cards and the MadWiFi-ng driver, while the well known sniffer TCPDUMP was used to sniff packets. STAs and APs transmit with a fixed power level of 100mw. The 10 STAs download packets from a server connected to the APs via an ethernet switch. Two traffic profiles are used as shown in tables 4.3 and 4.4. In the first traffic profile, we fix the packet size and decrease the offered load after half of the experiment duration. In the second traffic profile, the offered load is fixed and the packet size is reduced over the experiment time.

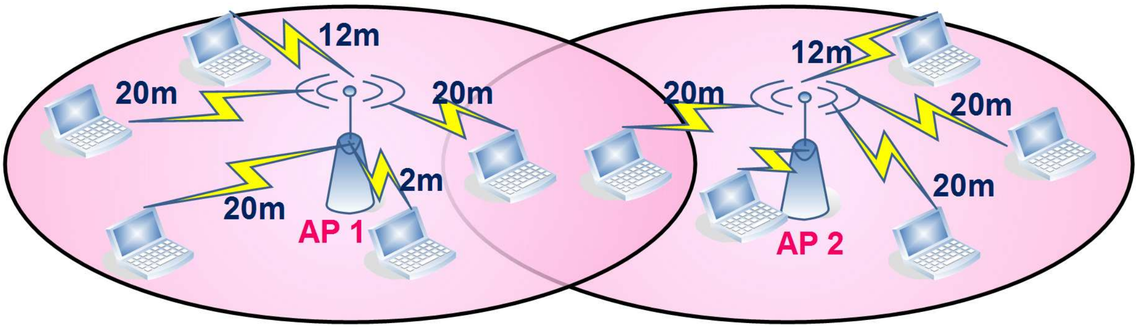


Figure 4.9: Experiment Setup

Time	Offered Load (Pkt/s)	Packet Size (B)
0 - 150	50	1500
151 - 300	8	1500

Table 4.3: Traffic Profile 1

Time	Offered Load (Pkt/s)	Packet Size (B)
0 - 150	20	1500
151 - 300	20	500
301 - 450	20	200

Table 4.4: Traffic Profile 2

Real Measurement Results

Figure 4.10 plots the number of corrupted packets during each second of the measurement time with traffic profile of table 4.3. As expected, the results show that less corruptions occurs at the low load. Figures 4.11 and 4.12 plot the total power and total interference level during each second of the measurement time, respectively. The power level is computed from the received signal strength while the interference level is computed using equation 4.9. The results show that both the power level and interference level metrics reflect the changes in the number of corrupted packets and consequently characterize interference conditions. Note that under low load, measuring STAs will receive less number of packets during the observation period. Hence, the power level metric is lower for lower load, though it does not consider activity level.

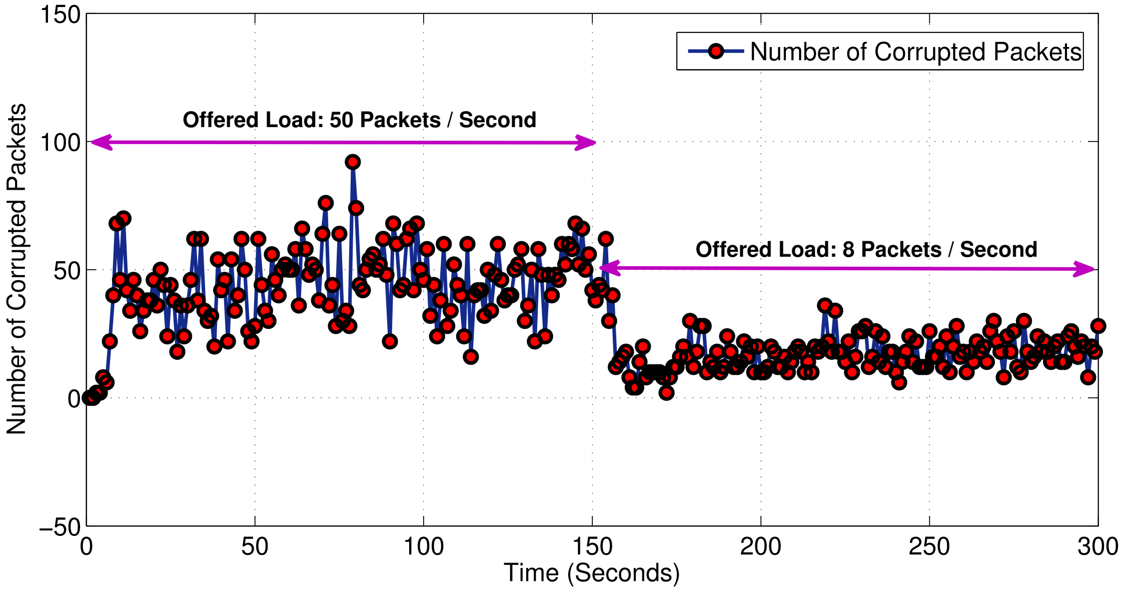


Figure 4.10: Real Experiments with Passive Interference Measurement: Number of Corrupted Packets with two different loads.

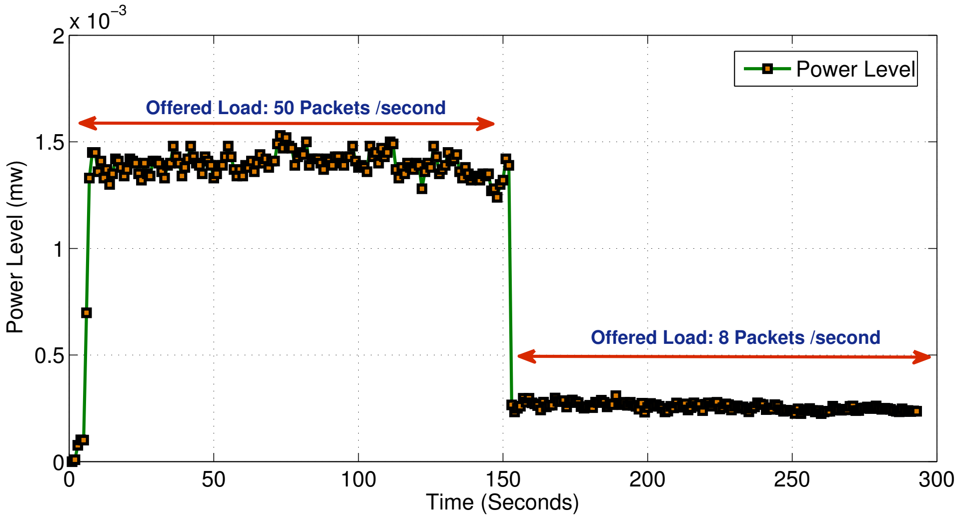


Figure 4.11: Real Experiments with Passive Interference Measurement: Total Power with two different loads.

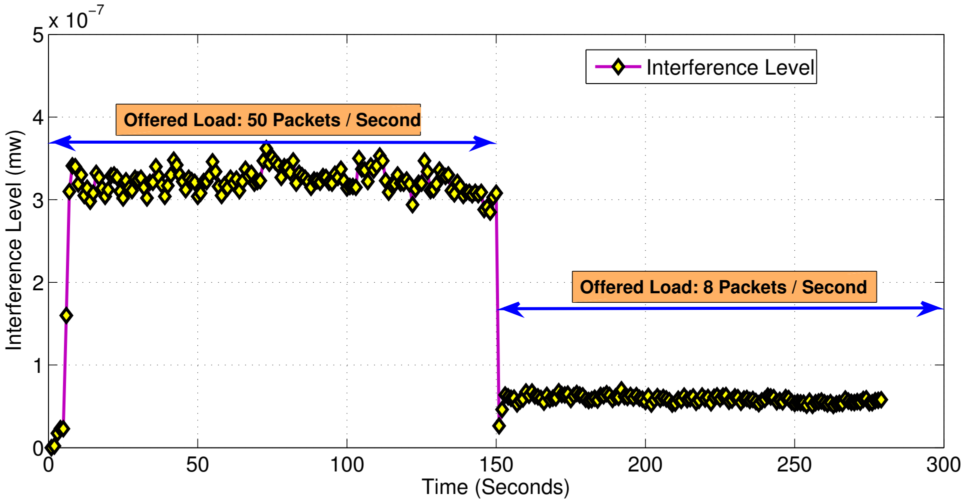


Figure 4.12: Real Experiments with Passive Interference Measurement: Interference Level with two different loads.

Now, we discuss the results for the traffic profile of table 4.4. Figure 4.13 plots the total number of received corrupted packets observed by all STAs versus the measurement time. Figures 4.14 and 4.15 plot the total power level and the total interference level, respectively. Note that in this traffic profile the load is fixed while the packet size is variable. The results show that the changes in power level does not reflect changes in the number of corrupted packets which becomes less as the packet size decreases. This will lead to erroneous characterization of interferers' impact. On the contrary, small increase in the power can be seen as the packet size decreases. In contrast, the interference level computed with equation 4.9 is able to track changes in the number of corruptions. This is because it considers the time an interferer packet occupies the medium which influence the probability of packet collision and corruption. Hence, it better characterizes the impact of an interferer.

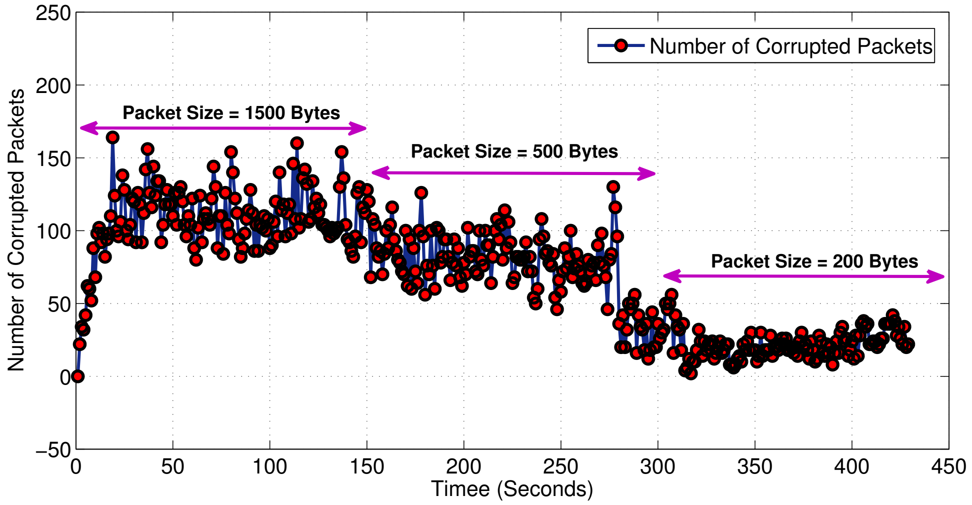


Figure 4.13: Real Experiments with Passive Interference Measurement: Number of Corrupted Packets for different packet lengths.

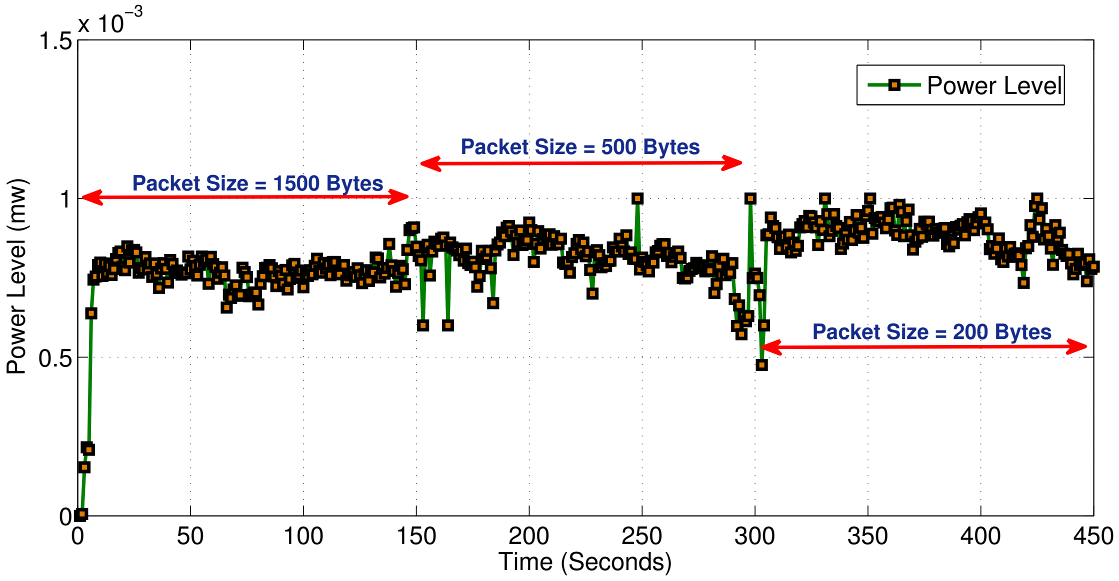


Figure 4.14: Real Experiments with Passive Interference Measurement: Total Power for different packet lengths.

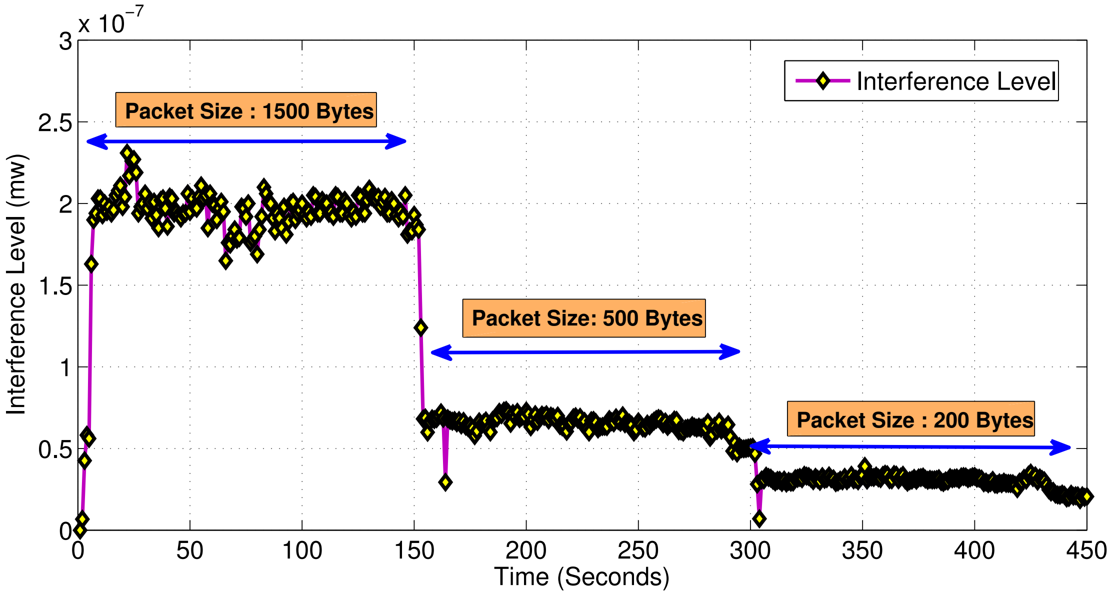


Figure 4.15: Real Experiments with Passive Interference Measurement: Interference Level for different packet lengths.

Simulation Results

Simulation results for the traffic profile of table 4.4 are shown in figures 4.16 and 4.17. The results are in agreement with the real measurement results.

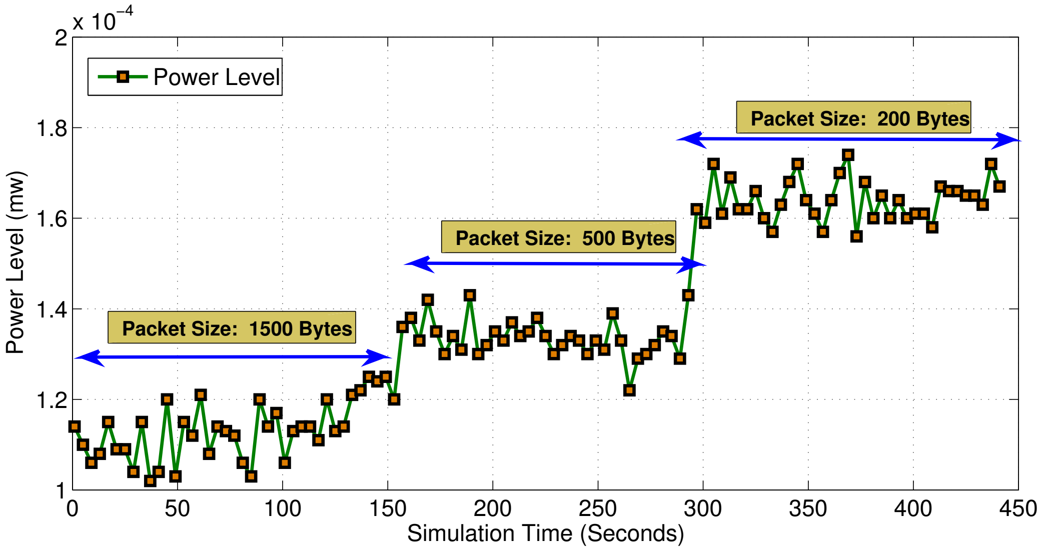


Figure 4.16: Simulation Experiments with Passive Interference Measurement: Total Power for different packet lengths.

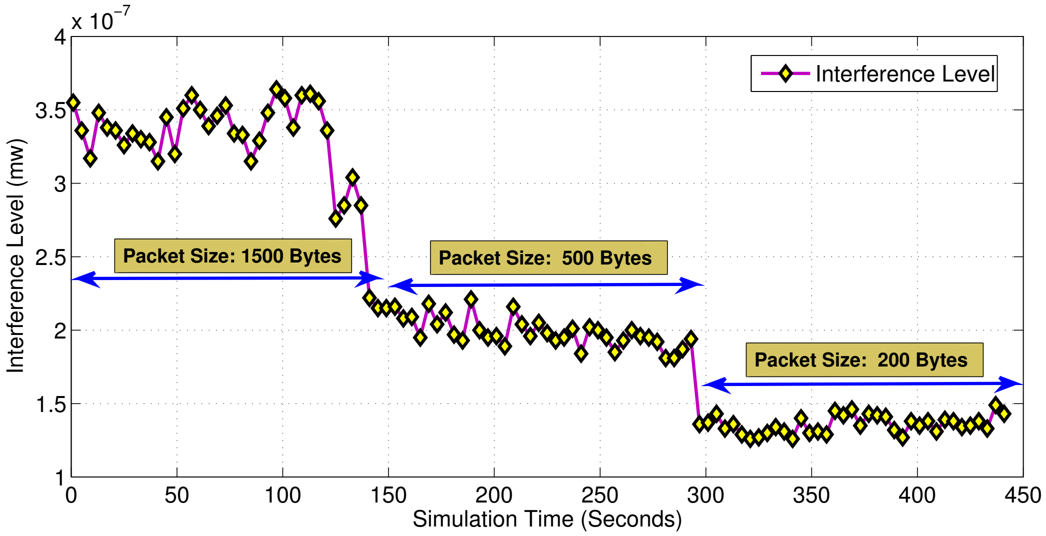


Figure 4.17: Simulation Experiments with Passive Interference Measurement: Interference Level for different packet lengths.

4.6 Conclusions

In this chapter, we proposed two complementary methods for determining interference relations among WLAN nodes and estimating interference conditions at a node receiver. Interference relations are determined through passive observation of the wireless channel. Packet loss discrimination has been used for estimating the impact of interference at the receiver side. The two methods will be used in the following chapters for interference mitigation through the tuning of the RTS/CTS protocol, and the coordination of channel access during high interference conditions. We showed that the proposed packet loss discrimination method performs better than some relevant approaches proposed in recent literature. We also showed that interference impact does not only depend on the received signal power from the interferer. Rather, other parameters such as packet size, modulation used by interfering nodes, and activity level of interferers are strong factors which characterize the impact of an interferer on the ability of a receiving node to correctly receive packets. By observing the number of corrupted packets, simulation and experimental results have shown that the proposed passive approach better characterizes impact of interfering nodes than the commonly used approach that is just based on total power level of received interfering packets. We showed that this approach may produce improper conclusion about interference conditions.

Chapter 5

Improving Access Point Selection in 802.11 WLANs

5.1 Introduction

In Infrastructure WLANs, a STA has to associate to an AP before it can access data transmission services of the WLAN BSS. A precursor to association is the selection of AP. After performing the scanning procedure (either passively or actively), a STA builds the scanning report which includes all information about the detected BSSs in its vicinity. Figure 5.1 depicts three BSSs covered by three APs. As it can be seen, each STA of the seven STAs that fall in the overlapping areas of the three APs may hear more than one AP. Thus, in principle, a STA can potentially associate with more than one AP on same or different channels. Consequently, the following significant issue arises: how to select an appropriate AP (BSS) among available APs.

As pointed out in chapter 1, the interference mitigation approach proposed throughout this thesis first reduces the impact of interference on a WLAN node at the selection phase. This is achieved by a new AP selection policy which provides a new STA with information about Intra-BSS interferers within the potential BSS and Inter-BSS interferers that belong to the neighboring BSSs. A STA uses this information jointly with the signal strength to each potential AP and produces an estimate of the goodput it will experience if it joins any of the candidate BSSs.

This chapter first discusses the AP selection policy currently implemented in todays WLAN cards. Then, it develops an improved AP selection policy that tries to achieve the aforementioned goal. To assess the proposed AP selection policy, its performance will be compared with other relevant ones proposed in the recent literature.

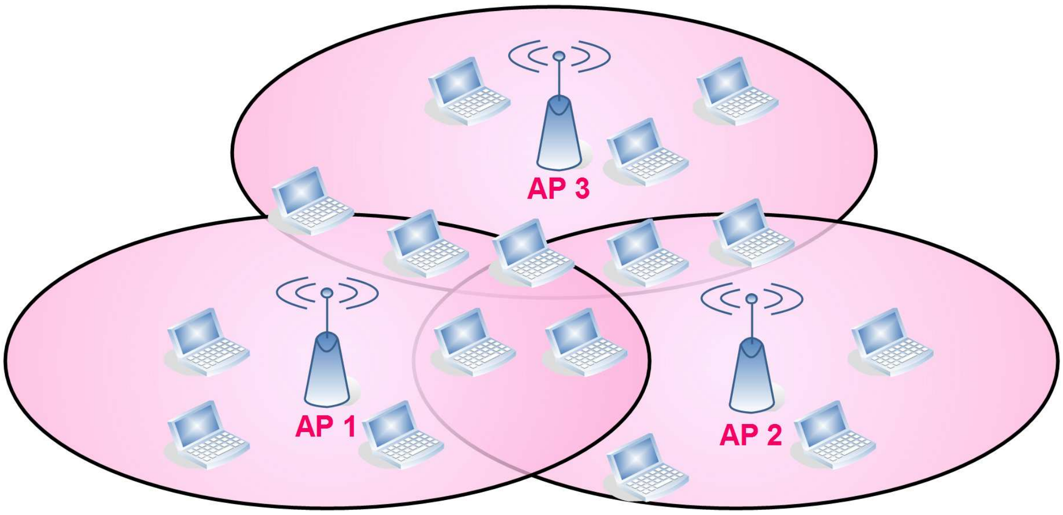


Figure 5.1: WLAN BSSs and AP Selection

5.2 Limitations of Legacy AP Selection Policy in 802.11 WLANs

In current IEEE 802.11, the user simply picks the AP from which it has received the strongest signal strength (RSSI) [26]. Afterwards, it stays associated until the STA is powered down or the AP shuts down its service. Unfortunately, this rather simple selection algorithm is not efficient and can even lead to problems regarding the network performance of larger areas with many STAs and several APs [27, 28]. This is due to the following reasons:

- In addition to the connection quality, the QoS depends on many other parameters like the number of contending users and their individual loads, the amount of interference on the channel the AP offers. In other words, the AP with which a STA has the highest RSSI does not necessarily provide the best service.

- RSSI based selection can cause load imbalance between several APs. In a dense Extended Service Set (ESS) with many APs, one could easily observe that many STAs associate with few APs while some other APs accommodate small number of STAs or even idle [29]. In this case, STAs do not efficiently utilize the available capacity. Consequently, with RSSI-based selection, radio resources are not effectively utilized and fairly shared among WLAN STAs.

- The multi-rate flexibility provided by several IEEE 802.11 variants can cause low bit rate STAs to negatively affect high bit rate ones and consequently degrade the overall network throughput. This sever problem is known as the Anomaly Problem [8] and can be mitigated at the selection phase. We elaborate more on this issue in section 5.3.

- Practically, many STAs may have same connection quality with several candidate APs and probably employ same transmission rate to communicate with them.

This is quite common with dense deployments of todays WLANs. The question still, how such STAs should select their APs?

5.3 Performance Anomaly of IEEE802.11

Although IEEE 802.11 provides a means for allocating a part of the radio channel bandwidth to some STAs (PCF - Point Coordination Function), the commonly implemented access mode (DCF - Distributed Coordination Function) uses the CSMA/CA protocol to share the channel in a fair way. However, it has been observed in [8] that in some common situations, the CSMA/CA results in a significant performance degradation.

In a typical WLAN, some STAs may have low radio transmission quality. In this case, WLAN products based on 802.11 standard reduce the bit rate from the nominal 11 Mbps rate to 5.5, 2 , or even to 1 Mbps (with 802.11b) to alleviate frame errors. Usually, STAs detect this situation from an increased number of frame retransmissions.

In [8], it has been shown that if a STA with a transmission rate of 11 Mbps shares the channel with a STA at a transmission rate of 1 Mbps, the throughput of the 11 Mbps STA is about the same as that of the 1 Mbps STA (assuming equal flow characteristics of each STA as well as the saturation mode). Such a behavior penalizes fast STAs and privileges the slow ones. In fact, the reason for this anomaly is the basic CSMA/CA channel access mode which provides ”per frame fairness”, meaning that in the long term STAs have the same chance to access the medium and send their frames (i.e. all STAs should transmit with an equal average frame rate over a longer time horizon). As the time duration required to transmit a frame with a low transmission rate is much longer than the duration for the same frame size with a higher transmission rate, a low transmission rate STA will occupy the channel for a longer time. This phenomena degrades the throughput of high rate STAs if they are associated to the same AP.

For the sake of illustration, we conducted a simulation experiment in order to show the impact of performance anomaly of 802.11. Figure 5.2 shows the throughput of an 11Mbps user when associates to an AP that accommodates different number of users. In a first case the other users also employ 11Mbps transmission rate. In a second case they transmit at a physical rate of 2 Mbps. Note that the goodput of the 11Mbps user is higher when it shares the AP with other high rate users specially when the the number of low rate users gets high.

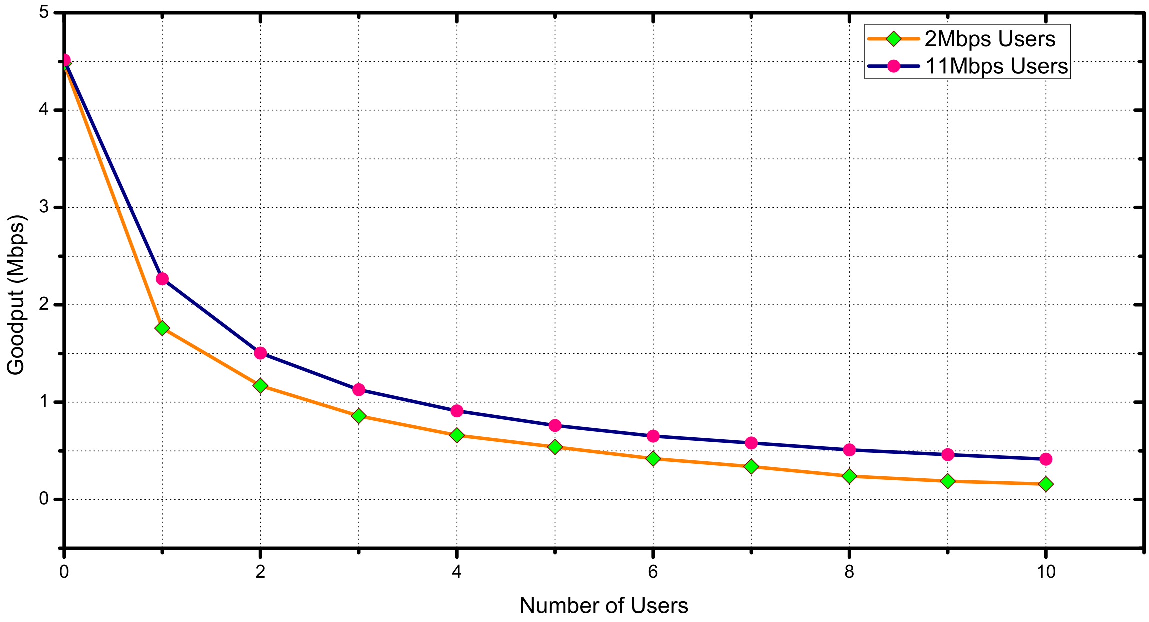


Figure 5.2: Performance Anomaly in 802.11 WLANs

5.4 State of the art

Currently, most of 802.11 WLAN adapters adopt the RSSI-based policy in order to select an AP to affiliate with. Previous works [30, 31, 32] have shown that the RSSI-based policy may lead to poor performance in terms of achieved throughput and load distribution. This has initiated intensive research studies that address this issue. A decentralized approach to load balancing has been proposed by Ekici et al. in [33]. With this approach, each STA decides independently on its association. Nevertheless, the authors suppose in their study that the achieved goodput per STA equals the transmission rate which is not the case in general. The authors of [34] compare the performance of selfish and centralized AP selection strategies. The paper [35] proposes a scheme for best AP selection during handover based on frame retransmissions. While the proposed scheme achieves good performance, its implementation requires two wireless interfaces for each STA. The recent paper [36] proposes to base AP selection on packet transmission delay. One concern about the proposed approach is the efficiency and possibility of estimating the set of required parameters during the scanning phase. In [37], the authors propose an AP selection policy that accounts for hidden node problem. With their approach, a STA selects the AP expected to provide the maximum throughput and minimum impact of STAs hidden from the new STA. Estimation of hidden STAs impact is based on channel busy time measurement during the scanning process and a channel busy time value provided by APs in beacon frames. A drawback of this approach is that a channel may be sensed to be busy due to transmissions in other BSSs other than the one under consideration. Moreover, the throughput is simply concluded from the transmission rate estimated via RSSI. These issues may influence the accuracy of estimation. The work in [29] proposes an AP selection approach that considers the loss rate and the number of STAs already associated to an AP as a metric for AP selection. However, the authors ignore the interference aspect and the approach has been only tested for downlink traffic.

In principle, the advantages of multi-rate protocols have been shown in [41]. The recent paper [42] addresses another decentralized AP Selection. With this scheme, a STA associates with the AP that provides the best service considering the connection data rate as well as the number of users accommodated by the AP. Kumar and Kumar [43] have presented a simple mathematical model for the multiple rate effect and the consequence for centralized, optimal load balancing. Although the authors consider the multi-rate effect, again the goodput per terminal is assumed to equal STA's physical transmission rate. A further centralized solution with a simplified load characterization can be found in [44].

The AP selection approach of [38] considers the interference in selection decisions. Nonetheless, the interference impact is derived from a curve generated experimentally for a specific topology and hence does not apply to all scenarios. Recently, the authors of [39] propose an AP selection policy based on the instantaneous rate and the fraction of time for which an AP acquires the channel for its transmission. While the derived model involves interference, it considers only downlink transmissions and assumes that channel contention is among APs.

5.5 Improved AP Selection

As a result of the previous discussion, the AP selection policy currently implemented in WLAN devices has to be refined and improved to consider the various parameters that influence the obtained QoS and the dynamics in the environment. Efficient AP selection calls for a decentralized policy implemented at the STA to enable it accurately assess the expected QoS it will experience if it joins a BSS. Such selection policy can be based on information about the BSS status, which includes: The number of currently associated STAs, the number of potential interfering nodes that belongs to neighboring BSSs, and physical rates being used by users. This information is distributed by the APs via the Beacon and Probe Response frames. This concept is discussed in reference [40]

In this section, an improved approach for AP selection is proposed. We identify the core problem of AP selection to be the choice of metric to consider and whether the choice should be (periodically) reevaluated or not. Firstly, we derive a metric that is beneficial in combination with a new static AP selection scheme for IEEE 802.11 WLANs. This new metric encapsulates important BSS and connection parameters into a single value. In section 5.5.2, the static scheme is enhanced towards a periodic reevaluation of the current association decision which we refer to as dynamic AP selection scheme in the following. In section 5.6, we evaluate the proposed selection through simulation experiments, by observing the impact of AP selection policy on the achieved goodput.

5.5.1 Decision Metric for AP Selection

Given a certain traffic characterization of a STA, ultimately a STA needs to join the BSS which can serve this traffic stream best. This might be the AP which has the highest SNIR. However, if the BSS is crowded with other STAs operating at a much lower SNIR than the currently observed STA or operating on a channel interfered by many other nodes belonging to neighboring BSSs, the new STA might not be served very well even though the SNIR indicates a good service.*Hence, a metric that captures the expected goodput of the STA if it joins a BSS is required.*

We start deriving such a metric by considering a certain BSS i operated by AP i. Assume that there are currently $U_i^{(t)}$ STAs associated to the AP. Some new STA k considers the association to BSS i. Hence, it has to evaluate the data rate it will receive from joining BSS i. We start deriving the data rate STA k will receive if joining BSS i.

Following the analysis in [45], STA k in BSS i successfully transmits a frame of length L bits after j consecutive unsuccessful transmissions within a time period of $T_{k,i}\left(j\right)$, given by:

$$T_{k,i}\left(j\right) = T_{\mathrm{P}} + T_{\mathrm{H}} + T_{\mathrm{DIFS}} + \frac{L}{R_k} + T_{\mathrm{SIFS}} + T_{\mathrm{ack}} + T_{\mathrm{backoff}}\left(j\right) \tag{5.1}$$

T_{P} and T_{H} represent the time duration of the physical layer preamble and header. T_{DIFS} is the Distributed Coordination Function Inter-frame Space, and T_{SIFS} is the Short Inter Frame Spacing, $L = (28 + L_{\mathrm{MSDU}}) \cdot 8$ is the length of the MAC packet in bits (where L_{MSDU} is the MAC Service Data Unit length and the 28 bytes stem from the MAC header), $T_{\mathrm{ack}} = (T_{\mathrm{P}} + T_{\mathrm{H}} + \frac{112}{R_k})$ is the duration of the ACK frame, and $T_{\mathrm{backoff}}\left(j\right)$ is the average backoff interval in μs after j consecutive unsuccessful transmission attempts given as:

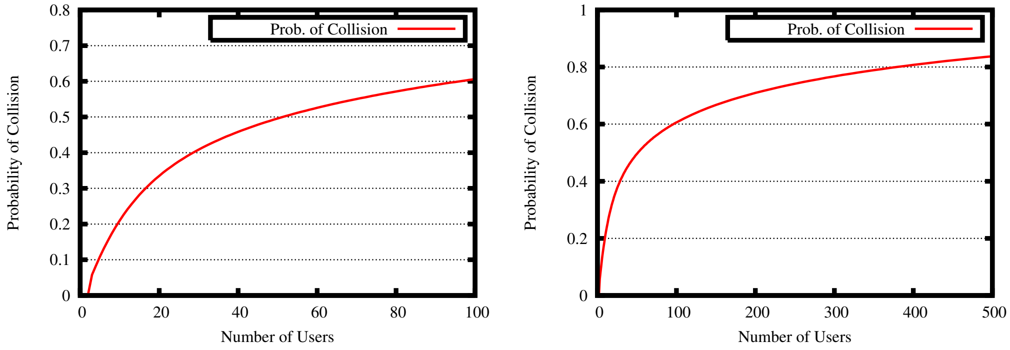
$$T_{\mathrm{backoff}}(j) = \begin{cases} \frac{2^j(T_{\mathrm{CWmin}}+1)-1}{2} \cdot T_{\mathrm{Slot}} & 0 \leq j < 6 \\ \frac{T_{\mathrm{CWmax}}}{2} \cdot T_{\mathrm{Slot}} & \mathrm{j} \geq 6 \end{cases} \tag{5.2}$$

where T_{Slot} is the basic slot duration, T_{CWmin} and T_{CWmax} are the minimum and maximum contention window sizes respectively.

However, $T_{k,i}\left(j\right)$ is only the *raw* average transmission time of a frame. The frame is still subject to frame errors, which requires one or several retransmissions. From [45], the average time span that STA k requires to transmit a single frame *correctly* is given as:

$$\overline{T_{k,i}} = T_{k,i}(0) + \sum_{j=1}^{\infty}(1 - P_{k,i})P_{k,i}^{j}\left[\sum_{m=0}^{j-1} T_f(m) + T_{k,i}(j)\right] \tag{5.3}$$

where $P_{k,i}$ is the frame error probability, and $T_f(m) = T_{\mathrm{P}} + T_{\mathrm{H}} + T_{\mathrm{DIFS}} + T_{\mathrm{backoff}}(m) + \frac{L}{R_k} + T_{\mathrm{SIFS}} + T_{\mathrm{ack}} + T_{\mathrm{Slot}}$ is the time between two consecutive transmissions if the frame transmission fails. In fact, the transmission can fail due to frame errors or collisions.



(a) (b)

Figure 5.3: Probability of Collision in IEEE 802.11 DCF under the Saturation Mode

Assuming that frame errors are independent from collisions, we could write $P_{k,i}$ as follows:

$$P_{k,i} = Pe_{k,i} + Pc_{k,i} - Pe_{k,i}Pc_{k,i} \tag{5.4}$$

where $Pe_{k,i}$ is the frame error rate due to the channel and $Pc_{k,i}$ is the error rate due to collisions.

In [46], Bianchi et al. derived an expression for the $Pc_{k,i}$ as follows:

$$Pc_{k,i} = 1 - (1-\tau)^{U_i - 1} \tag{5.5}$$

where τ represents the probability that a STA transmits in a randomly chosen time slot expressed as:

$$\tau = \frac{2(1-2Pc_{k,i})}{2(1-2Pc_{k,i})(CW_{min}+1) + Pc_{k,i}CW_{min}(1-(2Pc_{k,i})^m)} \tag{5.6}$$

where $CW_{max} = 2^m CW_{min}$. (i.e m=5 if CW_{min}=32 and CW_{max}=1024).

The authors of [46] proposed to solve the non linear system in 5.5 and 5.6 using numerical techniques. We solved the system using the Lingo optimization package [47]. Figures 5.3(a) and 5.3(b) show how the probability of collisions varies as a function of the number of users which share the same wireless channel. Interestingly to note is that the packet loss rate due to collisions may exceed 30% if about 20 users share the channel. This motivates the consideration of interference in the selection decision.

To incorporate the influence of inter-BSS interference on the achieved goodput (i.e interference due to transmissions in neighboring BSSs), we modify 5.5 as follows (taking into account the new STA S_k):

$$Pc_{k,i} = 1 - (1-\tau_k)^{U_i} \prod_{\forall j, j \notin S_i} \Theta_{j,k} \tag{5.7}$$

where S_i is the set of STAs associated with AP i and $\Theta_{j,i}$ is the probability that STA j does not collide with the transmission of STA k which can be expressed as:

$$\Theta_{j,k} = (1 - \tau_j) + \tau_j(1 - \xi_{k,j}) \tag{5.8}$$

where $\xi_{k,j}$ is the probability that a transmission from STA j in a neighboring BSS disrupts a simultaneous transmission of STA k. In fact, the value of $\xi_{k,j}$ depends on channel conditions and specifically the level of the received signal from STA j at AP i, the AP of STA k. The first term on the right side of (5.8) represents the probability that STA j does not transmit while the second term represents the probability that STA j transmits but does not disrupt STA's k transmission. Assuming $\tau_j = \tau, \forall j$ and substituting (5.8) in (5.7), we have:

$$Pc_{k,i} = 1 - (1 - \tau)^{U_i} \prod_{\forall j, j \notin S_i} (1 - \tau\xi_{k,j}) \tag{5.9}$$

While an AP already knows the number of users it accommodates U_i, it can infer information about interfering nodes by two ways:

- **(i) The local measurements at the AP:**

  Through the passive interference measurement approach presented in section 4.5, each AP can monitor its operational channel and observe the activity of unassociated STAs in its vicinity by operating in the promiscuous mode of the 802.11 standard. The main drawback of this option is the difficulty for the AP to perform measurements when the downlink traffic is high. Note that an AP can not monitor and transmit simultaneously. Nonetheless, the AP can spread the observation period over some smaller non-contiguous time slots. Therefore, instead of continuously monitoring the channel for an observation period of length, say T and blocking the communication in the BSS during this period, the AP can monitor the channel during N smaller periods the length of each is T/N. The separation between each period can be dynamically selected by the AP depending on the communication conditions. The AP can stop uplink traffic from its associated STAs before starting a monitoring slot by sending them a packet with a NAV period set to the length of a monitoring slot. This gives more opportunities for the nodes belonging to neighboring BSSs to access the channel and send their traffic, improving the efficiency of the interferers detection process at the monitoring AP.

- **(ii) Utilizing the 802.11k Beacon Report:**

  APs send Beacon requests to associated STAs, asking these to report beacons they receive from other BSSs that use the same channel. A STA observes all beacons transmitted by other APs in its vicinity. At the end of the measurement time, a STA processes measurements and sends the beacon report to its AP.

  Since the CSMA/CA provides per frame fairness, each STA will have the chance to use the channel. Therefore, it is possible for each AP to estimate the activity of all STAs it accommodates by observing the in/out frames during some time interval. Consequently, each AP has the knowledge of: ***Which of its associated STAs may interfere other neighboring BSSs***.

To avoid excessive overhead, APs increment the time between two consecutive beacon requests if the most recent beacon report does not differ from its precedence.

A fundamental question arises in connection with measurement-based approaches is about the duration of measurements. Practically, an AP either transmits a beacon every 10 or 100ms depending on the configuration. In order to assure that transmitted beacons from neighboring APs fall in the observation period, this period has to be at least 100ms.

If APs share the measurement results, each one can deduce the number of interfering STAs N_j in its neighborhood and belong to other BSSs. Then, the error probability due to collisions (equation (5.9)) may be written as:

$$Pc_{k,i} = 1 - (1-\tau)^{U_i + N_j} \tag{5.10}$$

where N_j is the number of potential interferers to STA k.

Now assuming that STA k is the only STA in the BSS i, the fraction $L/\overline{T_{k,i}}$ would yield the average goodput of STA k in the BSS (assuming also that the AP does not transmit any data). However, we assume that there are in general $U_i^{(t)}$ active STAs in BSS i of equal transmission probabilities, therefore it is quite likely that the channel is occupied by some other STA if STA k wants to start a data transmission. Due to performance anomaly of 802.11, STA k's goodput also depends on the channel occupancy time of other STAs in the BSS. We capture this effect by modeling the average rate of correctly transmitted bits by:

$$G_{k,i} = \frac{\mu_{k,i} L}{\overline{T_{k,i}}} \tag{5.11}$$

where $\mu_{k,i}$ is the fraction of channel time consumption "left over" for STA k, given as:

$$\mu_{k,i} = \frac{\overline{T_{k,i}}}{\overline{T_{k,i}} + \sum_{j=1}^{U_i^{(t)}} \overline{T_{j,i}}} \tag{5.12}$$

Recall that STA k has not joined BSS i yet. Finally, we obtain the average goodput of correct bits $G_{k,i}$ (combining Equations (5.11) and (5.12)) as:

$$G_{k,i} = \frac{L}{\overline{T_{k,i}} + \sum_{j=1}^{U_i^{(t)}} \overline{T_{j,i}}} \tag{5.13}$$

From Equation (5.13) it is clear that STA k's goodput depends on the channel occupancy time of frames transmitted by other STAs in BSS i (apart from other issues like the SNIR and chosen rate).

To compute the previous metric, a STA needs the following pieces of information, the number of STAs the AP currently accommodates $U_i^{(t)}$, the number of interferers from neighboring BSS N_j, the summation value in equation (5.13) and the current SNR between AP and STA. The AP could include the first three values in a new information field in the Beacon and Probe Response frames. Obviously, the length of this field is only a few bytes, so that it does not impose a significant overhead. For computing $\overline{T_{k,i}}$ and $\overline{T_{j,i}}$, $Pe_{k,i}$ and $Pe_{j,i}$ can be evaluated as described in [48], where a STA can use the perceived SNR and the AP can use the uplink SNRs for the STAs (assuming similar wireless channel conditions in both uplink and downlink directions).

5.5.2 Dynamic AP Selection

As the wireless environment is dynamically changing, after a period of time any selected AP may no longer remain the best one regarding the derived metric in the previous section. Therefore, a STA k should be required to evaluate the function $G_{k,i}$ after some time period T_c and re-associate if it found a better AP. T_c can be constant and the STA can re-scan BSSs over all supported channels as proposed in [49]. However, we believe that the frequency of re-evaluating the current association and the set of channels to be used in re-scanning should be dynamically adjusted. Therefore, we improve the procedure of [49] in this sense. This topic and a corresponding idea to address this issue is discussed in references [50, 51]. Specifically, the value of T_c is adjusted in order to avoid unnecessary scanning and a frequent "ping-pong" effect. Moreover, a STA scans all channels only after it has been powered up. Afterwards, a mask is used to filter out all channels from which a Beacon or Probe Response frame have not been received. However, the set of all non-overlapping channels (channels 1,6, and 11 in IEEE 802.11b/g) are not masked since those channels are most likely to be used by APs. This is expected to reduce both the number of scans and the scanning time, which is obviously very critical for delay sensitive applications. For example, considering voice over IP (VoIP traffic), which has very strict requirements, the maximum tolerable end-to-end networking delay is about 150 ms. The typical scanning and re-association time with the legacy 802.11 approach is between 1 and 2 seconds, which will hardly allow a good VoIP quality. This time is reduced by using the combination of dynamic selection and masking. However, this reduction is still not satisfactory.

The scanning time span can be mitigated further by "spreading" the scanning process over time. Specifically, once the STA has a list of neighboring APs, it can sequentially send probe request frames to the APs. The time separation between two successive probe request frames T_w could be selected such that the quality of service of ongoing calls is not degraded significantly. After receiving probe responses from all neighboring APs, the STA has the required information to decide whether to join a new AP or not.

Apart from that, the emerging 802.11k and the 802.11r standards as well as the 802.11 power-save mechanism can further contribute in resolving the scanning latency problem. 802.11k [11] enables a STA to request a list of candidate neighboring APs from the AP to which the STA is associated. 802.11r [12] defines mechanisms for fast and secure transition between APs. Dependent on the duration of the scanning latency, a STA will experience packet losses since it is not able to receive frames being sent by its old AP. With the power-save mechanism of legacy 802.11, one is able to minimize packet losses while the STA scans for APs on other channels. During this period, the AP buffers frames dedicated to the scanning STA such that they can be conveyed after STA's reappearance. Huang et al. [52] used this scheme to optimize selective scanning prior to fast WLAN handoffs.

Therefore, by combining the spreading scanning concept with the 802.11 power-save mechanism as well as with IEEE802.11k and IEEE802.11r technologies, the dynamic selection scheme is expected to be possible with real time applications.

A pseudocode for the dynamic AP Selection algorithm is provided in algorithm 2.

Algorithm 2 Dynamic AP Selection Algorithm

```
 1: ChannelList ⇐ {All Supported Channels}
 2: Non-Overlapped ⇐ {Non-overlapping Channels}
 3: Send Probe Request Frames or Listen to Beacons over ChannelList
 4: $AP_{new}$ ⇐ Select AP based on $G_{k,i}$ (as explained in Section 5.5.1).
 5: for ($time = 0$ to $T_c$) do
 6:    do normal communication
 7: end for
 8: Send Probe Request Frames or Listen to Beacons over ChannelList.
    Alternatively:
 9: for all Channels ∈ ChannelList do
10:              {
11:              Send Probe Request over a Channel;
12:              do normal communication for Some Time $T_w$;
13:              }
14: end for
15: ChannelList ⇐ Non-Overlapped ⋃ {Channels over which Probe Responses or Beacons were received}
16: $AP_{new}$ ⇐ Select AP based on $G_{k,i}$
17: if ($AP_{new}$ better than current $AP$) then
18:    $T_c \Leftarrow T_c/2$
19:    Re-associate
20: else
21:    $T_c \Leftarrow 2\ .\ T_c$
22: end if
23: go to step 5
```

5.6 Performance Evaluation of the Proposed AP Selection Policy

In this section, we evaluate the performance of the proposed AP selection policy. Interference mitigation shall impact the amount of data transmitted successfully by each user. Hence, aggregate goodput is the main performance metric of interest. We compare the proposed policy with the default RSSI-based policy implemented in IEEE 802.11b WLAN cards, and some other relevant and recent approaches by Fukuda [29] and Kaufmann [39]. The performance results are obtained by means of simulation.

5.6.1 Simulation Scenario

The simulation scenario is comprised of 10 APs that use the same channel and provide services to users that reside within their coverage area. The simulation parameters are similar to the ones described in section 4.3.4. However, we focus here on two scenarios regarding the distribution of users across the coverage area of APs. In the **First Scenario** (shown in figure 5.4), all users are randomly and uniformly distributed across the coverage area of the APs. In the **Second Scenario**, we consider a case where a high user density exist around some APs while some other APs are deployed in the neighborhood with less users density as shown in figure 5.5.

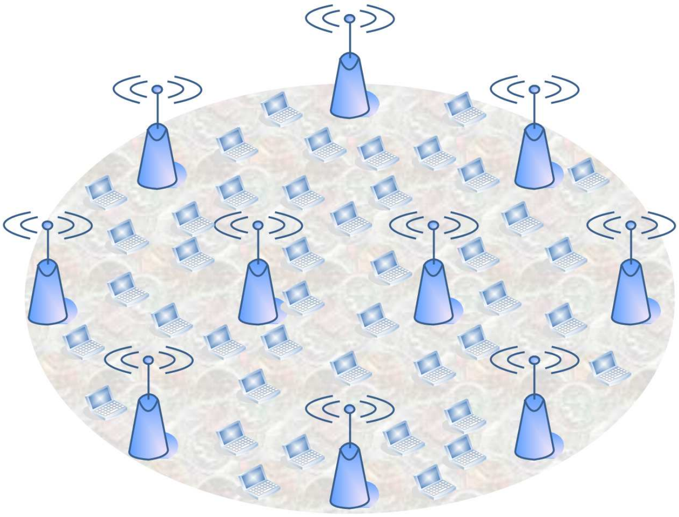


Figure 5.4: First Scenario used in Evaluation Experiments

5.6.2 Users Traffic

Both synthetic and real WLAN traces are used in the evaluation process. Evaluation using synthetic traces gives intuition about how the performance gain varies with different parameters. Simulations with realistic traces provide the knowledge of how really the performance of the policy looks like if it is deployed in a realistic network. Realistic

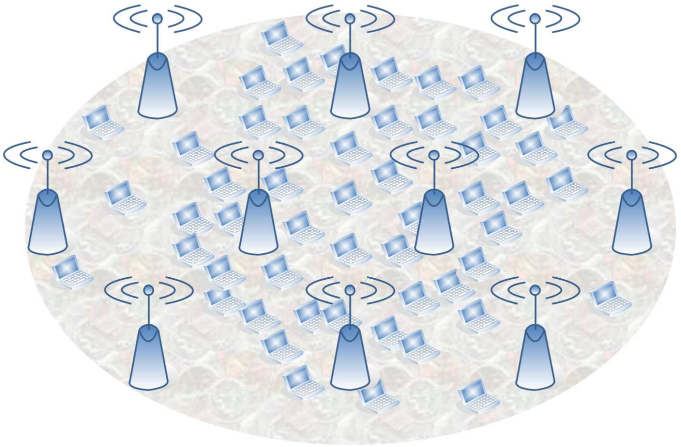


Figure 5.5: Second Scenario used in Evaluation Experiments

SIGCOMM 2001 and SIGCOMM 2004 WLAN traces (available from [53]) are used in the following way: Using CoralReef Software [54], users' flows are first extracted from the dump file. Then, the flows of users during 1 hour are selected. We used the total number of bytes, number of packets of each flow to characterize a user load and compute an average packet length. Then, the **stg** tool which comes with the NCTUns simulation package is used to emulate users' flows.

5.6.3 Evaluation Results

In this section, the simulation results of the proposed AP selection mechanism will be presented and discussed. First, we present and discuss results with synthetic traffic. Then, we present the evaluation results of the selection schemes with real WLAN traces.

Goodput with Saturated Synthetic Downlink Traffic

Let us initially consider the case of saturated downlink traffic. We are interested in comparing the aggregate goodput performance of the static selection policy presented in this chapter with the ones proposed by Fukuda [29] and Kaufmann [39]. We have included both policies in the simulator. Fukuda's approach bases AP selection on the loss rate due to channel errors (i.e. BER) and the number of STAs already associated to an AP. On the other hand, Kauffmann's approach bases AP selection on the instantaneous physical transmission rate and the fraction of time for which an AP acquires the channel for its transmission, assuming that channel contention is among APs. Simulation results are shown in figure 5.6. Because there is relatively low interference from users (only ACKs) in this scenario, we observe that the policy proposed in this chapter is just 6% better than the policy of Kauffmann and 21% better than the RSSI-based approach. The differences between the results here and the improvements published in [29] and [39] are simply due to a different scenario choice.

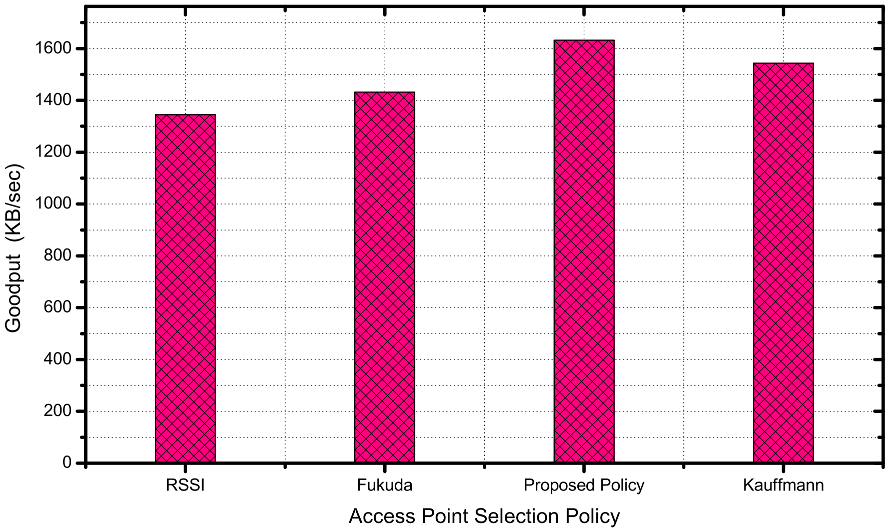


Figure 5.6: Performance comparison of AP Selection policies with saturated downlink traffic for 50 users.

Goodput with Synthetic Uplink Traffic

Now the goodput performance of the static selection policy is compared with the RSSI-based and Fukuda's schemes with synthetic uplink traffic and different load levels for the two scenarios discussed in section 5.6.1. Figure 5.7 compares aggregate goodput performance of the RSSI-based, Fukuda's [29] and the proposed AP selection policies under different uplink CBR UDP traffic loads when the network accommodates 50 users. Figure 5.8 shows the aggregate goodput achieved with the three policies as a function of the number of users. We make the following observations on these results:

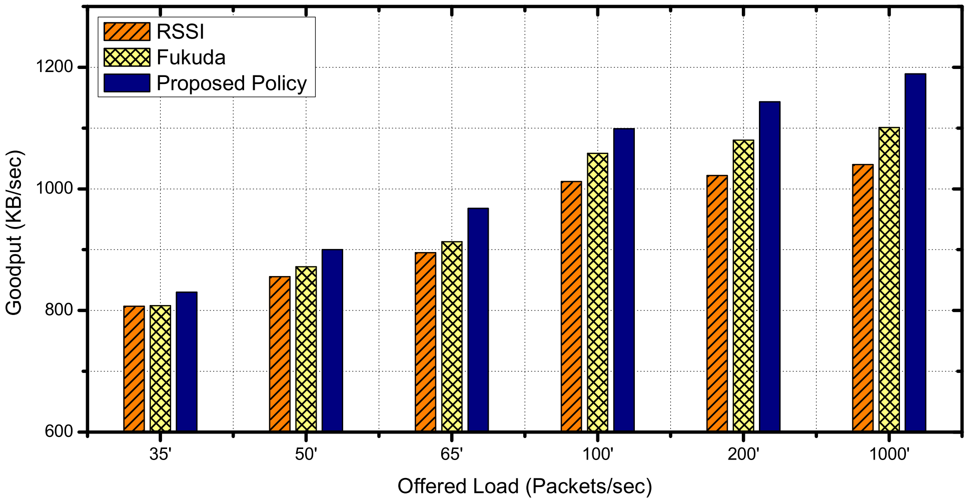


Figure 5.7: First Scenario: Goodput Performance of uplink CBR traffic from 50 users for different offered loads.

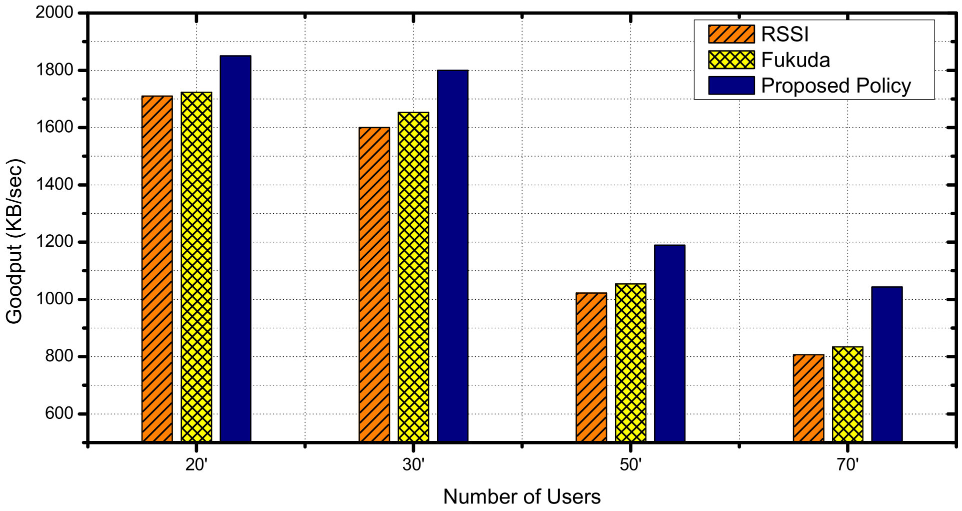


Figure 5.8: First Scenario: Goodput Performance of different AP selection policies with saturated uplink UDP traffic for different number of users.

- In general, the approach proposed in this chapter outperforms the other two approaches especially with heavy load as it tries to avoid possible collisions due to interference.
- Under low load, the performance of the three polices is comparable. This is due to the fact that the MAC will have some time to retransmit a lost packet before the next comes from upper layers, when the load is quite low. Actually, this observation advocates the necessity of considering user's activity. A user that does not intensively inject packets into the medium should not be counted as interferer.
- As the proposed policy guides a user to avoid an AP that is reached by other interfering users, figure 5.8 reveals that the achieved gain improves as the number of users increases (29% with 70 users).

Figure 5.9 compares the goodput performance of the proposed policy with other policies for the second scenario. Since Fukuda's algorithm considers the number of users in it's decision metric, it also pushes many users to the far APs and consequently achieves good gain. However, the results show that more gain can be achieved if STAs select their APs with the metric derived in this chapter.

Impact of AP Selection on Packet Collisions

As the interference leads to packet collisions, it is interesting to investigate the impact of the proposed AP selection policy on the percentage of collided packets. We log the ratio of total packets dropped by the MAC due to collisions to the total number of received packets. This ratio, computed over all APs, is plotted in figure 5.10 as a function of number of users. The figure shows that the percentage of packets dropped due to collision has been reduced when the proposed AP selection policy is used. This

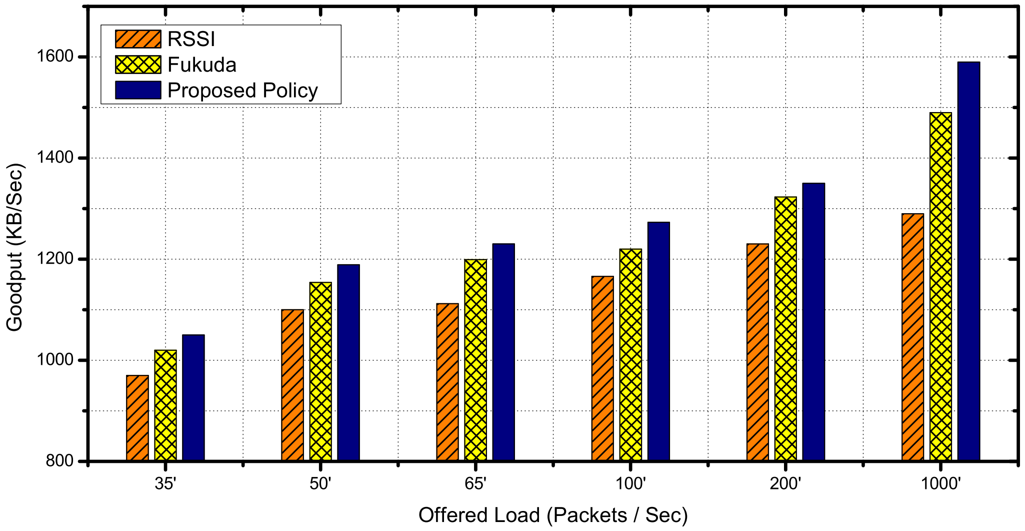


Figure 5.9: Second Scenario: Goodput Performance of uplink CBR traffic from 50 users for different packet inter-arrival time and different selection policies

gain increases as the number of users the WLAN accommodates increases. Additionally, the percentage of dropped packets is found also to be less with Fukuda's AP selection policy, as it considers the number of users in a BSS in its selection metric. Nonetheless, the results show that even both AP selection policies are able to reduce the collision rate, the rate is still high and further mitigation of interference is essential, especially for dense deployments.

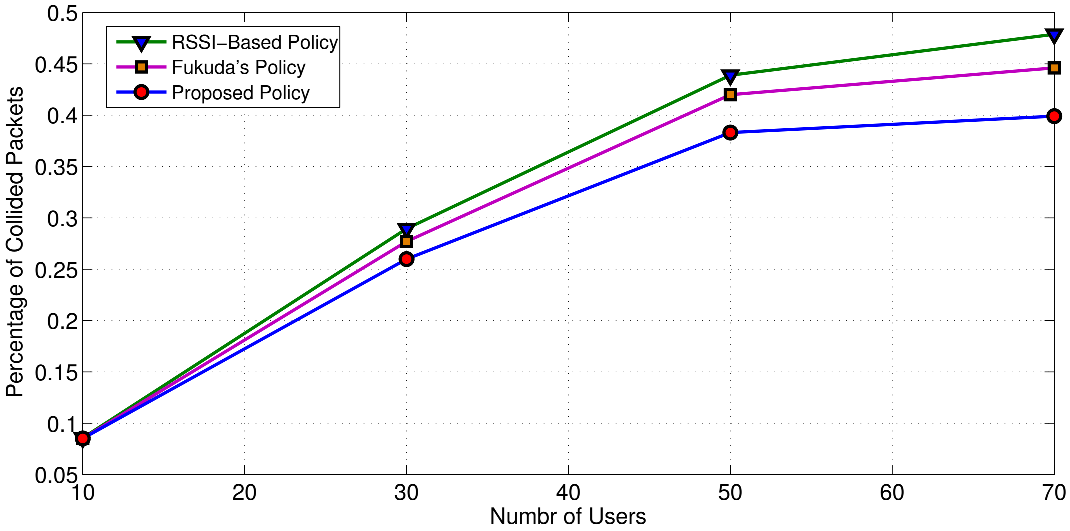


Figure 5.10: First Scenario: Percentage of Collided Packets for different number of users.

Real WLAN Traces

In this part, we present the simulation results of the experiments carried out with realistic WLAN traces from SIGCOMM 2001 and SIGCOMM 2004 conferences. Again we present the results for the two scenarios described in section 5.6.1.

Figure 5.11 plots the goodput performance for the first scenario, whereby STAs are

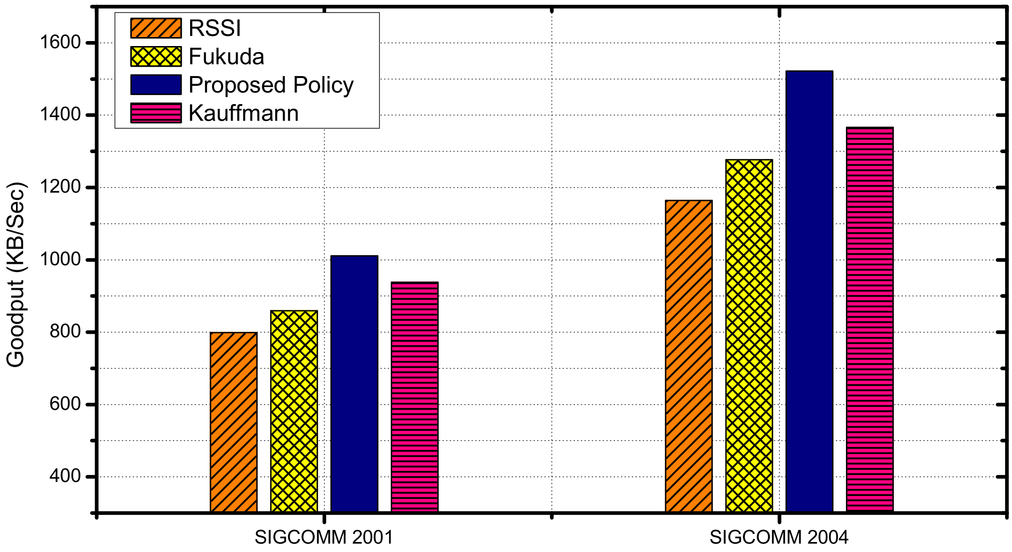


Figure 5.11: First Scenario: Goodput Performance Comparison of AP Selection Policies with realistic WLAN Traces.

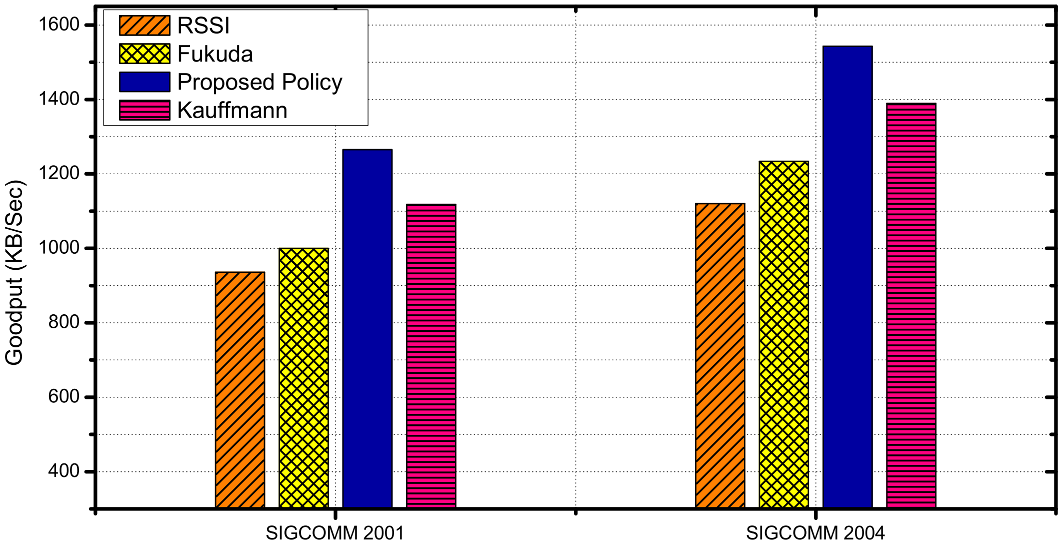


Figure 5.12: Second Scenario: Goodput Performance Comparison of AP Selection Policies with realistic WLAN Traces.

randomly distributed across APs coverage area. Figure 5.12 plots the goodput performance for the second scenario, whereby most of STAs are concentrated around 5 APs and few are located across the coverage area of the other APs. The figures compare the aggregate goodput performance between the AP selection policy proposed in this chapter, RSSI-Based, Fukuda's policy and Kauffmann's policies.
It follows from these figures that the proposed policy outperforms the others. In addition, the goodput performance of Kauffmann's policy outperforms Fukuda's policy with the realistic traffic.

5.7 Conclusions

The legacy AP selection policy implemented currently in IEEE 802.11 WLANs adapters does not effectively utilize WLAN resources as it ignores important parameters that determines the QoS. To reduce the interference at the selection phase, this chapter proposes an improved AP selection policy for 802.11 WLANs. The proposed policy takes care of both Intra-BSS and Inter-BSS interference as well as the anomaly problem of 802.11. The metric used in the selection encapsulates several BSS and connection parameters into a single value. Simulation results with both synthetic and realistic traffic show that the proposed AP selection policy can reduce the interference impact and enhance network goodput, especially under high load and uneven STAs distribution across the coverage area of APs. Nonetheless, the results show that the interference is just partially reduced and further interference mitigation strategies are still needed.

Chapter 6

Improving the Setting of RTS/CTS in Multi-Rate Multi-BSS 802.11 WLANs

6.1 Introduction

Within the interference mitigation framework of this thesis, the WLAN first considers tuning the RTS/CTS mechanism to improve the operational conditions if high interference is detected and the cause is hidden nodes. Otherwise, the network will consider a change of channel access scheme and start operating using a time slotted access scheme rather than the CSMA/CA as will be explained in the next chapter. In principle, the RTS/CTS is expected to be helpful:

- If detected interference is due to existence of hidden nodes in the network.
- If the wasted channel time due to collisions is high.
- If the usage of RTS/CTS by some nodes in a BSS do not negatively impact other nodes, including those belonging to neighboring BSSs in multi-BSS deployments.

As mentioned in section 4.2, the 802.11 standard combats interference resulted from the hidden node problem by specifying an optional handshake protocol at the MAC layer, the RTS/CTS protocol. Despite the standard suggests to use the RTS/CTS for large packets, it does not recommend any specific threshold value and the decision is left for the vendors and even for the end user in some productions.

Numerous algorithms have been proposed in the literature for controlling the RTS/CTS mechanism. However, most of them have been assessed through observation of the total throughput performance in the WLAN. Since the optional usage of an RTS/CTS signaling by some node(s) may impact the performance of its potential neighbors, individual users' perspectives are essential to be considered while assessing any RTS/CTS tuning algorithm. One user may be negatively influenced if RTS/CTS is signaled by some other user(s) even if this improves the total throughput of all users. On the other hand, some user could experience throughput improvement even if the total throughput degrades. Therefore, the question whether the usage of RTS/CTS is beneficial or not is scenario dependent. Additionally, most of the previous investigations on the effectiveness of RTS/CTS have used similar transmission rates for all users. Since the collision duration and re-transmission time depend on the used transmission rates for data packets, the impact of collisions and re-transmissions on self and other users depends on the individual employed physical rates and not only on the size of retransmitted packets as the 802.11 standard suggests.

This chapter aims at two aspects:

- First, two criteria for improving the setting of the RTS/CTS signaling are studied. The first is based on number of detected hidden node pairs in a BSS. The second is a collaborative criterion which bases the decision on QoS measurements within overlapping BSSs.

- Second, it will be shown that RTS/CTS control criteria shall be evaluated in multi-rate environment.

6.2 State of the art

The RTS/CTS protocol has been an attractive issue for many researchers. Reference [67] has studied the effect of the hidden node problem on the performance of 802.11 Adhoc WLANs. The results have shown that the RTS/CTS mechanism improves the WLAN throughput as the number of hidden node pairs exceeds 10% of the total number of node pairs. The impact of the RTS threshold on the performance of 802.11 MAC protocol in Adhoc networks has been investigated in [90]. The authors conclude that the number of nodes that share a channel is the factor that RTS threshold should be based on and not only the packet length. Nevertheless, the study recommends to always enable RTS/CTS. The work in [56] analyzes the throughput performance of 802.11 DCF with RTS/CTS in multi-hop Adhoc networks. A hidden node mitigation algorithm for infrastructure WLANs has been proposed in [57]. Under the assumption that APs which operate over the same channel do not hear each other, the authors recommend to use RTS/CTS just if APs transmit to the nodes that lie in the overlapping areas of APs to avoid collisions in these areas. In addition to the weak assumption of [57], the algorithm has been tested in specific network configuration regarding APs and nodes placement. Reference [58] presents a real time algorithm for updating the RTS/CTS threshold to enhance the performance of IEEE802.11e WLANs that employ the EDCA MAC protocol. The main result was a recommendation to update the RTS threshold according the number of transmission attempts as well as the number of nodes in the BSS. Another study on the self-tuning of RTS/CTS can be found in [59]. The setting of the RTS threshold depends on delay estimations. Also, the work in [60] proposes a dynamic mechanism for setting the RTS/CTS threshold based on estimation of successful transmission probability of packets. The main shortcoming of [58],[59], and [60] is that the decision wether to use RTS/CTS or not depends on packet loss rate which in fact depends on wireless channel conditions and not only on interference from other nodes. The impact of RTS/CTS mechanism on throughput performance has been investigated in [61]. The results have shown that the mechanism might block some successful transmissions in the network. However, the study and the analysis were limited to specific configuration of two APs and three nodes. A further study on the impact of RTS/CTS on transmissions is published in [62]. The paper concluded that the problems introduced by RTS/CTS can sometimes be more than its positiveness in solving the hidden node problem.

6.3 Improved tuning of RTS/CTS

6.3.1 Intuition

Basically, the 802.11 standard defined a manageable parameter called *RTSThreshold* which determines when the RTS/CTS handshake should precede a packet. Different vendors have different control algorithms of the *RTSThreshold*. Nevertheless, the different values never impact interoperability of devices.

From the discussion in section 6.2, one sees different conclusions of research activities. While some studies concluded that the RTS/CTS should be enabled, some others recommended to disable it. As a matter of fact, the different views are due to the differences in the scenarios considered regarding network topology, traffic pattern, modulation, and evaluation metrics. Almost in all the work discussed in section 6.2, the total throughput has been used as the performance evaluation metric. Individual perspective of users, the fairness among them have not been considered. Although a maximum aggregate throughput is an important goal, the impact of RTS/CTS mechanism on individual users is also of significant important, since the usage of this mechanism is optional. It could happen that certain management policy much improves the throughput of some users but degrades the throughput of many others. If one just observes the aggregate throughput, the impression would be that the algorithm is a good and efficient one but the fact could be that many other users become less happy with the new settings. This is due to the fact that the performance depends on many correlated factors like: The physical transmission rates, the number of users, the traffic characteristics, the location of users in the BSSs, and interference from neighboring BSSs. In some cases, enabling RTS/CTS might be useful albeit with packets of moderate lengths despite the overhead it adds. Also, there exist some cases, where RTS/CTS should be turned off.

To this end, the impact of RTS/CTS on individual users and the overall performance is very much scenario dependent and is a function of numerous parameters. This should actually drive any RTS/CTS control criterion.

6.3.2 RTS/CTS in Multi-Rate WLANs

In principle, the intuition behind the RTS/CTS packet length threshold defined in 802.11 standard is that long packets consume long time if retransmitted due to collisions of hidden nodes' transmissions. In a multi rate WLAN, this time is however a function of both packet length and the used transmission rate for data packets. Therefore, a better threshold that considers both parameters shall be defined. A node can easily anticipate the physical rate of the next packet from the recent history.

A common shortcoming of the cited work in section 6.2 and even some recent ones like [63, 64, 65] is the assumption of similar transmission rates of data packets for all nodes. The focus has been devoted to investigations of RTS/CTS impact on the achieved throughput since these handshake packets are transmitted using lower rate than data packets transmission rate. ***Since the cost of collisions depends on the used data rates, the efficiency of any algorithm that reduces the collision rate should be investigated in a multi-rate environment.*** Note that the required time for re-transmitting a packet at 1Mbps is 11 times greater than transmitting the same packet at 11Mbps. Therefore, re-transmitting small packets (after collisions) at lower rates may consume considerable bandwidth and will indeed impact other users that employ high physical rates negatively due to the long collision time periods, i.e worsening the well known Anomaly Problem [8]. ***Thus, reducing the collisions and consequently re-transmissions at low physical rates is expected to improve the performance of high rate users which can not be observed when all users employ the same transmission rate.***. Reference [66] discusses this issue in details.

6.3.3 Tuning RTS/CTS in a BSS based on Number of Hidden Node Pairs

A first criterion proposed here is to control the RTS/CTS based on the number of hidden node pairs in a BSS covered by an AP. The intuition behind this criterion is that the RTS/CTS is expected to be useful if hidden nodes do really exist in the network despite the overhead it adds. In [67], it has been shown that the performance of 802.11 CSMA/CA protocol drops sharply when the number of hidden node pairs exceeds 10 percent of the total number of node pairs. We make use of this finding as part of the RTS/CTS tuning criterion as follows: First, each BSS has to detect the hidden nodes pairs. Then, the AP instructs only those detected hidden pairs within its BSS to use the RTS/CTS signaling before data packet transmission if they are more than 10 percent of the total number of nodes within a BSS. By this, it will be possible for the AP to locally reduce interference due to local hidden nodes and consequently improve communication quality within its BSS without the involvement of other BSSs in the neighborhood. Hereafter, we refer to this criterion as "Criterion-1".

A challenging requirement for the above criterion is the detection of hidden node pairs. We use the following approach which benefits from the standardized reports defined in the IEEE 802.11k standard as well as the interference measurement approaches proposed in chapter 4:

- Each node monitors all transmissions in the BSS (using promiscuous mode of operation), it reports the average power received from each address to its AP.

The IEEE 802.11k standard specifies the mechanisms that allow STAs and APs to exchange this information.

- The AP then constructs an Interference Map from which it determines the set of hidden node pairs by correlating the information received from nodes.
- Two nodes in a BSS are assumed to be hidden from each other (hidden pair) if both do not hear each other.

The main drawback of this detection approach is its dependency on packet decoding ability. Note that a node may sense a busy medium due to a packet transmission by others despite inability of decoding the bits of this packet. This means that the detection process may identify some nodes to be hidden although they are not. This shortcoming can be alleviated if the AP uses interference map information jointly with source addresses of collided packets in order to improve the accuracy of the detection process. This can be achieved by observing and memorizing the MAC header of corrupted packets due to collision. In section 4.3, it has been shown that this is likely possible in case of collisions due to hidden nodes since the header of a packet that arrives first is likely to be correctly received and decoded. Therefore, if a packet header (300μs) is correctly decoded but the packet is judged to be corrupted due to collision, the sending node of this packet is likely to be hidden from some other node(s). i.e. the AP can have a list of addresses of hidden nodes within its BSS. We refer to this approach as the combined algorithm for detecting hidden node pairs. The algorithm takes the following form:

Algorithm 3 Combined Hidden Node Detection

```
for i = 1 to N do
    for j = i to N do
        HIDDEN[i][j]=0;
    end for
end for
INPUT: MAP[N][N];            /*Interference Map Matrix for N nodes*/
INPUT: COLLISION[N];         /*A List of detected hidden nodes through source
    address observation of a corrupted packets due to collision*/
OUTPUT: HIDDEN[N][N];    /*Hidden Pair Matrix*/
for i = 1 to N do
    for j = i+1 to N do
        IF (MAP[i][j]=0 AND MAP[j][i]=0 AND i ∈ COLLISION AND j ∈ COLLI-
        SION)
                    HIDDEN[i][j]=1;
    end for
end for
```

6.3.4 Collaborative tuning of RTS/CTS

In multiple-AP deployments, hidden nodes may belong to multiple BSSs. Additionally, neighboring BSSs may influence the operation of RTS/CTS. The usage of RTS/CTS by some nodes in a BSS may impact other nodes belonging to neighboring BSSs. To illustrate this, consider the two BSSs in figure 6.1. According to the 802.11 standard, User 2 will not be able to respond to the RTS sent by its AP 2 until the exchange of data and ACK between User 1 and AP 1 completes. However, the RTS from AP 2 will mislead users 3 and 4 which think that a data transmission is taking place and hence prevented from accessing the channel (even if no nearby user is transmitting). Consequently, this causes throughput degradation if User 3 and/or User 4 have packets to upload. We simulated this example and plot the aggregate network goodput in figure 6.2. Despite that only APs use RTS/CTS to deliver packets of users 1 and 2, the figure shows that the aggregate goodput has substantially degraded regardless of the offered load.

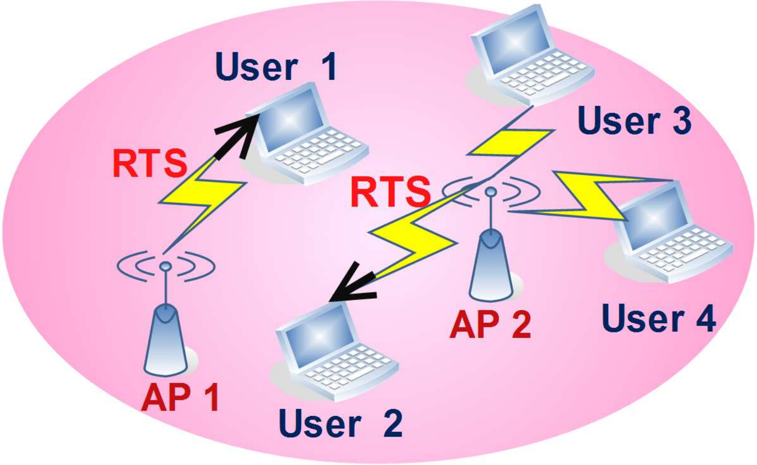


Figure 6.1: Negative influence of RTS/CTS in Multi-Cell WLANs

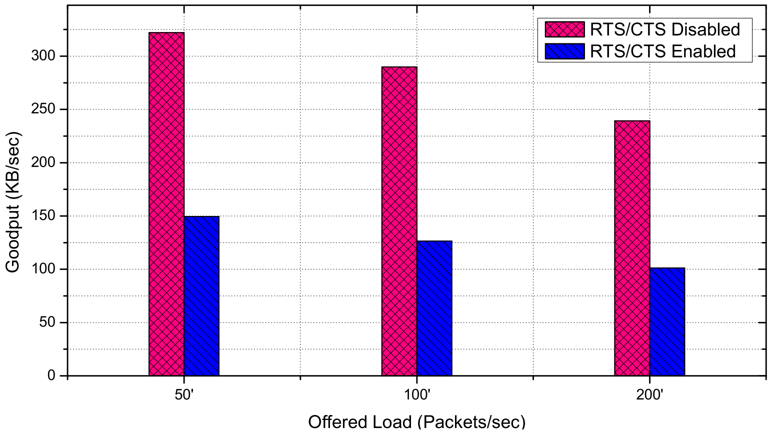


Figure 6.2: Aggregate Goodput for the network topology of figure 6.1

Therefore, local decisions by individual BSSs may not be sufficient and a joint decision on the setting of RTS/CTS is necessary. This is especially needed when hidden nodes do not belong to the same BSS and traffic is sent in both directions (i.e. Uplink and Downlink). In this section, a collaborative approach for the setting of RTS/CTS is proposed. The motivation for the collaborative criterion we present in this section is the very high dependency of the achieved performance with or without RTS/CTS exchange on the scenario (i.e number of hidden node pairs across the BSSs, interference from neighboring BSSs, users' traffic characteristics, who sends to whom, and activity levels, etc.) and the complexity of inferring this performance apriori.

With the collaborative approach and based on some policy, neighboring BSSs that operate over the same channel decide jointly wether their users should use RTS/CTS based on QoS measurements as follows:

- Each AP in a BSS shall instruct the nodes it accommodates to disable RTS/CTS, observe, measure and quantify their current QoS for some time period T. The period T shall be long enough for better capture and characterization of the traffic. In the evaluation experiments presented in section 6.5, a period of 5 seconds has been used.
- At some time instant, all nodes shall use RTS/CTS prior data packets and start to observe their QoS for another testing phase of length T.
- At the end of the test period, nodes report the QoS measurements to their respective APs. Measurements of each node may be concluded in one number.
- APs share measurement information or their local recommendations based on the testing phase results.
- One AP processes the measurements and decides whether RTS/CTS shall be used based on probable improvement in the QoS after using the RTS/CTS mechanism. The decision is then signaled to other BSSs which distribute it to the users.
- After some time period, the current status of RTS/CTS is inverted and the testing takes place.
- In order to avoid excessive signaling and processing, the periodicity of the testing phase can be adaptively selected based on difference between the most recent decision and the previous one. In the evaluation experiments, the period has been doubled when two similar decisions are successively made, but halved if the next decision is found to be different than its predecessor.
- The potential QoS metrics for the decision could be: goodput, delay, fairness or a combination of them. In the evaluation experiments presented in section 6.5, a new setting (either Enable or Disable RTS/CTS) takes place if found to improves the overall goodput by at least 10%.

Hereafter, we refer to the collaborative criterion as "Criterion-2".

6.4 Usage of the RTS/CTS control criteria within the interference mitigation framework

In this section, we show how the criterion proposed for controlling the RTS/CTS signaling will be used within the interference mitigation framework we suggest in this thesis.

- If diagnoses reveal that performance degradation is due to packet collisions from hidden nodes belonging to the same BSS, the detected hidden node pairs are instructed locally by their AP to use the RTS/CTS.

- If the performance degradation is resulted from hidden node pairs across overlapping BSSs, then the network uses the collaborative criterion, trying to mitigate mutual interference.

6.5 Performance Evaluation of the proposed RTS/CTS tuning criteria

This section evaluates the goodput performance of the proposed criteria for setting RTS/CTS parameter through simulations as well as some real experiments. The simulation scenario is comprised of 10 APs that use the same channel and provide services to users that reside within their coverage area. The configuration of simulation parameters is similar to the one described in section 4.3.4. The setup of the real experiments is described in section 6.5.4. Both synthetic and real traces are used in the evaluation process. The real traces are used as described in section 5.6.2.

6.5.1 Hidden Nodes Detection

We start investigating the results of the proposed hidden node detection approach that is based on power level measurement of all received packets during an observation interval. We also examine the impact of the usage of source addresses of corrupted packets due to collisions on the detection accuracy (Algorithm 3). The results of the experiments are plotted in figure 6.3. The x-axis represents the length of observation period. For the counting of true hidden nodes, two nodes are assumed to be hidden if neither measures from the other a signal of power level greater than the Carrier Sense Power Threshold (CSPTh) set to -100dBm. The results show that the combined detection approach (Algorithm 3) provides better accuracy in terms of percentage of correct detection decisions. This is because, it filters some of the nodes that are outside the decoding range of a measuring node and hence considered hidden, while in fact they are not (within the Carrier Sense Range). Additionally, the results reveal that the accuracy starts to stabilize if the length of the observation period exceeds about 3 seconds.

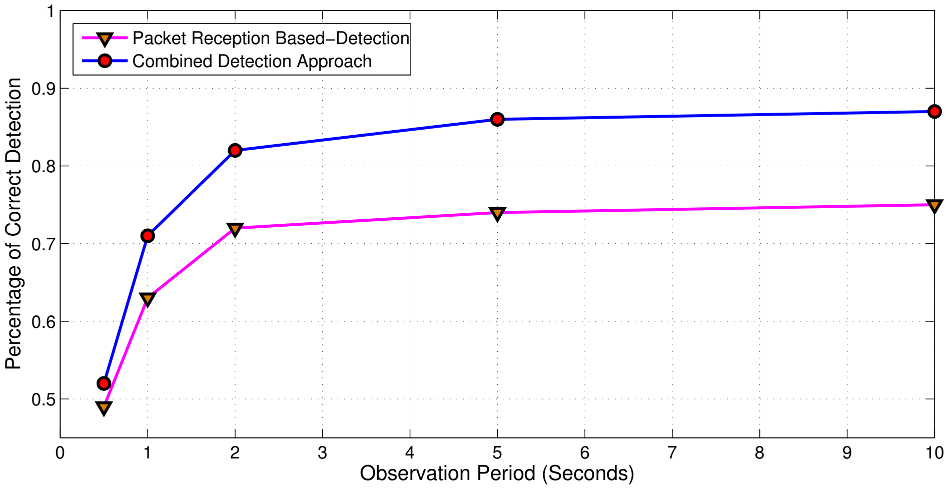


Figure 6.3: Performance comparison between the Packet Decoding based hidden node Detection and the Combined Hidden Node Detection.

6.5.2 Simulation Results with Synthetic Traffic

A) RTS/CTS Efficiency is scenario dependent

We firstly distribute 100 users randomly in small areas around the 10 APs assuring that no hidden nodes exist within each BSS. Users send CBR UDP data packets to a server through a switch connected to all APs. The sending rate in this experiment is 100 packets/second. Figure 6.4 plots the aggregate goodput of all users with large packets. The figure shows that even for large packets the goodput performance may significantly degrade with RTS/CTS enabled. This is due to the absence of hidden nodes in this configuration and consequently the low collision rate. Hence, algorithms that suggest to always enable RTS/CTS may sometimes degrade the system performance even with large packets.

B) Impact of Hidden Nodes on Goodput Performance

In this section we study the impact of hidden nodes on the goodput performance in multi-BSS multi-rate 802.11 WLAN. We investigate the efficiency of the RTS/CTS mechanism for mitigation of interference resulted from hidden node pairs. In particular, we would like to understand how does the usage of RTS/CTS impact the network goodput for different network topologies that differ in the percentage of hidden pairs. In these experiments 80 users have been considered. They send UDP packets to their APs. Nodes i and j are counted as hidden pair if they are outside the CS of each other and the transmission of at least one interfere the transmission of the other, despite they transmit to different APs. Experiments have been conducted for two cases: In the first case, users use the basic access mode (CSMA/CA), while in the second case they use CSMA/CA with RTS/CTS.

Figure 6.5 plots the gain in goodput if RTS/CTS is used for different percentage of

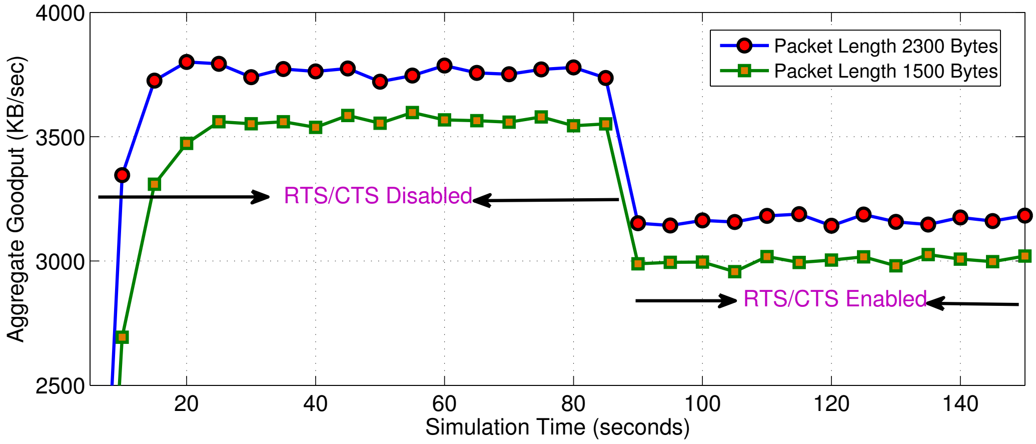


Figure 6.4: Aggregate Goodput Performance of all users for large packets and 100 Packets/sec offered load.

hidden node pairs (α) and different packet sizes. The Y axis represents the percentage of increase or decrease in the goodput when RTS/CTS is used. The reported results

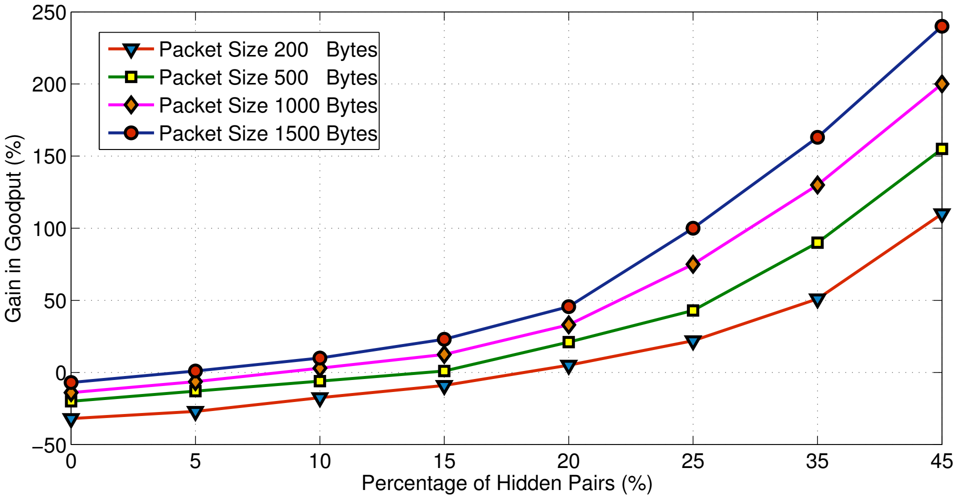


Figure 6.5: Impact of RTS/CTS with different level of hidden pairs and packet lengths.

show that:

- Although the gain in throughput with RTS/CTS highly depends on the packet size, this gain is positive only if the percentage of hidden nodes is above a threshold. Otherwise, the usage of these handshake packets highly degrades the aggregate goodput. This means that the usage of the mechanism shall be considered only if the network detects a large number of hidden node pairs.

- The percentage of hidden node pairs (α), above which positive gain is achieved (threshold) depends on the packet size. For example, for 1500 Bytes packets, the gain in goodput starts to be positive if at least 5% of node pairs are hidden. However, for 200 Bytes packets, the RTS/CTS improves the goodput only if at least about 20% of node pairs are hidden.

Let us now focus on the case of large packets (1500 Bytes). In figure 6.6, we plot the gain in goodput achieved for different percentage of hidden node pairs and traffic load. The figure shows that in addition to the packet length and the existence of hidden pairs, the gain in goodput does also depend on the amount of traffic users inject in the network. In particular, under high load conditions, the usage of RTS/CTS improves the gooput gain as the number of hidden pairs increases. However, under low traffic conditions, the gain is marginal. On the other hand, in the absence of hidden nodes, the usage of the RTS/CTS starts degrading the goodput as traffic load increases.

In fact, these results advocate the collaborative criterion which decides on the usage of the RTS/CTS mechanism based on measurements. This is due to the reason that the gain with the mechanism is scenario dependent and difficult to be anticipated.

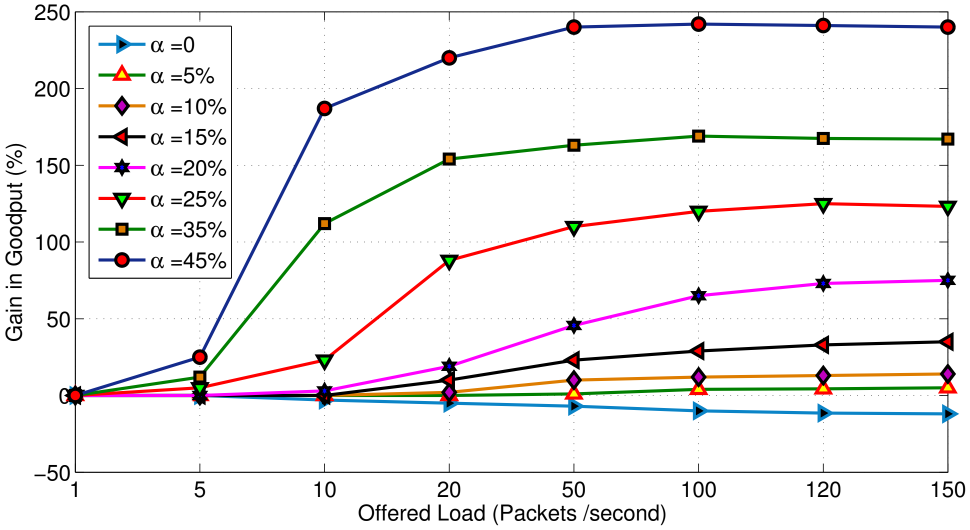


Figure 6.6: Impact of RTS/CTS for different level of hidden pairs and load.

C) Performance of Proposed Criteria

Now we deeply study the goodput performance of **Criterion 1** and **Criterion 2** (proposed in section 6.3. We compare their performance with three cases proposed in the literature: always enable RTS/CTS, always disable RTS/CTS, and enable RTS/CTS for packets above an RTSThreshold. For the last case, we select a moderate RTSThreshold of 700 bytes, which also has been found to achieve good performance improvement for comparable STAs density in [59]. With the collaborative criterion (**Criterion 2**), APs that operate over the same channel instruct their users to enable/disable RTS/CTS if the new setting (during testing) improves the overall goodput by at least 10%. In this experiment, STAs are randomly and uniformly distributed across the coverage area of

APs. STAs transmit CBR UDP data packets of different lengths drawn from a uniform distribution with 200 and 1500 bytes minimum and maximum respectively. In a first experiment, the offered load is varied and the number of users is fixed to 80 users, where many of them were found to be hidden from each other.

The aggregate goodput performance for this experiment is plotted in figure 6.7. In a second experiment, the number of users is varied and the offered load is fixed at 100 Packets/s. We plot the aggregate goodput achieved with this experiment in figure 6.8.

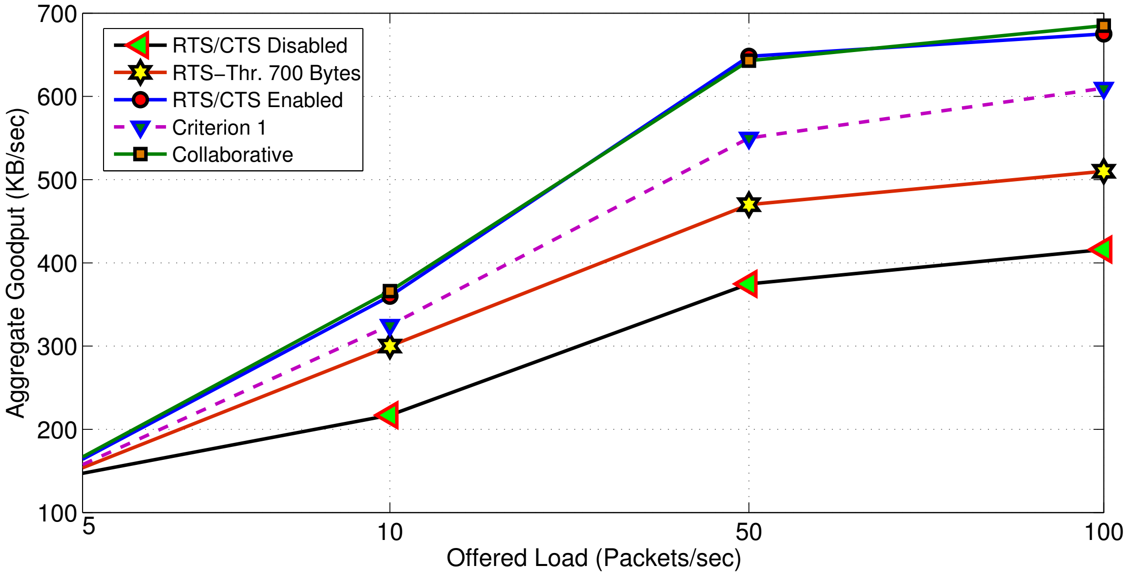


Figure 6.7: Goodput Performance Comparison between different RTS/CTS setting criteria.

We make the following observations on the achieved results:

- At low traffic load, enabling or disabling RTS/CTS has no significant impact on the goodput. This is because the collision probability is lower and MAC has time to retransmit a collided packet. Addionally, the RTS/CTS is not an overhead in this case. Thus, it does does not degrade goodput if it precedes data packets.
- As the load increases, the collision rate increases. In this case, always using RTS/CTS becomes a better choice.
- With low number of contending users and due to the decreased collision rate, the usage of RTS/CTS degrades the goodput performance. However, as the number of users increases and due to possible increased hidden nodes and collisions, the usage of RTS/CTS starts to be helpful even if always used for any packet size.
- The collaborative criterion always achieves either similar or better goodput than the CSMA/CA without RTS/CTS. This is because users are only instructed to use the RTS/CTS if found to improve the aggregate goodput.

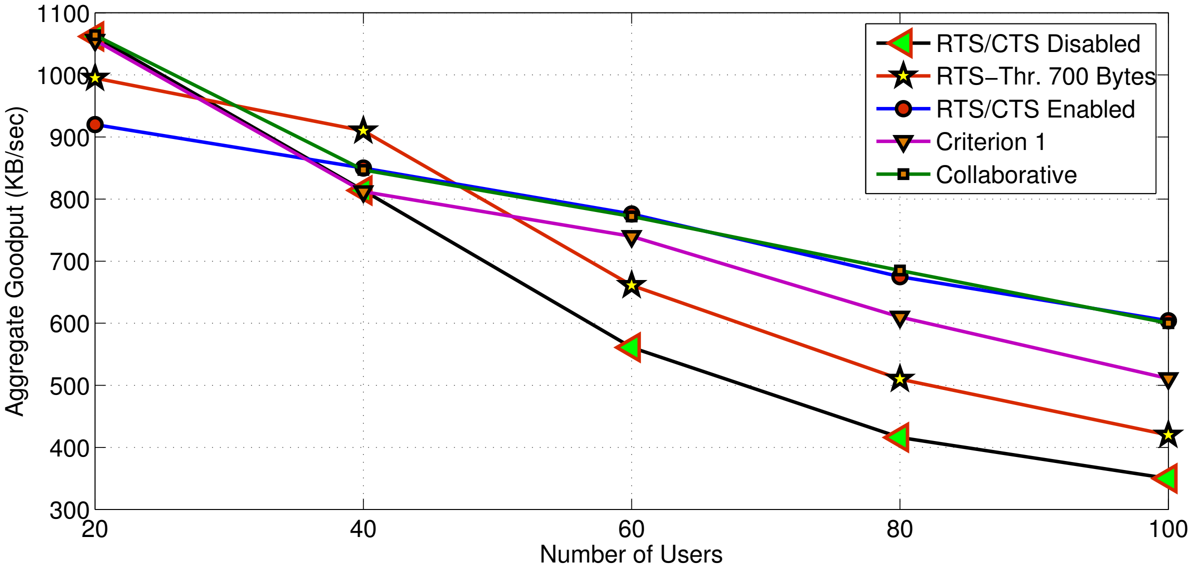


Figure 6.8: Goodput Performance Comparison between different RTS/CTS setting criteria.

- Criterion 1, by which each AP locally detects its hidden node pairs within its BSS and instructs them to use RTS/CTS if found to be greater than 10 % of the number of node pairs in the BSS, achieves a better goodput performance than the case where RTS/CTS is always disabled or always enabled if packet length exceeds 700 bytes.
- With all assessed criteria, the goodput fairness index has been found to improve by at lest 17% over the case when the RTS/CTS was always disabled.

D) Impact of RTS/CTS settings on Packet Collision Rate

One interesting issue to study is the impact of RTS/CTS settings on the packet collision rate. The configuration is similar to the previous experiment in **C)**, wherein 80 users are randomly uniformly distributed across the coverage area of APs. The number of dropped packets by the MAC due to collisions are logged for different RTS/CTS settings. In order to study how does AP selection impact the efficiency of RTS/CTS, the experiments have been conducted with the RSSI-based AP selection and the AP selection proposed in chapter 5. The results are reported in figure 6.9 against different values of offered load.

The following conclusions can be drawn from this figure:

- In general, the percentage of collided packet increases as the load increases up to a maximum value that corresponds to the saturation level.
- Enabling RTS/CTS significantly decreases the collision rate which consequently leads to improved goodput as shown in figure 6.7 .

- It can be observed from the reported results that the percentage of collided packets is less if the users select their APs using the proposed AP selection policy discussed in chapter 5. Nonetheless, the difference in collision rate for both RSSI-based and the proposed AP selection policies is a bit smaller if RTS/CTS is enabled. The reason is that the proposed AP selection does also reduce interference resulted from hidden nodes and consequently the gain from using RTS/CTS becomes smaller.

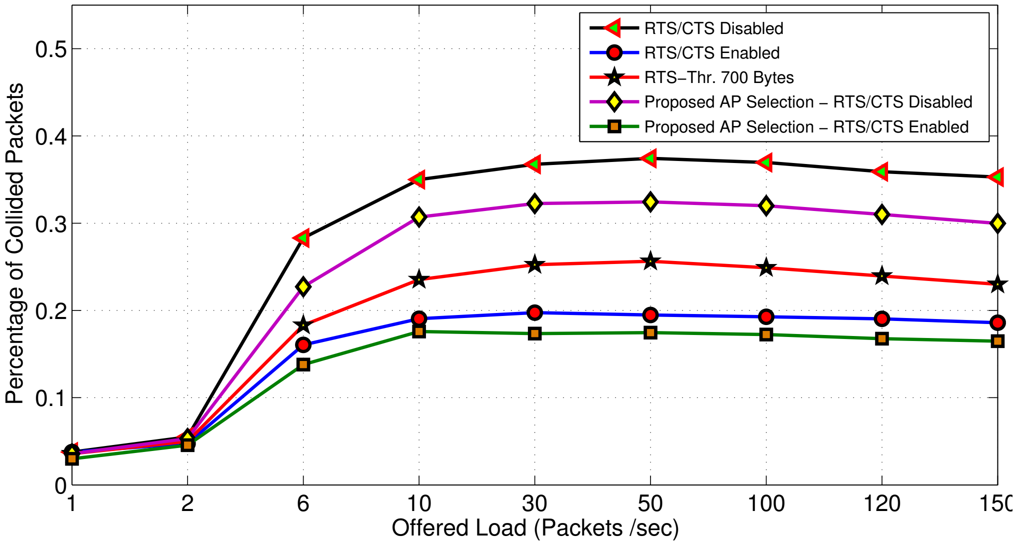


Figure 6.9: Percentage of Dropped Packets due to Collision for Different AP Selection Policies and RTS/CTS settings.

E) Efficiency of RTS/CTS with Downlink Traffic and Hidden Access Points

Another important question that arises in multi-BSS deployments is the efficiency of the RTS/CTS signaling mechanism in mitigating interference resulted from hidden APs in the downlink traffic. In order to investigate this issue, we conducted an experiment in which APs send to the STAs they accommodate CBR UDP data packets of different lengths drawn from a uniform distribution with 200 and 1500 bytes minimum and maximum, respectively. In this configuration, APs are hidden from each other. We compare goodput performance for two cases: In the first case, APs transmit their packets without using the RTS/CTS, while in the second case each data packet is preceded with RTS/CTS regardless of its length.

Figure 6.10 shows the results of this experiment for different levels of offered load. The results reported in this figure are obtained for 80 STAs. The main ultimate result to note is that the RTS/CTS degrades the goodput performance even at high load and despite all APs are hidden. The collaborative approach decides that the RTS/CTS shall not be used. Then, we fixed the packet size to 1500 bytes (i.e. all packets are

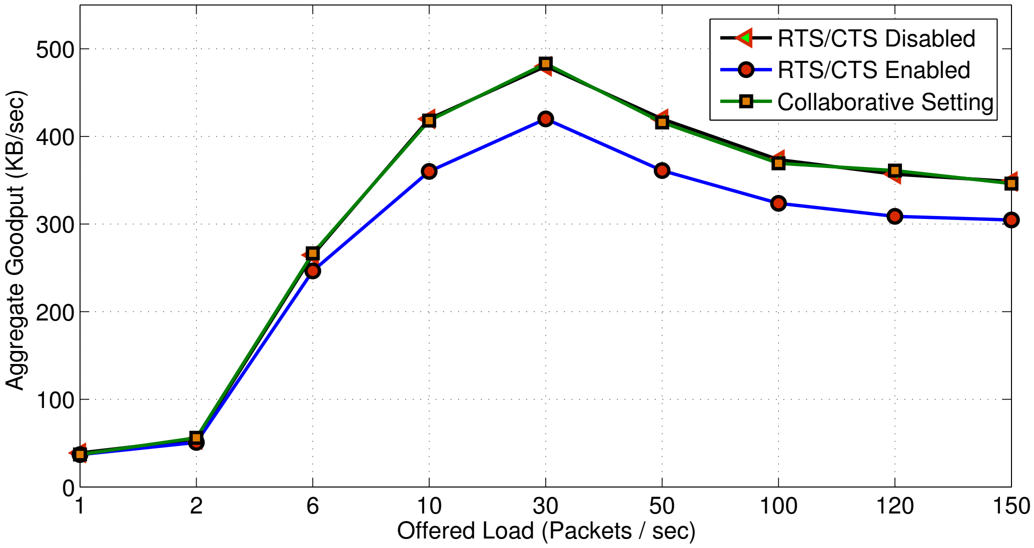


Figure 6.10: Efficiency of RTS/CTS with downlink traffic and hidden APs- 80 Users, Packet size: 200-1500 Bytes.

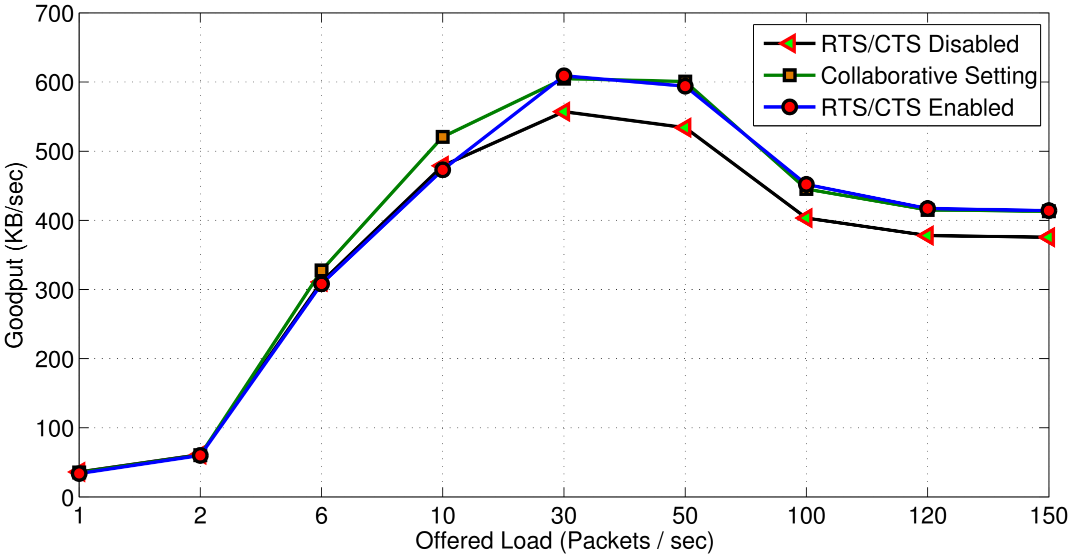


Figure 6.11: Efficiency of RTS/CTS with downlink traffic and hidden APs- 80 Users, Packet size: 1500 Bytes.

long) and repeated the experiment. The results are shown in figure 6.11. In this case, the cost of collision becomes larger and the RTS/CTS slightly improves the aggregate goodput. ***As a result, the RTS/CTS is not sufficient to solve the hidden node problem when APs are the hidden nodes.*** Note that the collaborative approach only decides enabling of RTS/CTS only if the gain is above 10% which occurs when the offered load exceeds 30 packets/sec.

F) RTS/CTS Setting shall Consider Physical Transmission Rates

Now, we show the necessity of evaluating the efficiency of RTS/CTS control criteria in multi-rate environment. In this experiment, users are also randomly and uniformly distributed across the coverage area of APs. We summed the goodput of all users that employed each physical transmission rate and plot the results in figure 6.12. The results show that aggregate goodput of users that use low transmission rate improves significantly when RTS/CTS is enabled. However, the gain in goodput decreases for the users transmitting at high rate if they use RTS/CTS. This result is attributed to the following reason: When a user transmits a data packet at high rate, the RTS/CTS

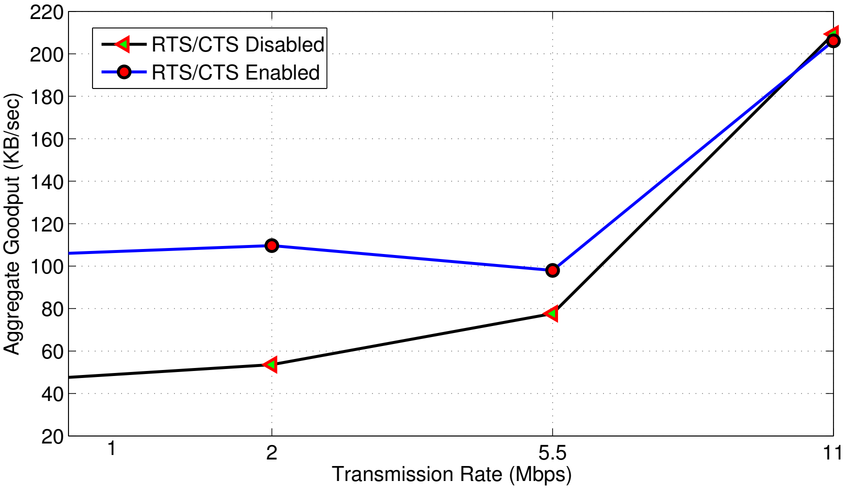


Figure 6.12: Impact of RTS/CTS on Goodput of Heterogeneous Rate Users with 1500 Bytes packets and 100 Packets/sec offered load.

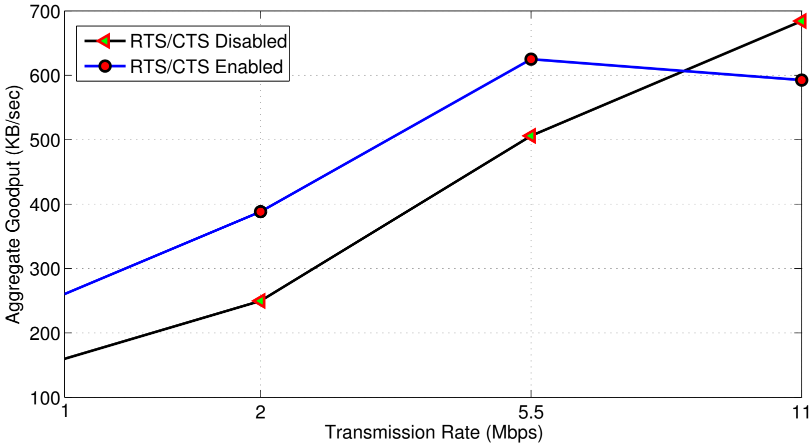


Figure 6.13: Impact of RTS/CTS on Goodput of Homogeneous Rate Users with 1500 Bytes packets and 100 Packets/sec offered load.

which is transmitted at a basic low rate (1Mbps in 802.11b) is an overhead. The RTS/CTS exchange consumes about 544 μs, while the average transmission time required for a data packet (average length 850 bytes) at 11Mbps requires about 808 μs. This means that the RTS/CTS needs 67.32% of data packet time.
Figure 6.13 plots the goodput performance when all users employ a homogeneous transmission rate. The figure shows that when all users employ 11Mbps transmission rate, the goodput performance degrades if RTS/CTS is used. Conversely, the goodput improves considerably if low rates are employed. From these results, we conclude that the employed physical transmission rate by users is an important factor that determines whether the usage of RTS/CTS improves goodput or not. Thus, RTS/CTS control algorithms have to be assessed in multi-rate environments.

6.5.3 Simulation Results with WLAN Traces

In this part we present the results of simulation experiments performed with realistic WLAN traces and focus on the collaborative criterion. In this experiment, users are also randomly and uniformly distributed across the coverage area of APs. Figure 6.14 depicts the goodput with the collaborative criterion for SIGCOMM 2001 traces. Figure 6.15 depicts the goodput with the collaborative criterion for SIGCOMM 2004 traces.

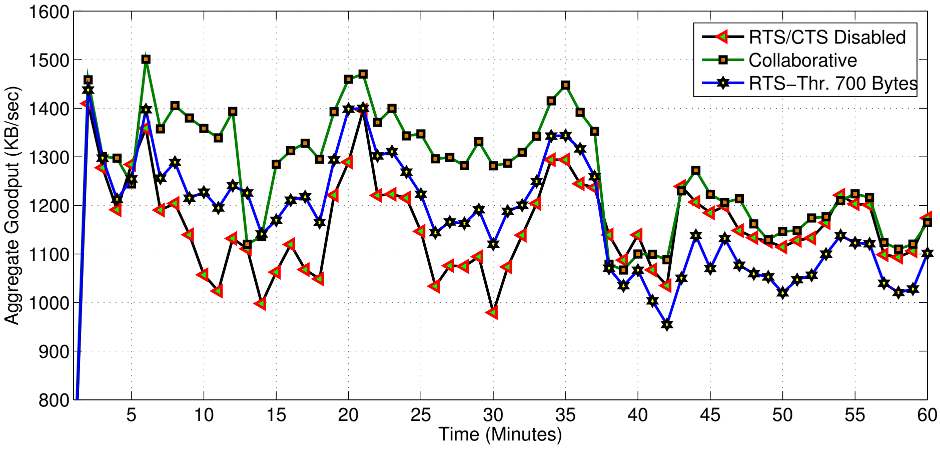


Figure 6.14: Goodput Performance of Collaborative Criterion with SIGCOMM 2001 Real Traces.

We make the following observations on both figures:

- The collaborative criterion tracks the situations in which enabling or disabling RTS/CTS is beneficial. It shows better performance than the case in which an RTS threshold of 700 bytes is used.
- Although a degradation in performance may occur before and during the testing phase (not clear in the figures since the scale is in minutes and the measurement duration was set to 5 seconds), this should not be harmful and is better than always enabling or disabling RTS/CTS which may degrade the performance for long time.

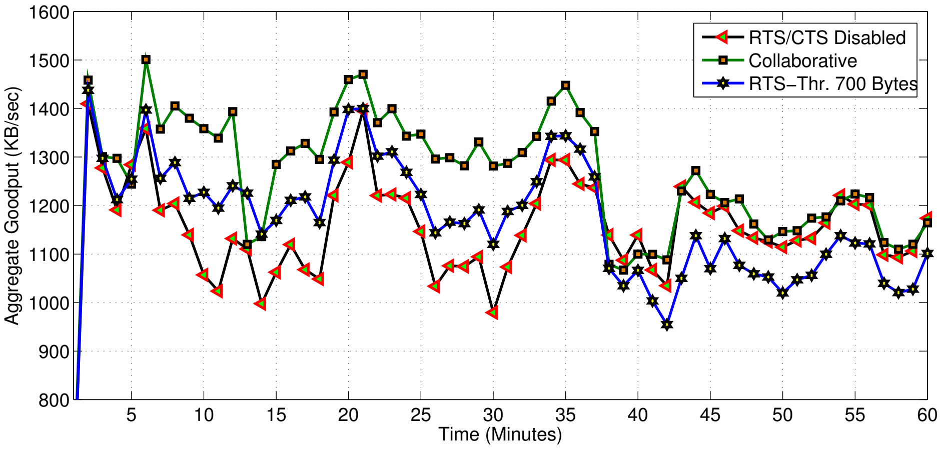


Figure 6.15: Goodput Performance of Collaborative Criterion with SIGCOMM 2004 Real Traces.

6.5.4 Real Experiments

Real Experimental Set-up

Four Laptops equipped with WPN511 RangeMax WLAN Adapters from Netgear (see figure 6.16) are used. Using MADWiFi driver, one laptop is configured in the AP mode.

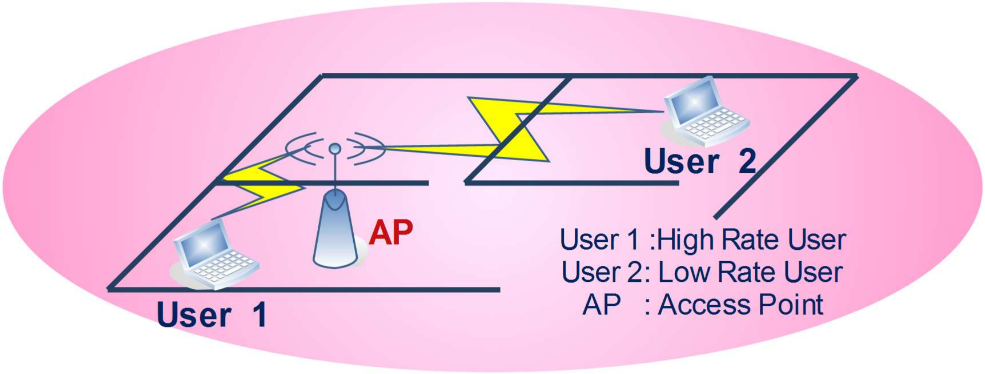


Figure 6.16: Real Experiments Setup.

The second one is placed close to the AP in an office and the third laptop is placed far from the AP in another office. Through transmission power control, the second and third laptops are made hidden from each other, but assured that each one can connect to the AP. Using **stg** traffic generator, both laptops send data packets to the AP which records the goodput of the received packets from each in a separate log file. While the far laptop is expected to utilize low transmission rate, the one close to the AP is expected to use high transmission rate due to the good signal level it receives from the AP. The experiment duration is three minutes. During the first minute, both transmitting laptops use the basic access scheme (i.e. RTS/CTS is off). During the second minute, both laptops signal RTS/CTS prior every data packet, while during the third minute only the far laptop uses RTS/CTS. The experiment is repeated 40 times in different times of a day. In another experiment, and in order to observe the percentage of retransmitted packets from the close laptop, the far laptop sends data packets to the AP and the close laptop copies a file to the AP using the **netcat (nc)** utility with the TCP protocol. A fourth laptop is configured in the monitor mode and used to sniff packets transmitted by the close laptop. The Ethereal - Network Protocol Analyzer has been used for this task.

Real Experimental Results

With the experimental setup presented in section 6.5.4, figure 6.17 shows an improvement in the goodput performance when both users/laptops have enabled RTS/CTS (between second 60 and second 120). The figure also shows that the maximum goodput was achieved when only the low rate user uses RTS/CTS (during the last 60 seconds).

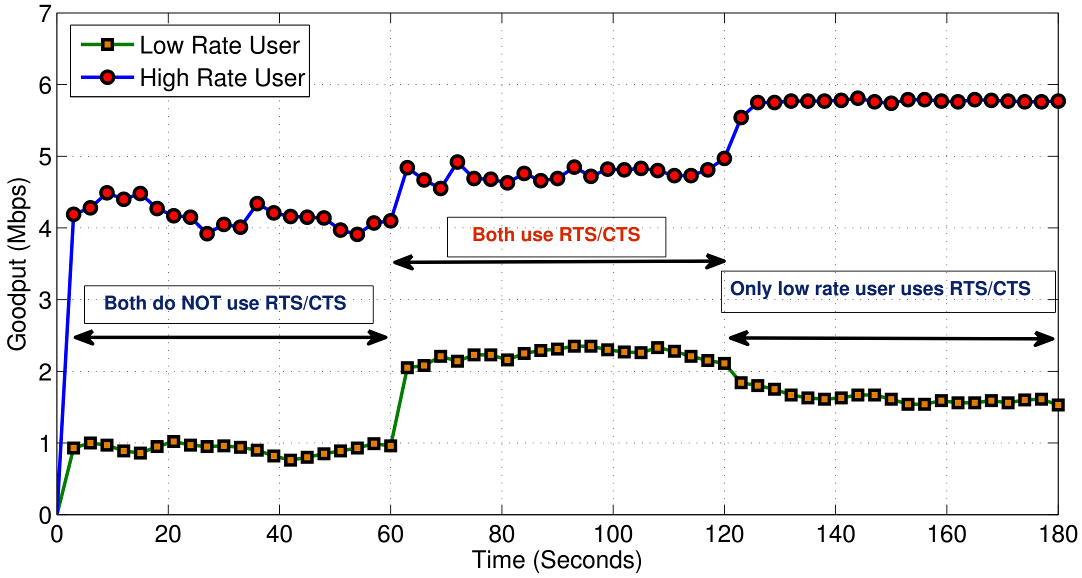


Figure 6.17: Impact of RTS/CTS in Heterogeneous Rate Scenarios.

On the other hand, figure 6.18 shows the goodput performance of the two users when both utilize the same data rate. Conversely, these results reveal that the RTS/CTS may degrade the performance if used. Additionally, figure 6.19 plots the percentage of TCP retransmissions from the user that is close to the AP during a real file transfer experiment using **netcat (nc)** utility. The sniffer captures packets for 1 minute. The experiment is done when the far laptop transmits with and without RTS/CTS. The results show that large amount of bandwidth is wasted when the far user does not use RTS/CTS. This is due to retransmissions caused by collisions whose duration depends on the used low rate by the far user. These results are in agreement with the conclusion

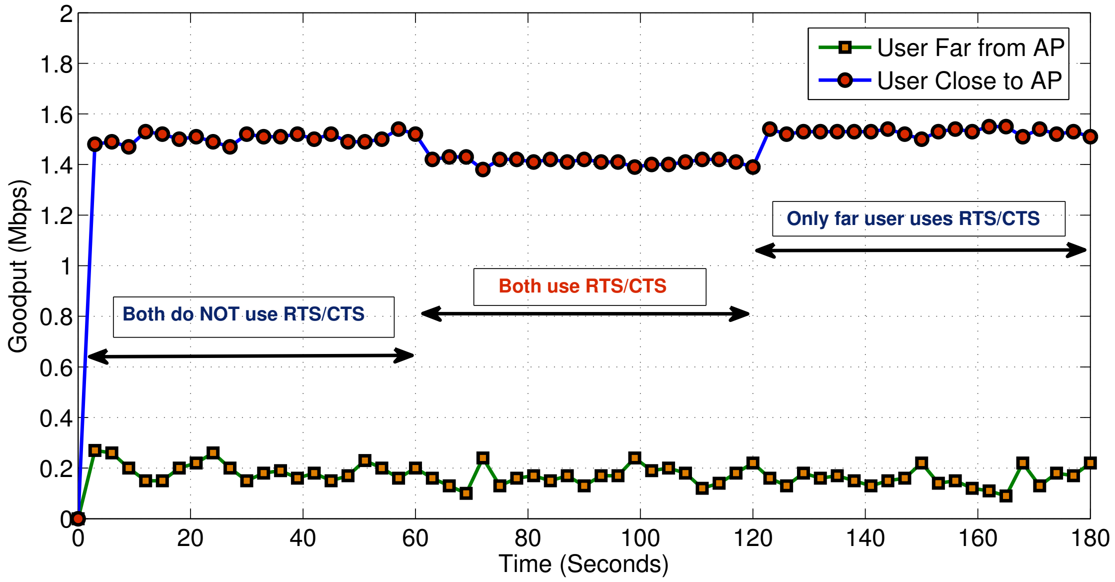


Figure 6.18: Impact of RTS/CTS in Homogeneous Rate Scenarios.

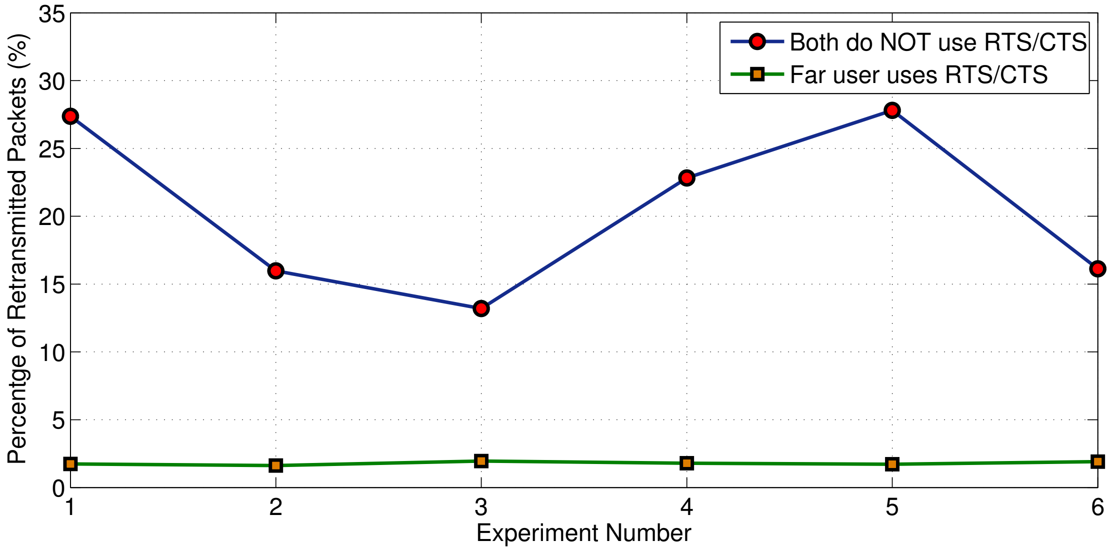


Figure 6.19: Impact of RTS/CTS on the TCP Retransmission for real file transfer in heterogeneous rate scenario.

of the simulation results.

6.6 Conclusions

In this chapter new criteria for setting the RTS/CTS mechanism are proposed. The main results that can be drawn from this chapter are:

- The setting of RTS/CTS shall depends on whether hidden nodes do exist in the WLAN rather than on packet length only. The usage of RTS/CTS signaling by detected hidden node pairs has found to improve the network goodput, especially for high uplink traffic and large number of hidden nodes. Nontheless, the mechanism is found to be not sufficient for alleviating interference due to hidden APs for downlink traffic.

- It has been shown that a collaborative decision on the usage of the RTS/CTS mechanism is essential when hidden nodes belong to different BSSs. The proposed collaborative approach has shown improved goodput performance compared to other approaches that suggest either enable or disable RTS/CTS.

- It has been shown that RTS/CTS control algorithms have to be evaluated in multi-rate WLANs. This is because in reality WLAN users employ different data rates and since the collision time is bounded by the time of the packet transmitted at low rate, the impact of collisions and consequently the gain from their reduction on self and others depend on the used transmission rates. The assumption of homogeneous rate may not reveal this fact.

Chapter 7

Interference Mitigation in WLANs via Access Point Coordination

7.1 Introduction

In chapter 6 we have shown that the RTS/CTS mechanism may not be sufficient for mitigating interference in multi-BSS deployments, especially when APs are the hidden nodes and the downlink traffic is high. It has been shown that the usefulness of the mechanism depends on numerous parameters other than the packet length, especially the network topology. In this chapter, we develop an AP Coordination approach for further mitigation of interference in infrastructure multi-BSS 802.11 WLANs. The network will consider this approach if the RTS/CTS is expected not to be useful for reducing the interference impact on users QoS. With the coordination-based approach, interfering BSSs negotiate and switch from the 802.11 CSMA/CA to a time slotted mechanism if the switch to the time slotted modus is expected to be useful and feasible. By combining the CSMA/CA and a time slotted access scheme, we try to preserve the best features of both schemes. The main goal of the approach is to improve the WLAN bandwidth utilization and the fairness among STAs. This is achieved by assuring a communication chance for every link in some time slot, but also activating all non-interfering links that can go in parallel within coordinating BSSs without collision in any time slot. The provided algorithms are driven by online measurements rather than fixed models which may not apply to all scenarios in such dynamic environment. This trend is advocated by upcoming standards and recent research results [11, 12, 68].

7.2 Relevant Work

The 802.11 standard provides the RTS/CTS mechanism to reduce interference. However, this mechanism is not always sufficient due to the followings:

- In general, the RTS/CTS helps if the number of hidden node pairs in the network is large and all nodes are able to hear CTS packets transmitted by APs.
- RTS/CTS may not always help across multiple BSSs. The main design assumption with RTS/CTS is that all nodes within sender and receiver vicinity will hear

the RTS or CTS packets and set their NAV accordingly. However, this assumption may not necessarily hold in multiple BSS deployments, whereby a node(s) may be busy receiving a frame generated within its BSS and therefore will not get the RTS or CTS sent by a neighboring BSS.

- For some topologies, RTS/CTS may unnecessarily decrease the communication efficiency [65].
- It has been shown in chapter 6 that the RTS/CTS is not efficient enough to solve the hidden node problem when APs are the hidden nodes.
- The RTS/CTS does not solve the exposed node problem, under which possibly successful transmissions are inhibited.

As explained in chapter 2, the IEEE 802.11e standard coordinates channel access within a BSS. Nevertheless, the standard does not address the problem of overlapping BSSs/-cells that use the same channel. There is no mechanism beyond CSMA/CA to coordinate the channel access across BSSs, thereby there is no guarantee that during the transmission of a frame by some STA in a time slot other STAs belong to neighboring BSSs will remain silent. This is due to the fact that BSSs operate asynchronously and independently.

The authors of [72] and [9] address time slotted access schemes with 802.11. Nonetheless, their work focuses on solving implementation challenges of a time slotted approach with 802.11 adapters in small testbeds of two nodes. Hence, the interference mitigation problem was not directly addressed.

The work of Bejerano et. al. [73] presents a managed WiFi system to support QoS in 802.11 WLANs with multiple BSSs. It uses coordinated channel access to allow overlapping BSSs coordinate their operation during up-link transmissions of the PCF modus so as to improve fairness among STAs. The presented solution proposes to assign disjoint time slots to BSSs that interfere with each other, whereby during a time slot assigned to one BSS other interfering BSSs should remain silent (i.e. Blocked). The length of the time slot that each BSS gets depends on the number of users the AP accommodates. Although the solution has shown improvement, still it has some drawbacks. First, the authors assume a circular channel model which is not the case in practice due to fading. Second, the PCF modus is not supported by most IEEE 802.11-compliant products. Third, the authors consider only uplink transmissions while in many cases most of the traffic is downlink and the collision rate due to hidden APs is quite high. One example is Internet type traffic in which the uplink traffic volume is relatively light and most of the traffic is downlink coming from Internet. Fourth, the BSS-based scheduling does not efficiently utilize the wireless bandwidth, since it does not exploit exposed nodes within interfering BSSs which can simultaneously send their packets.

Recently, there has been a significant amount of research activities in the area of wireless mesh and sensor networking, aiming for network performance enhancement through channel access coordination [74, 75, 76, 77, 78]. While the coordination-based approach proposed in this chapter follows the same general ideas of scheduling transmissions, it differs from the foregoing efforts in that we are aiming at development of a holistic solution for the interference problem, covering interference estimation and switching between a CSMA/CA and a time slotted access schemes depending on interference conditions. Additionally, a different approach for solving the scheduling problem will be considered here.

7.3 Coordination-Based Interference Mitigation

This section elaborates the proposed coordination-based approach for interference mitigation in IEEE 802.11 multi-BSS infrastructure based WLANs. We first give an overview of system operation and describe its blocks.

7.3.1 Solution Idea

We exploit the efficiency of a temporal separation approach to mitigate interference in multi-BSS 802.11 WLANs. As pointed out previously, the 802.11 CSMA/CA channel access scheme provides best effort service. It is easy to implement, does not need synchronization among contending nodes, and works well at low traffic load. At increased traffic levels, frequent collisions and retransmissions due to interference occur, degrading the QoS the wireless users experience. On the other hand, a collision-free channel access scheme, such as a time slotted access scheme, is known to perform better than the CSMA/CA at high traffic loads despite the signaling overhead it adds [73, 79]. We combine the CSMA/CA and a time slotted channel access scheme [81]. To preserve the features of current 802.11 MAC, interfering BSSs switch from the CSMA/CA access mechanism to the time slotted mechanism only if high interference is detected and the RTS/CTS mechanism does not help alleviating it. A switch-back to the CSMA/CA operating modus takes place when interference conditions are observed to improve. A detailed description of the system blocks and their functionalities is provided in section 7.3.2.

The proposed approach tries to achieve interference mitigation by:

- Adopting measurement-based optimization that considers the real network status rather than fixed mathematical models which may not always reflect the real status in such dynamic environment. This is due to the stochastic nature of channel conditions (path loss, fading), traffic pattern and distribution of users across the BSSs (see [68]). In this case, measurements is the proper way to discriminate who does interfere and how high the interference is ? Hence, the system switches between the two access schemes if it concludes (after processing measurements) that the performance can be improved after switching to time slotted channel access mechanism. This is also in alignment with the ongoing discussions within the standardization bodies, whereby the emerging standards specifies the mechanisms to facilitate measurements and exchange of measurement results among WLAN nodes (see 802.11k [11]).

- Reducing the silent (blocking) time of the nodes during a time slot, i.e. the time during which nodes are not allowed to use the channel to avoid interfering an ongoing transmission of a neighboring node which owns a slot. We achieve this goal by enabling APs of interfering BSSs to negotiate and agree on some disjoint time slots to use the shared channel on link-basis rather than BSS-basis. Therefore, instead of assigning a time slot for non-interfering BSSs, all non-interfering links should have the right to occupy the channel in a time slot. Such scheduling jointly optimizes the usage of channel bandwidth and improves the fairness among WLAN nodes by assuring that every node will have a chance to deliver a frame in one of the time slots.

In general one could argue that the transmission in time slots and consequently blocking some communication in neighboring BSSs would waste the WLAN capacity. On the one hand, this might be true, but on the other the reduction of overall collisions and consequently the reduction of the time span a MAC protocol needs to hold a packet until it is successfully transmitted would probably compensate this capacity reduction. Despite the importance of aggregate throughput of all users, the portion that each user gets is very important. One should also try to maximize the number of users that are happy with the offered service. Therefore, fairness among WLAN users should be given considerable attention.

7.3.2 Solution Description

An architectural block diagram for AP operation is shown in Figure 7.1. The basic system components are:

- **Interference Conditions Estimator.**
- **Channel Access Scheme Selector.**
- **Slot Scheduler.**
- **Signalling Mechanism.**

In this section and the following ones, we elaborate our design principles of the various system components.

Interference Conditions Estimator

The Interference Conditions Estimator resides at each AP. It processes AP's local (”own”) observations and interference measurement information reported by STAs and produces an estimate of the interference in the BSS. The measurement information from any STA includes an estimate of interference at the STA side and the identity of each interferer. The estimate of interference conditions will then be used as input to the access scheme selector as well as the slot scheduler as will be described in the following sections. For estimating interference conditions and determining interfering links, we use the two measurement-based approaches discussed in chapter 4:

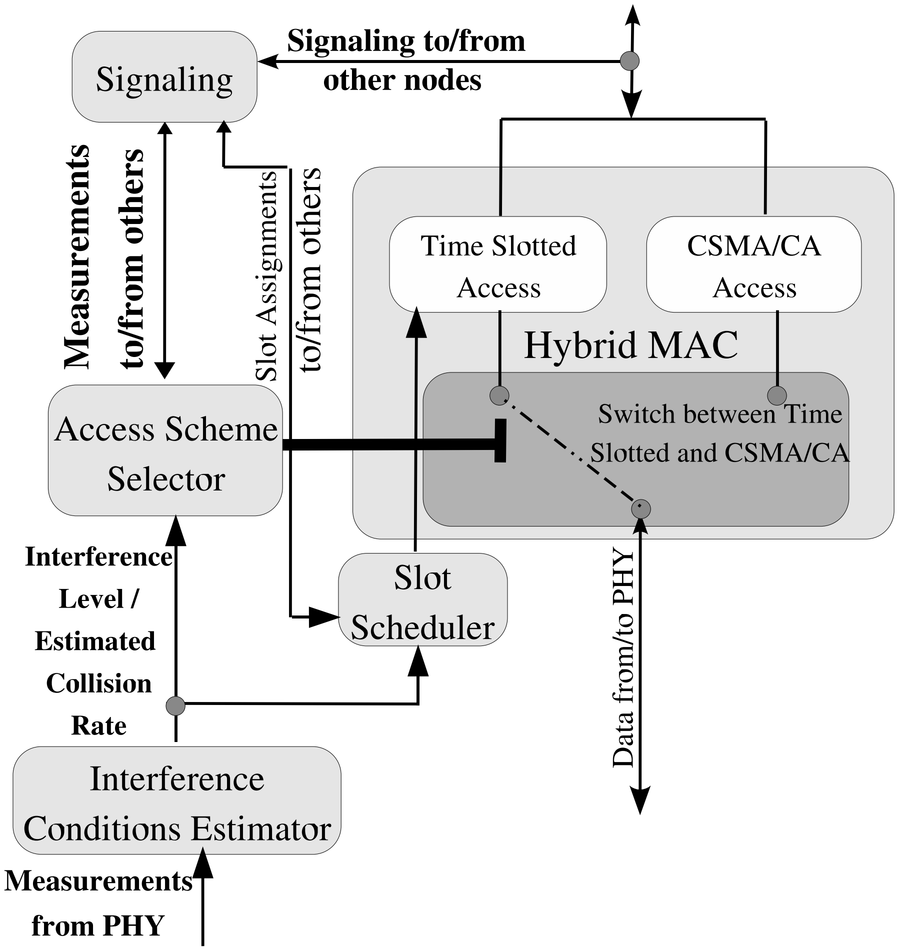

Signaling
Signaling to/from other nodes
Measurements to/from others
Slot Assignments to/from others
Time Slotted Access
CSMA/CA Access
Hybrid MAC
Switch between Time Slotted and CSMA/CA
Access Scheme Selector
Slot Scheduler
Data from/to PHY
Interference Level / Estimated Collision Rate
Interference Conditions Estimator
Measurements from PHY

Figure 7.1: Architectural Block Diagram

- Packet loss Diagnosis.
- Passive interference estimation using packet decoding.

Access Scheme Selector

The access scheme selector is mainly responsible for selecting the proper access scheme to be employed within the BSSs. Also, it has to determine the scope of BSSs which shall employ a channel access mode. This issue will be discussed in section 7.6. The decision on the mode to be used within BSSs is based on:

- Access Mode Switch Rules.
- Observations and diagnosis of the QoS degradation reported by local interference conditions estimator and measurements signalled from other APs.

Potential rules for access mode selection are discussed in section 7.4.

Slot Scheduler

Basically, slot scheduler is an algorithm for assigning disjoint time slots to all links within a group of BSSs which have been selected for potentially simultaneous switching to the time slotted modus. The input to the algorithm is interference relations among the links within the group. The scheduling algorithm should find out the set of transmissions/links that can go in parallel without collision. This becomes extremely important as the number of STAs and cooperating APs increases. In this case, the sequential assignment of time slots (i.e. the assignment of one long time slot to each participating AP as done in [73]) becomes not possible since other BSSs cannot be blocked (wait) for long time. Section 7.5 elaborates on slot assignment algorithms.

Coordination Protocol

The interference mitigation approach we propose in this chapter involves two types of signaling. We assume that information exchange works perfectly, i.e. we do not consider errors in data exchange for the sake of coordination. Here, we generally outline the signaling requirements for the described system operation.

The first signaling will be needed for ***the passing of interference measurements from STAs to their respective APs***. STAs report to their respective APs:

- The interference level from every potential interferer as estimated at the STA side.
- The collision rate as estimated at the STA side.

The second signaling will be needed for:

- The distribution of access scheme selector decisions.
- The distribution of slots allocation results.
- Achieving reliable mode switching (i.e. assuring that all nodes switch operation mode at the same time).
- The decision on the scope of BSSs within which an operation mode (CSMA/CA or slotted time) shall be used since the usage of a mode can not happen for an arbitrary subset of BSSs.

Primarily, the information includes:

- Access scheme change messages.
- Interference measurement information.
- Slot assignment results once a change to the time slotted access mode is decided.

Interference measurement information includes the amount of estimated interference in the BSS and the set of interferers for each STA in the BSS. Slot assignment results include the identity of nodes that can access the channel at the beginning of each time slot.

7.4 Switching Rules

The general reasons for changing the operation modus are:

- Potential improvement of users' satisfaction level.
- improvement of the channel usage efficiency in terms of the ratio of number of packets successfully ACKed from the first transmission to the total number of transmissions.

In this work, we only focus on the users' satisfaction level and try to improve that while designing a mode switching rule by considering the user load and the MAC ability to deliver this load.

Now we elaborate a criterion for checking if switching from CSMA/CA to the time slotted mode might help improving the user satisfaction level.

Intuitively, the crucial question here is whether the time span a MAC spends in resolving collisions and delays blocks incoming frames from upper layers from being transmitted or not. The answer depends on: the traffic load, the amount of time a transmitter spends sending retransmissions, and the amount of time it spends in states other than transmitting frames. Let us consider an observation period of length T. Denote the time a transmitter spends sending retransmissions during T as T_r. Denote T_o (a fraction of T) as the time period during which the MAC was busy due to reasons other than sending frames. This includes back-off time, NAV delays, and time spent receiving frames destined to other nodes. A sender MAC can estimate the time W of all frames it rejects while being busy sending retransmissions, waiting backoff/NAV counters, or receiving frames destined to other nodes during T. Note that the MAC would have attempted to send those frames during the time period $T_r + T_o$. The estimation of W can be achieved by observing the destination MAC address of a rejected frame, its length, and the potential physical rate which can be learned from the recent history. If the MAC has enough time to send incoming frames despite the wasted time $T_r + T_o$, then retransmissions time T_r and the delays T_o do not introduce much overhead (i.e. they do not block data frames comming from upper layers from being transmitted). This characterizes the low load case, in which there will be no need to switch to the time slotted modus. However, if the overhead is greater than W, then the MAC is not able to pass frames and a switch to the time slotted modus might be useful. In equation form:

$$Mode = \begin{cases} \text{CSMA/CA} & \text{W} \leq T - (T_r + T_o) \\ \text{Slotted might be useful} & \text{W} > T - (T_r + T_o) + \Delta \end{cases} \tag{7.1}$$

where Δ is a hysteresis margin introduced to avert the network from perpetually flipping back and forth between the two access schemes as a result of small fluctuations in W,

T_r, and T_o. In the experiments provided in section 8, a switch to the time slotted modus takes place if all interfering BSSs agree on the switch using the above rule.

7.5 Slot Scheduling

Slot scheduling is the function of the slot scheduler. It is an algorithm that finds the set of links that can be activated concurently in each time slot. This chapter develops such algorithm. The main design objectives are:

- Maximizing the number of active links in each slot.
- Minimizing number of required slots.
- Achieving some fairness in terms of number of slots during which a link is active.

7.5.1 An Optimal Slot Assignment Algorithm

We first develop an optimal slot assignment approach based on graph coloring that assures a slot for each STA while minimizing the total number of required slots. The input to the algorithm is the interference relations among the links. For now we just consider the downlink direction, i.e. the links from APs to their associated users.

Problem Definition

The following information is given:

- The set of APs $\tilde{a} := \{a_1, .., a_\mathrm{A}\}$ assigned channels $(ch_1, .., ch_\mathrm{A})$, respectively.
- The set of STAs $\tilde{s} := \{s_1, .., s_\mathrm{S}\}$ where a STA s_i is associated to some AP $b_j \in \tilde{a}$, $i = 1..S$, $j = 1..A$
- The matrix $L_{i,k} := \{1$, iff a_k interfere s_i
  0, otherwise$\}$

The problem is to find the scheduling with minimal number of time slots for downlink traffic (from APs to all STAs) so that any reception at any STA is not interfered from other APs at any time.

Mathematical Formulation

Mathematically, this problem can be converted into a graph colouring problem as follows: If a_k is sending to s_i, then a_q is allowed to send to s_j at the same time if it operates on a different channel, i.e.

$$ch_k \neq ch_q$$

or iff:

$$L_{i,q} = 0$$

$$L_{j,k} = 0$$

The last conditions mean that any transmission by AP q does not hit the receiver of s_i and any transmission by AP k does not hit the receiver of s_j. From the above criteria and given the input parameters listed above, it is possible to generate a graph $G = \{\tilde{v}, \tilde{e}\}$ where the nodes of the graph represent the STAs, i.e. $\tilde{v} = \tilde{s}$. An edge $(i, j) \in \tilde{e}$ between two STAs s_i and s_j represents whether the two STAs are allowed to receive from their associated APs at the same time. Assuming that L is a symmetric matrix, the definition of $\tilde{e}$ is the following:

$$\tilde{e} := \{(i,j) = 1 : \; ch_{b_i} = ch_{b_j} \text{and } (L_{i,b_j} = 1 || L_{j,b_a} = 1), \; \forall (i,j) \in \tilde{s}^2\}$$

This means that an edge exists between two nodes if they operate over the same channel and the the transmission of at least one interfere the other. Now we apply an integer program (IP) to solve the graph colouring problem over G. Let $C_{i,c}$ be the matrix of binary decision variables for the resulting color assignments; note that here the color assignment means slot assignment to the STA, i.e., it determines which AP in which slot should send to which STA. $C_{i,c}$ is one, iff s_i is assigned color c. Further, let A be the matrix form of G that represents the edges between each pair of nodes, i.e. $A_{i,j}$ is one, iff $(i, j) \in \tilde{e}$. The IP model can be written as:

$$\min \quad \sum_c x_c \tag{7.2}$$

$$\text{s.t.} \quad \sum_c C_{i,c} = 1 \qquad \forall i \tag{7.3}$$

$$C_{i,c} + C_{j,c} \leq 2 - A_{i,j} \qquad \forall i \neq j, \text{and } \forall c \tag{7.4}$$

$$x_c \geq C_{i,c} \qquad \forall i, c \tag{7.5}$$

The objective function (7.2) is the total number of the colours extracted from C with the help of a constrained vector $\overline{x}$, the elements of which depends on whether a color is used or not. Therefore, constraint (7.5) ensures that $x_c = 1$ iff color c is used by any node in graph G, and 0 otherwise, thus the sum of $\overline{x}$ gives the total number of colours used. Constraint (7.3) is for assigning exactly one color for each node, and constraint (7.4) ensures that no two interfering nodes can get the same color.

After solving the above IP, the matrix C will contain the slot assignments with the objective of minimizing the total number of slots for the whole system, thus maximizing the spatial reuse of the slots.

7.5.2 A Heuristic Slot Assignment Algorithm

In section 7.5.1, we have developed an optimal algorithm for time slots allocation. Despite that the optimal algorithm provides optimal time slots assignment, it is rather computationally expensive, especially for large number of STAs and APs. Hence, the question about a heuristic algorithm is relevant. This section develops such algorithm. The slot assignment problem has to be solved for each channel. The main design objectives are:

- Maximizing the number of active links in each slot.
- Minimizing number of required slots.
- Achieving some fairness in terms of number of slots during which a link is active.

Let us consider a set of N APs that operate over the same channel. Assume that the N APs provide communication services to M stationary STAs. Each STA sends and receives traffic to/from its AP. Hence, there is one uplink and downlink for each STA. Denote $L(i, j)$ as the communication link from transmitter i to receiver j, where a transmitter or receiver is a STA or an AP. Basically, two links $L(i, j)$ and $L(m, n)$ can be active simultaneously (i.e. within the same time slot) iff: transmitter i does not interfere receiver n, transmitter m does not interfere receiver j, receiver j does not interfere transmitter m, and receiver n does not interfere transmitter i. The first two constraints are for data packets protection and the latter two ones are for ACKs protection. Therefore, what do we really need to know is the set of interferers for each node. Given this information, the objective is to assign a time slot for each link, during which this link has the right to access the channel.

The scheduler starts with the link that experiences the highest interference and finds out all links that can run parallel to it. This set of links are marked as **done** and should be assigned a time slot. Then, it proceeds with the next link and again finds out all links that can receive in parallel with it starting with those that are not marked as **done** yet. The algorithm proceeds until all links are marked as **done**. The algorithm is shown in Algorithm 4, it has the following features which differentiate it from other algorithms proposed in the literature:

1. Due to delay constraints, the algorithm sets an upper bound on the number of time slots to be used in scheduling. Note that a node can not be blocked from accessing the channel for a long time. This happens when the number of interfering nodes gets large. So, we extend other scheduling algorithms by allowing some (probably) small interference between links whenever it is impossible to schedule all links without exceeding a pre-defined maximum SlotCount threshold.

2. In order to minimize the number of needed slots and the search time, the algorithm first sorts the set of links in descending order according the interference each measures.

3. Note that step (10) achieves the objective of maximizing the number of links that use a slot, while in the meanwhile it tries also to improve fairness by considering the ones that already got minimal slots as first candidates.

Algorithm 4 Heuristic Slot Assignment

```
INPUT: $\boldsymbol{S}$= {Set of all links};
OUTPUT: The scheduled links in each slot;
Initialization: SlotCount=0; Done={};
Sort $\boldsymbol{S}$ (descending) according the interference level;
MAX : a maximum upper bound on the number of slots that can be allocated;
Repeat {
Select the Next link $l$ from $\boldsymbol{S}$ AND $\notin$ Done.
Find the set of links $\boldsymbol{K} \subset \boldsymbol{S}$ that can be active parallel to each other and to link $l$ AND $\notin$ Done.
Done= Done U $l$ U $\boldsymbol{K}$.
Find the subset $\boldsymbol{T} \subset$ Done that can be active parallel to each other and to $l$ and every link $n \in \boldsymbol{K}$, starting with those that occupy less slots.
Assign SlotCount to links $l$ U $\boldsymbol{K}$ U $\boldsymbol{T}$
SlotCount = SlotCount + 1
if (SlotCount > MAX) distribute all remaining links among the slots in a way that keeps interference among scheduled links in each slot minimal.
} Until all links $\in$ Done
```

7.6 Clusters Determining

One key issue of the coordination-based approach discussed in this chapter is the determination of which BSSs shall employ which access mode. This is a functionality of the access scheme selector. In this section we use density-based clustering techniques to solve this challenge. Density-based clustering techniques were originally developed to recognize dense areas within an object space. They have the advantage for allowing arbitrary shape of clusters and do not require the number of clusters as input. The most common approach for density-based clustering is so-called bump-hunting. It starts finding dense or "hot-spots" and then expands the cluster boundaries outward, until it meets a low density region.

Specifically, our goal here is to find out the groups or clusters of interferring BSSs that shall employ a time slotted access scheme and those BSSs that shall operate using the CSMA/CA modus.

We model our WLAN as a weighted conflict graph $G = (V; E; W)$, where $V = \{1, 2, 3, ..., N\}$ is the set of vertices or nodes which represent the BSSs of the WLAN, N is the total number of nodes, and E is the set of edges between the nodes. The weight w_{ij} on an edge connecting two nodes i and j denotes the amount of interference estimated within node j from node i. From the conflict graph, the set of loosely coupled or independent clusters of nodes need to be identified.

We assume that two nodes (BSSs) interfere if the interference level measured by at least one from the other ($w_{i,j}$) is above some threshold value $InterfThreshold$. An informal algorithm for solving this problem would be: Each cluster starts at the cluster root (a BSS that measures the highest interference in the cluster) and expands until the the interference between any cluster member and its neighbors at the cluster borders is less than $InterfThreshold$. Thus, the algorithm starts with the BSS that experiences the highest interference from its neighbors, say BSS I. This will be a first cluster root. The algorithm finds out all interfering neighbors of BSS I. All these BSSs will be members of the first cluster. Then, the algorithm finds out the neighbors that interfere with each member of the first cluster. It expands on a path until the interference impact of a BSS and its neighbors is below $InterfThreshold$. Then, the next cluster root is selected. Similarly, all interfering BSSs and their neighbors are included in the new cluster until a light region is detected. The algorithm continues until each BSS is a member of a cluster. Note that a cluster may include one BSS member. All such BSSs will operate in the CSMA/CA access mode.

The formal algorithm is given in algorithm 5. Note that the *ADDInterferers(I)* function is recursive. The complete developed C-code is provided in Appendix-1.

Algorithm 5 Clustering Algorithm

```
INPUT: An interference map of the WLAN BSSs.
OUTPUT: Members of each cluster.
Mark all BSSs as Non-Member.
while (their is some BSS that are still Non-Members)
{
        Next = The Next BSS I that experiences highest interference;
        Construct a new Cluster;
        ADDInterferers(Next);
}
Output Clusters;
*************************************************
ADDInterferers(I) {
        If (no more interferer BSS to I)
                return();
        J = Select the next Interferer to BSS I;
        Include J as a member of cluster I;
        Mark J as DONE ;
        ADDInterferers(I) ;
        ADDInterferers(J) ;
}
```

7.6.1 Illustration Example

Consider the topology shown in figure 7.2. Nodes represent the network BSSs. A

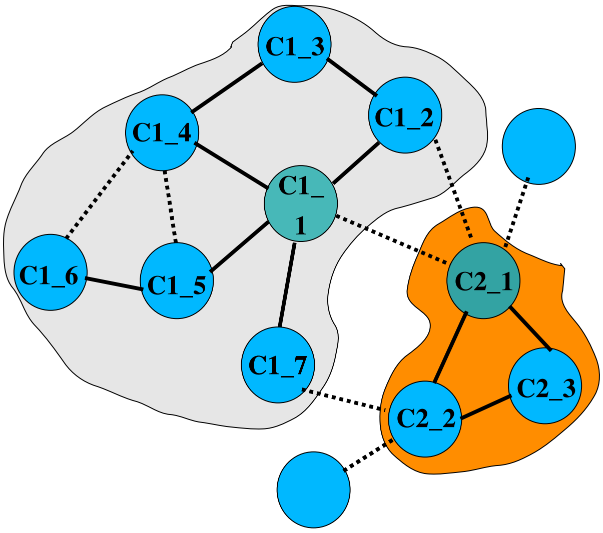


Figure 7.2: Clustering Algorithm- Illustation Example

solid line between two nodes indicates that the interference between them is above the pre-defined threshold $InterfThreshold$. If an edge does not exist or if a dashed line connects two BSSs, indicates that interference between the two BSSs is below the $InterfThreshold$ or does not exist.

The algorithm starts with Node $C1_1$. It will be the root of the first cluster $C1$. Then, the algorithm moves to the first interfering neighbor $C1_2$, then to $C1_3$ (the neighbor of $C1_2$), which also has an interfering neighbor $C1_4$. All these nodes are marked as members of the first cluster $C1$. Since $C1_4$ has no interfering neighbor, the execution falls back to the second neighbor of $C1_1$, which is $C1_4$. However, $C1_4$ has been already visited. Thus, the algorithm moves to $C1_5$, which has only one interfering neighbor $C1_6$. After adding $C1_5$ and $C1_6$, the algorithm moves to $C1_7$, which is the last neighbor to the root. $C1_7$ is added to the cluster. Now, there are no more interfering neighbors to the root $C1$. At this point, the algorithm has formed the first cluster $C1$ whose members are $\{C1_1, C1_2, C1_3, C1_4, C1_5, C1_6, C1_7\}$. Then, the next BSS that measures highest interference is selected as a second root $C2_1$. Similarly, $C2_2$ and $C2_3$ are marked as members to the cluster $C2$. Still we have two nodes that are not cluster members. However, since these two nodes do not interfere with other BSSs (i.e. isolated), each one is considered a cluster that will operate in the CSMA/CA mode.

7.6.2 Case Study

In this section, the provided algorithm for the determination of groups of interfering BSSs will be applied a real case. This will provide the knowledge about:

- The possible usefullness of the proposed algorithm for real WLANs.
- How deployed WLANs may look like in reality.

- The scope of scenarios, wherein the whole coordination-based approach promises to be useful.

- A sharpend understanding of side effects and any potential issues that shall be considered further.

Considered Case

We have decided to study a WLAN in a rather dense unplanned deployments. A residential area which is known to be quite dense is the city of San Diego (USA), where hundreds or even thousands of APs are being deployed by individuals and Internet service providers. We use data from the WifiMaps.com website. The data is obtained through wardriving. For each AP, the database provides the AP's geographic coordinates, its wireless network ID (ESSID), channel employed and the MAC address. We have used a GIS visualization tool to plot the points (APs) using their geographic coordinates. We plot the results in a selected dense region in figures 7.3, 7.4, 7.5, and 7.6. Figure 7.3, shows all APs that operate over the three non-overlapping channels of 802.11 (channels 1, 6, and 11), while figures 7.4, 7.5, 7.6 show the APs configured on channels 1, 6, and 11 respectively.

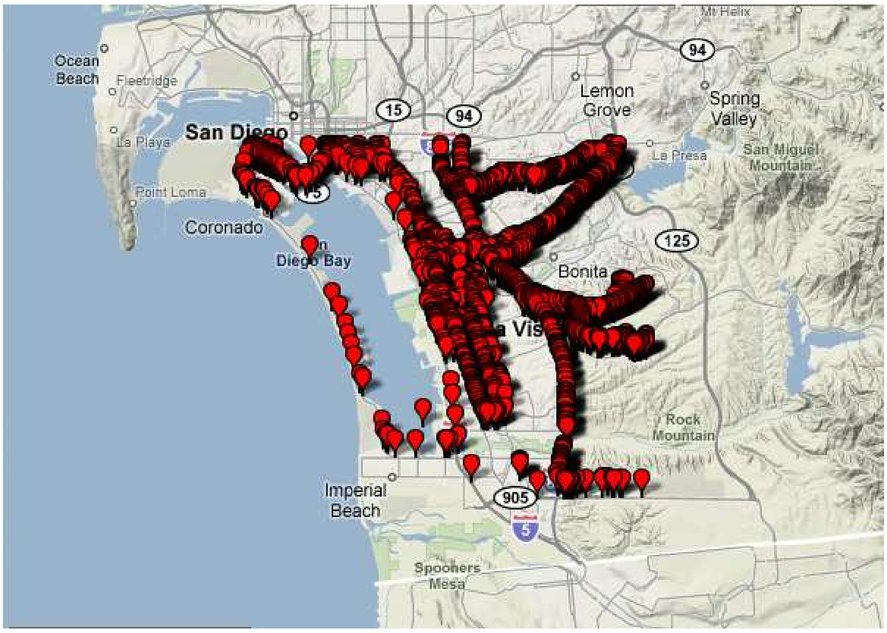


Figure 7.3: A Residential Area in San Diego - APs configured on channels 1,6, and 11

General Observations

Looking at the maps, we can make the following observations:

- Most of the APs (about 1150) in the shown region operate on channel 6. Potentially, this is the default channel configured by APs' manufacturers, leading to the

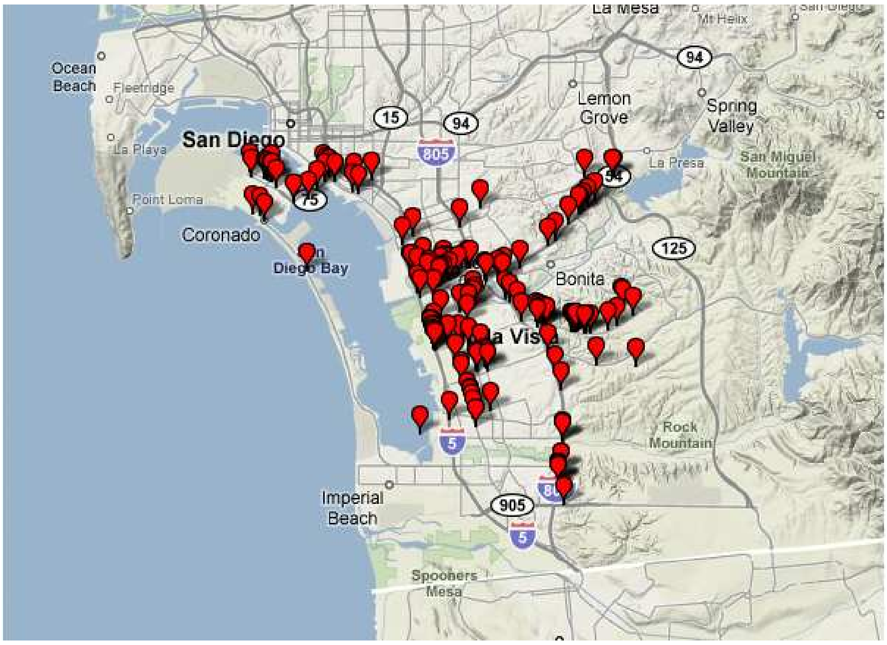


Figure 7.4: A Residential Area in San Diego - APs configured on channel 1

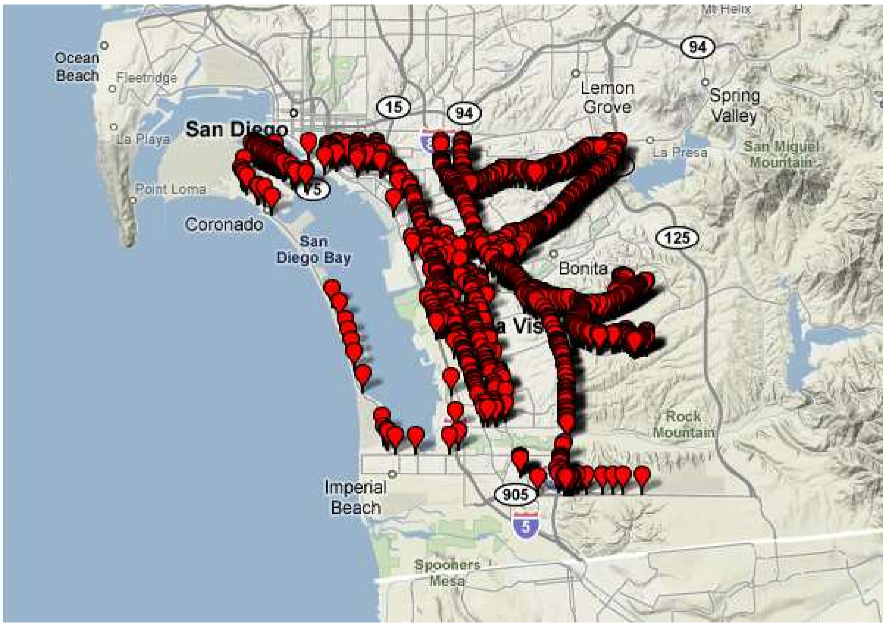


Figure 7.5: A Residential Area in San Diego - APs configured on channel 6

result that people seem to deploy the APs without any planning. Additionally, more APs are configured on channel 11 (about 300) than channel 1 (about 160).

- There seems to be dense regions and some light regions, which advocates the necessity of grouping BSSs into clusters for the sake of coordination.

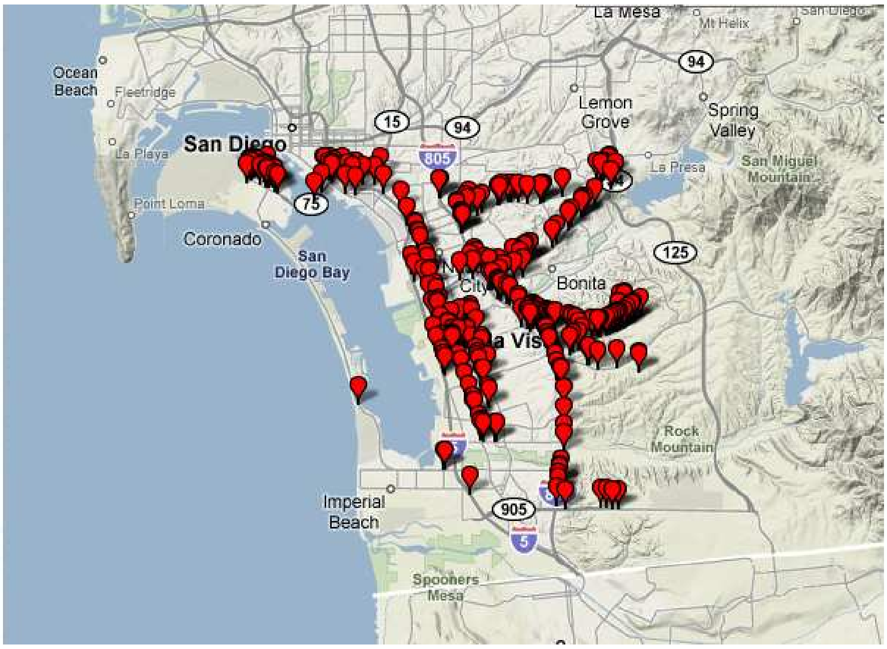


Figure 7.6: A Residential Area in San Diego - APs configured on channel 11

Results of BSSs clustering

We applied the clustering algorithm provided in algorithm 5, grouping interfering BSSs into clusters. A fundamental question is the selection of the interference threshold $InterfThreshold$, the threshold above which two BSSs shall be identified as interfering neighbors, requiring an edge between them in the conflict graph. Due to the lack of any other interference relevant information in the database, we decided to use the only real information available, the location of APs. A script has been used for computing the distance between APs from their GPS coordinates. We assumed that two BSSs are interfering if the distance between them is less than 250 meters. Additionally, the mostly interfered BSS is assumed to be the one that has more in range APs on the same channel. The results of this test are provided in table 7.1. We make the following comments on these results:

Channel	**Nr. of Produced Clusters**	**Nr. of one Member Clusters**	**Nr. of 10 or more Members Clusters**
1	86	57	2
6	102	38	25
11	117	54	3

Table 7.1: A Residential Area in San Diego - Clustering Results

- Despite the high density of APs, it is likely possible to group them into loosely coupled or independent clusters.

- From about 1610 APs in the selected region, only 149 (9.25%) of them are isolated, i.e. they have no neighbors (one member clusters).

- While 25 Clusters on channel 6 have more than 10 or more members, only few clusters on channels 1 and 11, have this number of members. This is expected since channel 6 is used by 72% of the APs.

- The allocation of time slots within clusters is expected to be more feasible and flexible within the clusters, wherein APs operate on channels 1 and 11. This is because of the small number of members within these clusters. Nonetheless, more than 60% (39 Clusters) of the clusters that operate on channel 6 are found to have between 2 and 9 members. Note also that not all members within a cluster may interfere with each other (i.e the BSSs graph may not be fully connected). To investigate this point deeper, we picked a point and included all APs that are within 1km range from this point. Then, we grouped all APs within this area into clusters using the clustering algorithm provided in 5. The real APs are shown in figure 7.7. The output of the algorithm is shown in figure 7.8. This result indicates that the number of members does not generally indicate the feasibility of time slot allocation within a cluster. In fact this depends on the location of users within BSSs and wether their links do really interfere or not.

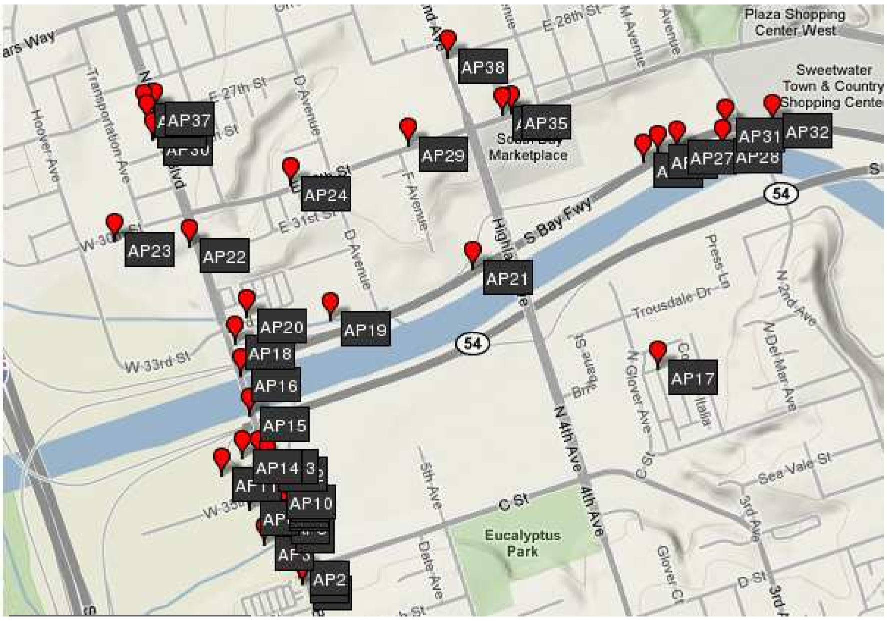


Figure 7.7: A Residential Area in San Diego - Some APs configured on channel 6

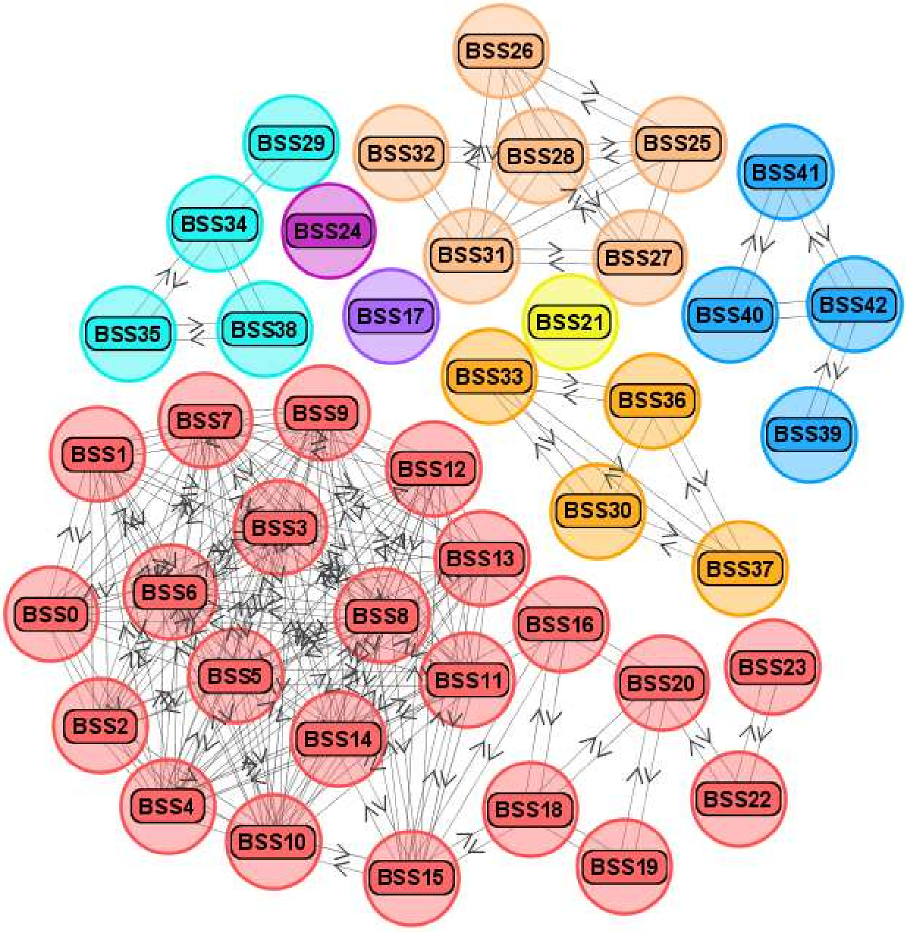


Figure 7.8: The Produced Clusters for the 43 APs

Chapter 8

Performance Evaluation of the proposed coordination-based approach

8.1 Introduction

In this chapter we assess the performance of the interference mitigation framework developed in this chapter. Intensive simulation experiments have been conducted. The slot assignment algorithm, interference estimation algorithms are fully implemented in the simulation, while the signaling protocol for the exchange of information among STAs and their respective APs and among the APs themselves is not. The measurement information is simply made accessible to APs. On the other hand, the heuristic slot assignment (Algorithm 4) of section 7.5.2 has also been implemented on top of the 802.11 MAC. Additionally, the coordinated channel access has been implemented in a small infrastructure WLAN of two APs and five STAs.

8.2 Simulation Setup

The scenario is composed of 4 BSSs and 75 STAs. APs operate over the same channel. STAs are randomly uniformly distributed across the coverage area of the APs. The simulation parameters were set as in section 4.3.4. Over a measurement period of 2 seconds, a STA monitors the wireless channel, it computes the interference level from each potential interferer as described in section 4.5. A node is identified as interferer to a STA if the measured interference level from that node is greater than a cutoff value of -83dBm. Throughout this study, the length of a slot in the time slotted modus was selected to be 10ms and the maximum number of slots was set to 20.

8.3 Traffic Model

In a first experiment, each user downloads infinite number of UDP packets from a server via its AP. The interval between two successive packets is drawn from an exponential distribution, while all packets are of same size chosen to be 1500 Bytes. In a second experiment, each user downloads UDP packets for 300 seconds using the traffic profile provided in table 8.1. It starts with a low load phase, followed by a high low phase and then back to low load. Since the interference depends on users' workload, we also tested coordination-based approach using realistic WLAN traffic traces provided in [80]. We used the realistic WLAN traces in the following way: Using CoralReef Software [54], we extracted users flows from the dump file. We selected the flows of 75 different users during 10 minutes. We used the total number of bytes, number of packets of a flow to characterize a user load and compute an average packet length. Then, the **stg** tool was used to emulate users' flows.

Simulation Time	Offered Load (Packets/second)	Packet Size (Bytes)
0 - 100	10	1500
101 - 200	200	1500
201 - 300	10	1500

Table 8.1: Traffic Profile

8.4 Simulation Results with Synthetic Traffic

8.4.1 Effect of Coordinated Channel Access on MAC Goodput

For different load levels, figure 8.1 shows the aggregate MAC goodput experienced by users when the network just employs CSMA/CA and when it employs coordinated channel access. Figure 8.2 plots the Jain's fairness index among the users. From these results, we draw the following observations:

- At high load, the aggregate goodput has been improved if APs coordinate channel access. Note that the goodput starts to degrade again at extremely high load conditions. We attribute this to the allocation of same time slot to some interfering STAs, where the impact of this interference starts to be harmful at very high loading.

- However, coordination degrades the goodput when the load becomes low. This is because we employed fixed slot assignment during our experiments, meaning that a slot is wasted if slot owner(s) has no data to send at the beginning of this time slot. Additionally, the probability of collisions with low load is lower and the CSMA/CA MAC can handle corrupted frames through retransmissions between successive arriving frames.

- With CSMA/CA, the goodput fairness among users decreases as the load increases. Conversely, with the time slotted modus it slightly decreases at high load which is again due to some increased interference.

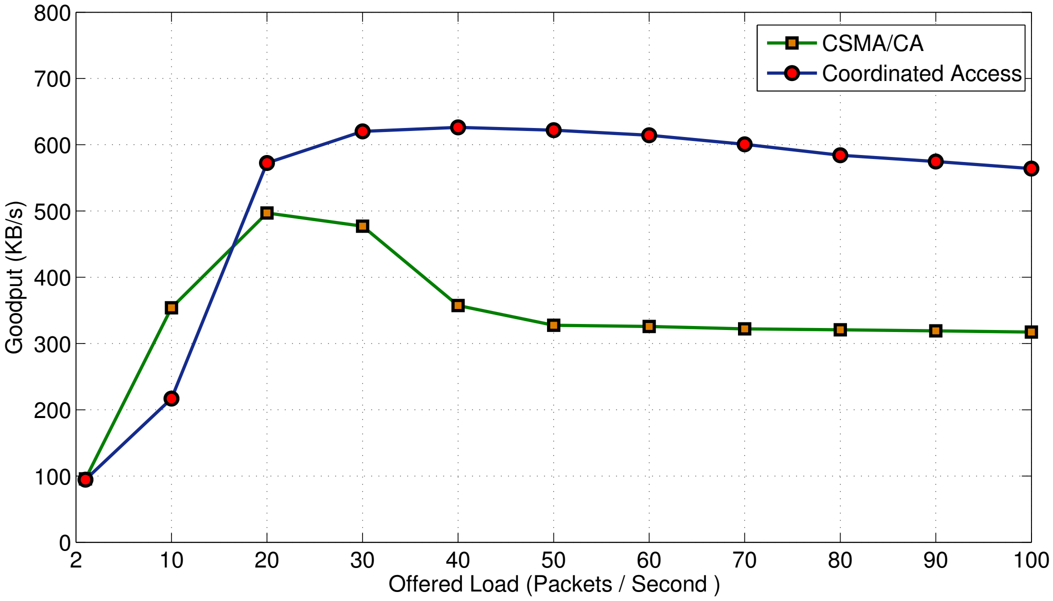


Figure 8.1: Aggregate Goodput experienced by all users with CSMA/CA and with coordinated access for different load levels.

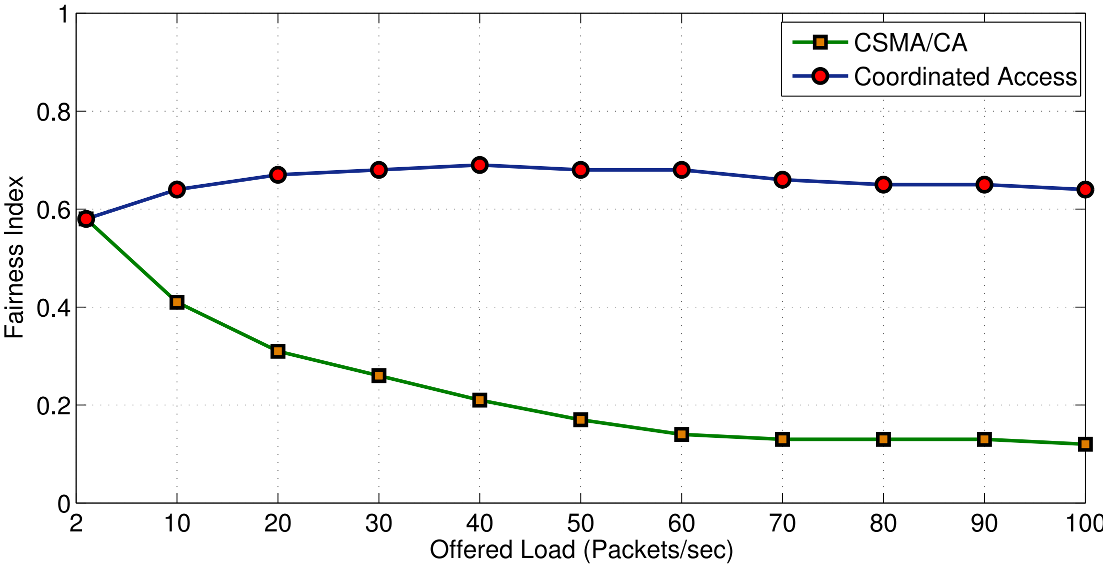
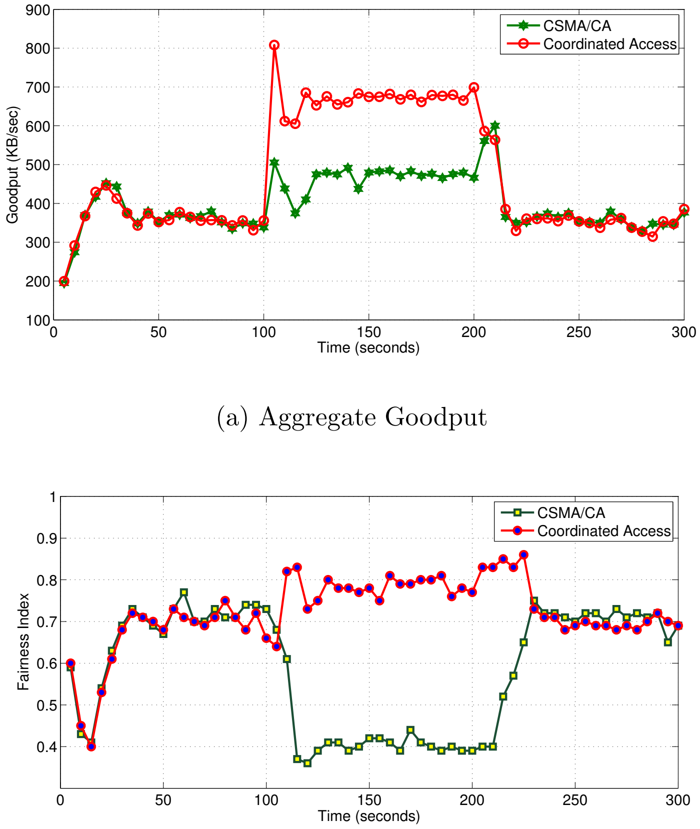


Figure 8.2: Fairness among users with CSMA/CA and Coordinated Access for different load levels.

8.4.2 Tracking high interference conditions

Now we run the simulation with the traffic profile of table 8.1 (subsection 8.3). In this experiment, APs use the rules described in section (7.4) for deciding on the operation modus. The observation period was set to 5 seconds. After operating in the time slotted modus for 20 seconds, APs change back to CSMA/CA and again decide on the operation modus to be employed. Figure 8.3(a) plots the aggregate goodput for two cases, where in the first case APs just use the CSMA/CA for channel access while in the second case they employ the time slotted channel access during high interference periods. The figure shows that, the aggregate goodput has been improved when APs coordinate channel access during the high load period. Further, figure 8.3(b) plots Jain's fairness level [10] among the 75 users, which also indicates a gain in fairness level among users as a result of coordinated channel access during the high load period.



(a) Aggregate Goodput

(b) Jain's Fairness Level

Figure 8.3: Aggregate Goodput and Fairness with CSMA/CA and Coordinated Access during Different Load Conditions

It is interesting to see how the aggregate goodput is distributed among WLAN users during high interference period for the case of CSMA/CA and time slotted channel access. We plot the portion of goodput that each user got during this period in figures 8.4, 8.5, and 8.6. The results reveal that some users get high goodput with CSMA/CA while many others are suffering from interference. Coordinated access improves the performance of such users. This leads to the result that the wireless channel is better shared among users with coordinated access during high interference periods.

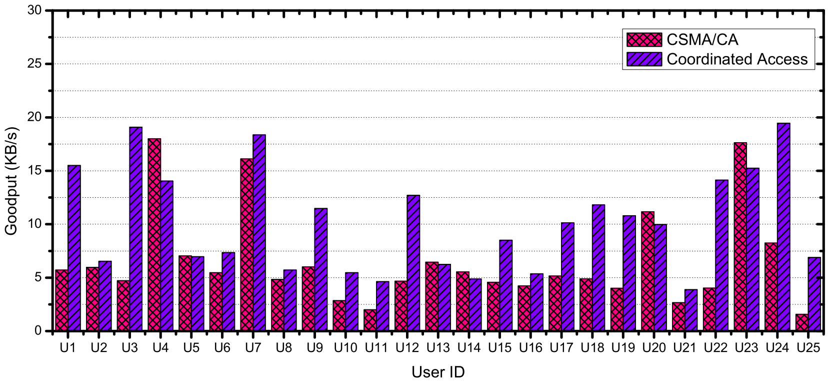


Figure 8.4: Users' Goodput During High Interference Period

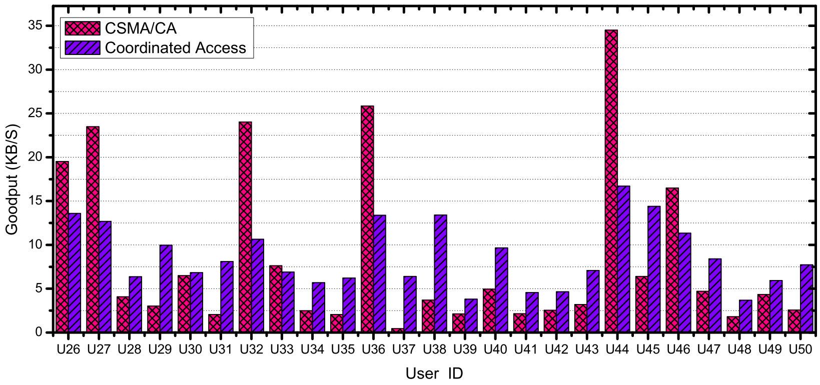


Figure 8.5: Users' Goodput During High Interference Period

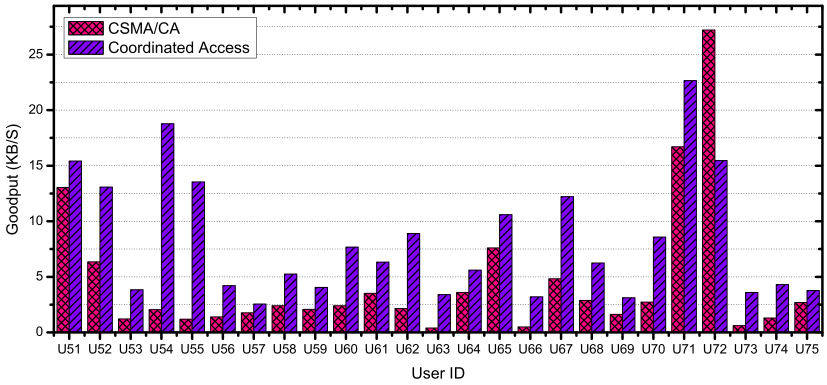


Figure 8.6: Users' Goodput During High Interference Period

8.5 Simulation Results for Chaotic Deployments with Realistic Traffic Traces

In this section, we present the simulation results of the proposed interference mitigation approach for a topology of the case study presented in section 7.6.2. We picked a point and included the APs that operate on channel 6 within 700m range of this point. We found that the selected topology includes some APs that are hidden from others as well as APs that are within range of some others. The selected set of APs is shown in figure 8.7. Users are distributed randomly across the coverage area of APs. We simulate the network for two cases, where in the first case the network operates using current 802.11 technologies and in the second case the network implements the proposed interference mitigation approach. We used traffic traces as described in section 8.3. The usage of realistic traffic is motivated by the fact that interference is dependent on traffic pattern which is dynamic in nature. We are interested to explore the usefulness of the proposed interference mitigation approach if used in real deployments.

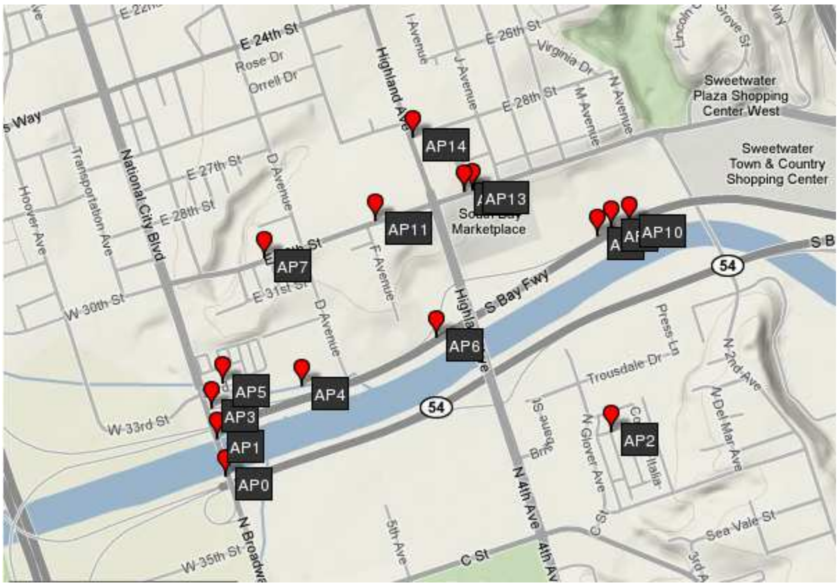


Figure 8.7: Simulated Topology of 15 APs

We used the rules provided in section 7.4 for the switching decision between the two modes, where a switch to the time slotted modus takes place only if all BSSs withis an interfering group agree on the mode switch. Figure 8.8 plots the aggregate network goodput for this experiment. The results show that coordination has a significant positive impact on the aggregate goodput during high interference period. Spikes seen in the aggregate throughput are due to bursty traffic and unsaturated channel conditions.

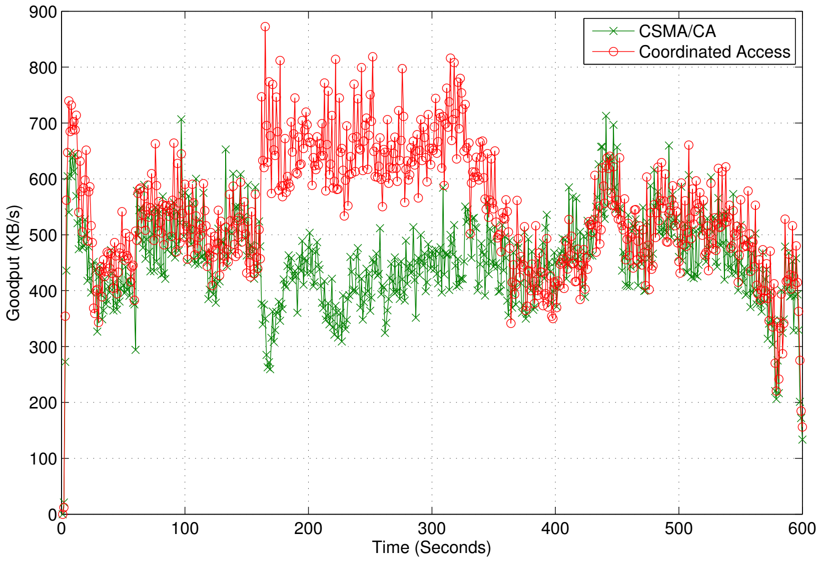


Figure 8.8: Goodput performance of a sample topology from the case study of section 7.6.2

8.6 Coordinated Channel Sharing - Real Experiments

In this experiment, we would like to observe the total system throughput and how this throughput is distributed among the STAs with and without coordinated channel access in a realistic network.

8.6.1 Experiment Setup

The experiment set-up is shown in figure 8.9. Two APs and five stationary STAs were deployed in two different LABs. The APs are WLAN adapters from Atheros configured in the master mode (AP mode) through the MADWIFI driver. The APs are connected via an Ethernet Switch. Over the ethernet connection, a master program runs on one AP synchronizes both APs. APs are assigned the same channel. Through transmit power control, APs are made hidden from each other. Two STAs are deployed in overlapping area of the two BSSs. APs transmit UDP traffic to the five STAs.

8.6.2 Experiment Results

In this experiment, the five STAs are scheduled as shown in table 8.2. Figure 8.10 plots the results of the real experiments. We make the following comments on thia result:

- **(A)** The total throughput with CSMA/CA and with coordinated channel access is comparable.

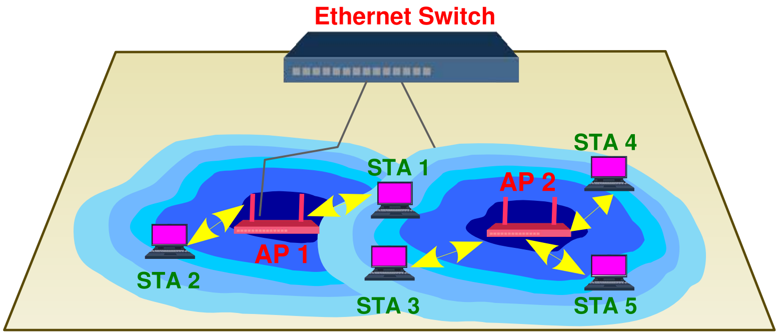


Figure 8.9: Topology used in Real Implementation

Slot	Stations
T1	STA 1
T2	STA 3
T3	STA 4, STA 2
T4	STA 5, STA 2

Table 8.2: Scheduling of the five STAs

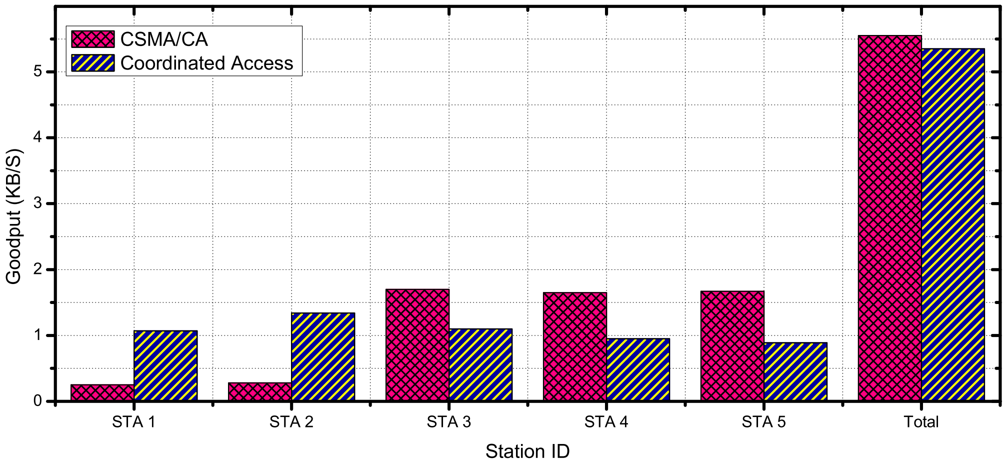


Figure 8.10: Real Implementation Results

- **(B)** With CSMA/CA, STA 1 (in the overlapping area) experiences degraded performance compared to other STAs due to increased collisions.

- **(C)** Although STA 2 is outside the interference region of AP 2, it also experiences degraded performance with CSMA/CA due to the time its AP (AP 1) spends retransmitting packets to STA 1. This means, in fact, that the whole BSS of AP 1 suffers communication problems. On the other hand, STA's 3 performance is not degraded with CSMA/CA despite it is located within the interference region of AP 1. By observing the received power at both STAs in the overlapping region, we found that one reason is the capture effect which helps STA 3 to maintain good performance. A second reason is the fact that AP 1 spends long time in back-off, which improves the communication conditions of STA 3.

- **(D)** With coordinated access, STA's 2 throughput is higher than other STAs as it is scheduled in two time slots.
- **(E)** In fact, the experiments have shown two main results: The first is the ability of coordination to improve system performance under high loading. With almost the same aggregate throughput, coordinated channel access was able to relief two users and consequently improves the fairness among WLAN users. The second result is the necessity of driving the whole adaptation process by measurements.

8.7 Time Slots Requirements

In this section, we study the impact of network density in terms of number of deployed APs and users on the number of time slots required for link scheduling. In order to investigate the impact of AP selection policy on time slots requirements, we consider both the RSSI-based AP selection and the AP selection policy proposed in chapter 5.

Let us consider an area of 300m X 300m dimensions. A number of APs will be deployed in this area. Users are randomly placed in the area following a uniform distribution. We vary the number of APs from 5 to 20 and the number of users from 20 to 120. We consider the downlink direction, where APs send data packets to the users they accommodate. What we would like to understand is how both the number of APs and users impact the number of time slots required to schedule the links and the total number of links that can be active in a schedule cycle. The schedule is generated using algorithm 7.5.2.

Figure 8.11 shows the number of slots needed when different number of APs and users are deployed in the area under consideration. The reported results are for the case of RSSI-Based AP selection generated based on the average of multiple topologies. The results show that for a given number of APs, more slots are needed as the number of users increases in the area, especially when just 5 APs are deployed. Moreover, for a given number of users, increasing the number of deployed APs from 5 to 10 APs has reduced the number of time slots required for links scheduling. Nonetheless, since APs are deployed in the same area and due to the mutual interference among them, the number of required time slots is not further notably decreased when 15 or 20 APs are deployed. Most importantly is to note that the number of required time slots is much less than the number of users. This is because the scheduling algorithm exploits all non-interfering links within the BSSs.

Figure 8.12 shows the total number of links that can be active in a schedule cycle under different density levels. The reported results show that for a given number of users, the total number of links that can be active is greater than the number of users. Again, the reason is that the scheduling algorithm activates all non-interfering links in each time slot. Now, the results with the proposed AP selection will be discussed.

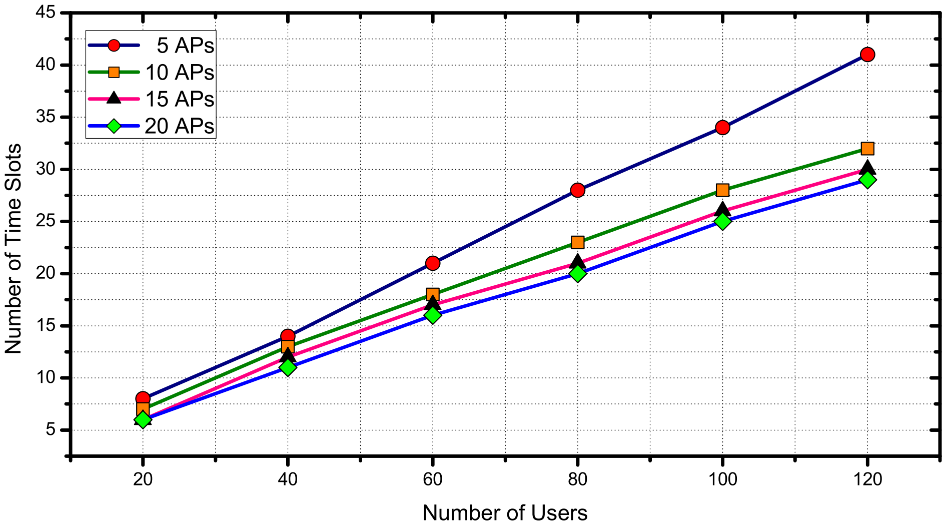


Figure 8.11: Time Slots Requirement with different number of APs and users - RSSI-Based AP Selection

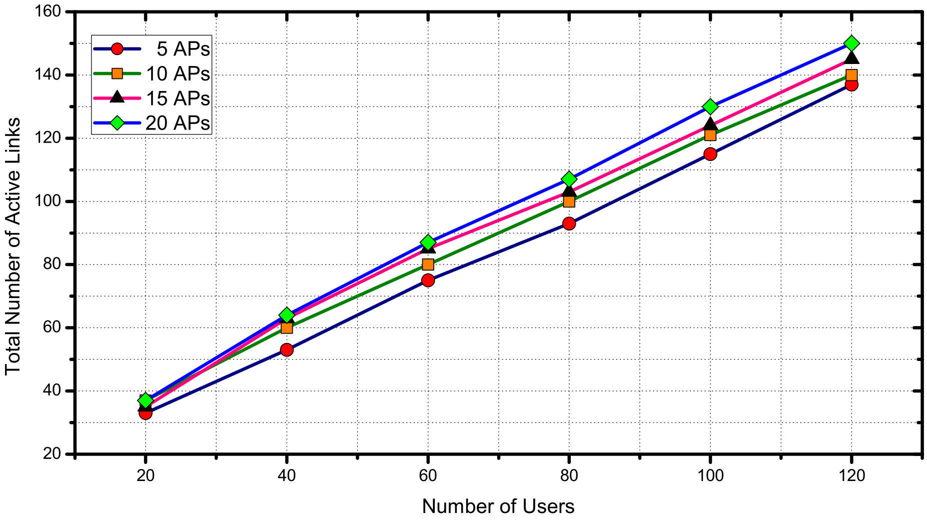


Figure 8.12: Activated Links with different number of APs and users - RSSI-Based AP Selection

Figure 8.13 plots the time slots requirements under different density levels. Figure 8.14 shows the total number of links that can be active in a schedule for different number of users and APs considerations. The main result of this investigation is that fewer time slots are required for link scheduling if users employ the AP selection policy proposed in chapter 5. We attribute this result to the reason that the proposed AP selection policy guides a new user to avoid a BSS that is interfered by other wireless nodes belonging to neighboring BSSs. Additionally, with fewer time slots, the proposed AP selection allows the activation of comparable number of links (with respect to RSSI-Based AP Selection). Consequently, it is rather better to use the time slotted access in conjunction with the AP selection policy proposed in chapter 5.

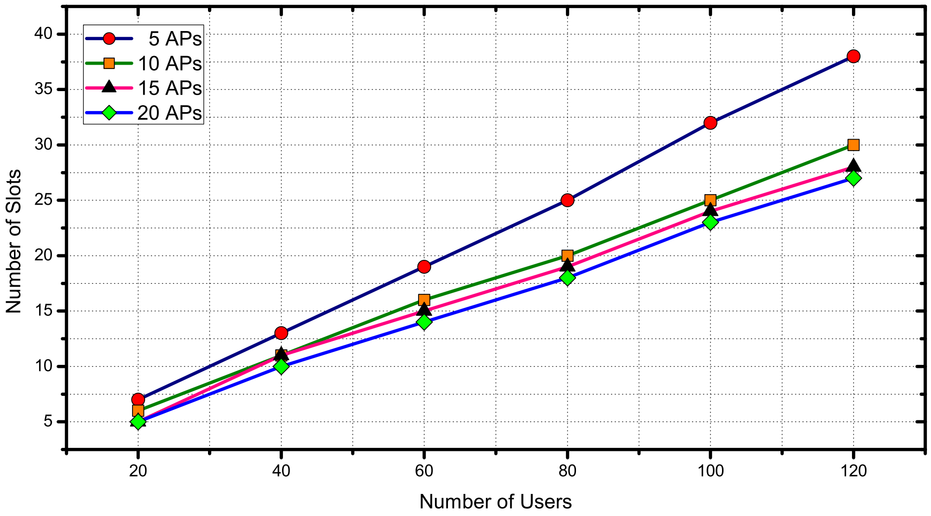


Figure 8.13: Time Slots Requirement with different number of APs and users - Proposed AP Selection

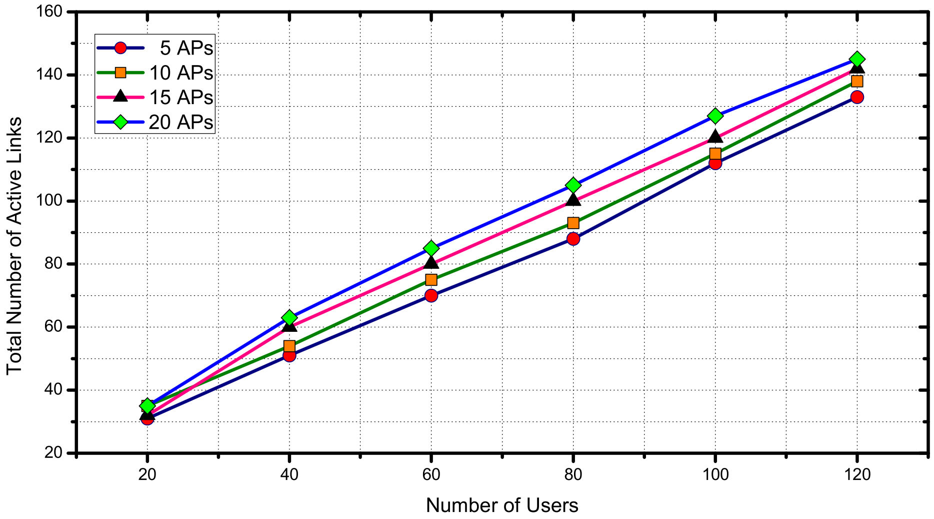


Figure 8.14: Activated Links with different number of APs and users - Proposed AP Selection

8.8 Impact of Interference Model on the Performance of Coordinated Channel Sharing

In this section, we study the impact of an interference model on the goodput performance of the coordinated channel access approach. We simulated multiple network topologies (different users and APs placements) using the measurement-based approach for determining interference relations (discussed in section 4.5) among the links as well as the simple interference model for different values of the factor d of equation 4.7. For the discussion of experiment results, the goodput performance for two topologies is plotted in figures 8.15 and 8.16. In the first topology, APs are spaced by 300m while in the second topology they are spaced by 200m. We make the following comments on

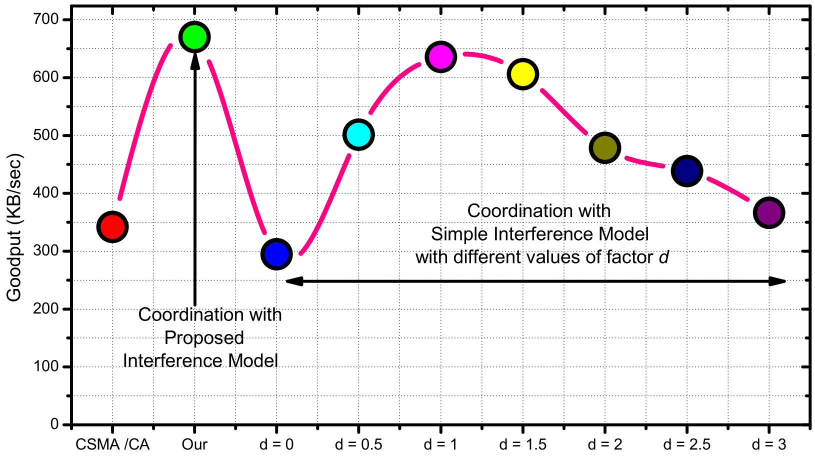


Figure 8.15: Network Goodput with Coordinated Channel Sharing for Different Interference Models

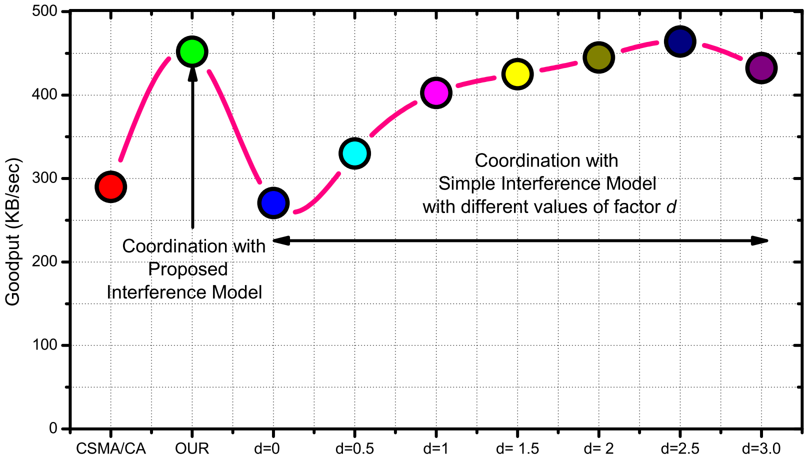


Figure 8.16: Network Goodput with Coordinated Channel Sharing for Different Interference Models

these results:

- The selection of an interference model for the time slotted modus does highly impact the achieved goodput. This is because the interference model for the determination of interfering links influences both the length of the schedule cycle (number of time slots required for scheduling the links) and the number of links that can be active in each time slot.

- For the examined values of the parameter d, the proposed measurement-based approach for the determination of interfering links achieves better goodput performance than the simple interference model.

- The simple interference model is very sensitive to the parameter d. Small changes in d translates to a considerable change in the achieved goodput.

- A proper selection of the d parameter is scenario dependent. In figure 8.15, the goodput performance using the simple interference model is comparable to proposed measurement-based approach for $d = 1$. Increasing the factor d reduces the range within which nodes will be identified as interferers and consequently leads to an increase in the number of time slots required for scheduling. The extra slots would not have been needed if the measurement approach is used. However, in figure 8.16, a value of $d = 2.5$ was necessary for comparable goodput performance to the proposed measurement-based approach.

8.9 Joint Performance of Coordinated Channel Sharing and the Proposed AP Selection and RTS/CTS tuning Policies

It is interesting to investigate the influence of an AP selection policy on the goodput performance when the network also switches to the time slotted operation modus. Experiments are also carried out to study this issue, where in these experiments 10 APs are used. They are hidden from each other. APs send CBR UDP data packets at a rate of 100 Packets / second to 80 users associated with them. Packet size was set to 1500 bytes. We investigate the goodput performance for the following cases:

1. The users use the RSSI-Based AP Selection and the CSMA/CA.

2. The users use the RSSI-Based AP Selection and APs enable the RTS/CTS.

3. The users use the RSSI-Based AP Selection and APs coordinate their transmissions.

4. The users use the proposed AP Selection (discussed in chapter 5) and the CSMA/CA.

5. The users use the proposed AP Selection and APs enable the RTS/CTS.

6. The users use the proposed AP Selection and APs coordinate their transmissions.

The results of these experiments are shown in figure 8.17. We make the following comments on these results.

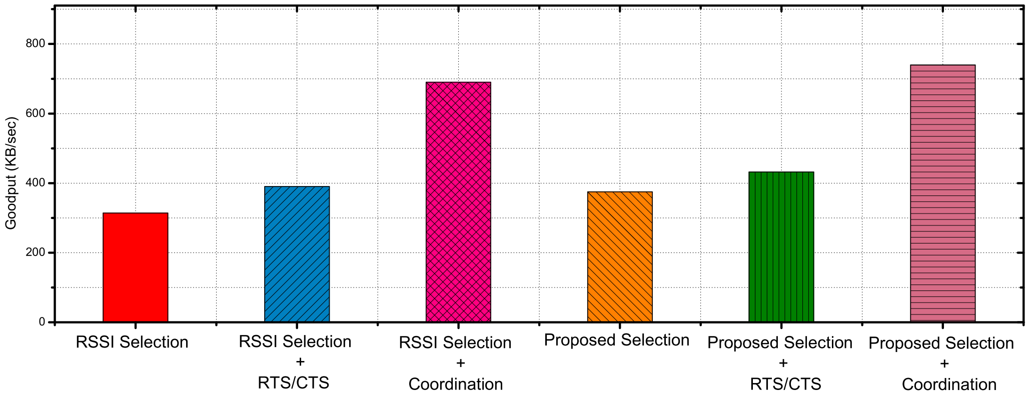


Figure 8.17: Network Goodput with Coordinated Channel Sharing, and the proposed AP Selection and RTS/CTS tuning Policies

- Regardless of the employed AP selection, the usage of RTS/CTS by the APs has improved the network goodput. However, the gain achieved with the mechanism is less if STAs select their APs with the proposed AP selection. The reason for this is that the proposed AP selection policy reduces some interference by guiding STAs to avoid BSSs within which high interference is expected. Consequently, the network suffers less from the hidden node problem. This leads to the result that the careful selection of the AP may reduce the necessity of using RTS/CTS.

- The network goodput with coordinated transmission was better for the case, wherein STAs employ the proposed AP selection policy. This is due the dependency of slot allocation results on the STAs associations which depends on the employed AP selection policy as shown in section 8.7.

8.10 Conclusions

In this chapter, it has been shown that the proposed coordination-based approach of chapter 7 is a promising strategy for interference mitigation in infrastructure WLANs. Through intensive simulations and real implementation, a good potential of the proposed policy has been observed, especially if jointly deployed with the AP selection policy proposed in chapter 5. We also showed that the approach can also be applied to chaotic deployment scenarios.

Chapter 9

Conclusions

Future WLANs should be cognitive. They should be able to monitor, learn, share information, and adapt to dynamical changes in the wireless environment. Such cognitive WLANs are promising to improve the quality of service of WLAN users.

This thesis contributes to the development of cognitive WLAN by developping a framework for interference mitigation. Within this framework, new STA-AP selection policy, criteria for RTS/CTS tuning, and coordination-based channel access mechanism are developed. The algorithms that drive the framework are based on observations and measurements.

The key technique used for measuring the interference impact at a receiving node is the packet loss discrimination jointly with passive observation of the wireless channel. It is shown that the developed methods for this purpose are able to characterize interference conditions. It is also shown that the impact of interference does not only depend on the received signal level from an interferer rather on other parameters such as the packet size and the transmission physical rate used by interferers. Despite the importance of the signal power received from interferers, the time span that interfering signal occupies the medium is also of significant importance regarding the impact of this signal on other nodes.

The improved STA-AP selection policy, proposed in chapter 5, tries to reduce the impact of interference at the selection phase. The policy considers other factors than the RSSI which impact the performance WLAN users experience. Such factors include inter-BSS and intra-BSS interferers, and channel occupancy time of nodes sharing the BSS, reducing the performance anomaly of 802.11. It is shown that such Interference-Aware AP selection policy improves the WLAN performance in terms of aggregate goodput, especially when the network load is high in terms of traffic pattern and number of users.

Then, we proposed criteria for improving the tuning of RTS/CTS signaling in order to mitigate interference resulted from hidden nodes across BSSs. In this context, we have shown that the RTS/CTS threshold should not be only determined by the packet size as the 802.11 standard recommends. This is because the cost of packet collision depends also on the rate at which collided packets have been transmitted, leading to the result that RTS/CTS tuning algorithms which try to reduce collisions due to hidden nodes shall be evaluated in multi-rate scenarios. The thesis has shown that introducing collaboration among interfering BSSs has the potential to improve the gain of the usage of RTS/CTS. We have found that RTS/CTS is helpful in improving operational conditions if the interference is due to hidden users that transmit uplink traffic to their APs. However, the RTS/CTS has been found to be not effective enough for mitigation of hidden node problem when APs are the hidden nodes and transmit high downlink traffic to the users they accommodate.

For further mitigation of interference, the thesis then developed a coordination-based channel access mechanism. Particularly, the thesis proposes a change of the channel access mechanism from the CSMA/CA to a time slotted access mechanism if RTS/CTS does not help to mitigate interference and the time slotted mechanism is expected to be helpful. Potential rules which drive the decision of channel access mode switch are also developed. Through simulation and real experimentation, it is shown that the proposed coordinated-based access scheme will be useful for improving users' QoS in terms of goodput and fairness, especially under high load and interference conditions. A case study based on real data has shown that the proposed policy will be beneficial for reducing interference impact also in chaotic deployment scenarios.

Overall, the proposed concepts throughout this thesis have shown good potential for improving the performance of current WLANs. They are expected to help the development of new cognitive WLAN products.

Appendix A

Source Code for Identifying Interfering BSSs Clusters.

```
/*
Programmed by: Murad Abusubaih, Telecommunication
Networks Group, Technical University Berlin.
Supervised by: Prof. Adam Wolisz.
This program finds the set of dense BSSs that should
employ a time slotted access scheme and those isolated
BSS that shall implement the CSMA/CA.
The input is a graph which edges represent the
interference among BSSs and nodes represent BSSs.
*/
#include <stdio.h>
#include <math.h>
#include <string.h>
#include <stdlib.h>
#include <time.h>
char *itoa(int value, char *digits, int base);
char *utoa(unsigned value, char *digits, int base);

int i,j;
int N=15,H;                 /* Number of BSSs */
int Done[15];               /* stores the already visited
                               BSSs*/
void PrepareMap();          /* reads an input graph from
                               a file*/
int FindNext();             /* find the next cluster root.*/
int AllDone();              /* check if all BSSs are
                               visited*/
void AddNeigbors(int I);/* Adds a found neighbor to the
                               cluster.*/
int MoreNeighbors(int I);/* Checks if there is more
                                interferring neighbor.*/
```

```
int FindNextNeigbor(int I);/* Finds the next
                             interferring BSS.*/
void CsmaNodes();
void WriteNodes();
/************************************************/
float Map[15][15];        /* represent interference
                             relation among BSSs*/
int CSMA[15],CS=0;
int Cluster[15][15];      /* Stores the members of each
                             cluster.*/
float Interference[15]; /* Stores the total
                             interference experienced
                             by each BSS.*/
float sum;
float InterfThreshold;    /* a threshold value above
                             which two BSS are assumed
                             to interfere.*/
int c,col,Cut;            /* c is cluster index*/
int ClusterSize=0,MaxClusterSize=1125;
/*Max Cluster Size, use a large number if you like
to ignore this restriction.*/
main()
{
int count;
InterfThreshold=250.0;
//GenerateGraph(N);
for (count=1;count<=1;count++){H=0;
c=0;    // c is cluster index
col=0;
//***************Initialize Arrays***************/
for (i=0;i<N; i++)
        for (j=0;j<N; j++)
                Cluster[i][j]=-10;
for (i=0;i<N;i++)
         Done[i]=0;
//**********************************************/
PrepareMap();
WriteNodes();
//***Finds the total interference at each BSS******/
for (i=0;i<N;i++)
        {
        sum=0;
        for (j=0;j<N;++j)
                {
                 if (Map[i][j]>InterfThreshold)
```

```
                                sum+=Map[i][j];
                      }

          if (count==1)
                    Interference[i]=1.0/sum;
          else
                    Interference[i]=1;
          }
/*********************************************************/
int Next;

while (!AllDone())     /* while some nodes are still
                          not members.*/
{
Next= FindNext();      /* find next cluster root, this
                          will be the one that measures
                          highest interf  and not a member
                          of any clusters yet.*/
ClusterSize=1;
Cut=0;
Cluster[c][col]=Next;
printf(”\n”);
printf(”********************************\n”);
printf(”*****Now Next Cluster for BSS %d******\n”,Next);
printf(”******************************************\n”);
printf(”\n”);
/* now include/add all interfering BSS and their
neighbors and neighbors of neigbors, it expands
until it reaches lightly region.
*/
AddNeigbors(Next);
c++;
col=0;
}
int Members,c1=0,c10=0;
printf(”\n\n********** Print Results ***********\n”);
for (i=0;i<N; i++)
{
if (Cluster[i][0]>=0)
          {
          printf(”Cluster %d Members are : ”,i+1);
          Members=0;
          }
          for (j=0;j<N; j++)
                    if (Cluster[i][j]>=0)
                    {
                    printf("BSS %d,  ",Cluster[i][j]);
                    Members++;
                    }
          if (Cluster[i][j]>=0)
                   {
                      printf("Members=%d\n",Members);
                      if (Members==1)
                           c1++;
                      if (Members>=10)
                           c10++;
                      printf("\n");
                   }
}
printf("H=%d\n",H);
CsmaNodes();
for (i=0;i<CS;i++)
          printf("CSMA=%d\n",CSMA[i]);
printf("CS=%d\n",CS);
printf("Nr of Clusters of one Member=%d\n",c1);
printf("Nr of Clusters of more that
                         10 Members=%d\n",c10);
}
}
/***********************************************/
void AddNeigbors(int I)
{
int K;
H++;
if (!MoreNeighbors(I))
  {
          printf("Not Found\n");
          return;
  }
ClusterSize++;
if (ClusterSize>MaxClusterSize)
  {
          printf("Cluster Cut\n");
          return;
  }
K=FindNextNeigbor(I);
printf("\nFound Interferring One BSS = %d\n",K);
Cluster[c][++col]=K;
Done[K]=1;
AddNeigbors(I);
AddNeigbors(K);
}
/***********************************************/
int MoreNeighbors(int I)
{
int s=0;
printf(”Now MoreNeighbors checks
      for BSS %d...”,I);
for (i=0;i<N;i++)
{
if (I!=i && Done[i]==0 && Map[I][i]<InterfThreshold)
        {
        s=1;
        break;
        }
}
return(s);
}
/***********************************************/
int FindNextNeigbor(int I)
{
int n;
int Matrix[6000],Loc[6000],c=0;
for (i=0;i<N;i++)
        if (Done[i]==0 && Map[I][i]<InterfThreshold)
        {
                Matrix[c]=Map[I][i];
                Loc[c]=i;
                c++;
        }
int Max=10000000;
for (i=0;i<c;i++)
        if (Matrix[i]<Max)
                {
                        Max=Matrix[i];
                        n=Loc[i];
                }
return(n);
}
/***********************************************/
void PrepareMap() {
FILE *fp;
char *line=(char *)malloc(256);
int i,j;
float n1,n2,n3,n4,n5,n6,
        n7,n8,n9,n10,n11,n12,n13,n14,n15;

fp=fopen("Map.txt","r");int r=0,c=0;
for (i=0;i<N*N; i++)
          {
          fscanf(fp, "%f", &Map[r][c++]);
          if (c==N)
                    {c=0;
                    r++;
                    }
          }
fclose(fp);

int COUNT=0,cn;
for (i=0;i<N; i++)
{
          cn=0;
          for (j=0;j<N; j++)
                    if (Map[i][j]<InterfThreshold)
                              cn++;
          if (cn>=10)
                    {
                    COUNT++;
                    printf("BSS %d\n",i);
                    }

}
printf("Nr. of BSSs that has more than
           10 neighbors is: %d\n",COUNT);
}
/*************************************************/
/**********************Functions*******************/
// Finds the next interfering AP
int FindNext()
{
int Max=100000000;
int Pos,k;
for (k=0;k<N;++k)
  if (Interference[k]<Max && Done[k]==0)
          {
                    Max= Interference[k];
                    Pos=k;
          }
Interference[Pos]=-10;//finished
Done[Pos]=1;
```

```
return(Pos);
}
/***********************************************/
int AllDone()
{
int d=1;
for (i=0;i<N; ++i)
        if (Done[i]!=1)
         {
                d=0;
                break;
         }
return(d);
}
/***********************************************/
void WriteNodes(){
FILE *fp;
fp=fopen(”/root/Nodes.txt”,”w”);

char fname[255]=”BSS”;
char fname1[255]=”BSS”;
char t[255],t1[255];

for (i=0;i<N; i++)
{
        char fname[255]=”BSS”;
        strcat(fname , itoa( i,t,10));
        for (j=0;j<N; j++)
        {
        char fname1[255]=”BSS”;
        strcat(fname1 , itoa( j,t,10));
        fprintf(fp,”%s\t%s\t%f\n”,fname,
                fname1,Map[i][j]);
        }
}
fclose(fp);
fp=fopen(”/root/MAP.txt”,”w”);
for (i=0;i<N; i++)
        {
        for (j=0;j<N; j++)
                fprintf(fp,”%.1f ”,Map[i][j]);
        fprintf(fp,”\n”);
        }
fclose(fp);
}
```

```
/****************************************************/
/* In case of limited cluster size,
this function determines the set of Neighboring
BSS that should run CSMA/CA despite in the time
slotted Modus */

void CsmaNodes(){
int i,j,k,Neighb,COUNT,STOP,n;
for (i=0; i<N; i++)
{
for (j=0; j<N; j++)
{
if (Map[i][j]<InterfThreshold && i!=j)
        Neighb=1;
else
        Neighb=0;
if (Neighb)
{
STOP=0;
for (k=0;k<N && !STOP; k++)
        {
        if (Cluster[k][0]>=0)
        {
        COUNT=0;
        for (n=0;n<N;n++)
        if (Cluster[k][n]==i || Cluster[k][n]==j)
                COUNT++;
        }
        if (COUNT==1)
        {
        int f=0,t;
        for (t=0;t<CS;t++)
                if (CSMA[t]==i)
                        f=1;
                if (!f) CSMA[CS++]=i;
                f=0;
                for (t=0;t<CS;t++)
                if (CSMA[t]==j) f=1;
                if (!f) CSMA[CS++]=j;
        }
        if (COUNT>0) STOP=1;
        }
}
}
}
```

```
}
/***********************************************/
char *itoa(int value, char *digits, int base)
{
    char *d;
    unsigned u;
    /* assume unsigned is big enough to hold all the
     * unsigned values -x could possibly be -- don't
     * know how well this assumption holds on the
     * DeathStation 9000, so beware of nasal demons
    */

    d = digits;
    if (base == 0)
        base = 10;
    if (digits == NULL || base < 2 || base > 36)
        return NULL;
    if (value < 0) {
        *d++ = '-';
        u = -((unsigned)value);
    } else
        u = value;
    utoa(u, d, base);
    return digits;
   }
char *utoa(unsigned value, char *digits, int base)
{
    char *s, *p;

    s = "0123456789abcdefghijklmnopqrstuvwxyz";
    /* don't care if s is in read-only memory*/
    if (base == 0)
        base = 10;
    if (digits == NULL || base < 2 || base > 36)
        return NULL;
    if (value < (unsigned) base) {
        digits[0] = s[value];
        digits[1] = '\0';
    }
else
{
for (p = utoa(value/((unsigned)base),digits,base);
*p;
p++);
atoa( value % ((unsigned)base), p, base);
}
return digits;
}
```

Bibliography

[1] IEEE Std. 802.11-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Reference number ISO/IEC 8802-11:1999(E), IEEE Std. 802.11, 1999 edition.

[2] William Stallings, Data and Computer Communications,Eighth Edition, 2007.

[3] Q. Pang, S. Liew, J. Lee, and V. Leung, Performance evaluation of an adaptive backoff scheme for WLAN, Wireless Communications and Mobile Computing, vol.4, issue 8, pp 867-879, December, 2004.

[4] L. Scalia, I. Tinnirello, G. Bianchi, MAC Parameters Tuning for Best Effort Traffic in 802.11e Contention-Based Networks, The Mediterranean Journal of Computers and Networks,January,2006.

[5] L. Scalia, I. Tinnirello, J.W. Trantra, C.H. Foh, Dynamic MAC Parameters Configuration for Performance Optimization in 802.11e Networks, IEEE Globecom 2006, November, 2006.

[6] Y. Xiao, IEEE 802.1 1 E: QOS PROVISIONING AT THE MAC LAYER, IEEE Wireless Communications, June, 2004.

[7] K.Ayyappan, I.Saravanan, G.Sivaradje and P.Dananjayan, Resource Management Strategy to Support Real Time Video Across UMTS and WLAN Networks, Proceedings of the 4th International Conference on Advances in Mobile Computing and Multimedia, Yogyakarta Indonesia, 2006.

[8] M. Heusse, F. Rousseau, G. Berge-Dabbatel, and A. Duda, Performance Anomaly of 802.11b, in Proc. of IEEE Infocom, March 2003.

[9] A. Rao and I. Stoica. An overlay MAC layer for 802.11 networks. *Proceedings of the 3rd international conference on Mobile systems, applications, and services*, 2005.

[10] R. Jain and D. Chiu. A Quantitative Measure Of Fairness And Discrimination For Resource Allocation In Shared Computer Systems. *DEC TR-301*, September, 1984.

[11] *IEEE 802.11k Radio Resource Measurement, IEEE Draft 2.0*, February 2005.

[12] IEEE 802.11 TGr, Fast BSS Transition, September 2006, P802.11r/D3.0.

[13] A. Kashyap, S. Ganguly, and S. Das. A measurement-based approach to modeling link capacity in 802.11 based wireless networks *In Proceedings of ACM MOBICOM*, 2007.

[14] IEEE Std. 802.11-2007, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11, 2007 edition.

[15] K. Whitehouse, A.Woo, F. Jiang, J. Polastre, and D Culler. Exploiting the capture effect for collision detection and recovery. *In Proceedings of EmNetS11*, 2005

[16] Ji-Hoon Yun and Seung-Woo Seo. Collision detection based on RF energy duration in ieee 802.11 wireless lan. *In Proceedings of Comsware*, 2006

[17] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, and S. Banerjee. Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal. *In Proceedings of IEEE INFOCOM08*, April, 2008.

[18] Qixiang Pang, Soung C. Liew, and Victor C. M. Leung. Design of an Effective Loss-Distinguishable MAC Protocol for 802.11 WLAN. *IEEE COMMUNICATIONS LETTERS*, 2006

[19] S. Wong, S. Lu, H. Yang, and V. Bhargavan. Robust rate adaptation for 802.11 wireless networks. *In Proceedings of ACM Mobicom*, 2006

[20] J. Kim. Cara: Collision-aware rate adaptation for ieee 802.11 wlans. *In Proceedings of INFOCOM06*, 2006

[21] D. Malone, P. Clifford, and D. J. Leith. MAC layer channel quality measurement in 802.11. *IEEE COMMUNICATIONS LETTERS*, February, 2007.

[22] Domenico Giustiniano, David Malone, Douglas J. Leith and Konstantina Papagiannaki. Experimental Assessment of 802.11 MAC Layer Channel Estimators. *IEEE COMMUNICATIONS LETTERS*, December, 2007.

[23] IEEE Std. 802.11k-2008, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 7: Radio Resource Measurement , IEEE Std. 802.11k, February, 2008.

[24] S. Y. Wang et al., NCTUns 3.0 Network Simulator and Emulator, http://nsl.csie.nctu.edu.tw/nctuns.html. http://isi.edu/nsnam/ns/

[25] http://isi.edu/nsnam/ns/.

[26] Anthony J. Nicholson, Yatin Chawathe, Mike Y. Chen, Brian D. Noble, and David Wetherall, Improved Access Point Selection, In Proceedings of MobiSys, June, 2006.

[27] W. Arbaugh, A. Mishra, and M. Shin, An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process, ACM SIGCOMM Computer Communication Review, March, 2003.

[28] Y. Bejerano and R. Bhatia, MIFI: A Framework for Fairness and QoS Assurance in Current IEEE 802.11 Networks with Multiple Access Points, in Proc. of IEEE Infocom, March 2004.

[29] Y. Fukuda and Y. Oie, Decentralized access point selection architecture for wireless LANs, IEICE Transaction on Communications, Vol. E90-B, Nr. 9, pp. 2513-2523, September, 2007.

[30] A. Balachandran, P. Bahl, and G. Voelker, Hot-spot congestion relief and service guarantees in public-area wireless networks, in SIGCOMM Computer Communication Review, 32(1), 2002.

[31] Y. Bejerano, S. Han, and L. Li, Fairness and load balancing in wireless lans using association control, in Proc. of ACM MOBICOM'04, 2004.

[32] G. Judd and P. Steenkiste, Fixing 801.11 access point selection, in Proc. In Poster in Proceedings of ACM MobiCom'02, 2002.

[33] O. Ekici and A. Yongacoglu, Predictive Association Algorithm for IEEE 802.11 WLAN, in Proc. of IEEE Inter. Conference on Information and Communication Technologies (ICTTA), April 2006.

[34] M. Berg and J. Hultell, On Selfish Distributed Access Selection Algorithms in IEEE 802.11 Networks, In Proceedings of 64th IEEE Vehicular Technology Conference, VTC-2006 Fall, September, 2006.

[35] Y. Taenaka, S. Kashihara, K. Tsukamoto, S. Yamaguchi, and Y. Oie, Terminal-Centric AP Selection Algorithm based on Frame Retransmissions, In Proceedings of the 2nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks, October, 2006.

[36] V. Siris and D. Evaggelato., Access Point Selection for Improving Throughput Fairness in Wireless LANs, In Proceedings of 10th IFIP/IEEE International Symposium on Integrated Network Management, IM '07, May, 2007.

[37] L. Du, Y. Bai, and L. Chen, Access Point Selection Strategy for Large-scale Wireless Local Area Networks, In Proceedings of IEEE Wireless Communications and Networking Conference WCNC 2007, March, 2007.

[38] Y. Fukuda, M. honjo, and Y. Oie, Development of Access Point Selection Architecture with Avoiding Interference for WLANs, In Proceedings of the 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06), 2006.

[39] B. Kauffmann, F. Baccelli, A. Chaintreau, V. Mhatre, K. Papagiannaki, and C. Diot, Measurement-Based Self Organization of Interfering 802.11 Wireless Access Networks,In Proceedings of the 26th IEEE International Conference on Computer Communications. IEEE INFOCOM 2007, May, 2007.

[40] M. Abusubaih, and A. Wolisz, Interference-Aware Decentralized Access Point Selection Policy for Multi-Rate IEEE 802.11 Wireless LANs,In Proceedings of the he 19'th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008, September, 2008.

[41] G. Holland, N. Vaidya, and P. Bahl, A Rate-Adaptive MAC Protocol for Multi-Hop Wireless Networks, in Proc. of ACM/IEEE Mobicom, July 2001.

[42] O. Ekici and A. Yongacoglu,A Novel Association Algorithm for Congestion Relief in IEEE 802.11 WLANs. *In Proceedings of the International Wireless Communications and Mobile Computing Conference*, July, 2006.

[43] A. Kumar and V. Kumar, Optimal Association of Stations and APs in an IEEE 802.11 WLAN, in Proc. of Nat. Conf. on Communications (NCC), February 2005.

[44] F. Guo and T. Chiueh, Scalable and Robust WLAN Connectivity Using Access Point Array, in Proc. of Inter. Conf. on Dependable Systems and Networks (DNS'05), June 2005.

[45] L. Gavrilovska and V. Atanasovski, Influence of Packet Length on IEEE 802.11b Throughput Performance in Noisy Channels, in Proc. of 1st Inter. MAGNET Workshop, November 2004.

[46] G. Bianchi and I. Tinnirello, Channel-dependent Load Balancing in Wireless Packet Networks, Wireless Communications and Mobile Computing, Number 4, 43-53, 2004.

[47] *Lingo User's Guide, LINDO Systems, Inc., Chicago, II*, 2004.

[48] D. Qiao, S. Choi, A. Soomro, and K. Shin, Energy-Efficient PCF Operation of IEEE802.11a Wireless LAN, in Proc. of IEEE Infocom, June 2002.

[49] Y. Fukuda and Y. Oie, Decentralized Access Point Architecture for Wireless LANs: Deployability and Robustness, in Proc. of IEEE Vehicular Technology Conference, September 2004.

[50] M.Abusubaih, James Gross, S.Wiethoelter, and A.Wolisz, On Access Point Selection in IEEE 802.11 Wireless Local Area Networks, in Proc. of Sixth IEEE International Workshop on Wireless Local Networks (WLN 2006), November 2006.

[51] Murad Abusubaih, Sven Wiethoelter, James Gross, and Adam Wolisz, A New Access Point Selection Policy for Multi-Rate IEEE 802.11 WLANs, International Journal of Parallel, Emergent and Distributed Systems (IJPEDS), vol. 23, pp. 291 – 307, August 2008.

[52] P. Huang, Y. Tseng, and K. Tsai, A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks, in Proc. of IEEE Vehicular Technology Conference, May 2006.

[53] *http://crawdad.cs.dartmouth.edu/.*

[54] *http://www.caida.org/tools/measurement/coralreef/.*

[55] Chi Pan Chan, Soung Chang Liew, and An Chan. Many-to-One Throughput Capacity of IEEE 802.11 Multi-hop Wireless Networks. *IEEE TRANSACTIONS ON MOBILE COMPUTING*, 2007.

[56] Ting-Chao Hou and Ling-Fan Tsao and Hsin-Chiao Liu. Analyzing the throughput of IEEE 802.11 DCF scheme with hidden nodes. *In Proceedings of the IEEE 58th Vehicular Technology Conference VTC 2003-Fall*,October, 2003.

[57] Y. Li and X. Wang and S.A. Mujtaba. Co-channel interference avoidance algorithm in 802.11 wireless LANs. *In Proceedings of the IEEE 58th Vehicular Technology Conference VTC 2003-Fall*,October, 2003.

[58] Woo-Yon and Choi and Sok-Kyu Lee. A real-time updating algorithm of RTS-CTS threshold to enhance EDCA MAC performance in IEEE 802.11e wireless LANs. *In Proceedings of the IEEE 60th Vehicular Technology Conference VTC 2004-Fall*,September, 2004.

[59] Liang Zhang and Yantai Shu. RTS threshold self-tuning algorithm based on delay analysis on 802.11 DCF. *In Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing*,September, 2005.

[60] Jun Liu and Wei Guo and Bai long Xiao and Fei Huang. RTS Threshold Adjustment Algorithm for IEEE 802.11 DCF. *In Proceedings of the 6th International Conference on ITS Telecommunications*,June, 2006.

[61] J.L. Sobrinho and R. de Haan and J.M Brazio. Why RTS-CTS is not your ideal wireless LAN multiple access protocol. *In Proceedings of the 6th International Conference on ITS Telecommunications*,March, 2005.

[62] A. Rahman and P. Gburzynski. Hidden Problems with the Hidden Node Problem. *In Proceedings of the 23rd Biennial Symposium on Communications*, June, 2006.

[63] P. Raptis and A. Banchs and V. Vitsas and K. Paparrizos and P. Chatzimisios. Delay Distribution Analysis of the RTS/CTS mechanism of IEEE 802.11. *In Proceedings of the 31st IEEE Conference on Local Computer Networks IEEE LCN*, Tampa, Florida, USA, November, 2006.

[64] Chin Keong Ho and Jean-Paul M. G. Linnartz. Delay Distribution Analysis of the RTS/CTS mechanism of IEEE 802.11. *In Proceedings of the 17th Annual IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06)*, 2006.

[65] Saikat Ray and David Starobinski. On False Blocking in RTS/CTS - Based Multihop Wireless Networks. *In IEEE Transactions on Vehicular Technology*, March, 2007.

[66] M.Abusubaih, B.Rathke, and A.Wolisz. Collaborative Setting of RTS/CTS in Multi-Rate Multi-BSS IEEE 802.11Wireless LANs. *In Proceedings of the 16'th IEEE Workshop on Local and Metropolitan Area Networks, IEEE LANMAN'08*, September, 2008.

[67] S. Khurana and A. Kahol and A.P. Jayasumana. Effect of Hidden Terminals on the Performance of IEEE 802.11 MAC Protocol. *In Proceedings of 23rd Annual Conference on Local Computer Networks LCN 98*,October, 1998.

[68] T. Moscibroda, R. Wattenhofer, and Y. Weber. Protocol Design Beyond Graph-based Models *In Proceedings of the 5th ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets1)*, 2006.

[69] J. Riihijarvi, M. Petrova, and P. Mahonen. Frequency allocation for WLANs using graph colouring techniques. *Proceedings of Second Annual Conference on Wireless On-demand Network Systems and Services WONS 2005*, January, 2005.

[70] A. Mishra, V. Brik, S. Banerjee, A. Srinivasan, and W. Arbaugh. Efficient Strategies for Channel Management in Wireless LANs *Technical Report-CS-TR-4729 and UMIACS-TR-2005-36 , University of Maryland*, June, 2005.

[71] M. Abusubaih, J. Gross, and A. Wolisz. An Inter-AP Coordination Protocol for IEEE 802.11 WLANs. *Proceedings of 1st IEEE Workshop on Autonomic Communications and Network Management (ACNM 2007)*, Munich, Germany, May, 2007.

[72] A. Sharma, M. Tiwari and H. Zheng. MadMAC: Building a Reconfiguration Radio Testbed using Commodity 802.11 Hardware. *Proceedings of the IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, September, 2006.

[73] Yigal Bejerano and Randeep S. Bhatia. MiFi: A Framework for Fairness and QoS Assurance for Current IEEE 802.11 Networks With Multiple Access Points *IEEE/ACM Transactions on Networking, vol. 14, No. 4, pp. 849-862*, August, 2006.

[74] H. Liu, H. Yu, X. Liu, C. Chuah, and P. Mohapatra. Scheduling Multiple Partially Overlapped Channels in Wireless Mesh Networks. *Proceedings of IEEE ICC 2007*, June, 2007.

[75] Leonardo Badia and Alessandro Erta,. A General Interference-Aware Framework for Joint Routing and Link Scheduling in Wireless Mesh Networks. *IEEE Network*, Vol. 22, pp. 32-38, 2008.

[76] D. Chafekar, D. Levin, V. S. Anil Kumar, M. V. Marathe, S. Parthasarathy, and A. Srinivasan. Capacity of Asynchronous Random-Access Scheduling in Wireless Networks. *Proceedings of IEEE INFOCOM'08*, April, 2008.

[77] W. Wang, X. Liu, and D. Krishnaswamy.Robust Routing and Scheduling in Wireless Mesh Networks. *Proceedings of 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON '07.*, June, 2007.

[78] W. Wangy, Y. Wang, X. Yang, L. Wen, Z. Songz, and O. Friedery. Efficient Interference-Aware TDMA Link Scheduling for Static Wireless Networks. *Proceedings of ACM MobiCom'06*, September, 2006.

[79] James F. Kurose and Keith W. Ross. Computer Networking: A Top-Down Approach (4th Edition) *Addison Wesley*, April, 2007.

[80] http://www.winlab.rutgers.edu/ ergin/mobicom2007/

[81] M. Abusubaih, B. Rathke, and A.Wolisz. A framework for Interference Mitigation in Multi-BSS 802.11 Wireless LANs. *In Proceedings of the 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2009)*, June, 2009.

[82] M. Abusubaih, J. Gross, S. Wiethoelter, and A. Wolisz, On Access Point Selection in IEEE802.11 Wireless Local Area Networks,In Proceedings of 6'th IEEE International Workshop on Wireless Local Networks, WLN'06, Tampa, FL, USA, November, 2006.

[83] A. Sang, X. Wang, M. Madihian, and R. Gitlin, Coordinated Load Balancing Handoff/Cell-Cite Selection and Scheduling in Multi-Cell Packet Data Systems, in Proc. of ACM/IEEE Mobicom, September 2004.

[84] A. Tang, J. Wang and S. Low, Is Fair Allocation always Inefficient, In Proc. of IEEE Infocom, March, 2004.

[85] S. Wiethoelter,Virtual Utilization and VoIP Capacity of WLANs Supporting a Mix of Data Rates, Technical Report TKN-05-004, Telecommunication Networks Group, Technische Universität Berlin, September 2005.

[86] J. Manner, Jugi's Traffic Generator (jtg), http://www.cs.helsinki.fi/u/jmanner/software/.

[87] Li Bin Jiang and Soung Chang Liew. Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks. *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 7, no. 1, January 2008.

[88] V. Bharghavan, MACAW: A Media Access Protocol for Wireless LANs, Proceedings of the conference on Communications architectures, protocols and applications, 1994.

[89] P. Karn, MACA: A New Channel Access Method for Packe Radio, Proceedings of ARRL/CRRL Amateur Radio 9'th Computer Networking Conference, September, 1990.

[90] Shiann-Tsong and Sheu Chen and T. Jenhui and Chen Fun Ye. The impact of RTS threshold on IEEE 802.11 MAC protocol. *In Proceedings of the Ninth International Conference on Parallel and Distributed Systems*,December, 2002.

[91] A. Mishra, S. Banerjee, and W. Arbaugh. Weighted coloring based channel assignment for WLANs. *Proceedings of ACM SIGMOBILE Mobile Computing and Communications*, 2005.

[92] S. Gobriel, R. Melhem, and D. Mosse. A Unified Interference/Collision Model for Optimal MAC Transmission Power in Adhoc Networks *In International Journal of Wireless and Mobile Computing*, Volume 1, Number 3/4, pp 179-190, August,2006.

[93] V. Kawadia and P. R. Kumar. Principles and protocols for power control in adhoc networks *In IEEE Journal on Selected Areas in Communications*, Vol I, 2005.

[94] A. Akella, G. Judd, S. Seshan, and P. Steenkiste. Self-management in chaotic wireless deployments *In Proceedings of the ACM MobiCom*, August, 2005.

[95] P. Gupta and P. R. Kumar. The Capacity of Wireless Networks *In IEEE Transactions on Information Theory*, 46(2), 2000.

[96] D. Kotz, C. Newport, R. S. Gray, J. Liu, Y. Yuan, and C. Elliott. Experimental evaluation of wireless simulation assumptions *In Proceedings of MSWiM*, October, 2004.

[97] A. Behzad and I. Rubin. On the performance of graphbased scheduling algorithms for packet radio networks *In Proceedings of GlobeCom*, 2003.

[98] J. Gronkvist and A. Hanssonn. Comparison between graphbased and interference-based STDMA scheduling *In Proceedings of ACM MobiHoc*, 2001.

[99] Charles Reis, Ratul Mahajan, Maya Rodrig, David Wetherall, and John Zahorjan. Measurement based models of delivery and interference in static wireless networks *In Proceedings of the 2006 ACM conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM*, 2006.

[100] Jitendra Padhye, Sharad Agarwal, Venkata N. Padmanabhan, Lili Qiu, Ananth Rao, and Brian Zill. Estimation of Link Interference in Static Multihop Wireless Networks *In Proceedings of the the Internet Measurement Conference, IMC05*, 2005.

[101] Dragos Niculescu. Interference map for 802.11 networks *In Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, 2007.

[102] S. M. Das, D. Koutsonikolas, Y. C. Hu, and D. Peroulis. Characterizing multi way interference in wireless mesh networks *In Proceedings of WiNTECH06*, 2006.

[103] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu. Impact of Interference on Multihop Wireless Network Performance. *In Proceedings of MOBICOM*, 2003.

[104] D. Chiu and R. Jain Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks *Journal of Computer Networks and ISDN Systems*, vol. 17,Nr.1, pp. 1-14, June, 1989.

List of Personal Publications

• Journal Papers

1. Murad Abusubaih, Sven Wiethoelter, James Gross, and Adam Wolisz, “A New Access Point Selection Policy for Multi-Rate IEEE 802.11 WLANs”, International Journal of Parallel, Emergent and Distributed Systems (IJPEDS), vol. 23, pp. 291 – 307, August 2008.
2. W. Hu, D. Willkomm, L. Chu, M. Abusubaih, J. Gross, G. Vlantis, M. Gerla, and A. Wolisz, “Dynamic Frequency Hopping Communities for Efficient IEEE 802.22 Operation”, IEEE Communications Magazine, Special Issue: Cognitive Radios for Dynamic Spectrum Access, vol. 45, no. 5, pp. 80-87, May 2007.

• Conference Proceedings

1. M.Abusubaih,B.Rathke, and A.Wolisz, ”A Framework for Interference Mitigation in Multi-BSS 802.11Wireless LANs”, In Proc. of the The 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2009, Kos, Greece, June 2009.
2. M.Abusubaih, B.Rathke, and A.Wolisz, ”Collaborative Setting of RTS/CTS in Multi-Rate Multi-BSS IEEE 802.11Wireless LANs”, In Proc. of the 16’th IEEE Workshop on Local and Metropolitan Area Networks, IEEE LANMAN’08, Cluj-Napoca, Romania, September 2008.
3. M.Abusubaih and A.Wolisz, ”Interference-Aware Decentralized Access Point Selection Policy for Multi-Rate IEEE 802.11 Wireless LANs”, In Proc. of the 19’th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008., Cannes, France, September 2008.
4. M.Abusubaih and A.Wolisz, ”An Optimal Station Association Policy for Multi-Rate IEEE 802.11 Wireless LANs”, In Proc. of the 10’th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Networks (MSWIM’07), Chania, Crete Island, Greece, October 2007.
5. M.Abusubaih, B.Rathke, and A.Wolisz, ”A Dual Distance Measurement Scheme for Indoor IEEE 802.11 Wireless Local Area Networks”, In Proc. of the 9’th IFIP/IEEE International Conference on Mobile and Wireless Communication Networks (MWCN’07), Cork, Ireland, September 2007.
6. M.Abusubaih, J.Gross, and A.Wolisz, ”An Inter-Access Point Coordination Protocol for Dynamic Channel Selection in IEEE802.11 Wireless LANs”, In Proc 1st IEEE Workshop on Autonomic Communications and Network Management (ACNM 2007), Munich, Germany, May 2007.

7. M.Abusubaih, James Gross, S.Wiethoelter, and A.Wolisz, ”On Access Point Selection in IEEE 802.11 Wireless Local Area Networks”, In Proc. of the Sixth International Workshop on Wireless Local Networks (WLN 2006), Tampa, FL, USA, November 2006.

Standardisation

1. Liwen Chu, Wendong Hu, George Vlantis, James Gross, Murad Abusubaih, Daniel Willkomm, and Adam Wolisz, ”Dynamic Frequency Hopping Community”, doc. 22-06-0113, IEEE 802.22 Working Group, June 2006, Technical proposal submitted to IEEE 802.22 WG.

Technical Research Reports

1. M.Abusubaih, Adam Wolisz, Berthold Rathke, and Daniel Hollos, ”A Framework for Interference Mitigation in Multi-Cell 802.11 Wireless LANs”, Technical Report TKN-08-011, Telecommunication Networks Group, Technical University Berlin, November 2008.
2. M.Abusubaih, Berthold Rathke, and Adam Wolisz, ”Packet Loss Discrimination in Multi-Cell 802.11 Wireless LANs”, Technical Report TKN-08-010, Telecommunication Networks Group, Technical University Berlin, October 2008.
3. M.Abusubaih and James Gross, ”Inter-AP Coordination Protocols”, Technical Report TKN-06-005, Telecommunication Networks Group, Technical University Berlin, August 2006.