Universidad de Las Palmas de Gran Canaria

Departamento de Señales y Comunicaciones

Programa: Tecnologías de las Telecomunicaciones

Tesis Doctoral

Caracterización y Modelado de Prestaciones en Redes Inalámbricas para Aplicaciones con Calidad de Servicio

Domingo Marrero Marrero

Las Palmas de Gran Canaria, Octubre 2015

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Departamento de Señales y Comunicaciones

Anexo I

DON PEDRO JOSE QUINTANA MORALES SECRETARIO DEL DEPARTAMENTO DE SEÑALES Y COMUNICACIONES DE LA UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA,

CERTIFICA,

Que la Comisión de Investigación del Departamento (que tiene delegadas las competencias en materia de doctorado), en su sesión de fecha tres de noviembre de dos mil quince, tomó el acuerdo de dar el consentimiento para su tramitación, a la tesis doctoral titulada "CARACTERIZACIÓN Y MODELADO DE PRESTACIONES EN REDES INALÁMBRICAS PARA APLICACIONES CON CALIDAD DE SERVICIO" presentada por el doctorando Don Domingo Marrero Marrero y dirigida por los Doctores Don Álvaro Suárez Sarmiento y Doña Elsa María Macías López.

Y para que así conste, y a efectos de lo previsto en el Artº 6 del Reglamento para la elaboración, defensa, tribunal y evaluación de tesis doctorales de la Universidad de Las Palmas de Gran Canaria, firmo la presente en Las Palmas de Gran Canaria a, tres de noviembre de dos mil quince.

t +34 928 451 265
f +34 928 451 279
e-mail secretaria@dsc.ulpgc.es
www.dsc.ulpgc.es
Edificio de Electrónica y Telecomunicaciones
Campus de Tafira
35017 Las Palmas de Gran Canaria

Anexo II

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

Departamento de Señales y Comunicaciones

Programa de doctorado: Tecnologías de las Telecomunicaciones

(bienio 98/00)

Caracterización y Modelado de Prestaciones en Redes Inalámbricas para Aplicaciones con Calidad de Servicio

Tesis Doctoral presentada por D/Dª DOMINGO MARRERO MARRERO

Dirigida por el Dr/a. D. Álvaro Suárez Sarmiento

Codirigida por el Dr/a. Dª. Elsa Mª Macías López

El/la Director/a, **El/la Codirector/a** **El/la Doctorando/a,**

(firma) **(firma)** **(firma)**

Las Palmas de Gran Canaria, a 09 de Octubre de 2015

A mi familia y

a las personas que me aprecian

AGRADECIMIENTOS

Llegados a este momento considero muy importante agradecer a todas aquellas personas que de una forma u otra me han animado o ayudado a la realización de esta tesis doctoral.

De manera especial a Álvaro Suarez y Elsa Macías por su tiempo, apoyo, sugerencias y ayuda en la finalización de la misma y por su esfuerzo y dedicación a la hora de elaborar las distintas publicaciones que han surgido durante su desarrollo.

Igualmente agradecer la colaboración en la parte final de la misma de José A. Santana y Vicente Mena por sus diferentes aportaciones.

También debo agradecer al resto de compañeros que se han interesado por su finalización.

Por último, agradecer especialmente a mi familia por su paciencia y sacrificio.

Las Palmas de G.C., Octubre 2015

Índice de contenidos

Índice de figuras

Índice de tablas

Acrónimos

AOA	Angle of Arrival
AP	Access Point
AVC	Advanced Video Coding
BS	Base Station
BSS	Basic Service Set
CBQ	Class Based Queuing
CBR	Constant Bit Rate
CSI	Channel State Information
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CDMA	Code Division Multiple Access
codec	Coder-Decoder
CW	Contention Window
DCF	Distributed Coordination Function
DCOM	Distributed Component Object Model
DECT	Digital Enhanced Cordless Telecommunications
DiffServ	Differentiated Services
DFS	Distribution fairness Scheduling
DHCP	Dynamic Host Configuration Protocol
DIFS	DCF InterFrame Space
DLNA	Digital Living Network Alliance
DNS	Domain Name Server
DRR	Deficit Round Robin
DS	Distribution System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSMASK	Differentiated Service Masking
DSSS	Direct Sequence Spread Spectrum
DVD	Digital Versatile Disc
EBSS	Extended Basic Service Set
ECN	Explicit Congestion Notification
EDCF	Extended Distributed Coordination Function

EDGE	Enhanced Data Rates for GSM Evolution
EGPRS	Enhanced GPRS
EMI	ElectroMagnetic Interference
FDD	Frequency Division Duplex
FDM	Frequency Division Multiplexing
FG	Fair Queue
FHSS	Frequency Hopping Spread Spectrum
FIFO	Fisrt In First Out
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GREM	Generic Random Early Detection
GSM	Global System for Mobile Communication
HDTV	High Definition TV
HEVC	High Efficiency Video Coding
HFSC	Hierarchical Fair Service Curves
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSUPA	High Speed Uplink Packet Access
HTB	Hierarchical Token Bucket
HTTP	HyperText Transfer Protocol
IBSS	Independent Basic Service Set
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMQ	Intermediate Queuing
IntServ	Integrated Services
IoT	Internet Of Things
IP	Internet Protocol
IPTV	Internet Protocol Television
IR	InfraRed
IRC	Internet Relay Chat
ISM	Industrial, Science and Medical
ISO	International Organization for Standardization
ITU	International Telecommunication Union

JTC /SC	Joint Technical Committees/Subcommittee
LLF	Least Loaded First
LMDS	Local Multipoint Distribution Service
LQI	Link Quality Indicator
LRW	Linux Router Wireless
LTE	Long Term Evolution
MAC	Medium Access Control
MANET	Mobile Ad-hoc NETworks
MIMO	Multiple In Multiple Out
MOS	Mean Opinion Score
MPEG	Moving Picture Expert Group
MPTCP	Multipath Transmission Control Protocol
NAS	Network Access Server
NAT	Network Address Translation
NDIS	Network Driver Interface Specification
OFDM	Orthogonal Frequency Division Multiple
OFDMA	Orthogonal Frequency Division Multiple Access
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PEVQ	Perceptual Evaluation of Video Quality
PEAQ	Perceptual Evaluation Audio Quality
PESQ	Perceptual Evaluation Speech Quality
POLQA	Perceptual Objective Listening Quality Analysis
PQ	Priority Queue
PSQM	Perceptual Speech Quality Measure
QoE	Quality of Experience
QoS	Quality of Service
RED	Random Early Dropping
REM	Random Early Detection
RSSI	Received Strength Signal Indicator
RSVP	Resource reSerVation Protocol
RTLS	Real Time Location System
RTP/UDP	Real Time Protocol/User Datagram Protocol
RTT	Round Trip Time

SDTV	Standard Definition Television
SFQ	Stochastic Fairness Queuing
SIFS	Short InterFrame Space
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNR	Signal to Noise Ratio
SSF	Strongest Signal First
SSH	Secure Shell
SSID	Service Set Identifier
SSL/TLS	Secure Socket Layer/Transport Layer Security
TBF	Token Bucket Fair
TCP	Transmission Control Protocol
TC	Traffic Control
TCINDEX	Traffic Control INDEX
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TDOA	Time Difference of Arrival
TOA	Time of Arrival
ToS	Type of Service
TTL	Time to Live
TXOP	Transmission Opportunity
UIT	Union International Telecommunication
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VBR	Variable Bit Rate
VQEG	Video Quality Experts Groups
VoD	Video Over Demand
VoIP	Voice Over IP
WDS	Wireless Distribution System
WiFi	Wireless Fidelity
WiGig	Wireless Gigabit
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extension

WMM	Wi-Fi MultiMedia
WNIC	Wireless Network Interface Card
WPAN	Wireless Personal Area Network
WRR	Weighted Round Robin
WSN	Wireless Sensor Network

Capítulo 1. Introducción

En este capítulo se realiza una introducción y presentación de la presente tesis doctoral, concretamente en los aspectos relacionados con sus orígenes, los antecedentes, la contextualización de la misma en el ámbito de las redes inalámbricas en general y WiFi en particular, y su uso para servicios que requieren calidad. Posteriormente se describen los objetivos que nos planteamos al inicio de la misma, las contribuciones que se aportan y la difusión de las mismas a la literatura, pasando por el estado actual de la investigación relacionada con las diferentes líneas de trabajo aquí contempladas. Finalmente se describe la organización global de los diferentes capítulos y apartados del presente documento.

1.1 Antecedentes

Las redes de comunicaciones de datos, las tecnologías y nuevos servicios soportados han inundado nuestras vidas. Términos como banda ancha, que constituye un nuevo conjunto de soluciones para conectividad, aparecen de forma habitual en nuestro vocabulario. Por otro lado, lo que representa hoy día Internet y su uso está omnipresente en el acervo cultural de nuestra Sociedad. Esto se debe en gran medida a la evolución y desarrollo de las tecnologías de comunicación de ámbito global, la estandarización de normas a nivel mundial y la reducción de costes de producción. Ya utilizamos Internet para comunicaciones entre personas, entre personas y máquinas o entre máquinas y máquinas.

Las tecnologías o métodos de acceso a Internet mayoritariamente utilizadas son:

- Línea digital de abonado (*DSL*, del inglés *Digital Subscriber Line*)
- Cable Módem
- Fibra Óptica
- Inalámbrica - Celular

De entre estas tecnologías, constituye un hecho muy revelador el que un elevado número de los hogares y empresas que cuentan con conectividad DSL o Fibra óptica (o similares), disponen en su mayoría con redes basadas en tecnología *Wireless Fidelity* (*WiFi*). Además se usan masivamente en múltiples zonas de ocio, aeropuertos, hoteles, centros comerciales y de negocios, estaciones de tren o autobús, instalaciones deportivas, avenidas... de forma gratuita o con regulación de uso. También conectan impresoras, *Network Access Server* (*NAS*), teléfonos de *Voz sobre Internet Protocol* (*VoIP*) o Telefonía IP, terminales para *streaming* o *Televisión sobre IP* (*IPTv*)... Es la base de muchos servicios basados en teléfonos móviles actuales y en la próxima generación de la Internet móvil (5G). En la actualidad, también se aplica para conectar objetos cotidianos en la denominada *Internet Of Things* (*IoT*).

Por último destacar que WiFi fue la tecnología más usada en las *Personal Digital Assistant* (*PDA*), y actualmente en los ordenadores portátiles y las tablets. Estos terminales interactúan cada vez más con equipos de ocio y entretenimiento, de manera especial en el sector audiovisual, en el que es cada vez más habitual encontrarlos

incorporando esta tecnología, sin la cual pierden funcionalidad. Todo ello dirigido hacia permitir conectividad local sin cables, y disponer de nuevos servicios y protocolos como: *Digital Living Network Alliance* (*DLNA*), control remoto, otros.

1.2 Motivación

Una vez realizada una visión general y contextual de las redes de acceso a Internet, deberíamos analizar que uso le estamos dando, y preguntarnos si realmente los requisitos o niveles de calidad están garantizados en todos los casos.

Se detecta un creciente aumento de la migración de la telefonía en redes dedicadas y la VoIP hacia la Telefonía IP. Los servicios de Televisión en redes dedicadas están dando paso a IPTv, y a una proliferación de servicios multimedia extremo a extremo, la mayor parte de ellos basados en servicios web, que se combinan naturalmente con servicios como: comercio electrónico, marketing, administración electrónica, transacciones comerciales, servicios de telecontrol y vigilancia. En la Figura 1 mostramos la integración de diferentes tecnologías y servicios en el contexto de Internet.

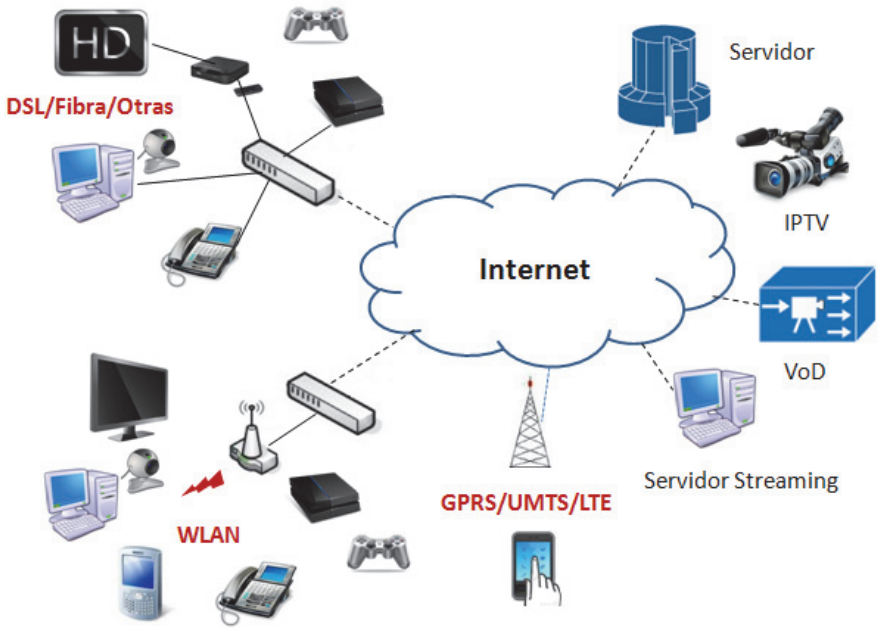


Figura 1. Integración de tecnologías de redes y servicios

La complejidad de los servicios anteriores, debido a la demanda de elevados volúmenes de datos en tiempo real y de forma interactiva, dificulta su implantación

sobre las redes de acceso móviles e inalámbricas. Por ejemplo, recordar que el servicio de videoconferencia nunca tuvo éxito en las redes móviles 3G y tampoco lo está teniendo en las 4G. Algo similar sucede con WiFi. Cabría por tanto preguntarse: por qué estas redes de acceso celulares o inalámbricas no soportan eficientemente estos servicios garantizando un mínimo de *Calidad de Experiencia de Usuario* (*QoE*, del inglés *Quality of Experience*), y son bastante dependientes de las condiciones de su uso (número de usuarios simultáneos, interferencias...).

En este contexto planteamos la tesis doctoral: la detección de usos incómodos, y muy habituales, de WiFi para el usuario. Ejemplos habituales son los problemas a la hora de asociar un terminal a un AP contando con suficiente nivel de señal; comunicaciones de video que se detienen, entrecortan o pixelan en exceso; ineficiente control de conexiones durante la movilidad del terminal; y otras. Para comprenderlo estudiamos la arquitectura WiFi, su tecnología, sus estándares, sus características y, sus configuraciones en diferentes sistemas operativos, drivers y dispositivos. Además, se detectan mayores problemas con el uso de aplicaciones dependientes del tiempo, en general comunicaciones multimedia. Consideramos que muchas veces los usuarios no hacemos uso de ciertos servicios, plenamente implantados, no porque no le veamos utilidad práctica, sino porque la red que le tiene que dar soporte y conectividad no lo garantiza. Para conocer mejor este tipo de comunicaciones, fue necesario hacer también un estudio de las tecnologías multimedia, formatos y estándares. Y, en general, entender los requisitos que tienen estos contenidos, su transmisión y las aplicaciones de red que los utilizan. Todo esto para constatar, de forma experimental, que estas comunicaciones solo se garantizan en WiFi bajo ciertas condiciones.

De la relación de WiFi y multimedia surge la búsqueda de aportaciones y contribuciones que mejoren su uso combinado. Especialmente soluciones independientes de hardware/software propietario, compatibles y portables.

1.3 Objetivos

Bajo cualquier punto de vista, se considera indispensable introducir iniciativas tendentes a mejorar las posibles debilidades o carencias de las redes WiFi, y más concretamente, en cuanto a la calidad de servicio (*QoS*, del inglés *Quality of Service*) ofrecida por las

mismas. Para ello nos basamos en la literatura existente, recomendaciones o estándares y, especialmente, en la experimentación. Esto último como soporte de evidencias empíricas del comportamiento de las redes *Institute of Electrical and Electronics Engineers* (*IEEE*) 802.11 bajo condiciones de elevada demanda o servicios especialmente sensibles a retrasos o reducido ancho de banda.

El objetivo principal que se pretende alcanzar con esta tesis doctoral consiste en proponer diferentes modelos para mejorar las prestaciones de las redes WiFi, y materializarlos en varias estrategias o actuaciones conducentes a mejorar los resultados en el uso de las mismas. Para ello nos centramos en aquellas situaciones especiales de elevado tráfico, como sucede en tráfico multimedia, y en las que la calidad de los resultados podríamos considerarlos inadecuada o inaceptable. En este tipo de servicios es necesario caracterizar el tráfico que generan para conocer sus atributos y requisitos. Con ello se pueden aplicar mecanismos que mejoren sus prestaciones de forma local, remota o integral. Planteamos para ello una optimización de los parámetros que le pudieran afectar.

Es evidente que toda red de comunicaciones, en especial las inalámbricas y en particular WiFi, tienen unas limitaciones prestaciones, que en muchos casos no se conocen con detalle y, en general, no se habilitan estrategias para mejorarlas. En el caso se superar las limitaciones de capacidad se produce pérdida de información o pérdida de calidad de señal y todo ello conduce, la mayor parte de las veces, a la desconexión de las comunicaciones existentes.

Si bien hemos planteado un objetivo general, este se podría separar en dos objetivos secundarios, relacionados con las siguientes actuaciones:

- Mediante la simulación y experimentación real con diferentes escenarios y dispositivos reales, comprobar dichas limitaciones o comportamientos, que podrían evitarse o reducir sus efectos en el uso de comunicaciones multimedia
- Proponer modelos que nos lleven a soluciones de mejora en diferentes líneas de actuación, desarrollar implementaciones reales que corroboren su aplicabilidad y, tras el análisis de resultados, proponer la aplicación de las mismas.

Estas propuestas se plantean básicamente dirigidas hacia una mejora en la QoS y para su aplicación en los terminales WiFi y en los propios dispositivos de acceso, concretamente en los *Puntos de Acceso* (*AP,* del inglés *Access Point*). De forma

complementaria, se podría requerir la posible intervención del usuario, si fuese necesario la misma, para poder contar con una valoración subjetiva o medida de QoE.

De entre las múltiples situaciones habituales que podrían producirse debidas a una saturación del canal WiFi o con limitadas prestaciones, nos centramos en esta tesis en las siguientes:

1. Interrupciones de vídeo que provocan visualización con cortes o saltos y *pixelado*
2. El terminal WiFi no siempre se asocia al AP más apropiado
3. El terminal WiFi se desasocia del AP al estar en límites de cobertura.

1.4 Estado del Arte

Podríamos indicar que constantemente surgen nuevos servicios o aplicaciones para que sean usadas sobre las redes disponibles, pero generalmente las mismas no se desarrollan pensando en una determinada tecnología de red, sino de forma independiente a la misma. Utilizan el modelo de diseño de la arquitectura de red por niveles independientes conectados mediante interfaces. Pero esto puede producir ciertos efectos negativos, cuando se pretende que dichos servicios puedan ser perfectamente soportados por todas las tecnologías de redes desplegadas actualmente. Es evidente que muchos de los nuevos servicios de comunicación que se desarrollan son independientes de las redes que le dan soporte. Ejemplo de ello es la TV de alta definición, que es previa a la existencia de WiFi, y cuyos primeros estándares no soportaban los requisitos de dicha tecnología de video. Esta primera versión de WiFi, estandarizada como IEEE 802.11b, que teóricamente soporta velocidades de 11 Mbps, esta constatado la imposibilidad real de compartir la red con otros usuarios y realizar una videoconferencia con alta calidad. Si bien la tecnología ha avanzado enormemente con nuevos estándares, como la IEEE 802.11g e IEEE 802.11n, que son las redes más ampliamente desplegadas, sucede algo similar, aunque en menor medida.

Bajo estas condiciones, con la existencia de multitud de redes desplegadas, adoptar como única solución para el soporte de estos nuevos servicios, tan exigentes en ancho de banda, la adquisición y despliegue de nuevos equipos sería desmoralizante. Por ello múltiples autores realizan aportaciones y propuestas en la línea de mejorar la eficiencia

de los dispositivos, optimizando sus recursos y, en algunos casos, variando la forma de funcionamiento de la red, especialmente en los niveles inferiores (físico y de enlace).

Ya, en el comienzo de la realización de esta tesis doctoral, detectamos las limitaciones de las redes IEEE 802.11, como describe Bharghavan en [1] y también lo han constatado otros autores. En [2] Sobrinho et al. realizan medidas sobre las bajas prestaciones de calidad de servicio (QoS) en redes de acceso WiFi.

Asimismo Lang et al., en [3], analizan el comportamiento de redes 802.11b en el modo ad-hoc y plantean consideraciones sobre la ineficiencia de usar el AP para comunicaciones entre terminales móviles, ya que está afectada por múltiples factores como: interferencias radio, limitado número de canales, sobrecarga por tráfico de seguridad... Jangeun et al., en [4], presentan las prestaciones de las primeras versiones de IEEE 802.11. Posteriormente en [5] [6] se plantea el uso de redes hibridas, mezcla de redes ad-hoc con modo infraestructura. Con ello se permite optimizar y reducir el tiempo de uso del canal así como permitir una más rápida liberación del mismo y, con ello, disponer de mayor throughput para el resto de comunicaciones. Maniyeri, en [7], presenta una implementación similar en la misma línea de usar solo redes ad-hoc.

Para mejorar las prestaciones de comunicaciones dadas las limitaciones que presentan las redes WiFi IEEE 802.11b, Prihandoko et al. en [8] y Fang et al. en [9] proponen un control de admisión para garantizar un grado de QoS a nivel *Medium Access Control* (*MAC*). Toh et al., en [10], presentan un uso más eficiente por parte de los AP para compartir la carga entre varios de ellos y reducir los efectos adversos de las interrupciones de servicio. Xiao et al., en [11], analizan el estándar IEEE 802.11e, que surge para mejorar las prestaciones al introducir prioridades en los diferentes tráficos. En [12], Boggia et al. proponen, de forma complementaria a las aportaciones presentadas en [8] [9], un control de admisión en un nuevo MAC coordinado con IEEE 802.11e. Para ello se definen varias clases de tráfico: *best-effort*, voz, video. Vinnakote et al., en [13], proponen un cambio en el MAC para soportar QoS mediante la alteración de tiempos de espera. Qiang en [14], de manera similar a [12], analizan las prestaciones del MAC con IEEE 802.11e planteando mejoras a nivel de MAC.

En [15] [16] [17] se analizan aspectos de posicionamiento de terminales y aplicaciones relacionado con el problema de las desconexiones, generalmente usando los valores de *Received Strength Signal Indicator* (*RSSI*), así como Karimi, en [18], da una visión general de las diferentes soluciones de localización y cómo se ve afectado

por las reasociaciones. Akiyama et al., en [19], y Ching et al. en [20], proponen nuevos métodos de localización en interiores de terminales en redes WiFi. Song et al., en [21], exponen el uso efectivo de *Global Positioning System* (*GPS*), pero solo para determinados casos.

Rodriguez et al., en [22], realizan y describen un análisis empírico del uso de *VoIP* sobre redes IEEE 802.11. Liu et al., en [23], presentan que el proceso de reasociación en WiFi implica un proceso de *roaming* y todas las consideraciones al respecto. Starsky et al., en [24], proponen que un AP debe regular la máxima cantidad de tráfico del terminal móvil que tenga autorizado a enviar al canal WiFi. Los autores de [25] proponen una lista de soluciones heurísticas y algorítmicas para resolver el problema de optimización de variables que afectan al uso del canal y resto de factores implicados. Silva et al., en [26], exponen cómo las redes de sensores hacen *tethering* para acceder a Internet y su modelo puede extrapolarse a redes WiFi.

Si bien la mayor parte de estas ideas o propuestas han sido dirigidas prácticamente a aumentar la velocidad o capacidad de la red, los problemas relacionados con la conectividad (pérdidas), la simultaneidad de uso, solape de canales y los cambios de AP (*handover* o *handoff*) han sido menos considerados.

En cuanto a literatura relativamente más reciente vinculada con los diferentes objetivos de esta tesis doctoral, consideramos que debemos hacerlo de forma separada y vinculada directamente con cada una de las tres líneas principales o actuaciones en que nos hemos centrado, pues no hemos encontrado ninguna referencia en la misma línea de una actuación combinada como la que aquí se presenta.

En cuanto a aspectos relacionados con las comunicaciones multimedia y el limitado ancho de banda de las redes WiFi ante tráficos dependientes del tiempo destacamos:

Zarki et al., en [27], analizan la transmisión de audio y video sobre WLAN 802.11. Miden las condiciones límite para comunicaciones de voz sobre sistemas sin contienda y con ella; concluyen que el alto *overhead,* en períodos de contienda, resulta en una reducida posibilidad de conversaciones de voz. Y, por otro lado, aumentos en el tamaño de los *frames* mejoran la oportunidad de más conversaciones, pero a costa de alterar el *Time To Live* (*TTL*) para mantener una calidad aceptable.

En el ámbito de cambios en el MAC, Krishnakumar et al., en [28], analizan el comportamiento del *Carrier Sense Multiple Access/Collition Avoidance* (*CSMA/CA*) y el hecho de ser independiente de las características del tráfico transportado. Proponen un procedimiento de acceso múltiple distribuido para dar prioridad de acceso a los terminales con tráfico *real-time* mediante el método "*black burst*", y transmiten paquetes con números variables de fuentes de bits. Esta propuesta puede coexistir con otros sistemas CSMA/CA. De manera algo similar, Chang et al., en [29], proponen una variante de *Distributed Coordination Function* (*DCF*) para mejorar tráfico real-time, más sencillo de implementar que el *Point Coordination Function* (*PCF*). Para soportar prioridad, cambian el tiempo de *backoff* a una función de generación aleatoria para terminales con alta prioridad y otra para terminales de baja prioridad, dividiendo el *backoff* en dos períodos. Vaidya et al., en [30], proponen un método de reparto completamente plano del ancho de banda en función del peso de los flujos que hacen uso del mismo. Se basa en el principio de algoritmo de colas justas, sobre la base de DCF. La propuesta se denomina *Distribution Fairness Scheduling* (*DFS*). Analizan otras propuestas basadas en aplicar una coordinación desde el AP como se realiza en redes celulares. Introducen umbrales y factores de escala. Se modela para tráfico *Constant Bit Rate* (*CBR*). Intenta emular el algoritmo *Self-Clocked Fair Queuing* (*SCFQ*). Se materializa, entre otros aspectos, variando el *backoff*. En [31] se analizan cuatro métodos de diferenciación de servicios PCF, *Enhanced Distributed Coordination Function* (*EDCF*), DFS y *blackburst*. Comparan sus prestaciones mediante la aplicación de las diferentes propuestas realizadas por el IEEE, especialmente PCF que junto con DCF fueron las primeras desarrolladas, luego la EDCF incluida en IEEE 802.11e y otras, como el reparto plano con DFS. Miden el throughput y analizan la dependencia del tamaño de tramas. Al analizarlos aplican cambios en ciertos parámetros configurables en los diferentes métodos. Especifican que la mejor solución es EDCF pero para casos puntuales de bajo retraso o tramas pequeñas. Vollero, en [32], analiza el comportamiento del mecanismo *Dropping framing* para el uso en tráfico multimedia, demostrando que el comportamiento es comparable al DFS. Analizan y estudian directamente el proceso de *backoff,* midiendo efectos sobre el throughput, retraso y utilización del canal. Por último muestra el efecto del factor de *dropping*.

En otras líneas diferentes Rezende et al., en [33], argumentan que los algoritmos de control de velocidad (*rate control*) para dispositivos comerciales actúan muy dirigidos por la pérdida de paquetes, en vez de distinguir aquellos debidos a verdaderas pérdidas

respecto a los debidos a colisiones. Evalúan un algoritmo de adaptación automática de rate control. Consiste en medir los niveles de contienda, infiriendo la probabilidad de colisión y escoger la tasa de transmisión que maximice el throughput. Analizan entre otras soluciones el no detectar ACK y medir SNR para bajar la tasa de transmisión. Definen su algoritmo denominado *YARA: Yet another rate adaptation algorithm*. Lo implementan en Madwifi y aseguran mejorar enormemente las prestaciones. Analizan variables de tiempos en el nivel MAC e incorporan pruebas de perdidas forzadas para evaluación. Por último, Nishimaki et al., en [34], presentan un nuevo sistema que visualiza las condiciones de los canales WiFi utilizando un nuevo método de estimación de congestión y detección de tráfico de *streaming* para evitar las interferencias entre ellos. Utilizan la técnica de detección de picos en los tráficos *streaming* mediante un sistema monitor, calculan el uso del medio y determinan la calidad del canal utilizado.

En lo que respecta a la segunda línea de estudio, elección eficiente de AP destacamos:

En la línea de uso de varios AP, Chandra et al., en [35], proponen utilizar la virtualización de la *Wireless Network Interface Card* (*WNIC*) para permitir contar con varios canales de conectividad inalámbrica y, con ello, mejorar la eficiencia, reducir el consumo y mejorar las prestaciones. Con esta propuesta, denominada *Multinet*, se establecen varias conexiones simultáneas transparentes al usuario, y sin alterar los niveles altos de la arquitectura. Requiere en su implementación modificar el driver para poder gestionar los paquetes, encolar y habilitar prioridades para el envío de los mismos. Lo implementan sobre *Windows XP Network Driver Interface Specification* (*NDIS*) y analizan las mejoras en retrasos y reducción de consumo. De manera similar, Shakkottai et al., en [36], proponen un método de distribuir el tráfico entre varios AP (*multihomed*) comparándolo con hacerlo con uno solo de ellos. Comentan también otras medidas de throughput independientemente de la velocidad. Además referencian la propuesta Multinet, en la que se fuerza a los terminales a activar en modo *sleep* a un interfaz, con ello el AP buferiza sus paquetes y posteriormente los reenvía de forma priorizada. Proponen un mecanismo basado en costes o precios para controlar el uso de los AP. Cassell et al., en [37], examinan el caso de uso de múltiples AP simultáneamente. Aplican estrategias y teorías de juegos para elección de un AP. Plantean varios modelos aleatorios para la elección al azar con una orientación hacia el

equilibrio de Nash. Aplican el algoritmo *hedge* para decisión teórica de optimización (asignar trabajo a aquellos AP que considera tendrán menor retraso). Otra variante se presenta en [38], donde Kumar et al. proponen una formulación de máxima usabilidad para el problema de la asociación óptima de los terminales a los AP. Permiten la asociación de un terminal a más de un AP a diferentes tasas de bits. Estudian el problema de asociación óptima para el caso de diferentes terminales con diferentes tasas de transmisión y su influencia sobre el throughput global. Plantean una solución matemática para esta distribución. Analizan el efecto de aplicar el método clásico de "*Branch-and-Bound*" para la optimización y lo usan sobre el paquete de optimización: *LINGO*. Exponen que el balanceo de carga tradicional no parece ser la solución óptima. Proponen la existencia de un sistema central que altere el comportamiento de la asociación, que se basa simplemente en intensidad de señal más fuerte, por otras consideraciones como basarse en la SNR. De forma similar, Giustiniano et al., en [39], presentan una solución (*WiSwitcher*) para permitir a un cliente conectar a múltiples AP, reduciendo el coste de conmutación entre ellos por el reparto de tiempo entre los mismos, e incrementa la estabilidad en el porcentaje de tiempo asignado al planificador. Consiste en un planificador temporal para asignar un porcentaje de tiempo de conexión a cada AP. Presentan otras propuestas y las comparan con la realizada por los autores. Lo materializan mediante la aplicación de virtualización de NIC. Analizan el efecto sobre la reducción de jitter, pérdida de paquetes y throughput.

En una línea parecida a las anteriores, aunque usando servicios especiales de nivel de transporte, Croitoru et al., en [40], proponen que los terminales se asocien a todos los AP que detecten y usen *Multipath Transmission Control Protocol* (*MPTCP*). Esta propuesta va dirigida a mejorar el problema de handoff/movilidad rompiendo el esquema tradicional de un solo AP en cada momento. Esto puede hacerse sobre el mismo o diferentes canales, pero en los casos que bajan las prestaciones sugieren cambios a aplicar en los clientes. Indican que, en esta línea, existen muchas estrategias o líneas de investigación para mejorar el proceso de *handoff* como son: sincronización de AP a través del *Distribution System* (*DS*), reutilizar direcciones IP para evitar *Dynamic Host Configuration Protocol* (*DHCP*), reescaneo adelantado, múltiples tarjetas WiFi... Analizan aportaciones de *Fast Handover* y de conmutación de canal, selección de AP y MPTCP. Prueban su propuesta con interfaces virtuales de Linux más el *patch* MPTCP y *Minstrel*, varios MAC y *Random Early Dropping* (*RED*) sobre la misma interfaz física usando *iperf*. Sugieren utilizar los bits de notificación de congestión en segmentos TCP

denominados *Explicit Congestion Notification* (*ECN*) para dirigir tráfico al mejor interfaz y mejor canal/AP.

En cuanto a la línea de descubrimiento y elección de AP, en [41], Nicholson et al. presentan un sistema automático de descubrimiento y selección de AP denominado *Virgil*. A diferencia de los sistemas existentes, que se basan únicamente en la intensidad de señal recibida, escanea todos los canales y se asocia a cada uno de los AP encontrados. Con ellos realiza una serie de pruebas (calculando el *Round Trip Time* (*RTT*)) utilizando varios servidores de test de ancho de banda estimado, accediendo a múltiples servidores: *Simple Mail Transfer Protocol* (*SMTP*), *HyperText Tranfer Protocol* (*HTTP*), *Distributed Component Object Model* (*DCOM*), Samba). Con toda esta información estiman la calidad de cada conexión. Comentan el hecho constatado de que la elección del AP es un problema crítico, y se cuestionan sobre qué AP proveería la mejor QoS. Exponen que la elección no siempre es eficiente porque es tomada por el nivel físico usando simplemente la política de señal más fuerte. Diferentes pruebas reales sobre *hotspots* abiertos en Chicago, con un Compaq iPAQ 802.11b y Linux *pthread* (*iwlists scan*), concluyen que la intensidad de señal es una insuficiente medida para predecir la calidad del AP. Los datos son guardados para no reescanear siempre y permiten aplicar umbrales de *scan* o actualización. Sugieren que los test sean realizados por los terminales en lugar de que los AP difundan su estado de carga. Para hacer una medida de elección del mejor AP en función de su carga, Vasudevan et al., en [42], proponen que se haga mediante la estimación del ancho de banda de subida y bajada midiendo los retrasos de los *beacons*. Proponen un algoritmo no intrusivo, que no requiera cambios en los AP, y sin existencia de una asociación previa. Esto se haría midiendo el tiempo en el que se planificó el envío del *beacon* y cuando se recibe, este retraso sería función de la carga del AP y el estado de congestión de la red. Consideran que los *beacons* no están priorizados por defecto, y parten de que la mayoría de las pérdidas de tramas o de *beacons* son debidas a las colisiones durante los intentos de transmisión entre terminales simultáneamente, y también, debido a efectos medioambientales como multiruta, *fading*... Las pérdidas de paquetes reducen el ancho de banda entre los terminales comunicantes, ya que causan que los nodos doblen su ventana de contienda y, que además, la duración de *backoff* se vea aumentada. Los terminales monitorizan las tramas y miran el bit *retry*, así detectan si esa trama ha sido retransmitida. Para estimar el ancho de banda ascendente, los terminales transmiten una trama, miden el tiempo y calculan la diferencia con la trama *ack* correspondiente. Para

hacer uso de este último método, debe cambiarse el driver, a pesar de que 802.11 permite el envío de tramas a un AP sin estar asociado (*Probe*).

En la línea de optimización de la distribución de terminales, Karimi et al., en [43], intentan encontrar una optimización en la distribución de los terminales entre los AP, a pesar de considerarlo un sistema *NP-Hard*. Hacen una propuesta de distribución óptima colaborativa en función del throughput disponible, en especial para redes densas, cada vez más disponibles, y en las que los AP utilizan o solapan los canales. Plantean una optimización centralizada para maximizar dicho throughput. La ventaja de la propuesta se consigue al usar el menor número de AP para atender a los clientes y, por tanto: reduce las interferencias entre ellos para mejorar el throughput, la mayoría de los usuarios están conectados al AP con mejores bitrates y la carga se balancea entre los diferentes AP.

Miu et al., en [44], presentan otra propuesta en la que analizan y describen la diversidad multiradio para mejorar las pérdidas y el throughput, mediante la coordinación de las señales recibidas por diferentes interfaces. Se basa en insertar tramas repetidas en una misma trama y así mejorar la capacidad de detectarla correctamente. Argumentan que, como la principal causa de perdidas es debida a *multifading* y eso es muy dependiente de la localización, repitiendo la información se puede recuperar de dichas pérdidas, sin necesidad de solicitar reenvíos de tramas. Realizan pruebas experimentales con varios AP escuchando en una misma radio.

En la misma línea que [40], para mejorar el proceso de handoff, Savage et al., en [45], presentan un sistema o técnica de bajo coste para poder seguir haciendo un seguimiento de los AP, para que la decisión de handoff sea más eficiente. Consiste en seguir escaneando en períodos cortos de tiempo para detectar la degradación de los servicios. Plantean el problema de cambios de AP, que pueden llevar demasiado retraso y con ello imposibiliten comunicaciones especiales como telefonía. Su propuesta pretende reemplazar el overhead de handoff tradicional barriendo todos los canales por un modelo basado en monitorización pasiva y sincronizada con los instantes en los que cada AP emite sus *beacons*.

Bejerano et al., en [46], presentan un estudio del problema de proveer un reparto de servicios plano para los usuarios y balancear la carga entre los AP. Proponen una solución algorítmica para asegurar un reparto del uso de los AP por parte de usuarios, obtenida por los terminales mediante un software en los clientes. Esto se realiza durante la asociación de usuario analizando la carga y el ancho de banda. Describe y compara

los dos métodos: *Strongest Signal First* (*SSF*), el más ampliamente implementado, y el método *Least Loaded First* (*LLF*). Analizan matemáticamente una serie de planteamientos en función de los pesos de los servicios y la suma de los mismos para proponer un reparto de los mismos en función de la carga de los AP. Introducen el concepto de *adjusted load balancing algorithm* y consideran que todos los servicios son limitados en demanda de usuarios y luego, agrupan los usuarios por grupos para encontrar el reparto óptimo de usuarios/servicios. De manera similar, en [47], se plantea el problema real de determinar con certeza el ancho de banda disponible. Realiza un estudio de necesidades de tasa de bits en función de la cantidad de bits a transmitir por cada trama 802.11. Exponen la dificultad de medir el ancho de banda de un enlace en intervalos de tiempo discretos, para luego promediarlos en un determinado momento. Posteriormente los aplican en el momento presente y, así, estiman el ancho de banda con condiciones totalmente desconocidas. Introduce un mecanismo de control de velocidad (rate control) y de control de tiempo de uso de canal.

En la línea de interferencias entre AP y sus efectos, Baid et al., en [48], estudian dicho problema y proponen un esquema de optimización cooperativa para mitigarlas. Modelan la interferencia entre AP y formulan una programación lineal para resolver la asociación proporcional plana de clientes a los AP. Introducen consideraciones diferentes a otros autores para resolver este problema *NP-hard*. Comparan los tres casos: menor distancia, optimización interna y optimización cooperativa. Consideran que ignorar la presencia de otras redes y sus efectos determina peores resultados que cuando no se tienen en cuenta.

Por último, resaltamos que el campo de la localización o posicionamiento en redes inalámbricas, especialmente en redes de sensores y vehiculares, es uno de los *topics* actualmente más destacados, y por ello existe abundante literatura vinculada; la que hemos analizado es la siguiente:

El artículo referente en temas de localización es presentado por Padmanabhan et al. en [49]. En él que se propone un sistema de localización y seguimiento de usuarios basado en RF denominado *RADAR*. Consiste en registrar y procesar información de la intensidad de la señal obtenida de múltiples estaciones base posicionadas para proveer una cobertura solapada. Capturan el RSSI o *Signal to Noise Ratio* (*SNR*) y aplican el modelo aproximación lineal.

Huang et al., en [50], indican que las señales inalámbricas están influenciadas por el entorno en el proceso de propagación, y que el modelo apropiado para interiores está basado en el valor del RSSI. Se propone su uso para redes de sensores WSN, exponiendo que las principales estrategias para medir la distancia entre los nodos son: *Time of Arrival* (*TOA*), *Time Difference of Arrival* (*TDOA*), *Angle of Arrival* (*AOA*) y RSSI. En todos los casos, para calcular las coordenadas de un nodo desconocido pueden aplicarse: algoritmos de trilaterización, el algoritmo de mínimos cuadrados o la estimación de máxima vecindad. Proponen un algoritmo robusto y con bastante exactitud basado en el uso del RSSI, en el que los parámetros que producen el error causado por parámetros fijos del modelo de propagación son eliminados. Introducen un rango de error sobre la seguridad del posicionamiento y un sistema de mapeo, uno a uno, entre el valor de RSSI y la distancia en función del exponente de pérdidas en el enlace. Discuten la relación entre los parámetros del modelo de propagación y rango de exactitud de RSSI. Obtienen el RSSI, hacen su media y, con triangulación, hacen una estimación de posición y ámbito de localización. En la misma línea, Mistry et al., en [51], dan una visión general de soluciones y técnicas para aplicar la localización o estimar la posición, aplicado en redes de sensores. Categorizan las mismas entre las basadas en rango: estimación de distancia (*RSSI*, *AoA*, *ToA* y *TDoA*) y estimación de posición (lateralización, triangulación y multilateralización); y las libres de rangos (asociación de patrones, *fingerprint*).

En la línea más próxima a nuestra propuesta, Chowdhury et al., en [52], destacan que la medida de la distancia a partir del RSSI es un desafío para la navegación y posicionamiento en interiores. Proponen un novedoso sistema multinivel combinando el modelo ”*Propagation* over *Earth Plane*”, para valores de RSSI menores que -52 dBm; el modelo de espacio libre de *Friis (Free Space Propagation)*, para valores de RSSI entre -53 y -44 dBm; y el modelo aproximación lineal, para valores de RSSI mayores de -44 dBm, con objeto de medir la distancia de dispositivos con conectividad bluetooth de bajo consumo. Aplican un suavizado de promediado de RSSI consiguiendo del orden del 13.4 % de reducción de error de medida de distancia. Similarmente Mukhopadhyay et al., en [53], analizan las prestaciones del uso de RSSI y *Link Quality Indicator* (*LQI*) para su aplicación en localización. Ante la evidente fluctuación del RSSI, se produce un error de localización. Proponen dos técnicas novedosas para localización usando RSSI+LQI en WSN. Aplican una solución *Recursive Bayesian* (RB)-RSSI-LQI (que requiere estimador de posición y observación) y otras de *Maximum at Posteriori*

(MAP)-RSSI-LQI, ambas son comparadas ambos con las tradicionales basadas en media de RSSI. Utilizan una matriz de posición para determinar la existencia de objetos de cada posición. Concluyen que el método MAP-RSSI-LQI es el que ofrece mejores prestaciones, en términos de error de localización y complejidad computacional.

Rencheng et al., en [54], proponen un nuevo algoritmo de localización por trilateralización basado en los arcos con los tres nodos más cercanos para WSN pudiendo suprimir los valores atípicos encontrados en otras propuestas.

Fundamentándose en la técnica AoA, Souvik et al., en [55], proponen un sistema que mejora la exactitud de la localización, analizando el efecto de señales directas frente a las reflejadas y la dependencia del ángulo de llegada de la señal. Igualmente estudian el efecto de obstáculos entre AP y terminal para determinar la posición de la forma más exacta. Garantizan una localización con un solo AP, y que cuando están disponibles varios AP, el error de localización es de unos 2.7 m. Intentan estimar la distancia y el ángulo en el caso de dirección directa, y de otras señales reflejadas que estarán directamente relacionadas con el nivel de potencia con que se reciba cada una de las señales. Utilizan perfiles de potencia recibida para relacionarlos con distancia y ángulo. También se basan en información de estado del canal (*CSI*, del inglés *Channel State Information*) extraída del nivel físico.

De manera especial se destaca [56], por la relación directa con nuestra propuesta, en la que Gough et al., describen que el uso de localización basada en "*fingerprint*" supone que los dispositivos usados durante el proceso de aprendizaje se van a comportar idénticamente a los usados para desarrollar la localización. Realizan pruebas experimentales que demuestran su elevada variabilidad. Comprueban que ciertos dispositivos fueron completamente inadecuados para posicionamiento, pues los nuevos valores que éstos informan están muy incorrelados con la distancia desde el transmisor. Realizan las pruebas con múltiples dispositivos *Universal Serial Bus* (*USB*) (concretamente 17) y smartphone en 2.4 GHz y 5 GHz. Determinan que en 5 GHz son más fiables las medidas. Sugieren una elevada dependencia del diagrama de antenas y la orientación de las mismas, y además requieren técnicas de filtrado para mejorar la exactitud en la presencia de "*RSSI dropouts*".

1.5 Contribuciones y aportaciones de esta tesis

Esta tesis doctoral ha dado lugar a varias contribuciones que consideramos relevantes:

1º) Una plataforma multifuncional integrada que gestiona de forma más eficiente el uso de los canales compartidos por diferentes terminales. Esta gestión se hace de forma centralizada en los AP, pero se aplica distribuida en los diferentes terminales. Con el conocimiento del estado de cada canal por parte de cada AP y el intercambio de información entre ellos, se puedan controlar y reducir los efectos negativos de unas comunicaciones sobre otras y, especialmente, evitar la saturación de los canales.

2º) De manera particular, una de las dos principales contribuciones es limitar el tráfico en general, o el vinculado a determinadas conexiones de cada terminal, cuando la importancia de esos tráficos es menor que el generado por otros terminales. Para ello partimos de la existencia de tráficos o flujos prioritarios (en general los dependientes del tiempo) y los no prioritarios. Actualmente las propuestas de control de tráfico se orientan para una implementación en los AP y nosotros la llevamos al terminal originario de cada tráfico. A esta contribución la denominamos control de admisión y regulación de tráfico en origen.

3º) Facilitar que la asociación de terminales a los AP y la reasociación no se realice de una forma tan básica como actualmente, basada generalmente en el nivel de señal recibida, sino que sea más dependiente del estado de todos los dispositivos participantes. Concretamente consiste en que los AP conocen a sus vecinos y los terminales a los que dan servicio, mediante el intercambio de información entre ellos. Tras la optimización de las variables o parámetros relacionados y la búsqueda de una mejor distribución, se traspasen terminales de unos AP a otros en donde obtengan mejores prestaciones los servicios demandados por cada uno de los terminales. Todo esto se realiza sin interacción de los usuarios de los terminales.

4º) Aplicar la localización física de los terminales en el ámbito de la cobertura de los AP para posibilitar la reubicación de los mismos allí donde mejore la conectividad o sus condiciones. La idea consiste en guiar a cada terminal a una ubicación más eficiente no solo de señal recibida sino de disponibilidad de otros AP, para poder permitir, junto con la anterior contribución, su traspaso a otro AP que ofrezca mejores resultados en cuanto a estabilidad y calidad de las comunicaciones.

En cuanto a la difusión de las propuestas planteadas y los resultados obtenidos con esta tesis en forma de aportaciones a la literatura, a continuación se relacionan

considerando ponencias en congresos nacionales e internacionales, artículos en revistas científicas y capítulos de libros científicos.

Congresos Nacionales

- D. Marrero Marrero, E. Macías López, A. Suárez Sarmiento. "Plataforma multifuncional para gestión del canal en redes IEEE 802.11". VIII Jornadas de Ingeniería Telemática (JITEL 09). 15-17 de Septiembre de 2009 en la Escuela Técnica Superior de Ingeniería de Telecomunicación (Universidad Politécnica de Cartagena - España). Ponencia. Libro de Actas del Congreso ISBN: 84-7653-783-2 ISBN: 978-84-96997-27-1. Páginas: 16-23.
- D. Marrero, E. Macías, A. Suárez. "Localización en interiores para mejorar rendimiento del acceso a Internet en redes WiFi con infraestructura". IX Jornadas de Ingeniería Telemática (JITEL2010). 29 Septiembre a 1 Octubre de 2010 en la ETSIT de la Universidad de Valladolid. Ponencia. Libro de Actas del Congreso ISBN: 978-84-693-5398-1. Páginas 191-198.
- D. Marrero Marrero, E. Macías López, A. Suárez-Sarmiento. "Mejorando el rendimiento de las redes de acceso WiFi". X Jornadas de Ingeniería Telemática (JITEL2011). 28-30 Septiembre de 2011 en la Universidad de Cantabria. Ponencia. Libro de Actas del Congreso ISBN: 978-84-694-5948-5. Páginas 385-388.
- Álvaro Suárez, Elsa Macías López, Vicente Mena, Domingo Marrero, José A. Santana. "Estimación Proactiva de QoS de Canales Inalámbricos para Mejorar la QoE en Servicios Multimedia". XII Jornadas de Ingeniería Telemática (JITEL2015). 14-16 Octubre de 2015 en la Universitat de les Illes Balears. Palma de Mallorca (Islas Baleares). Libro de Actas del Congreso ISBN: 978-84-606-8609-5. Páginas: 347-354.
- José A. Santana, Elsa Macías López, Vicente Mena, Domingo Marrero, Álvaro Suárez. "Estimación Eficiente del RSSI en Redes WiFi para Servicios Inalámbricos Futuros". XII Jornadas de Ingeniería Telemática (JITEL2015). 14-16 Octubre de 2015 en la Universitat de les Illes Balears. Palma de Mallorca (Islas Baleares). Libro de Actas del Congreso ISBN: 978-84-606-8609-5. Páginas: 247-254.

Congresos Internacionales

- D. Marrero Marrero, Elsa Mª Macías López, Álvaro Suárez Sarmiento. "Dynamic interconnection of Ad-Hoc nodes based on the type of service to be accessed". ICWN'05 (International Conference on Wireless Networks). Las Vegas, Nevada, USA. 27-30 de Junio de 2005. ISBN: 1-932415-55-6.
- D. Marrero Marrero, Elsa Mª Macías López, Álvaro Suárez Sarmiento. "Dynamic Traffic Regulation for WiFi Networks". World Congress on Engineering 2007 (WCE2007). ICWN'07 (International Conference on Wireless Networks 07). London, UK. 2-4 de Julio de 2007. ISBN: 978-988-98671-2-6.

Capítulos de Libros y Revistas Internacionales

- Domingo Marrero, Elsa Macías y Álvaro Suárez. "An Admission Control and Traffic Regulation Mechanism for Infrastructure WIFI networks". IAENG International Journal of Computer Science, 35:1, pages 154-160, ISSN: 1819-656X. Marzo 2008. Artículo en publicación científica.
- Domingo Marrero, Elsa Macías y Álvaro Suárez."Improving of QoS in Wifi Access Networks". Wireless Multi-Access Environments and Quality of Service Provisioning – Solutions and Application" editado por Gabriel-Miro Muntean & Ramona Trestian. IGI Global. Cap. 14. Pág. 337-360 ISBN: 978-1-4666-0017-1. Año: 2012. Capítulo de Libro.
- Álvaro Suárez, José Aurelio Santana, Elsa Macías, Vicente Mena, José Miguel Canino y Domingo Marrero. "RSSI Prediction in WiFi Considering Realistic Heterogeneous Restrictions", Network Protocols and Algorithms. Editorial: ©Macrothink Institute, Ref. ISSN 1943-3581. Diciembre 2014. Lugar de publicación: Las Vegas, Nevada. United States. Artículo en Revista.
- José Aurelio Santana, Elsa Macías, Vicente Mena, Domingo Marrero, Álvaro Suárez. "Estimación Adaptativa del RSSI de WiFi y su Impacto en Servicios Inalámbricos Avanzados". Special Issue Recent Advances on Telematics Engineering. ACM/Springer Mobile Networks and Applications (MONET) (JCR Q2). NOV15. Pendiente de publicación.

1.6 Organización de la tesis

En este apartado se presenta el desglose, a modo de resumen, de los diferentes capítulos, apartados y subapartados de lo que se compone esta memoria de tesis doctoral. Concretamente está formada por 6 capítulos y un anexo.

El presente capítulo está formado por 6 apartados. En el apartado 1.1 se realiza una presentación, a modo de introducción general, acerca de las redes de acceso, sus tipos y características, así como la situación actual de su penetración en nuestra sociedad. A continuación, en el apartado 1.2 se describen los motivos por los que se ha desarrollado la tesis en el campo de las redes inalámbricas. Posteriormente en el apartado 1.3 se exponen los objetivos que nos propusimos para realizar esta tesis doctoral. A continuación, en el apartado 1.4 se detalla el estado del arte, o situación actual de investigación, describiendo la literatura analizada relacionada con los temas desarrollados. De manera especial, se analizan otras propuestas, iniciativas o experiencias de otros investigadores o autores. En el apartado 1.5, se describen las contribuciones que se realizan tras la realización de esta tesis y las aportaciones o difusión de resultados. Finalmente se encuentra el presente apartado con la organización por temas.

El capítulo 2 lo hemos denominado Comunicaciones multimedia en WiFi debido a que en él se presenta la base teórica de aquellos aspectos relacionados con el desarrollo de esta tesis doctoral y los problemas o carencias que se detectan. El mismo se divide en cuatro apartados.

En el apartado 2.1 se realiza una descripción general de lo que representa la Multimedia como conjunto de contenidos digitales y se presentan los aspectos más relacionados con el resto de apartados, concretamente en la parte de audio y video por sus especiales requisitos.

En el apartado 2.2 se presentan ideas generales sobre las redes inalámbricas, dando una visión general de sus características y estándares, y particularizando el documento en las redes inalámbricas de área local, concretamente las IEEE 802.11 comúnmente conocidas como WiFi.

A continuación, en el apartado 2.3, describirnos la importancia de la QoS en el conjunto de los servicios actuales que cada vez requieren unos mínimos aceptables, sin

los cuáles no es posible garantizar una óptima utilización. Se presentan soluciones y tecnologías desarrolladas para mejorar la percepción que se tiene de dichos aspectos tanto en QoS o QoE.

Por último en este capítulo 2, se presentan en el apartado 2.4, las consideraciones especiales que presentan las comunicaciones multimedia en general, y en particular, cuando hacen uso de las redes WiFi.

En el capítulo 3 y apartado 3.1 se presenta, a pesar de estar bastante documentado y corroborado, la existencia de diferentes problemas y carencias de las redes WiFi. Describimos y analizamos diferentes evidencias empíricas mediante experimentación real con diferentes casos y dispositivos que sustentan las mismas. Posteriormente justificamos la necesidad de desarrollar propuestas o aportaciones como las que se realizan en esta tesis. Se realiza un análisis y una caracterización de ciertos aspectos de las comunicaciones multimedia sobre las redes WiFi. Por último, en el apartado 3.2, se expone el método de trabajo que nos propusimos basado en definir un conjunto de parámetros vinculados con diferentes aspectos, niveles o recursos de estas redes. Con el tratamiento de los mismos buscamos una optimización del uso y reparto de recursos dirigidos a alcanzar una mejor eficiencia y prestaciones.

En el capítulo 4 se presentan las propuestas para abordar los problemas anteriores, se expone la metodología seguida, consideraciones de contexto y modelo, si fuese el caso, así como una descripción detallada de cómo implementar cada propuesta. Además presentamos las diferentes aportaciones frente a otras planteadas por otros investigadores en las mismas o similares líneas de trabajo. Como se comenta en los objetivos, todas las propuestas están dirigidas hacia mejorar la calidad de servicio de las redes WiFi para soportar servicios dependientes del tiempo y aportar contribuciones para mejorar la distribución y uso del canal radio correspondiente. Para ello analizamos qué parámetros están vinculados con cada uno de los objetivos o relacionados con ellos. Con la gestión de los mismos de forma combinada y complementaria se mejoren los resultados para una mejor distribución de uso del canal, selección de AP y localización de terminales.

En el capítulo 5 se presentan las diferentes pruebas experimentales tras la implementación real de las propuestas descritas en el capítulo anterior. Se analizan los resultados desde un punto de visto comparativo y destacando las mejoras que se introducen en los resultados buscados y/o alcanzados.

A continuación, en el capítulo 6 se describen las conclusiones finales obtenidas tras el desarrollo de esta tesis y de manera especial se presentan líneas abiertas relacionadas con los diferentes aspectos tratados durante el proceso de realización de la misma.

Finalmente indicamos la relación de referencias bibliográficas analizadas y vinculadas directa o indirectamente con los diferentes temas o aspectos estudiados y presentados.

Se incluye un anexo donde se relaciona la información complementaria que puede ser consultada en la web habilitada para ello.

Capítulo 2. Comunicaciones multimedia en WiFi

En este capítulo se presentan aspectos generales sobre multimedia y su importancia en las comunicaciones actuales, así como sus requisitos. Posteriormente dedicamos un apartado especial sobre aspectos generales de redes inalámbricas pero centrándonos en redes WiFi. Damos un repaso general sobre la QoS, dada su importancia en las redes de comunicaciones, como medida de valoración de las mismas y por último analizamos los desafíos sobre comunicaciones multimedia sobre WiFi.

2.1 Multimedia

La información audiovisual disponible para el ocio, formación y desarrollo intelectual y social del ser humano ha aumentado de forma sustancial durante los últimos años tanto en calidad como en cantidad. Asimismo, la comunicación humana, haciendo uso de medios electrónicos, ha sufrido un gran número de cambios gracias al desarrollo de las tecnologías de comunicación, la digitalización de señales y el procesado de la información. Este desarrollo incluye nuevos formatos de información digital que han venido a agruparse bajo el término Multimedia [57].

Actualmente, la multimedia se utiliza en múltiples ámbitos como son: la formación y educación, entretenimiento (juegos, música y video), publicidad y marketing, *streaming* de radio y televisión... Este hecho se evidencia por la gran cantidad de recursos disponibles.

De entre los diferentes contenidos multimedia, los relacionados con el audio, especialmente la voz, y el video, son los que abordamos porque su comunicación eficiente en redes de difusión multimedia, suponen un desafío actual. A continuación revisamos algunos parámetros sobre la codificación de la información de audio y video.

Hoy en día existe un gran número de técnicas de codificación, compresión y descodificación, descompresión (*codec*) de audio y voz. Estas técnicas se estandarizan, por ejemplo por la *International Telecommunication Union* (*ITU*) [58] mediante normas G7** [59] (**indica diferentes versiones), que han promovido múltiples recomendaciones estándar para codificación de voz. De igual manera, múltiples tecnologías propietarias están disponibles para el tratamiento de audio y voz pero muchas de ellas incompatibles entre sí. También otros organismos de estandarización han promovido otros estándares.

Algunos parámetros básicos que describen un codec de voz/audio son:

- *Tasa de bits* (*bitrate*): número de muestras tomadas por segundo en cada canal.
- *Frecuencia de muestreo*: frecuencia utilizada para muestrear la señal original.

- *El número de canales*: 1 para mono, 2 para estéreo, 4 para el sonido cuadrafónico...
- *Número de bits por muestra*: información para cuantificación de cada muestra, habitualmente 8 ó 16 b.

De entre las normas ITU más importantes, destacamos la G729 [60], ya que con su elevada tasa de compresión y, por tanto, menor tamaño, es la que mejor calidad relativa de audio presenta.

La característica principal de los codec de voz es el *bitrate* [bps]. De este valor depende en gran medida la calidad de la voz digitalizada. Este parámetro resulta aun más determinante si la voz se transmite por una red de comunicación en tiempo real, ya que si no se garantiza dicho bitrate, la señal no podría reproducirse con la adecuada calidad. En estos casos pueden producirse cortes y retrasos que impiden la correcta recepción del mensaje de audio.

En el caso de audio digital, por ejemplo música digitalizada, las exigencias son superiores en cuanto a la banda de frecuencias se refiere (generalmente de 20 Hz a 20 kHz), muy superior a la banda vocal (300 Hz - 3400 Hz).

De todos los estándares de codificación de audio, el más ampliamente utilizado es la denominada *Moving Picture Expert Group (MPEG-1) Audio Layer III (MP3)*, que prácticamente ha sustituido a sus antecesores: MPEG-1 Audio Layer II (MP2) y MPEG-2 Audio Layer II (MP2) [61]. MP3 se convirtió en el estándar utilizado para emisión de audio y compresión de audio con pérdidas de mediana fidelidad gracias a la posibilidad de ajustar la calidad de la compresión de forma proporcional al tamaño (bitrate).

Existen muchos codec de video (estándares o propietarios). Sus principales características son:

- *Tasa de muestreo* para la codificación de la imagen.
- *Número de fotogramas* (*frames*) por segundo.
- *Resolución de pantalla* (número de pixeles: ancho por alto).
- Tamaño de *frame* de reproducción.
- *Número de colores* (paleta).
- *Número de bits de la paleta* de colores.

En el caso de ir acompañado de audio, se le suelen aplicar alguno de los diferentes codecs de audio indicados anteriormente. En este último caso se requiere de forma especial incorporar mecanismos de sincronización entre ambos medios. También podría ir acompañado de texto o subtítulos en diferentes idiomas.

La *International Organization for Standardization* (*ISO*) / *International Electrotechnical Commission* (*IEC*) [62] desarrolla, mediante el grupo de trabajo *Joint Technical Committees/Subcommittee* (*JTC 1/SC 29*) [61] un cierto número de estándares relacionados. De entre ellos destacamos: MPEG1, MPEG2, MPEG4 y MPEG4-*Advanced Video Coding* (*MPEG4-AVC*). Especial consideración se debe tener con la serie de estándares de codificación de video de la ITU-T representadas por H.26X [63]. Concretamente estos estándares ITU-T más representativos son H.261 [64], H.263 [65] y H.264, también conocida como MPEG-4 Part 10 (MPEG-4 AVC) [66]. Actualmente, esta última recomendación es uno de los formatos más usados para grabar, comprimir y distribuir contenidos de video/audio en modo local o por Internet y utilizado por múltiples plataformas de distribución de televisión. Fue desarrollado para su uso en sistemas de alta definición *High Definition TV* (*HDTV*), Blu-ray y *Digital Versatile Disc* (*DVD*). El más reciente H.265 o MPEG-H Parte2, también denominado *High Efficiency Video Coding* (*HEVC*) [67] es compatible con la televisión en ultra alta definición y se encuentra en desarrollo.

Este gran número de técnicas están orientadas a conseguir video de alta calidad. Es sabido que para conseguir una elevada calidad de señal se necesitan elevadas tasas de muestreo, y consecuentemente, la cantidad de información (tamaño de archivo o bitrate) es elevada. Por ello se aplican potentes codec (que trabajan a nivel de bits) para reducir su tamaño y sin pérdida de calidad. Una característica importante a destacar sobre los codecs es que sean escalables pudiéndose con ello adaptar a las condiciones de uso y según los requisitos o recursos disponibles del usuario. En [68] se puede encontrar diferentes recomendaciones.

Un aspecto bastante importante es la falta de compatibilidad entre los diferentes *codecs*. La gran cantidad existente y su constante evolución es un gran hándicap a la hora de facilitar la integración de soluciones de múltiples fabricantes. Es habitual encontrarnos dispositivos en los que se indica claramente en sus especificaciones que codecs son soportados para posibilitar su interconexión con otros dispositivos.

Por otra parte, las actuales tecnologías de redes de comunicación permiten el desarrollo de múltiples aplicaciones para la transmisión de mensajes multimedia,

especialmente los basados en información de audio y video. De manera muy especial, las tradicionales redes de telefonía están siendo sustituidas por redes de datos basadas en *Internet Protocol* (*IP*) [69] para comunicaciones de voz, audio y video. En [70] y [71] se describen de manera pormenorizada las más importantes tecnologías de codec de audio y video para su transmisión a través de redes de comunicación.

Por último consideramos especialmente importante destacar la cada vez más creciente demanda de contenidos de video y audio de forma continua, donde la interacción del usuario es fundamental y sobre la que se apoyan nuevos servicios como Videoconferencia, *Video bajo demanda* (*VoD*), *IPT*v [72]... Estos servicios, por sus especiales características requieren de tecnologías de red, protocolos de comunicaciones y mecanismos de control muy específicos para gestionar su comunicación eficiente. De forma particular la comunicación multimedia en redes de comunicación inalámbrica son tan o más demandadas que en sus homólogas basadas en cable y fibra óptica en regiones geográficas reducidas. En [73] se presenta una visión general de la comunicación multimedia en redes inalámbricas relacionando las aplicaciones multimedia y su íntima vinculación con la calidad de servicio (*QoS*, del inglés *Quality of Service*).

2.2 Las redes de comunicación inalámbricas

Las redes de acceso inalámbricas se pueden clasificar en:

- Red celular de área extensa o metropolitana.
- Red de área local inalámbrica (*WLAN*, del inglés *Wireless Local Area Network*).
- Red vía satélite o modem-RF.

En la actualidad, en cuanto a redes celulares [74] las que mayoritariamente están siendo utilizadas son:

- 2G: *Global System for Mobile Communication* (*GSM*), *General Packet Radio Service* (*GPRS*) y *Enhanced Data Rates for GSM Evolution* (*EDGE*) o Enhanced GPRS (*EGPRS*) [75],
- 3G: *Universal Mobile Telecommunications System* (*UMTS*) [76],
- 3.5G: *High Speed Packet Access* (*HSPA*), *High Speed Downlink Packet Access* (*HSDPA*), *High Speed Uplink Packet Access* (*HSUPA*), y

- 4G: *Long Term Evolution* (*LTE*) [77].

Entre las tecnologías de red metropolitana reseñamos a *Worldwide Interoperability for Microwave Access* (*WiMAX*) [78] [79] [80] y, ya en desuso, *Local Multipoint Distribution Service* (*LMDS*) [81].

Wireless Fidelity (*WiFi*) es la tecnología de WLAN que mayor cantidad de tráfico y número de usuarios soporta. Prácticamente todos los teléfonos móviles de última generación, ordenadores portátiles, tablets, videojuegos, receptores de televisión, servidores multimedia, *hard disks* portátiles… lo incorporan de fábrica. Por eso nos centramos en esta tecnología. Los diferentes estándares WiFi [82] [83] constituyen en el hogar, empresas de todo tipo y hotspots el mayor número de redes inalámbricas desplegadas. Esto se debe, entre otras, a contar con dos características principales: no requerir licencia y su bajo coste.

Según los datos disponibles [84] [85], el número de usuarios que accede a Internet de forma inalámbrica crece exponencialmente y este acceso se realiza mayoritariamente desde redes WiFi y redes celulares 3G-UMTS, y en menor medida redes basadas en tecnología Wimax.

Indicar que si bien 4G se encuentra todavía en proceso de despliegue, ya aparece la propuesta 5G [13] como evolución inmediata. Estas nuevas tecnologías mejoran las prestaciones en cuanto a la velocidad o capacidad en el ámbito de las redes celulares. No parece que pretenda sustituir o reemplazar en el ámbito de redes locales a WiFi y posiblemente puedan coexistir ambas en un futuro próximo.

Además, con la aparición de nuevos dispositivos y nuevos servicios se añaden nuevos requisitos o prestaciones de dichas redes. Ejemplo de ello son los servidores multimedia inalámbricos o similares, desarrollados especialmente para añadir recursos de ocio en el hogar. Dispositivos como ChromeCast [86], reproductores de flujos multimedia, lectores de medios inalámbricos, proyectores inalámbricos, cada vez están más presentes.

Estos nuevos servicios introducen diferentes posibilidades de comunicación pero también, dadas las características o requisitos de los tipos de tráficos que se generan, demandan elevadas velocidades (anchos de banda (bps)) y bajos retrasos en la llegada de paquetes de datos al receptor. Estos requisitos están reñidos con la limitación del espectro radioeléctrico (capacidad limitada) y la falta de regulación en cuanto a libertad de instalación y uso de canales. En general la saturación por tan rápido despliegue no

favorece a estos servicios. No parece que se pueda garantizar una calidad de las comunicaciones cuando un cierto número de usuarios comparten el mismo recurso radio.

Por otro lado la existencia de otras tecnologías de redes, como redes de área personal inalámbrica (*WPAN*, del inglés *Wireless Personal Area Network*), por ejemplo Bluetooth [87], redes de sensores inalámbricos (*WSN*, del inglés *Wireless Sensor Network*), por ejemplo 802.15.4 [88] o Zigbee [89], multitud de sistemas de telecontrol, mandos a distancia RF... que hacen uso de alguna de las bandas de frecuencia utilizadas por WiFi, pueden dar lugar a ciertas limitaciones en las posibilidades y prestaciones por las interferencias que se pueden producir entre ellas. Esto ha sido analizado en la literatura existente especializada [90] [91] [92].

El *Institute of Electrical and Electronics Engineers* (*IEEE*) especifica las características técnicas de los estándares IEEE 802.11 [93] [94] para WLAN. Los estándares más representativos de las diferentes evoluciones de WiFi son:

- IEEE 802.11b, ancho de banda teórico de 11 Mbps operando en la banda de 2.4 GHz (canalización de 22 MHz). Es poco utilizado en la actualidad.
- IEEE 802.11a, ancho de banda teórico de 54 Mbps operando en la banda de 5 GHz (canalización de 20 MHz). Es muy utilizado en la actualidad en países como Estados Unidos de Norteamérica.
- IEEE 802.11g, ancho de banda teórico de 54 Mbps operando en la banda de 2.4 GHz (canalización de 20 MHz). Es el más utilizado actualmente.
- IEEE 802.11n, ancho de banda teórico de más de 300 Mbps, con posibilidad de aumentar ya que permite múltiples flujos mediante *Multiple In Multiple Out* (*MIMO*) en las bandas 2.4 y 5 GHz (canalización de 20 y 40 MHz). Progresivamente ha ido sustituyendo a las versiones anteriores.
- IEEE 802.11ac, anchos de banda teóricos superiores a 800 Mbps permitiendo múltiples flujos en la banda de 5 GHz (canalización de 20, 40, 80 y 160 MHz). Todavía su despliegue no es masivo.

- IEEE 802.11ad, en el más recientemente desarrollado y opera en la banda de 60 GHz soportando muy altas tasas de bits, del orden de 7 Gbps (canalización de 2.16 GHz). Todavía no se está usando en la práctica de forma masiva.

En la Figura 2 se muestra una gráfica comparativa con las capacidades de las diferentes tecnologías.

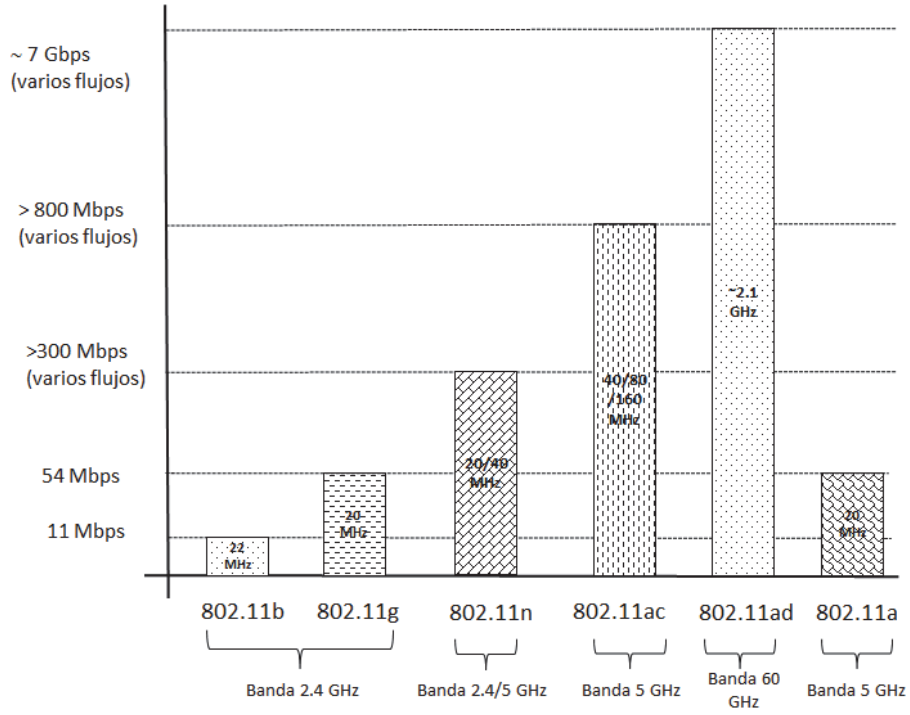


Figura 2. Características diferentes versiones del IEEE 802.11

A grandes rasgos podemos indicar que el IEEE 802.11, representa la evolución natural del IEEE 802.3 a escenarios en los que no es posible usar cables o fibra óptica o facilita la movilidad del usuario. Esta tecnología mantiene el principio de funcionamiento de su antecesora cableada, no orientada a conexión (difusión) y operando en modo *best-effort*. Para ello, la base principal de esta tecnología podemos considerar que es la técnica de acceso al medio denominada CSMA/CA. Esta garantiza el acceso al canal de forma equitativa (no se reserva recurso: frecuencia, slot de tiempo u otros). Cada terminal tiene la misma oportunidad para acceder al canal y la utilización del canal por un terminal puede ser definida como la relación entre el tiempo de transmisión de cada terminal y el tiempo total de transmisión de todos los otros terminales. De esta forma, los terminales transmitiendo a una alta tasa de transmisión obtienen el mismo throughput que los otros terminales transmitiendo a baja tasa de transmisión, que es conocido como una anomalía de prestaciones descrita en [18].

El CSMA/CA consiste en que después de un tiempo de inactividad denominado *DCF InterFrame Space* (*DIFS*), la terminal entra en la fase *backoff* en la que selecciona un contador aleatorio de *backoff* entre [0, CW]. Donde CW es la *Contention Window* o ventana de contienda. El contador de backoff se decrementa en uno por cada slot inactivo si el canal está ocupado. El terminal transmite la trama cuando el contador de backoff llega a cero. Si no ha recibido una trama de confirmación (*ACK*) debido a colisión o transmisión de errores, el tamaño de la ventana de contienda se va doblando iterativamente hasta alcanzar su máximo valor y el transmisor vuelve a planificar la transmisión de acuerdo a la regla del backoff. Después de la transmisión satisfactoria, se restaura CW a su valor inicial. Si se recibe una trama satisfactoriamente, el receptor transmite un ACK justo después de *Short InterFrame Space* (*SIFS*). En la Figura 3 se muestra gráficamente la evolución temporal de CSMA/CA. Además, debe respetarse unos tiempos mínimos entre tramas de datos y confirmaciones para garantizar los envíos sin interferencias.

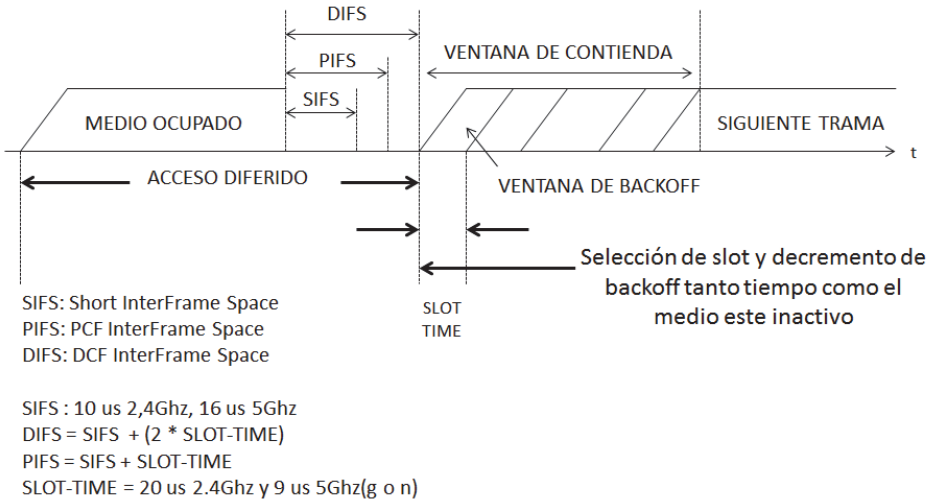


Figura 3. Método CSMA/CA y tiempos entre tramas

El proceso que garantiza que varios terminales hagan uso del canal de forma compartida se muestra en la Figura 4.

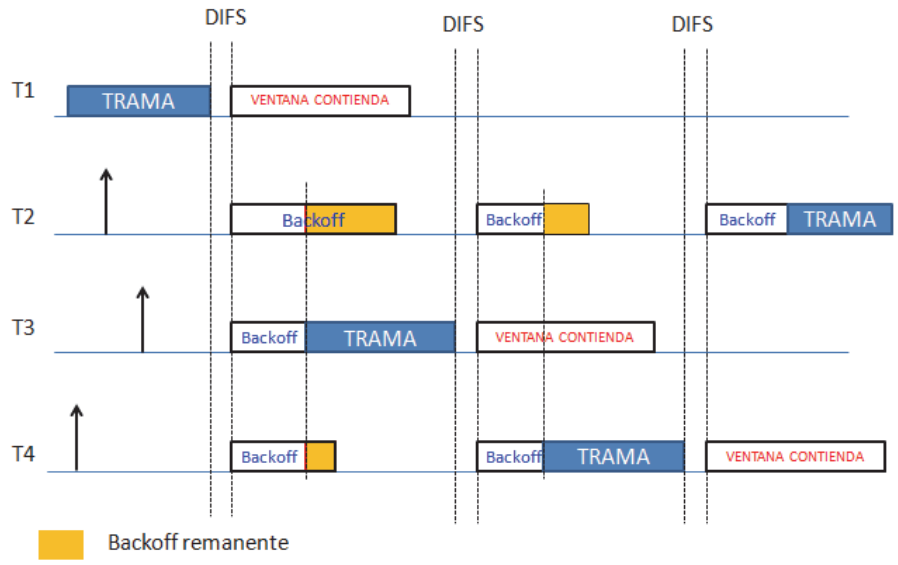


Figura 4. Mecanismo de acceso compartido al canal inalámbrico

WiFi opera básicamente en tres modos diferentes:

- *Modo ad-hoc* (*Independent Basic Service Set* (*IBSS*)) en la que los terminales de clientes se conectan e intercambian información directamente (esquema mostrado en la Figura 5).

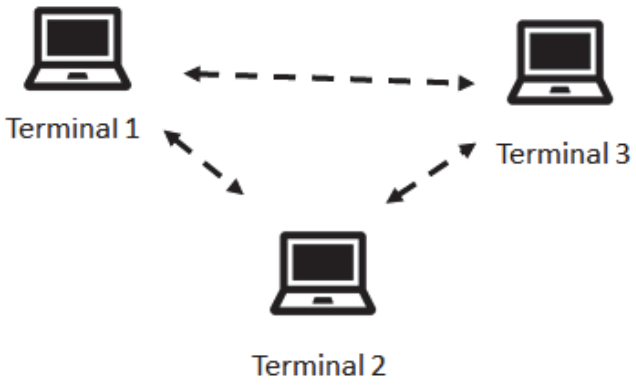


Figura 5. Configuración WiFi modo ad-hoc

- *Modo infraestructura* (*Basic Service Set* (*BSS*) *o Extended Basic Service Set* (*EBSS*)), más ampliamente utilizado y consistente en un dispositivo denominado *Access Point* (*AP*) que se comporta como un nodo central (Figura 6). Éste posibilita la conexión como nodo intermedio entre los diferentes terminales y todo el tráfico debe atravesarle. Además suele utilizarse para dar conectividad a la red cableada.

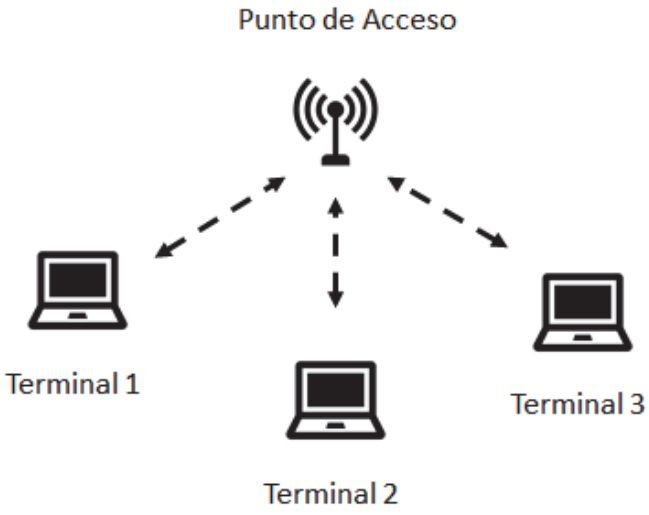


Figura 6. Configuración WiFi modo infraestructura

Su funcionamiento es el siguiente:

1. Los AP, una vez configurados por un administrador o controlador, emiten una señal de forma periódica identificando su canal, su *Service Set IDentifier* (*SSID*), el término técnico es *beacon*. Este incluye toda una serie de características del AP.
2. En cada terminal inalámbrico que quiera conectarse con un determinado AP, el usuario de dicho terminal selecciona manualmente o configura de forma automática con qué SSID desea conectarse. Podría hacerlo indicando un AP concreto, una frecuencia concreta, canal o dirección MAC del AP deseado.
3. El dispositivo de red WiFi intercambia mensajes especiales de petición dirigidos al AP seleccionado para asociarse (proceso de asociación) y autenticarse (proceso de autentificación), cuando este activado este método de seguridad.
4. Una vez el AP "seleccionado" responda afirmativamente, el terminal obtendría conectividad de enlace mediante WiFi con el AP.
5. Por último, si se opera como red IP, que es lo más habitual, una vez se le dote al terminal de la correspondiente identificación de nivel de red (dirección IP y resto de información de routing, *Domain Name Server* (*DNS*),…), el usuario podría hacer uso de la aplicación que desee mediante su interfaz de aplicación correspondiente.

- *Modo Malla* (*mesh*): consiste en que los diferentes AP pueden configurar una red mallada con enlaces inalámbricos entre ellos. Algunos de ellos pueden dar conectividad a la red cableada. En estos casos se requieren software adicional y protocolos específicos de encaminamiento para elegir, cuando existan varias opciones, el camino óptimo entre los dispositivos inalámbricos. Paralelamente puede formarse una malla entre los terminales y coexistir con la malla formada por varios AP. Desde el punto de vista de los terminales, estos continúan viendo la red en modo infraestructura, salvo que estos configuran una malla u operan modo *mesh* con conexiones directas entre ellos. El estándar que lo especifica es el IEEE 802.11s [95]. En la Figura 7 se muestra un ejemplo de topología en modo malla entre AP y entre terminales.

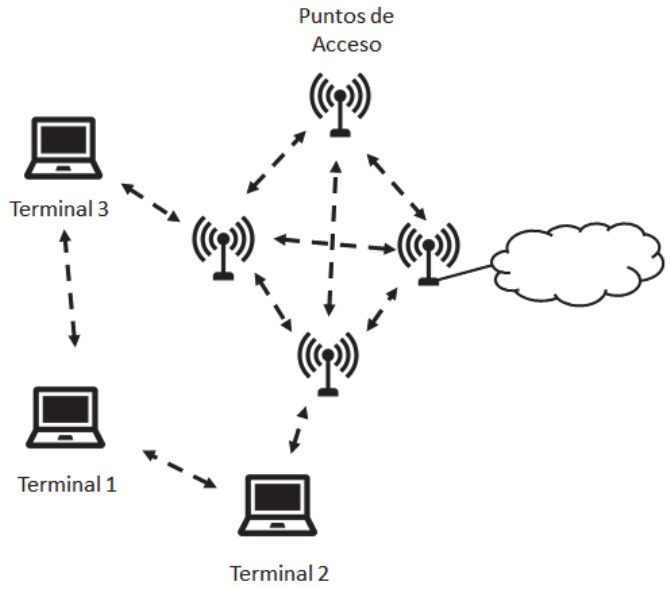


Figura 7. Configuración WiFi con topología en malla

Adicionalmente los AP pueden operar en otros modos como son: *Wireless Distribution System* (*WDS*) permitiendo establecer puentes inalámbricos entre ellos, WDS y modo infraestructura de forma combinada (comúnmente denominada modo AP) que en la práctica es muy ineficiente, *Wireless Client* en los que los AP se comportan como terminales y Modo repetidor (*Range Extender*) en los que los AP son simples amplificadores de señal RF.

WiFi trabaja en la banda de frecuencias médica, científica e industrial (*ISM*, del inglés *Industrial, Science and Medical*), siendo las bandas de 2.4 GHz y 5 GHz las más

utilizadas. La versión más reciente opera en la banda de 60 GHz y está siendo reconocida como *Wireless Gigabit* (*WiGig*). Estas bandas se caracterizan por ser completamente libres para cualquier uso, salvo ciertas restricciones de potencia de transmisión en determinados países.

La forma de una red con tecnología WiFi consiste en seleccionar un determinado canal (frecuencia central) para que todos los terminales que se quieran comunicar deban usar ese canal común. Como ya se indicó, en el caso de modo infraestructura, el AP fija el canal/frecuencia de trabajo y define el identificador de red o *SSID*, a modo de referencia. Con este ID, los terminales seleccionan el AP correspondiente. Dichos canales se distribuyen como se muestra en la Figura 8 en el caso de la banda de 2.4 GHz con IEEE 802.11b. En la misma se muestra la distribución de 13 o 14 canales (depende de países o zonas como EEUU, Japón, Europa, otros). Cada canal tiene un ancho de 22 MHz y las frecuencias centrales de cada canal están separadas 5 MHz.

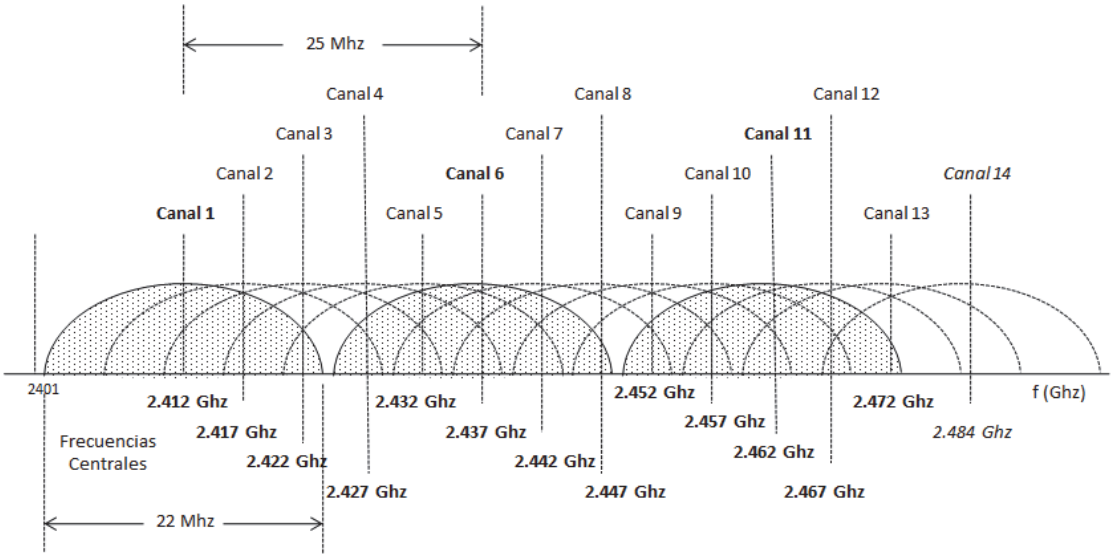
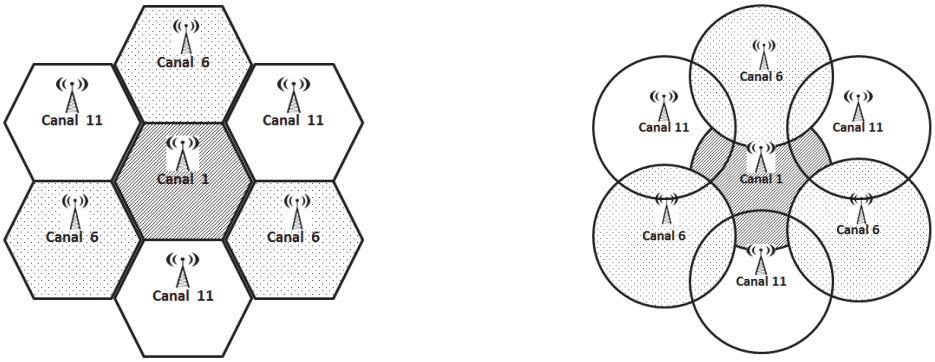


Figura 8. Canalización en la banda 2.4 GHz para IEEE 802.11b

El estándar original para el nivel físico define tres técnicas de modulación: *Direct Sequence Spread Spectrum* (*DSSS*), *Frequency Hopping Spread Spectrum* (*FHSS*) e *InfraRed* (*IR*). IEEE 802.11b utiliza DSSS, pero estándares más recientes se basan en *Orthogonal Frequency Division Multiple* (*OFDM*) [19] que es más eficiente que los anteriores. La cercanía entre los diferentes canales da lugar a cierto solape de los mismos, tanto mayor cuanto más cercanos estén. Este solape de canales da lugar a interferencias y pérdidas de capacidad. Si bien pueden provocar interferencias entre

canales, se utiliza porque resulta ser el más eficiente y garantiza un mayor throughput frente a las modulaciones clásicas.

El despliegue óptimo de redes inalámbricas que deseen cubrir zonas amplias es en forma de celdas donde cada AP configura y controla su celda. En la Figura 8 se muestra que los tres canales que no se solapan son el canal 1, el canal 6 y el canal 11. En la Figura 9.a se muestra una forma común de representar las redes celulares, basadas en estaciones base o redes inalámbricas a modo de celdas basadas en AP. En la figura 9.b se muestra una aproximación más real, en la que se representa como un círculo el radio de cobertura y con zonas ligeramente solapadas entre ellos. Estos solapes de canales distintos son recomendables para evitar zonas sin cobertura y permitir la movilidad de los terminales sin perder conectividad. En ambos casos la representación es ideal ya que el diagrama de radiación de una antena omnidireccional suele ser bastante más irregular, aunque se puede aproximar al mostrado en la Figura 9.b.



a. Esquema celdas ideal *b. Aproximación real*

Figura 9. Estructura basada en celdas de redes inalámbricas

El principal reto que se ha seguido para el diseño e implantación de las redes WiFi es el aumento de velocidad de transmisión mediante un aumento de canalización o técnicas de modulación. Además, en ciertos casos es necesario el uso de múltiples *streams* (múltiples antenas) conocido como diversidad espacial, para con ello aumentar la capacidad real y así poder teóricamente, soportar toda la serie de nuevos servicios, especialmente multimedia de alta calidad, que demandan elevadas prestaciones como ya comentamos en el apartado anterior.

Debemos resaltar la ventaja que representa que los estándares IEEE 802.11 mantengan una compatibilidad entre sus diferentes variantes y evoluciones. Concretamente se permite que terminales o equipos que operen en el estándar IEEE

802.11b y el IEEE 802.11g sean soportados por AP que operen en IEEE 802.11n. Esta compatibilidad permite la reutilización de gran cantidad de interfaces de red incorporados en los terminales fijos o móviles, aunque pueda representar una pérdida de capacidad global al adaptarse el AP a las condiciones de cada terminal.

2.2.1 Carencias o limitaciones de redes inalámbricas

Toda tecnología de red inalámbrica no está exenta de problemas o limitaciones, como también tienen o pueden tener las redes cableadas. Tanto en un tipo de red como en la otra, el compartir un recurso con capacidad limitada puede dar lugar a diferentes situaciones no deseadas. Ejemplos de ello son la congestión o saturación de líneas, los retrasos o pérdidas de paquetes...

Usar como medio un canal de comunicaciones radioeléctrico está sujeto a un mayor número de efectos adversos. Si bien esto se resuelve con cierta QoS en redes celulares [96], debemos recordar que la calidad de una red está relacionada con la tasa de datos soportada y con la tecnología utilizada. Pero además, depende especialmente, del estado o condiciones de la red de acceso y de transporte, o en general de las condiciones del canal o medios utilizados. La evidencia empírica así lo demuestra que en WiFi la QoS no se controla aceptablemente. Concretamente no se puede garantizar ciertos aspectos como:

- Evitar pérdida de conectividad (cobertura).
- Registrar zonas de sombra de señal.
- Mantener un throughput constante independientemente del tipo de servicio o número de usuarios.
- Controlar la congestión o saturación del canal.
- Evitar interferencias *ElectroMagnetic Interference* (*EMI*).
- Evitar solapes de canales.
- Selección de terminal base o AP en mejores condiciones.
- Elección de canales más eficientes.
- Bloquear o limitar tráficos no permitidos.
- Evitar la captura de tráfico por terceros (vulnerabilidad).
- Optimizar el gasto de batería de dispositivos portátiles.

Para mejorar muchos de estos aspectos otros autores han propuesto multitud de iniciativas. De entre ellas resaltamos [97], en la que Gong et al. plantean un problema de optimización en el que hay que maximizar el throughput, Ratnam et al., en [98], donde se evalúan las prestaciones de TCP en presencia de congestión y pérdidas en redes inalámbricas, Heusse et al., en [99], describen la anomalía en las prestaciones que es intrínseca al funcionamiento de WiFi y a su compatibilidad entre tecnologías y estándares, Velayos et al., en [100], miden las prestaciones de capacidad en 802.11b para diferentes fabricantes y diferentes resultados, Kouhbor et al., en [101], detallan la importante tarea de diseño de la red así como la localización y el número óptimo de AP; proponen un modelo matemático para determinar ambos parámetros.

Muchos de estos problemas son habituales y lamentablemente no pueden evitarse. Para otras situaciones no se han buscado soluciones. Por ejemplo, subrayar que el propio IEEE ha estandarizado la gestión en el cambio de una celda a otra (AP a AP), (IEEE802.11f) [102] y quedó obsoleto por la falta de iniciativas de los fabricantes para aplicarlo en sus productos. Sobre la base de estas situaciones especiales, es donde hemos centrado el desarrollo de esta tesis, partiendo de detectar situaciones comunes no deseables en el uso cotidiano de las redes WiFi y aportando soluciones de mejora.

De entre los posibles aspectos que hemos realizado su estudio, comportamiento, análisis de evidencias y desarrollado propuestas de mejora están:

- Control de admisión para garantizar un reparto más equitativo entre los servicios que hacen uso de canal en función de las necesidades y capacidad disponible. Esto incluye regulación de tráfico y servicios así como el balanceo de terminales.
- Elección guiada de AP que pueda ofrecer mejores prestaciones a los terminales que lo demanden según condiciones de cada canal.
- Aplicación de localización de terminales para mejor distribución y control de situaciones especiales.

Planteado de forma general se busca la forma de dotar a los AP de un papel más importante en la gestión de los mecanismos que regulan las redes WiFi en modo infraestructura y no solo sean simples anunciadores de su disponibilidad para dar servicio de conectividad a los terminales que lo requieran.

En el contexto de esta tesis doctoral se considera que los AP podrían tener un papel más activo (de forma proactiva y reactiva) en el control y gestión del canal inalámbrico gestionado por cada uno de ellos, y en el uso que hacen los terminales del mismo. Esto podría ser habilitado de manera similar a como lo realizan las redes celulares, en las que la *Base Station* (*BS*), dispositivo con funciones equivalentes a las de los AP, si realizan funciones de control y tienen un mayor protagonismo.

2.3 Calidad de servicio en WiFi

Hoy en día hay poco consenso sobre la definición precisa de QoS en redes de comunicación, como lo indica [73]. Los proveedores de red (operadoras) se refieren a ella como la calidad del servicio o nivel de servicio que la red ofrece a las aplicaciones o usuarios en términos de parámetros de QoS de la red, incluyendo latencia o retrasos de paquetes que atraviesan la red, fiabilidad de la transmisión de paquetes y throughput. No obstante, desde el punto de vista de los usuarios de aplicaciones, la QoS generalmente se refiere a la calidad de la aplicación como es percibida por el usuario, por ejemplo la calidad de la presentación de un video, la calidad de un sonido, la capacidad de respuesta en voz interactiva...

Dada la importancia de este tema en las comunicaciones multimedia en las redes veamos algunas definiciones. Según la Real Academia de Ingeniería, calidad de servicio se define como "*Efecto global de las características de servicio que determinan el grado de satisfacción de un usuario del servicio*" [103] . Según Wikipedia "*QoS o Calidad de Servicio (Quality of Service, en inglés) es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente para medir la calidad de servicio son considerados varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter, etc*." [104], y según la *Unión International de las Telecomunicaciones* (UIT, del inglés *Union International Telecommunication*) se define como "*el efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción de un usuario de dicho servicio*." [96]. Finalmente podemos indicar que según [105] QoS puede entenderse como la "*capacidad para controlar tráfico mediante mecanismos de manejo*

en la red de tal forma que la red acuerde los servicios necesarios de ciertas aplicaciones y usuarios sujetos a políticas en la red".

Independientemente de su definición, lo que parece evidente es que la calidad de servicio en redes de comunicaciones es bastante importante para determinadas aplicaciones y en especial en redes inalámbricas como WiFi. Existen diferentes servicios en los que si no se cumplen determinados valores mínimos podría ser inaceptable la calidad de los mismos. Por ejemplo la pérdida de muchos paquetes de datos en una red puede ser inaceptable aunque haya retransmisiones. Incluso pueden perderse algunos de ellos y no sea necesario reenviarlos para una imagen en la que solamente algunos pixeles podrían verse afectados, en cambio en un servicio de transferencia de archivos, la integridad y exactitud de los mismos tiene que estar garantizada. Por otro lado en una comunicación de voz retrasos superiores a 400 ms son inaceptables como indica la recomendación G.114 [106] de la ITU-T, pues el oído humano es capaz de detectar ese efecto.

Los requisitos básicos que determinan la calidad de servicio de una conexión o comunicación son: tiempo de respuesta de los servicios, pérdidas de paquetes, SNR, diafonías, eco, interrupciones, frecuencia de respuesta, niveles de sonido, y otras variables como son la capacidad de tráfico, cobertura de una red, limitaciones de usuarios o servicios, probabilidades de error o pérdidas...

La relación de parámetros más relevantes que determinan la calidad para aplicaciones multimedia o de la red de comunicación que provea dicha QoS es:

- *Throughput:* el volumen de información o la tasa de paquetes atraviesan la red por unidad de tiempo. Disponer de la máxima tasa de bits siempre sería deseable. Algunas veces se suele usar el término bitrate (bps). Este término se aplica aquí como un recurso de la red que necesita ser apropiadamente gestionado y asignado a las aplicaciones.
- *Retraso (Delay):* este es el tiempo en que un paquete tarda en atravesar desde un extremo al otro. El mínimo retraso es siempre deseable.
- *Jitter:* representa una medida de las variaciones del retraso producidas durante una comunicación.

- *Latencia:* suma de los retrasos parciales de una comunicación o duración global de la transmisión de los paquetes. Este parámetro debería ser el mínimo posible.
- *Tasa de paquetes perdidos* (*Packet Loss Rate*): la cantidad de paquetes perdidos global o en proporción frente a los recibidos. Este parámetro debería ser el mínimo posible.
- *Tasa de paquetes erróneos* (*Packet Error Rate*): la cantidad de paquetes recibidos con alguno de sus datos erróneos. Este parámetro también debería ser lo mínimo posible.
- *Fiabilidad* (*Reliability*): medida de la disponibilidad de una conexión o medida de las caídas del enlace.

2.3.1 Grado de Servicio

En el ámbito de las redes telefónicas, para llamadas de voz, existe otra medida de calidad que se denomina *Grado de Servicio*, que representa un aspecto de la calidad que un cliente espera durante su experiencia cuando realiza una llamada telefónica. Puede medirse como la probabilidad de que una llamada sea bloqueada o retrasada más de un determinado período de tiempo. Generalmente suele representarse como el cociente entre el número de llamadas satisfactorias y llamadas pérdidas, en el caso de medida basada en pérdidas.

Otras medidas provenientes del ámbito de las redes públicas (normas ITU-T o ITU-R) son:

- *Mean Opinion Score (MOS*): medida aplicada para las redes telefónicas para determinar la calidad de sus comunicaciones. Es una recomendación ITU-T de la norma P.800 [107]. Esta define métodos de determinación subjetiva de la calidad de transmisión. Su aplicación ha sido trasladada a las tecnologías VoIP.

En la Tabla 1 se muestran los valores de MOS asociados por el esfuerzo para comprender un mensaje.

Tabla 1. Valoración MOS según estándar P.800

MOS	Calidad	Esfuerzo necesario para comprender el significado de las frases
5	Excelente	Ningún esfuerzo
4	Buena	Cierta atención es necesaria; ningún esfuerzo apreciable
3	Regular	Esfuerzo moderado

2	Mediocre	Esfuerzo considerable
1	Mala	Significado incomprensible, aun con el mayor esfuerzo

- *Perceptual Evaluation of Video Quality* (*PEVQ*): proyecto ganador organizado por el grupo de trabajo *Video Quality Experts Groups* (*VQEG*) se convirtió en la recomendación ITU-T J.247 [108] en 2008. Provee medidas MOS de la calidad de video de IPTV, *streaming* de video, TV móvil y videotelefonía. Hace una medida completa comparando cada fotograma o *frame* de una señal de video bajo prueba con el video original (*master*) sin comprimir.
- *Perceptual Evaluation Audio Quality* (*PEAQ*): es un algoritmo estandarizado por la ITU-R para medir la calidad objetiva percibida del audio recibido. Es la recomendación ITU-R BS.1387. Utiliza una medida similar que el MOS para medir la calidad del audio [109].
- *Perceptual Evaluation Speech Quailty* (*PESQ*): sucede a la solución *Perceptual Speech Quality Measure* (*PSQM*) y constituye una familia de estándares para medir la calidad de la señal de voz detectada por un usuario a través de una línea telefónica. Existen diferentes notas para su aplicación en GSM, *Code Division Multiple Access* (*CDMA*), Wimax y otras redes móviles [110].
- *Perceptual Objective Listening Quality Analysis* (*POLQA*): es la siguiente generación de tecnologías para análisis de la calidad vocal para redes fijas, móviles y basadas en IP. Fue estandarizado por la ITU-T como recomendación P.863 en 2011 y puede ser aplicado para análisis de calidad de voz de HD, redes 3G y 4G/LTE. En septiembre de 2014 fue adoptada una nueva versión [111].

Desde un punto de vista de requisitos que deberían cumplir los diferentes operadores de redes telefónicas, existe legislación al respecto para medir la tasa de satisfacción de sus usuarios. Esta reglamentación pretende fijar unos mínimos desde los organismos competentes en la materia de cada país. En el caso español, tenemos que el Ministerio de Industria, Energía y Turismo específica en [112] información relativa a la regulación de condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas.

Parece evidente la necesidad de proteger los datos de voz, video y críticos a través de mecanismos que provean QoS en las redes de datos, máxime cuando las mismas ya

aplican la convergencia de todos los servicios (audio, video y datos) sobre las mismas infraestructuras y tecnologías existentes.

Para ello se introducen mecanismos de gestión de colas en los nodos de la red y en los terminales para priorizar un tipo de paquetes frente a otros. En general los sistemas operan mediante colas de tipo *Fisrt In First Out* (*FIFO*), en la que no existe diferenciación entre los paquetes. Este método es ineficiente para aplicaciones dependientes del tiempo. Por ello se han propuesto de manera general dos esquemas de colas:

- Conservativas.
- No conservativas.

El segundo caso de esquema de colas está orientado hacia flujos constantes que requieran solo una determinada cantidad de ancho de banda (bps) y ese es el que se utiliza. Por ejemplo no tiene sentido consumir 40 kbps de audio muestreado a 20 kbps si su reproducción debe hacerse a esta tasa preestablecida. Con esta solución se optimiza la capacidad de la red, se minimiza los requerimientos de buffers en nodos y terminales y no tiene impacto adverso sobre la información transmitida.

De forma más específica podemos indicar que las colas pueden ser sin prioridad *Fair Queue* (*FQ*) o con prioridad *Priority Queue* (*PQ*). Incluso pueden ser clasificadas por clases y filtrado por tipo de servicio u otras características. Las técnicas más utilizadas, además de la mencionada *FIFO*, son: *Token Bucket Fa*ir (*TBF*), *Stochastic Fairness Queuing* (*SFQ*), *Class Based Queuing* (*CBQ*), *Hierarchical Token Bucket* (*HTB*), *Random Early Detection* (*REM*), *Generic Random Early Detection* (*GREM*), *Hierarchical Fair Service Curves* (*HFSC*), *Differentiated Service Masking* (*DSMASK*), *Traffic Control INDEX* (*TCINDEX*), *Intermediate Queuing* (*IMQ*) [5].

Las tres primeras no permiten clases y el resto sí. Además se pueden aplicar varias políticas como:

- *Weighted Round Robin* (*WRR*).
- *Deficit Round Robin* (*DRR*).

Estos requisitos de calidad de servicio parecen evidentes que son más críticos en redes inalámbricas por la vulnerabilidad de las mismas. Están sujetas a mayor cantidad de efectos que podrían producir valores inaceptables de QoS para ciertos servicios.

2.3.2 Aspectos particulares de QoS en redes IEEE 802.11

En el caso especial de redes WiFi, el IEEE ha estandarizado un gran número de normas adicionales y relacionadas con las redes IEEE 802.11. De entre ellas hay que resaltar la norma IEEE 802.11e por estar especialmente relacionada con la calidad de las comunicaciones. Este estándar fue necesario desarrollarlo desde las primeras versiones de WiFi al detectarse limitaciones o carencias en el tratamiento de tráfico dependiente del tiempo (multimedia y otros), pues estos compiten en igualdad de condiciones que otros tráficos menos exigentes. Para aliviar estos problemas, pero no eliminarlos, se realizan clasificaciones de tráfico y una priorización de los mismos. A esta solución se le denomina *Wireless Multimedia Extension* (*WME*), también conocido como *Wi-Fi MultiMedia* (*WMM*). Esta denominación está relacionada con la certificación de interoperabilidad de la alianza WiFi [113]. Este estándar provee características de QoS básicas para redes IEEE 802.11. Concretamente prioriza el tráfico de acuerdo a 4 categorías de acceso, denominadas *Access Categories* (*AC*) - voz, video, *best-effort* y *background*, e identificadas con las etiquetas *AC_BK*, *AC_BE*, *AC_VI* y *AC_VO*. Con dichas etiquetas y la clasificación de los tráficos, se procesan para su envío en 4 diferentes colas permitiendo priorizar tráfico de voz frente al de video y el resto. En la Figura 10 se muestra dicha clasificación. No obstante esta norma no provee un throughput garantizado y se estandariza pensando en su uso especialmente en aplicaciones como *VoIP* sobre teléfonos WiFi (*VoWLAN*).

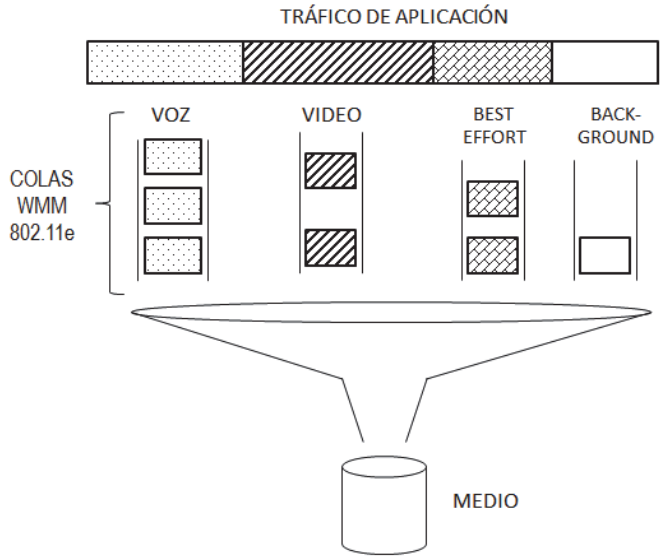


Figura 10. Colas y clasificación de tráficos para WMM

WMM reemplaza la original DCF operando mediante CSMA/CA por EDCF. Esta característica la utiliza el terminal que tenga habilitado WMM y así podría modificar los tiempos de transmisión según sea las categorías del tráfico y los valores de *Transmission Opportunity* (*TXOP*).

En [96] se realiza una exposición bastante detallada de la calidad de servicio en redes inalámbricas en general y en IEEE 802.11 en particular, mediante diferentes contribuciones de diferentes autores.

En cuanto a los parámetros que permiten medir la calidad de servicio de una red, en el caso de WiFi, por sus propias características, consideramos que además de los generales comentados al principio de este apartado, hay otros parámetros que influyen en la calidad de las mismas. Algunos aspectos que consideramos relevantes son:

- Capacidad de mantener la conexión entre el terminal y el AP bajo condiciones extremas (caídas de nivel de señal, baja sensibilidad del receptor, saturación del canal por otros servicios activos, elevado número de terminales...).
- Soportar movilidad entre celdas con fiabilidad, sin desconexión de servicios y mínimo tiempo de reconfiguración.
- Disponibilidad de canales o bandas de frecuencia disponibles para permitir cambios dinámicos entre los mismos.
- Disponibilidad de servicios de localización.

Si bien nos hemos centrado en la parte del canal inalámbrico, no debemos olvidar la dependencia directa de las condiciones de la subred cableada a la que dan acceso los AP. De forma directa, la saturación y los problemas de sobrecarga existentes en la red cableada y resto de la red inevitablemente se reflejarán en el AP y, por tanto, en la disponibilidad de acceso.

Todos estos aspectos consideramos que podrían ser complementarios para medir el grado de QoS de una red WiFi. La mayor parte de ellos se deben al acceso compartido a un canal radioeléctrico de limitada capacidad y la ausencia de ninguna reserva de tiempo, frecuencia o código para las comunicaciones. Además el acceso suele realizarse sin restricciones y esto produce, en determinadas condiciones, una reducción de la calidad de las comunicaciones existentes o no se pueda alcanzar la calidad deseada en la entrante. Tanto mayores serán estás variaciones de condiciones y sus parámetros

asociados de calidad cuanto más exigente sean las aplicaciones utilizadas por los diferentes usuarios.

El efecto más importante se detecta en aquellas aplicaciones en las que intervienen personas y requieren tiempo real, llamadas conversacionales o interactivas, dado que la visión o valoración de dichos servicios es determinante, expresada generalmente como QoE. En otras aplicaciones, puede no ser relevante la percepción sino que se prioriza la fiabilidad y por ello se apoyan en mecanismos de transporte basados en retransmisiones o reconocimientos para conseguirlo. Aplicaciones de mensajería instantánea, transferencia de archivos, correo electrónico, web estática,… se adaptan a los cambios para garantizar la integridad frente a otros aspectos.

2.4 Desafíos en investigación sobre comunicaciones multimedia en WiFi

El IP define un servicio *best-effort,* además en la red de acceso inalámbrica WiFi los terminales y resto de dispositivos compiten para acceder al canal sin tener en cuenta prioridades entre ellos. En muchos casos la entrega de paquetes no se garantiza. Para las aplicaciones *elásticas* esto no es un problema, pues no son sensibles a retrasos y pérdidas de paquetes y se pueden adaptar a la saturación del canal. Pero, las aplicaciones multimedia de tiempo real *no son elásticas*, y si son sensibles a estos problemas. En las aplicaciones multimedia de medios continuos (audio o video) suelen soportar retrasos de 250 ms [73], como por ejemplo la telefonía. En el caso de las aplicaciones multimedia de tiempo real *hard* estos límites temporales son más estrictos, como por ejemplo las aplicaciones de control o vigilancia.

Para proporcionar QoS en la comunicación IP se plantean tres posibles estrategias:

- *Solución 1*: aumentar ancho de banda (bitrate o capacidad disponible). Solución basada solamente en añadir recursos y conlleva un sobrecoste.
- *Solución 2*: modificar el comportamiento de las aplicaciones en tiempo real para que no dependan del tiempo y, por tanto, puedan adaptarse a las condiciones del canal (por ejemplo reproducciones demoradas en destino (buferizado en

recepción), transmisiones diferidas en origen (tiempo real no garantizado), replicación de tráfico…). Solución basada en rediseñar las aplicaciones que no son elásticas para que si lo sean y se adapten a las condiciones de la red. Esta solución es muy difícil o imposible de realizar en la mayor parte de las aplicaciones en tiempo real.

- *Solución 3:* añadir recursos con funciones de gestión a la red (control de congestión, priorización de tráficos, protocolos específicos de soporte de QoS…) y con ello posibilitar una adaptación o redistribución de recursos según necesidades. Podría considerarse una solución intermedia entre las dos primeras.

Los requisitos de cada aplicación no siempre se pueden garantizar debido a un uso compartido de los canales o enlaces. Una forma práctica de detectar esto es aplicar un *Service Level Agreement* (*SLA*), mediante el cual se especifiquen qué condiciones mínimas se supone que puede ofrecer un determinado servicio. Esta estrategia es muy habitual para proveedores de conexión a Internet y operadoras. En el caso de que no se cumplieran los requisitos acordados demandar en consecuencia las responsabilidades que se derivasen de su no cumplimiento. Para ello, se suele también clasificar los flujos en determinadas calidades en función de sus requisitos, desde un servicio denominado por ejemplo *clase oro* con las mejores prestaciones de ancho de banda, retrasos… frente a otros con menores requisitos (*best-effort*). Complementariamente a esto, los proveedores del servicio suelen incorporar mecanismos de control de admisión para mantener las especificaciones acordadas y garantizar que no se superen determinados umbrales. Estos umbrales suelen ser:

- Número de clientes o usuarios demandantes del servicio o
- Número o tipo de servicios por estos demandados

La mayor parte de las actuaciones para garantizar una QoS, especialmente en comunicaciones, están dirigidas a alcanzar una máxima QoE.

Lo que resulta evidente es que no hay una solución cerrada que resuelva los problemas relacionados con la QoS en todas las redes de comunicación. El gran reto es alcanzar unos mínimos parámetros de QoS y además, de forma continuada en el tiempo durante la provisión del servicio.

2.4.1 Consideraciones sobre aplicaciones no elásticas sobre WiFi

La mayor parte de las aplicaciones actualmente utilizadas son elásticas, o sea toleran retrasos y pérdidas y pueden adaptarse a situaciones de congestión. Pero todo esto está cambiando cada vez más, en tanto en cuanto, hay una tendencia a utilizar las redes WiFi de datos para comunicaciones de voz, por ejemplo *VoIP* que es un servicio no elástico. Lo mismo sucede con las comunicaciones de video, como videoconferencia, que no se adaptan tanto a los cambios de ancho de banda (bps) disponible. Por último el uso de aplicaciones de control con respuestas inmediatas o estrictas también introduce nuevas exigencias. Ante estas realidades se aprecia la necesidad de adoptar toda una serie de iniciativas encaminadas hacia garantizar mejor la QoS demandada por todos estos nuevos servicios.

En las Tablas 2, 3 y 4 [73], se ilustran los valores de retraso, jitter y requisitos de ancho de banda típicos para VoIP y video, incluyendo la QoE.

Tabla 2. Guía de retrasos para VoIP

Retraso una vía	Efecto sobre la calidad percibida
< 100 - 150 ms	Excelente QoE (retrasos no detectables)
150 - 250 ms	Aceptable QoE (ligeros retrasos)
250 - 300 ms	Inaceptable QoE

Tabla 3. Guía de jitter para VoIP

Jitter	Efecto sobre la calidad percibida
< 40 ms	Excelente QoE (jitter no detectable)
40 - 75 ms	Aceptable QoE
> 75 ms	Inaceptable QoE

Tabla 4. Requisitos de ancho de banda de codec de video

Codec de video	Ancho de Banda
HDTV no comprimido	1.5 Gbps
HDTV	360 Mbps
SDTV (Standard TV)	270 Mbps
MPEG2 4:4:4 comprimido	25 - 60 Mbps
HDTV calidad difusión (MPEG2)	19.4 Mbps
SDTV MPEG2	6 Mbps
MPEG1	1.5 Mbps

MPEG4	5 Kbps - 4 Mbps
H.323 (H.263)	28 Kbps - 1Mbps

Asimismo, en la Tabla 5 [114] se ilustra la sensibilidad que tienen ciertas aplicaciones de video sobre los principales parámetros que determinan la QoS.

Tabla 5. Sensibilidad de las aplicaciones de video en función de requisitos de QoS

Servicio	**Latencia**	**Jitter**	**Throughput**	**Pérdida de paquetes**
Teleconferencia de Video	Alta	Alta	Baja	Media
T. video de alta definición (*HD*)	Alta	Alta	Alta	Alta
Video bajo demanda (*VoD*)	Baja	Baja	Media	Baja
Video *streaming* en vivo	Media	Media	Media	Alta

Analizadas las diferentes tablas anteriores, resulta evidente que las redes WiFi no garantizan los requisitos de las aplicaciones no elásticas más exigentes; y en general, todas las redes IP que operan en modo *best-effort*. El reducido bitrate de las primeras versiones del IEEE 802.11 y, de manera más especial, el compartir el canal con otros usuarios reduce la disponibilidad de capacidad útil de las mismas. La capacidad de uso del canal decrece de forma directa con el número de servicios que soporta. Ante ello resulta indispensable aplicar mecanismos de control de admisión y control de tráfico.

Si bien existen diferentes definiciones, consideramos en nuestro contexto que un control de admisión es un proceso fuera de banda por el que un elemento de la red (o un conjunto de elementos) decide qué recursos están disponibles y son los suficientes para peticiones de nuevos servicios sin comprometer los servicios ya admitidos. Por ejemplo si el canal tiene un máximo ancho de banda de 3 Mbps y se cuenta con tres conexiones con bitrate de 1 Mbps, cualquier nuevo servicio entrante compromete los anteriores. Este control de admisión permite garantizar una mínima disponibilidad y permitiría calcular cuando la aparición de nuevos flujos redundaría en una reducción de la capacidad de uso con mínimas garantías. O sea que con ello básicamente lo que pretende es evitar la sobrecarga por el aumento de flujos y, especialmente en función de los requisitos de los mismos.

Un ejemplo claro es el comportamiento de tráfico en tiempo real con requisitos estrictos, que si no se alcanza un mínimo de ancho de banda [bps] (umbral) no se garantizan sus prestaciones.

Aunque podría pensarse que con solo aumentar el ancho de banda de la red WiFi y con ello, su capacidad, este problema se solucionaría, resulta evidente que mientras la red WiFi continúe operando en modo *best-effort* no garantiza los requisitos de las aplicaciones. Estos requisitos de QoS no pueden garantizarse por el reparto intrínseco en el uso del canal y porque las demandas de otros servicios crecerán o el número de potenciales usuarios también aumentarán. Por ejemplo no por contar con un elevado ancho de banda *de reserva* se pueden soportar todas las conexiones VoIP simultáneas y con ello desaparezcan los tan indeseados retrasos o cortes de comunicación.

Bajo esta premisa, volvemos a ver la necesidad de contar con mecanismos de reserva de recursos con control de admisión y clasificar las aplicaciones según sus características.

2.4.2 Estrategias dirigidas a mejorar la calidad de aplicaciones multimedia

Una de las técnicas más ampliamente utilizadas para reducir los efectos de la red que no garantizan ciertos parámetros de QoS es definir puntos específicos de reproducción y almacenar en buffer locales cierta cantidad de paquetes. Con ello se pueden reducir las variaciones en el retraso introducido en la red o reducido bitrate pero pierden inmediatez y características de tiempo real. Además para estas aplicaciones es preferible que, en general tengan el menor retraso posible y no tiene tanta importancia cuando llegan los paquetes, siempre que lo hagan antes del punto de reproducción. Incluso estas aplicaciones toleran bien algunas pérdidas de paquetes.

En general estas aplicaciones pueden ser:

- *Rígidas*: el momento de reproducción es fijo.
- *Adaptativas*: en las que el punto de reproducción se adapta a las condiciones.

En este último caso, no siempre la red cuenta con mecanismos para estimar las variaciones de condiciones en la misma para variar los puntos de reproducción.

Por otro lado, podríamos también decir que las aplicaciones pueden ser:

- *Tolerantes a interrupciones del servicio.*

- *No tolerantes a interrupciones del servicio.*

Relacionando ambas clasificaciones podríamos combinarlas de forma:

- *Intolerantes y rígidas.*
- *Tolerantes y adaptativas.*

Desde el punto de vista de la red, deberíamos preguntarnos qué servicios debería ofrecer para cada caso, y ante ello tenemos:

- *Garantizado para aplicaciones intolerantes y rígidas*: donde la garantía es fija y la red se compromete con los clientes con un acuerdo de tráfico. Este caso es de difícil aplicación para redes WiFi pues operan *best-effort*.
- *Servicio de predicción para aplicaciones tolerantes y adaptativas:* que siguen alguno de los siguientes patrones:
  - Si las condiciones no cambian, se puede adquirir un compromiso con el servicio actual. No aplicable a redes WiFi.
  - Si las condiciones cambian, tomar acciones para una entrega con prestaciones consistentes (ayudar a las aplicaciones para minimizar los retrasos en la reproducción). Aplicar mecanismos correctores, control de admisión..., especialmente recomendado en redes WiFi.
  - Asumir de forma implícita que la red no cambia en el tiempo.
- *Servicio best-effort:* modo actual en WiFi, ineficiente bajo ciertas circunstancias.

Tras esta visión de casos, podemos indicar que existen un gran número de propuestas, mecanismos y tecnologías para proveer QoS en aplicaciones multimedia en cualquier red de comunicación y en particular para WiFi. Ya que el ancho de banda es el principal recurso de las redes WiFi, este debe ser distribuido en una forma que simultáneamente satisfaga todos los requisitos de cada aplicación. Para ello se plantean dos posturas o estrategias básicas:

- *Sobre-aprovisionamiento de ancho de banda*: cuando la red no puede soportar QoS entonces se actualiza la infraestructura o

- *Gestión de ancho de banda*: consistente en aplicar mecanismos de QoS para gestionar el ancho de banda.

Mientras la primera técnica suele aplicarse para redes cableadas, en el caso de redes inalámbricas, al usar un canal radio limitado, la segunda estrategia es la que se debe desarrollar [73].

Además de las dos anteriores, existen otras soluciones bastante utilizadas y estándares para proveer QoS en LAN y WAN pero ineficientes para WLAN. Estas se clasifican en:

- *Servicios Integrados Garantizados (IntServ).*
- *Servicios Integrados de Carga controlada.*
- *Servicios Diferenciados (DiffServ).*

Indicar que *IntServ* constituye un protocolo fuera de banda para reservar recursos en los nodos para determinados flujos o conversaciones. El protocolo más conocido es *Resource reSerVation Protocol* (*RSVP*) [115]. En cuanto a *DiffServ* se basa en marcar los paquetes para su clasificación y priorización. Mediante el análisis de la cabecera de los paquetes IP (Campos: *Type of Service* (*TOS*) o *Differentiated Services Code Point* (*DSCP*) + ECN) [116], los nodos determinan el reenvío priorizado de los mismos mediante un tratamiento especial por colas con prioridad.

En la Tabla 6 se muestran algunos valores estándar para los campos del cabecero IP específicos por tipo de servicio.

Tabla 6. Valores estándar de variables de priorización

Tipo de servicio	**DSCP**	**Prioridad IP**	**IEEE 802.1p**
Control de red	30	6	7
Garantizado	28	5	5
Carga controlada	18	3	3
Resto de tráfico	0	0	0

Las aplicaciones o servicios multimedia que están requiriendo especial atención sobre las redes WiFi en particular y en Internet en general son *IPTv* [117] con soporte de alta definición y 3D, videoconferencia entre uno o varios interlocutores, *VoIP* con requisitos especiales de bajo retraso, servicios de *streaming* multicast eficiente [118],

juegos on-line con requisitos estrictos temporales, tecnologías en el campo de los codecs [119]...

Una vez analizado el marco teórico sobre las tecnologías de redes WiFi y los servicios que pueden soportar, así como las limitaciones que presentan para proveer QoS, nosotros nos centramos en dotar de métodos o modelos para favorecer tráfico no elástico que consideramos prioritarios para mejorar la QoS de los mismos, sin entrar en consideraciones sobre codec ni aplicaciones específicas.

Capítulo 3. Contextualización, evidencias y caracterización

En este capítulo presentamos nuestras propias experiencias, medidas y evidencias empíricas que complementan la literatura existente y que están relacionadas con las carencias o limitaciones intrínsecas de WiFi. Planteamos un modelo de optimización de parámetros vinculados directamente con el modo de operación y la respuesta de WiFi. Nos centramos en comunicaciones de video, aunque podría extrapolarse al resto de aplicaciones en tiempo real como comunicaciones de voz, juegos on-line, videovigilancia... al ser las principales afectadas por el modo de funcionamiento a nivel físico y MAC.

3.1 Contextualización

Como paso previo a la descripción de diferentes propuestas dirigidas a mejorar las prestaciones de redes WiFi que constituyen el objeto de esta tesis, hemos realizado un análisis de diferentes problemas o limitaciones detectadas en dichas redes. Algunas son muy habituales debidas a diferentes causas como errores de planificación de la instalación o configuración de canales, limitada cobertura y capacidad, falta de estandarización… Diferentes evidencias existen en la literatura existente como se pueden encontrar en [97] [98] [99] [100] [101] ya comentadas en el capítulo 2 apartado 2.2.

Para realizar este estudio y contar con conocimientos detallados del comportamiento de estas redes nos hemos basado en la experimentación previa. Ésta consistió en analizar casos reales con diferentes plataformas de test así como simulaciones basada en ordenador. Tras estos estudios empíricos consideramos que se justifica la necesidad de aplicar actuaciones o mecanismos de mejora en ciertos aspectos.

En el capítulo anterior ya describimos algunas situaciones no deseadas que se pueden producir durante el uso de las redes WiFi que no han sido completamente resueltas. En especial centramos nuestra atención en las siguientes direcciones:

1. Búsqueda de un modelo de distribución ponderado en el uso del canal inalámbrico por terminales y tráficos (flujos),
2. Búsqueda de un modelo y método de elección de AP por parte de los terminales más eficiente,
3. Búsqueda de un modelo y método para prevenir desconexiones y re-asociaciones de terminales a AP basadas en localización.

Estas y otras líneas de actuación consideramos que podrían verse de forma global como un sistema integrado en el que los AP realicen una mayor gestión del uso del canal radioeléctrico y no dejar a los terminales la toma de muchas decisiones que actualmente les son asignadas y pudieran resultar no ser las óptimas.

Consideramos que, para acometer diferentes actuaciones sobre diferentes aspectos de las redes WiFi, es necesario plantear un modelo basado en múltiples parámetros que, de forma directa o indirecta, pudieran afectar a sus prestaciones. Estos parámetros pueden ser medibles computacionalmente (ancho de banda, número de terminales, número de AP, número conexiones entrantes...) o relacionadas con la calidad subjetiva de un sonido o video según la percepción de cada receptor. Otros parámetros podemos considerarlos funcionales o no funcionales que condicionan el comportamiento de ciertos servicios bajo ciertas condiciones de contexto.

Para desarrollar la explicación de este análisis previo o experimental que da lugar al análisis de casos y propuestas, se debe contextualizar nuestra experimentación. En la Figura 11 se ilustran las tres topologías de acceso más habituales. En todas ellas se aprecia la necesidad de contar con un dispositivo que concentra y redirija el tráfico. Estos dispositivos, conocidos como nodos, encaminador, BS o AP según cada caso, suelen reenviar o encaminar los paquetes hacia otro dispositivo de la red para que estos alcancen otro elemento intermedio o el destino final correspondiente.

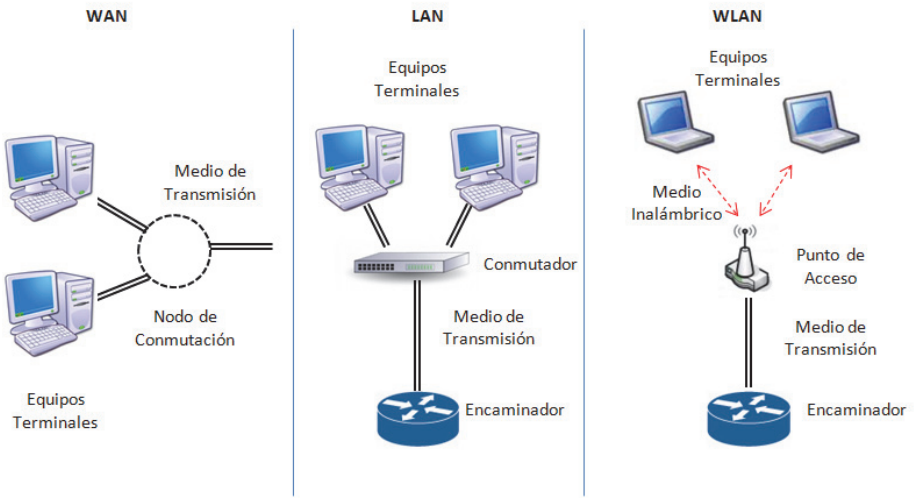


Figura 11. Topologías de acceso más habituales

En los tres casos mostrados en la Figura 11, determinados medios de transmisión son compartidos por las diferentes comunicaciones. En el caso de acceso a Internet (WAN) se comparte el enlace de salida después del nodo de conmutación, en la LAN el segmento de red que llega desde el conmutador al encaminador y en la LAN inalámbrica (WLAN) el segmento entre el AP y el encaminador, pero además y de forma especialmente importante, el canal radioeléctrico entre los terminales y el elemento que gestiona esa celda o BSS, en terminología IEEE 802.11.

En el caso de LAN y WLAN, como son Ethernet o WiFi, no se reserva ningún tipo de recurso para cada conexión y la principal diferencia es que mientras en la LAN el último segmento de cable es utilizado solamente por el tráfico que sale o va dirigido a cada terminal, en WiFi se comparte el canal inalámbrico. Otras tecnologías no WiFi reservan recursos como ancho de banda, frecuencia o sub-portadoras, slots de tiempo, código, otros. Las tecnologías que asocian recursos a servicios son conocidas como *Frequency Division Multiplexing* (*FDM*), *Time Division Multiplexing* (*TDM*), *Ortoghonal Frequency Division Multiple/Access* (*OFDM/OFDMA*), *Frequency Division Duplex* (*FDD*) y *Time Division Duplex* (*TDD*), que se aplican en otras tecnologías de redes inalámbricas como celulares, Wimax…

En lugar de reservar recursos, todos los terminales compiten en igualdad de condiciones por acceder al canal (cableado o inalámbrico). Este modo de acceso se ha mostrado bastante eficiente para las LAN y WLAN pues operan en modo difusión y se reduce el retraso vinculado con establecer y liberar circuitos o canales lógicos como en las redes WAN. Si bien este aspecto puede ser eficiente para garantizar elevadas velocidades puede no serlo bajo ciertas condiciones, pues cada terminal inserta tráfico cuando encuentra el canal libre sin ninguna regulación adicional. En esto consiste el método de acceso best-effort ya comentado, todos los terminales hacen uso del canal "*en cuanto puedan y todo el tiempo que puedan*", y por ello servicios que generan un mayor volumen de tráfico harán un uso más intenso del canal limitando las posibilidades a otros servicios.

Centrándonos en redes WiFi en modo infraestructura y bajo estas consideraciones a continuación procedemos a presentar diferentes pruebas experimentales realizadas y el análisis de los resultados sobre casos reales.

3.1.1 Simulación de comportamiento de flujos en WiFi

Como primer paso para evaluar el comportamiento y caracterizar el tráfico (flujos) no elástico sobre una red WiFi en modo infraestructura, procedimos a realizar diferentes pruebas de simulación con la herramienta ns-2 [120] para diferentes configuraciones de simulación. La primera simulación consistió en analizar el comportamiento de un nodo ante volúmenes de tráfico superiores a los soportados por el canal. Denominamos flujo

al conjunto de paquetes vinculados a una determinada conexión que tiene características de velocidad (bitrate), retraso, pérdidas...

Para ello se creó un escenario como el mostrado en la Figura 12, en el que participan dos terminales, etiquetados como 0 y 1 asociados a un canal de 1 Mbps a un dispositivo que hace las veces de AP, etiquetado con 2 y esté está conectado por un enlace de 10 Mbps y 10 ms de retraso en modo SFQ a un nodo destino etiquetado con 3. Las condiciones del canal WiFi se han configurado para valores básicos para facilitar el tratamiento de los resultados de la simulación. Las características del canal son las predefinidas para IEEE 802.11b, siendo perfectamente exportables los resultados para cualquier versión con los correspondientes factores de escala de IEEE 802.11g/n… y modelo de propagación, tipo de antena, colas y MAC.

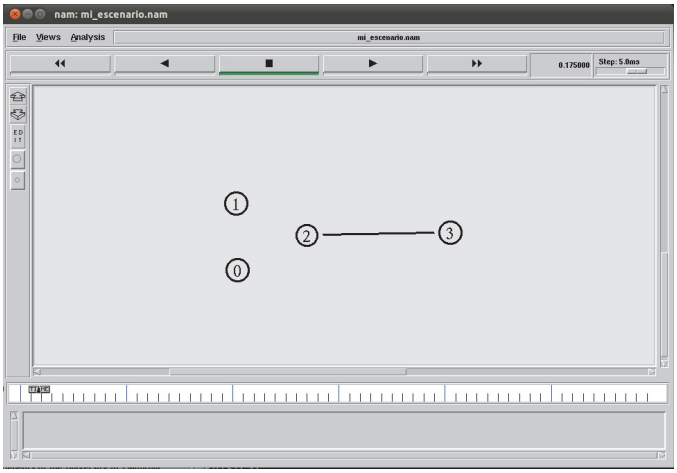


Figura 12. Escenario de simulación de subred WiFi modo infraestructura en NS-2

Nuestro objetivo fue analizar el comportamiento de los flujos CBR originados por un dispositivo, denominado nodo en el ns-2 y como se vería afectado por otro originado por otro nodo. En este caso el nodo 0 genera tráfico con destino al nodo 2 y observamos el efecto producido por otro originado por el nodo 1 con destino el mismo nodo 2. Ambos flujos denominados f1 y f2 son iguales y de aproximadamente 800 Kbps y con un tamaño de 1500 B. Con este valor garantizamos que un solo flujo puede perfectamente ser soportado por el canal pero ambos a la vez no. Utilizamos tráfico CBR al ser el más exigente en cuanto a QoS que junto con tráfico *Variable Bit Rate* (*VBR*) es el tipo de flujo más habitual (inelástico) dependiente del tiempo para comunicaciones de audio/video. De entre las múltiples simulaciones que realizamos, mostramos solamente aquellas que reflejan el comportamiento de los flujos ante variaciones en los tamaños de los paquetes y en las tasas de inserción de paquetes

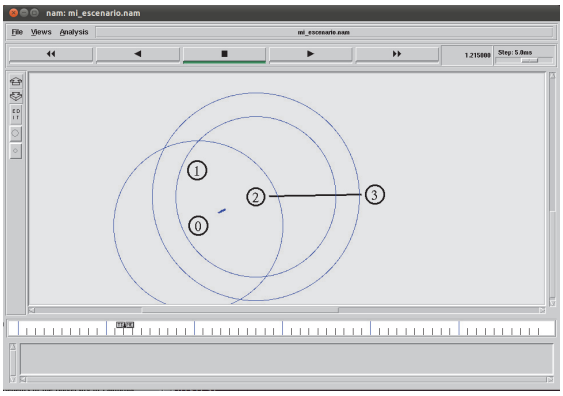
(bitrate) en el canal inalámbrico. Nuestra intención consistió en analizar como la capacidad limitada de los buffer en los nodos y especialmente la capacidad del enlace inalámbrico común compartido se ven afectadas por cambios en los bitrate y tamaño de paquetes insertados en el mismo. Para ello habilitamos en la simulación el código necesario para la generación de medidas de ancho de banda (bps) utilizado, visto también como velocidad de transferencia así como medidas en el número de paquetes recibidos o perdidos.

La duración de la simulación que representamos es de 7 segundos, suficiente para sacar conclusiones evidentes. La secuencia de instantes temporales donde se inician o finalizan los flujos se representa en la Tabla 7.

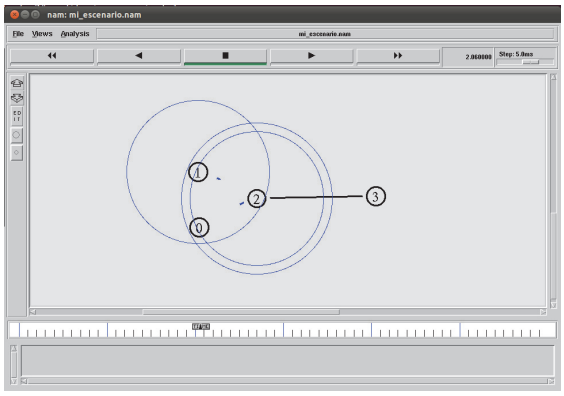
Tabla 7. Instantes temporales de inicio y fin de flujos

Instante temporal	Actividad
t = 0	*Inactividad. Se inicia simulación.*
t = 1	*Se inicia el flujo 1 (0-2) con un tamaño de paquetes de 1500 bytes y tasa de inserción cada 15 ms.*
t = 2	*Se inicia el flujo 2 (1-2) con un tamaño de paquetes de 1500 bytes y tasa de inserción cada 15 ms.*
t = 4	*El flujo 2 (1-2) finaliza.*
t = 5	*El flujo 1 (0-2) finaliza.*
t = 7	*Se finaliza simulación.*

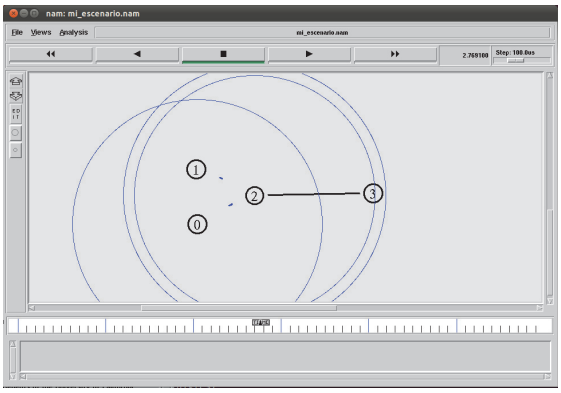
En las Figuras 13.a hasta la Figura 13.f se muestran diferentes instantes de la simulación en momentos especialmente interesantes para este caso.



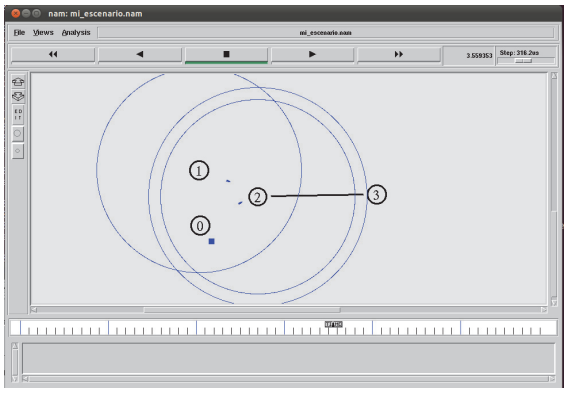
a) Instante 1,2 s



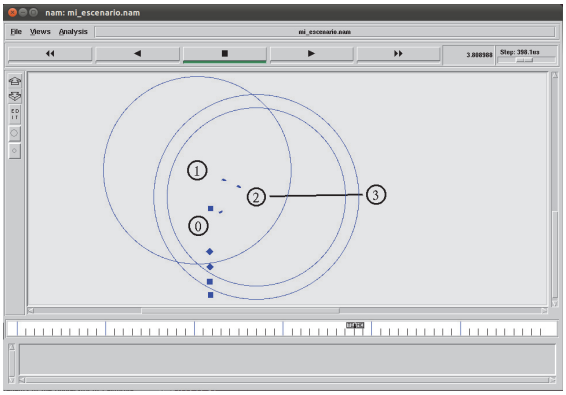
b) Instante 2,2 s



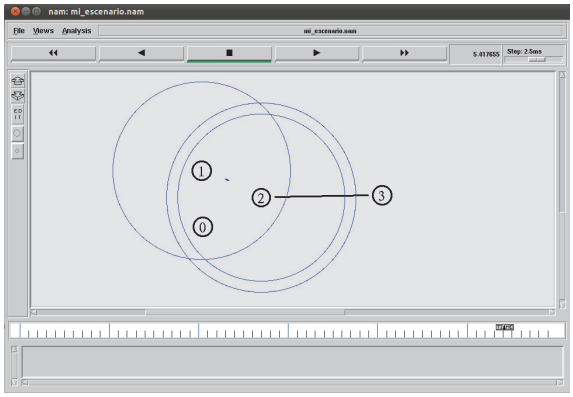
c). Instante 2,8 s



d). Instante 3,5 s



e). Instante 3,8 s



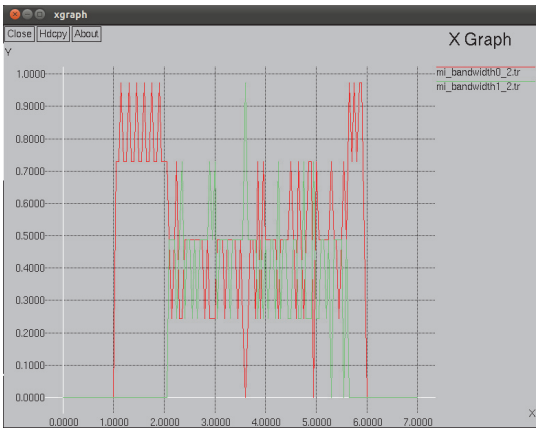
f). Instante 4,6 s

Figura 13. Instantes destacados de simulación NS-2

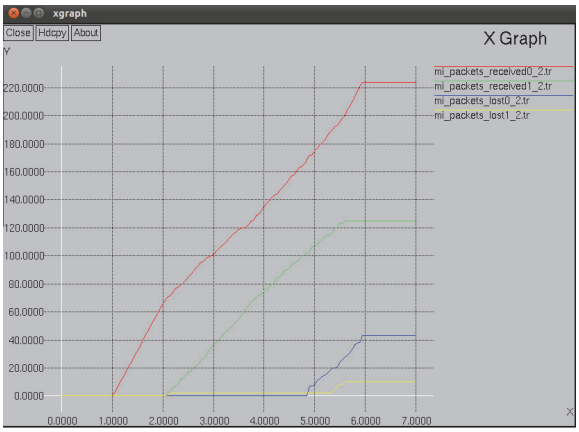
**Un video completo de esta simulación puede ser visualizado o descargado desde http://seritel.teleco.ulpgc.es/personal/tesis/simulacion_wifi_ns2.mp4*

En el instante t=1,2s (Figura 13.a) solo hay tráfico del primer flujo (0-2), en los instantes t=2,2s y t=2,8s (Figura 13.b y Figura 13.c) se comparte el canal con el segundo flujo sin ningún problema, sin embargo se aprecia que a partir de cierto instante, alrededor de los instantes t=3,5s y t=3,8s (Figura 13.d y Figura 13.e), debido a que la red no es capaz de absorber todo el tráfico generado por los dos emisores y ante el desbordamiento de los buffers de transmisión en cada nodo origen empiezan a descartarse (*drops*) paquetes del primer flujo (f1 (0-2)), y con posterioridad también se empiezan a perder paquetes del flujo f2 (1-2). Finalmente en la Figura 13.f se muestra como dejan de perderse paquetes pues ya después del instante t=4s, el f2 ya no está presente y por tanto se terminan de enviar los paquetes restantes.

Los datos obtenidos de ancho de banda (bps) y número de paquetes recibidos/perdidos de ambos flujos se muestra la Figura 14.a y la Figura 14.b, respectivamente.



a) Medida de ancho de banda (bps) utilizado por f1 (0-2) y f2 (1-2) para paquetes de 1500 bytes.



b) Paquetes recibidos y perdidos del flujo f1 (0-2) y de f2 (1-2) para paquetes de 1500 bytes

Figura 14. Resultados de simulación para flujos iguales

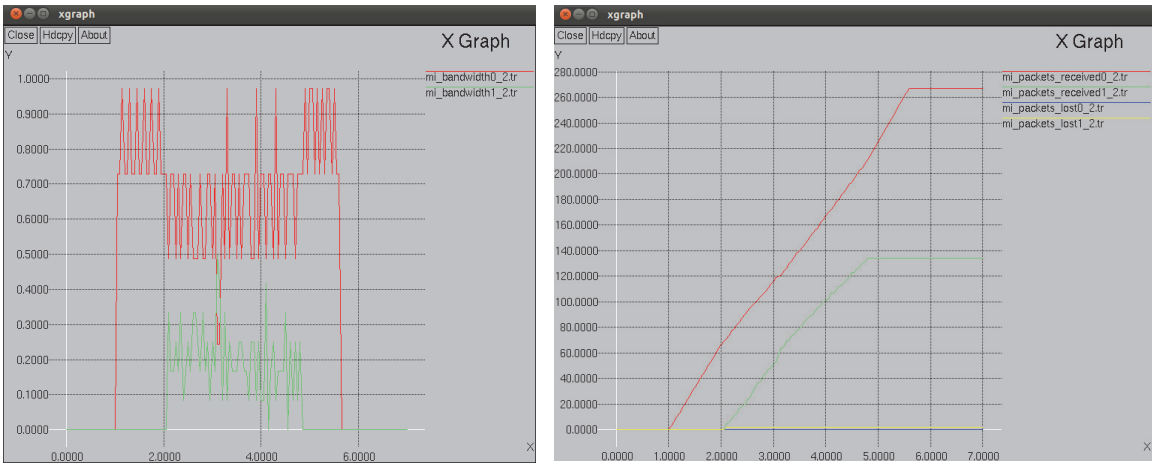
Como era de esperar, en la Figura 14.a se observa como al hacer uso en exclusiva del canal el flujo 1 en los primeros instantes, se alcanza de media la tasa máxima disponible. Tan pronto surge el flujo 2, a partir del instante t=2 se produce el reparto prácticamente equitativo del canal entre ambos flujos al no existir prioridades entre ellos. Durante el uso compartido del canal, se puede apreciar en la Figura 14.b que la proporción de paquetes recibidos y perdidos es prácticamente igual para ambos flujos, dado que ambos flujos tenían las mismas características. La diferente cantidad global se debe a que el flujo f1 estuvo activo 4 segundos (entre los segundos t=1 y t=5) y el flujo f2 estuvo solo 2 segundos, entre los segundos t=2 y t=4, como se indicó.

Es evidente que esta pérdida de paquetes relativamente alta en un canal limitado esta debida a dos grandes variables: al tamaño de los paquetes y la tasa de inserción de los mismos.

Simulación 1. Efecto de variación del tamaño de paquetes

A continuación procedimos a alterar el tamaño de paquetes de uno de los flujos para evaluar el resultado.

Si al flujo f2 le reducimos el tamaño de sus paquetes en 1/3, o sea unos 512 bytes, obtenemos los resultados mostrados en la Figura 15.a y Figura 15.b como en el caso anterior.



a) Medida de ancho de banda (bps) de f1(0-2) de 1500 bytes y f2 (1-2) de 512 bytes

b) Paquetes recibidos y perdidos de f1 (0-2) y de f2 (1-2)

Figura 15. Resultados de simulación con paquetes de f2 de 512 bytes

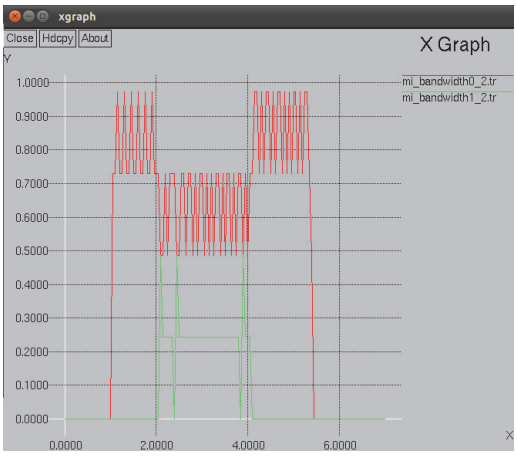
A la vista de las Figuras 15.a y 15.b, observamos que reducir en 1/3 el tamaño de los paquetes del flujo 2 permite que no se pierda ningún paquete de ninguno de los dos flujos. El reparto del ancho de banda disponible ha permitido insertar los paquetes de menor tamaño y con ello el flujo 1 no se vio afectado en cuánto a pérdidas, si en cambio en una evidente reducción de velocidad. El flujo 2 ha transmitido mayor cantidad de paquetes pero una menor cantidad de información. El menor tamaño de los paquetes permite que se inserten entre los slots temporales o períodos de *backoff* que el flujo 1 deja sin usar al liberarse el canal y menor uso los buffers. En este caso el flujo 0 encuentra el canal libre, hecho que en el caso anterior no se producía y por tanto de eliminaban muchos paquetes.

El objetivo de esta simulación era evidenciar y contrastar que alterando los tamaños de los paquetes de todos o ciertos flujos se puede optimizar el reparto del canal para favorecer un flujo frente a otros. Por tanto podemos concluir que con esto se prioriza un flujo frente a otro en condiciones de alta carga, y de forma evidente, un parámetro a configurar es el tamaño de paquetes de ciertos flujos, reduciéndolo para los que podríamos seleccionar como de menor prioridad.

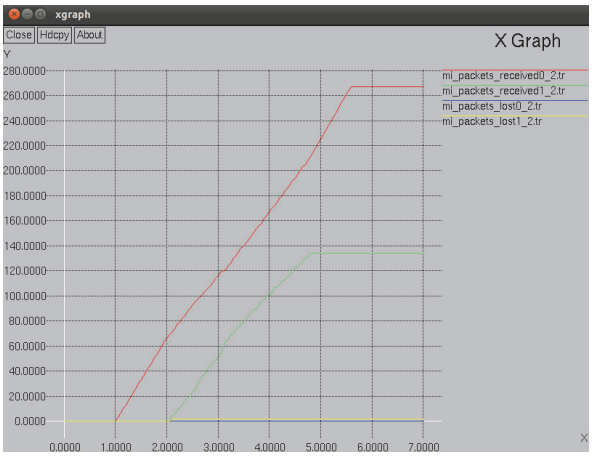
Simulación 2. Variación de la tasa de bits (bitrate)

Otra medida que consideramos necesaria simular para evidenciar el comportamiento de ciertos flujos es alterar la velocidad de inserción de paquetes o el bitrate. En este segundo caso mantuvimos ambos flujos a 1500 B pero el flujo f2 lo redujimos a una tasa de inserción de 50 ms (≈248 Kbps). Evidentemente este valor es

bastante bajo y el flujo 2 transfiere muy poca información. Los resultados se muestran en la Figura 16.a y Figura 16.b.



a) Medida de ancho de banda (bps) de f1 y f2 de 1500 byte, f1 a 15ms y f2 a 50ms

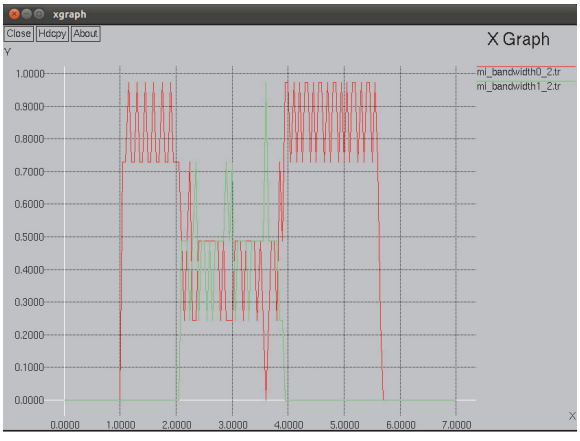


b) Paquetes recibidos y perdidos de f1 (0-2) y de f2 (1-2) para f2 a 248 Kbps

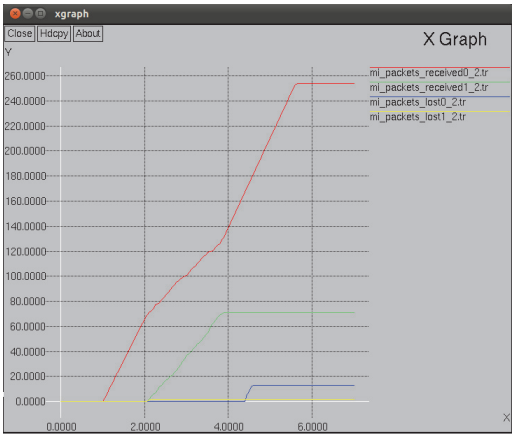
Figura 16. Resultados de simulación para f2 a 248 Kbps

Los resultados muestran que no se pierde ningún paquete de ninguno de los flujos, aunque el flujo 2 ha reducido de forma sustancial la cantidad de información transmitida.

Para evaluar los efectos de un cambio dinámico de bitrate durante la simulación, utilizamos un valor intermedio de unos 25 ms de tasa de inserción del flujo 2 para las condiciones del escenario inicial, pero actuando cuando empiecen a degradarse las prestaciones del flujo 1. Los datos obtenidos se muestran en la Figura 17.a y Figura 17.b.



a) Medida de ancho de banda (bps) f1 y f2 de 1500 byte, f1 y f2 a 15ms y f2 a 25 ms t=3



b) Paquetes recibidos y perdidos de f1 (0-2) y de f2 (1-2)

Figura 17. Resultados de simulación para f2 a 400 Kbps en t=3s

En este último caso hemos forzado que inicialmente ambos flujos tuvieran una tasa de inserción de 15 ms pero durante la simulación reducimos la tasa de f2 a 25ms. Como se observa en la primera simulación (Figura 13.d), aproximadamente en el instante t=3'5 s se empezaban a perder paquetes, por tanto para ver el efecto de reducir la tasa del flujo 2 en ese instante y poder actuar para evitarlo, exactamente en t = 3s el flujo f2 reduce su tasa de inserción a 25 ms y con ello reducimos su efecto sobre el flujo f1. La Figura 17.b muestra como la pérdida de paquetes del flujo f1 se detiene al reducir la tasa de inserción de f2 aproximadamente a la mitad, que era el objetivo buscado mediante esta simulación.

A la vista de los resultados anteriores, determinamos que se puede hacer uso de los mismos para gestionar las características de determinados flujos en beneficio de otros, especialmente alterando el bitrate o el tamaño de los paquetes. Para aplicar estos resultados hacemos las siguientes consideraciones según las necesidades de los flujos en cada caso:

- Para estas simulaciones, el flujo 1 lo hemos considerado prioritario frente al flujo 2 y por ello la actuación en beneficio de f1 están dirigidas a alterar características de f2 (concretamente reduciendo su velocidad (bitrate) y/o tamaño de paquetes).
- El flujo f1 podría también reducir su tamaño de paquete, aun siendo prioritario, si es asumible una reducción de información enviada.
- El flujo f1 también podría reducir su tasa de inserción por la misma cuestión anterior.
- Si el flujo f1 fuera muy prioritario, considerado como un servicio dependiente del tiempo, debería verse mínimamente afectado por otros.
- A igualdad de prioridades o requisitos de bitrate de ambos flujos y bajo las condiciones límite como las simuladas, no se pueden mantener o garantizar (canal inalámbrico limitado), y se necesitan otras actuaciones.

Como resumen y análisis final tras esta experimentación, indicar que conociendo o estimando la capacidad del canal WiFi podría realizarse una distribución más eficiente del mismo, alterando características de unos flujos para beneficiar a otros cuando las condiciones así lo permitan. Por tanto, en general es prioritario tener perfectamente caracterizados los servicios para poder garantizar sus requisitos.

En el siguiente apartado, describimos las diferentes pruebas y medidas realizadas sobre diferentes plataformas de prueba reales configuradas con diferentes estándares IEEE 802.11, canales y condiciones.

3.1.2 Medidas de capacidad en redes WiFi infraestructura

En este apartado, con el objetivo de tener evidencias empíricas de valores reales de capacidad de los canales de comunicaciones en redes WiFi, realizamos una serie de medidas de la tasa de bits promedio o velocidad alcanzable con diferentes dispositivos de última generación. Para ello utilizamos una plataforma de pruebas básica como la mostrada en la Figura 18. Esta configuración consistió en un AP, un terminal portátil (emisor de tráfico de pruebas) y un PC (destinatario del tráfico) conectado a uno de los interfaces *Fast Ethernet* del AP. Con otro terminal portátil actuando como *sniffer* complementario se pretendió detectar la existencia de tráfico de otras comunicaciones.

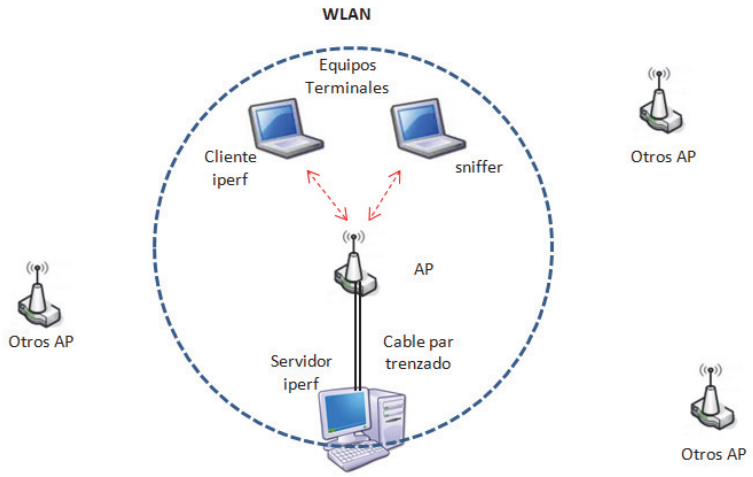


Figura 18. Escenario de experimentación de capacidad WiFi

Las características de los equipos utilizados se relacionan en el Tabla 8.

Tabla 8. Especificación de equipamiento utilizado

Equipo	Características
PC cliente iperf	Ordenador portátil ASUS i7 64 bits 8 Gb RAM. Wireless wlan0 Qualcom b/g/n ath9k MAC. 6C:71:D9:DB:3D:BD, IP: 192.168.1.124 Sistema Operativo Ubuntu 12.04 LTS

Punto de Acceso	ASUS RTAC66U 802.11a/b/g/n/ac MAC: , IP 192.168.1.1
PC Servidor iperf	Ordenador Personal Pentium IV 3 Ghz, S.O. Linux Ubuntu 10.10, Interfaz Fast Ethernet 100 Mbps. MAC. 00:19:66:84:37:A5, IP: 192.168.1.54
PC Sniffer	PC Portátil Asus aspire One Intel Celeron 2 GB RAM, Ubuntu 10.10, Interfaz Linksys/Cisco ra0 mon0 WUSB300N

Los equipos se ubicaron en el interior del despacho 223 de la 2ª planta del pabellón C de los edificios de telecomunicación de la ULPGC, y a una distancia de 20 cm entre el terminal cliente y el AP. Con esta distancia tan pequeña quisimos evitar alteraciones en las medidas debidas a niveles bajos RSSI por atenuación. En el caso de producirse elevadas variaciones, deberían ser motivadas por un aumento del nivel de ruido, existencia de otros tráficos en canales adyacentes debido a los terminales o al propio AP.

La zona de pruebas está formada por despachos y laboratorios a ambos lados y un pasillo central de unos 2.5 m de ancho y 3m de altura. Los AP con SSID ULPGC y TELEMATICA_2 están ubicados cerca del techo, a unos 2,80 m del suelo, mientras que TELEMATICA_1 se encuentra ubicado a la entrada, a unos 2 m del suelo. Nuestro AP de pruebas está ubicado en el interior del despacho 223. En la Figura 19 se muestra de forma aproximada la zona de pruebas y la ubicación de los 4 AP.

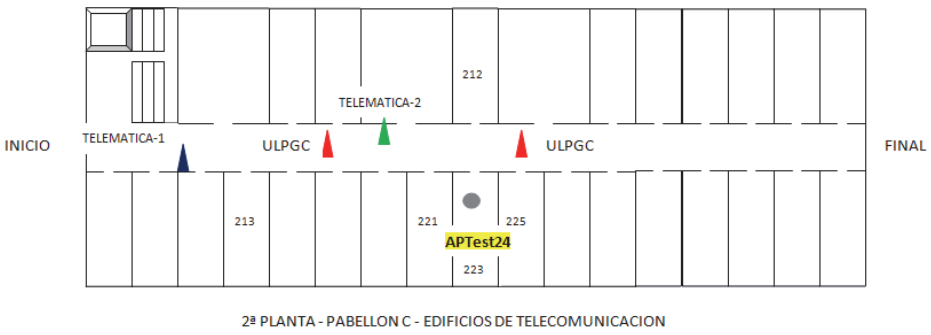


Figura 19. Plano aproximado de zona de pruebas

Para realizar el más riguroso análisis de las medidas realizadas, fue necesario tener conocimiento exacto del estado general del espectro radioeléctrico en la banda de trabajo en la ubicación de pruebas (interior del despacho). Dado que las pruebas las realizamos en la banda de 2.4 GHz tuvimos que detectar canales utilizados por otros

AP. Para ello utilizamos la aplicación *linssider* [121] (versión para el sistema operativo *Linux* de *inssider* para entornos *Windows* de *Microsoft*®). El resultado obtenido ha sido el mostrado en la Figura 20.

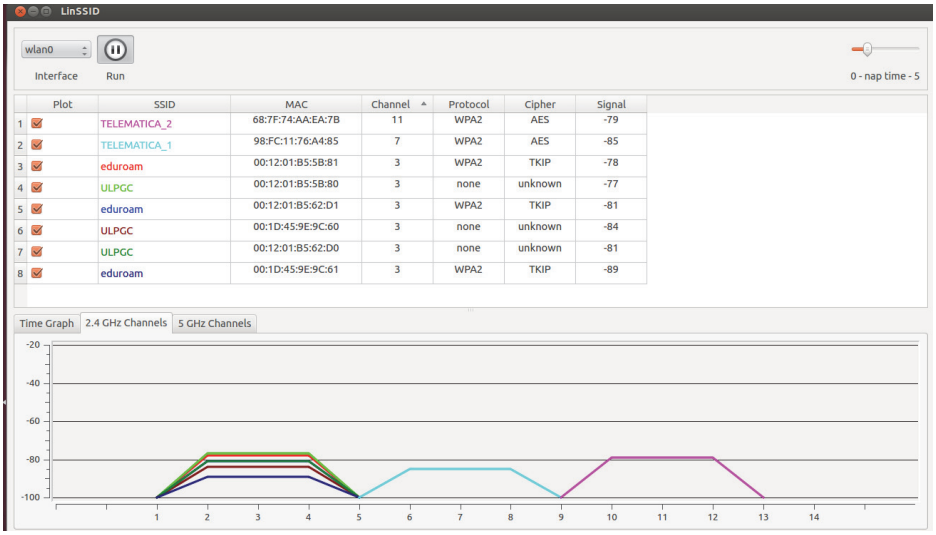


Figura 20. Estado de dispositivos WiFi 2.4GHz detectables desde ubicación

De forma complementaria se hizo uso de las utilidades Linux [122] (*iwlist scan*) para rastrear (hacer *scanning)* los canales WiFi y obtener una mayor información acerca de niveles de señal y características generales de cada AP. De entre todos los datos obtenidos de los diferentes AP detectables mostramos los más importantes en la Tabla 9. Concretamente se muestra el SSID, Canal/Frecuencia y el RSSI (promedio).

Tabla 9. Relación de AP accesibles desde ubicación

AP	Canal	Frecuencia (MHz)	SSID	MAC	RSSI (promedio)
1	3	2422	ULPGC	00:12:01:B5:65:D1	-81
	3	2422	eduroam	00:12:01:B5:62:D0	-81
2	3	2422	ULPGC	00:12:01:B5:5B:80	-78
	3	2422	eduroam	00:12:01:B5:5B:81	-77
3	3	2422	ULPGC	00:1D:45:9E:9C:60	-84
	3	2422	eduroam	00:1D:45:9E:9C:61	-89
4	7	2442	TELEMATICA_1	98:FC:11:76:A4:85	-85
5	11	2462	TELEMATICA_2	68:7F:74:AA:EA:7B	-79

A la vista de los datos mostrados, indicamos que se detectaron 5 AP, 3 de ellos en el canal 3 (frecuencia 2422 MHz), otro en el canal 7 (frecuencia 2442 MHz) y otro en el

canal 11 (frecuencia 2462 MHz). Los tres primeros estaban formando parte de la misma subred lógica ESS con SSID="ULPGC" y operando en abierto (sin restricción ni clave de acceso), y además incorporan cada uno de ellos un AP virtual con SSID="eduroam" con acceso restringido. Los otros AP utilizan diferentes SSID e incorporan el mecanismo de seguridad WPA2. Todos los 5 AP solamente están habilitados para dar conectividad a la red cableada. En la tabla se muestra uno de los valores más comunes de RSSI para indicar la intensidad con la que se detectó cada AP desde la ubicación de las pruebas.

Solo 4 de los 5 AP detectados son accesibles para su uso desde nuestra ubicación. El 5º, numerado con un 3 en la Tabla 9, tiene una aparición esporádica por lo que no permite asociación. Su detección está relacionada con las condiciones radio que permiten captar su señal al rastrear AP accesibles. Este hecho nos evidencia que es habitual que se detecten ciertos AP pero luego no pueden ser utilizables al no contarse con un mínimo nivel de señal y, además mantenido en el tiempo. En la Figura 21 se muestra el pasillo con los AP reseñados.

Figura 21. Pasillo central de zona de pruebas y localización de AP

Las medidas realizadas consistieron en utilizar la herramienta *iperf* [123] para obtener una medida de la velocidad que se puede alcanzar entre el terminal portátil y el PC. Esta herramienta permite emitir desde un cliente un gran número de paquetes hacia un servidor y este los devuelve al cliente. Con ello ambas partes pueden calcular la cantidad de tráfico procesado (bytes y paquetes) y estimar la capacidad (bits por segundo). El cliente *iperf* se instaló en el terminal portátil y el servidor *iperf* en el PC. Si bien las medidas se realizaron entre el terminal inalámbrico y el PC, consideramos despreciable los efectos del segmento de red cableado hasta el PC para analizar los

resultados obtenidos, y consideramos que los mismos están relacionados directamente con la capacidad del canal WiFi, y no tanto afectado por los del segmento cableado.

Para realizar las medidas hicimos uso de 4 AP comerciales de diferentes características. Las mismas medidas fueron realizadas en los estándares disponibles para cada AP utilizado, en diferentes versiones IEEE 802.11b, g, n y ac en todos los canales válidos (1 a 13). Los 4 AP utilizados se relacionan a continuación:

1. Wireless Router Linksys Cisco modelo WRT540GS
2. Wireless Router DLINK modelo DSL-2740B
3. Wireless Router Linksys/Cisco WRT160NL
4. Wireless Router ASUS RT-AC66U

Mediante diferentes scripts (lenguaje de órdenes *Linux*) elaborados para este fin, se ejecuta la aplicación en varias ocasiones y se registraron las medidas. Inicialmente realizamos más de un centenar de medidas para cada caso y, como se esperaba, y así se constata en la literatura existente, se detecta un comportamiento relativamente equivalente en todas ellas. Para hacer los datos más manejables se analizan unas 20 sesiones por cada uno de los 13 canales en los 4 AP, obteniéndose un total de 1040 medidas. En todos los casos los AP no tenían ningún terminal asociado sino solamente el que realizaba las medidas y por tanto no existía tráfico adicional que afectase a los resultados.

En la Tabla 10 se muestra un resumen con los promedios de las velocidades alcanzadas de los tres primeros AP indicados.

Tabla 10. Medidas de velocidad promedio de tres primeros AP de pruebas

Velocidad (Mbps)	AP1		AP2		AP3	
	C1-7	C8-13	C1-7	C8-13	C1-7	C8-13
IEEE 802.11b	≈3Mbps	≈4Mbps	≈4Mbps	≈4.5Mbps	≈4Mbps	≈4.5Mbps
IEEE 802.11g	<12Mbps	<17Mbps	<17Mbps	<20Mbps	<17Mbps	<22Mbps
IEEE 802.11n 20	No	No	<39Mbps	<41Mbps	<39Mbps	<42Mbps
IEEE 802.11n 40	No	No	No	No	<75Mbps	<78Mbps

De entre todos los resultados obtenidos destacamos:

1. Capacidad real de cualquiera de los estándares ronda el 50% de capacidad teórica especificada.
2. El estándar 802.11b presenta unas muy bajas prestaciones para soportar servicios que demanden cierto ancho de banda.
3. La compatibilidad hacia atrás de los estándares puede redundar negativamente en la capacidad total disponible, si algún terminal opera en un estándar o versión anterior.
4. Efecto de reducción de capacidad al existir canales solapados, total o parcialmente con otros AP existentes.
5. Efecto de potencial congestión durante la aparición de tráfico en esos otros AP.

Dada la gran cantidad de información obtenida, solamente detallamos los datos obtenidos para el 4º AP al ser el más recientemente adquirido y cuenta con mejores especificaciones. El resto de medidas están accesibles en el documento disponible en sitio web [124].

Medidas en AP nº 4

Este equipo es el más actual con el que contamos y técnicamente más completo pues incorpora toda la funcionalidad IEEE 802.11n, en 20 MHz y 40 MHz, y además incorpora el estándar IEEE 802.11ac. Por ello es posible usarlo de forma simultánea en la banda 2.4 GHz y 5 GHz. Para interpretar las gráficas hemos configurado su SSID como APTest24. El aspecto externo se muestra en el Figura 22.

Figura 22. AP ASUS RT-AC66U

Las características técnicas de este AP se muestran en la Tabla 11.

Tabla 11. Características AP nº 4 de pruebas

Especificaciones	Caraterísticas
Estándar de red	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE802.11ac, IEEE 802.3u
Velocidad de transferencia:	
IEEE 802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11b	1, 2, 5.5, 11Mbps
IEEE 802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11n	hasta 450Mbps
IEEE 802.11ac	hasta 1300Mbps
Antena Desmontable	3 Antenas
Frecuencia de funcionamiento	2.4G~2.4835GHz /5.1~5.8GHz
Protocolos de Red	IPv4, IPv6

Analisis de estado de banda 2.4 Ghz

Como complemento de estas medidas experimentales, antes de analizar las medidas de capacidad, hemos querido ver el efecto sobre el canal que producen otros AP sobre canales solapados y, de manera especial, el efecto de la ampliación de la canalización a 40 MHz. Con la utilidad *Airview* [125] y su dispositivo hardware asociado (*pendrive*), que es un analizador de espectro 2.4 GHz, pudimos analizar el espectro 2.4 GHz y ver el estado del canal de forma más detallada de forma complementaria a la información obtenida con los analizadores software básicos como *inssider* o *linssider*. El estado del canal antes de activar este dispositivo en la banda de 2.4 GHz era el mostrado en la Figura 23.

Figura 23. Estado inicial de la banda 2.4 GHz detectable por el analizador

Esta utilizad muestra en el eje horizontal la frecuencia en MHz, en la primera gráfica (parte superior) el porcentaje (%) de uso de cada canal, en la gráfica central el nivel de señal (en dBm) mediante una visualización en forma de onda para las muestras de cada canal detectadas y en la gráfica inferior la misma potencia de señal pero en cada instante temporal.

Nótese la existencia de gran cantidad de tráfico en la zona del canal 3 (2.422 GHz) y cercanos (espectro ensanchado) así como de forma más esporádica sobre el canal 7 y el 11. Este tráfico puntual se corresponde prácticamente con los beacons de los AP con SSID: *TELEMATICA_1* y *TELEMATICA_2*, como se puede comprobar en la Figura 20. Además se detectan otros 2 AP sobre el mismo canal 3 (descartamos el tercero). Los datos mostrados se corresponden claramente con el estado real del canal en el momento de la realización de las pruebas, ya que los AP ubicados en los canales 7 y 11 prácticamente no se utilizan de forma habitual. Esto se debe a que requieren autenticación y los potenciales usuarios están muy limitados. Los otros dos están en abierto para uso general de cualquier usuario.

En esta situación, tras arrancar nuestro AP de pruebas con SSID: *APTest24* configurado en el canal 1 y con IEEE 802.11n (20Mhz) obtenemos el resultado mostrado en la Figura 24 con la utilidad *linssider* ejecutada en el ordenador portátil y *Airview* (Figura 25) en otro terminal (para no cargar los equipos de prueba).

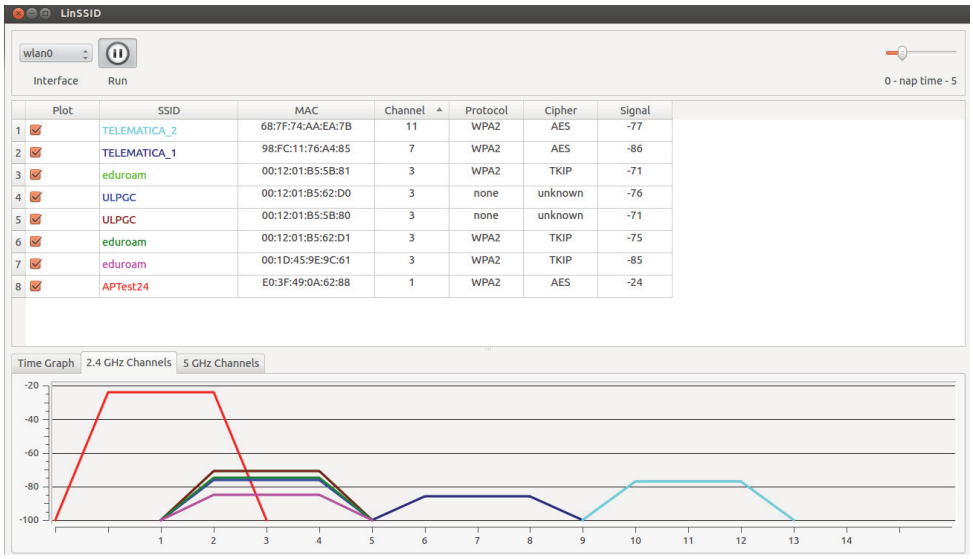


Figura 24. AP detectados. AP de prueba (APTest24) en canal 1

En la Figura 24 se detecta claramente la presencia de nuestro AP (trapecio más alto) con un elevado nivel de señal (≈-25 dBm) frente al resto de dispositivos (< -70 dBm) (menor señal al estar más distantes). Además ya no aparece el tercer AP (SSID: ULPGC) comentado previamente. En esta configuración, y complementando el análisis con la información de la Figura 25, sin iniciar tráfico alguno, vemos que para el analizador se detectan las tramas de este AP en el canal, pero al ser un análisis de nivel físico y en frecuencia no identifica de que AP proceden.

Figura 25. Espectro en 2.4 GHz con APtest24 en canal 1 y IEEE 802.11n (20MHz)

Para detectar el efecto producido por la configuración del mismo AP pero para un uso del doble de canalización, o sea 40 MHz, mostramos el resultado en la Figura 26.

Figura 26. APTest24 en canal 1 en IEEE 802.11n (40Mhz)

Aparentemente no se aprecia ningún cambio. Esto es debido a que el aumento de canalización se produce cuando se genere tráfico entre algún terminal y el AP operando ambos con dicha canalización de 40 MHz. En este caso solo se detectan los *beacons* y él porcentaje de uso de otros AP en canales cercanos. Debemos resaltar el hecho de que hay dos AP ya comentados, y en algún caso un tercero, operando en el canal 3. Esto es contraproducente pues se van a interferir entre ellos por sus ligeros solapes en frecuencia. Este hecho es detectable en nuestro APTest24, pues parte de su banda se solapa con las ocupadas por los anteriores (Figura 24). Las interferencias serán mutuas y ello se debería reflejar en la capacidad de dichos canales.

A continuación cambiamos de canal nuestro APTest24, concretamente al canal 11 solapándolo completamente con otro AP existente en dicho canal (frecuencia 2462 MHz), y mostramos otras situaciones muy interesantes que fueron detectadas en las Figuras 27, 28 y 29, con diferentes configuraciones IEEE 802.11 (*legacy*=bgn), IEEE 802.11n (20) e IEEE 802.11n (40).

Podemos apreciar el tráfico de la zona baja del espectro y en la zona de canales altos donde esta nuestro AP de pruebas (*APTest24*) y el otro AP (*TELEMATICA_2*) (prácticamente inactivo).

Figura 27. IEEE 802.11n en canal 11 modo legacy (compatibilidad bgn)

Figura 28. IEEE 802.11n en canal 11 (20 MHz)

Figura 29. IEEE 802.11n en canal 11 (40 MHz)

A la vista de todos los datos obtenidos, volvemos a resaltar que es muy recomendable ubicar nuestro AP en la zona alta del espectro para obtener mejores prestaciones al estar más libre de interferencias de otros AP. Para hacer estas pruebas finales buscamos una zona menos saturada y lo ubicamos en el canal 9 (Figura 30) evitando centrarlo en el 7 o el 11 al estar usados, pero sabiendo que sus partes superior e inferior del canal están claramente solapadas.

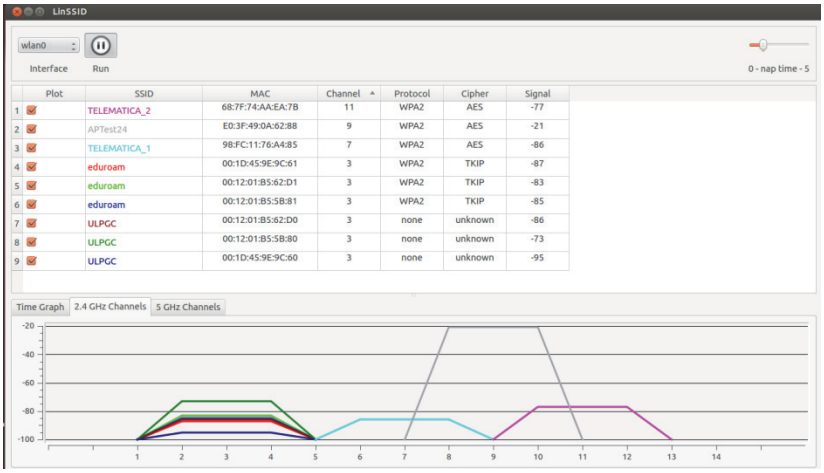


Figura 30. APTest24 en canal 9 en IEEE 802.11n (20/40)

En la Figura 31 se muestra el efecto que produce generar tráfico en el *APTest24* ubicado en el canal 9 y operando en IEEE 802.11n (40 MHz), o sea máximas prestaciones para el estándar.

Figura 31. Resultado de hacer uso intensivo del APTest24 en el canal 9

Observamos que una canalización de 40 MHz hace que se expanda el mismo sobre muchos canales cercanos (6, 7, 8, 9, 10, 11 y 12) y el efecto negativo que produce compartir canales sobre el tráfico existente en esos otros AP y estos últimos sobre el

tráfico propio. Si bien el ampliar la canalización es la solución adoptada por IEEE 802.11n (40) para aumentar el *throughput* y es muy beneficioso para conseguir las altas tasas indicadas, para el resto de AP en esas bandas cercanas no lo es tanto. A continuación comprobamos que la elección de los canales resulta crucial para obtener las máximas prestaciones.

Ubicando el AP de pruebas *APTest24* nuevamente en el canal 11 y tras un tiempo de uso y captura de *beacons* obtuvimos algo similar a lo mostrado en el Figura 32.

Figura 32. Espectro WiFi con zona baja muy utilizada y APTest24 en canal 11.

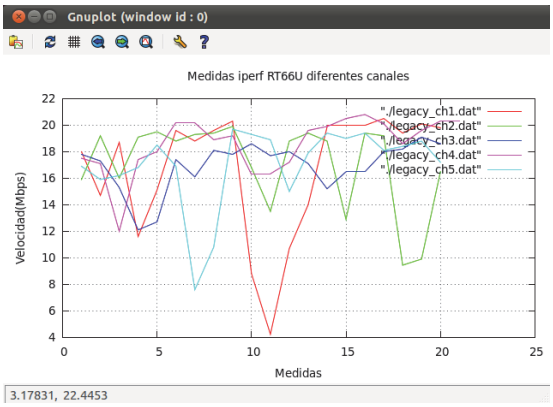
Análisis de velocidad (capacidad)

Una vez analizado el espectro 2.4 GHz, realizamos las medidas de velocidad de este dispositivo para los diferentes estándares.

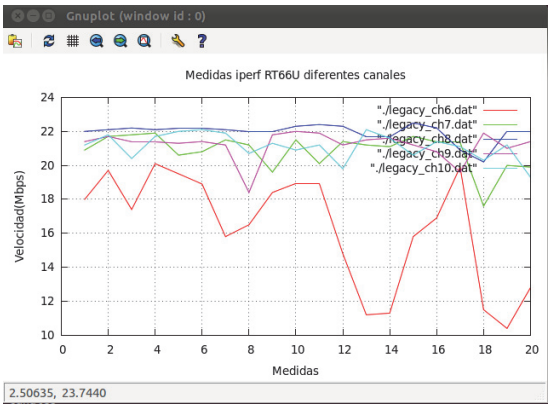
- IEEE 802.11bg: varía entre los 16 Mbps y los 22 Mbps.

Estos resultados para este AP son equivalentes a los de los otros tres equipos para analizados. De forma gráfica se muestran todas las 20 medidas en la Figura 33.a hasta la Figura 33.c. Tenemos que resaltar que la variabilidad de las medidas de la velocidad medida con la utilidad iperf debe relacionarse con las condiciones propias del estado interno de los equipos utilizados salvo que el canal este siendo utilizado. Por este hecho resulta evidente utilizar el promedio de los datos para estimar la capacidad teórica máxima. Debemos resaltar que aquellos valores extremadamente bajos deben ser

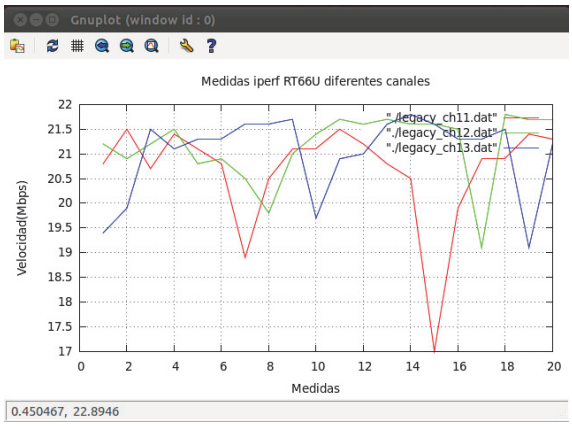
descartados y están claramente vinculados con la aplicación, los recursos utilizados y el uso de canales solapados.



a. Velocidades alcanzadas con iperf en 802.11bg para canales del 1 al 5



b. Velocidades alcanzadas con iperf en 802.11bg para canales del 6 al 10



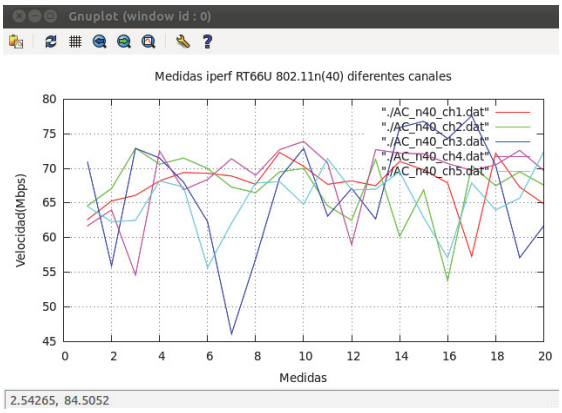
c. Velocidades alcanzadas con iperf en 802.11bg para canales del 11 al 13

Figura 33. Velocidades alcanzadas en los 13 canales para IEEE 802.11bg

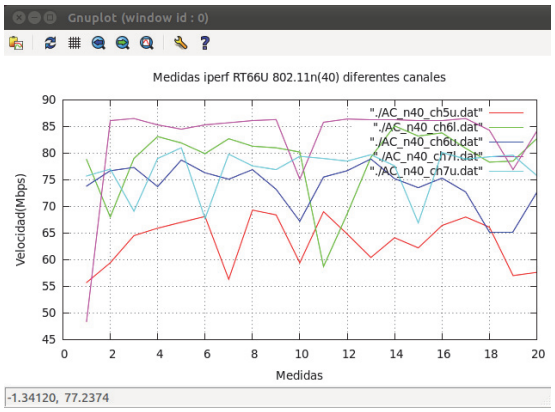
- IEEE 802.11n (20): varía entre los 40 Mbps para canales bajos y los 49 Mbps para canales altos.
- IEEE 802.11n (40): varía entre los 67 Mbps y los 85 Mbps de canales altos de media.

A la vista de los resultados detectamos nuevamente que en los canales altos se obtienen mucho mejores prestaciones que en los bajos, diferencias apreciables y superiores a 18 Mbps.

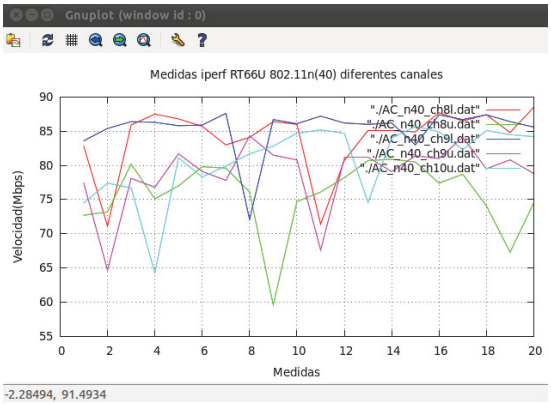
Este último caso de máximas prestaciones para IEEE 802.11n y canalización 40 MHz se muestran en la Figuras 34.a hasta la Figura 34.d.



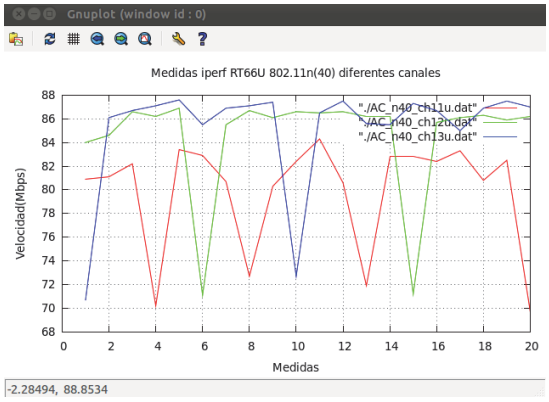
a. Velocidades alcanzadas con iperf en 802.11n(40Mhz) para canales del 1 al 5



b. Velocidades alcanzadas con iperf en 802.11n(40Mhz), canales del 5u al 7u



c. Velocidades alcanzadas con iperf en 802.11n(40Mhz) para canales del 8l al 10u



d. Velocidades alcanzadas con iperf en 802.11n(40Mhz), canales 11u al 13u

Figura 34. Velocidades alcanzadas para IEEE 802.11n (40)

Esta experimentación nos ha servido para contar con valores reales de velocidad o capacidad precisos sobre diferentes dispositivos y conocer las prestaciones de los mismos sobre diferentes situaciones reales. Asimismo se detecta claramente que las prestaciones de los canales WiFi son muy dependientes de la correcta elección de canales usados por los AP y los solapes que se produzcan entre ellos, tanto si son los mismos como cercanos.

En el siguiente apartado procedimos a realizar las pruebas experimentales sobre tráfico multimedia real.

3.1.3 Efectos de restricciones en canal sobre tráfico no elástico

Para evaluar el comportamiento de comunicaciones de audio/video sobre redes WiFi, hemos realizado diferentes pruebas con diferentes contenidos multimedia pregrabados.

Los contenidos de los videos utilizados para facilitar su estudio visualizan un contador descendente, a modo de secuencia de números, en negro con fondo gris desde el 5 al 1 y un sector circular que gira en el sentido de las agujas del reloj. Además incluyen una pista de sonido de un pitido en cada segundo. El mismo video ha sido creado con diferentes calidades (compresiones) y formatos. En la Figura 35 se muestra uno de los primeros y últimos fotogramas.

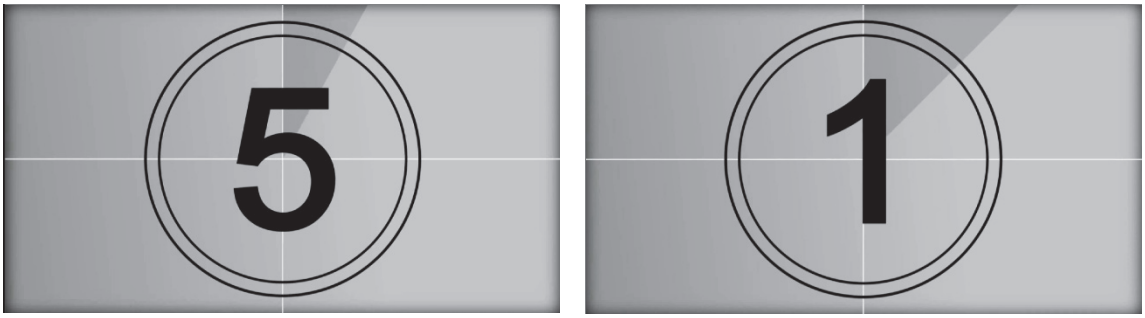


Figura 35. Ejemplo de fotograma inicial y final de archivo de prueba

Las pruebas realizadas consistieron en transmitir el video mediante *Real Time Protocol/User Datagram Protoco*l (RTP/UDP) con la herramienta *VideoLan Client* (*VLC*) [126] desde el ordenador portátil en la red WiFi de pruebas pero forzando restricciones (tasa de bits de salida) en el envío para simular un canal con reducidas prestaciones. La secuencia seguida consistió en ir emitiendo a una máxima tasa de emisión de 1 Mbps e ir ascendiendo progresivamente este valor en las diferentes pruebas. El *streaming* recibido fue procesado en el ordenador personal destino también con VLC conectado a uno de los interfaces *Fast Ethernet* del AP. Para ello hemos utilizado el dispositivo más avanzado disponible, el ASUS 802.11ac RT-AC66U [127] y operando en 802.11n. Los dispositivos utilizados fueron:

- AP: RT-AC66U
- Ordenador Personal Origen: Portátil Asus i7, 8 GB RAM. Asociado a AP (802.11n). S.O. Linux Ubuntu 12.04.
- Ordenador Personal Destino: PC Pentium IV conectado a un interfaz cableado del AP (Fast Ethernet). S.O. Ubuntu 10.10.
- Ordenador Personal Sniffer: Portátil Acer Aspire One 752 C. Herramienta *tcpdump* [128].

Las especificaciones principales del AP se presentaron en el apartado anterior así como el escenario utilizado se muestra en la Figura 18. Las condiciones de contexto en

la banda de trabajo, o sea en 2.4 GHz, ya las presentamos con detalle en el apartado anterior y destacamos una mayor saturación en canales bajos (otros AP existentes), un AP en el canal 7 y otro AP en el canal 11. Para hacer las primeras pruebas ubicamos el AP en el canal 9, teóricamente más libre (solo afectado por estos dos AP). La ubicación física de los equipos de prueba es la misma que en los casos anteriores (Figura 19).

Análisis y medidas de limitación de tráfico y calidad visual

Las diferentes pruebas que realizamos consistieron en transmitir diferentes archivos con diferentes requisitos. Para simular un canal de reducida capacidad, forzamos limitaciones en el kernel para reducir el caudal máximo de salida. Con ello pudimos medir como afecta al número de paquetes transmitidos/recibidos y evaluar la percepción calidad visual del receptor (QoE relativa entre diferentes casos). Concretamente se usaron diferentes colas TBF [96] en la salida del interfaz hacia la red en origen y repetimos el envío en múltiples ocasiones. Para forzar las diferentes situaciones se han utilizado las funciones de control de tráfico disponibles para Linux *tc* [129]. De entre todas las transmisiones, resaltamos las realizadas con uno de los archivos, concretamente *Countdown_with_Sound_mpHD.mpg,* por tener unos requisitos de elevado ancho de banda (bitrate de video 5.617 Kbps). Las características más importantes del mismo son:

- Formato: MPEG-PS. Tamaño: 4,13 Mbytes, bitrate total: 5796 Kbps.
- Video: MPEG Video Versión 1, bitrate: 5.617 Kbps, 1920x1080, 30 fps.
- Audio: MPEG Audio Nivel 2, bitrate: 64 Kbps y fmuestreo: 44.1 KHz.
- Duración: 5 s.

En unas pruebas preliminares se realizaron 5 transmisiones repetidamente para diferentes colas de salida y medimos la cantidad de paquetes transmitidos. El promedio de estos valores están en un rango que va desde los 420 paquetes para 1 Mbps, pasando por 1700 paquetes para 4 Mbps hasta los 2700 paquetes para 10 Mbps. De entre las más de 50 medidas realizadas, la cantidad de paquetes transmitidos más elevada fue de 2833 paquetes para un tiempo de transmisión (medido para cada emisión) de unos 6'03 segundos, que representan un bitrate de:

$$Bitrate = (2833 * 1500 * 8) / 6 = 5666000 \text{ bps} \approx 5'66 \text{ Mbps}$$

El caso peor, para una cola de salida teórica de 1 Mbps, se tiene:

$$Bitrate = (409 * 1500 * 8) / 6 = 818000 \text{ bps} \approx 0'8 \text{ Mbps}$$

Este valor determina la muy baja calidad visual de la información recibida pues solo alcanzan al destino una séptima parte (2833 / 409 ≈ 7) de los paquetes de datos que deberían recibirse. La cantidad efectiva de bytes recibidos se obtendría restando los 12 bytes de la cabecera RTP, 8 bytes de la cabecera UDP, 20 bytes de la cabecera IP y unos 30 de la cabecera 802.11, que representan aproximadamente unos 70 bytes adicionales, con lo que el bitrate real de información útil es ligeramente inferior.

- **Prueba: 100 emisiones del mismo video**

Con el mismo archivo indicado anteriormente, repetimos el proceso pero durante unas 100 sesiones o transmisiones separadas 20 segundos entre cada una de ellas, para tener una mayor cantidad de muestras y poder caracterizar el comportamiento ante las diferentes restricciones aplicadas. Con ello pudimos determinar los efectos frente al caso en el que no haya restricciones, así como el número de paquetes que se transmiten.

- **AP aislado**

Los datos estadísticos obtenidos para las 100 pruebas se pueden resumir en una media de 2795 paquetes, un máximo de 2828 y un mínimo de 2777 paquetes. En la Figura 36 se muestra la distribución de los tamaños de paquetes de forma puntual y en modo histograma.

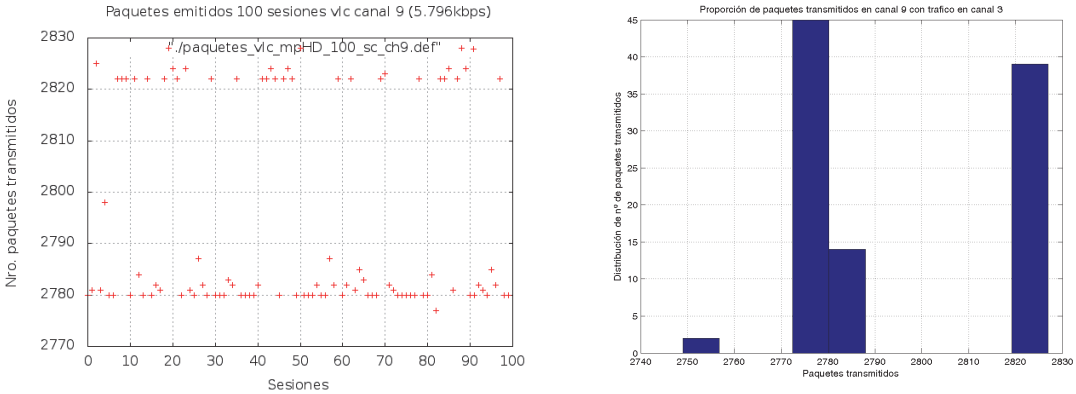


Figura 36. Paquetes transmitidos en 100 sesiones vlc en canal 9

En la Figura 36 se puede observar que prácticamente el número de paquetes transmitidos oscilan entre dos posibles franjas.

- **AP con tráfico interferente**

Para forzar los efectos de canales limitados o congestionados, hemos ubicado el AP en el canal 3 y procedido a ejecutar una aplicación que hace un uso intensivo del canal WiFi. La misma ha sido desarrollada por nosotros en lenguaje C, denominada *PacketInjection* (3.5KB) [130] y se ejecuta en otro ordenador. Al tráfico generado por esta aplicación lo consideramos interferente a efectos de analizar sus efectos sobre los videos emitidos. Con el uso de un tercer equipo portátil operando en el canal 3, insertamos dicho tráfico en modo broadcast después de la sesión 80. Concretamente en las sesiones 82, 86, 92, 95 y 98. Esta aplicación intenta ganar el canal a las máximas posibilidades que ofrece el dispositivo transmisor y por ello reduce la capacidad disponible para nuestro video de prueba. Con ello vamos a analizar que sucede con la calidad del video recibido y los paquetes transmitidos. En la Figura 37 se muestra el número de paquetes transmitidos antes y después de la aparición de este tráfico "interferente".

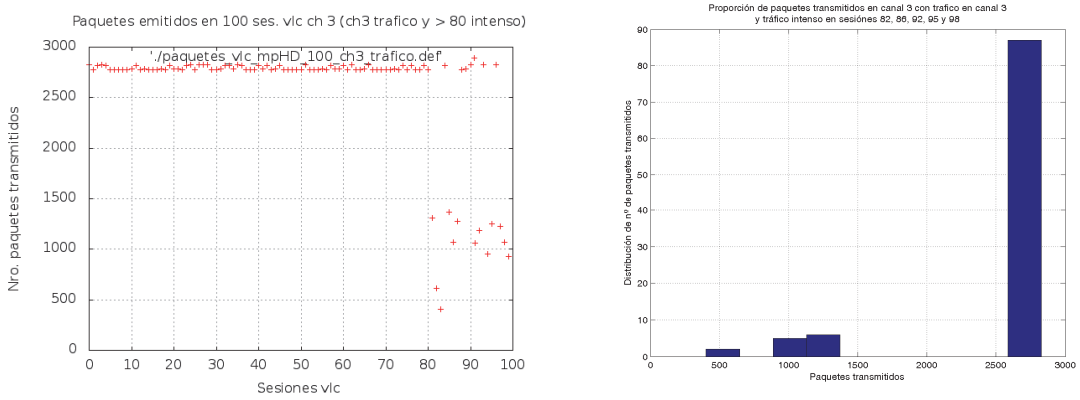


Figura 37. Número de paquetes transmitidos con tráfico interferente en canal 3

Se aprecia claramente la reducción en el número de paquetes transmitidos una vez aparece este tráfico (después de la sesión 80) y eso se materializa en una muy baja QoE en destino e inaceptable reproducción de nuestro video de test.

Para caracterizar el efecto de tráfico interferente sobre la calidad del video reproducido hemos variado el número de sesiones a un valor de 10 e insertamos el tráfico con diferentes bitrates, concretamente en el instante 3 a 1 ms, instante 6 a 10 ms y en el instante 8 a 100 ms. El resultado se muestra en la Figura 38.

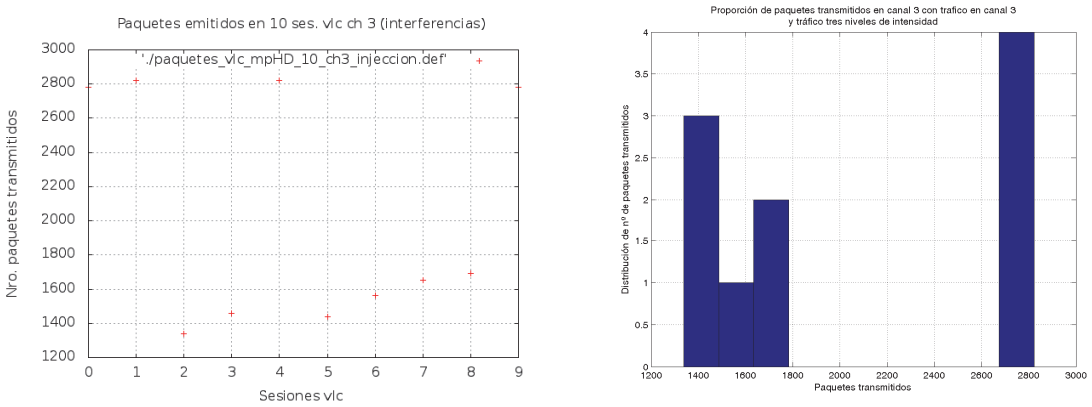


Figura 38. Paquetes transmitidos (interferente 2-3, 5-6 y 7-8) e histograma

Analizando la Figura 38 se detecta que el número de paquetes transmitidos cuando no hay tráfico interferente supera los 2800 paquetes frente al caso afectado por este tráfico que se reduce en torno a los 1400-1600 paquetes.

Análisis y medidas ante variaciones de retrasos entre paquetes

A continuación procedimos a medir el retraso de los paquetes para la transmisión multimedia y analizar su efecto visual, viendo la dependencia directa de la limitación del canal (bitrate, retrasos y pérdidas) con la calidad de la reproducción. Concretamente calculamos la variación del retraso entre cada paquete y su anterior del *stream* durante el envío del mismo. Hemos seleccionado el mismo archivo de video *Countdown_with_Sound_mpHD.mpg* por sus elevados requisitos y ser el mismo utilizado en las secciones anteriores. Para poder representar la posible variación muy elevada de valores, fue necesario truncar a 9999 microsegundos los valores superiores.

- **Efecto de reducido bitrate**

En este apartado hemos procedido a repetir las pruebas anteriores de reducir el bitrate pero capturando tráfico con el *sniffer* y así poder calcular el retraso producido entre cada paquete. En esta primera prueba activamos una cola TBF a la salida del transmisor de 1 Mbps, 3 Mbps, 5 Mbps y 10 Mbps, valores ya utilizados en otras pruebas.

Las pruebas realizadas consistieron en 10 sesiones para cada una de las restricciones impuestas en el canal. Analizamos solamente una de ellas, que por semejanza constatada con el resto, no parece necesario analizarlas todas de forma

individual. Los valores calculados para las diferentes colas en las sesiones analizadas para cada restricción se muestran en la Tabla 12.

Tabla 12. Retrasos entre paquetes para diferentes cola de salida

Bitrate limitado	Nº paquetes transmitidos	Retraso medio entre paquetes (µseg)	Valor máximo de retraso (µseg)	Valor mínimo de retraso (µseg)	Nº de valores superiores a 10 ms
1 Mbps	290	9200	9977	343	247
3 Mbps	1270	3738	9126	88	8
5 Mbps	2024	2189	7691	127	4
10 Mbps	2630	1679	7883	308	6

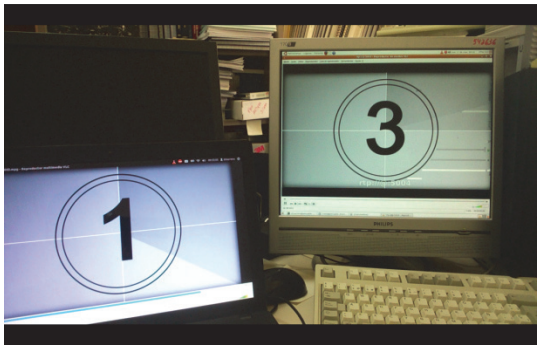
Nótese los casos más representativos para valores bajos de bitrate que producen grandes variaciones en el retraso (jitter elevado). Eso indirectamente provoca, no solo como vimos al principio de este tema baja calidad de la reproducción al no garantizarse el bitrate del *stream*, sino que unos paquetes estén demasiado separados de otros. Esto asimismo provoca que muchos de ellos lleguen demasiado tarde y no puedan ser reproducidos al detectare falta de sincronismo temporal (tiempo de reproducción en cabecera de paquete fuera de secuencia). Nótese también, que en el caso de 1 Mbps se ha producido en 247 ocasiones retrasos próximos a 1000 ms. Esto es enormemente desfavorable y hace imposible la reproducción con unos mínimos de QoE. Los archivos generados con los resultados se denominan: *captura_1M.mp4, captura_3M.mp4, captura_5M.mp4 y captura_10M.mp4* están disponibles en el sitio web [124].

En la Figura 39.a hasta la Figura 39.d mostramos diferentes fotogramas para diferentes casos de la emisión analizada y para los datos indicados en la Tabla 12. En la parte izquierda de cada figura se muestra una imagen capturada en un instante de la transmisión y en el monitor de la derecha la imagen que se recibe en ese instante. Las 4 figuras se corresponden con cada una de las limitaciones: 1 Mbps, 3 Mbps, 5 Mbps y 10 Mbps, respectivamente. Se puede apreciar en todos los casos el retraso motivado por la decodificación, procesado de paquetes y ajuste con la base de tiempos del receptor.

a. Emisión limitada a 1 Mbps

b. Emisión limitada a 3 Mbps

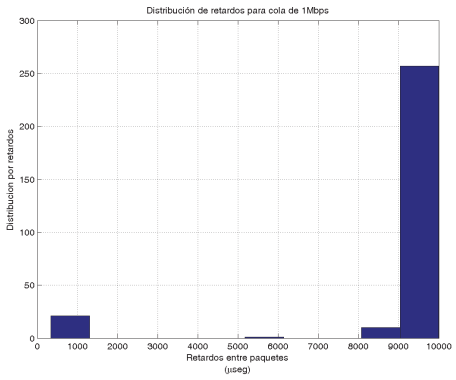
c. Emisión limitada a 5 Mbps



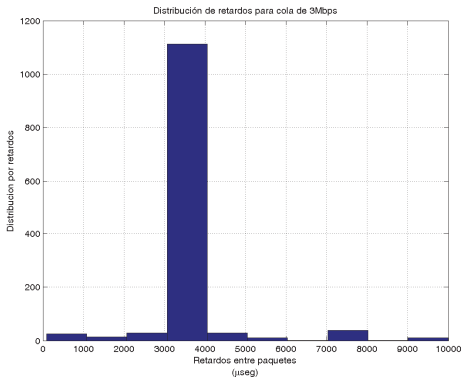
d. Emisión limitada a 10 Mbps

Figura 39. Resultado visual de efectos de bitrate limitado a 1, 3, 5 y 10 Mbps

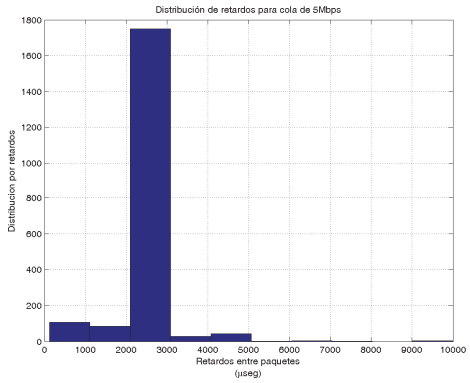
A continuación, mostramos en la Figura 40.a hasta la Figura 40.d los histogramas correspondientes a cada uno de los cuatro casos concretos analizados. Con ello se puede determinar la dispersión de valores en los tamaños de paquetes cuando se utilizan valores bajos de *bitrate* (3 Mbps) frente a una concentración de los mismos para un *bitrate* elevado, necesario para posibilitar el envío del *stream* con mínimas garantías; recordemos que el *bitrate* total del archivo de pruebas ronda los 6 Mbps.



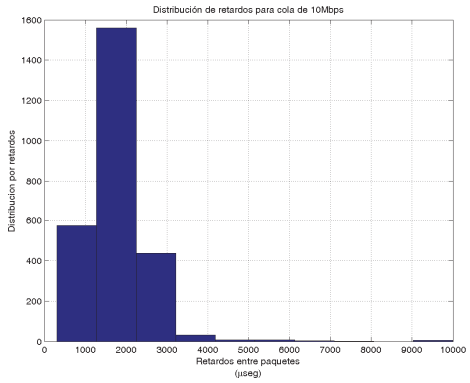
a. Histograma para cola de 1 Mbps



b. Histograma para cola de 3 Mbps



c. Histograma para cola de 5 Mbps



d. Histograma para cola de 10 Mbps

Figura 40. Histogramas de paquetes para cada limitación de salida

Desde un punto de vista de la calidad visual, si analizamos la Figura 39 podemos destacar que en los casos de solo disponer de 3 Mbps e inferiores es completamente inaceptable. Incluso para 5 Mbps, aunque pudiera deducirse el mensaje esto no sería aceptable, en cambio solo en el caso mostrado en 39.d sería óptima la recepción. Nótese que al ser un contador descendente es apreciable el retraso que se produce entre lo que se está visualizando en origen y lo que se está reproduciendo (aproximadamente 2 segundos de diferencia) debido al retraso intrínseco de procesado de conexiones de RTP/UDP y la descodificación. Este análisis es aplicable a cualquiera de las otras sesiones realizadas aunque, evidentemente, los cortes o pixelados son completamente aleatorios y no siguen ningún patrón. Lo que es semejante es la interpretación relativa de sus efectos en la calidad visual para cada caso según las restricciones del canal.

- **Efecto de retrasos forzados**

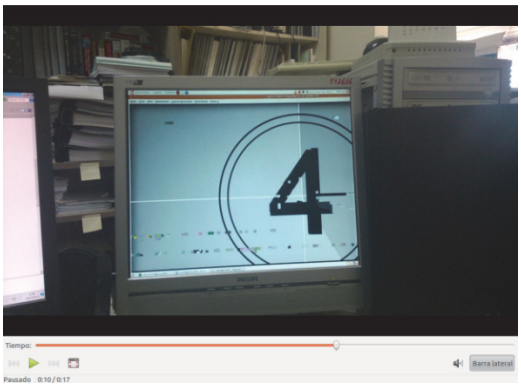
A continuación procedimos a determinar el efecto del retraso de la transmisión multimedia sobre la calidad de la recepción y calcular la variación del retraso entre cada paquete del *stream*. Para ello realizamos el envío del mismo *stream* de video *Countdown_with_Sound_mpHD.mpg* pero activando una cola a la salida del transmisor que fuerce determinados retrasos. Al igual que en el caso anterior hicimos uso de la utilidad *tc* para linux forzando mediante colas el comportamiento de una red con retrasos mediante *netem* [131]. En la Tabla 13 se muestra el resumen de los resultados de paquetes transmitidos y retrasos entre ellos para un retraso forzado en la transmisión (nuevamente hemos obviado mostrar el elevado número de capturas y gráficas para no sobrecargar el documento).

Tabla 13. Retrasos entre paquetes para cola de salida con retraso global

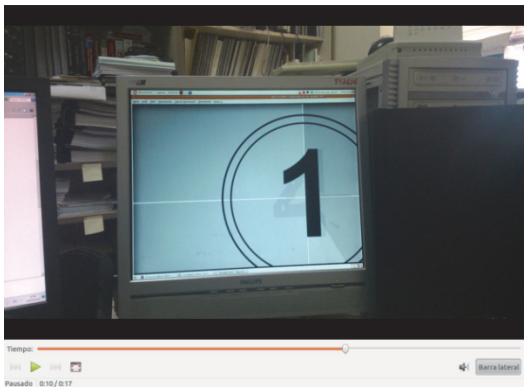
Retraso impuesto	Nº paquetes transmitidos	Retraso medio entre paquetes (µseg.)	Valor máximo de retraso (µseg.)	Valor mínimo de retraso (µseg.)	Nº de valores superiores a 10 ms
200 ms	2772	1623	8160	106	5
400 ms	2779	1694	9782	198	7
600 ms	2767	1645	9356	211	14
1'4 s	2674	1649	9354	120	12
2 s	2222	1627	8478	307	7
4 s	1171	1584	8914	281	8

Para todos los casos inferiores a 2 s la reproducción en el destino pareció perfecta. Sobre los 2s se producen cortes apreciables en la reproducción (archivo: *captura_delay_2s.mp4*) y en el caso de 4s aproximadamente la mitad del video no se reproduce (archivo*: captura_delay_4s.mp4*).

Los resultados obtenidos con el *sniffer* demostraron que el valor del retraso en la transmisión de video no es tan representativo como la reducida capacidad del canal (bitrate). Solo cuando el retraso es bastante elevado (del orden de varios segundos) es cuando se ve afectada la reproducción del video. En la Figura 41.a y Figura 41.b se muestran dos fotogramas extraídos de la reproducción del video con un retraso de 4 s. Para aclarar la misma, indicar que la fotografía de la izquierda fue capturada en el instante t = 10 s y la de la derecha el instante t=10,5 s. En ella se observa un gran salto, en el que no se han reproducido los números 3 y 2 en toda la duración que deberían ser visibles (1 segundo para cada uno de ellos). Esto evidencia que se pierden el resto de paquetes ya sea en origen o que son descartados al llevar un retraso muy grande.



a. Retraso de 4 segundos (t = 10 s)



b. Retraso de 4 segundos (t = 10'5 s)

Figura 41. Fotogramas de efectos de retrasos excesivos

Mediante el análisis de parte de los histogramas (recordamos que no se muestran todos ellos por su elevado número) concluimos que la variabilidad en los retrasos no parece que afecte a video pregrabado de forma apreciable salvo, evidentemente, en el caso de retrasos elevados (del orden de varios segundos).

- **Efecto de perdidas forzadas**

De manera similar a la prueba experimental anterior, procedemos en este apartado a analizar el efecto de las pérdidas de paquetes en la reproducción del video. Para ello hicimos nuevamente uso de una cola en la salida del transmisor configurada para varios porcentajes de pérdidas de paquetes. Estos porcentajes fueron 1%, 2%, 4 % y 10 %. Valores superiores obviamente darán un comportamiento equivalente a una reducida capacidad del canal. Los datos obtenidos y promediados de paquetes transmitidos y retraso de paquetes consecutivos para una proporción de pérdidas forzadas se muestran en la Tabla 14. Como en casos anteriores, se han obviado muchas de las gráficas con los diferentes valores capturados en cada sesión.

Tabla 14. Retrasos entre paquetes para cola de salida con pérdidas forzadas

Perdidas impuestas	Nº paquetes transmitidos	Retraso medio entre paquetes (µseg.)	Valor máximo de retraso (µseg.)	Valor mínimo de retraso (µseg.)	N de valores superiores a 10 ms
1 %	2696	1631	9954	281	7
2 %	2672	1635	9778	294	5
4 %	2703	1628	8905	300	3
10 %	2508	1848	9295	163	8

Haciendo un análisis de estos resultados podemos indicar que para:

- 1%: leves efectos pero con una calidad aceptable (*captura_loss1pc.mp4*)
- 2% : efectos anteriores aumentados pero se mantiene calidad de video y audio (*captura_loss2pc.mp4*)
- 4%: efectos apreciables. Baja calidad pero aceptable (*captura_loss4pc.mp4*)
- 10% : demasiados cortes y mala calidad (*captura_loss10pc.mp4*)

A modo de prueba del resultado visual, en la Figura 42 se muestra un fotograma para el caso de pérdidas del 10% que es el que consideramos que empiezan a ser representativos los efectos en cuanto a pérdidas de paquetes y calidad visual.

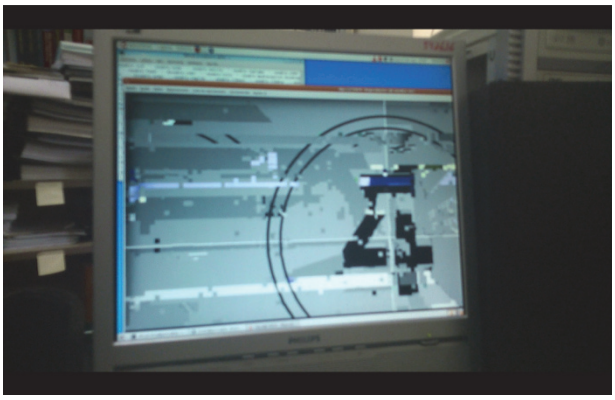


Figura 42. Fotograma de recepción para pérdidas superiores al 10 %.

A la vista de los resultados obtenidos se concluye que solo la pérdida de unos 190 paquetes de un total de casi 2700 recibidos consideramos inaceptable la calidad del *stream* recibido. Por tanto, como era de esperar, para comunicaciones multimedia basadas en video y audio (videoconferencia, *streaming* de video/audio...) son bastante sensibles a reducido *bitrate* o elevadas pérdidas pero no tanto para bajos retrasos de los paquetes, salvo para elevados valores (varios segundos). Esto contrasta con la literatura existente sobre los servicios no elásticos sobre redes WiFi. A pesar de ser bastante evidente, consideramos importante evaluarlos para poder caracterizar o tener medidas reales sobre el comportamiento de este tipo de aplicaciones y que nos permitan afrontar estrategias o actuaciones para paliar estos problemas.

El resultado visual en el receptor para cada una de las transmisiones con diferentes colas y efectos está disponible en [124], como ya se comentó previamente. Con ello se pueden contrastar los datos analíticos y el análisis subjetivo a modo de valoración de QoE.

Por último, presentamos en el siguiente apartado los resultados de una serie de medidas del RSSI o nivel de señal captado por los terminales bajo diferentes contextos, dado su importancia al ser utilizado para diferentes acciones en las redes WiFi.

3.1.4 Análisis sobre aplicación de RSSI para optimizar uso del canal

Ya se ha comentado la importancia de los valores de nivel de señal recibida o el equivalente valor de RSSI en las redes WiFi, y en general, en la mayoría de las redes inalámbricas. De estos valores obtenidos directamente del tráfico de la red (generalmente de la cabecera de los *beacons*) o calculados en los receptores, y de otros

similares como la *SNR*, el LQI [132] ... dependen una gran cantidad de actuaciones. En función del valor que tenga, si está en un determinado rango o alcanza determinados umbrales se realiza alguna acción. Ejemplos de ello son la toma de decisión de realizar un *handoff* o *handover* (cambio de AP), avisar de posibles pérdidas de conexión, detección de límites de cobertura, poder aplicar localización...

En el caso concreto de localización de dispositivos o terminales, es muy importante la fiabilidad del *RSSI* y especialmente en interiores ya que otras tecnologías, más exactas como GPS, no son accesibles.

Lamentablemente el gran hándicap que presenta su utilización es por una parte su variabilidad con la distancia, pues se reduce a medida que nos alejamos de la fuente de transmisión (AP) y, por otra parte la dependencia del dispositivo que capte dicho valor. Teóricamente, según la fórmula de *Friis*, expresada en dB, se define que en el espacio libre el valor que debería obtenerse de recepción de señal está directamente relacionada con la potencia de transmisión descontando las pérdidas.

$$P_{RX} = P_{TX} - L\,(dB) - 10\,\log\frac{d}{d_0} - X_\sigma \tag{3.1.1}$$

Siendo

P_{RX}:	Potencia de recepción
P_{TX}:	Potencia de transmisión
L:	Pérdidas en antenas y enlace
d:	Distancia entre el receptor y el transmisor
d_o:	Distancia de referencia (1 m)
Xσ:	Variable aleatoria gaussiana

Según (3.1.1), ampliamente utilizada de sistemas de transmisión en RF, la potencia de recepción está directamente relacionada con la distancia, ya que a mayor distancia mayor atenuación y menor potencia recibida (potencias en dB restan y en vatios dividen).

En general, el RSSI puede representarse como:

$$RSSI\,(dBm) = 10\,\log\frac{P_{RX}}{P_{REF}} \tag{3.1.2}$$

Siendo P_{REF}= 1 mw.

También podría obtenerse o representarse el valor de señal (S) de la relación señal-ruido, en la forma:

$$SNR = RSSI - Ruido\ (dB) \tag{3.1.3}$$

Siendo *Ruido*, el valor de potencia de ruido detectado por los receptores como el nivel de referencia más bajo para determinar cuándo es posible discernir señal útil de ruido. En el ámbito de WiFi suele representarse el valor de ruido (N, del inglés *Noise*) como -256.

Otra variante de la fórmula de *Friss* aplicada para el conocido balance de potencia es:

$$P_{RX} = P_{TX} + G_{TX}\ (dB) + G_{RX}\ (dB) - L_{TX}\ (dB) - L_{RX}\ (dB) - 20\ \log\frac{\lambda}{4\pi d} \tag{3.1.4}$$

Siendo:

G_{TX}:	Ganancia de antena transmisora
G_{RX}:	Ganancia de antena receptora
L_{TX}:	Pérdidas en adaptadores de antena transmisora
L_{RX}	Pérdidas en adaptadores de antena receptora
λ:	Longitud de onda para la frecuencia de trabajo
d:	Distancia entre antenas

Y siendo $\lambda = c/f$, donde:

c:	$3x10^8$ *mps* (velocidad de transmisión (luz))
f:	Frecuencia de trabajo

Suponiendo que las pérdidas sean nulas (caso ideal) y las ganancias de antenas también nulas, se puede simplificar y quedar:

$$P_{RX} = P_{TX} - 20\ \log\frac{\lambda}{4\pi d} \tag{3.1.5}$$

Que nos permitiría calcular cual sería la potencia de señal recibida. Por otra parte y lo que resulta mucho más problemático, y además está bastante documentado en la literatura existente, es la variabilidad con el tiempo de dichos valores, es decir se producen valores aleatorios incorrelados desde el mismo punto receptor y además en muchas ocasiones dependientes de las características de los equipos receptores.

Este efecto es bastante importante para tomar decisiones y para poder estimar una localización con el mayor grado de exactitud posible. Como ya se comentó, técnicamente la idea consiste en que obtenido el valor de RSSI (nivel de señal) y promediado para evitar desajustes, determinar la ubicación del terminal o conocida la posición del AP calcular que distancia existe entre el terminal y dicho AP. En la Figura

43 se muestra en un plano, que posibles zonas nos podemos encontrar si contamos con un solo AP de referencia. En este caso el nivel de señal que se recibe de dicho AP es la única información disponible para estimar la ubicación del terminal.

En tal caso, teóricamente considerando una superficie plana, diagrama de radiación plano y para antenas omnidireccionales el resultado estimado está más o menos en cualquiera de las zonas internas a la corona circular definida mediante un rango de valores [inferior, superior].

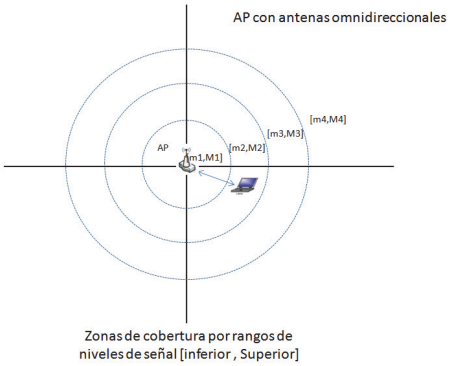


Figura 43. Zonas con niveles de RSSI en rangos prefijados

Esta zona teóricamente nos determinaría la distancia desde el AP (área limitada por dos radios (interior y exterior)), pero no sería posible saber en qué dirección podría encontrarse. Esta zona se muestra en la Figura 44.

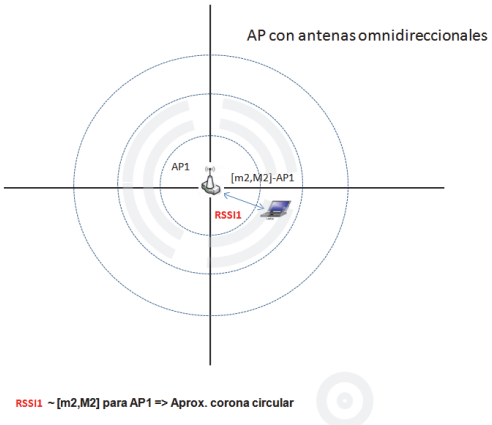


Figura 44. Zona de ubicación (corona circular)

En cambio si se cuenta con otro AP en la zona de cobertura nos encontraríamos en un escenario como el mostrado en la Figura 45. En este caso, se genera aproximadamente una elipse con valores de señal de dos AP debido la intersección de

señales. Con ello se puede obtener una mayor exactitud tomando el rango de valores del AP1 y el correspondiente al AP2. Los valores obtenidos por el terminal deberían ser coincidentes con los valores de ambos rangos en la elipse indicada.

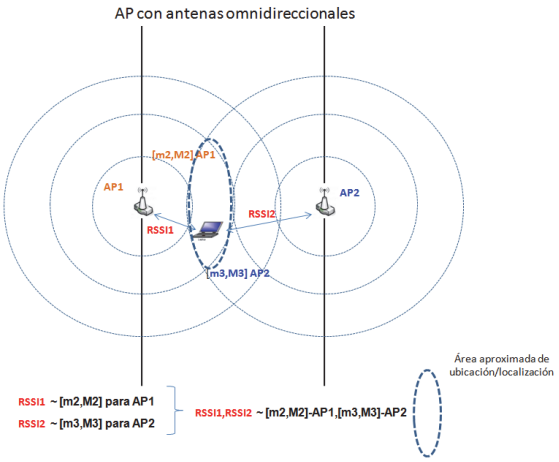


Figura 45. Zona de ubicación (elipse de coberturas solapadas)

En el caso de contar con tres AP en la zona de cobertura y mejor si están ubicados en modo de malla, estaríamos ya en el escenario prácticamente ideal con mayores garantías de localización precisa pues se cuenta con tres referencias. En la Figura 46 mostramos esta situación en la que la intersección de las tres coberturas es un área más limitada. Ahora la ubicación debería ser más precisa que las anteriores. Contar con más AP, y con ello más señales de referencia, podrían mejorarse todavía más la precisión.

El control y reducción de esta variabilidad de los valores con el tiempo no parece que sea un objetivo importante o prioritario en entornos WiFi. En otras tecnologías sí parece que resulta muy relevante minimizar esta variación o aplicar otras medidas diferentes. Técnicamente hablando, parece que es altamente complejo resolver este problema dado que es intrínseco a la tecnología de modulación utilizada, las reflexiones y el *fading*, las frecuencias de operación, pues se ven afectadas por interferencias electromagnéticas y meteorológicas y otros factores.

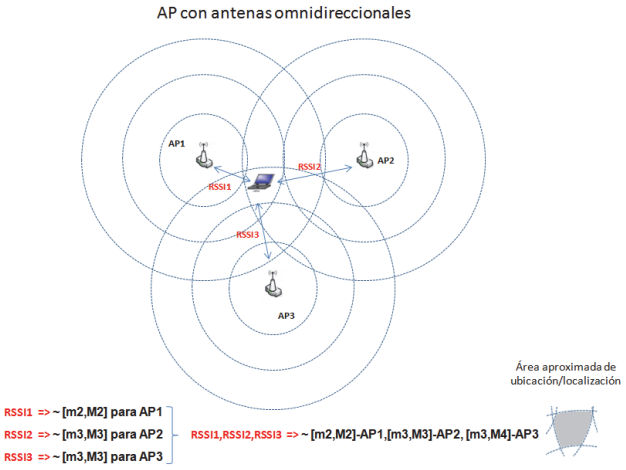


Figura 46. Zona de ubicación (área de intersección)

Las principales iniciativas para mejorar estos efectos se centran en el diseño de antenas más eficientes e inteligentes [133] [134], en las que la direccionalidad de sus diagramas de radiación son configurables y con ello mejoran las prestaciones de las señales recibidas, así como sistemas cognitivos [135] [136] [137] en los que la elección de canales se hace más dependiente de las condiciones del canal para buscar señales más estables en el tiempo.

Análisis experimental

Dado que pretendemos utilizar los valores de RSSI para aplicarlos como método complementario para mejorar las prestaciones de las redes WiFi, hemos considerado muy importante analizar la variación y comportamiento de los niveles de señal recibida y en consecuencia los valores de RSSI tanto en interiores como en exteriores. Para ello hemos escogido la zona del pasillo de las dependencias del Departamento para las medidas en interiores, por ser una zona relativamente saturada con varios AP operando en diferentes canales y por otro lado en una zona en exteriores, libre de interferencias de otros AP o señales en la banda de 2.4 GHz.

La primera de las medidas que realizamos consistió en capturar los *beacons* emitidos por un AP con SSID denominado *APTest* (Modelo *Linksys Cisco*© [138] con sistema *DD-WRT* [139]) ubicado en el despacho 223 (Figura 19). Para ello ubicamos aproximadamente a unos 50 m un ordenador personal portátil detectando un número elevado de sus *beacons*. Concretamente se han podido realizar unas 3300 medidas y extraer de ellos el nivel de señal recibida. Para ver el efecto de utilizar diferentes potencias de transmisión, hemos realizado la misma captura para potencias de

transmisión de 10 mw, 50 mw y 100 mw. Como es sabido, este último valor es el máximo permitido en la legislación española. Para realizar las capturas hacemos uso del portátil con S.O. *Linux Ubuntu* 12.04 LTS [140] y *kernel* 3.13.049 y activamos el dispositivo de red WiFi para que opere en modo monitor. De esta manera permitimos a la utilidad *tcpdump* capturar todos los *beacons* del AP indicado que la NIC es capaz de leer. Los resultados obtenidos de nivel de señal para el caso de 100 mw se muestran en la Figura 47.

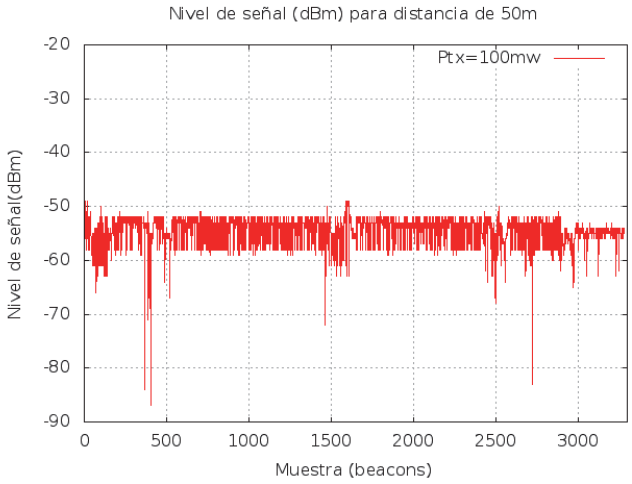


Figura 47. Nivel de señal recibida para una potencia de transmisión de 100mw

En la Tabla 15 se muestran datos estadísticos vinculados a los datos capturados.

Tabla 15. Valores estadísticos para P_{TX} =100 mw

Número de capturas	Mínimo	Media	Máximo	Desviación típica	Nro. >= media	Nro. < media
3281	-87dBm	-54.48 dBm	-49dBm	2.72	2128	1153

En la Figura 48 se muestra el histograma de valores de señal para detectar y analizar la concentración o dispersión de los mismos de forma más precisa.

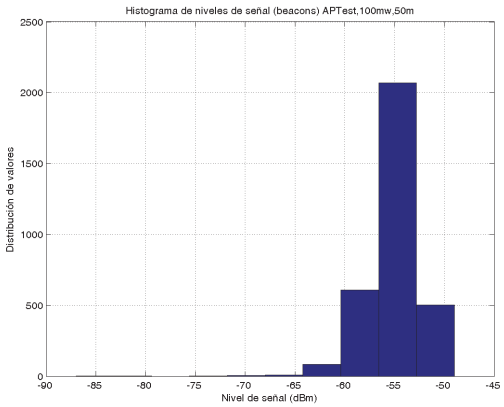


Figura 48. Histograma de valores de señal para 100 mw de P_{TX}

En este caso se observa que los valores de nivel de señal varían aproximadamente desde unos -51 dBm hasta unos -58 dBm en su mayor parte. Es bastante apreciable la elevada variabilidad, e incluso de forma especial ciertos valores excesivamente bajos. Estos valores tan bajos, por ejemplo de -80 dBm o, en general cualquier variación del orden de decenas de dBm puede ser interpretado erróneamente a la hora de hacer una estimación de posición del terminal, o en general para cualquier otra toma de decisión en función de dicho valor pues las variaciones son del orden de unidades. Para intentar resolver este hecho, la solución más ampliamente utilizada es recurrir al promediado de valores consecutivos, técnicas de filtrado o estimación,.. , las cuáles salen fuera de nuestro trabajo.

Para comprobar analíticamente estas medidas, hemos realizado los cálculos correspondientes usando la fórmula de *Friss* simplificada (3.1.5) para una frecuencia de trabajo de 2.400 MHz para las diferentes distancias. En la Tabla 16 mostramos el valor de P_{RX} para una potencia de transmisión de 100 mw (20 dBm). Obviamente estos valores son teóricos e ideales pues hemos despreciado las pérdidas de transmisión y de adaptadores.

Tabla 16. Medidas de aplicación de Friis sin pérdidas para P_{TX}=100 mw

	1m	2m	5m	10m	20m	50m	100m
P_{RX} (dBm)	-20.04	-26.06	-34.02	-40.04	-46-06	-54.02	-60.04

Nótese que para el caso de 50 m la potencia de recepción (P_{RX}) debería ser aproximadamente -54 dBm que coincide aproximadamente con la media de los valores que aparecen mayoritariamente en la Figura 48.

A continuación procedimos a reducir la potencia de señal transmitida a 50 mw y obtuvimos los resultados mostrados en la Figura 49.

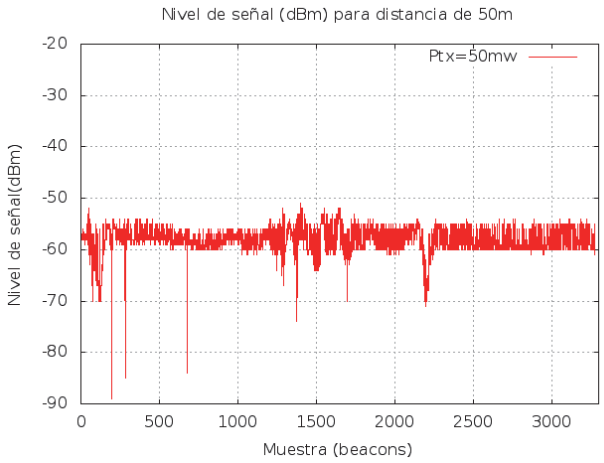


Figura 49. Nivel de señal recibida para una potencia de transmisión de 50 mw

En la Tabla 17 se muestran los valores estadísticos asociados.

Tabla 17. Valores estadísticos para 50 mw

Número de capturas	Mínimo	Media	Máximo	Desviación típica	Nro. >= media	Nro. < media
3278	-89 dBm	-58 dBm	-51dBm	2.6	1776	1502

Como en el caso anterior, mostramos el histograma en la Figura 50.

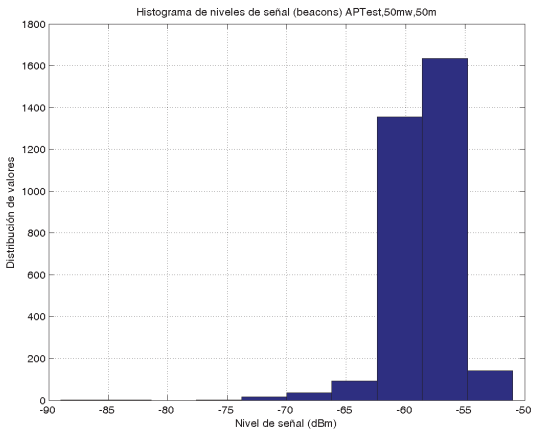


Figura 50. Histograma de valores de señal para 50 mw de P_{TX}

Para esta configuración, la mitad de potencia de transmisión, volvimos a aplicar (3.1.5) y obtuvimos una potencia de recepción teórica de -57.02 dBm. Volvemos a detectar que se aproxima bastante a la media de los datos mostrados en la Figura 49.

En este caso se detecta que se mantiene la variabilidad del nivel de señal recibida aunque hemos empeorado los valores máximos obtenibles, dado que hemos reducido la potencia a la mitad. Además se aprecia que la mayor parte de los valores están en torno a -55 dBm y los mínimos a -60 dBm. Nuevamente se aprecian caídas de niveles de señal excepcionales. Se considera importante resaltar que los valores muy bajos aislados no representan ningún problema dado que son puntuales. Los que realmente son problemáticos son aquellos que muestran tendencia o están muy incorrelados, como por ejemplo los que se ubican sobre las muestras 1400, 1700 y especialmente en torno a la 2200.

Por último hemos repetido el proceso para una potencia de transmisión de 10 mw, valor relativamente bajo si lo comparamos con el máximo permitido, y por ello la potencia recibida es también baja, en consecuencia el alcance es realmente pequeño. El resultado se muestra en la Figura 51.

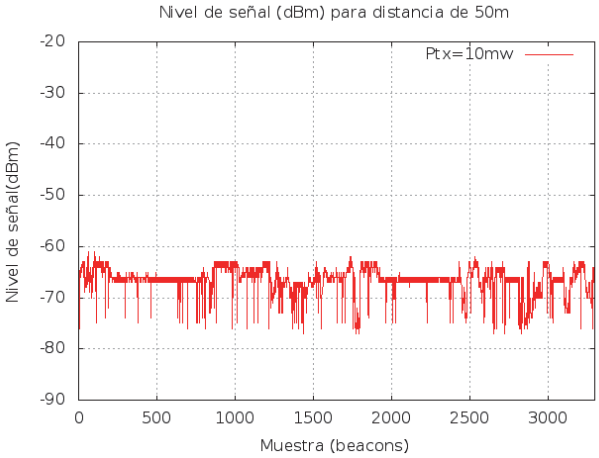


Figura 51. Nivel de señal recibida para una potencia de transmisión de 10 mw

En la Tabla 18 se muestran algunos valores estadísticos.

Tabla 18. Valores estadísticos para 10 mw

Número de capturas	Mínimo	Media	Máximo	Desviación típica	Nro. >= media	Nro. < media
3306	-77dBm	-66 dBm	-61dBm	2.6	1901	1405

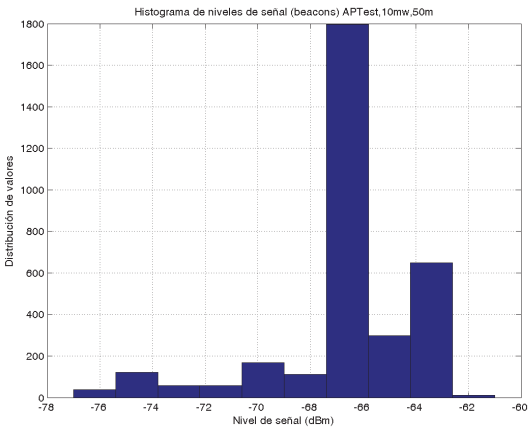


Figura 52. Histograma de valores de señal para 10 mw de P_{TX}

Nuevamente aplicando *Friis* simplificado (sin pérdidas) se obtiene una potencia de recepción de -64.02 dBm. A la vista de los datos incluidos en la Tabla 16 y en la Figura 52 (histograma), en este caso se detecta una gran cantidad de valores bastantes bajos, sobre los -66 dBm, e incluso extremadamente bajos (en torno a -75 dBm).

Si analizamos todos los casos, observamos que en todos ellos existe una gran variabilidad de valores tanto mayor cuanto menor sea la potencia de transmisión dado que la propia atenuación de la señal con la distancia, ubicación tras obstáculos y las condiciones del canal le afecta especialmente.

Por tanto se contrasta una situación evidente y compleja de resolver, que es la aleatoriedad de los valores del nivel de señal recibida (S) o de valores de RSSI. Este comportamiento relacionado directamente con la reducción de potencia de transmisión, vendría a representar el mismo efecto que se produciría si nos alejamos del transmisor y con ella se realizan cambios de ubicación del receptor. Cuanto más cerca se esté del AP, la variabilidad es algo menor y por tanto el uso de RSSI para toma de decisiones para localización y otras actuaciones es más precisa; cosa bien distinta sucede en el caso de distancias elevadas desde el AP, en los que tanto la estimación de desconexión o de localización basada en valores de RSSI es mucho más inexacta.

Para complementar una experimentación, analizamos si el comportamiento en la variabilidad de la señal recibida se mantiene constante en cualquier dirección y es independiente de la ubicación del receptor manteniendo el mismo radio a su alrededor. Es sabido, que el diagrama de radiación de las antenas es también especialmente importante a la hora de saber el grado de direccionalidad de las mismas. Lo más habitual en entornos que desean cubrir grandes zonas, es utilizar antenas

omnidireccionales o sectoriales, en los que supuestamente la señal debe ser prácticamente igual en toda la zona de cobertura. En la Figura 53 mostramos un ejemplo de diagrama de radiación típico en su distribución vertical y horizontal de una antena omnidireccional.

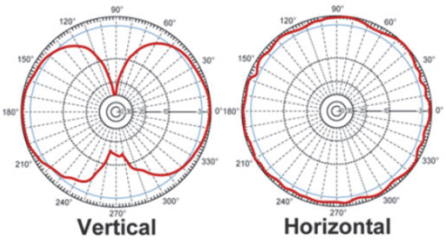


Figura 53. Diagrama de radiación de antena genérica

Medidas en interior

El primer experimento realizado consistió en determinar en qué medida la dirección en que se encuentra el terminal respecto al AP puede ser un factor importante para usar el nivel de señal recibida o de manera especial el RSSI para localización. Se midieron los niveles de señal recibidos en un PC portátil durante 60 segundos a distancias de 1m, 2 m, 5 m, 10 m y 20 m en varias direcciones geográficas (lado izquierdo, lado frontal y lado derecho) en el pasillo utilizado en las anteriores medidas. La ubicación aproximada del AP de pruebas se muestra en la Figura 54. Exactamente a 1,5 m del suelo en la parte izquierda del pasillo en sentido hacia el final del mismo.

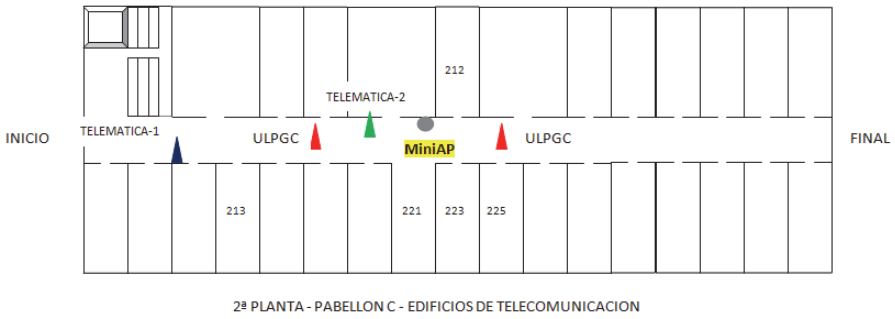


Figura 54. Ubicación de AP de pruebas de direccionalidad

Para facilitar la movilidad de los recursos y su orientación, hemos utilizado un miniAP [141] IEEE 802.11n (Figura 55). El motivo de su utilización fue básicamente por la posibilidad de alimentación por USB, tamaño y bajo consumo, que lo hacen ideal para variar su ubicación, orientación y especialmente su uso en exteriores con

alimentación autónoma. Las pruebas se realizaron configurándolo en el canal 1 (2412 MHz) y una potencia teórica de transmisión de 19 dBm (según especificaciones).

Figura 55. MiniAP Tenda

Antes de proceder a realizar las medidas, como en las pruebas anteriores, hicimos un análisis de campo (*linssider*) del estado de la zona de experimentación donde se ubica este miniAP en lo que respecta al uso de la banda RF que nos ocupa. Dicha información obtenida se muestra en la Figura 56. A la vista de dicha figura, vemos una banda bastante más saturada de señales WiFi. Entre las señales representadas podemos indicar que la primera de ellas, en el canal 1, se corresponde con nuestro miniAP, los 4 AP ya comentados con ubicación conocida y el resto procedentes de otros AP en otras plantas o exteriores del edificio.

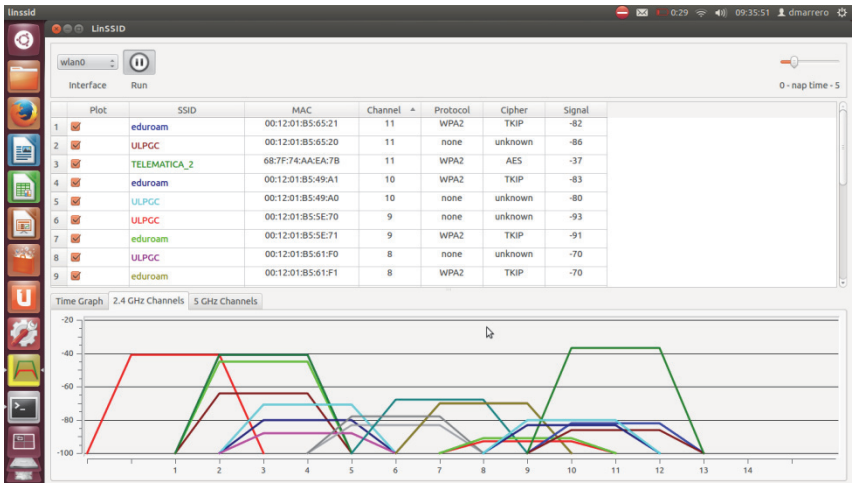


Figura 56. Estado de la banda 2.4 GHz (beacons WiFi) en pasillo

La ubicación del miniAP en justo en el centro del pasillo cerca de la pared sobre un estante. Durante la sesiones de medidas, capturamos el nivel de señal recibido a su alrededor, concretamente a su lado izquierdo (dirección entrada del pasillo) y derecho (dirección fondo del pasillo). En la Figura 57 ilustramos como se realizaron las medidas, pues el ancho del pasillo es 2,5 m y por tanto solo fue posible hacerlo en las

dos direcciones laterales (izquierda hacia la entrada del pasillo y derecha hacia el fondo del pasillo) para valores superiores a 2 m.

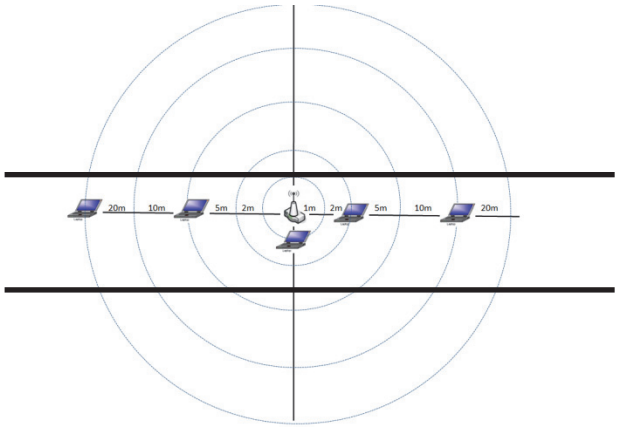


Figura 57. Círculos de distancia de medidas de nivel de señal

En la Figura 58 se muestra el nivel de señal recibido en cada segundo a una distancia de 1 m durante una sesión de 60 segundos.

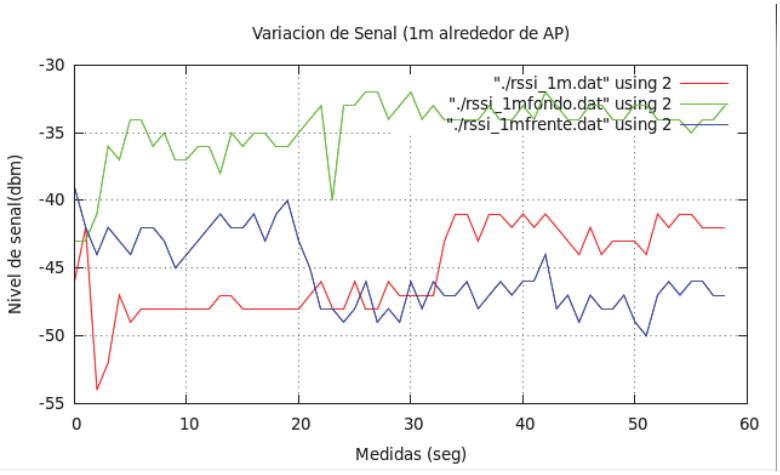


Figura 58. Nivel de señal recibida a 1 m (izquierda, derecha y frente)

Analizando la Figura 58 se aprecia que los niveles de señal fueron superiores para el caso en el que el portátil se encontraba hacia el lado derecho (dirección fondo del pasillo) frente a los otros dos casos.

Repitiendo el proceso pero a 2 m de distancia se obtienen los datos mostrados en la Figura 59.

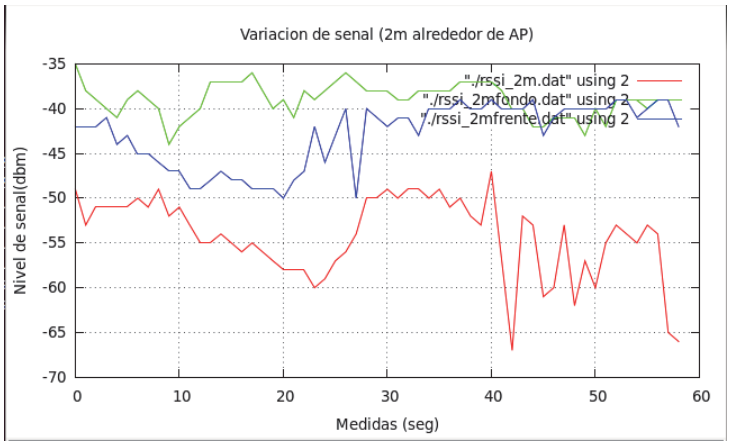


Figura 59. Nivel de señal recibida a 2 m (izquierda, derecha y frente)

Nuevamente detectamos que para la ubicación en el lado derecho (dirección hacia fondo de pasillo) el nivel de señal es algo superior al resto. Igualmente se detecta que en dirección izquierda (entrada del pasillo) los niveles de señal son del orden de unos -20 dBm peores, lo cual puede indicar una falta evidente de omni-direccionalidad de la antena interna del AP ante la inexistencia de obstáculos, o la existencia de un mayor número de AP en las cercanías cuyas reflexiones u otros aspectos afectan a las señales.

Resultados similares se obtuvieron para distancias de 5 m, 10 m y 20 m, pero solo realizados en los laterales del miniAP, los cuales se muestran en las Figuras 60, 61 y 62, respectivamente. Nuevamente se detecta que la señal se recibe mejor en sentido fondo del pasillo que hacia el principio del mismo a la misma distancia.

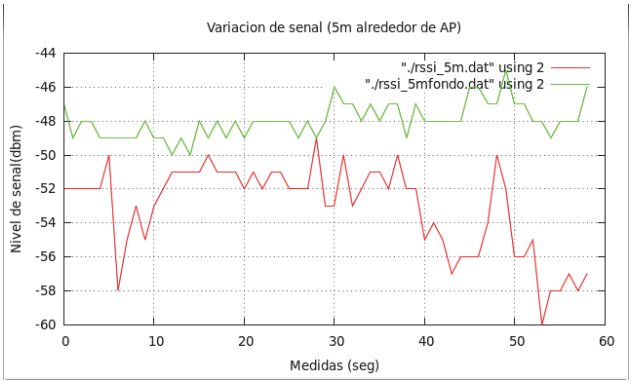


Figura 60. Niveles de señal recibida a 5 m

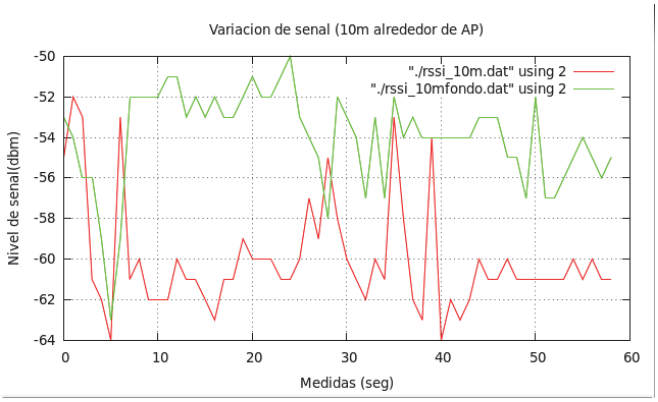


Figura 61. Niveles de señal recibida a 10 m

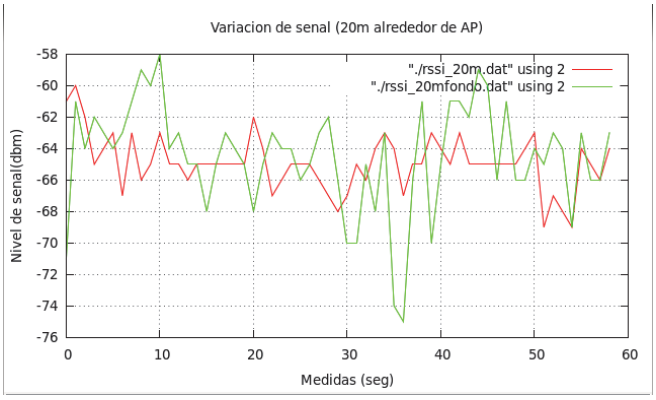


Figura 62. Niveles de señal recibida a 20 m

Especialmente detectamos un hecho interesante y es que a 20 m, los niveles de señal parecen muy similares en un sentido que en el otro pero se aprecia una mayor variabilidad en los que se detectan en la entrada del pasillo frente a los que se detectan hacia el fondo. Si bien no se pueden obtener resultados concluyentes si es evidente la elevada variabilidad de las medidas como en las anteriormente realizadas.

Para eliminar la incertidumbre que representa la existencia de otros AP operando en zonas solapadas y variando sus canales de operación de forma dinámica, hemos procedido a repetir las medidas en espacio libre (exteriores) sin ningún otro AP que pudiera afectar.

Medidas en exterior

Las medidas que realizamos en exteriores con el mismo miniAP y las mismas distancias se representan en la Figura 63, concretamente a 1 m, 2 m, 5 m, 10 m y 20 m en las cuatro orientaciones.

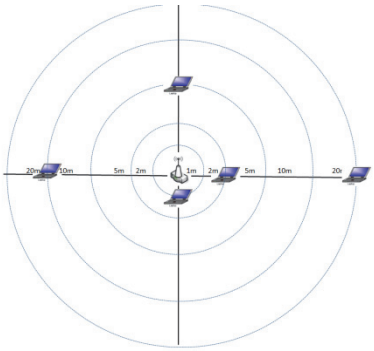


Figura 63. Círculos de distancia de medidas de nivel de señal

En el caso de exteriores, hemos analizado previamente la no existencia de otras señales WiFi y corroborado que no hay presencia de otras que pudieran afectar y que pudieran llevar a una interpretación errónea de los resultados.

La imagen real de la zona a estudiar con el miniAP se muestra en la Figura 64.

Figura 64. Imagen real de zona en exterior libre de WiFi

En la Figura 65 mostramos la comparativa del nivel de señal recibida a 1 m de distancia en las 4 direcciones.

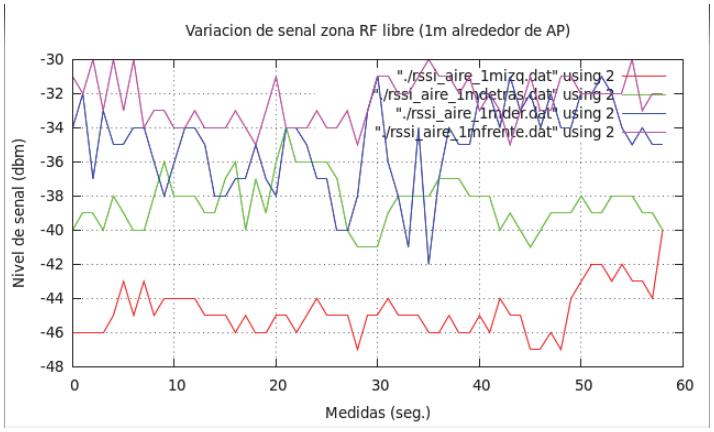


Figura 65. Niveles de señal en las 4 direcciones a 1 m de distancia

Analizando Figura 65 se observa nuevamente que las peores condiciones de señal se presentan en la parte izquierda y, coinciden con los resultados obtenidos en interior, por lo que se puede concluir que el diagrama de radiación es bastante irregular, especialmente en su parte izquierda (visto desde su frontal (posición del *led*)). Igualmente presenta unos resultados inferiores en la parte trasera, siendo prácticamente iguales la parte frontal y derecha. Evidentemente estamos suponiendo que los efectos de las diferentes superficies de alrededor al miniAP no son representativos.

Repitiendo el proceso pero a 2 m de distancia se obtienen los valores mostrados en la Figura 66.

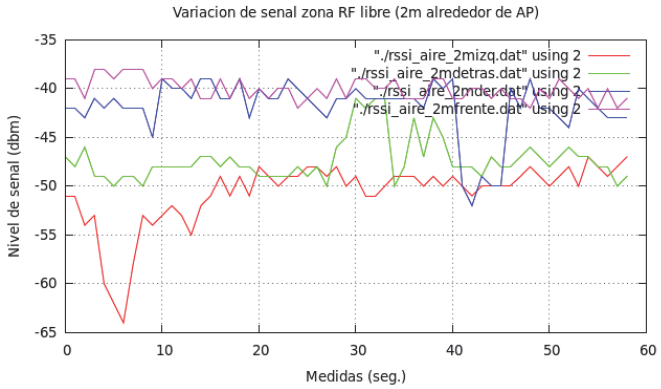


Figura 66. Niveles de señal en las 4 direcciones a 2 m de distancia

Como se puede apreciar los resultados mantienen la distribución del caso anterior. En la Figura 67 mostramos los valores para 5 m de distancia.

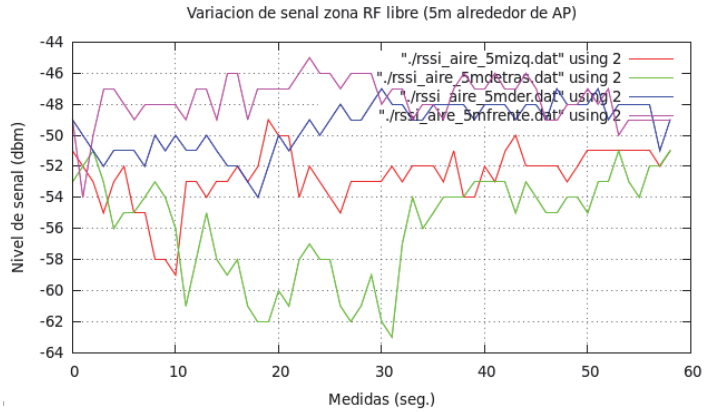


Figura 67. Niveles de señal en las 4 direcciones a 5 m de distancia

En el caso de ubicarnos a 5 m del miniAP, se aprecia un leve cambio de tendencia pues aparece que las peores condiciones se presentan en la parte trasera. El resto de zonas se mantienen sobre un rango muy equivalente, rondando entre -46 dBm y -54 dBm.

Lo que sigue manteniéndose en todos los casos es la aleatoriedad de los valores, lo que permite contrastar y corroborar que este comportamiento no depende de manera predominante de la existencia de otros AP operando en el mismo canal o adyacentes, sino de la propia tecnología de transmisión y de la orografía (obstáculos, objetos, materiales...). Evidentemente el tipo de antena que incluye este miniAP no parece contar con los mejores diagramas de radiación al ser interior al mismo.

Los dos últimos casos, 10 m y 20 m se muestran en la Figura 68 y 69, respectivamente. No se muestran los datos de la parte frontal y trasera para 20 m, dado que el lugar utilizado no permitía ubicarse el receptor a dichas distancias.

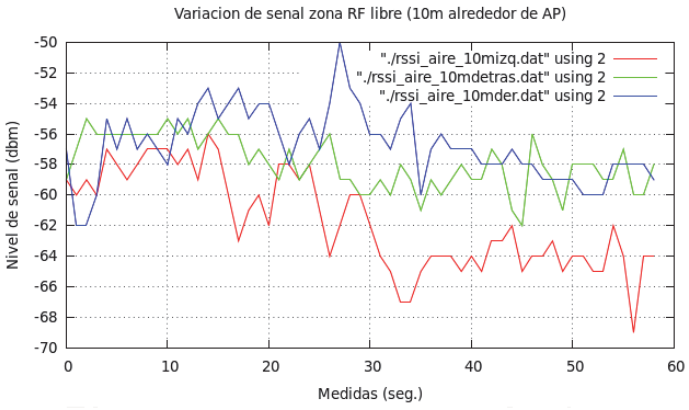


Figura 68. Niveles de señal en varias direcciones a 10 m de distancia

Analizando el caso de 10 m aparece nuevamente un cierto cambio de tendencia y la señal del lado izquierdo parece que en cierto momento presenta peores valores aunque no es constante en todas las medidas, por lo que no se puede de forma tajante ser concluyente. Resultado similar, aunque menos apreciable, se puede ver en la Figura 69 para 20 m.

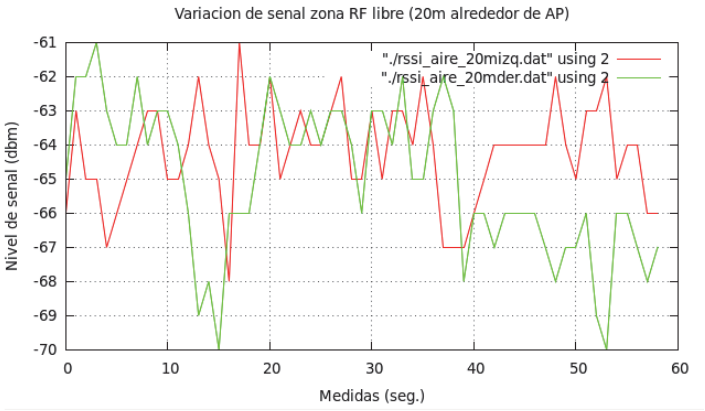


Figura 69. Niveles de señal en varias direcciones a 20 m de distancia

Como conclusión final podemos indicar lo siguiente:

1. Existencia de una elevada variabilidad de señal en todas las distancias y orientaciones del terminal receptor frente al AP transmisor.

2. Comportamiento en interiores saturados de señales RF en 2.4 GHz similar a situaciones en exteriores en cuanto a valores de nivel de señal recibida o *RSSI*.

3. Distribución de valores de *RSSI* irregular según orientación, orografía, obstáculos y distancia.

Por todo lo anterior, consideramos que se tienen limitadas posibilidades de uso de *RSSI* para toma de decisiones ante su elevada variabilidad y aleatoriedad (medidas poco correladas) como plantean [52] [53]. Por ello, sistemas de localización basados en los valores de RSSI pueden resultar poco precisos. Esto es especialmente sensible cuando se cuenta con pocos AP y por tanto pocos valores de referencia. Para mejorar estos datos, soluciones propietario recurren a otros dispositivos complementarios (tags, sensores,…). En el caso de usar varios AP, cuanto mayor sea el número de ellos, mejores posibilidades se tiene para realizar triangulación (tiempo, ángulo o distancia) y estimar la ubicación del terminal lo más exacta posible. Igual problema presentan las técnicas basadas en mapa o patrón (*fingerprint*) y comparación, que pueden tener un alto grado de inexactitud en la estimación de la posición si no se cuenta con referencias estables en el tiempo y en el espacio (distancia).

3.2 Formalización de parámetros de contexto

De entre los objetivos que han motivado el desarrollo de los estándares IEEE 802.11 que consideramos más relevantes destacamos:

1º Maximizar la velocidad o *throughput*, como lo demuestra las diferentes tecnologías estándar desarrolladas (IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac). En todas ellas la principal característica que aportan es el aumento de velocidad.

2º Maximizar capacidad mediante nuevos diseños de antenas (antenas inteligentes para orientar las señales). El ejemplo más representativo de nuevas técnicas dirigidas a aumentar la capacidad de la red es el uso de MIMO que permite el uso de múltiples *streams* de tráfico, redes *mesh* con puntos de acceso actuando como nodos intermedios o en modo *relays*...

3º Maximizar disponibilidad (picoceldas). Esto se refleja en que los puntos de acceso cubren menores zonas pero con mayor número de ellos ("always on").

Si bien todas estas nuevas características o posibilidades determinan una más que evidente mejoría en sus prestaciones, no existen excesivas restricciones ni limitaciones a la hora de realizar despliegues de las redes ni en el uso de las mismas. Más bien solo se hacen simples recomendaciones sobre su planificación para limitar interferencias entre canales (solapados o adyacentes), elección de zonas de cobertura (tipo de antena), evitar las interferencias de otros aparatos eléctricos, evitar obstáculos o zonas ocultas… para mejorar los tres objetivos anteriores.

Dado que todas las redes mantienen un acceso a un canal compartido, seguirán existiendo problemas de saturación por el creciente número de servicios que hacen un mayor uso de ellas. Por tanto, situación de interferencias o congestión no son fácilmente resolubles. Como ya se comentó previamente, el objetivo de esta tesis es proponer soluciones que ayuden a mejorar la capacidad o la disponibilidad de recursos en las redes WiFi. Esto se debería materializar en una mejora de las prestaciones o requisitos de las comunicaciones, especialmente en las dependientes del tiempo. Podríamos decir que es un desafío complejo, dada la gran cantidad de variables que afectan a la calidad de las comunicaciones inalámbricas. Recordemos la vulnerabilidad del medio a aspectos meteorológicos, radioeléctricos y en muchos casos a la sobrecarga de servicios o

usuarios. En cualquier caso nos planteamos proponer ideas de mejora partiendo del conocimiento general de la red y el estado de la misma para adecuarnos, en cierta medida, a las condiciones de contexto.

Los problemas anteriormente mencionados con los que nos podemos encontrar en las redes WiFi están relacionados con diferentes elementos o partes de las mismas (medio radioeléctrico, recursos hardware o software y servicios/usuarios), ubicados algunos de ellos como entidades de diferentes capas de la arquitectura de la red. Dada la gran cantidad de variables que afectan directa o indirectamente a la calidad de las comunicaciones, no parece que exista una solución integral que abarque todos los componentes de la red. Por ello la mayor parte de las aportaciones o iniciativas que existen en la literatura se dirigen de forma focalizada a alguna de ellas, por ejemplo proponiendo nuevas técnicas de modulación o combinación de las existentes, incorporar técnicas de multiplexación temporal o espacial inexistentes en WiFi pero si en otras tecnologías de redes celulares, nuevos aspectos de control de acceso al medio, nuevos protocolos de transporte adaptados a las condiciones del nuevo medio RF o dependientes de los requisitos de las aplicaciones no elásticas, mejorar aspectos de codecs, nuevos algoritmos de compresión...

Nosotros hemos considerado el problema mediante un modelo contextual basado en el conocimiento general de diferentes parámetros. En este modelo consideramos el contexto de la red como un conjunto de parámetros funcionales, medibles y otros no funcionales. Con el análisis y optimización de los mismos podemos contar con mejores resultados en cuanto a la QoS de ciertas aplicaciones.

Para definir nuestro modelo contextual representamos en la Figura 70 las diferentes partes o módulos que confirman una red WiFi. En la misma se muestran los componentes de los terminales inalámbricos y las de los AP. Estos parámetros pueden estar relacionados con uno o varios de los 7 bloques: los servicios, procesos de aplicación utilizados, usuarios, capas de la arquitectura, sistema operativo, dispositivos de red y el canal inalámbrico.

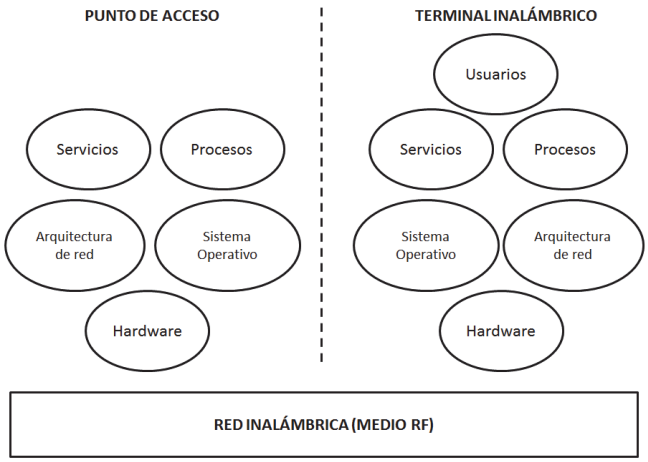


Figura 70. Esquema modular de partes que forman una red WiFi

En esta primera aproximación, detectamos que en la red intervienen de manera principal los usuarios pues son ellos los que activan los servicios de comunicación. Estos están solo presentes en los terminales inalámbricos. Además ya indicamos que su opinión o valoración subjetiva es, en muchos casos, indispensable para valorar la calidad de una comunicación conversacional (QoE, MOS…).

El resto de bloques están presentes en los dos dispositivos. Por tanto las variables o parámetros que consideramos objetivo de posible estudio son similares para los dos sistemas. Esto se debe a que la funcionalidad de un AP no es la misma que la de un terminal. Los terminales son originarios o destinarios de la comunicación y los AP son dispositivos de interconexión entre terminales o con la red cableada. Baste indicar que las colas existentes en los AP se pueden ver afectadas por diferentes conversaciones de diferentes terminales y usuarios, mientras que en cada terminal solo se ve afectada por tráfico saliente o entrante a dicho terminal.

En cuanto a que parámetros utilizar o definir, dónde se aplican y especialmente cómo afectan a las comunicaciones o cómo se ven afectados por las mismas es un punto importante en este modelo. Por ejemplo el aspecto que podríamos considerar más importante es el parámetro *throughput* de la red, especial medida de QoS. Este parámetro puede verse globalmente desde la aplicación que genera la comunicación hasta en el medio inalámbrico. De igual importancia son el retraso, el jitter (variaciones del retraso), la latencia, la tasa de pérdidas... En medio nos encontramos con protocolos y el tratamiento de unidades de datos. Asimismo nos encontramos con diferentes formas de acceso al medio, mecanismos de control de congestión o gestión de tráfico que redundan en la valoración objetiva de QoS. Y por último nos podríamos encontrar con

otras situaciones no siempre medibles como pérdida de cobertura, inadecuada elección de AP, saturación de canal por múltiples servicios simultáneos... que podríamos considerar parámetros funcionales o no funcionales, según cada caso.

Nuestra propuesta, por tanto, parte de definir los parámetros que consideramos importantes, analizar su estado y aplicar mecanismos correctores, de forma que alguno o varios de ellos puedan ser maximizados o minimizados, buscando un cierto grado de optimización de los mismos. Es decir, conjugar el conocimiento del estado de la red para modificar o adaptarse en la línea de mejorar la valoración de los servicios.

Basándonos en la Figura 70, se muestra en la Figura 71 algunas interacciones entre los diferentes módulos o bloques y puntos de interés que afectan globalmente al funcionamiento de las redes WiFi. Distinguimos las acciones del usuario y el proceso de la aplicación (interfaz de usuario) para acceder a un servicio determinado (ejemplos de procesos de aplicación son browsers, *vlc*, *skype*...). En la parte de la izquierda mostramos la necesidad de contar con hardware especial para comunicaciones conversacionales y la codificación/compresión de estas señales (audio/video). Además hemos incluido en la parte central el resto de servicios elásticos, que por su no dependencia del tiempo tendrían menor prioridad. Ya comentamos que sus requisitos no son especiales y por tanto pueden ser tratados de forma diferente.

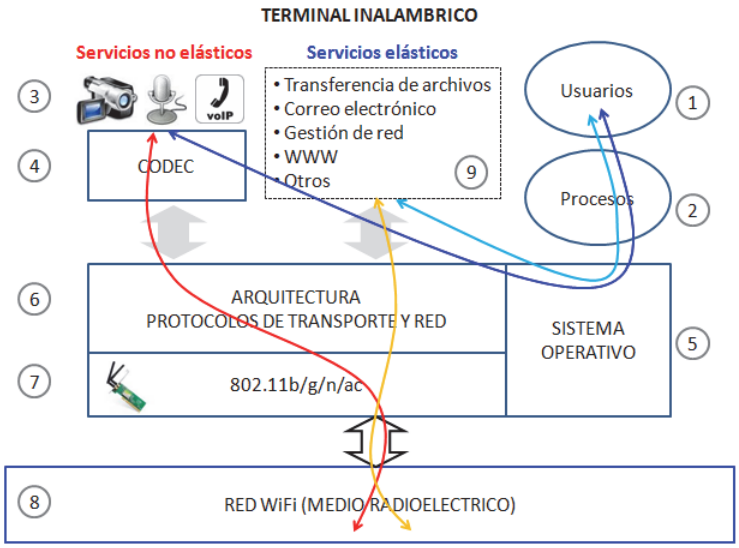


Figura 71. Esquema de elementos intervinientes en un terminal WiFi

Los parámetros vinculados con el tratamiento de las señales de audio y video, marcados con ③ y ④, así como los procesos y sistemas operativos que soportan al sistema, ② y ⑤ no han sido considerados. Si analizamos parámetros vinculados con los

elementos ① (número de usuarios, servicios generados y características o requisitos), ⑥ variables de control de conexionado de transporte y de red, ⑦ aspectos de control de acceso al medio, priorización de tráficos y encolado, ⑧ estado del medio incluyendo tráficos existentes y número de AP disponibles y, por último⑨, como actuar con el resto de tipos de tráfico.

En la Figura 72 se indican los elementos principales, de forma más concreta, que forman la red, agrupando terminales y sus características frente a AP y sus características.

3.2.1 Parámetros y relaciones

Para plantear una descripción de parámetros o condiciones de contexto de una red WiFi tenemos que partir de aquellas características elementales o variables que determinan en gran medida su funcionamiento.

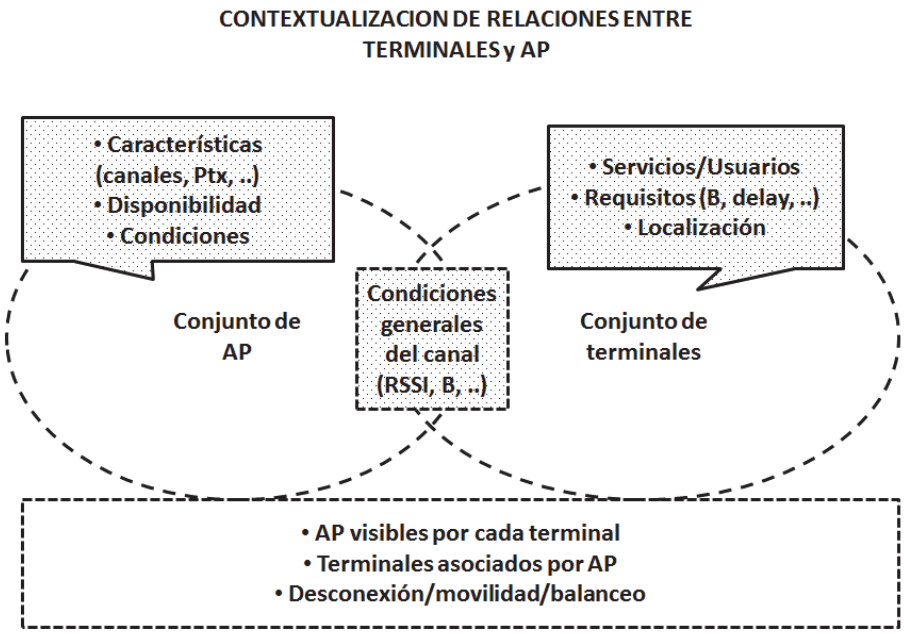


Figura 72. Elementos que forman la red WiFi y posibles relaciones

En la Tabla 19 se enumeran las principales características de los AP y de los terminales que pueden ser configurables. No incluimos aspectos de cifrado, autenticación como 802.1x (*RADIUS*), cuentas de acceso, gestión de direcciones IP, servidores DHCP o DNS, filtrado... pues salen fuera de nuestro ámbito.

Tabla 19. Parámetros medibles en los AP y terminales

Dispositivo	**Parámetro**
Punto de Acceso	SSID (redes lógicas)
	Tecnología 802.11 a, b, g, n, ac
	Canalización (20 MHz, 40 MHz, 80 MHz, otras)
	Velocidades disponibles 1, 2, 5,5, 11, 32, 46, 54 Mbps... automática o fija
	Potencia de transmisión
	Frecuencia de operación/Canal
	Tamaño de preámbulo (*long-short*)
	Intervalo de *beacon*
	Umbral RTS/CTS
	Umbral de fragmentación
	Modo gestión de consumo
	Intervalo de DTIM
Terminal WiFi	Tecnología 802.11 a, b, g, n, ac, otras.
	Velocidades disponibles 1, 2, 5,5, 11, 32, 46, 54 Mbps... automática o fija
	Nivel de señal recibida (RSSI) de cada AP
	Sensibilidad del receptor

De entre los anteriores, le prestamos atención especial a: la potencia de transmisión de los AP pues determina la cobertura, la frecuencia y canalización pues pueden generar solapes de canales entre los AP, la tecnología/canalización pues determina en gran medida la capacidad teórica de cada AP y en el caso de terminales: los valores de RSSI detectados de cada AP (coberturas y control de desconexión), y su relación con la sensibilidad y tecnología/velocidad. De forma conjunta los servicios o tráficos generados por los terminales son las principales características que determinan la posibilidad de uso y definen en gran medida el contexto.

Antes de proceder a formalizar los parámetros, indicar que se usa la notación *TER* y un subíndice para referenciar a cada terminal WiFi y *AP* y un subíndice para indicar un determinado AP. Para nuestro modelo basado en el contexto utilizamos una aproximación y uso de ideas de teoría de conjuntos. Nos basamos en una representación mediante *Diagramas de Venn*, para buscar con ellos correspondencias matemáticas o lógicas y relaciones entre los elementos de los conjuntos. Se puede establecer una correspondencia matemática entre elementos de un conjunto X y otro conjunto Y, y se representa como:

$$f: X \rightarrow Y \tag{3.2.1}$$

Siendo f una función que relaciona los elementos del conjunto origen X sobre uno o varios elementos del conjunto Y.

Para nuestro modelo tenemos que considerar que f no necesariamente es una expresión matemática sino una representación de diferentes vínculos o relaciones entre

los elementos de un conjunto con respecto a los elementos del otro, y estas relaciones tienen determinadas restricciones, según cada uno de los estados en que se puedan encontrar dichos elementos.

Con estas consideraciones pensamos que una red WiFi está formada básicamente por dos conjuntos: el de los TER (conjunto origen) y el de los AP (conjunto destino). En la Figura 73 se muestran los AP_1, AP_2 y AP_3 (integrantes de una red) en un conjunto; a los TER_1 y TER_2 en otro conjunto; y *f* como la correspondencia no unívoca (cada terminal del conjunto origen solo puede estar asociado a un AP pero un AP puede tener varios terminales asociados) que indica qué un TER concreto está en cobertura con un AP particular.

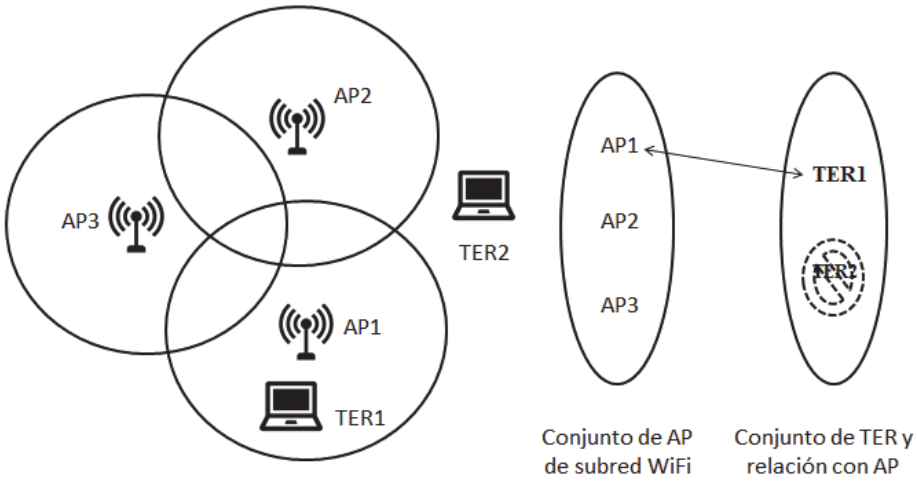


Figura 73. Diagrama de Venn (conjuntos) y correspondencias matemáticas

Definimos el conjunto de terminales como C_{TER}, y el conjunto de AP, C_{AP}, formado por *n* y *m* elementos, respectivamente:

$$C_{TER} = \{TER_1, TER_2, , \dots, TER_i, \dots, TER_n\} \quad (3.2.3)$$

$$C_{AP} = \{AP_1, AP_2, \dots, AP_j, \dots, AP_m\} \quad (3.2.4)$$

Asimismo definimos la red como:

$$Red\_WiFi = \{C_{AP}, C_{TER}\} \quad (3.2.5)$$

En el conjunto de terminales, C_{TER}, se incluyen todos los terminales accesibles por cualquiera de los AP, aunque estos aun no estén asociados. Recordemos que los terminales no son detectados por los AP hasta que se manifiesten con mensajes *Probe* o soliciten una *asociación*. Este aspecto lo consideramos muy importante, pues nos

permite actuar de forma proactiva en el proceso de optimización paramétrica aplicado. Por tanto vamos a considerar que los terminales accesibles a la red WiFi pueden estar en uno de los siguientes cinco estados:

- *e1* (inactivo/inicial): el terminal está inactivo (no asociado) pero en el radio de cobertura de alguno de los AP (detecta al menos uno de los *beacon* emitidos por los AP).
- *e2a* (no asociado pero no detectado por ningún AP): el terminal realiza rastreos pasivos (*scan*) y detecta uno o más AP (el AP no sabe de su presencia).
- *e2b* (no asociado pero detectado por al menos un AP): el terminal realiza rastreos activos (*Probes*), anuncia su presencia y detecta uno o más AP (el AP sabe de su presencia).
- *e3* (asociado pasivo): el terminal está asociado a un determinado AP (registrado) pero no genera ni recibe tráfico.
- *e4* (asociado activo): el terminal está asociado a un determinado AP (registrado) generando o recibiendo tráfico.

En la Figura 74 se muestra una representación del diagrama de estados entre los que podrían encontrarse los terminales según las consideraciones que proponemos. Además se muestran las transiciones entre los mismos, no incluyendo situaciones de desconexiones inesperadas por problemas de la red o salida de cobertura, en cuyo caso el estado sería indeterminado.

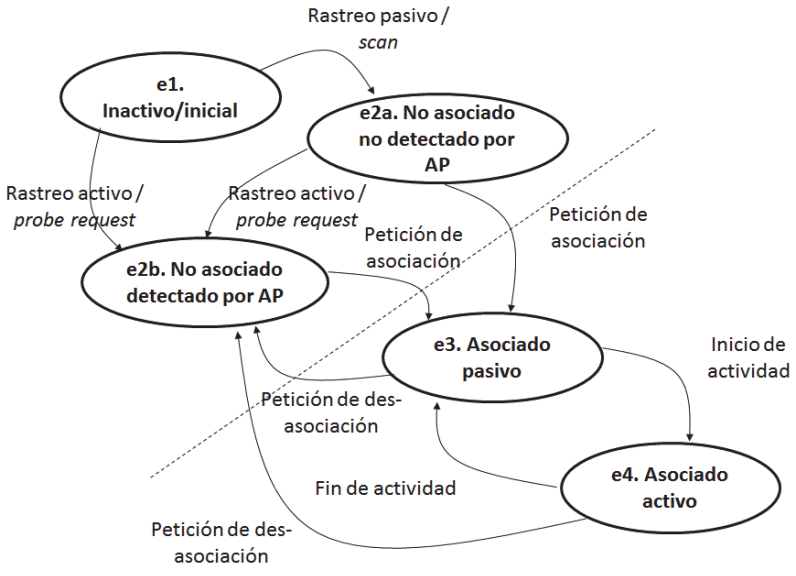


Figura 74. Diagrama de estados de los terminales para nuestra propuesta

Como ya es sabido, los terminales en una red WiFi en modo infraestructura necesitan estar asociados a un solo AP y solo en ese estado pueden establecer conexiones. Analizando las diferentes etapas o estado por lo que puede pasar un terminal podemos optimizar los parámetros y actuar previamente según cada caso. Con ello definimos nuevos conjuntos y subconjuntos de TER y AP y no solo el que se suele utilizar actualmente en cada AP, que no es más que la lista de terminales que tiene asociado.

Si analizamos la Figura 74, consideramos que los terminales que se encuentren en cobertura con cierto AP, pueden anunciarse, en cuyo caso realizan un rastreo activo y con ello los AP pueden registrar la presencia de dichos terminales, aunque ello no represente que se asocien. De igual manera, los terminales pueden realizar rastreos pasivos detectando los AP accesibles pero los AP no detecten su presencia. Nuevamente podemos crear otros conjuntos de terminales: los TER presentes en cobertura por cada AP pero no detectados por los AP y los TER presentes en cobertura por cada AP pero detectados por los AP. Tanto en un caso como en el otro, que son los correspondientes a los estados *e2a* y *e2b*, respectivamente, los terminales para iniciar cualquier comunicación deben solicitar la asociación a un determinado AP y sólo puede asociarse a uno de ellos. Aquí podríamos intervenir para mejorar la elección. Además, el hecho de que se acepte una asociación, no implica necesariamente que se genere tráfico de usuario, por tanto consideramos un estado *e3* como transitorio y previo al de actividad plena. Por último el estado e4 representa que el terminal está participando del canal insertando o recibiendo tráfico de datos de usuario. Con todo esto podemos definir conjuntos, estados y relaciones para el objetivo buscado.

Del estado *e4*, podemos agrupar en otro conjunto a todos los terminales asociados por cada AP_j, $C_{TER\_asociados\_APj}$, en la forma:

$$C_{TER\_asociados\_APj} = \{TER_k, \ldots\ldots, TER_i\} \tag{3.2.6}$$

Con este conjunto podríamos controlar el número de terminales que soporta cada AP y las condiciones de uso del canal compartido por los TER conociendo los tráficos que cada TER maneja.

En este punto, podemos indicar que estos tres conjuntos que hemos definido hasta ahora constituyen la información comúnmente utilizada en redes WiFi por usuarios y administradores: número de AP, número de terminales y cuántos de ellos están

asociados a cada AP. Si los TER transmiten o reciben paquetes, podemos establecer relaciones entre AP, TER y flujos, considerando este último término, como la ristra de paquetes vinculados con cada conexión que se procesan por cada TER. Para nuestra aplicación y propuesta, consideramos flujos como un parámetro medible y como medida de velocidad o ancho de banda (bps). En la Figura 75 se muestra esta relación.

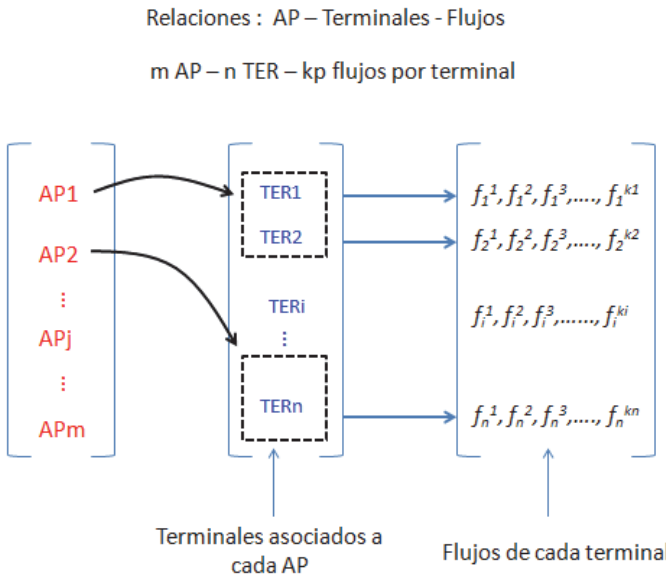


Figura 75. Relación AP - TER asociados y flujos de cada TER con cada AP

Como parte de esta relación destacamos la importancia de los flujos originados en cada TER o dirigidos a cada uno de ellos sobre los que prestar especial atención. Sobre estos flujos se controla el ancho de banda (bps) que utilizan o deberían disponer del total disponible, así como tamaño de paquetes, retrasos, latencia... así como las valoraciones de la QoE. Como la razón de ser de las redes WiFi es la transmisión de flujos, consideramos necesario definir el conjunto de flujos que soporta cada TER y el conjunto de flujos que procesa cada AP.

Partiendo de que cada TER puede establecer diferentes conexiones, consideramos cada una de ellas como un flujo diferente. Por tanto si el terminal TER_1 solo estableciera una comunicación gestionaría el flujo f_{TER1}^{1}, si gestionara dos flujos los representaríamos como f_{TER1}^{1} y f_{TER1}^{2} y así sucesivamente. En general podríamos definir C_{FTERi} como el conjunto de flujos que gestiona el terminal TER_i y expresarlo de la forma siguiente:

$$C_{F_{TER_1}} = \left\{ f_{TER_1}^{1}, f_{TER_1}^{2}, \ldots, f_{TER_1}^{k1} \right\} \tag{3.2.7}$$

$$C_{F_{TER_2}} = \{f^1_{TER_2}, f^2_{TER_2}, \dots., f^{k2}_{TER_2}\}$$
$$\dots\dots$$
$$C_{F_{TER_i}} = \{f^1_{TER_i}, f^2_{TER_i}, \dots., f^{ki}_{TER_i}\}$$
$$\dots\dots$$
$$C_{F_{TER_n}} = \{f^1_{TER_n}, f^2_{TER_n}, \dots., f^{kn}_{TER_n}\}$$

Debemos resaltar que en (3.2.7) no necesariamente todos los terminales gestionan el mismo número de flujos, luego los valores k_1, k_2,…, k_i,…, k_n pueden ser diferentes para cada terminal *i*.

Si consideramos, que de forma habitual, más de un terminal está asociado al mismo AP y que cada terminal puede tener distinta cantidad de flujos, podríamos agrupar todos los flujos soportados por un AP concreto como el conjunto de flujos de todos los terminales asociados.

Para realizar estas consideraciones nos basamos en el estándar WiFi, no contemplando configuraciones multi-interfaz ni multi-transporte como MPTCP [142], ya que consideramos que todos los flujos de un determinado TER son gestionados por el mismo AP, y por ello, generalmente los flujos de cada AP se corresponden con la suma de los flujos de los TER asociados al mismo.

En este caso si suponemos que se cuenta con *n* terminales con k_i flujos cada uno de ellos asociados a un determinado AP_j podríamos agruparlos como un total de flujos que soporta dicho AP_j como:

$$f\_AP_j = \sum_{i=1}^{n} C_{F_{TER_i}} \qquad (3.2.8)$$

A partir de la formalización anterior controlamos los flujos, la ubicación de los TER, la re-asociación de los TER entre los AP… aplicando mecanismos concretos de regulación como mostramos gráficamente en la Figura 76.

Definimos $B_m\_AP_j$ como la capacidad teórica del canal de trabajo del AP_j (o sea el ancho de banda estimado disponible medido previamente). El ancho de banda necesario para atender diferentes flujos (de los diferentes terminales) no puede ser superior a $B_m\_AP_j$, e incluso debería mantenerse por debajo en un margen inferior de guarda.

Si consideramos un flujo $f^{i}_{TER_j}$ como prioritario, se debería controlar y garantizar que dicho flujo no requiera un ancho de banda superior a la capacidad disponible. Cumpliendo este requisito, se calcula o estima que disponibilidad de ancho de banda se tendría en función del resto de flujos que comparten dicho canal, y se busca una solución para que los requisitos demandados puedan ser alcanzados limitando otros flujos en beneficio de este.

En el ejemplo de la Figura 76, mostramos que el AP_1 tiene asociados los terminales TER_1 y TER_2 con sus flujos correspondientes. El AP_2 tiene asociado el TER_3 y finalmente el AP_m tiene asociado el TER_n. En la matriz o conjunto de la izquierda indicamos una situación en la que, tanto el AP_2 como el AP_m soportan perfectamente todos los flujos de los TER_3 y TER_n. En ambos casos, con los datos disponibles de cada flujo y la capacidad de cada AP_j, se comprueba que se garantiza que $f\_AP_2 < B_m\_AP_2$ y $f\_AP_m < B_m\_AP_m$, en general $f\_AP_j < B_m\_AP_j$. En cambio para el AP_1 se indica que los flujos que soporta de los dos terminales asociados (TER_1 y TER_2) superan la capacidad ($f\_AP_1 > B_m\_AP_1$). En tal caso, se necesitaría, o bien, como opción 1: reducir alguno de los flujos de alguno de los terminales, por ejemplo del TER_2, si alguno de sus flujos fuese no prioritario y así limitar la demanda global de ancho de banda, indicado con②, o bien, opción 2: traspasar todo el tráfico del TER_2 al AP_2 u otro AP_j accesible (marcado con ③). En la Figura 76 se representa este efecto de hacer que los flujos f_2^3 y f_2^{k2} se vean limitados con la flecha mostrada sobre los mismos (②), como resultado de la primera opción. Recordemos que los flujos no pueden dirigirse individualmente hacia otro AP, sino que se agrupan como parte de todo el tráfico del terminal. En ambos casos lo que se pretende es descargar de tráfico el canal del AP_1 para que 1º) no se supere la capacidad máxima del mismo $B_m\_AP_1$ y 2º) que los flujos prioritarios puedan disponer de más ancho de banda libre. Este proceso requiere de un control previo de los flujos a procesar (control de admisión de flujos), un tratamiento dinámico de uso del canal, un análisis detallado de las condiciones de contexto; y aplicar algún método de optimización basado en: bloqueo de flujos y/o terminales, alteración de variables de los flujos y/o redistribución de terminales.

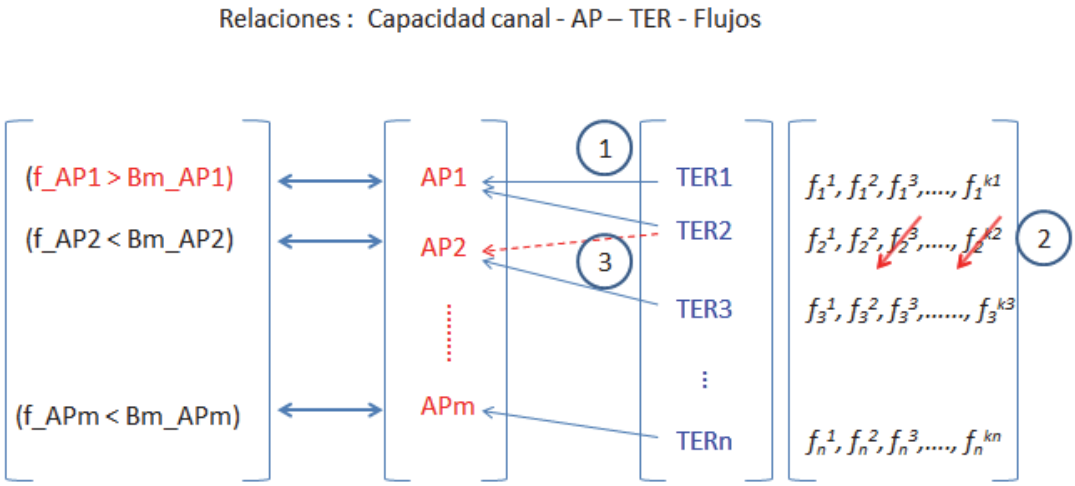


Figura 76. Regulación de flujos y control de ubicación de TER

Un aspecto muy importante es el que es preceptivo que los TER sepan a qué AP de los que estén en su zona de cobertura pueden asociarse, pues de no ser así, es imposible establecer cualquier conexión o incluso, no poder asociarse a otro AP cuando sea necesario. A estos AP, los agrupamos en un nuevo conjunto que denominamos conjunto de AP visibles por cada TER_i. Este conjunto se puede obtener de cualquiera de los estados e2. Lo denominamos $C_{AP\_visibles\_TERi}$ y lo representamos como:

$$C_{AP\_visibles\_TER_i} = \{AP_k, \ldots\ldots, AP_j\} \tag{3.2.9}$$

Otro conjunto muy importante, íntimamente relacionado con (3.2.5), es el conjunto de valores de RSSI detectados de cada AP visible por cada TER_i, y lo representamos como $RSSI_{TERi}$:

$$RSSI_{TER_i} = \{RSSI\_AP_1, RSSI\_AP_2, \ldots\ldots RSSI\_AP_j, \ldots. RSSI\_AP_m\} \tag{3.2.10}$$

Este último conjunto, como ya se indicó, tiene muchísima importancia, dado que de sus elementos dependen muchas de las acciones y nuevos servicios dentro de una red WiFi, como son: mínimo nivel de señal con garantías de asociación, control IEEE 802.11 *Request To Send/Clear To Send* (*RTS/CTS*), proceso de *handover*, control de desconexiones, servicios de localización...

Aparte de los anteriores conjuntos, consideramos que se pueden plantear otros conjuntos adicionales y relaciones entre TER y AP, concretamente:

1. *Relación de AP en cobertura entre ellos*. Con esta información se puede detectar problemas de solapes o TER en zona de cobertura compartida y con ello permitir *handover* dirigido.
2. *Relación de TER que cada AP detecta aun no estando asociado*. Este permite mejorar la localización de TER y reasociación entre los AP.
3. *Relación de TER detectables entre ellos*. Con esta información se permite contar con información de estado y ubicación de cada TER. Con ello se mejora la predicción de ubicación y comportamiento de la red.

Estas relaciones, las consideramos adicionales dado que no están incluidas en los estándares IEEE 802.11, pues no se indica nada respecto a que los AP entre ellos se detecten mediante *scanning* ni que los TER se detecten entre ellos. Solamente el papel activo de las redes es realizado por los TER al detectar que AP están accesibles y seleccionar uno de ellos.

En la Figura 77 se representan gráficamente las 4 relaciones entre los AP y los TER, destacando la que es indispensable (3.2.9), o sea la lista de AP en cobertura de TER ($C_{AP\_visibles\_TERi}$), y las tres adicionales que incorporamos a nuestro modelo basado en conjuntos y relaciones.

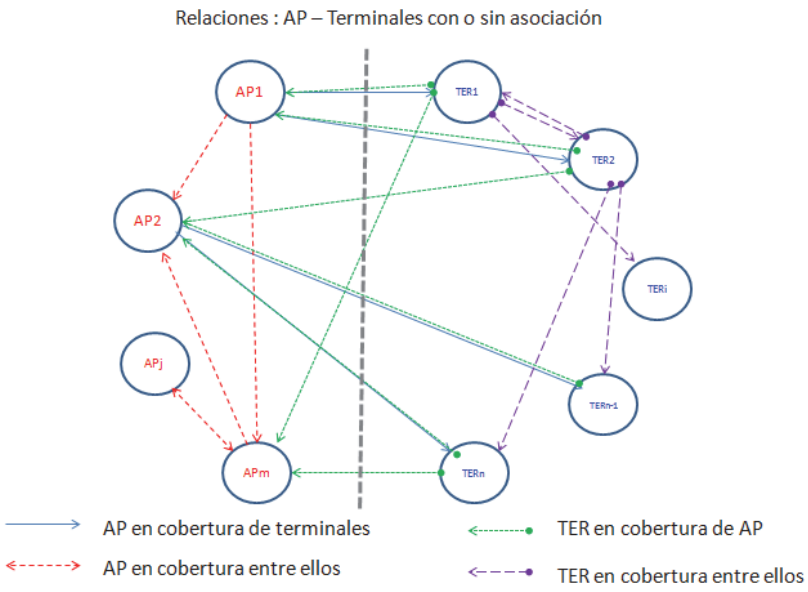


Figura 77. Relaciones entre AP y TER

Para estas tres últimas relaciones definimos los conjuntos:

- Conjunto de AP detectables (visibles o en cobertura) para cada AP_j como:

$$C_{AP\_visibles\_APj} = \{\forall\, AP_k(en\ cobertura\ de\ APj)\ \neq\ AP_j\} \quad (3.2.11)$$

- Conjunto de TER detectables (visibles o en cobertura) por cada AP_j como:

$$C_{TER\_visibles\_APj} = \{\forall\, TER_k\ (en\ cobertura\ APj)\} \quad (3.2.12)$$

- Conjunto de TER detectables (visibles o en cobertura) para cada TER_i como:

$$C_{TER\_visibles\_TERi} = \{\forall\, TER_k(en\ cobertura\ de\ TERi)\ \neq\ TER_i\} \quad (3.2.13)$$

Para aplicar la última relación o gestionar el conjunto asociado, $C_{TER\_visibles\_TERi}$, es necesario acometer cambios en el funcionamiento de los TER, pues estos deberían participar activamente en el intercambio de información de control entre ellos, inexistente en WiFi en la actualidad. Básicamente se requeriría que los TER se anunciasen o el resto de TER tuvieran que escanear el espectro para detectar presencia de tráfico del resto de TER.

Contando con las cuatro relaciones o conjuntos asociados (3.2.9), (3.2.11), (3.2.12), (3.2.13) y con la información vinculada a cada elemento (flujos, RSSI, tecnología soportada, estado, condiciones...), se tendría un conocimiento completo de todos los elementos participantes de la red y podemos aplicar mecanismos de optimización, ya sea de forma centralizada desde el/los AP o mixta entre AP y TER.

A continuación definimos en la Tabla 20 una serie de factores o condiciones de contexto, complementarios a los conjuntos anteriores, que consideramos pueden aportar información representativa del estado del mismo.

Tabla 20. Relación de parámetros a considerar para contextualización

Parámetro	Descripción
PRES_INACTIVA_TERi	Indica la presencia de un TERi en el área de cobertura de un determinado AP que pudiera solicitar asociación (situación previa a una asociación).
PRES_NO ASOC_PAS_TERi	Indica la presencia de un TERi en la zona de cobertura del AP de que se trate pero realiza rastreos pasivos (e2a).
PRES_NO_ASOC_ACT_TERi	Indica la presencia de un TERi en la zona de cobertura del AP de que se trate pero realiza rastreos activos (e2b).
PRES_ASOC_PASIVO_TERi	Indica la presencia de un TERi en la zona de cobertura del AP de que se trate, que ya se encuentra asociado o registrado al mismo y

	potencialmente procesaría tráfico con el mismo como origen o destino (e3).
PRES_ASOC_ACTIVO_TERi	Indica la presencia de un TERi en la zona de cobertura del AP de que se trate, que se encuentra originando o recibiendo tráfico de usuario a nivel de aplicación (e4).
LOCALIZACIÓN_DE_TERi	Indica una posición estimada del TER dentro del ámbito de la zona de cobertura del AP de que se trate o en que intersección se encuentra.
REQUISITOS_DE_TERi	Indica un conjunto de necesidades de servicio relacionadas con el uso que pretende hacer cada TER de la red (AP), para determinar si son posibles atender o cuál de los AP disponibles pudieran hacerlo. Estas pueden incluir: - Mínimo bitrate requerido - Máximo retraso permitido - Mínima latencia permitida - Máximo jitter permitido - Máximo Bit Error Rate (BER) soportable - Mínimo tamaño de paquete permitido
ESTADO_DE_TERi	Indica un conjunto de variables del/los servicio/s que cada TERi está haciendo uso para determinar mecanismos de corrección, si no se garantizan los requisitos iníciales. Este parámetro está ligado directamente con los REQUISITOS_DE_TER y estado del AP que gestiona el servicio.
NRO_DE_TER	Indica el número total de TER que están en el ámbito de cobertura de la red de que se trate (número de elementos o cardinal de $\mathbf{C_{TER}}$ **(3.2.3)**).
NRO_DE_AP	Indica el número de AP que configuran la red WiFi (número de elementos o cardinal de $\mathbf{C_{AP}}$ **(3.2.4)**).
ID_AP	Indica un identificador del AP que estemos tratando y su relación con el resto de la red.
ID_TER	Indica un identificador del TER que estemos tratando y su relación con el resto de la red.
NRO_DE_TER_ASOC_APj	Indica el número de TER asociados a un determinado AP (número de elementos de $\mathbf{C_{TER\ asociados\text{-}APj}}$ **(3.2.6)**).
LISTA_DE_TER_ASOC_APj	Indica un vector de ID de TER. Se enumeran los TER que están asociadas a un determinado APj ($\mathbf{C_{TER\ asociados\text{-}APj}}$ **(3.2.6)**).
NRO_DE_TER_VIS_APj	Indica el número de TER en el ámbito de cobertura de un determinado APj (número de elementos de $\mathbf{C_{TER\ visibles\ APj}}$ **(3.2.12))**.
LISTA_DE_TER_VIS_APj	Indica un vector de ID de AP. Se enumeran los TER que son detectables por cada AP ($\mathbf{C_{TER\ visibles\ APj}}$ **(3.2.12)).**
NRO_DE_AP_VIS_APj	Indica el número de AP detectables por cada AP (solapes) (número de elementos de $\mathbf{C_{AP\ visibles\ APj}}$ **(3.2.11)**).
LISTA_DE_AP_VIS_APj	Indica un vector de ID de AP. Se enumeran los AP que son detectables por cada AP ($\mathbf{C_{AP\ visibles\ APj}}$ **(3.2.11)**).
DISPONIBILIDAD_DE_APj	Indica el estado en que se encuentra cada AP. Por ejemplo un AP puede estar NO DISPONIBLE para que otros AP le pasen TER por balanceo.
CARACTERISTICAS_DE_APj	Indica una relación de características de cada APj (vecino o en general) en cuanto a prestaciones (ancho de banda, tecnologías soportadas, número de interfaces, capacidad total (B_T_APj) y medida estimada (Bm_APj)…), número y estado de conexiones activas, restricciones de usuarios, terminales o tráfico de aplicación....
VECINOS_AP_CERCANOS_APj	Indica una lista AP que se encuentran con sus bordes o límites solapados de área de cobertura para cada AP. Solo se utiliza para conocer zona de intersecciones.
LISTA_DE_AP_VIS_TERi	Indica un vector de ID de AP. Se enumeran los AP detectables por cada TERi ($\mathbf{C_{AP\ visibles\ TERi}}$ **(3.2.9)**).
LISTA_DE_TER_VIS_TERi	Indica un vector de ID de TER. Se enumeran los TER que son detectables por cada TER de que se trate ($\mathbf{C_{TER\ visibles\ TERi}}$ **(3.2.13)**)
LISTA_RSSI_AP_VIS_TERi	Indica un vector de valores de RSSI. Se enumeran los valores de

	RSSI detectados de cada AP en cada TERi (**$RSSI_{TERi}$ (3.2.10)**)
BALANCEO_TERi	Indica la posibilidad efectiva de realizar un traspaso de TER asociados inicialmente a un AP por disponer de otro VECINO que pueda aceptarlo (depende directamente de condiciones de LOCALIZACION_DE_TERi, VECINOS_AP_CERCANOS_APj y CARACTERISTICAS_DE_APj).
NRO_FLUJOS_TERi	Cantidad de flujos o conexiones activas o solicitadas por cada TERi.
LISTA_FLUJOS_TERi	Relación de flujos y sus características manejados por cada TERi (3.2.7).
FLUJOS_TERi	Capacidad demandada por las suma de los flujos de cada TERi.
NRO_FLUJO_APj	Cantidad de flujos o conexiones activas en cada APj.
LISTA_FLUJO_APj	Relación de flujos y sus características soportados por cada APj (3.2.8).
FLUJOS_APj	Capacidad soportada por la suma de todos los flujos soportados por el APj de los diferentes terminales TERi.

Esta relación de parámetros no es exclusiva ni tampoco completa, sino representa aquellos que consideramos más representativos para la toma de decisión de su optimización. Podemos ordenarlos y ubicarlos en la Tabla 21 atendiendo a qué dispositivo debería gestionar cada parámetro o tener conocimiento de su valor (AP, TER o ambos). Esta relación podría ampliarse e irse complementado en función de los objetivos concretos, y formaría parte de los que ya habíamos denominado factores que determinan las condiciones de contexto.

Tabla 21. Relación de parámetros considerados y definición de tipo de datos

Nombre	***Denominación***	***TER → i***	***AP → j***	***Tipo***
$P_{TER\_INACTIVO}(i)$	*PRES_INACTIVA_TERi*	*X*		*Booleano*
$P_{TER\_NO\_ASOC\_PASIVO}(i)$	*PRES_NO ASOC_PAS_TERi*	*X*		*Booleano*
$P_{TER\_NO\_ASOC\_ACTIVO}(i)$	*PRES_NO_ASOC_ACT_TERi*	*X*	*X*	*Booleano*
$P_{TER\_PASIVO}(i)$	*PRES_ASOC_PASIVO_TERi*	*X*	*X*	*Booleano*
$P_{TER\_ACTIVO}(i)$	*PRES_ASOC_ACTIVO_TERi*	*X*	*X*	*Booleano*
$U_{TER}(i)$	*LOCALIZACIÓN_DE_TERi*	*X*	*X*	*Estructura*
$R_{TER}(i)$	*REQUISITOS_DE_TERi**	*X*		*Estructura*
$S_{TER}(i)$	*ESTADO_DE_TERi*	*X*		*Estructura*
F_{TERi}	*FLUJOS_TERi (3.2.7)*	*X*		*Entero*
f_{TERi}	*LISTA_FLUJOS_TERi (3.2.7)*	*X*		*Estructura*
Nf_TERi	*NRO_FLUJOS_TERi*	*X*		*Entero*
$N_{AP} = j$	*NRO_DE_TER*		*X*	*Entero*
$N_{TER} = i$	*NRO_DE_AP*	*X*		*Entero*
AP_j	*ID_AP*		*X*	*ID*
TERi	*ID_TER*	*X*		*ID*
$RSSI_{TERi}$	*LISTA_RSSI_AP_VIS_TERi (3.2.10)*	*X*		*Vector*
$N_{TER\_ASO\_APj}$	*NRO_DE_TER_ASOC_APj (3.2.6)*		*X*	*Entero*
$L_{TER\_ASO\_APj}$	*LISTA_DE_TER_ASOC_APj (3.2.6)*		*X*	*Vector*
$N_{TER\_VIS\_APj}$	*NRO_DE_TER_VIS_APj (3.2.12)*		*X*	*Entero*
$L_{TER\_VIS\_APj}$	*LISTA_DE_TER_VIS_APj (12)*		*X*	*Vector*

$N_{AP\_VIS\_APj}$	*NRO_DE_AP_VIS_APj (3.2.11)*		*X*	*Entero*
$L_{AP\_VIS\_APj}$	*LISTA_DE_AP_VIS_APj (3.2.11)*		*X*	*Vector*
$D_{AP}(j)$	*DISPONIBILIDAD_DE_APj*	*X*	*X*	*Booleano*
$Car_{AP}(j)$	*CARACTERISTICAS_DE_APj*[*]	*X*	*X*	*Estructura*
$V_{AP}(j)$	*VECINOS_AP_CERCANOS_APj*		*X*	*Vector*
Nf_APj	*NRO_FLUJOS_APj*		*X*	*Entero*
L_{F_APJ}	*LISTA_FLUJOS_APj*		*X*	*Estructura*
f_APj	*FLUJOS_APj < Bm_APj*		*X*	*Entero*
$L_{AP\_VIS\_TERi}$	*LISTA_DE_AP_VIS_TERi (3.2.9)*		*X*	*Vector*
$L_{TER\_VIS\text{-}TERi}$	*LISTA_DE_TER_VIS_TERi (3.2.13)*	*X*		*Vector*
$Bal_{TER}(i)$	*BALANCEO_TERi*	*X*	*X*	*Booleano*

Algunos de estos parámetros los consideramos booleanos, dado pueden estar en dos posibles valores, o habilitan o no el tratamiento o utilidad de otros parámetros. Otros son simples contadores (números enteros positivos), otros son una lista de valores (vector) y finalmente otros son un conjunto de variables en modo arreglo o estructura de datos. En este último caso, utilizamos el formato *variable=valor* con datos o medidas que serían tratadas de forma particular dentro de su ámbito (por ejemplo localización de TERi puede indicar las coordenadas geográficas, una posición relativa dentro de un recinto, una zona específica...).

Todos los anteriores parámetros están vinculados con los TER o con los AP o ambos. El que relaciona ambos dispositivos es el que denominamos *matriz de asociación,* que representamos como $A_{TER\_AP}\ (i,j)$, de manera similar a como un producto cartesiano se define en teoría de conjuntos. Con dicha matriz indicamos como están los terminales asociados a alguno de los AP. Gráficamente, en forma de tabla podemos verlo como se muestra a modo de ejemplo en la Tabla 22. En ella se vincula el índice de cada TER con el correspondiente de cada AP. Esto equivaldría a gestionar todos los conjuntos $C_{TER\_asociados\_APj}$ definidos en (3.2.6).

$$A_{TER\_AP}(i,j) \tag{3.2.14}$$

Tabla 22. Tabla de asociaciones de AP y TER

APj / *TERi*	*j=1*	*j=2*	----	*j=m*
i=1	*x*	*x*	----	*x*
i=2	*x*	*x*	----	*x*
-----	*x*	*x*	----	*x*

i=n	*x*	*x*	----	*x*

Si en la matriz o tabla solo queremos representar los conjuntos (3.2.3), podríamos hacer un simple tratamiento booleano, poniendo un 1 para indicar el estado asociado y un 0 para no asociado. A modo de ejemplo, si en un momento dado se tiene que TER_1 y TER_2 están asociados al AP_1, el TER_3 asociado al AP_2 y TER_4 asociado al AP_3 tendríamos la matriz de asociación A_{TER_AP} *(i,j)* y conjunto-relación mostrado en la Figura 78.

$$\begin{matrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

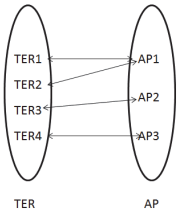


Figura 78. Ejemplo de matriz de asociación y conjuntos-relación

De esta forma, en horizontal solo podemos encontrar un solo 1 representando a que AP está asociado cada TER, pero en vertical pueden haber varias TER asociados al mismo AP. En una segunda versión ampliada, consideramos a cada elemento de la matriz como un *vector de parámetros*, que denominamos ***estado (i,j).*** La matriz tiene una forma similar a la mostrada en la Figura 79.

$$\begin{matrix} \textit{estado (1,1)} & 0 & 0 \\ \textit{estado (2,1)} & 0 & 0 \\ 0 & \textit{estado (3,2)} & 0 \\ 0 & 0 & \textit{estado (4,3)} \end{matrix}$$

Figura 79. Matriz de asociación mejorada

Esta información de estado incluye información propia de cada TER como del AP al que está vinculado, RSSI detectado en cada TER_i para cada AP_j, frecuencia/canal de AP_j (Fr_AP_j / Ch_AP_j), ancho de banda teórico total (bps) (B_{T_APj}), ancho de banda medido promedio (Bm_AP_j), número de conexiones activas en AP_j (Nc_j), número de TER asociados al AP_j ($N_{TER\_AP(j)}$)...

$$Estado_{i,j}[-] = [RSSI\_AP_j, fr\_AP_j, ch\_AP_j, Bt\_AP_j, Bm\_AP_j, Nc_j, N_{TER\_APj}, ..] \quad (3.2.15)$$

Algunos parámetros funcionales son necesarios para completar el estado global de todos los dispositivos activos o no. Uno de ellos es el que relacionamos con los estados en que hemos planteado se pueden encontrar los TER, ya mostrados en la Figura 74. Para ello, el hecho de encontrarse en un determinado estado lo vamos a materializar con las variables *PRESENCIA*, cuyo valor para cada TER_i solo puede estar en uno de los cinco valores considerados: inactivo, no asociado pasivo, no asociado activo, asociado pasivo o asociado activo. De ello podemos calcular la cantidad de TER que se encuentran en cada estado y la formulación utilizada es:

$$\begin{aligned} N_{TER\_INACTIVOS} &= \sum P_{TER\_INACTIVOS} \\ N_{TER\_NO\_ASOC\_PASIVOS} &= \sum P_{TER\_NO\_ASOC\_PASIVOS} \\ N_{TER\_NO\_ASOC\_ACTIVOS} &= \sum P_{TER\_NO\_ASOC\_ACTIVOS} \\ N_{TER\_ASOC\_PASIVOS} &= \sum P_{TER\_ASOC\_PASIVOS} \\ N_{TER\_ASOC\_ACTIVOS} &= \sum P_{TER\_ASOC\_ACTIVOS} \end{aligned} \quad (3.2.16)$$

Esta información tiene que corresponder con el número total de terminales presentes en la red:

$$N_{TER} = N_{TER_{INACTIVOS}} + N_{TER\_NO\_ASOC\_PASIVOS} + N_{TER\_NO\_ASOC\_ACTIVOS} + \quad (3.2.17)$$

$$+ N_{TER\_ASOC\_PASIVOS} + N_{TER\_ASOC\_ACTIVOS}$$

Con esta clasificación de estado (PRESENCIA) de TER gestionamos de forma *proactiva* un control de admisión y asignación de recursos. Ante la presencia de un TER en el área de cobertura de cualquiera de los AP, que si bien pudiera no estar asociado o generando tráfico, sería susceptible de hacerlo. Si no fuese así, la actuación debe ser *reactiva* y, esta no siempre es lo suficientemente eficiente, frente a si se aplica de forma proactiva.

- **Ejemplo genérico parámetros para red WiFi formato 3 AP y 1 TER**

Para ilustrar algunos de los parámetros que hemos expuesto, y a modo de ejemplo más completo, utilizamos la red mostrada en la Figura 80. Esta red está formada por tres AP con zonas de intersección (celdas) y un TER1 asociado al AP2.

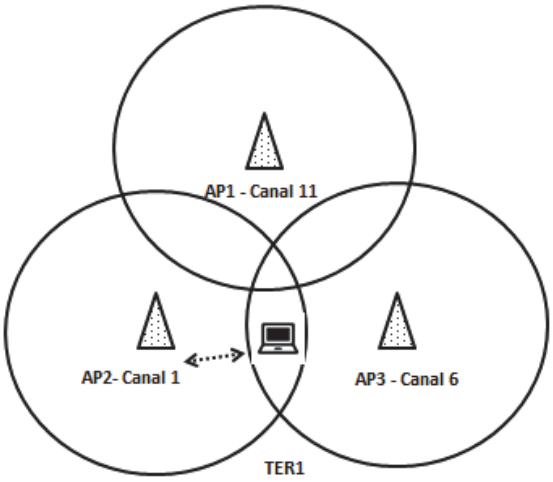


Figura 80. Configuración de ejemplo de optimización paramétrica

En este ejemplo los parámetros tienen los valores:

Conjuntos globales:

$$C_{AP} = \{AP_1, AP_2, AP_3\}$$
$$C_{TER} = \{TER_1\}$$
$$Red_{WiFi} = \{C_{AP}, C_{TER}\}$$

Terminales asociados por AP:

$$C_{TER\_asociados\_AP_1} = \{null\}$$
$$L_{TER\_ASO\_AP1} = null$$
$$N_{TER-ASO-AP1} = 0$$

$$C_{TER\_asociados\_AP_2} = \{TER_1\}$$
$$L_{TER\_ASO\_AP2} = (TER_1)$$
$$N_{TER\_ASO-AP2} = 1$$

$$C_{TER\_asociados\_AP_3} = \{null\}$$
$$L_{TER\_ASO\_AP3} = null$$
$$N_{TER\_ASO-AP3} = 0$$

Visibilidad de terminales desde AP (ubicación):

$$C_{TER\_visibles\_AP1} = \{null\}$$
$$L_{TER\_VIS\_AP1} = null$$
$$N_{TER\_VIS\_AP1} = 0$$

$$C_{TER\_visibles\_AP2} = \{TER_1\}$$
$$L_{TER\_VIS\_AP2} = (TER_1)$$
$$N_{TER\_VIS\_AP2} = 1$$

$$C_{TER\_visibles\_AP3} = \{TER_1\}$$
$$L_{TER\_VIS\_AP3} = (TER_1)$$
$$N_{TER\_VIS\_AP3} = 1$$

Visibilidad de AP desde terminales:

$$C_{AP\_visibles\_TER1} = \{AP_2, AP_3\}$$
$$L_{AP\_VIS\_TER1} = (AP_2, AP_3)$$

Visibilidad entre AP:

$$C_{AP\_visibles\_AP1} = \{null\}$$
$$C_{AP\_visibles\_AP2} = \{null\}$$
$$C_{AP\_visibles\_AP3} = \{null\}$$

Visibilidad entre terminales:

$$C_{TER\_visibles\_TER1} = \{null\}$$

Estado de terminales:

$$P_{TER\_PASIVO(1)} = 1$$

Matriz de asociación:

	AP_1	AP_2	AP_3
TER_1	0	estado(1,2)*	0

**Estado (1,2): conjunto de variables o condiciones de flujos y parámetros propios del canal*

Factores/Parámetros generales

$ID\_TER = TER_1$	*(puede ser el valor de i o un id. único para cada TER)*
$ID\_AP = \{AP_1, AP_2, AP_3\}$	*(puede ser el valor de j o un identificador único para cada AP)*
$N_{TER} = 1, i = 1$:	*(cantidad de terminales)*
$N_{AP} = 3, j=1..3$:	*(cantidad de AP)*
$N_{TER\_ASO\_ACTIVE} = 1$:	*(número de terminales activos igual a 1)*
$D_{AP1} = ON$:	*(AP_1 está disponible para aceptar asociaciones)*
$D_{AP2} = ON$:	*(AP_2 está disponible para aceptar asoc. (TER_1 asociado))*
$D_{AP3} = ON$:	*(AP_3 está disponible para aceptar asociaciones)*

Hemos obviado, para simplificar el ejemplo, las características de los AP (Car_{AP_j}) y los requisitos del TER_1 (R_{TER1}).

Factores de topología

$V_{AP1} = \{2,3\}$ *(AP vecinos de cada AP con cierto solape de cobertura)*

$V_{AP2} = \{1,3\}$

$V_{AP3} = \{1,2\}$

Factores para ubicación/localización

$U_{TER1} = \{2,3\}$ *(Ubicación relativa de TER_1 entre zona de AP_2 y AP_3)*

$B_{TER1} = ON$ *(Posibilidad de balanceo o reubicación al estar en intersección de AP_2 y AP_3)*

3.2.2 Optimización paramétrica para mejorar prestaciones

Desde un punto de vista general, sabemos que un problema de optimización consiste en minimizar o maximizar el valor de una variable. O sea, se trata de calcular o determinar el valor mínimo o el valor máximo de una función de una o varias variables.

Dada una función f: A → R el resultado de la optimización consiste en encontrar un elemento x_0 en A tal que $f(x_0) \leq f(x)$ para todo x en A ("minimización") o tal que $f(x_0) \geq f(x)$ para todo x en A ("maximización").

Se debe tener presente que la variable que se desea minimizar o maximizar debe ser expresada como función de otra de las variables relacionadas con el problema.

El problema de minimizar las pérdidas de calidad de las comunicaciones en WiFi, las pérdidas de conectividad (salida de cobertura), minimizar el retraso de paquetes, minimizar la potencia de transmisión, minimizar el número de dispositivos pero maximizando cobertura, maximizar la durabilidad de batería o ahorro energético... en este tipo de redes es un problema de optimización matemático imposible de ser resuelto matemáticamente de forma cerrada [41] [47] [97] . Existe una gran cantidad de factores o parámetros que le afectan. Es evidente que conseguir la máxima calidad de una comunicación con un canal saturado de otras conexiones es imposible, así como que la batería perdure más tiempo con un terminal en modo reposo frente a transmitiendo y recibiendo tráfico.

Por tanto, la existencia de esos factores interrelacionados, que según los fijemos como prioritarios o no, y gestionando los mismos de forma que puedan descartarse, acotarse o fijarse con unos criterios iniciales, permite alcanzar una determinada solución de las muchas posibles al objetivo buscado. De entre estos factores que influyen indiscutiblemente resaltamos los siguientes:

1. Disponibilidad de varios AP como primer factor y de primordial importancia, dado que la razón de ser de los AP es dar conectividad a cualquier TER que lo demande, salvo restricciones de acceso (clave, limitación de usuarios,..).
2. El uso de diferentes tecnologías o versiones del estándar dentro de la misma infraestructura de red WiFi, para mantener compatibilidad, implica diferentes requisitos y limitaciones de cada uno de ellos (por ejemplo IEEE 802.11b, g y n deben coexistir).
3. La existencia de una conexión de cada AP con la red cableada (interfaz LAN), en combinación con el indispensable interfaz WLAN que permita la comunicación entre dos TER o entre dos AP.
4. Otros factores relacionados con el número de clientes asociados (TER) y el número y tipos de conexiones que están haciendo, representa otro conjunto de factores de suma importancia y que de forma creciente complican el problema de optimización.
5. El uso de diferentes anchos de banda (bps) de ciertas tecnologías como IEEE 802.11n e IEEE 802.11ac, que de su tamaño depende la capacidad del canal (20Mhz, 40MHz, 80 MHz, según cada caso), produce efectos directos sobre la capacidad de los canales de los AP afectados. Limitar la capacidad de transmisión (reducir ancho de banda de la modulación utilizada) afecta directamente a una reducción de consumo a costa de reducir velocidad y/o capacidad.
6. Otros factores podrían relacionarse con el nivel de aplicación, pues de las características de la aplicación o servicio demandado se pueden o no aplicar acciones de control.

En cualquiera de los casos, como se observa, hay diferentes factores que podrían ubicarse en alguno de las niveles de la arquitectura de red (Figura 71), o podrían afectar

a varios de ellos (*cross-layer*); y que sus efectos sobre el *throughput*, retrasos, desconexiones y consumo puede ser mayores o menores.

Todos los factores anteriores se podrían agrupar dentro del ámbito de aplicación para cada AP de forma individual. A continuación podríamos enumerar otros que se agruparían cuando se dispone de varios AP:

1. Una inadecuada planificación en la asignación de los canales utilizados por diferentes AP provoca un ineficiente acceso al canal, pues se introducen mayores interferencias y colisiones en los propios *beacon* y a la hora de transmitir el tráfico de conexiones de usuario.
2. La existencia de varios AP en la zona de cobertura de un determinado TER posibilita que mediante los adecuados mecanismos de gestión de conexión de TER pueda balancearse entre los AP.
3. La localización exacta de la ubicación de cada TER y una más eficiente planificación de que AP debe atender a cada TER, facilita una optimización acerca de que AP pueda atender la demanda de TER de forma óptima.
4. En el caso de redes *mesh*, en donde los AP cuentan con el mismo o diferente interfaz WLAN para configurar una malla, es otro factor que afecta de forma importante a mejorar la interconexión entre ellos.
5. El contar con múltiples AP permite cubrir mayores zonas de cobertura y facilita la movilidad de los terminales sin perder conectividad.

En este marco, podemos plantear el siguiente problema de optimización matemático, en el que aparecen las siguientes ecuaciones e inecuaciones que expresan las relaciones entre los parámetros relacionados anteriormente.

- Índices:
  - i: para indicar terminales
  - j: para indicar AP
  - k_i: para indicar flujos por cada TERi
- De entre las características de los APj ($Car\_AP_{j)}$ tenemos:
  - Capacidad máxima (bps) teórica: $B_T\_AP_j$,
  - Capacidad medida (bps): $B_m\_AP_j$
  - ID de canal / frecuencia: Ch_AP_j / Fr_AP_j
  - Identificador de AP: AP_j

- Número total de terminales: N_{TER}
- Número total de AP: N_{AP}
- Número de terminales asociados a AP_j: $N_{TER\_ASO\_APj}$
- Identificador de terminal = TER_i
- Índice terminales i por cada AP_j desde 1 hasta $N_{i,j}$
- Lista de terminales asociados a AP_j: $L_{TER\_ASO\_APj}$
- Flujos (conversaciones) de TER_i: f_{TERi}^{ki}
- Número total de flujos por terminal TER_i: Nf_{TERi}
- Flujos soportados por AP_j: F_{APj}
- Número de flujos soportados por APj: N_{f_APj}
- Características de cada flujo (requisitos)
    - Retraso máximo permitido de flujo ki para TERi: $R_{i,ki}$
    - Throughput mínimo aceptable de flujo ki para TERi: $T_{i,ki}$
    - Latencia permitida de flujo ki para TERi: $L_{i,ki}$
    - Jitter permitido de flujo ki para TERi: $J_{i,ki}$
    - Otras (Tasa de pérdidas máxima, Tamaño mínimo de paquetes...)

Recordando que i es el índice de TER, j el índice de AP y k el índice de flujos por TER, nos vamos a centrar de manera prioritaria en los siguientes problemas de optimización, concretamente:

- *Maximizar el ancho de banda (bps) disponible en cada canal WiFi para ciertos flujos k por cada TER_i que requieran de mayor cantidad del mismo*.

  Considerando un flujo como prioritario $f_i^{ki} \in F_P$ (en especial flujos CBR dependientes del tiempo) de entre los flujos del TER_i , o entre cualquiera de los terminales existentes asociados a determinado AP_j, y suponiendo fijo el ancho de banda máximo disponible (bps) de cada AP_j, podemos suponer que:

  $$B_{m\_APj} \approx (\frac{1}{2} B_{T\_APj})$$ (promedio de medidas con iperf para cada AP_j)

  Buscando que su uso sea inferior al estimado (promedio) dado su variabilidad y dependencia de estándar (IEEE 802.11b/g/n):

  $$B_{APj\_disponible} \leq B_{m\_APj}$$

Limitando con un umbral de guarda el mismo, para garantizar disponibilidad de uso de canal de AP_j de forma:

$$B_{APj\_usado} \leq B_{APj_{disponible}} - B_{guarda}$$

Lo habitual es que sistemas *best-effort* compitan libremente por el uso del canal:

$$B_{APj\_usado} = \sum F_{AP_j}$$

Diferenciando flujos por categorías (prioritarios (f_p) y no prioritarios (f_{np})) y suponiendo que los prioritarios no superan al disponible:

$$B_{APj\_usado} = \sum F_{AP_j} = \sum f_P + \sum f_{np}$$

$$B_{APj\_usado} = B_{APj\_protegido} + B_{APj\_restante}$$

Haciendo, si fuera posible, que se garanticen los requisitos mínimos para los prioritarios:

$$B_{APj\_mínimo\_prioritarios} = \sum f_P = B_{APj\_protegido}$$

Se puede mantener y tratar de garantizar los requisitos de f_P limitando los recursos para los f_{np}:

$$B_{APj\_restante} = min \sum f_{np}$$

Si el ancho de banda usado lo consideramos una consecuencia de los requisitos de ancho de banda de cada flujo, se puede garantizar un aumento de disponibilidad, si se reducen o limitan las posibilidades de uso de los flujos no prioritarios en beneficio de los prioritarios.

Un ejemplo numérico puede servirnos de explicación. Supongamos que no aplicamos el ajuste de capacidad de guarda ($B_{guarda} = 0$), así como que el promedio medido de ancho de banda máximo de un AP es de 12 Mbps, tendremos que $B_{APj\_disponible} = 12\ Mbps$ y $B_{APj\_usado} = \sum F_{AP_j} < 12\ Mbps$, podemos expresar que:

$$12\ Mbps = \sum f_p + \sum f_{np}$$

Si solo hubiese un solo flujo prioritario que requiriese 6 Mbps, se debe evitar que el ancho de banda utilizado o disponible para los otros posibles flujos no prioritarios no superen los aproximadamente 6 Mbps restantes:

$$B_{APj\_restante} = \sum f_{np} \; < 6\; Mbps$$

Para ello es preceptivo realizar un control de admisión de servicios (flujos). Con este control de admisión se conocen los requisitos de los flujos y con ello distribuir el uso del canal.

En el caso más simple, considerando un solo flujo por cada TER y contando con dos asociados al mismo AP (NF_{TER1} = 1 y NF_{TER2} = 1), podemos reducir el uso que haga del canal uno de ellos para favorecer el flujo del otro terminal. El flujo 1 del terminal 1 podría verse limitado para favorecer al flujo 1 del terminal 2 considerando F_{NP} la relación o conjunto de servicios o flujos no prioritarios y F_P los prioritarios, si:

$$f_1^1 \; \in \; F_{NP}$$

$$f_2^1 \; \in \; F_P$$

Se puede hacer que $f_1^1 \; sea \; limitado \; frente \; a \; f_2^1$ ya sea en bitrate, tamaño de paquetes… En el caso de varios flujos por terminal, podrían igualmente priorizarse unos frente a otros. Buscamos por tanto:

$$\max\{B_{APj\_disponible}\} \; para \; \Delta \; f_P$$

$$\max\left\{disponibilidad \; de \; B_{f_{Pi}^{ki}}\right\}$$

$$\min\{f_i^{ki} \; para \; \forall \; f_{NP}\}$$

- *Minimizar el número de terminales/flujos asociados a cada AP con tráfico prioritario:*

$$\min\{N_{TER\_ASO\_APj}\}$$

- *Maximizar el número de AP detectables por cada terminal (búsqueda de disponibilidad de otros AP):*

$$\max\{N_{AP\_visibles\_TERi}\}$$

Para finalizar relacionamos e identificamos las cuatro tareas que han dirigido este trabajo: la primera de ellas relacionada con la búsqueda de la comunicación más eficiente entre terminales en la misma subred evitando el uso del AP y, de manera especial estas tres que hemos relacionado basados en la optimización de parámetros. De forma específica son:

- Maximizar el uso del canal mediante la reducción de tráfico, evitando el uso del AP en redes WiFi modo infraestructura y cuando las conexiones entre TER pueden hacerse en el mismo canal.
- Minimizar los efectos de tráfico no prioritario sobre la capacidad disponible en el canal para maximizar la disponibilidad para tráficos prioritarios.
- Maximizar la capacidad de los AP mediante la redistribución de terminales entre AP.
- Mejorar la capacidad de los canales mediante la localización de TER y posible reubicación en zonas de intersección (disponibilidad varios AP).

Una vez descrito y formulado el problema de optimización, en los siguientes capítulos detallamos las diferentes actuaciones y propuestas realizadas para mejorar las prestaciones analizando determinados parámetros, su relación con el problema y proponiendo cambios en los mismos de forma analítica o algorítmica, para cada objetivo concreto, así como los resultados obtenidos tras su implementación y experimentación.

Capítulo 4. Propuestas planteadas

En el presente capítulo se realiza una descripción de las cuatro propuestas planteadas para mejorar las prestaciones de WiFi. Las mismas consisten en la posibilidad de conexiones directas entre terminales de la misma subred, el control de admisión y regulación de tráfico desde origen, el traspaso de terminales entre los AP y la aplicación de la localización de los terminales para una distribución más eficiente de los terminales entre los AP disponibles. Se propone una aplicación combinada de las cuatro propuestas en una plataforma multifuncional.

4.1 Modo de operación todo ad-hoc. Conexiones directas

Como punto de partida del desarrollo de esta tesis, tenemos que remontarnos varios años atrás, cuando iniciamos los análisis de las características de las redes WiFi para proponer mejoras en su eficiencia.

Recordemos que haya por el año 2005, las redes inalámbricas IEEE 802.11a/b/g [143] [144] [145] eran ya bastante comunes y podían configurarse de dos maneras principales, conocidas como modo infraestructura y modo ad-hoc. Ya actualmente se cuenta con la variante *WiFi-direct* [146] desarrollada a finales de 2009 y más recientemente redes en modo mesh.

Si hacemos un breve repaso, podemos decir que en la configuración en modo ad-hoc, los terminales forman la red sobre la marcha y se comunican directamente entre pares no requiriendo dispositivos adicionales. Esta topología se puede observar en la Figura 5 del apartado 2.2. Mobile Ad-hoc NETworks (*MANET*) [147] ha desarrollado y estandarizado diferentes protocolos y mecanismos para estas redes. En cambio, en el modo infraestructura, que es el más común, requiere de la existencia de un AP para permitir la comunicación entre los terminales inalámbricos, pero además suele incorporar conectividad con la red cableada. Este AP se constituye en el núcleo central de todas las comunicaciones, o sea todo el tráfico tiene que pasar por su interfaz de red. Además cada terminal debe realizar un proceso de autenticación y asociación al mismo para llevar un registro y poder acceder a los terminales bajo su ámbito. Generalmente la conectividad es con redes Ethernet, DSL u otras. Además según el estándar posibilita la configuración de un sistema de distribución entre diferentes subredes formadas por otros AP. La configuración en modo infraestructura se muestra en la Figura 6 del apartado 2.2.

El modo *WiFi-Direct*, llamado inicialmente WiFi P2P, es similar al modo ad-hoc pues no necesita de AP, ya que diferentes terminales configuran un grupo y uno de ellos se configura como nodo central de dicho grupo manteniendo las comunicaciones directas.

Según el modo infraestructura, si el tráfico está dirigido a un terminal fuera de la subred inalámbrica debe atravesar el AP. Pero en el caso de estar en la misma subred

inalámbrica resulta poco eficiente acceder al AP desde el terminal origen para que este reenvíe el mismo tráfico al terminal destino. Esto representa dos saltos y un aumento del tiempo de envío de cada paquete o tiempo de ida y vuelta, RTT, frente al caso de que las comunicaciones se hiciesen de forma directa, como en el caso de red ad-hoc. Este efecto se visualiza en la Figura 81. Por ello el ancho de banda o la capacidad disponible se ve reducida por el intercambio de paquetes y la confirmación entre los tres elementos participantes, terminal origen, AP y terminal destino [1] [3] [7].

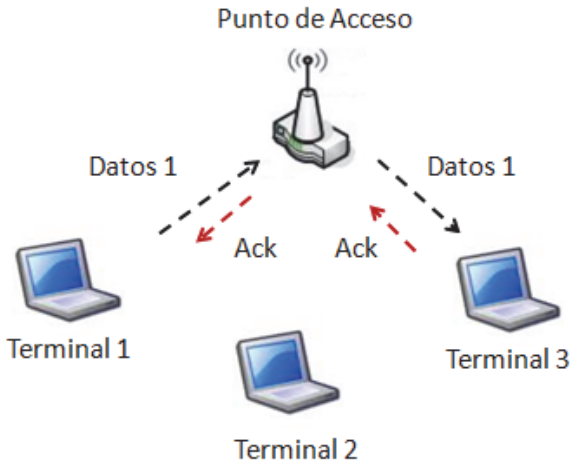


Figura 81. Intercambio de tramas de enlace en modo infraestructura

Hasler et al., en [5], proponen un modelo de red híbrida en el que una red de estaciones base están conectadas por una red cableada dentro de una red ad-hoc. Esta solución presenta desafíos entre las redes celulares tradicionales y redes puras ad-hoc. En ella coexisten la infraestructura cableada y el reenvío multisaltos. Las *redes híbridas* constituyen una solución viable para mejorar las limitaciones de la redes WiFi en modo infraestructura pero permitiendo la conectividad con Internet y las redes ad-hoc. Liu et al., en [6], exponen aportaciones en esa misma línea de investigación.

Considerando la comunicación entre dos terminales de la misma subred inalámbrica de forma directa, y ello implica que no se puede realizar varias transmisiones simultáneas, el RTT se puede obtener como la diferencia de tiempos que hay entre el instante en que se envía el primer bit de la trama de datos y la recepción del último bit de la trama *ACK*; en tal caso tenemos:

$$RTT = t_{ack} - t_{data} \tag{4.1.1}$$

En la Figura 82 se muestran los tiempos en el caso de red ad-hoc frente a modo infraestructura. En el caso ad-hoc tenemos que:

$$t_{ack} = t_4 - t_3 \qquad (4.1.2)$$
$$t_{data} = t_2 - t_1$$

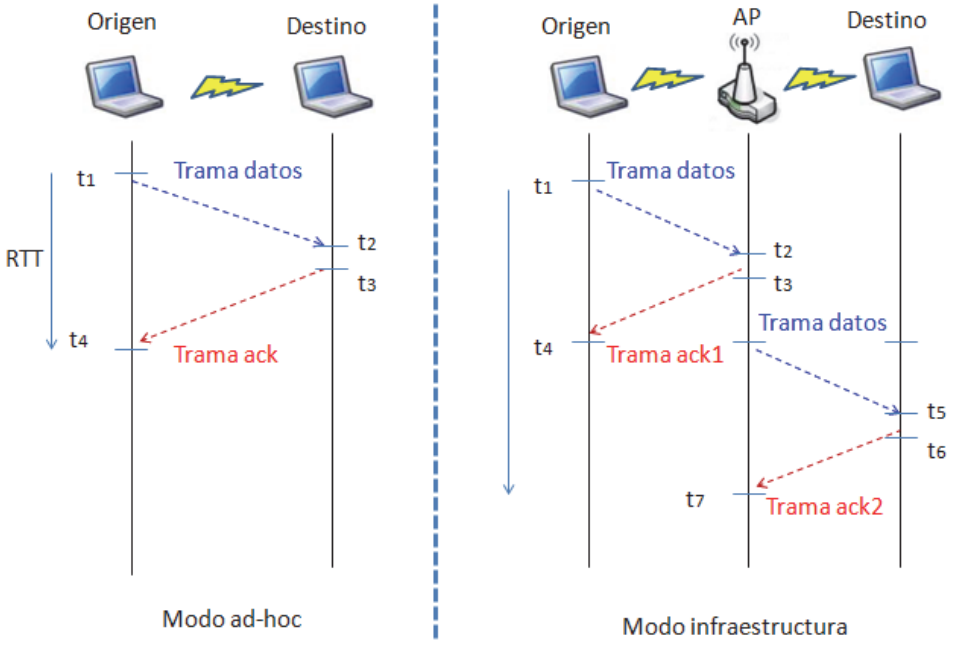


Figura 82. Cálculo de RTT en modo ad-hoc frente a modo infraestructura

En el caso de modo infraestructura tendríamos cuatro fracciones temporales motivadas por el acceso intermedio al AP. Por tanto

$$RTT = t_{ack1} - t_{data(1)} + t_{ack2} - t_{data(2)} \qquad (4.1.3)$$

Considerando los tiempos (4.1.1) entre origen y AP y (4.1.2) entre AP y destino. En este caso el RTT no puede ser utilizado como medida global para determinar el tiempo de ida y vuelta sino como entrega en destino, lo llamamos RTT', en cuyo caso debería complementarse con el tiempo de entrega o de confirmación final, o sea:

$$t_{ack1} = t_4 - t_3 \qquad (4.1.4)$$
$$t_{data} = t_2 - t_1$$
$$t_{ack2} = t_7 - t_6$$
$$t_{data} = t_5 - t_4$$

Despreciando retrasos en espera del canal libre y de proceso en cada dispositivo, tenemos que:

$$RTT' = t_7 - t_1 \tag{4.1.5}$$

y en este caso considerar el tiempo de entrega de cada trama de datos como:

$$t_{entrega} = t_5 - t_1 > t_4 - t_1 \tag{4.1.6}$$

En la línea de aportar soluciones en este contexto, nosotros realizamos diferentes estudios comparativos del uso de conectividad en subredes WiFi en modo ad-hoc y propusimos que todos o alguno de los terminales incorporase la funcionalidad de AP. O sea, que incorporando los interfaces necesarios inalámbricos o cableados se utilice para dar conectividad (hacer de puente) a los terminales en la red WiFi con la red cableada y, en general a Internet u otras subredes. Ello permite mantener las conexiones directas entre pares y, solo en el caso de comunicación con terminales externos, utilizar este terminal "especial" que lo permite. Para realizar las experimentaciones habilitamos un terminal que actúa como un nodo más de la red pero con funciones especiales, y lo denominamos *Linux router*. A diferencia de otras propuestas que se basaban en *multihop*, nosotros configuramos el sistema para comunicaciones directas con el Linux router. La propuesta de usar un terminal con el sistema operativo Linux se debe a ser un sistema operativo abierto, disponer del código fuente y una gran cantidad de servicios, aplicaciones, drivers y funcionalidades que nos ofrece para nuestra investigación. En la Figura 83 se muestra la configuración utilizada.

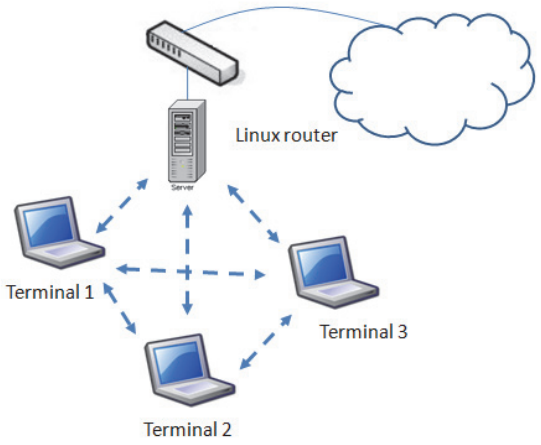


Figura 83. Modo Ad-hoc con salida mediante Linux router

Sabemos que cuanto mayor sea el número de conexiones entre terminales de la misma subred, como hemos analizado, menor capacidad disponible se tiene por la duplicidad de tráfico. Este ancho de banda disponible estimado ($B_{disponible} < B_{m\_APj}$) es inferior que cuando solo existen conexiones de entrada y salida. También sabemos que *Bm_APj* y las posibilidades de cada terminal dependen directamente de la tecnología utilizada (IEEE 802.11b/g/n), la distancia entre los dispositivos y las condiciones del canal. Recordemos que la tecnología WiFi se adapta a las condiciones del canal, de forma que si se aumenta la distancia o sube el nivel de ruido se reduce el bitrate para suavizar su efecto [93]. Si el tráfico es de entrada/salida con el exterior de la subred, la velocidad depende directamente del terminal y del interfaz del Linux router o AP. En cambio, sí es entre terminales de la misma subred, depende de los tres elementos terminal origen, AP y terminal destino. En el caso de habilitarse la conexión directa solo depende de la tecnología del terminal origen y terminal destino local. Con todo esto como la velocidad de transmisión y capacidad depende del tráfico existente y del tiempo de uso del canal, si se reduce el tráfico que atraviesa el AP para conexiones entre terminales de la misma subred o el tiempo de uso del canal, como sería en nuestra propuesta, el ancho de banda disponible se vería mejorado.

En nuestro modelo contextual consideramos que la capacidad del canal puede ser mejorada optimizando los tiempos de uso del canal o el número de tramas que lo atraviesan. Como la capacidad o ancho de banda disponible depende de las tecnologías de los equipos participantes en óptimas condiciones:

$$B_{m\_APj} = f\ (tecnología\ 802.11b, g, n) \tag{4.1.7}$$

Si buscamos maximizar la $Capacidad_{disponible}$ del canal WiFi y consideramos N_{tramas} como el número de tramas que se pueden entregar por unidad de tiempo a un dispositivo destino (incluyendo *ACK*) y $t_{uso\ del\ canal}$ como el tiempo necesario para hacerlo, podemos indicar que:

$$Capacidad_{disponible} = f(N_{tramas}\ , t_{uso\ del\ canal}) \tag{4.1.8}$$

$$Si\ \uparrow N_{tramas}\ |\ \uparrow t_{uso\ del\ canal}\ \Rightarrow \downarrow Capacidad_{disponible} \tag{4.1.9}$$

$$Si\ conexión_{directa} => \downarrow\ t_{uso\ del\ canal}\ y\ \downarrow N_{tramas} => \uparrow Capacidad_{disponible} \quad (4.1.10)$$

Esta propuesta podemos resumirla en que, a pesar de la posible existencia de un Linux router o un AP en una red WiFi, es más eficiente, que cuando la conexión sea entre dos terminales de la misma subred inalámbrica, realizar dicha conexión de modo directo, o sea no atravesando el Linux router o un AP. El resto de conexiones con el exterior deberían realizarse por medio del Linux router. Si los terminales en la misma subred inalámbrica no tuviesen visión o un mínimo nivel de señal recurren al Linux router como elemento intermedio.

Las ventajas añadidas de incorporar algún terminal como Linux router, aparte de ser punto de interconexión con el sistema de distribución, es que puede gestionar otros conjuntos de servicios que generalmente se encuentran en un AP o dispositivo externo sobre la red cableada. Ejemplos de ello son Firewall/*Network Address Translation* (*NAT*) [148], Servidor DHCP [149], Servidor local de DNS [150] , Servidor de autenticación (*RADIUS*) [151]...

Con esta propuesta se considera que si todos o una cierta parte de los terminales de una determinada red WiFi incorporan esta funcionalidad (Linux router), cualquiera de ellos habilitaría conectividad de salida. Ello dotaría de redundancia a la hora de encontrar conectividad con la red cableada y sistema de distribución; y no sería necesario contar con un AP, con la ventaja de tráfico directo entre pares y mejor eficiencia de la subred en su conjunto.

En este situación, los terminales o dispositivos inalámbricos continúan operando en modo ad-hoc preservando las ventajas en cuanto a RTT y solamente cuando necesiten utilizar el sistema de distribución, se especifica la ruta de salida a través del Linux router. Entre los terminales y el Linux router se realizan todas las comunicaciones directamente.

Además, destacamos que cuantos más terminales incorporasen la funcionalidad de Linux router, la carga de tráfico se podría balancear entre los mismos con el beneficio complementario que eso incorpora. En la Figura 84 se muestra esta posibilidad de red con dos Linux router para dar mayor conectividad. El único requisito es que todos los terminales y los Linux router se encuentren en cobertura, hecho que en la red modo infraestructura era necesario entre los terminales y el AP.

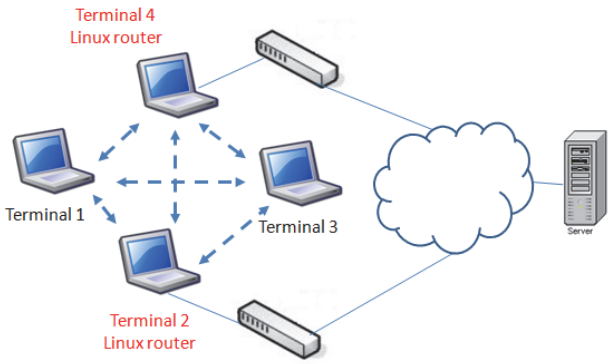


Figura 84. Modo Ad-hoc con dos Linux router con conectividad cableada

Adicionalmente, el o los Linux router se convierten en monitores del tráfico en la red WiFi y pueden aplicar mecanismos de filtrado y control de acceso a la red cableada, dado que todo el tráfico de entrada/salida pasa a través de los mismos. Asimismo podrían ser los dispositivos que configuren la red ad-hoc, cambiando los parámetros o características de la misma para mejora la calidad de las comunicaciones. Igualmente, puede contar con varios interfaces inalámbricos WiFi y con ello gestionar varias subredes. De esta forma puede repartir terminales entre los diferentes canales reduciendo la carga de cada uno de ellos y mejorando por tanto las prestaciones globales.

En el apartado 5.1 se describen las pruebas experimentales realizadas con esta nueva configuración y se analizan los resultados. Queremos resaltar el hecho constatado con el paso del tiempo, de que esta configuración evidentemente tenía que ser posible en las configuraciones futuras de WiFi. Esto se evidencia en *WiFi-Direct* estandarizada en 2009, con posterioridad a la realización de estas actuaciones, en la que además de permitir coexistencia de conexión directa con modo infraestructura se simplifica el proceso de asociación y autenticación.

4.2 Control de admisión y regulación de tráfico en origen

Siguiendo con la serie de actuaciones realizadas, consideramos que dado que la mayor parte de los recursos se encuentran en la red cableada y por extensión en Internet, es necesario centrar el estudio en los AP, o en nuestra configuración con Linux router que haga las veces de dispositivo de acceso. Teniendo en cuenta su posición estratégica y

que todo el tráfico que entra y sale de la subred lo atraviesa, se debería potenciar su funcionalidad en la línea de ser más eficientes en el reparto y uso de la subred. Por ello nos centramos en analizar las características de las tecnologías disponibles.

Remontándonos al año 2007, con la aparición del estándar IEEE 802.11g parecía que era la solución definitiva para los problemas de reducida capacidad de las redes IEEE 802.11. La tasa máxima de datos de nivel físico para esta versión, la más avanzada en aquel momento, era de 54 Mbps [152] [153]. Esta tasa de bits, evidentemente es teórica, pues habría que descontar cabeceros de enlace y físico; y la codificación binaria utilizada determinan que el throughput máximo varía sobre un orden de magnitud el 50%. Asimismo, las condiciones ambientales y el estado de la red, ya sea en modo ad-hoc como en modo infraestructura, son determinantes.

Algunos estudios muestran que los usuarios del estándar IEEE 802.11b [93] no superan los 4 y 5.5 Mbps. Además contamos con nuestras propias evidencias descritas en el capítulo 3. De manera similar, los usuarios de IEEE 802.11a/g pueden alcanzar sobre los 25 Mbps [4] [154]. Algunos vendedores ofrecían productos con más altas tasas de bits [155], pero solo operaban con productos de la misma familia e incluso son incompatibles con otros productos, al no utilizar tecnologías estándar. En aquellos momentos del año 2007, el actual estándar IEEE 802.11n [156] se encontraba en proceso de diseño por un grupo de trabajo de estándares IEEE 802.11, y cuyo objetivo primordial era proveer un alto throughput. Este estándar, si bien en aquel momento aún no estaba ratificado ni estandarizado, ya estaba siendo utilizada por algunos set-top box propietario [157] para retransmisión de la señal de televisión desde un PC o TV.

El MAC para estas redes inalámbricas, ya sea IEEE 802.11b, IEEE 802.11g y IEEE 802.11n, como se comentó en el capítulo 2 opera generalmente mediante un mecanismo basado en contienda. Por ello, los terminales inalámbricos tienen la misma oportunidad para transmitir datos. Esta característica no es óptima para tráfico prioritario, por ejemplo transporte de voz, audio y video, videoconferencia, distribución de flujos media y otros. Por ello el grupo de trabajo IEEE 802.11e [158] estaba desarrollando este estándar para manejar calidad de servicio (QoS), definiendo clases de servicio, mejorando aspectos de seguridad, control de acceso y autenticación. Estas mejoras, en combinación con la mejora de las capacidades del nivel físico incrementaban las prestaciones del sistema.

Ante la carencia de tecnologías más avanzadas, nos planteamos que el uso indiscriminado de la red de forma completamente plana o equitativa era y es ineficiente.

O sea consideramos que se podría determinar y regular diferentes throughput dependientes de la aplicación y el tipo de tráfico para mejorar las prestaciones globales del sistema. Todo esto, además de usar las tasas de datos más altas gracias a nuevas técnicas de codificación, modulación a nivel físico y nuevo subnivel MAC que maneje de forma más óptima la QoS.

Por ejemplo consideremos dos terminales que compiten por enviar datos, uno enviando *streams* de video y el otro enviando paquetes de un archivo mediante *File Transfer Protocol* (*FTP*). En esta situación los MAC resuelven la contienda dando la oportunidad de transmitir a los dos terminales en igualdad de condiciones, salvo si el IEEE 802.11e fuese utilizado, en cuyo caso se priorizaría el tráfico de *streams* de video frente a otro dentro de la misma máquina, pero desconociéndose el tráfico generado por otro terminal. Si no se contase con IEEE 802.11e, que en aquel momento no estaba muy difundido, el acceso era completamente aleatorio sin provisión de QoS. En cualquiera de los casos, para el caso del tráfico FTP, sería deseable que el canal inalámbrico estuviera libre tan pronto como fuera posible.

O sea el ratio de paquetes enviados para el tráfico *stream* debería ser superior que el tráfico FTP para garantizar una mayor eficiencia según los requisitos de cada aplicación. Para hacer esto, los datos FTP deben ser enviados a una tasa máxima de datos de nivel físico y para ello la cantidad de datos entregado por la aplicación que los origina los pasaría al MAC de forma regulada a una tasa menor. En la Figura 85 se muestra el comportamiento natural de cada terminal haciendo uso del canal radio compartido de forma equitativa y, en la parte inferior, el modelo de canal regulado limitando ciertos flujos en beneficio de otros.

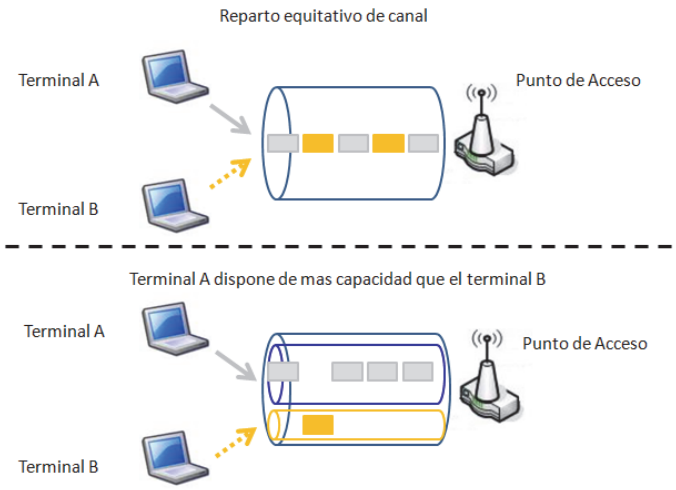


Figura 85. Situación normal y con regulación de uso del canal

Si el ancho de banda teórico disponible en una red IEEE 802.11a/g es de aproximadamente 25 Mbps cualquier terminal inalámbrico con tráfico prioritario, podría contar con una cierta cantidad de la capacidad disponible reservada, por ejemplo se podría plantear una relación de 3 a 1. Esto podría hacerse limitando o regulando el uso del canal a un máximo del 25% de la máxima capacidad del canal disponible, quedando por tanto disponible el 75 % restante. Para el ejemplo anterior, parece evidente limitar el tráfico FTP para que disponga de un máximo de 6 Mbps mientras el flujo *stream* disponga de 18.75 Mbps. Con ello se garantiza el uso compartido del canal pero priorizando unos tráficos frente a otros, concretamente el tráfico *stream* de video requiere de mayores prestaciones de la red para no bajar la experiencia de usuario, frente a la otra aplicación que no tiene esos requisitos especiales. Obviamente esta estimación de reparto de tasa de datos se recalcula dinámicamente dependiendo de los cambios y condiciones de la red.

Además una distribución eficiente debe ver los requisitos de ancho de banda que requiere una comunicación, especialmente multimedia o dependiente del tiempo en general, para que se pueda garantizar el caudal necesario.

Complementariamente, en la documentación disponible, hay otros autores que proponen otras soluciones para mejorar los problemas derivados del limitado ancho de banda (bps) de la red WiFi. En [159] se presenta una solución para extender la reserva de recursos, basándose en la misma solución de QoS extremo a extremo en WAN, pero aplicada en redes WiFi. Otras soluciones, proponen modificar el actual mecanismo MAC para la distribución del acceso entre los terminales participantes mediante la asignación de slots temporales o diferentes frecuencias. Obviamente, esta solución no es compatible con el estándar y representa un cambio radical. Hay otras soluciones para regular el ancho de banda desde la red cableada [160] o desde el AP. En estos casos, el terminal inalámbrico podría seguir afectando a las prestaciones globales de la red y, en especial a la parte inalámbrica, pues según la aplicación que se utilice, esta podría absorber el ancho de banda disponible al no estar regulado desde su origen.

Para garantizar un óptimo y más eficiente reparto compartido del canal inalámbrico según necesidades de cada conexión, nosotros proponemos una solución que consiste en un control de admisión a nivel de aplicación incorporado en los AP, o en nuestros *Linux router* para garantizar una regulación de tráfico. Para nuestra variante o modelo diferenciado, proponemos que esta regulación se aplique en el origen de los flujos o conexiones, pudiendo ser especialmente útil en los terminales inalámbricos o en

cualquiera de los terminales participantes en la comunicación.

La idea consiste en que el AP permite o deniega el acceso a la red a un nuevo terminal WiFi dependiendo del tipo de tráfico que el terminal generaría, y del estado del canal inalámbrico en términos de ancho de banda utilizado y disponible. Los terminales inalámbricos asociados al AP, dinámicamente reajustarían su tasa de datos a nivel MAC de acuerdo con las indicaciones o las informaciones que reciba del AP. Este difundiría las condiciones y limitaciones que deben aplicar cada terminal que hace uso del canal WiFi. El AP actúa como monitor para vigilar y detectar que se mantienen las condiciones especificadas para cada terminal y flujo.

El principal beneficio de esta aproximación, es que es más eficiente que manejar el ancho de banda inalámbrico en comparación con otras soluciones basadas solo y exclusivamente en control de admisión en el AP a nivel MAC y dejar a los terminales libertad de acceso.

Para materializar esta propuesta, nos basamos en la optimización de uso del canal según flujos que se soportan de forma proactiva, mediante un reparto en uso del mismo realizado por cada AP. Concretamente los parámetros que son considerados en este caso son los vinculados para un solo AP o *Linux router* y los diferentes terminales asociados. Los parámetros necesarios son:

- AP o *Linux router*
    - Características del AP: *Car_APj* (ancho de banda teórico y medido: B_{T_APj}, B_{m_APj}, tecnología b/g/n.., frecuencia/canal: *Ch_APj* / *Fr_APj*...), *RSSI*.
- Terminales
    - Conjunto de terminales (C_{TER} , ec. (3.2.1)).
    - Número de terminales asociados (N_{TER})
    - Número de flujos por terminal (NF_{TERi}).
    - Relación de flujos (f_i^{ki}, ec. (3.2.7)).
    - Suma de flujos soportados por AP (f_AP_j, ec. (3.2.8)).
- Flujos prioritarios y no prioritarios (configurable) [F_p , F_{np}].

Control de admisión y mecanismo de regulación de tráfico

El mecanismo que nosotros proponemos está básicamente compuesto de dos

diferentes entidades: el manager o gestor que está ubicado en el AP (o Linux router) y los agentes ubicados en los terminales inalámbricos, y opcionalmente en los terminales en la red cableada.

En la Figura 86 se muestra una representación gráfica de los componentes de software planteado. El sistema propuesto consiste básicamente de tres módulos o elementos:

- Un servidor web a modo de portal cautivo. Después de que un terminal se asocia a un determinado AP (para esta propuesta el terminal se encuentra en el estado e3 (Figura 74)), el usuario de dicho terminal debe solicitar el acceso a través de su browser. A través del mismo debe especificar los parámetros básicos de la comunicación que desea realizar para que pueda ser autorizado. De forma más detallada, una vez el terminal está asociado y dispone de conectividad física y de enlace, debe especificar el tipo de tráfico que genera después del proceso de asociación. Esta información es utilizada por el mecanismo de regulación para determinar las condiciones que debe aplicar a sus flujos.

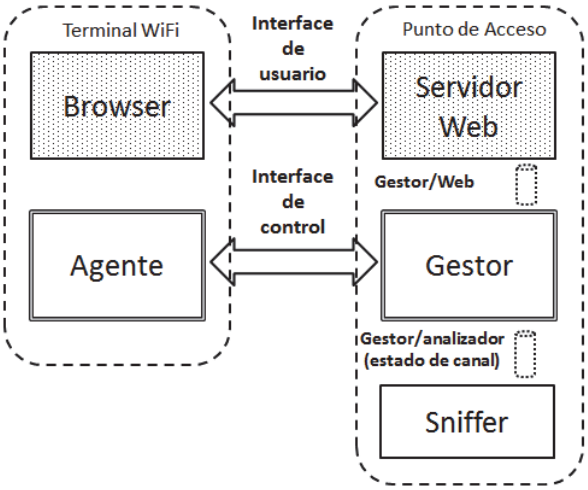


Figura 86. Arquitectura software.

- Un sistema modular basado en modelo Gestor/Agente para configurar dinámicamente la tasa de tráfico para todos los terminales asociados. El gestor se implanta en el AP (nosotros suponemos que el AP es programable, en otro caso podemos habilitar un PC con dos NIC, una inalámbrica para gestionar la subred inalámbrica y comunicar con los terminales inalámbricos y otra cableada (p. e. Ethernet) para conectar con la red cableada e Internet). En este último

caso, podríamos hacer uso del *Linux router* utilizado con anterioridad. Los agentes están distribuidos entre los diferentes terminales inalámbricos que participen de este sistema propuesto (Figura 87). El gestor y cada uno de los agentes se comunican a través de un canal de control enviando mensajes específicos que contienen información útil para la gestión del sistema tal como tasa máxima de datos, tamaño de paquetes máximo... que cada agente debe regular para cada aplicación o flujo.

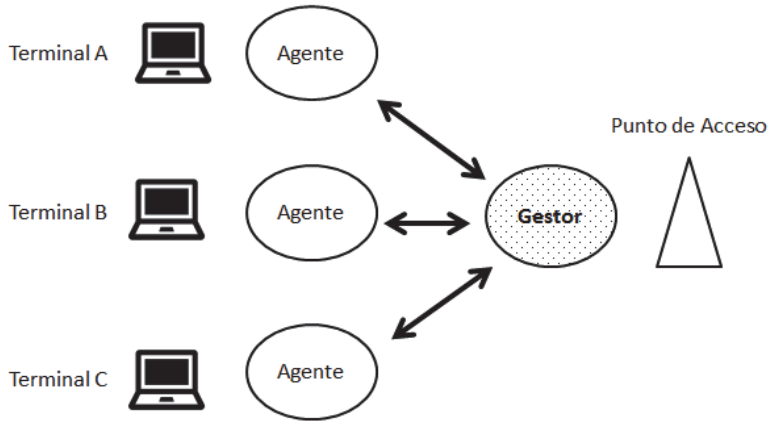


Figura 87. Sistema basado en modelo Gestor/Agente

En la Figura 88 se representa esta nueva configuración lógica con el canal de control que intercambia órdenes entre gestor y agentes.

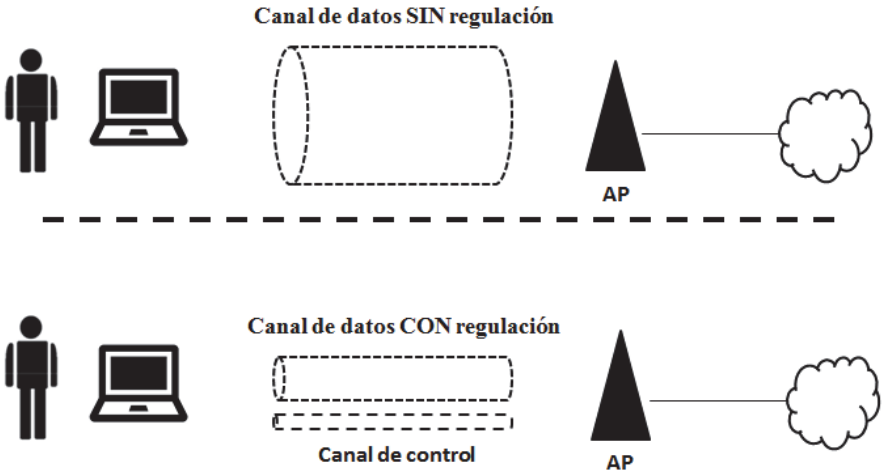


Figura 88. Configuración con canal de control

- Un proceso (sniffer) que monitorice la red en el AP, para llevar un registro de todo el tráfico que fluya por el canal y otro para el que atraviese el AP. Esta información acumulada incluye el número de paquetes/bytes inyectados en la

red inalámbrica durante un tiempo, que podría ser el último segundo, últimos 3 segundos y promedio en últimos 5 segundos. En el caso de usar *Linux router* contamos con las librerías *libpcap* [161] para capturar el tráfico de la red que se inserta y dentro del AP las medidas *iptables/netfilter*.

Toda esta información se usa por el gestor para configurar la tasa de datos para cada flujo y terminal, incluyendo los que accedan nuevamente y soliciten conexión. El *sniffer* (monitor) monitoriza los puertos utilizados para cada terminal inalámbrico, especialmente que tráfico están procesando, bloqueando aquellas comunicaciones que vengan de terminales no asociados y que usen puertos no permitidos. De manera muy especial, se bloquean aquellas comunicaciones que superen el máximo throughput asignado a la misma.

Por otro lado, chequea si hay uno o más terminales inalámbricos no asociados usando el mismo canal o adyacente y están generando datos. Recordamos que en el caso de IEEE 802.11b/g solo hay tres canales que no se solapan entre ellos. Con esta última opción, el AP tendría conocimiento de la presencia de terminales u otros AP que puedan reducir las prestaciones del sistema, ya que sus comunicaciones pueden colisionar con las comunicaciones de los terminales asociados a la red que se pretende regular.

Es evidente, que según las especificaciones del estándar IEEE 802.11, no se puede evitar el tráfico intrusivo de cualquier otro terminal de los que no se tiene acceso ni control. Pero, si en cambio, se puede habilitar desde el AP un cambio de canal a otro menos congestionado para reducir sus efectos.

El proceso que se sigue tiene cuatro fases que hemos denominado:

Fase 1: control de admisión y registro
Fase 2: regulación
Fase 3: sondeo o polling
Fase 4: actualización, time-out o bloqueo

En la Figura 89 ilustramos la fase 1 y la fase 2 con las diferentes acciones y mensajes intercambiados entre el terminal inalámbrico y el AP. Destacamos que en la fase 1, se considera solo interacción entre el cliente web y el servidor web para intercambiar información vía *http* sobre la conexión. Las interacciones se corresponden con los números (1), (2), (3) y (9). El paso (1) y (2) representan la petición y descarga

desde el servidor web de la página de control de acceso (registro de usuario, clave y, especialmente servicio, mediante su denominación o especificando sus requisitos de bitrate,…). Una vez el usuario entrega los datos solicitados, con (3), el servidor web se intercomunica con (4) con el gestor y se pasa a la fase 2. En esta fase, el Gestor toma el control para determinar el estado, definir si es necesaria regulación o no y se notifica la decisión al agente (6). Una vez se aplican las acciones solicitadas, se respondería con (7) y se confirma o no la actuación del agente (7'). Posteriormente, tras su procesado se resuelve a través del servidor web (8) y la respuesta visual al cliente web con (9).

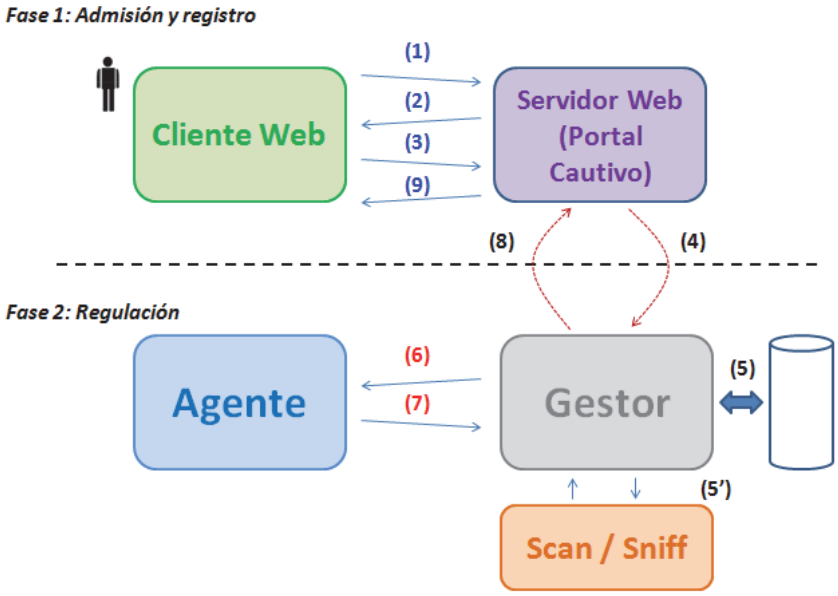


Figura 89. Intercambio de mensajes para las fases 1 y 2

En la fase 2 existe un paso intermedio, numerado con (5), que se corresponde al registro en BD local con los datos del terminal, conexión y tipo de flujo habilitado, regulación (caso de existir) y tiempo asignado a la misma. Igualmente, el paso 5', opcional, se corresponde con la consulta al sniffer sobre el estado del canal.

En la Figura 90 se muestra la fase 3. Esta representa el intercambio de información entre el gestor y los agentes para detectar su presencia con los mensajes de sondeo (polling) periódicos, que son respondidos convenientemente. Si no se reciben los mensajes (11) la comunicación sería bloqueada.

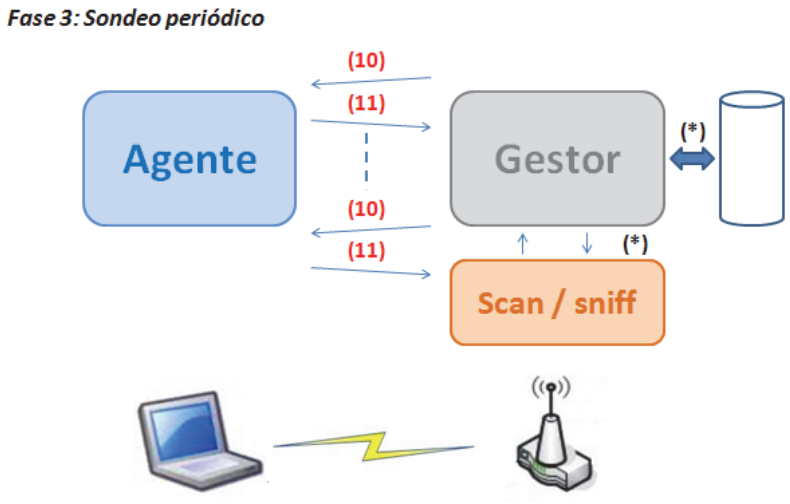


Figura 90. Intercambio de mensajes para la fase 3 (sondeo periódico)

Finalmente la fase 4, mostrada en la Figura 91, representa la actualización del estado de las conexiones (12) y sus regulaciones motivadas por la salida o entrada de otras conexiones o terminales. Igualmente puede ser provocada una finalización de la conexión regulada motivada por el vencimiento del tiempo de conexión (14). Todas estas comunicaciones deben ser confirmadas ((13) y (15)), dado que en caso contrario la comunicación sería inmediatamente bloqueada.

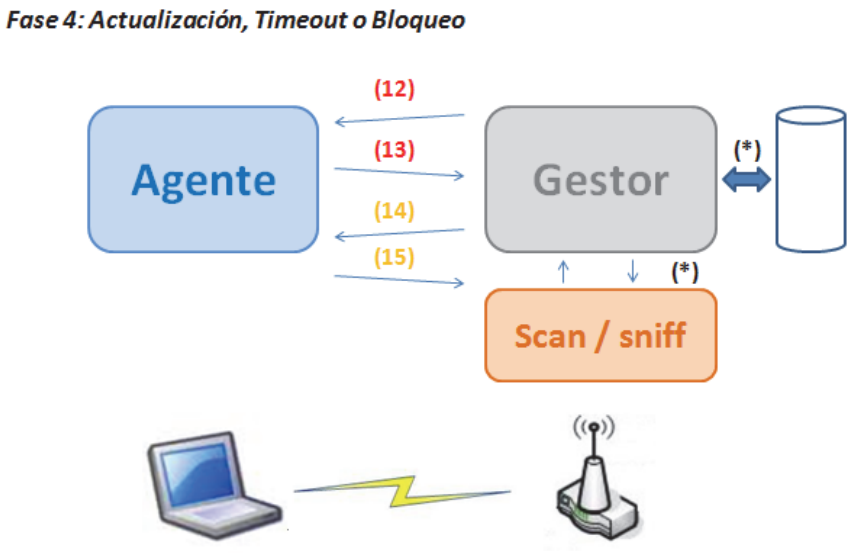


Figura 91. Intercambio de mensajes para la fase 4 (Actualización o bloqueo)

Ante cualquier falta de respuesta desde cada agente al gestor, o se supere la tasa de regulación a aplicar, el gestor procedería a bloquear la conexión relacionada. En la Figura 92 se muestra esa situación.

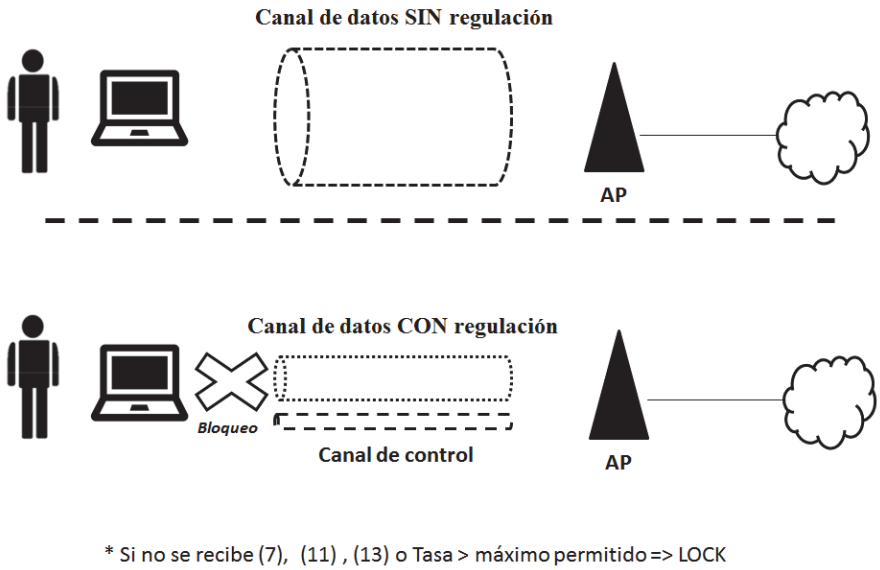


Figura 92. Situación de bloqueo ante ausencia de respuesta o superar restricciones

En la Figura 93 se muestra a modo de organigrama las diferentes acciones que realizan tanto un terminal inalámbrico, que solicita una asociación hasta que la misma es aceptada o rechazada por el AP seleccionado.

A continuación se describen cada uno de esos pasos y cuál de los módulos está afectado:

1. El cliente web (browser) del usuario se conecta al servidor web de AP a través de su portal cautivo. Este sería la única vía de comunicación o interfaz con el usuario del terminal. El resto de mensajes se intercambia con el agente correspondiente por otro canal de comunicación propio. La respuesta del servidor web sería una ventana donde se le solicita al usuario que introduzca su nombre de usuario, una clave de acceso (*password*) y que especifique que tipo de servicio pretende utilizar. En nuestra propuesta, el usuario puede seleccionar una de las aplicaciones más habituales.
2. La identificación anterior es analizada por el servidor para detectar que es correcta.
3. El servidor podría denegar el acceso a la red cableada o a Internet, si el nombre de usuario o su clave no fuese correcto y, con ello, se genera un primer control de admisión.

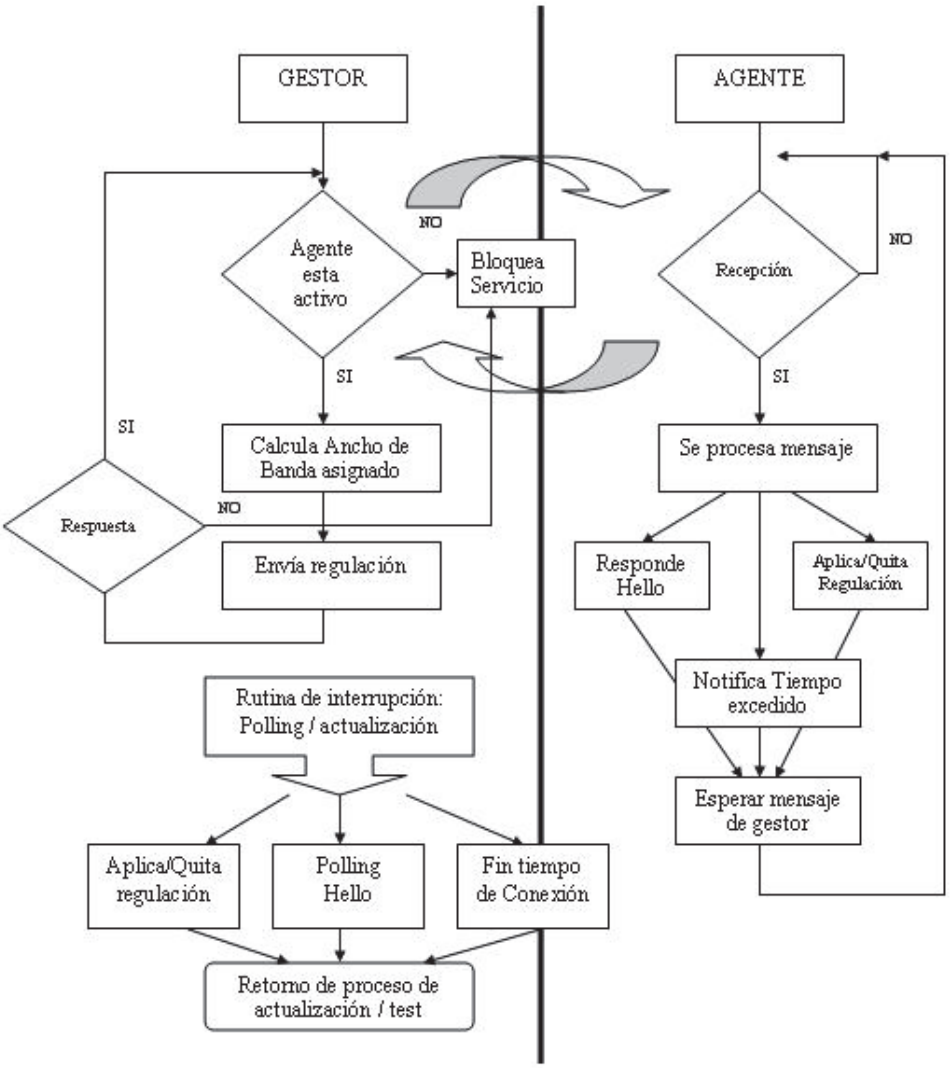


Figura 93. Pasos para regular el tráfico por el acceso del terminal inalámbrico

4. Si todo está correcto, el servidor web notifica al gestor el tipo de servicio solicitado por el terminal entrante o presente ya en la subred, y espera su respuesta.
5. El gestor consulta el estado del canal y el registro interno que contiene información sobre otros flujos gestionados por el mismo.
6. El gestor puede solicitar información al sniffer, que constantemente monitoriza el trafico RF, antes de dar una respuesta y asignar las restricciones, si fuesen necesarias, o las condiciones en las que accede al canal.
7. Con toda la información disponible, el gestor decide si los requisitos básicos mínimos necesarios para el tipo de servicio solicitado se pueden garantizar o por

el contrario, algún tipo de regulación tiene que ser aplicada en el propio terminal así como en el resto de terminales.

8. Este último caso sería de aplicación, cuando el tráfico solicitado requiera cierta capacidad del canal y los otros flujos no sean tan exigentes o no dependan del tiempo. Por ejemplo si este flujo tiene alta prioridad en comparación con los existentes.
9. Toda la información se empaqueta en un formato y enviada por el canal de control al agente del terminal solicitante y el correspondiente mensaje al resto de terminales por medio de sus agentes. El gestor envía los datos con la tasa de bits que el agente debe pasar al nivel MAC para regular el tráfico de salida.
10. El agente debe responder aceptando las condiciones o en caso contrario, podría desistir de hacer la comunicación.
11. Si el agente no responde aceptando las condiciones, el gestor bloquearía el acceso a dicho terminal y sería notificado al usuario a través de otra ventana en el browser.
12. Si la respuesta es aceptada, se habilita el reenvío de flujos con las funciones *iptables* [162].

Una vez el terminal inalámbrico inicia la comunicación de datos, el gestor regularmente chequearía que el agente esté activo (en ejecución) y que aplica la regulación y condiciones indicadas por el gestor, ayudado por el monitor de canal. Si no estuviese activo o no se cumpliesen las condiciones especificadas inicialmente, el servicio sería bloqueado en el AP (o Linux router).

En nuestra propuesta de implementación, el agente en cada terminal configura la tasa de bits desde el propio MAC de cada terminal usando las funciones de Control de Tráfico, implementadas en Linux, que ha sido la plataforma de pruebas escogida. Gracias al mismo, podemos definir diferentes tipos de políticas, clasificación de tráfico, regulación de tasa… En las versiones preliminares hemos usado un filtro TBF [163] para restringir el bitrate en el MAC del terminal emisor.

El conjunto de mensajes (*Protocol Data Unit* (*PDU*)) que hemos definido para su uso en el canal de control y materializar esta solución se relacionan en la Tabla 23.

Tabla 23. Relación de mensajes de control

PDU	Sentido	Significado
HELLO	Gestor → Agente	Sondeo a agente para confirmar presencia y solicitar condiciones. [Mensaje (10) Fig. 90].
HELLO_ACK	Agente → Gestor	Confirma presencia de agente y confirma condiciones [Mensaje (11) Fig. 90].
UPDATE	Gestor → Agente	Indica condiciones de regulación que agente debe aplicar para el servicio especificado. [Mensajes (6) Fig. 89 y (12) Fig. 91].
UPDATE_ACK	Agente → Gestor	Confirmación de aplicación de condiciones especificadas en mensaje *Update* [Mensajes (7) Fig. 89 y (13) Fig. 91].
UPDATE_NACK	Agente → Gestor	Notificación desde agente que condiciones especificadas en mensaje *Update* no pueden ser aplicadas. Esta respuesta provoca un bloqueo de servicio en Gestor [Mensajes (7') Fig. 89 y (13´) Fig. 91].
TIME_OUT	Gestor → Agente	Notificación al agente que ha vencido el tiempo permitido para el servicio regulado [Mensaje (12) Fig. 91]
INFO_REQUEST	Gestor → Agente	Petición desde gestor al agente sobre el estado actual de su regulación de tráfico (mensaje para administración y depurado)
INFO_REPLY	Agente → Gestor	Notificación de estado actual de regulación en terminal (mensaje para administración y depurado)

En cuanto a la información que intercambian el servidor web y el cliente web tras la petición Web segura (*https://*) correspondiente (se propone un servidor web seguro sobre *Secure Socket Layer/Transport Layer Security* (*SSL/TLS*) consiste básicamente en una página web estática soportando un formulario como proceso inicial (mensajes (2) y (3) de la Figura 89). Mediante el mismo, el usuario se tendría que autenticar como control de acceso y admisión, especificando de manera prioritaria el servicio por su nombre o por el puerto que utiliza. En una primera versión solo se aplica regulación por puertos de servicios prioritarios y no prioritarios. En cuanto al mensaje final (9) de la fase 1,2 sería el resultado de la ejecución de los scripts desarrollados para interconectar con el gestor mediante (4) y su respuesta (8). Para la interacción entre el scripts de la página de acceso y el gestor se realiza mediante la técnica de comunicación interprocesos, ampliamente utilizada en sistemas *Unix/Linux*.

En la Tabla 24 se muestra el pseudocódigo general del gestor dividido en dos grandes bloques: el núcleo del gestor y la parte de sondeo de los agentes.

Tabla 24. Pseudocódigo del Gestor

Algoritmo 1. Pseudocódigo Gestor (núcleo central)

```
1: While (true)
2:   Se esperan peticiones desde admision.cgi (no bloqueante)
3:   If solicitud es aceptada then
4:       Analiza tipo de flujo (fp o fnp)
5:       Se calcula B_disponible y requisito de flujo entrante
6:       If fp then
7:           No aplica regulación (opcional aplicable por configuración)
8:           if  rate solicitado > B_disponible then
9:               Mensaje agente requisitos no garantizados
10:      else  /* fnp */
11:          Se calcula regulación a aplicar a f_np entrante
12:          Se calcula nueva regulación a aplicar al resto de f_np
13:      end if
14:      Comunica mensaje o regulación a agente (UPDATE) (agente-f_np <- regulación)
15:      If no hay respuesta (UPDATE_ACK) then
16:          No se activa conexión
17:      else
18:          Se activa conexión
19:          Se añade entrada a registro de conexiones
20:          Se marca tiempo (duración de sesión)
21:      end if
22: end if
23: If hay conexiones activas then
24:      Se activa alarma de sondeos
25:      Se llama a sondeo de agentes según BD registro. (bloque conexiones entrantes)
26: end if
27: If no hay conexiones activas then
28:      Se desactiva alarma de sondeos
29: end if
30: end while
```

Algoritmo 2. Módulo de Sondeo

```
1: while hay entradas en BD registro do
2:       Se lee BD registro
3:       Se transmite HELLO a cada agente
4:       If respuesta no es HELLO_ACK o  no hay respuesta en t then
5:               Se bloquea conexión, Elimina entrada registro, Nueva regulación resto
6:       end if
7:       If time out then
8:               Se comunica mensaje time-out,
9:               Se bloquea conexión, Elimina entrada registro, Nueva regulación resto
10:      end if
11:      Se consulta sniffer (si está presente)
12:      If rate > regulado then
13:              Se comunica mensaje overrun,
14:              Se bloquea conexión, Eliminación de registro, Nueva regulación resto
15:      end if
16: end while
```

Adicionalmente a las anteriores funciones, se incorporan dos características muy importantes a esta propuesta e implementación. Ambas están muy relacionadas con el estado del canal y la toma de decisiones.

La primera de ellas permite que el gestor realice consultas a los agentes sobre el estado de cada terminal, concretamente conozca todas sus características técnicas de su interface y su situación actual (tecnologías, potencia, configuración MAC, estadísticas de tráfico,..). Para habilitar esta funcionalidad, se hace uso de un mensaje que hemos denominado INFO_IFACE_REQUEST y su correspondiente mensaje de respuesta INFO_IFACE_REPLY. Con los datos retornados desde el agente, el gestor tendrá un mejor conocimiento de cada terminal para la toma de decisiones posteriores relacionadas con la regulación o condiciones del canal.

La segunda función posibilita que el gestor reconfigure el canal de trabajo del AP o LRW sobre el que opera. Esta función se activa, si el estado del canal se encuentra excesivamente saturado por otras redes o equipos operando en el mismo canal, que pueden interferir o impedir alcanzar el objetivo buscado con esta propuesta de regulación y control. Esta función está muy relacionada con el rastreo de canales (scanning) y la disponibilidad del *sniffer*, pues si se detecta tráfico no regulado, se busca un canal que este libre o en mejores condiciones. Recordemos que cualquier equipo WiFi puede configurar una red en el canal que desee pudiendo afectar al tráfico de canales o subredes existentes. Los mensajes correspondientes son CHANGE_CH_REQUEST y CHANGE_CH_REPLY. El proceso consiste en que si el gestor, tras el análisis del estado de canal utilizado, detecta unas condiciones inadecuadas, notifica a todos los agentes que pretende cambiar de canal, los agentes responden confirmando su recibo y, trascurrido el tiempo indicado, el gestor cambia de canal, así como los agentes.

En la Tabla 25 se muestran los mensajes vinculados a estas dos funcionalidades adicionales.

Tabla 25. Relación de mensajes de control adicionales

PDU	Sentido	Significado
INFO_IFACE_REQUEST	Gestor → Agente	Solicitud de información de estado del terminal
INFO_IFACE_REPLY	Agente → Gestor	Respuesta con estado del terminal y características
CHANGE_CH_REQUEST	Gestor → Agente	Notificación de cambio de canal (modo ad-hoc)
CHANGE_CH_REPLY	Agente → Gestor	Confirmación de recibo de cambio de canal (ad-hoc)

En esta propuesta solo contemplamos el cambio de forma abrupta, al proponerla para el modo de funcionamiento ad-hoc, si algún terminal queda aislado, reinicia asociación.

Para calcular la tasa permitida de envío de datos para cada terminal, es necesario conocer el ancho de banda WiFi disponible medido para el APj de que se trate ($B_{m\_AP_j}$), parámetro descrito en el apartado 3.2; y lo simplificamos como B_m. Como ya se comentó previamente, siempre sería menor que la tasa teórica del nivel físico del estándar que se utilizase, dado las restricciones insalvables existentes en la capa física.

Para evaluar el caso de máximas prestaciones, nosotros usamos la herramienta *iperf* [123] para obtener este valor, y luego analizamos que interfaz IEEE 802.11b, g, n... incorpora el cliente específico y el AP. Tenemos que resaltar que el ancho de banda que nosotros calculamos es estimado, pues en cada momento puede variar dependiendo de las condiciones del canal y factores medioambientales. Consideramos que hacer múltiples medidas previas a modo de aprendizaje y sacar una media podría ser adecuado, como evidenciamos en el capítulo 3.

Dado que estamos diferenciando tráfico prioritario de otros no prioritarios, agrupamos la demanda de ancho de banda de los prioritarios en B_P (ancho de banda requerido para flujos prioritarios). De igual manera denominamos B_{NP} para el resto de flujos no prioritarios de forma que podríamos aproximar:

$$B_m \sim B_P + B_{NP} \tag{4.1.11}$$

Para realizar una primera distribución o regulación hemos seguido una metodología basada en que si B_m es el ancho de banda obtenido por *iperf* para conexión b o g, podría buscarse el que al menos 2/3 de B_m se podría reservar para una comunicación prioritaria (dependiente del tiempo y no de muy alta calidad) frente a otra que no lo fuese, y para esta última solo el 1/3 restante de B_m. Si hubiese más de una comunicación no dependiente del tiempo, entre ellas se reparten de modo best-effort el uso de esa fracción, para no reducir el resto de ancho de banda "reservado" para el flujo prioritario. Evidentemente saber exactamente el ancho de banda disponible [46] [47] es un problema bastante documentado, aunque nosotros lo aproximamos al caso medido.

Este caso fue el más simple que evaluamos y como se puede observar, no tiene en cuenta las necesidades específicas de cada flujo sino que el reparto esta prefijado y estático. Ya en el capítulo 2, se analizaron los requisitos básicos para los formatos de video más habituales, en los que para MPEG-4 y SDTV eran aceptables. En sistemas

con IEEE 802.11b que no se superan en general los 5 Mbps de capacidad medida ($B_m \approx$ ½ B_T) y con la distribución anterior tenemos:

$$B_P = 2 \times {}^{B_m}/_{3} = 2 \times {}^{5\ Mbps}/_{3} = 3.3\ Mbps \qquad (4.1.12)$$

$$B_{NP} = {}^{B_m}/_{3} = {}^{5\ Mbps}/_{3} = 1.6\ Mbps$$

Esta distribución es óptima en aquellos casos en los que solo se realiza una comunicación de video y esta generalmente requiriese velocidades inferiores a 1 Mbps, salvo alguna con alta calidad, en la que no siempre los resultados eran aceptables. Es evidente que con 3.3 Mbps es suficiente para una o dos comunicaciones con bitrate que ronden 1 Mbps, por ello habilitamos otras comunicaciones prioritarias que compartiesen estos 3.3 Mbps. Tengamos en cuenta que hoy en día el estándar IEEE 802.11b se mantiene por simple compatibilidad y sus prestaciones son demasiadas bajas para soportar la mayoría de las comunicaciones actuales, y en especial los requisitos multimedia.

En el caso de AP con IEEE 802.11g tendríamos un ancho de banda medido aproximado de 25 Mbps ($B_m \approx 1/2\ B_T$) siempre que contemos con dispositivos en los terminales operando en el mismo estándar, pues si no fuese así, probablemente estaríamos en las tasas anteriores, como se ha evidenciado empíricamente. Para el caso de sistemas IEEE 802.11g tendríamos la expresión (4.1.13):

$$B_P = 2 \times {}^{B_m}/_{3} = 2 \times {}^{25\ Mbps}/_{3} = 16.6\ Mbps \qquad (4.1.13)$$

$$B_{NP} = {}^{B_m}/_{3} = {}^{25\ Mbps}/_{3} = 8.3\ Mbps$$

En este caso la distribución inicial puede ser alterada con mucha mayor capacidad de reparto y obviamente las condiciones son más eficientes para ambos flujos. Hemos de recordar, que los flujos que consideramos no prioritarios podrían ser verdaderos "devoradores" de ancho de banda si no se le aplica regulación, por ejemplo peer-to-peer, FTP...

Una variante o modificación que permite ser más flexibles según necesidades o condiciones incorporamos para cuando haya múltiples flujos prioritarios. En estos casos

la expresión anterior se adapta para permitir cambios dinámicos mediante la expresión (4.1.14) en la forma:

$$B_P = 2 \times \frac{B_m}{3} + n \times Ref \qquad (4.1.14)$$

$$B_{NP} = \frac{B_m}{3} - n \times Ref$$

Donde *Ref.* es un patrón de referencia de 100 Kbps (o configurable) y n sería el número de terminales que demanden flujos prioritarios. La razón consiste en aumentar la disponibilidad en centenas de kilobits por segundo para flujos prioritarios y reducirlos de los no prioritarios, si los primeros detectan limitaciones en sus prestaciones: por la aparición de nuevos flujos, porque bajen las condiciones del canal o porque empiece a deteriorarse la calidad de las comunicaciones.

Estas dos anteriores formas de distribución, fijas o ligeramente dinámicas es evidente que son elementales y no se ajustan a los diferentes casos. Por ello se propone considerar las demandas reales de cada flujo prioritario para garantizar el mismo en la última versión del sistema. Asimismo, B_P se calcula como la suma de las demandas de ancho de banda de cada flujo prioritario, f_P para cada AP de que se trate:

$$B_P = \sum f_P \qquad (4.1.15)$$

Bajo esta premisa, se debe limitar el valor de B_{NP} que permita no reducir el ancho de banda disponible total en la forma:

$$B_{NP} = B_m - B_P \qquad (4.1.16)$$

Conociendo B_m y B_P se podría estimar el valor aproximado de B_{NP} que no debe superarse para garantizar cierta capacidad disponible. Recordemos nuevamente que como el valor de B_m es bastante variable, es recomendable obtenerlo como la media de múltiples pruebas o medidas sin carga en la subred WiFi. Tras diferentes pruebas consideramos que podría ajustarse mejor la expresión (4.1.16) si añadimos un margen de control de aproximadamente un 10% inferior (consideramos una variable configurable de optimización) y con ello minimizar el efecto de una estimación al alza del valor de B_m, por tanto modificando con (4.1.16) con esta aproximación tenemos:

$$B_{NP} \sim (B_m - 10\%\, B_m) - B_P = 0.9\, B_m - B_P \qquad (4.1.17)$$

Nuestra propuesta de regulación de flujos de forma básica en forma de pseudocódigo es como el mostrado en la Tabla 26.

Tabla 26. Pseudocódigo para limitación de flujos desde AP

Algoritmo 3. Pseudocódigo básico de regulación

```
1:    If ∃f_P then
2:        If f_P || Σf_P > 0.9B_m then
3:            Reserva no garantizada
4:            Notificación a TER con f_P
5:        else
6:            B_NP ≈ 0.9B_m - Σf_P
7:            Aplicar regulación para de f_NP en TER_i según B_NP
8:        end if
9:    else
10:       No aplicar regulación
11:   end if
```

Si los requisitos superan las limitaciones de *Bm* disponible, nuestra propuesta aplica reducciones equitativas, salvo que se realicen otras configuraciones manuales aplicadas por el administrador de la misma durante el arranque del gestor. Sería poco eficiente priorizar una comunicación solo por sus requisitos de bitrate frente a otras sin considerar la importancia o relevancia de la misma, en la que la intervención del administrador o usuario puede ser indispensable.

Como generalización de esta propuesta de regulación distribuida del tráfico, presentamos una formulación matemática definiendo unos coeficientes de regulación para aplicar a cada flujo en cada terminal y hacemos uso de los parámetros especificados en el apartado 3.2. Para ello nos basamos en la parametrización e incluimos el concepto de tráfico en los terminales como el conjunto de paquetes entrantes o salientes a los terminales. En la Figura 94 se muestra el concepto de tráfico y flujos.

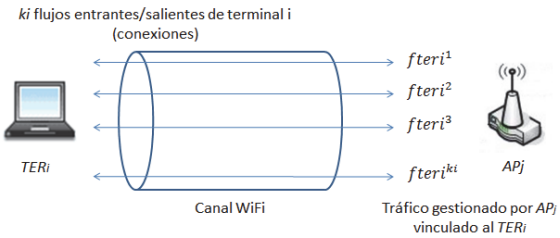


Figura 94. Esquema de tráficos y flujos

Sea T_{TERi} el tráfico de TER_i y sea T_{APj} el tráfico entrante o saliente por un determinado AP_j (al que se supone que existen *n* terminales asociados) entonces se cumple que:

$$T_{APj} = \sum_{i=1}^{n} T_{TERi} \tag{4.1.18}$$

Recordando la expresión (3.2.7) del apartado 3.2 los flujos de cada terminal se pueden representar como:

$$f_{TERi} = \{f_i^1, f_i^2, \ldots\ldots, f_i^{ki}\}$$

Ya que cada terminal podría tener un número de flujos diferente k_i podemos considerar que el T_{TERi} está constituido por *ki* flujos de tráfico (f_i^{ki}, k_i=*1..p,* $p \geq 1$) heterogéneos (vídeo, audio, *best effort*...), en general. Esto es,

$$T_{TERi} = \sum_{ki=1}^{p} f_i^{ki} \tag{4.1.19}$$

Con lo cual, partiendo de la ecuación (4.1.18) y sustituyendo en ella la ecuación (4.1.19), tenemos:

$$T_{APj} = \sum_{i=1}^{n} \sum_{ki=1}^{p} f_i^{ki} \tag{4.1.20}$$

Lo cual explica la contribución de tráfico de cada terminal y sus flujos en el AP al que se vinculan los diferentes terminales. Esta contribución se puede representar con una matriz cuyas *n* columnas representan los T_{TERi} de los terminales y las k_i filas todos

los flujos por cada terminal (k_i es la suma de todos los valores de p de cada T_{TERi}). Si denominamos $\propto_i^{ki} \quad (0 \leq \propto \leq 1)$ un coeficiente de reducción del tráfico vinculado a cada f_i^{ki}, la regulación se puede expresar como:

$$f_i^{ki} = \propto_i^{ki} \; B_m \tag{4.1.21}$$

Lo cual indica que cada flujo solo podría hacer uso de una proporción $\propto_i^{ki}$ de la capacidad total máxima del canal. Con lo cual, sustituyendo f_i^{ki} en (4.1.20) y factorizando:

$$T_{AP_j} = B_m \sum_{i=1}^{n} \sum_{ki=1}^{p} \propto_i^{ki} \tag{4.1.22}$$

Siendo:

$\propto_i^{ki} = 0$	el valor para un f_i^{ki} no permitido.
$0 < \propto_i^{ki} < 1$	el valor para un f_i^{ki} regulado. Los valores próximos a 1 se asignan para flujos de vídeo/audio y bajos para los *best-effort*.
$\propto_i^{ki} = 1$	el valor para un f_i^{ki} no regulado.

Lo que se pretende representar es que, de forma general, se pueden aplicar mecanismos de regulación de flujos individualmente para reducir su efecto sobre los restantes, y de esta manera minimizar los $\propto_i^{ki}$ vinculados con tráfico no prioritarios y maximizar (no regular) los tráficos prioritarios.

Esta regulación se puede representar como una *matriz de coeficientes de regulación de tráfico,* cuyas n filas representan los terminales (*TERi*) asociados a un AP y las columnas representan los flujos de cada terminal. Esta matriz puede alcanzar las p columnas para aquel o aquellos terminales que tenga el mayor número de flujos f_i^{ki}.

En la Tabla 27 se muestra la representación que relaciona terminales y flujos asociados, así como una representación de esta matriz de coeficientes se muestra en la Figura 95.

Tabla 27. Representación de terminales y flujos con coeficientes de regulación

	$k_i = 1$	$k_i = 2$	…..	$k_i = p$
TER_1	$f_1^1 = \propto_1^1 B_R$	$f_1^2 = \propto_1^2 B_R$	…..	$f_1^p = \propto_1^p B_R$
TER_2	$f_2^1 = \propto_2^1 B_R$	$f_2^2 = \propto_2^2 B_R$	…..	$f_2^p = \propto_2^p B_R$
…..	…..	…..	…..	…..
TER_i	$f_i^1 = \propto_i^1 B_R$	$f_i^2 = \propto_i^2 B_R$	…..	$f_i^p = \propto_i^p B_R$
…..	…..	…..	…..	…..
TER_n	$f_n^1 = \propto_n^1 B_R$	$f_n^2 = \propto_n^2 B_R$	…..	$f_n^p = \propto_n^p B_R$

Operando de forma distribuida entre el gestor y los agentes sobre esta matriz de tráfico, se puede alcanzar una mejor distribución del uso de cada canal por los distintos terminales. Para ello es necesario que el gestor averigüe el estado del mismo de forma regular.

$$\begin{pmatrix} \propto_1^1 & \propto_1^2 & \dots & \propto_1^p \\ & \propto_2^2 & & \dots \\ \dots & & \dots & \propto_{n-1}^p \\ \propto_n^1 & \propto_n^2 & \dots & \propto_n^p \end{pmatrix}$$

Figura 95. Matriz de coeficientes de regulación de tráfico

Como en el caso de las medidas experimentales del apartado anterior, en el apartado 5.2 se analizan los resultados empíricos de esta propuesta.

4.3 Traspaso de terminales entre AP

Esta nueva propuesta está también relacionada con los problemas de un uso compartido de un canal o celda WiFi. Está contrastado, que en este modo de operación existen restricciones para aplicaciones demandantes de ancho de banda, en especial aquellas dependientes del tiempo cuya QoS no se puede garantizar.

Como ya hemos comentado, en la mayor parte de las aplicaciones o servicios actuales (web estáticas informativas, correo electrónico y transferencia de archivos), la velocidad en la que debe ser recibida la información no es tan importante frente a la integridad de la misma. Por contra para servicios dependientes del tiempo, como por

ejemplo transmisión de video, audio o ambos (VoIP, VoD, videoconferencia, video-vigilancia...), la velocidad o throughput, pérdida de paquetes, retraso y jitter sí son aspectos determinantes que afectan muchísimo a su calidad, y aun en muchos casos no están garantizados en la mayoría de los productos disponibles.

Es en este contexto y como nueva aportación de esta tesis, se presenta otra propuesta en la misma línea y complementaria a las anteriores que consiste en poder hacer unas distribuciones más idóneas de los terminales entre los AP disponibles, cuando sean accesibles a los terminales. Este planteamiento podríamos verlo como una optimización de la asociación de los terminales más eficiente de forma que se maximice la capacidad disponible de los AP para los terminales. Nosotros consideramos que en redes WiFi donde haya varios AP pueden producirse cambios de AP o "*traspasos*" de terminales vinculados a ellos de forma controlada por los AP, obviamente dentro de sus zonas de cobertura comunes. Este traspaso se realizaría en base al cálculo de la disponibilidad del canal (ancho de banda disponible (bps)), número de terminales, estado del canal...). Si diferentes terminales pueden acceder a más de un AP, se podría distribuir la carga soportada por cada uno de ellos, en la búsqueda de liberar ancho de banda disponible en dichos canales. Así el tráfico propio o el del resto de terminales se vería beneficiado por la reducción en el número de terminales y flujos vinculados que utilizan ese AP.

Consideramos importante destacar que los AP:

- Gestionan el tráfico que debe pasar a través de ellos, incluso para las comunicaciones entre los terminales de la propia subred (salvo con la aplicación de nuestra primera propuesta).
- Ocupan una posición estratégica y clave en el control del funcionamiento de la red WiFi.
- Tienen o deben tener un conocimiento detallado de terminales, capacidades y servicios activos o disponibles.

Por ello, creemos que deben tener un mayor protagonismo que el que les otorgan los estándares IEEE 802.11* en el control y gestión de la red WiFi, especialmente en el uso compartido del canal radioeléctrico, especialmente para poder participar activamente en la elección de los AP por parte de los terminales.

Al contar con el sistema de regulación expuesto en el apartado 4.2, que dispone de un gestor y los agentes en los terminales, pensamos que se podría utilizar el mismo sistema, para que sirva de experimentación real para esta nueva propuesta.

Por ello, pensamos que esta propuesta junto con la anterior pueden entenderse como integradas dentro de lo que hemos denominado "*plataforma multifuncional*" para la gestión del canal en redes IEEE 802.11.

Propuesta de optimización de terminales y flujos por traspaso

El mecanismo que siguen los terminales para asociarse a un determinado AP está basado en detectar el *SSID*, canal o frecuencia de cada AP y solicitarle asociación. Este proceso generalmente es trasparente a los usuarios dado que pueden haber diferentes AP con el mismo *SSID*; es el modo de operación definido para mantener diferentes subredes vinculadas. Además, esto es necesario para configurar una red con mayor cobertura o mayor disponibilidad de AP. La decisión de cuál de los AP detectados sería utilizado para su asociación no está especificado por el estándar IEEE 802.11, solamente se especifica el mecanismo utilizado. Según [164], la decisión suele basarse en el mejor nivel de señal recibida de entre los AP detectables. La mayor parte de los terminales inalámbricos hacen un proceso de rastreo (*scanning*) de los diferentes canales y entre todos los *beacons* que se detecten de los AP con el mismo SSID se escoge uno de ellos. Como ya se comentó, el nivel de señal recibido suele interpretarse con un valor de RSSI [165]. Este es un valor de una escala de referencia y se utiliza como parámetro para medir la intensidad de la señal recibida. Este valor numérico es dependiente de la relación señal/ruido detectado. Generalmente suele medirse en *mw* o *dBm* y se obtiene desde el controlador de nivel físico y de entre los bits de la cabecera de tramas de control (*beacons*).

Un dato muy interesante es que los valores obtenidos para los *beacons* son muy diferentes y dependientes del dispositivo que lo capture. El mismo AP puede ser detectado con diferentes RSSI por diferentes terminales o interfaces en una misma ubicación [166].

En cualquiera de los casos, creemos que solo considerar el valor del RSSI calculado o medido por el controlador para decidir que AP utilizar es válido en general, siempre que sea un nivel superior a un umbral. Este umbral está relacionado con la sensibilidad

del receptor y por debajo del cual, el nivel de señal es inaceptable para mantener una conexión con unas mínimas garantías.

Como se comprueba experimentalmente y en la literatura analizada, el valor del RSSI no tiene ninguna dependencia del estado del AP en cuanto al número de conexiones activas, ni número de terminales en la misma celda... Ya es conocido que estas variables si son importantes para determinar la capacidad del canal y la posibilidad de obtener una mínima calidad para comunicaciones que lo requieran.

Con estas consideraciones, proponemos que la decisión de elección de un AP por parte de los terminales sea complementada con la información de estado del canal que es conocida por cada AP, también presentada en [41], en la que se indica que es un problema optimización bastante duro. Como variante, nosotros consideramos que esos mismos AP puedan elegir determinados terminales para que cambien o se asocien a otro AP, si las condiciones podrían ser mejoradas tras una redistribución de los mismos entre los AP disponibles.

En la Figura 96 se muestra una situación muy habitual de una red WiFi en modo infraestructura con varios AP y dos terminales en la que reflejamos la propuesta planteada con este apartado.

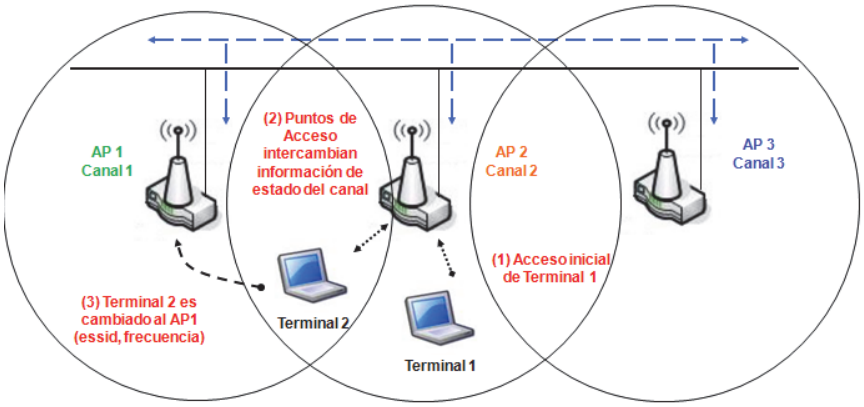


Figura 96. Propuesta de redistribución de terminales entre AP

Esta propuesta consiste en forzar que los terminales seleccionados entre los asociados a un determinado AP, que llamamos AP origen, puedan cambiarse (re-asociarse) a otro AP, que llamamos AP destino, si este último pudiera ofrecer mejores condiciones (canal libre, mayor ancho de banda disponible, inexistencia de servicios no dependientes del tiempo...). Esta funcionalidad se restringe a terminales que detecten más de un AP, pues se ubican en zonas de intersección de coberturas. Esta situación es muy habitual en zonas con gran número de AP y gran cobertura (por ejemplo

aeropuertos, campus universitarios...) en las que se intenta evitar que existan zonas oscuras.

Con esta idea, se pretende optimizar, en cierta medida, el uso del canal, pues su saturación o sobrecarga puede ser debida a que existen muchos terminales haciendo uso del mismo canal/AP en la intersección de dos canales o celdas. Si analizamos la Figura 96, se puede observar que si esta situación se presenta, pudo ser debido simplemente porque el criterio para la elección del AP2 frente al AP1 por parte del terminal 2, a la hora de asociarse a uno de ellos, se realizó simplemente por cuestiones de mejor calidad de señal (mejor RSSI) y no en base a información de estado del canal y de los AP.

Se observa que los terminales 1 y 2 están asociados al AP2. El canal 1 gestionado por el AP1 está libre y en cambio en el canal 2 está siendo compartido por las comunicaciones de los terminales 1 y 2. Si el terminal 2 se asociara al AP1, la disponibilidad del canal, medido como mayor ancho de banda disponible para sus comunicaciones, sería mejor en el canal 1, así como la disponibilidad del canal 2 para el terminal 1, al hacer uso de él en exclusividad.

Por tanto, no siempre la elección automática de un AP basándose solo en el nivel de RSSI medido no es lo óptimo, pues se pueden detectar niveles de señal similares, y así el AP1 en el canal 1 no tenga terminales conectados y en cambio el AP2 tenga un mayor número de terminales (clientes).

Consideramos que ante esta situación, los AP al tener un conocimiento preciso del estado de sus interfaces, terminales asociados y servicios (tráficos) generados, puedan gestionar intercambios o traspasos de terminales entre los AP afectados.

Los parámetros que consideramos deben ser tratados para la optimización buscada son los siguientes:

- Terminales:
  - Número de TER por APj (N_{TER_APj}).
  - Conjunto de TER asociado a APj ($C_{TER\_ASOCIADO\_APj}$, ec. (3.2.6)).
  - Flujos por cada terminal asociado (f_{TERi}, ec. (3.2.7)).
  - Conjunto de AP visibles por TER ($C_{AP\_VISIBLES\_TERi}$, ec. (3.2.9)).
  - Nivel de RSSI detectado por cada TER ($RSSI_{TERi}$, ec. (3.2.10)).
  - Características de flujos (tipo (prioritario o no prioritario), direcciones, puertos, protocolo de transporte, requisitos (bitrate, retraso, jitter …)).
- AP:

- Lista de AP vecinos por cada APj ($V_{AP}(j)$).
- Características de canales (AP vecinos) (Car_AP_j, Bm_APj, $B_T\_APj_{...}$).
- Flujos totales soportados por APj (f_AP_j, ec. (3.2.8)).
- Potencia de transmisión (Pot_{APj}).
- Canal/Frecuencia (Ch_{APj}, Fr_{APj}).

o Matriz de Asociación (A_{TER_APj} (i,j), ec. (3.2.14)).

o Posibilidad de balanceo de terminales (parámetro).

De entre los parámetros relacionados debemos resaltar la importancia de determinar que los terminales escogidos detecten a los AP participantes (origen y destino) y ello podría comprobarse con la existencia en la lista de AP vecinos (zona de cobertura solapada (intersección)). Además es indispensable conocer: los flujos por terminal, sus características y condiciones de los AP: anchos de banda teórico, medido. Además, de manera especial, los flujos totales soportados, y especialmente sus efectos sobre la capacidad disponible antes y después de cualquier traspaso. Nuevamente tenemos especial consideración con flujos dependientes del tiempo, que son hacia los que se dirigen todas las iniciativas planteadas.

Para implementar esta segunda funcionalidad, vamos a hacer uso de los gestores que puedan incorporar los AP y, dado que ellos deben saber necesariamente los terminales que tienen asociados, entre dichos gestores se intercambien esa información por la red cableada a través del sistema de distribución. Con la información recibida, cada AP, a través de su gestor, podría ofrecerse como potencial receptor de algún terminal de otro AP, liberando con ello a este último del tráfico generado y, por tanto de todos sus flujos. Ante un determinado ofrecimiento, el AP sobrecargado podría iniciar un proceso que hemos denominado "de cambio de AP o traspaso" para uno de los terminales conectados. La decisión de qué terminal se traspasaría, se realizaría por el conocimiento de todos los existentes y los servicios utilizados. Podría hacerse el traspaso de aquel que esté en la intersección o en el caso de que hubiera varios, aquel que al traspasarse libere tráfico del canal o se mejore sus condiciones en el nuevo canal o celda. El gestor de cada AP, al recibir el mensaje de cambio de AP o traspaso analiza su situación actual, determina el proceso de traspaso y a qué terminal se le aplicaría. Para ello primero notifica al AP destino que se ha de iniciar dicho proceso, tras la

comunicación y confirmación por el agente del terminal correspondiente, este se re-asocia al nuevo AP.

Si bien el criterio seguido para decidir cuándo hacer un traspaso y con qué terminal puede ser configurable, partimos de la idea de intentar que los flujos prioritarios estén aislados, sin verse afectados de flujos no prioritarios, agrupados o individualmente siempre que se garanticen sus bitrate o características mínimas. Debemos recordar aquí que la mayor parte de los flujos prioritarios se soportan sobre servicio de transporte no orientado a conexión, o sea UDP, dada las características de los mismos. Igualmente podríamos agrupar todos los no prioritarios y así puedan mantener un acceso *best-effort* (los problemas relacionados con la limitación del canal y otros efectos son subsanados mediante el servicio de transporte orientado a conexión). En estos casos, mediante retransmisiones de transporte y reconocimientos, se garantiza la integridad de la comunicación. Recordemos que esto mismo imposibilita el uso de TCP para flujos prioritarios (un paquete de video retrasado debe ser descartado y no reproducido).

Asimismo, se incorpora un control para evitar un intercambio de terminal de ida y vuelta (histéresis) y situaciones inestables debidas a traspasos en bucle, para ello se aplican variables de control de histórico y tiempos mínimos de mantenimiento.

Para explicar mejor esta funcionalidad utilizamos una secuencia de acciones y nos basamos en la Figura 96 como ejemplo gráfico, indicando la información que se intercambian los dos AP y el terminal WiFi que se “traspasa”:

1. Los gestores de todos los AP difunden (modo *broadcast*) por la red cableada información de estado (terminales, servicios (flujos), características...).
2. Si el AP1 está en mejores condiciones que el AP2 (comparando información de estado recibida desde el AP2) responde de forma *unicast* al AP2 ofreciéndose (parámetro *DISPONIBILIDAD_DE_APj*) a recibir algún terminal (con o sin restricciones).
3. El AP2 al recibir el ofrecimiento del AP1, consulta a todos los agentes de los terminales si detectan al AP1. Con los datos de aquellos terminales que respondan afirmativamente se decide cuál de ellos traspasar.
4. Si el terminal 2 responde que sí detecta al AP1, el gestor del AP2 podría forzar por medio del agente de dicho terminal para que se asocie al AP1. Este terminal cliente debe confirmar que inicia el proceso de traspaso.

5. Una vez está asociado al AP1, este último debe confirmar al AP2 que el terminal está asociado con él. Si no se confirmase este hecho, se perdería la conexión con el agente desde cualquiera de los dos AP implicados. Además esto garantiza que se realice perfectamente la baja y el alta en los registros correspondientes de cada gestor.
6. Finalmente el terminal 2, está asociado al AP1. En cualquiera de los casos, el usuario de este terminal debe ser notificado de cualquier incidencia, y en caso de situación irregular o no asociado por algún fallo del proceso, podría reiniciar la asociación en el AP que desee, como se realiza de forma natural.

Esta propuesta la hemos planteado formada por cuatro etapas o fases denominadas:

Fase 1. Anuncio	(Los AP intercambian mensajes con AP vecinos)
Fase 2: Ofrecimiento	(Los AP se ofrecen a recibir un nuevo terminal)
Fase 3: Traspaso	(Traspaso entre AP con selección de terminal)
Fase 4: Confirmación	(Finalización o confirmación de traspaso)

Las órdenes vinculadas con cada acción se relacionan en la Tabla 28.

Tabla 28. Relación de órdenes para gestionar traspaso de terminales entre AP

Cód.	Nombre	Sentido	Descripción
21	*ANUNCIO*	Gestor ↔ Gestor	Difusión de estado de cada AP entre AP vecinos (*broadcast*).
22	*OFRECIMIENTO*	Gestor ↔ Gestor	Respuesta *unicast* de AP destino al AP origen con ofrecimiento.
23	*OFRECIMIENTO_REPLY*	Gestor ↔ Gestor	Confirmación al AP destino de inicio de proceso.
24	*SONDEO*	Gestor → Agente	Consulta a los terminales asociados sobre que AP detectan o un especificado AP.
25	*SONDEO_REPLY*		Respuesta con AP detectados, o confirmando o no, la detección del AP destino especificado.
26	*TRASPASO*	Gestor → Agente	Indicación a terminal especifico su traspaso desde el AP origen al especificado AP destino.
27	*TRASPASO_REPLY*	Agente → Gestor	Comunicación de traspaso desde terminal a AP destino.
28	*TRASPASO_FIN*	Gestor → Gestor	Notificación de traspaso desde AP origen a AP destino
29	*TRASPASO_FIN_REPLY*	Gestor ← Gestor	Confirmación de traspaso desde AP destino a AP origen.

Las órdenes 21, 22, 28 y 29 son intercambiados entre AP (gestor-gestor) y las órdenes 23, 24, 25, 26 y 27 entre AP y el terminal (gestor-agente).

Con la secuencia de acciones descrita anteriormente y usando las órdenes presentadas, los gestores pueden realizar el traspaso de terminales, con la necesaria conformidad de los agentes. Esto es necesario y preceptivo para evitar lo que denominamos terminal "aislado", que se daría cuando el proceso de traspaso no se culmina correctamente y el terminal seleccionado no queda asociado a ningún AP. Si el agente del terminal que se traspasa no recibe ningún mensaje del nuevo AP, activaría de nuevo un proceso de rastreo (*scanning*) y se asociaría a cualquiera de ellos, iniciándose el proceso completo, por lo tanto seguiría actuando de forma normal.

En la Figura 97 se muestra un diagrama temporal con las diferentes órdenes o mensajes intercambiados entre los elementos intervinientes.

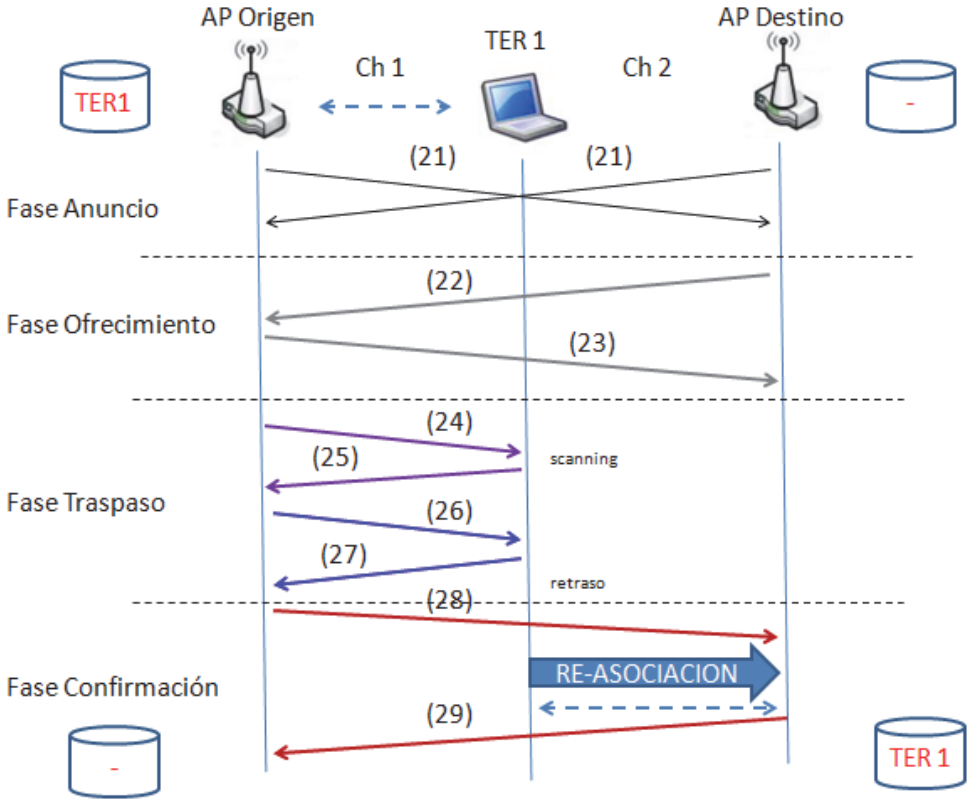


Figura 97. Intercambio de órdenes entre elementos relacionados con el traspaso

Si analizamos la Figura 97 debemos destacar que los mensajes de *broadcast* de la fase de anuncio (21) se realizan por la red cableada o sistema de distribución que interconecta los AP, dado que ellos no pueden detectarse si usan diferentes canales o no

estar en cobertura. Si es una red *mesh* WiFi, donde generalmente se cuenta con otro canal inalámbrico para *routing* entre los AP, podría usarse este canal o interfaz de interconexión entre ellos. Lo mismo sucede en la fase de ofrecimiento con el mensaje (22) y su confirmación positiva o negativa. La pérdida de cualquiera de estos mensajes no afecta al funcionamiento de esta propuesta, pues tanto los terminales como los AP no habrían alterado sus estados.

Una vez un determinado AP destino se ofrece (AP destino=AP1 en la Figura 97) y se confirma con (23) desde el AP origen, ambos pasan a la fase de traspaso. En esta fase todos los intercambios se realizan mediante el canal que exista entre AP origen y el TER. Obviamente, el traspaso depende especialmente de que el terminal implicado detecte con un mínimo de señal (RSSI) al AP destino. Si no fuese así, el traspaso no se realiza y quedando ambos AP y TER en la situación inicial, o sea continuar anunciando estado de AP.

Para realizar el traspaso, el AP origen mediante (24) consulta al terminal si detecta al AP destino, y para ello el terminal hace el proceso de rastreo (*scanning*) conveniente y devuelve con (25) si lo detecta o no. En el caso de que se den las condiciones adecuadas, el AP origen solicita con (26) al terminal que se desvincule del AP origen. Para ello se requeriría, después de la confirmación (27) pertinente por el canal que todavía les une, que se produzca el traspaso guiado desde el propio agente incluido en el terminal. Esto implica que el terminal se re-asocie al AP destino indicado por el AP origen como parte del mensaje (26). En el momento que el AP origen reciba la confirmación por parte del terminal de que se asociaría al AP destino se pasa a la fase de confirmación.

Por último, el AP origen (AP2) notificaría con (28) al AP destino las características del terminal que se traspasa, perdería contacto con dicho terminal y lo eliminaría de su registro de terminales asociados, como se observa en la Figura 97. El proceso de re-asociación se activaría desde el agente del terminal y sería el mismo que se aplica en cualquier entorno WiFi, sin ningún comportamiento especial. En el caso de formar parte del sistema de regulación explicado en el apartado 4.2, se podría obviar el control de admisión, pues ya ha sido admitido el servicio. Una vez la asociación se haya completado, el AP destino registraría el nuevo terminal y notificaría nuevamente con (29), por la red de distribución que ha aceptado a dicho terminal, confirmando el proceso satisfactoriamente. Si la fase de confirmación no se produjese y cualquiera de

sus acciones no se realizasen o se perdiese cualquiera de los mensajes, ninguno de los AP tendría asociado al terminal, en este caso, el terminal por medio de su agente, transcurrido un temporizador iniciaría una asociación a cualquiera de los dos AP, pudiéndose repetir el proceso. Si se pierde el mensaje (28), el terminal continua con su proceso de asociación pero se considera como un terminal nuevo, y si se pierde el mensaje (29), no tendría ningún efecto dado que el AP origen presupone la pérdida de contacto en cualquiera de los casos; probablemente el terminal se habría pasado al canal 2 para comunicarse con el AP destino.

En la Tabla 29 se muestra el pseudocódigo de nuestra implementación de este mecanismo de traspaso guiado por los AP para redistribuir de forma más eficiente los terminales.

Tabla 29. Pseudocódigo de traspaso guiado desde AP

```
1:    Anuncio de forma broadcast estado de AP (ANUNCIO)
```

Parte de AP Origen

```
2:    If Recibo ofrecimiento de traspaso (AP ORIGEN) (OFRECIMIENTO) then
3:        If condiciones mejores then
4:            Responder a ofrecimiento (OFRECIMIENTO_REPLY)
5:            Sondear terminales si detectan AP ofrecido (SONDEO)
6:            If recibe confirmación then
7:                Posible traspaso TER i (SONDEO_REPLY (OK))
8:                Traspaso TER entrante o Selección de TERi para traspaso*
9:                Forzar traspaso a TER i
10:               Envio de mensaje (TRASPASO) a agente
11:               If recibo confirmación (TRASPASO REPLY) then
12:                   Notificación a AP DESTINO información de TER i
13:                   Ha sido traspasado (TRASPASO_FIN)
14:                   Actualizar BD  eliminando TER i
15:               else
16:                   Break (aborta traspaso para TER i)
17:               end if
18:                   Break (aborta traspaso para TER i)
19:                   goto  inicio 1
20:           else
21:               Break (aborta traspaso por no respuesta (SONDEO_REPLY(NO))
22:           end if
23:       else
24:           goto inicio 1
25:       end if
26:   else
27:           goto inicio 1
28:   end if
```

Tabla 29. Pseudocódigo de traspaso guiado desde AP (cont.)

Parte de AP destino

```
30:   Recibo ANUNCIO,
31:   If condiciones mejores then
32:       Envío ofrecimiento (AP DESTINO) (OFRECIMIENTO)
33:   If Recibo confirmación (OFRECIMIENTO_REPLY) then
34:       Activo proceso de traspaso y mantengo estado
35:       If recibo TRASPASO_FIN then
36:           Espera t por solicitud de acceso de  TER i (FASE CONFIRMACION)
37:           If TERi asociado then
38:                   Envío confirmación TRASPASO_FIN_REPLY
39:                   Registro datos nuevo TERi
40:                   Volver inicio 1
41:           else
42:                   If  timer=0 then
43:                       Traspaso no realizado por vencer temporizador
44:                       Envío TRASPASO_FIN_REPLY(NO)
45:                       Volver inicio 1
46:                   end if
47:           end if
48:       else
49:           Traspaso abortado ante ausencia de notificación de AP origen
50:       end if
51:   end if
52:   goto inicio 1
```

*Los criterios que definimos para optimizar el traspaso de los terminales y sus flujos entre los AP son:

1. Existencia de flujos prioritarios entre AP implicados
2. Ningún *APj* sin terminal y flujo
3. Agrupar terminales con solo flujos no prioritarios en *APj*
4. AP receptor de anuncio se ofrece a traspaso si no cuenta con flujos prioritarios
5. AP receptor de ofrecimiento traspasa terminal con flujo no prioritario si existe otro terminal con otro flujo prioritario
6. Búsqueda de $B_{m\_APj} < \sum f_p$
7. Garantizar disponibilidad de ancho de banda para flujo prioritario en *APj*
8. Cada *APj* cuente con el menor número de flujos prioritarios (min N_{Fp}, optimo: $N_{Fp} = 1$)
9. Cada *APj* cuente con el menor número de terminales o flujos (caso más simple con un solo flujo por *TERi,* N_{TER}=1)
10. *TERi* entrante tiene prioridad para ser traspasado (por no haber iniciado tráfico)

11. Ante igualdad de condiciones o parámetros, si el flujo entrante es prioritario se traspasa al $AP_{destino}$ con mejor $B_{M\_disponible}$.

En la Tabla 30 se relacionan los parámetros relacionados con esta funcionalidad, gestionados por los AP y los códigos que hemos utilizado.

Tabla 30. Codificación de parámetros

Parámetro	<valor>	Campos <codigo-longitud-valor>
ID de TERi	*1*	*Dirección MAC TERi*
ID de APj	*2*	*Dirección MAC* AP_j
Número de TER	*3*	N_{TER}
Lista de TERi asociados a APj	*4*	$C_{TER\ ASOCIADOS\text{-}APj}$
Lista de flujos por TERi	*5*	F_{TERi}
Lista de AP detectables por TERi	*6*	$C_{AP\ VISIBLES\ TERi}$
Características de flujo	*7*	*{puerto, regulación, bitrate, retraso, jitter,..}*
Potencia de transmisión de APj	*8*	Pot_{APj} *(si > 0 mw, < 0 dbm)*
Canal/frecuencia	*9*	$Ch\_{}_{APj}$ / $F_{r\ APj}$
Características de APj	*10*	$B_{T\text{-}APj}$ *(Mbps),* $B_{m\ APj}$ *(Mbps)*
Lista de AP vecinos por cada AP	*11*	V_{APj} *={AP0, AP1,….APj}*
Nivel de señal de cada APj	*12*	$RSSI_{TERi}$
Matriz de asociación	*13*	$A_{TER\text{-}APj}(i,j)$

De igual manera, representamos en la Tabla 31 la codificación que hemos realizado para cada tipo de mensaje.

Tabla 31. Codificación de mensajes y parámetros incluidos

TIPO	<valor>	Parámetros incluidos en PDU
ANUNCIO	*21*	*2,3,4,5,7,8,9,10,11*
OFRECIMIENTO	*22*	*2,3,4,5,7,8,9,10,11*
OFRECIMIENTO_REPLY	*23*	*2*
SONDEO	*24*	*2 (AP-Destino)*
SONDEO_REPLY	*25*	*Afirmativa: {2,RSSI_AP-Destino}* *Negativa: 6{Parejas(2, RSSI_APj)}*
TRASPASO	*26*	*2 (AP-Destino)*
TRASPASO_REPLY	*27*	*Afirmativa => 1* *Negativa => Razón*
TRASPASO_FIN	*28*	*1,5,7*
TRASPASO_FIN_REPLY	*29*	*1,4*

Con esta nueva propuesta o funcionalidad, los terminales que detectan varios AP, sin necesidad de moverse físicamente, una vez asociado y pasado el control de

admisión, podrían ser guiados hacia un determinado AP que pudiera estar en mejores condiciones para los servicios demandados. Esto se realizaría por los terminales de forma dinámica y distribuida activada por los agentes, pero dirigido por los gestores de forma centralizada en cada uno de ellos. Los gestores llevan un registro de terminales y las altas y bajas correspondientes vinculadas a los traspasos. Además, algo que consideramos muy importante, sin intervención de los usuarios, o sea de forma transparente a los mismos.

Una variante a este mecanismo de traspaso guiado que hemos contemplado, es aquella que consideramos podría aplicarse cuando un terminal aún no se encuentre registrado con un determinado AP. En estos casos, directamente el AP al que se solicita admisión, puede redirigir al terminal mediante el intercambio de los mensajes 24, 25, 26 y 27 (Figura 97) con el agente del terminal. Esto es posible, si en el momento en que un terminal intenta solicitar conectividad durante la fase de control de admisión, se detectan unas condiciones en el canal/AP que no garanticen unos mínimos requisitos para el servicio solicitado. En este caso el AP, conociendo los anuncios anteriores, puede invitar a que el terminal seleccione el AP destino de forma inmediata, pero no garantizando que este acepte la conexión. Debemos resaltar este hecho, ya que en este caso el AP destino verá al terminal como uno nuevo y no procedente de un traspaso; no tiene porqué aceptar al terminal entrante dado que no ha habido un ofrecimiento previo y por tanto no se puede imponer el traspaso. En el caso general visto anteriormente, si debe aceptarlo dado que se había negociado el traspaso con todas las condiciones y requisitos. A esta otra forma de guiar los terminales lo denominamos "*traspaso modificado sin negociación"*.

4.4 Localización de terminales. Reubicación

En este apartado continuamos con la serie de propuestas dirigidas hacia la búsqueda de la optimización de los parámetros o recursos utilizados en redes WiFi para mejorar las prestaciones de las mismas. En este caso presentamos una propuesta para mejorar la QoS del acceso de terminales móviles a servicios de Internet. Para ello hemos estudiado cómo utilizar aspectos de la ubicación de un terminal móvil en función de su posición

dentro de su espacio de localización. Los niveles de señal que un terminal pueda detectar desde un AP puede ser útil para:

- Que el terminal WiFi tome acciones correctivas (reubicación, reorientación, variaciones físicas...).
- Balancear el acceso a Internet teniendo en cuenta la carga de los AP.
- Planificar el despliegue de los AP a partir de un histórico de localizaciones estables de los terminales.

La localización de terminales es un clásico de las redes móviles [167] y existen muchos métodos de localización ampliamente estudiados [16]. Asimismo, éstos tienen muchas aplicaciones recientes que se usan masivamente [17] [18]. Los métodos de localización suelen ser dependientes de la red, la aplicación y la tecnología inalámbrica utilizada. En el caso de redes WiFi se han desarrollado soluciones propietarias, como por ejemplo la de *skyhook* [168] basada en el uso de Base de Datos que contienen las localizaciones de los AP en una región amplia (ciudad). Con ello se intenta proveer servicios de localización bajo el abanico de servicios que puede ofrecer un operador de comunicaciones. Igualmente la empresa *Ekahau* dispone de soluciones especializadas en *Real Time Location System* (*RTLS*) [169]. Cisco también tiene sus propias aplicaciones [170]. Otros trabajos sobre localización en interiores se presentan en [171] basándose en trilateralización mediante cálculo de distancias y distribución de probabilidad (histograma). Ninguno de estos métodos se usa para mejorar el acceso a servicios de Internet de la misma forma en que la aplicamos.

Dada la variabilidad física de los niveles de señal radio en redes WiFi, la dependencia de un canal compartido por muchos clientes, el uso libre para múltiples aplicaciones y su vulnerabilidad relativa a interferencias externas, las posibilidades de aplicar técnicas de TDOA, AoA, triangulación [15] o marcas de tiempo se limitan bastante. Incluso hemos constatado la dependencia de múltiples factores y que va a existir una dificultad intrínseca para conseguir una buena precisión, como otros autores indican en [52] [53]. En lugar de aplicar complejos métodos, nosotros usamos el método de determinación de la localización de terminales mediante comparación y aproximación a los valores del mapa de referencia de coberturas (niveles de RSSI [172]). El terminal se localizaría en un espacio $\overrightarrow{RSSI}$ de dimensión *m*, siendo *m* el número de AP registrados en una *BD* de coberturas por cada AP. Si retomamos los parámetros del apartado 3.2 que consideramos necesarios, recordamos que la ec.

(3.2.10) representaba el conjunto de niveles de RSSI detectados por cada TER de todos los AP detectables.

$$\overrightarrow{RSSI} = \{RSSI_1, RSSI_2, \dots, RSSI_j, .. RSSIm\}.$$

Hemos demostrado que el cálculo eficiente de la localización puede ser aprovechado como parámetro muy importante de QoS en el acceso a Internet. Una ventaja adicional es que por su sencillez el tratamiento de los valores de este parámetro se puede llevar a cabo en los AP o en un servidor especializado. Entre los diferentes objetivos que podemos alcanzar que mejoren la QoS, especialmente en situaciones de movilidad o reducido número de AP se encuentran:

- Guiar a un terminal hacia la ubicación más adecuada dentro de su espacio de localización.
- Prever zonas con caídas bruscas de conectividad y evitación de las mismas.
- Reubicación de terminales a AP con mejores prestaciones.

Como primera línea de actuación en esta propuesta permitimos que el usuario dispusiera de los mapas de cobertura en su terminal (uno por cada AP próximo a él) para que pueda elegir el AP que le proporcione una conexión más duradera o de mejor calidad con garantías aceptables de acceso a Internet. El usuario haría esta conexión dependiendo de su trayectoria o de forma automática pudiera ser guiado por el sistema. La definición de los mapas de cobertura se puede hacer con una aplicación sencilla, como la que se desarrolló durante las primeras experiencias en este campo [173]. La integración de estas dos aplicaciones permitiría que el usuario se subscribiese a este servicio de localización recibiendo los mapas de cobertura que previamente se habían definido para una Organización concreta y posteriormente actuar con la información obtenida.

Para las pruebas experimentales contamos con la *plataforma funcional* ya desarrollada que implementa las otras propuestas anteriores, que recordamos permitían un control de admisión y regulación dinámica de flujos, y por otro lado la reubicación de terminales entre los AP según condiciones de los canales. En la Figura 86 (apartado 4.2) se muestra el esquema modular utilizado de que se compone la plataforma de pruebas comentada.

Esta propuesta parte de contar con una *Base de Datos* (*BD*) de valores de RSSI o niveles de señal creada previamente y comparar en ella los datos. En cualquiera de los

casos, los cambios de intensidad o potencia de señal y la variabilidad de la señal hacen complejo el proceso de obtención de resultados con buena exactitud. Sería deseable que el nivel de señal de cada AP fuese estable para conseguir una posición exacta. Este problema se aprecia claramente, como ya se comentó, en la Figura 98.b donde los niveles de señal no se distribuyen acordes con la teoría. Igualmente en el capítulo 3, describimos múltiples evidencias de esta variabilidad que dificulta la precisión en esta aplicación.

(a) (b)

a) Áreas de solapamiento teórico de cobertura de los AP de una Organización. b) Diagrama de radiación real medido en interiores para WiFi: diagrama de colores (dBm): -26(marrón),-28,-30…,-44(azul), (ejes) niveles teóricos: -50,-40,-30,-20,-10,0,10,20,30,40,50 dBm.

Figura 98. Esquema de coberturas teórico y diagrama de radiación de AP real.

Esta *BD* debe contar con los niveles de señal de todos los AP existentes incluyendo los SSID, frecuencia de trabajo e identificación de cada AP (por ejemplo la dirección MAC) para las diferentes zonas a controlar. Partiendo de la variabilidad de los niveles de señal, se hace necesario generar la BD haciendo una gran cantidad de muestras, realizadas en diferentes momentos del día y con diferentes estados de carga, para darle un mayor rigor y exactitud a los valores de los diferentes parámetros a utilizar, así como registrar valores mínimos y máximos, cuando éstos sean variables. En cualquier caso, siempre hay un margen de error, debido a la variabilidad de muestras de RSSI. Esta BD se debería actualizar regularmente siempre que haya cambios de SSID de celdas, frecuencia o cambios de ubicación. Tanto más fiable sería este modelo, cuanto mayor número de AP estén disponibles.

Para la materialización de esta propuesta vamos a hacer una separación en dos procesos o pasos:

1. Fase de Aprendizaje. Creación de la BD de coberturas de AP (mapas de coberturas)

2. Fase de Búsqueda de localización. Proceso de determinación de la localización del terminal WiFi

El primer paso lo llevamos a cabo mediante un proceso de realización de medidas de campo de forma manual seleccionando zonas a controlar. Con un ordenador portátil se registran los niveles de señal y resto de datos de los diferentes AP visibles, y al final, se crea el archivo o BD de coberturas para un espacio de localización RSSI. Paralelamente y como comprobación, hemos utilizado otra aplicación para *Personal Digital Assistant* (*PDA*), que de forma gráfica muestra los mapas y las ubicaciones.

En la Figura 99 se ilustran un par de capturas de la aplicación durante su ejecución en una PDA *HP iPAQ 5555*. Usándola se recorre toda la Organización y elabora un mapa con coordenadas de cada espacio de localización, los AP y niveles de RSSI. Con estos datos, el servidor los registra y los vincula a un plano real de la zona en estudio. Con esta información, posteriormente, se determina la localización de forma eficaz. Esta aplicación podría de forma relativamente fácil adaptarse a los nuevos dispositivos, especialmente en Smartphone basados en Android o similar. Otras formas similares de realizar este proceso en interiores y exteriores se plantean en [174].

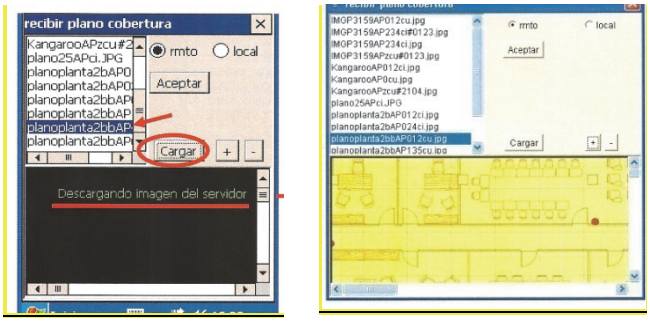


Figura 99. Ejemplo de aplicación de localización de AP en interiores

En cuanto al proceso de determinación de la localización automática sin intervención del usuario, proponemos una forma diferente en la que cada terminal móvil debe barrer el espectro, registrar a todos los AP detectados y esta información deba ser enviada al AP. Con esta información, el AP o un servidor especializado, si lo hubiese, determina la posición del terminal móvil solicitante en lugar de que sea el terminal el que reciba los mapas y tenga que realizar ese trabajo. Evidentemente es recomendable evitar la transmisión de la BD de zonas a los terminales para no aumentar el tráfico en la red. Igualmente consideramos deseable evitar el uso de los

recursos de los terminales para esta tarea cuando el AP, o un servidor especializado, puede hacerlo.

En la Figura 100 se muestra el proceso, incluyendo las diferentes fases o etapas y particularizado para su aplicación con un equipo a modo de *Linux Router Wireless* (*LRW*) y con ello poder implementar la propuesta. Obviamente, la propuesta sería perfectamente portable a un AP mediante su programación conveniente según nuestro diseño.

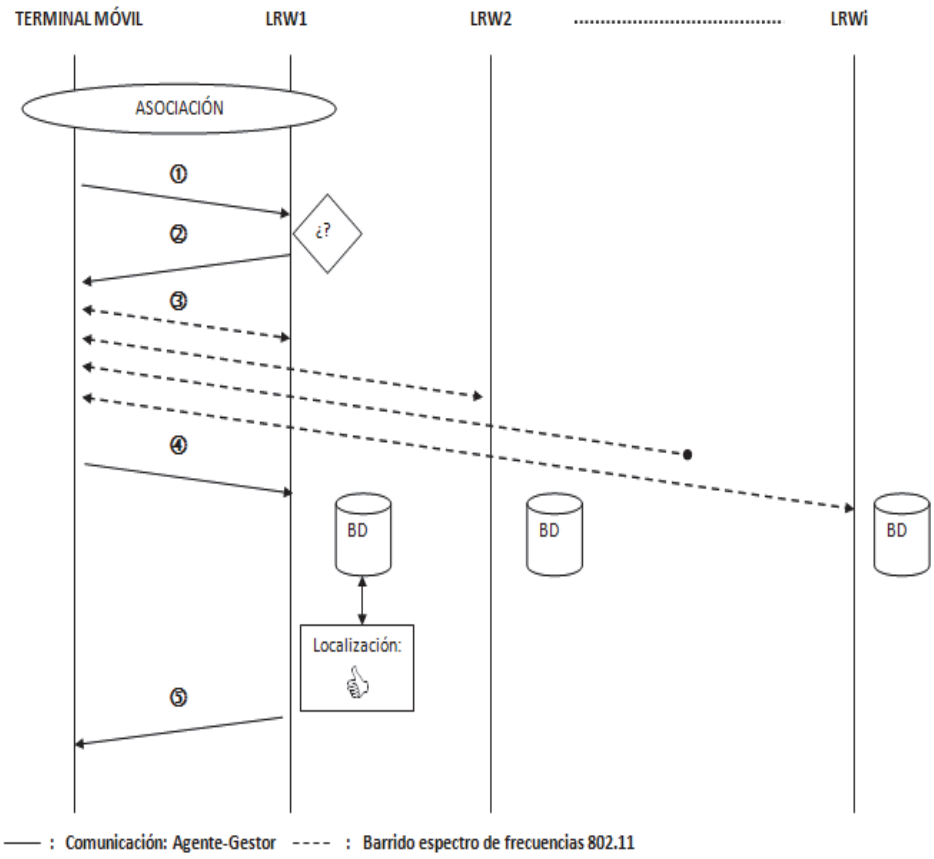


Figura 100. Secuencia de acciones de localización basado en BD (mapa)

Una vez se encuentre el terminal móvil asociado a un *LRW*, en nuestro caso está asociada al LRW1, podría solicitar su localización (paso ① en la Figura 100). Para ello se haría la solicitud correspondiente a dicho LRW1. El LRW1 ante esa petición, y quizás contar con información insuficiente o no actualizada para poder determinar dónde está dicho terminal, podría requerirle información complementaria, actualizada o más detallada (como el nivel de RSSI e identificaciones de todos los *LRWi* que él detecte) (②).

Después, el terminal móvil realizaría un barrido del espectro (③) y capturaría los diferentes datos de los diferentes *LRW* accesibles (AP). Esta información una vez estructurada de forma correcta, se enviaría al *LRW1* (④). Con dichos datos, el *LRW1* localizaría en la BD, creada y cargada previamente, los datos coincidentes o más próximos con los diferentes rangos, y determinaría la localización. Finalmente se le devolvería al terminal móvil solicitante la posición (⑤), o en su defecto, cualquier incidencia que pudiera haberse producido.

El tratamiento y búsqueda en la BD consiste en ir buscando el mayor número de coincidencias (pudiéndose encontrar múltiples *LRW* que las satisfagan) y pudiéndose dar múltiples casos:

- Se encuentra información de localización insuficiente (un solo *LRW*), o sea, sólo se puede determinar un área de localización del terminal (una esfera teórica o una corona circular sobre el plano) que coincide con el área de cobertura definida por $RSSI_1$. Nuestra aplicación hace que el *LRW*1 conociendo la ubicación del terminal puede sugerir reubicaciones y controlar el reparto del canal para mejorar la QoS del acceso a Internet.
- Se encuentra información de localización (dos *LRW*) poco adecuada y con baja exactitud. En teoría, el terminal móvil se encuentra en el área de cobertura intersección de las definidas por $RSSI_1$ y $RSSI_2$. La aplicación detectaría de manera aproximada las fronteras de esa área de cobertura observando los niveles de RSSI registrados en la BD que coinciden con esa zona. De esta manera la QoS de acceso a Internet mejoraría porque la aplicación aconsejaría al terminal móvil que se moviese hacia una determinada zona cercana donde se obtiene un nivel mejor de RSSI.
- Se encuentra información de localización (tres o más *LRW*) adecuada. En este caso se cuenta con bastante información para localizar las coincidencias o aproximaciones en la BD y, además se pueden sugerir movimientos lineales o puntuales hacia zonas con mejor calidad de señal, cuando se den dichas zonas en la BD de referencia.

Para tratar estos casos introducimos una clasificación, que denominamos *grado de exactitud* de la información de localización. El *LRW*, por medio del gestor indica con un número entre 1 y 5 un baremado de la determinación de la localización. Concretamente, un 1 representa el caso peor, debido probablemente a contar con un sólo *LRW* y, el caso

optimo, con un 5, cuando se cuente con tres o más *LRW*. Notar que hemos distinguido 5 casos, pudiendo variarse según se determine.

Este grado de exactitud se ve más necesario después de las evidencias empíricas presentadas en el capítulo 3, donde se constata la elevada variabilidad de los valores de RSSI o nivel de señal recibida, que son usados para la BD patrón de referencia.

En base a los resultados de localización, el gestor determina, según la configuración que hayamos hecho de su funcionamiento, bajo qué condiciones de grado de exactitud sugeriría al terminal móvil un cambio de localización o activaría un cambio automático/manual de *LRW* (segunda funcionalidad de la aplicación (plataforma funcional).

Los mensajes definidos para esta funcionalidad se muestran en la Tabla 32.

Tabla 32. Relación de mensajes para gestión de localización

Código	Denominación	Sentido	Descripción
31	*LOCATION*	Browser →Web	Petición de localización realizada desde el browser al gestor (canal web).
32	*SCAN*	Gestor → Agente	Petición enviada del gestor al agente para que realice un rastreo de todos los canales inalámbricos y realizar la detección de *LRW* o AP.
34	*SCAN_REPLY*	Agente → Gestor	Información sobre AP detectados devuelta desde el agente al gestor.
35	*INFO_LOCATION*	Web → Browser Gestor → Agente	Resultado de localización (formato html) devuelto al browser del cliente y al agente desde el gestor. Como parte de este mensaje se incluye el grado de exactitud.

Para la codificación de los mensajes y su integración en la plataforma combinada se ha pensado codificarlos con números diferentes a los de las anteriores funcionalidades. Por ello se numeran con dos dígitos, el primero un 3 para indicar tercera funcionalidad y segundo dígito el número de orden de la secuencia de la Figura 100. No se usa la codificación con valor 33, dado que esta acción no implica un mensaje transmitido ensimismo, sino que representa en la Figura 100 el proceso de rastreo (*scanning*) de todos los AP detectables desde el terminal.

Dado que nuestra aplicación, como ya se comentó, se ha implementado en un servidor Linux con la funcionalidad *LRW* y éste cuenta con una más que adecuada capacidad de computación, hemos incorporado la BD y el cálculo de la localización

como parte del gestor, si bien podría descargarse de trabajo al gestor implantándolo en una aplicación independiente. Esto formaría parte de una posible evolución futura de la implantación de esta funcionalidad de localización de forma local (proceso interno) o remota (en otro servidor en la red cableada). En la Tabla 33 se muestra el pseudocódigo de esta nueva funcionalidad para el gestor.

Tabla 33. Pseudocódigo básico de localización de terminales

Algoritmo. Pseudocódigo localización (Gestor)

```
1:    If recibe petición de localización desde browser (LOCATION) then
2:        Marcar petición como iniciada desde usuario (vía web)
3:        Envío mensaje realizar rastreos (1 o 5 rastreos y promediar)(SCAN)
4:        If recibe mensaje con resultado de rastreo (SCAN_REPLY) then
5:            Buscar y comparar en BD localización
6:            Estimar zona y grado de exactitud
7:            If mensaje está marcado web then
8:                Enviar mensaje con resultado a browser (INFO_LOCATION)
9:            else
10:               Rastreo iniciado por gestor directa al agente (admin)
11:               No hay mensaje de respuesta al browser
12:           end if
13:       end if
14:   end if
```

Consideramos importante resaltar que para el *handoff* de teléfonos móviles en redes celulares se utiliza un sistema similar al nuestro. La diferencia es que en nuestro caso, el proceso sobre IEEE 802.11 es mucho más complejo debido a las condiciones ambientales, la variabilidad del RSSI y las pequeñas distancias de las zonas de cobertura de los AP.

Además debemos resaltar que si la BD se crea con un determinado dispositivo, la localización sería más exacta si se utiliza esta funcionalidad desde el mismo dispositivo que tomó los datos. Si fuese otro diferente podrían darse variaciones dada la variabilidad intrínseca de los valores RSSI obtenidos por cada dispositivo y por la propia variabilidad de los mismos. Por tanto sería recomendable hacerla con datos capturados desde varios dispositivos distintos para buscar la más próxima a todos ellos incluso, podría optarse por crear diferentes BD según tipo de dispositivo y adaptarse ellos según cada caso. Ya Lui et al., en [56], presentan la elevada dependencia de los dispositivos que dificulta su exactitud.

Capítulo 5. Resultados experimentales

Las diferentes propuestas presentadas y descritas en el capítulo anterior se implementan de forma práctica en una plataforma de pruebas real. Mediante la misma, se realizan diferentes pruebas experimentales y se alcanzan diferentes resultados. El análisis de los mismos permite concluir que se consigue una mejoría en las prestaciones de las redes WiFi. Esta plataforma está basada en un portal cautivo, la implementación del código de los agentes para su instalación en los terminales y, en especial, la programación del gestor, que ubicado en la misma máquina que el portal cautivo, gestiona directa o indirectamente las cuatro propuestas anteriores sin la intervención de los usuarios de los terminales.

5.1 Modo de operación todo ad-hoc. Conexiones directas

Una vez presentadas las diferentes propuestas, como parte de la visión histórica de la presente tesis, en este apartado se presentan las medidas y resultados experimentales de la primera de las propuestas presentadas en el apartado 4.1. Resulta necesario resaltar que la disponibilidad de recursos en aquel momento no era la actual y por ello aparecen medidas que pueden parecer relativamente bajas. Eso es debido al uso de dispositivos que solo soportan el estándar IEEE 802.11b y que aun actualmente siguen operativos. A pesar de ello, estos resultados o medidas son exportables con el adecuado efecto de aumento de ancho de banda que actualmente se soporta (bps) y la reducción del RTT relacionado con los estándares más actuales 802.11g, 802.11n y otros.

En la Tabla 34 se presentan las características técnicas de los ordenadores personales, dispositivos de red y software que hemos utilizado para comparar las medidas relacionadas con las prestaciones de las redes en modo infraestructura frente al uso de nuestra configuración basada en el uso de un *Linux router* en vez de AP.

Tabla 34. Ordenadores portátiles, dispositivos de red y software utilizado

Recurso	Características
Ordenador Portátil: Terminal WiFi 1	Pentium IV 1.7Ghz. PCMCIA 802.11b WL110 [175] Lucent Compaq. Red Hat 9.0 [176]
PC 1: Terminal cableado 1	Pentium II 100Mhz. NIC Compatible NE2000 Ethernet. Slackware [177]
PC 2: Terminal WiFi 2	Pentium II 400Mhz. PCI-PCMCIA 802.11b WL310 [178] Lucent Compaq. NIC Ethernet Realtek [179]. Red Hat 9.0
AP	Dlink DWL900+ 802.11b [180]
HUB	Genius 8 Ports Ethernet 10 Mbps [181]

En las Figuras 101 y 102 se muestran las dos configuraciones utilizadas para hacer las pruebas experimentales. La primera en modo infraestructura tradicional y la segunda eliminando el AP y añadiendo al PC2 la funcionalidad de un Linux router. Hemos

utilizado tres herramientas de medida de prestaciones. La primera herramienta es el programa estándar *ping* [182] [183] para calcular la media del RTT. La segunda herramienta es *iperf* [123] que usamos para medir el ancho de banda (bps) disponible teórico. Finalmente nosotros utilizamos *netperf* [184] para comparar con los datos obtenidos con *iperf*.

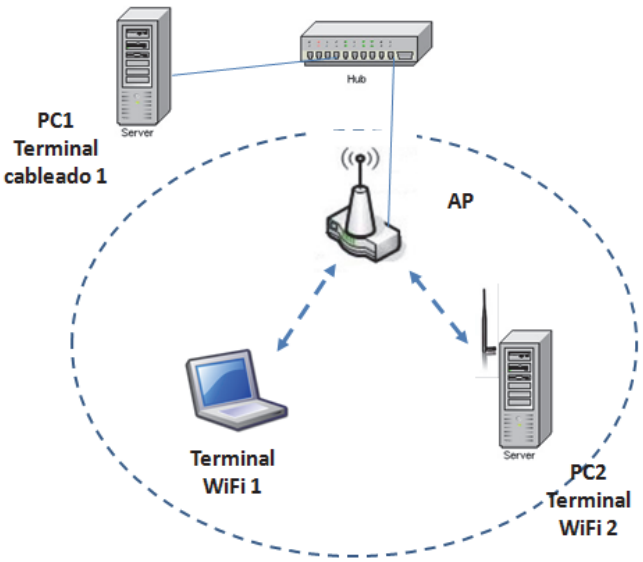


Figura 101. Configuración WiFi modo infraestructura

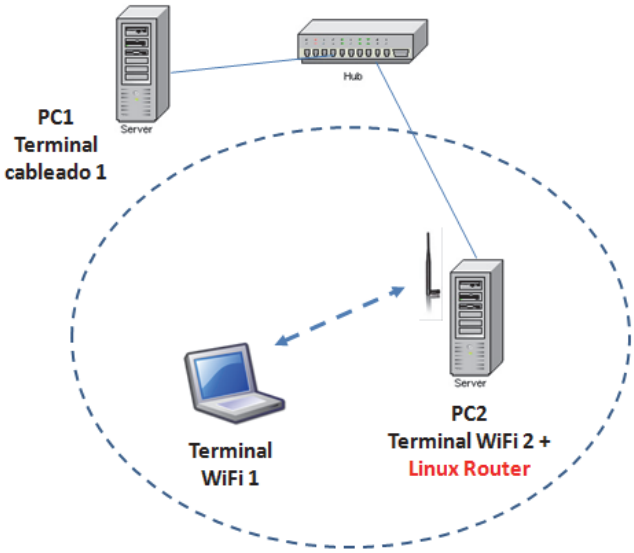


Figura 102. Configuración WiFi en modo Ad-Hoc y Linux router

Las pruebas fueron realizadas en la configuración WiFi en modo infraestructura y luego repetida para una configuración en modo ad-hoc con el *Linux router* como el

gestor del canal/celda inalámbrica. De forma detallada, las pruebas experimentales fueron las siguientes:

1. ping entre terminales WiFi.
2. iperf entre terminales WiFi.
3. netperf entre terminales WiFi.
4. ping e iperf entre terminales WiFi.
5. ping entre terminales WiFi combinados con otros tráficos e iperf.
6. ping e iperf entre terminales WiFi y terminal en la red cableada.

A continuación describimos las medidas obtenidas para ambas configuraciones.

1. Ping entre terminales WiFi

Los resultados obtenidos al medir el RTT en 50 ocasiones entre el terminal WiFi 1 y el PC2 en la configuración infraestructura (en ambas direcciones) se muestran en la Figura 103. Similares resultados fueron obtenidos en sentido contrario, o sea desde el PC2 al terminal WiFi 1.

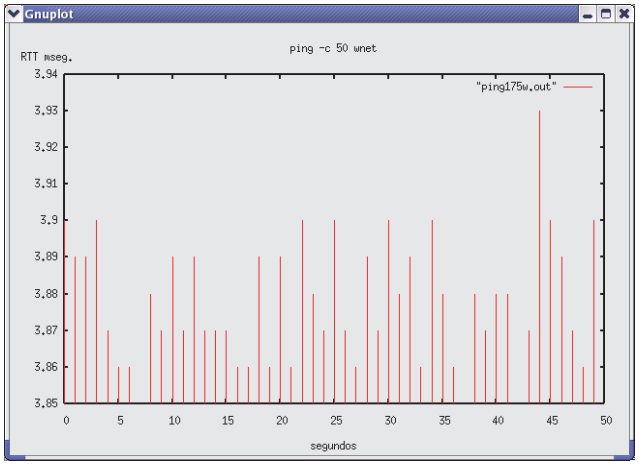


Figura 103. Ping entre terminales inalámbricos (a través del AP)

El RTT promedio es de 3,882 ms. El resultado para la misma prueba usando la configuración ad-hoc esta presentado en la Figura 104.

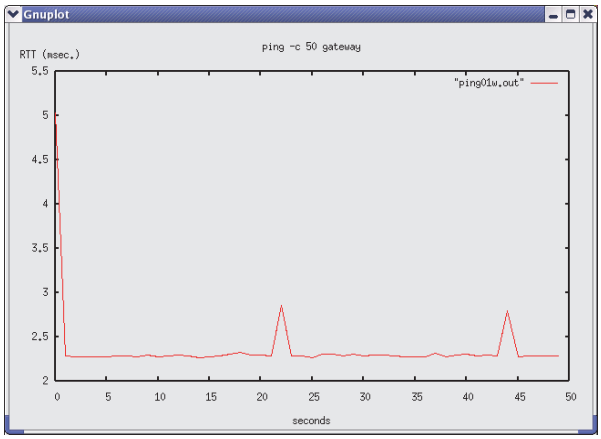


Figura 104. Ping entre los dos terminales WiFi (comunicación directa)

El RTT promedio es de 2,363 ms, que es menor que el caso anterior y también presenta una menor desviación estándar.

2. Iperf entre terminales WiFi

Los resultados obtenidos cuando medimos el ancho de banda (bps) estimado con *iperf* entre los dos terminales WiFi para la configuración en modo infraestructura se muestra en la Figura 105. En este caso se ha repetido el proceso unas 10 ocasiones. El ancho de banda promedio es 1,98 Mbps.

Los resultados para la misma prueba pero usando configuración ad-hoc se muestra en la Figura 106. El ancho de banda promedio es de 3,46 Mbps.

El ancho de banda en la red ad-hoc (comunicación directa) es aproximadamente el doble que en el caso de usar la configuración en modo infraestructura como era de esperar.

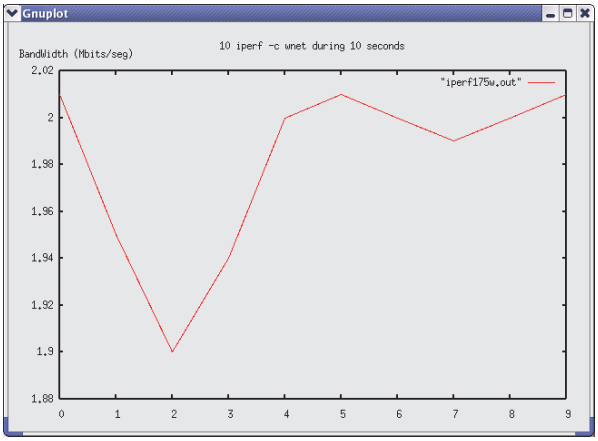


Figura 105. Resultado de iperf en modo infraestructura (a través del AP)

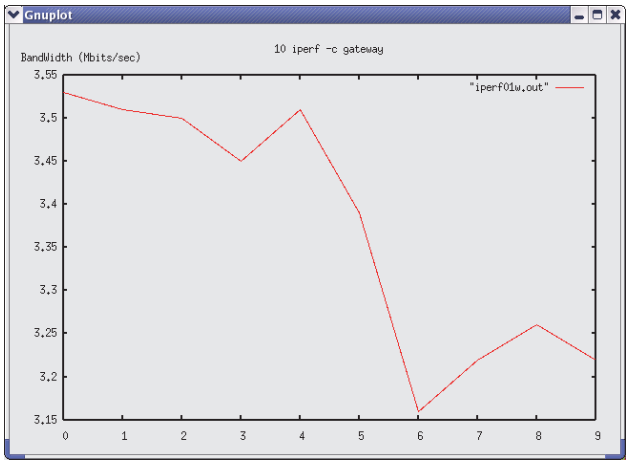


Figura 106. Resultado de iperf en modo ad-hoc (directo)

3. Netperf entre terminales WiFi

Similares resultados fueron obtenidos con la herramienta *netperf* repitiendo el proceso en 10 ocasiones (en configuración modo infraestructura y modo ad-hoc, respectivamente). Para el primero de ellos, el ancho de banda calculado y promediado es de 2,425 Mbps y para la última es de 3,96 Mbps. Igualmente como se esperaba, el ancho de banda es mejor en configuración modo ad-hoc como nosotros mostramos con la herramienta *iperf*.

4. Ping e iperf entre terminales WiFi

Esta prueba consistió en usar simultáneamente *ping* e *iperf*. Es importante resaltar el incremento detectado de los valores de RTT debido al tráfico iperf de forma simultánea. En la configuración en modo infraestructura, el promedio fue 29,102 ms y en la configuración ad-hoc 20,951 ms. Nuevamente es apreciable que los valores promedio son menores para la configuración ad-hoc.

5. Ping entre terminales WiFi con otros tráficos e iperf

En esta prueba combinamos el uso de *ping*, *iperf* y el envío de un archivo mediante FTP [185]. Los resultados en ambas configuraciones se muestran en la Figura 107 y Figura 108, respectivamente.

Como puede observarse, la utilidad ping y sus resultados están afectados por *FTP* e *iperf*. El RTT promedio en configuración modo infraestructura es 92,734 ms y el ancho de banda estimado 1,19 Mbps. En configuración modo ad-hoc, el RTT promedio fue

43,721 ms y el ancho de banda estimado 1,80 Mbps. Nuevamente es apreciable que las prestaciones en modo ad-hoc son mejores.

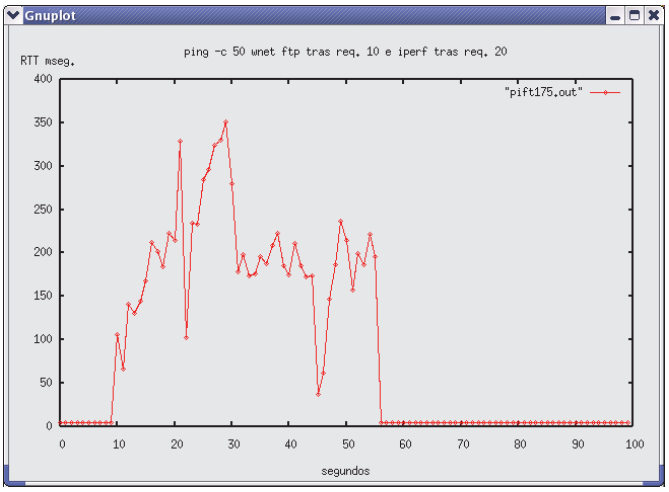


Figura 107. Medidas de RTT con ping, iperf y FTP en modo infraestructura

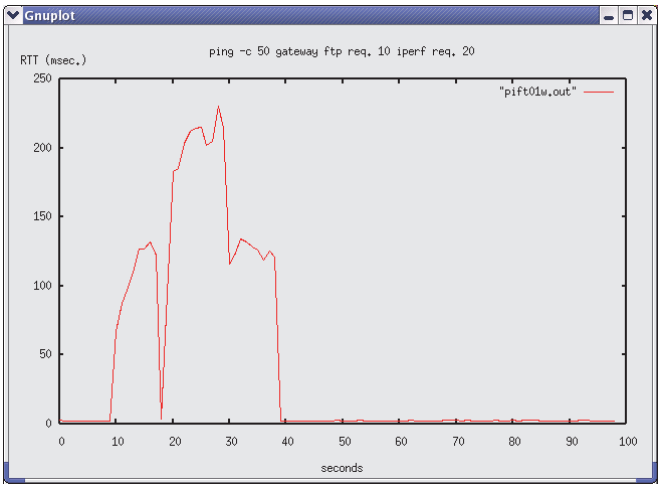


Figura 108. Medidas de RTT con ping, iperf y FTP en modo ad-hoc

6. Ping e iperf entre terminales WiFi y en red cableada

Finalmente, hemos medido el RTT entre el terminal WiFi 1 y el terminal en la red cableada (portátil y PC1 mostrado en las Figura 101 y 102). En la configuración infraestructura (Figura 101) la comunicación viaja a través del AP. Para la configuración ad-hoc, el Linux router (Figura 102) es el único que accede a la red cableada.

En las Figuras 109 y 110 mostramos los resultados obtenidos de ejecutar *ping* unas 50 veces (en configuración infraestructura y ad-hoc, respectivamente) y sobre el instante 10 insertar tráfico adicional con *iperf*.

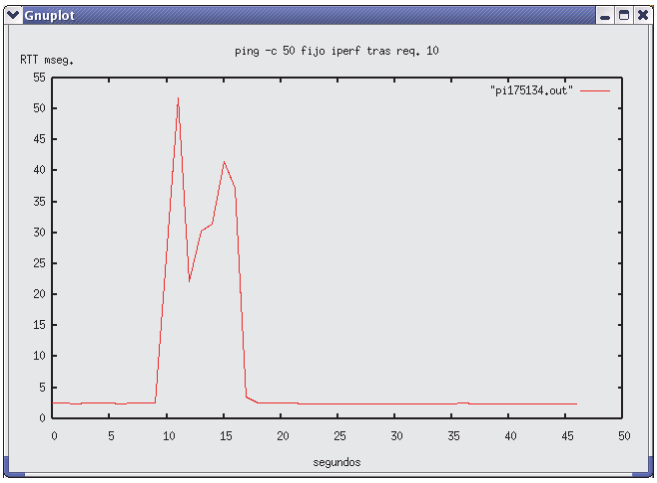


Figura 109. Medidas de RTT con ping en configuración infraestructura

El RTT promedio usando el AP sin tráfico adicional generado por *iperf* es 2,80 ms. Después de activar el tráfico de *iperf* (entre los paquetes 11 y 20), los valores mínimo, medio y máximo del RTT fueron 2,401 ms, 7,267 ms y 51,864 ms, respectivamente.

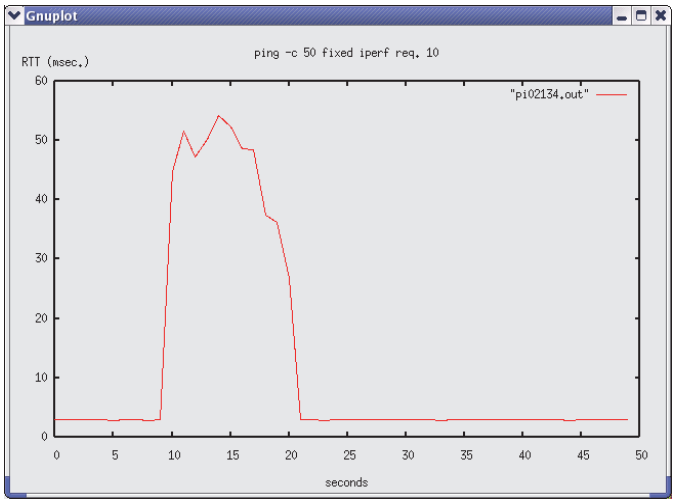


Figura 110. Medidas de RTT con ping en configuración ad-hoc con Linux router

El RTT promedio usando *Linux router* sin tráfico *iperf* fue 2,80 ms. Después de añadir el tráfico *iperf* (entre los paquetes el envío 11 y 20), los valores mínimo, medio y máximo fueron 2,825 ms, 12,197 ms y 54,242 ms, respectivamente.

Los valores obtenidos con *iperf* fueron de 5,54 Mbps y 4,18 Mbps, en configuración infraestructura y ad-hoc, respectivamente.

Por último, a modo de análisis final, tenemos que indicar que hemos observado que la configuración ad-hoc con el *Linux router*, el RTT promedio con tráfico *iperf* fue el mismo que usando un AP. No obstante, después de añadir el tráfico *iperf* en configuración ad-hoc el RTT es mayor. Estos resultados son debidos a las utilidades

IPtables [162] y la gestión NAT [186] en el PC2 (Linux Router), así como otras tareas propias de un computador de propósito general que están en ejecución. Obviamente, el AP es un dispositivo especializado que solo hace de puente entre la red WiFi y la red cableada pero el *Linux router* ejecuta otras muchas tareas. Esa es la razón porque nosotros obtenidos los resultados anteriores.

En la Tabla 35 se muestran los valores promedio de las diferentes pruebas realizadas en ambas configuraciones.

Según los resultados experimentales obtenidos, un aspecto bastante importante y relevante es que la configuración ad-hoc tiene mejores prestaciones que la configuración infraestructura, cuando los dispositivos que se comunican están en la misma subred y pueden comunicarse directamente, o sea es innecesario atravesar el AP si se garantiza conectividad física directa. En la configuración infraestructura, todos los paquetes requieren usar el AP a través del cual se establecen las comunicaciones entre los terminales inalámbricos localizados en la misma celda. Aunque nuestros resultados experimentales están en sintonía con la teoría clásica de estudios de transmisiones en WLAN, es importante medir estos efectos en entornos reales como el que nosotros hemos probado con tráfico real.

Tabla 35. Sumario de resultados experimentales (valores promedio)

Medida	*Número de experimentos*	*Configuración infraestructura (promedio)*	*Configuración ad-hoc (promedio)*
1	50 (solo RTT)	3,882 ms	2,363 ms
2	10 (*iperf)*	1,98 Mbps	3,46 Mbps
3	10 (*netperf*)	2,425 Mbps	3,96 Mbps
4	50 (RTT)	29,102 ms	20,951 ms
5	50 (RTT*, iperf, ftp*)	92,734 ms, 1,19 Mbps	43,721 ms, 1,80 Mbps
6	50 (RTT sin tráfico, RTT promedio, *iperf*)	2,80 ms, 7,267 ms 5,54 Mbps	2,80 ms, 12,197 ms 4,18 Mbps

El RTT promedio en redes WiFi en modo ad-hoc es menor que en modo infraestructura (ver pruebas 1, 4 y 5 en la Tabla 34) para comunicaciones entre terminales de la misma subred, ya que en el caso de modo infraestructura el AP debe ser

utilizado como un nodo intermedio. El RTT promedio entre el terminal WiFi 1 y el PC1 cableado (ver prueba 6 en la Tabla 34) es similar para ambas configuraciones.

Igualmente, el ancho de banda (bps) estimado en configuración ad-hoc en mayor que en configuración infraestructura para comunicaciones entre terminales WiFi (pruebas 2, 3 y 5). Por el contrario, cuando la comunicaciones son entre los terminales inalámbricos y los terminales en la red cableada, los resultados para configuración ad-hoc son peores (ver prueba 6), ya que el *Linux router*, como ya se indicó es un sistema más pesado y debe ejecutar otras muchas tareas.

Como los objetivos fueron obtener las mejores prestaciones para comunicaciones directamente sin perder la conexión con la red cableada, consideramos que estos resultados no reducen las ventajas y posibilidades de nuestra propuesta de configuración.

Algunas importantes consideraciones para usar un AP son los siguientes:

- Bajo coste.
- Incluye servidor DHCP [187].
- Soporta filtrado MAC.
- Mejor cobertura.
- Gestión de potencia de transmisión.
- Señalización.

No obstante, los dispositivos como los *Linux router* presentan algunas ventajas, como pueden ser:

- Mejor ancho de banda y RTT promedio para las comunicaciones entre terminales inalámbricos con conectividad física directa.
- Puede ser usado como servidor DHCP, DNS [188] y de autenticación.
- Puede ser utilizado para redireccionar/trasladar direcciones de red.
- Puede ser usado para filtrado MAC e IP.
- Permite intercambiar interfaces NIC/PCMCIA.
- Antiguos PC con Linux pueden ser usados y configurados como *Linux router* (reutilizar viejos PC).
- Fácil actualización de software y drivers.
- Es un computador que soporta los niveles transporte y aplicación.

- Soporte de otras aplicaciones (middlewares, control de admisión...).
- Puede ser usado como un potente instrumento para caracterizar el tráfico inalámbrico y cableado en la red. Nosotros podemos generar alguna información útil para almacenar trazas de tráfico de un terminal inalámbrico particular, que sea dependiente de la clase de tráfico que se utilizaría (cableado o inalámbrico).

5.2 Control de admisión y regulación de tráfico en origen

La arquitectura hardware que hemos usado para testear nuestra propuesta software esta mostrada en la Figura 111. En lugar de usar un AP convencional, decidimos usar un ordenador personal que se comporte como un encaminador hacia la red cableada con sistema operativo Linux y dos tarjetas de red: una Ethernet para la conexión con la red cableada y una NIC IEEE 802.11b/g para la red WiFi. Haciendo operar este como un Linux router tiene múltiples ventajas para nuestros objetivos: fuentes disponibles en código abierto (*kernel* y aplicaciones), soporte para base de datos de registro de nuestros usuarios, gestión de retransmisiones, filtrado y *masquerading* (*iptables* [162]), servidor web seguro (*https*) y funciones de control de tráfico.

En la Tabla 36 se muestra las características técnicas de los dos terminales cableados (ordenadores personales), los dos terminales WiFi (ordenadores portátiles), el ordenador personal que implementa el *Linux router* y el hub usado para nuestra implementación. Deliberadamente usamos inicialmente un PC de bajas prestaciones y ordenadores portátiles (excepto uno de ellos) ya que, en general, los PDA y muchos de los primeros teléfonos móviles con WiFi existentes en aquel momento tenían bajas prestaciones hardware. De esta forma, podemos obtener resultados relativos que pueden ser usados con esta clase de terminales WiFi. Las WNIC de terminales WiFi han sido configuradas en modo ad-hoc aunque el terminal remoto (destino) se encontraba en la red cableada. En cualquier caso, esta propuesta trabaja de la misma manera para una configuración en modo infraestructura dado que es trasparente a la misma.

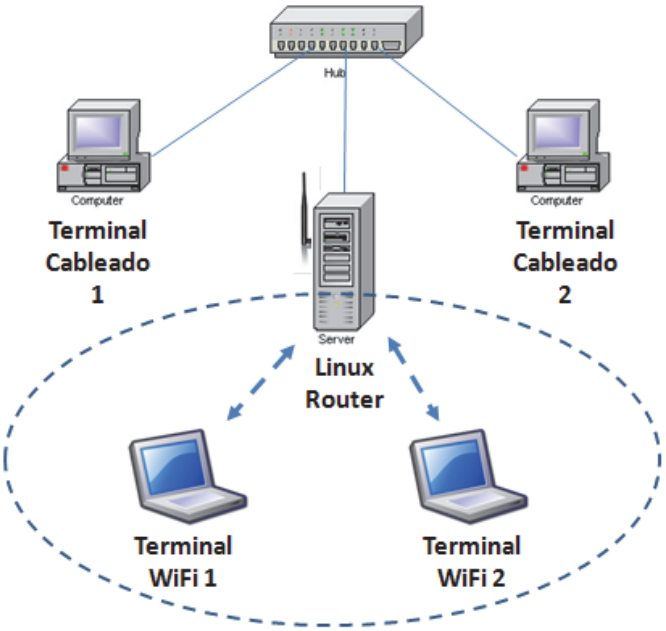


Figura 111. Arquitectura de pruebas con Linux Router (LRW)

Tabla 36. Características del hardware utilizado en la plataforma de pruebas

Terminal / hub	***Hardware***	***NIC***
Terminal cableado 1 (Linux Fedora Core 3)	PC, Pentium III 1Ghz, 512K RAM[1]	Ethernet / Fast Ethernet 10/100BaseT
Terminal cableado 2 (Linux Fedora Core 2)	PC, Pentium II, 400Mhz, 128M RAM	Ethernet / Fast Ethernet 10/100BaseT
Terminal WiFi 1	Pentium III 1Ghz, 256M RAM	*PCMCIA*[2] Compaq[3] IEEE 802.11b
Terminal WiFi 2	Pentium IV 3Ghz, 1G RAM	PCMCIA Dlink[4] IEEE 802.11b/g
Linux router (Fedora Core III)	PC, Pentium II 400Mhz, 196M RAM	PCMCIA Compaq IEEE 802.11b
Hub	Genius 8 Ports	Ethernet / Fast E. 10/100

[1] RAM (del inglés Random Access Memory), [2] PCMCIA (del ingles Personal Computer Memory Card International Association). [3] Compaq es una compañía registrada. [4] DLink es una compañía registrada.

Para posibilitar nuestro mecanismo de acceso a la red, es necesario realizar un proceso de solicitud a modo de control de admisión previo. Esto está materializado sobre un interfaz web a modo de portal cautivo que es gestionado por el gestor en el *Linux Router*. Cada usuario debe identificarse, como la mayor parte de sistemas, pero en este caso y de manera especial, se debe especificar qué servicio va a utilizar (opcionalmente, notificará sus requisitos de bitrate (ancho de banda necesario) para tráficos dependientes del tiempo). Con ello, como ya se comentó, el gestor podrá

calcular qué regulación debería aplicarse al terminal entrante y/o resto de terminales ya asociados, concretamente en el flujo o flujos activos o en proceso de iniciación.

En la Figura 112 se muestra la última versión de interfaz gráfica de la página web de entrada al portal cautivo. Este se configura en nuestro LRW gracias a los servicios web basados en *Apache*. Este incluye los documentos *html* (*admision.html* (5.6KB), *grafica.html* (6,5KB), *ayuda.html* (9,8KB), *barras.html* (1,6KB)), scripts de evaluación de formularios (*gen_validador.js*), archivos temporales (*registro_clientes.reg*), y especialmente, los scripts *admision.cgi* (13 KB) y *grafica.cgi* (11,3KB). Estos han sido programados en lenguaje C (*admision.c* (10 KB), *grafica_trafico.c* (12.1K)) y tiene un papel primordial para aceptar los datos de entrada necesarios, establecer la comunicación con el gestor y devolver respuestas al browser del cliente. Este canal de comunicación entre el motor web y el gestor se implementa mediante el mecanismo de comunicación entre procesos Linux.

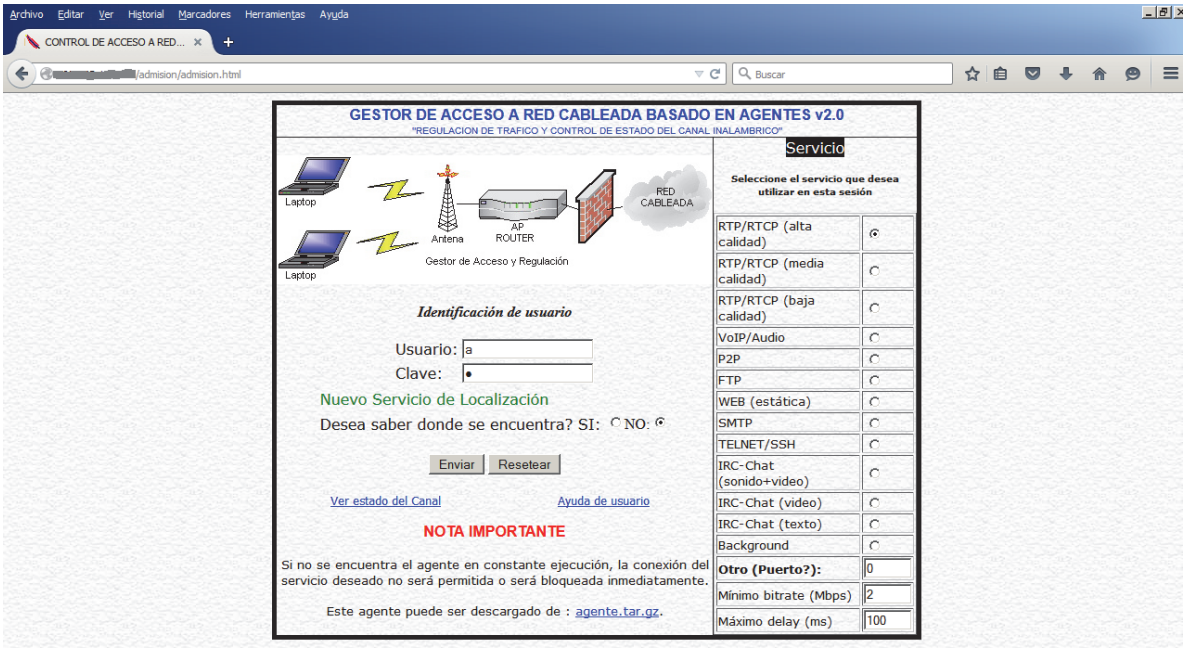


Figura 112. Interfaz web del portal cautivo del gestor en el LRW

Una vez procesada la solicitud, el gestor determina si se acepta o no la conexión y si el servicio puede ser atendido, se notifica al agente (en ejecución en los terminales WiFi) y al usuario del terminal las condiciones, o especialmente las restricciones de bitrate que tendría, salvo que haya habido algún error, como podría indicarse en la forma como la mostrada en la Figura 113.

Figura 113. Situación de acceso bloqueado por la plataforma

Si la solicitud ha sido aceptada, tras la comunicación entre gestor y el agente, se mostrará en el browser una página similar a la mostrada en la Figura 114.

Figura 114. Mensaje de acceso habilitado

El gestor (117KB) representa el núcleo central de nuestra plataforma y está programado en lenguaje C de forma modular con diferentes fuentes .c (*gestor.c* (163KB), *funcion_estado.c* (32 KB)). Requiere de varios archivos de configuración y gestión de accesos e incidencias (gestor.config, gestor.log), así como de diferentes archivos scripts para la gestión de servidor DHCP, NAT,... Los agentes, agente.c (75KB) han sido desarrollados igualmente en lenguaje C (plataforma Linux) y se puede descargar desde el propio portal cautivo (se presenta empaquetado y comprimido en el archivo agente.tar.gz (*agente.c* (57.6 KB), *funcion_estado.c* (32 KB), scripts Tcl/tk, imágenes en formato png y gif, otros). Ambos requieren los archivos fuente *iwlib.c* (80 KB) e *iwlib.h* (16 KB) que forman parte de las librerías *wireless-tools* [190]. Entre el gestor y los agentes se crean y se gestiona el intercambio de mensajes (órdenes y respuestas) a través del canal de control. Mediante los mismos, el agente deberá actuar sobre las colas internas de salida en la WNIC de los terminales WiFi implicados. Dado

el lenguaje utilizado para los agentes y el gestor, nuestras pruebas han sido realizadas sobre terminales WiFi operando con Linux. Implementaciones sobre otros sistemas operativos requerirían la programación de los agentes y su interacción específica con el núcleo del Sistema Operativo local para la gestión de colas y el canal de comunicaciones UDP/IP con el gestor. Para el agente hemos considerado que su ejecución se realizase en segundo plano, para que su presencia sea transparente al usuario del terminal. En cuanto al gestor, este puede activarse tanto en segundo plano como de forma interactiva, si se desea hacer un seguimiento por parte del administrador.

Los agentes procesan las órdenes del gestor de la siguiente forma:

- Ante la orden *HELLO* deberá responder automáticamente con información de estado del terminal correspondiente.
- Ante las órdenes *UPDATE*, se utilizará la orden apropiada del *kernel* para reducir/aumentar la tasa de bits por segundo indicada y posteriormente, confirmar al gestor su aplicación. Esto se realiza haciendo uso de la utilidad *tc* (*traffic control*) [129] de Linux.
- Ante la orden *TIME-OUT,* se confirma al gestor la recepción y se notifica al usuario visualmente. Tras esta orden, el servicio que estaba siendo utilizado está bloqueado por haberse excedido el tiempo de conexión. En la Figura 115 se muestra el mensaje que se visualiza en el cliente ante la recepción de esta orden (tiempo excedido de conexión).

Figura 115. Mensaje de aviso de tiempo de acceso excedido

Para las diferentes pruebas realizadas de esta implementación de regulación dinámica, inicialmente, evaluamos el ancho de banda disponible real (B_m). Se obtuvo un valor promedio de unos 5 Mbps con la herramienta disponible *iperf* para la configuración WiFi IEEE 802.11b. Las mismas medidas han sido realizadas y se aprecia su escalabilidad extensible para redes IEEE 802.11 mejoradas (g, n...).

A continuación, se introduce tráfico desde el terminal WiFi 1 dirigido hacia el terminal cableado 1 usando la aplicación *iperf*. El primero actúa como el cliente *iperf* y el último como el servidor. El experimento fue repetido con el terminal WiFi 2 y el terminal 2 de la red cableada. El objetivo de este experimento fue calcular la máxima tasa que podríamos obtener cuando existe solo una comunicación en la red procedente desde el terminal WiFi 1 o del terminal WiFi 2, respectivamente.

La Tabla 37 muestra un resumen de los resultados obtenidos. La segunda columna muestra la tasa de datos y la tercera columna muestra la cantidad de información transmitida. Las diferencias obtenidas en ambos experimentos son debidos a las diferentes WNIC usadas para ambos pruebas (el terminal WiFi 1 usa una WNIC IEEE 802.11b y la segunda una WNIC IEEE 802.11g).

Tabla 37. Máxima tasa de datos entre una fuente (WiFi) y un destino (cableado)

Fuente→Destino	***Tasa de datos***	***Información***
Terminal WiFi 1 → Terminal cableado 1	3.89 Mbps	4.71 MB
	3.95 Mbps	4.74 MB
	3.95 Mbps	4.73 MB
	3.94 Mbps	4.70 MB
	3.93 Mbps	4.70 MB
	3.95 Mbps	4.70 MB
Terminal WiFi 2 → Terminal cableado 2	5.44 Mbps	6.52 MB
	5.48 Mbps	6.58 MB
	5.44 Mbps	6.52 MB
	5.47 Mbps	6.58 MB
	5.47 Mbps	6.55 MB

A continuación, repetimos el experimento considerando ambos terminales WiFi transmitiendo simultáneamente. Como se ve en los resultados, las tasas se han reducido en ambos terminales debido a la contienda en el canal físico entre los dos terminales y sin aplicar la regulación de tráfico como se muestra en la Tabla 37. En este caso la tasa de datos y la cantidad de información del terminal WiFi 1 son ahora reducidas por un factor de 2, aproximadamente. Para el tráfico del terminal WiFi 2 este factor es aproximadamente 1,4.

Para evaluar nuestro mecanismo de regulación de tráfico, el gestor se configura para forzar al terminal WiFi 1 a limitar su tasa de inserción de tráfico a 125 Kbps de forma prefijada.

Tabla 38. Máxima tasa sin regulación dos fuentes (WiFi) y dos destinos (cableados)

Fuente→Destino	***Tasa de datos***	***Información***
Terminal WiFi 1 → Terminal cableado 1	1.73 Mbps 1.75 Mbps 1.73 Mbps	2.08 MB 2.11 MB 2.08 MB
Terminal WiFi 2 → Terminal cableado 2	3.66 Mbps 3.69 Mbps 3.68 Mbps	4.39 MB 4.44 MB 4.43 MB

En este experimento, la regulación no es aplicada al terminal WiFi 2 para simular que este terminal gestiona un tráfico de alta prioridad (por ejemplo tráfico dependiente del tiempo CBR). Los resultados se muestran en la Tabla 39. Como se puede observar, con la regulación, el terminal WiFi 2 puede transmitir una mayor cantidad de datos y opera a una muy cercana tasa máxima de datos, como la mostrada en la Tabla 37.

Tabla 39. Máxima tasa de datos con regulación entre terminales WiFi y cableados

Fuente→Destino	***Tasa de datos***	***Información***
Terminal WiFi 1 → Terminal cableado 1	125 Kbps 125 Kbps 125 Kbps 125 Kbps 125 Kbps	168 KB 168 KB 168 KB 168 KB 168 KB
Terminal WiFi 2 → Terminal cableado 2	5.27 Mbps 5.24 Mbps 5.26 Mbps 5.31 Mbps 5.27 Mbps	6.32 MB 6.28 MB 6.30 MB 6.38 MB 6.33 MB

El siguiente experimento consistió en testear los efectos de la inyección de tráfico *FTP* desde terminal WiFi 2 (tráfico no prioritario), y tráfico *RTP/RTCP* desde el terminal WiFi 1 (tráfico prioritario). Hicimos el experimento múltiples veces: algunas de ellas sin el mecanismo de regulación de tráfico y otras con él. Para transmitir un video MPEG-4 de 2.992 KB de tamaño y 17 segundos de duración, usamos como servidor y reproductor el software *VLC* de *VideoLAN*. Con ambos experimentos, estábamos interesados en analizar la experiencia del usuario según la mayor o menor disponibilidad de canal para este video prioritario. En el caso de que el usuario conozca el bitrate del video puede indicarlo en el interfaz de control de admisión para afinar

mejor la regulación. Si no lo conociese simplemente indicaría alta, media o baja calidad para tráfico RTC/RTCP.

Cuando ninguna regulación de tráfico fue aplicada para el tráfico FTP, muchas tramas de video se perdieron y como resultado, el usuario experimenta reproducciones intermitentes y *pixelados*. Por el contrario, cuando la regulación fue aplicada, la calidad de la reproducción mejoro enormemente, no detectándose ninguna incidencia relevante ni pérdida de paquetes. Obviamente, la duración de la transmisión FTP se incrementó, ese era el compromiso de este tráfico no prioritario como ya describimos en el apartado 3.2.

Posteriormente repetimos el proceso anterior pero con dispositivos basados en tecnologías más recientes como IEEE 802.11n y con configuración dinámica de regulación desde el gestor. En todas las pruebas realizadas, al contar con la estimación de máximo ancho de banda del canal gestionado por el *Linux Router*, el gestor calcula los requisitos que debe aplicar a los flujos no prioritarios, y por tanto el valor de coeficiente de regulación para garantizar una mayor disponibilidad de canal para flujos prioritarios. Recordemos que estos coeficientes de regulación los definimos como unos parámetros específicos para cada flujo y eran la base de nuestro modelo de optimización paramétrica aplicando regulación de flujos $C_T = \sum\sum \propto_i^{ki} f_i^{ki}$, comentados al final de apartado 3.2. Con nuestro sistema de regulación de tráfico en el terminal guiado desde el gestor, hemos obtenido unos resultados adecuados asignando un alto coeficiente $\propto_i^{ki}$ para flujos multimedia y bajos para otros flujos. En todos los casos de prueba realizados, la QoE observada para flujos multimedia se mejoró considerablemente cuando se limitaron los flujos no prioritarios respecto a cuándo no se aplicaron regulaciones. Como ya se comentó previamente, los agentes aplican la regulación con funciones de control de tráfico desarrolladas para el *kernel* de Linux (*iproute* y *Traffic Control* (*TC*)).

Como últimas pruebas hemos utilizado la misma herramienta como generadora de tráfico y de medida, o sea *iperf*, que permite medir las prestaciones de las redes (throughput). Dado que inyecta una gran cantidad de tráfico, crea muchos problemas al resto de aplicaciones (retrasos, pérdidas y cortes en la comunicación). Para analizar la experiencia visual del usuario, hemos vuelto a generar tráfico multimedia *RTP*/*RTCP* mediante la aplicación *VLC* y usando *mplayer* desde un servidor web como soporte de dichos contenidos. La calidad de la señal multimedia cuando *iperf* inyectaba tráfico era

muy mala (largos períodos de inactividad, pérdida de paquetes y *pixelados*). Por el contrario estos efectos se limitaron cuando a *iperf* se le aplicó regulación mediante esta funcionalidad aplicada por el agente correspondiente.

Hay que tener en cuenta, que dado el dinamismo de terminales que entran o salen de la red, se requiere adaptar el tráfico no sólo para el terminal que se asocia, sino también para el resto de terminales. Por ello existe en el gestor una base de datos con todos los terminales participantes para controlar su estado y sus regulaciones de tráfico, así como el resto de parámetros que afectan a esta funcionalidad (ver apartado 4.2). De forma repetitiva y basada en temporización, cada cierto tiempo (configurable para no sobrecargar la red con tráfico de control) se sondea a todos los terminales para determinar su estado.

La comunicación del canal de control se ha realizado mediante el protocolo de transporte UDP. Esto permite no sobrecargar el canal con mucho tráfico y reducir las conexiones existentes con los Linux router (recursos limitados). Además, el protocolo de comunicación y las acciones a realizar siguen un modelo petición-respuesta.

Complementariamente a las pruebas anteriores, mediante una aplicación independiente también desarrollada en C y comentado previamente, denominada *Packetinjection*, pudimos generar tráfico masivo en el canal (denominado *tráfico interferente*). Con esta aplicación hemos creado e insertado tráfico en la red que produce una saturación del canal y, además podemos variar la latencia y el tamaño de las tramas insertadas para testear su efecto sobre otras comunicaciones, con y sin regulación. En la Figura 116 se muestra la capacidad teórica disponible en *Mbps* (C_T) para nuestro escenario y los instantes de tiempo en los que usó de forma simultánea con la herramienta *Packetinjection.*

Los resultados experimentales mostrados en la Figura 116 en intervalos temporales de 10 en 10 representan:

- Instantes de prueba entre el 1 y 10: solamente tráfico *iperf*. En este caso se obtienen valores en torno a los 65 Mbps.
- Instantes de prueba entre el 11 y 20: se inyecta tráfico interferente con tramas de 1.500 Bytes con la mínima latencia entre tramas. En este caso se aprecia que este tráfico interferente permite solo unos 2 Mbps (excesivamente bajo para soportar cualquier comunicación prioritaria (por ejemplo video en formato MPEG4).

- Instantes de prueba entre el 21 y 30: se detiene el tráfico interferente y la velocidad retorna a los niveles iniciales aunque algo más dispersos.

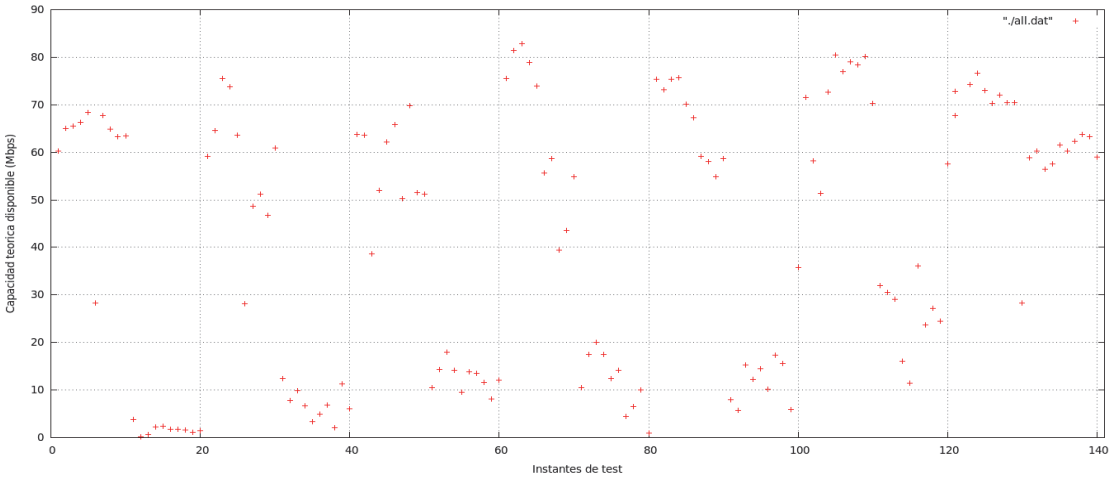


Figura 116. Efecto de tráfico interferente en capacidad de canal en IEEE 802.11n

A la vista de los resultados obtenidos, se observa una degradación importante en la disponibilidad del canal WiFi. A continuación se analiza el comportamiento de la regulación del tráfico interferente limitándolo con distintos valores de los coeficientes $\propto_i^{ki}$ (nótese que tenemos un solo flujo interferente a regular (*Packetinjection*) y otro sin regulación (*iperf*)).

- Instantes de prueba entre el 31 y 140: se aplica diferente regulación al tráfico interferente:
  - 20 Mbps entre los instantes 31 y 40,
  - No se regula el tráfico interferente en el intervalo entre el 41 y 50,
  - 18 Mbps entre los instantes 51 y 60,
  - No se regula el tráfico interferente en el intervalo entre el 61 y 70,
  - 15 Mbps entre los instantes 71 y 80,
  - No se regula el tráfico interferente en el intervalo entre el 81 y 90,
  - 10 Mbps entre los instantes 91 y 100,
  - No se regula el tráfico interferente en el intervalo entre el 101 y 110,
  - 5 Mbps entre los instantes 111 y 120,
  - No se regula el tráfico interferente en el intervalo entre el 121 y 130,
  - 1 Mbps entre los instantes 131 y 140.

Nótese que solamente se consiguen capacidades elevadas, por encima de 50 Mbps, cuando el tráfico interferente está limitado a 1 Mbps frente a los 75 Mbps que solo se consiguen cuando no hay tráfico interferente. Estos datos corroboran la necesidad de aplicar regulación a ciertos flujos en beneficio de otros, que hemos considerado prioritario y por ser en general dependientes del tiempo. Con ello se puede garantizar una mayor disponibilidad del canal para los mismos y alcanzar sus requisitos de máximo bitrate, mínimos retrasos u otras características.

Indicar, que además de las funciones principales indicadas para este módulo, el gestor está configurado para localizar el canal menos ocupado y se active para operar en dicho canal. Para ello hace un scanning inicial y de forma automática se configura en el que menos dispositivos de red encuentre. Gestiona los diferentes archivos de registro de usuario y tráficos, además permite obtener información desde los agentes acerca del estado de sus interfaces mediante el mensaje INFO_IFACE_REQUEST/REPLY. Además como se comentó en el apartado 4.2, si dispone de un sniffer operando en otro interface (opcional) y se detecta excesiva tráfico, automáticamente se notifica a los agentes un cambio de canal con los mensajes CHANGE_CH_REQUEST/REPLY, que hemos denominado forzado. Este cambio de canal, también está habilitado para que sea opcional y se invite al agente del terminal especificado, y este lo haga al usuario, de un cambio manual a un especificado AP. Además incorpora un control de número de conexiones permitidas así el tiempo de duración de las mismas configurable por el administrador en el archivo gestor.config.

5.3 Traspaso de terminales entre AP

Para evaluar la propuesta planteada de traspaso de terminales WiFi entre los diferentes AP, hemos hecho uso de la misma plataforma de pruebas utilizada en las propuestas anteriores. Ahora la hemos renombrado plataforma multifuncional, dado que le incorporamos diferentes funcionalidades. A modo de recordatorio indicar que está formada por varios ordenadores personales que ejecutan el sistema operativo Linux. Uno de estos ordenadores actúa como AP y se les ha habilitado la funcionalidad de *Linux router* para implantar el gestor. Por otro lado, en cada terminal asociado al Linux router (AP en general) se instalan los agentes. Como ya se ha indicado, ambos programas gestor y agente, han sido programados en el lenguaje C. Para definir claramente cada funcionalidad las hemos denominado mediante el término módulo. De

tal forma el mecanismo de regulación y control de admisión lo denominamos Módulo I: Mecanismo de regulación de tráfico (ya analizado en los apartados 4.2 y 5.2) y Módulo II: Traspaso de terminales, del que ahora presentamos su implementación práctica y los resultados experimentales.

Para evaluar la implementación del Módulo II fue necesario añadir otro *LRW* que gestione otra celda y con ello habilitar el mecanismo de traspaso entre *LRW* de terminales WiFi. Para esta funcionalidad se considera que su uso es particularmente importante en el caso de configuraciones modo infraestructura, si bien el modo ad-hoc como vimos en la primera de las propuestas podría ser perfectamente válido, pues la conectividad entre los LRW o AP se garantizaba por su interfaz con la red cableada. Por tanto vamos a suponer que los LRW operan más como un AP tradicional y se configuran en modo infraestructura, a diferencia de cómo hasta ahora estábamos haciendo en modo ad-hoc. Resultados equivalentes se obtienen si se instalan en los LRW el software *hostapd* [189] [190] [191], ampliamente utilizado por otros autores, que habilita a un ordenador personal con Linux comportarse perfectamente como un AP. Esta consideración parece evidente hacerla pues las redes basadas en múltiples AP son muy habituales y dan conectividad a terminales WiFi en diferentes zonas manteniendo su acceso a Internet, quedando las comunicaciones entre terminales en segundo plano.

En la Figura 117 se muestra la configuración utilizado para las pruebas experimentales de la propuesta de traspaso de terminales entre AP (*Linux router*).

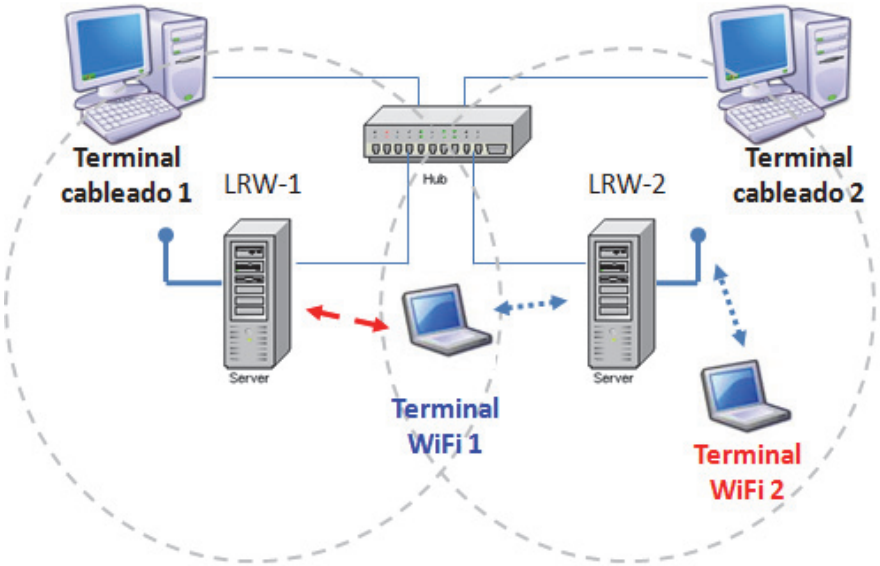


Figura 117. Plataforma de pruebas experimentales del módulo II (caso 1)

En la Tabla 40 se detallan las características de los equipos utilizados para evaluar la funcionalidad planteada.

Si recordamos brevemente la idea propuesta, esta consistía en habilitar desde los LRW la posibilidad de guiar o forzar a un determinado terminal asociado a alguno de ellos a cambiarse de LRW para mejorar las prestaciones de él o del resto de terminales. En la Figura 117 observamos que el terminal WiFi 1 podría estar asociado al LRW-1 y en cambio lo está con el LRW-2 compitiendo por el uso del canal con el otro terminal que no tiene otra opción que hacer uso del LRW-2 para acceder a cualquiera de los terminales cableados o en general a Internet.

Tabla 40. Características hardware y software plataforma de la Figura 115

Terminal / hub	***Hardware***	***NIC***
Terminal WiFi 1	Pentium IV 3Ghz, 1G RAM	PCMCIA Dlink [155]IEEE 802.11b/g
Terminal WiFi 2	Pentium III 1Ghz, 256M RAM	*PCMCIA*[2] Compaq [175]IEEE 802.11b
LRW-1 (Linux router1) (Fedora Core III)	PC, Pentium II 400Mhz, 196M RAM	PCMCIA Compaq IEEE 802.11b
LRW-2 (Linux router2) (Fedora Core III)	PC, Pentium II 400Mhz, 128M RAM	PCMCIA Compaq IEEE 802.11b
Hub	Genius 8 Ports	Ethernet /Fast Ethernet 10/100 Mbps

Tras varias pruebas realizadas, se ha comprobado que con el uso de esta funcionalidad, el terminal WiFi 1 aparece asociado al LRW-1 (en general AP1) dejando el canal 2 completamente libre para el terminal WiFi 2. En esta plataforma, dado que solo el terminal 1 detecta a ambos LRW (AP), es el único terminal que podría ser objeto de traspaso. En este caso no solo por ser la única opción válida dado que el terminal WiFi 2 no detecta (fuera de cobertura) al LRW-1, sino que además como el LRW-1 no tenía terminales asociados, las condiciones de traspaso indicaban como primer criterio: un terminal por cada LRW (AP). Estas primeras pruebas en las condiciones mostradas en la Figura 117 eran técnicamente muy simples. En cambio, en

otros casos más complejos, hemos hecho múltiples pruebas en las que dos o más terminales se ubican en la intersección (Figura 118).

Obviamente, en estos casos, el proceso es mucho más elaborado y complejo. Requiere un mayor tratamiento algorítmico de análisis y comparación de las condiciones de estado de cada terminal (flujos) y estado de los canales. En estos casos si los terminales están asociados al LRW-2 (AP2), este determinará dinámicamente que terminal traspasar en base al servicio que esté utilizando cada terminal y el conocimiento que tiene del estado del LRW-1 (AP1) receptor. Dependiendo de dichas condiciones, especialmente que flujos soportaban cada terminal se traspasaba uno u otro siguiendo los criterios marcados en base a los parámetros predefinidos indicado en al apartado 4.3.

Esto confirma la flexibilidad del proceso y su dependencia de las condiciones. Para tener un mayor control de estas acciones, las características para realizar el traspaso son configurables en el módulo desarrollado (umbrales para comparación y evitar bucles (histéresis), máximo número de terminales, servicios soportados, umbrales de traspaso, condiciones temporales...).

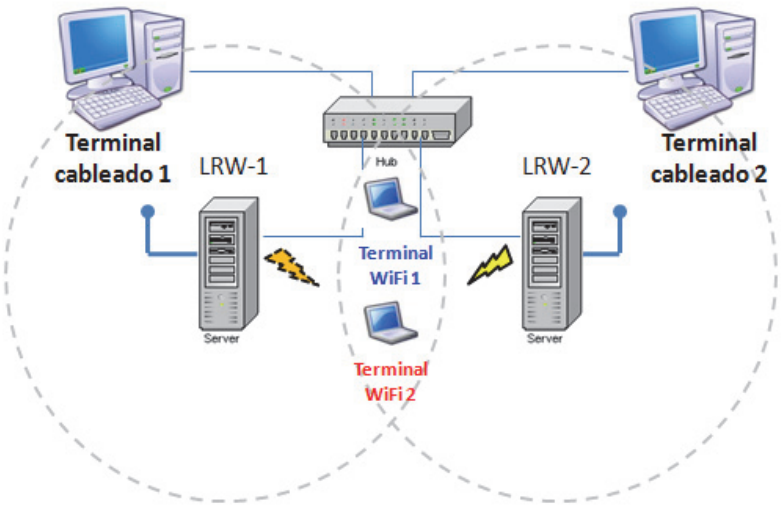


Figura 118. Plataforma de pruebas experimentales del módulo II (caso 2)

Las órdenes o mensajes (PDU detalladas en el apartado 4.3) transmitidos entre todos los elementos participantes se soportan sobre el protocolo de transporte UDP, para no sobrecargar la red. Para evitar bloqueos ante mensajes sin respuesta, se han habilitado los correspondientes temporizadores e interrupciones.

Para hacer un proceso de traspaso más completo, hemos permitido dos tipos de traspaso: uno manual y otro automático. En el primer caso, como su nombre indica, una vez los gestores han decidido traspasarse un terminal, solamente se le notifica al usuario del terminal escogido para que inicie la re-asociación al AP especificado de forma manual. En este caso, se trata de una sugerencia que se le hace al usuario y, puede éste, decidir si lo realiza o no. El mensaje que se visualiza es similar al mostrado en la Figura 119.

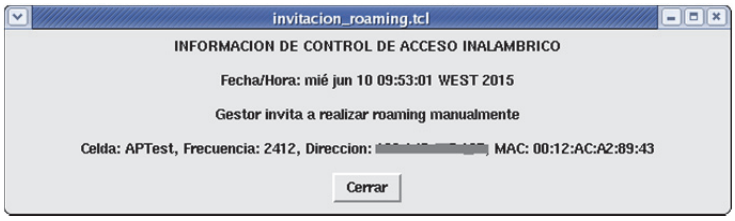


Figura 119. Mensaje visual sugiriendo un traspaso al LRW (AP) indicado

En el segundo caso es totalmente transparente y automático, apareciendo el terminal asociado al LRW-1 (AP) receptor correspondiente, si todo ha ido bien. En la Figura 120 se muestra información al usuario al producirse un traspaso correctamente con el mensaje enviado por el LRW-1 (AP) receptor.

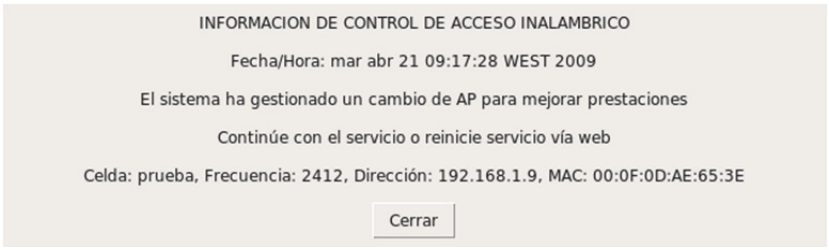


Figura 120. Mensaje mostrado tras un traspaso automático

Destacar que en las múltiples pruebas realizadas para los traspasos de terminales se comprueba que los tiempos de transmisión, RTT, bitrates y calidad visual conseguida (por ejemplo para las aplicaciones *ftp*, *iperf*, *vlc*...) eran mejores cuando se disponía de un uso exclusivo de celdas/canales o un menor número de flujos en el canal, tal y como pretendíamos con la funcionalidad de este módulo. Como ya se ha comentado, esta característica es especialmente necesaria cuando los servicios utilizados son dependientes del tiempo y evidentemente complementaria a la anterior propuesta. Mantener los servicios activos durante el traspaso no son motivo de estudio en esta propuesta ni forman parte de esta tesis, sino simplemente reubicar/reasociar los terminales. En cualquier caso, consideramos importante indicar que para un

mantenimiento de las conexiones fuese posible, ya existen especificaciones de *handoff o handover* [192] implementadas en el MAC IEEE 802.11 y además podrían requerirse de una gestión o reconfiguración de direcciones de red (direcciones IP mediante *mobile IP* [193] u otras acciones) de forma complementaria, si fuese necesario para mantener las conexiones de niveles superiores (red, transporte y aplicación).

5.4 Localización de terminales. Reubicación

Una vez implantada esta funcionalidad en nuestra aplicación, que recordemos se denomina plataforma multifuncional, se han realizado diferentes pruebas. En este caso es necesario recordar la zona utilizada para dichas pruebas son las dependencias del Departamento de Ingeniería Telemática en la segunda planta del Pabellón C de los Edificios de Telecomunicación de la Universidad de Las Palmas de Gran Canaria (ULPGC). Se han utilizado como patrones para la BD de coberturas, los AP que dan cobertura WiFi a la red universitaria de acceso gratuito con *SSID: ULPGC* y, complementariamente con la red virtual de acceso inter-universitario *SSID: EDUROAM* con acceso restringido. Además, hemos activado uno de los gestores en uno de los equipos actuando como *LRW* actualizado con la funcionalidad de localización en el interior de uno de los despachos. Además se ha adaptado el interfaz web para soportar la petición de localización inicial realizada por el usuario desde el terminal WiFi.

Esta funcionalidad está habilitada para los usuarios a través del interfaz web (Figura 112), ya que se permite a cualquier cliente desde su browser acceda al portal cautivo y solicite dicha petición (*LOCATION*). Tras la entrega del formulario, se activa el proceso con el gestor. Este solicita los rastreos actualizados al agente correspondiente y con su respuesta busca en la BD la estimación de posición. Esta estimación será devuelta al browser en una página html (*INFO_LOCATION*). Esta puede incluir una imagen de la zona (si se dispone) o en modo texto, según se configure. El gestor dispone de la capacidad de activar de forma autónoma el proceso de *SCAN* sin que el intervenga el usuario, como complemento a la funcionalidad de *TRASPASO*, pues del conocimiento físico del terminal puede servir para mejorar la visión de AP/LRW vecinos.

Para crear la BD hemos utilizado un ordenador portátil con *Ubuntu 8.10* [194]. Primero se realizó un proceso de captura de datos de AP visibles (barrido de frecuencias) desde cada una de las diferentes dependencias, y con esos datos y su tratamiento posterior (eliminación de datos aislados, erróneos, cálculo de valores medios, búsqueda de mínimos y máximos…), se elabora el mapa de coberturas (BD). Para realizar las medidas hemos utilizado las funciones *wireless-tools* de Linux [190]. En la Figura 121 se muestra la planta de la zona de medidas en el momento como se encontraba durante estas pruebas experimentales.

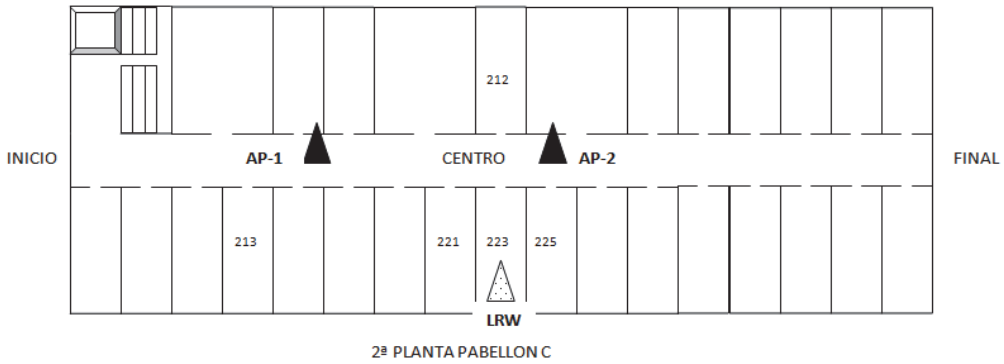


Figura 121. Esquema interno de distribución de despachos y AP

La zona escogida se describe en el capítulo 3. Para realizar estas pruebas se seleccionaron diferentes despachos y al menos cuatro zonas del pasillo. Durante la mismas, únicamente se encontraban activos 2 AP denominados *AP-1* (aproximadamente a 1/4 del fondo del pasillo) y *AP-2* (aproximadamente a 3/4 del pasillo) (marcados con triángulos en la Figura 120). En estas zonas se han capturado los siguientes datos: *Zona* (cadena de caracteres que identifica posición), *MAC* (cadena formado por los 6 bytes separados por el carácter "**:**" como dirección MAC de cada interfaz IEEE 802.11 de cada AP), *SSID* (cadena de caracteres de identificación del AP), *Frecuencia* (valor de frecuencia, en la forma de un número entero de 4 cifras 24**), *Canal* (canal de emisión (en la forma de un número entero de una o dos cifras)), *Niveles de RSS* (valor mínimo, medio y máximo del valor de RSS y de referencia de señal recibida), *Niveles de Señal* (valor mínimo, medio, máximo del nivel de señal recibida), *Niveles de Ruido* (valor mínimo, medio, y mínimo del nivel de ruido recibido). Una aproximación sobre la cobertura de los dos AP se muestra en la Figura 122.

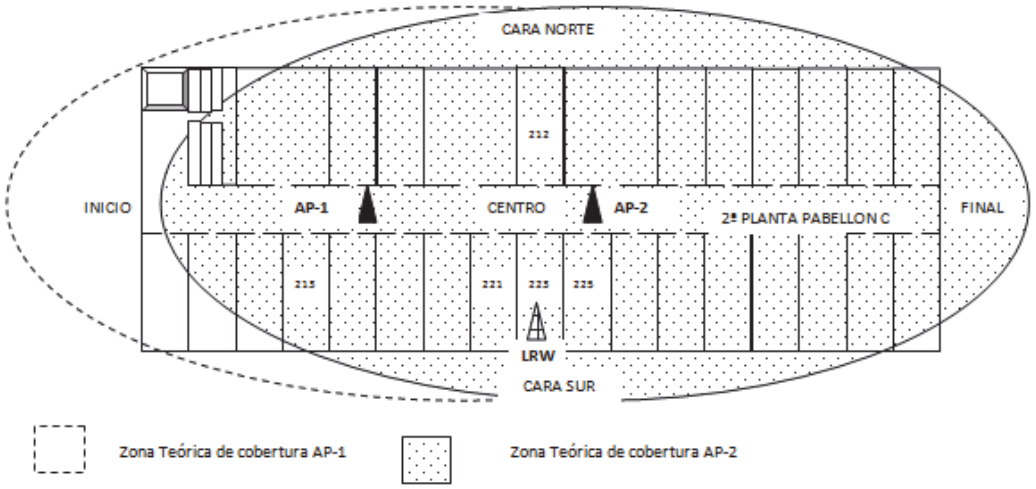


Figura 122. Recreación de coberturas de AP-1 y AP-2 en zona de pruebas

El *driver* utilizado para gestionar dispositivos basados en el chip de comunicaciones *Atheros* [195] incorporados en la interfaz inalámbrica del terminal WiFi Linux fue *mad-wifi* [196]. En la Figura 123 se muestra un fragmento de la BD creada.

ZONA	MAC	SSID	Freq./Canal	RSS Min, med, max	RSS Min, med, max	Señal min-med-max	Ruido min-med-max
.....							
Inicioct	00:12:01:B5:5B:81	ULPGC	2412 1	13 21 33	70 70 70	-62 -73 -82	-95 -95 -95
Inicioct	00:12:01:B5:62:D1	ULPGC	2432 5	21 28 39	70 70 70	-56 -66 -74	-95 -95 -95
Inicioct	00:0F:24:EC:FA:41	ULPGC	2412 1	14 15 16	70 70 70	-79 -79 -81	-95 -95 -95
Inicioct	00:14:A9:75:09:11	ULPGC	2462 1	11 12 13	70 70 70	-82 -85 -93	-95 -95 -95
Inicioct	00:12:01:B5:61:F1	ULPGC	2442 7	32 33 36	70 70 70	-59 -61 -63	-95 -95 -95
Inicioct	00:12:01:B5:69:71	ULPGC	2422 3	23 29 38	70 70 70	-57 -65 -72	-95 -95 -95
Inicioct	00:12:01:B5:66:B1	ULPGC	2447 8	21 22 27	70 70 70	-68 -72 -74	-95 -95 -95
Inicioct	00:12:01:B5:65:21	ULPGC	2447 8	17 19 25	70 70 70	-70 -75 -78	-95 -95 -95
Inicioct	00:12:01:B5:5E:71	ULPGC	2452 9	18 21 30	70 70 70	-65 -73 -77	-95 -95 -95
Inicioct	00:12:01:B5:49:A1	ULPGC	2457 10	24 25 27	70 70 70	-68 -69 -71	-95 -95 -95
Inicioct	00:14:A9:75:05:B1	ULPGC	2422 3	9 9 9	70 70 70	-86 -86 -86	-95 -95 -95
Inicioct	00:12:01:B5:61:81	ULPGC	2452 9	6 6 6	70 70 70	-89 -89 -89	-95 -95 -95
Inicioct	00:0F:24:EC:FE:71	ULPGC	2437 6	10 11 12	70 70 70	-83 -84 -85	-95 -95 -95
.....							
213	00:12:01:B5:5B:81	ULPGC	2412 1	18 23 26	70 70 70	-69 -71 -77	-95 -95 -95
213	00:12:01:B5:62:D1	ULPGC	2432 5	29 31 35	70 70 70	-60 -63 -66	-95 -95 -95
213	00:12:01:B5:5B:80	EDUROAM	2412 1	18 23 26	70 70 70	-69 -71 -77	-95 -95 -95
213	00:12:01:B5:62:D0	EDUROAM	2432 5	29 31 34	70 70 70	-61 -63 -66	-95 -95 -95
213	00:12:01:B5:69:71	ULPGC	2422 3	2 2 2	70 70 70	-93 -93 -93	-95 -95 -95
213	00:12:01:B5:69:70	EDUROAM	2422 3	4 4 5	70 70 70	-90 -90 -91	-95 -95 -95
223	00:12:01:B5:5B:81	ULPGC	2412 1	22 27 29	70 70 70	-66 -67 -73	-95 -95 -95
223	00:12:01:B5:62:D1	ULPGC	2432 5	18 20 23	70 70 70	-72 -74 -77	-95 -95 -95
223	00:12:01:B5:5B:80	EDUROAM	2412 1	23 27 30	70 70 70	-65 -67 -72	-95 -95 -95
223	00:12:01:B5:62:D0	EDUROAM	2432 5	19 20 23	70 70 70	-72 -74 -76	-95 -95 -95
.....							

Figura 123. Fragmento de la BD creada (incluye RSSI y Señal)

Las diferentes columnas de la BD representan:

- *Zona* de ubicación (pasillo, despacho, escalera...).
- Dirección MAC de cada AP detectado.
- SSID de cada AP.

- Frecuencia de trabajo y canal de cada AP.
- RSS:
  - Valor más bajo de RSSI obtenido.
  - Valor medio de RSSI calculado.
  - Valor más alto de RSSI obtenido.
- Los tres siguientes representan: valor más bajo, medio y más alto de RSSI (referencia).
- Señal: los tres valores siguientes representan: valor más bajo, medio y más alto de nivel de señal obtenido (*Signal*).
- Ruido: los tres últimos representan el valor más bajo, medio y más alto de nivel de ruido obtenido (*Noise*).

En la BD hemos denominado a cada zona de ubicación con las palabras inicioct, 211, 213, 223... Según sea cada caso, los AP detectados pueden diferir, como sucede al principio del pasillo (inicioct) y al final del mismo (extremos del edificio) que son señales procedentes de AP de otras plantas o del exterior. Además, estos no son visibles o registran valores no representativos en la parte central e interior de los despachos por la poca penetración de su señal, y no han podido ser utilizadas para mejorar la precisión.

Estudiando los datos para los despachos 213 y 223 y reflejados en la Figura 124 observamos varios aspectos a destacar:

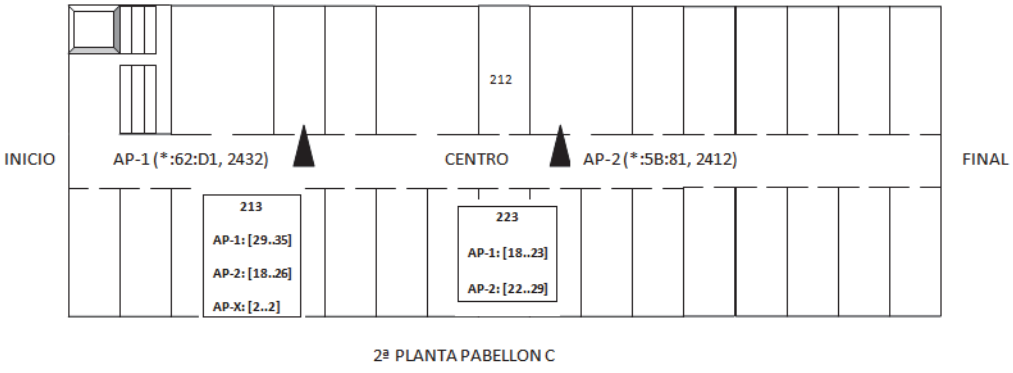


Figura 124. AP detectados y niveles de RSSI en los despachos 213 y 223

1º) La variabilidad de valores de RSSI a pesar de la cercanía de los AP a las ubicaciones seleccionadas. Por ejemplo, en el interior del despacho 223, y solamente a unos 4 m del AP-2 (*00:12:01:B5:5B:81, SSID: ULPGC, FREQ:*

2412), los márgenes de RSSI variaron desde 22 a 29 para una captura de unas 200 medidas. Estas medidas fueron realizadas en varias sesiones durante diferentes días y separadas en el tiempo.

2º) En algunos casos, estos márgenes para la ubicación 223 variaron a niveles de 16 a 18, medidos otro día diferente y para otra gran cantidad de muestras. Hecho similar ocurrió para el resto de ubicaciones (primera columna). Si bien esto plantea un serio problema para definir una BD patrón o referencia de medidas, podemos partir del caso más común, promediar medidas y evaluar los resultados.

3º) Los rangos RSSI más comunes para el AP-2 no son iguales para las ubicaciones 213 y 223. Esta información puede ser determinante para tener una mejor predicción de la posición.

4º) La cercanía de los AP entre sí, provoca que muchos valores sean iguales en dos ubicaciones distintas. Por ejemplo el rango de valores de RSSI entre 22 y 26 se encuentra entre los posibles para el AP-1 y el AP-2 en las ubicaciones 213 y 223. Por tanto, con un valor en este rango, a menos que se complemente con otras medidas, no es útil para discernir en cuál de las dos posiciones se encuentra el terminal.

5º) Se observa que, en ciertas ubicaciones, como por ejemplo la 213, se detecta un AP (*00:12:01:B4:69:71, SSID: ULPGC, FREQ: 2422*) no localizado en la segunda planta y que probablemente está ubicado en los exteriores u otras plantas del edificio (muy bajo RSSI y pocas veces detectado). Esta información podría ser relevante (si tuviese valores aceptables y mantenidos en el tiempo) para diferenciar si se está en la ubicación 223 o 213 ante otras situaciones coincidentes de los dos otros márgenes.

6º) Algunos AP cambian su frecuencia/canal de trabajo. Estos casos han sido eliminados de la BD, dado que esta aleatoriedad es un aspecto que genera distorsiones o interpretaciones errores de los datos de la BD.

Una vez inicializada la BD en el *LRW* y, ubicado a modo de prueba, en la zona 223, realizamos múltiples pruebas de esta funcionalidad. Para ello, simplemente utilizamos un ordenador portátil con el agente instalado y nos ubicamos en diferentes zonas (despachos y pasillos) y procedemos a solicitar el servicio implementado como parte de la aplicación desde dicho ordenador portátil atacando al *LRW*. El gestor procesa la petición y comprobamos que éste, solicita al agente que se realice el barrido

de espectro. Una vez finalizado el barrido, se envían los datos capturados (en un formato equivalente al de la base de datos) al gestor. Tras la búsqueda en la BD, devuelve el nombre de la ubicación más probable según la estimación realizada por el gestor, con la indicación numérica del grado de exactitud. Se puede configurar para que devuelva toda la lista de localización. En base a éste el usuario y el agente realizan las acciones oportunas según desee, tras su valoración acerca de los resultados obtenidos. El gestor haría lo propio una vez se active el traspaso u otras acciones contempladas en las anteriores propuestas.

Para la implementación de esta nueva funcionalidad fue necesario añadir en el gestor la función o código para el tratamiento de los nuevos mensajes así como el módulo (*lee_BD_scan.c,* (16KB)*)* que lee el mapa pregrabado en el servidor con los valores de nivel de señal (RSSI) por ubicaciones. En cuanto a los agentes fue necesario añadir un módulo o función para el procesado de mensajes y la función de rastreo de AP.

Tras diferentes pruebas de uso de esta nueva funcionalidad de la aplicación, detectamos que la gran mayoría de los resultados fueron muy aproximados. En varios casos la variabilidad de los niveles de señal o la reducida información disponible (solo 2 AP disponibles) impidieron obtener la localización con un mayor grado de exactitud. Esto sucedió por ejemplo, en el interior del despacho 223. En varios casos, el agente detectaba al AP-2 con valor 18 (no contemplado como posible en la BD para dicha zona, pues según la misma variarían entre 22 y 29), por lo que el gestor determinaba la ubicación 213 con grado exactitud 2. Una forma de eliminar estos problemas pensamos en repetir el proceso para descartar un falso resultado y no pudimos concluir que tras varios intentos el resultado fuera el correcto. Obviamente no podemos olvidar que con solo 2 AP la limitada y variable información disponible, y el no contar con una BD patrón garantizada, no permite mejorar la exactitud de los resultados.

Todos los anteriores resultados evidencian que se requiere una mejor distribución física de los AP (no en línea como en la zona de pruebas) y un mayor número de AP para mejorar la precisión y exactitud de la localización de los terminales. Esto puede implicar un mayor tiempo de proceso para mapear y comparar la mayor cantidad de datos que se pueden obtener. No podemos olvidar que, como se evidencio de forma empírica tras las múltiples medidas realizadas del RSSI presentadas en el apartado 3.1.5 y la literatura existente al respecto, ya partimos del gran hándicap que representa la

variabilidad de los valores de RSSI durante la creación de la BD (aprendizaje) y en la posterior captura (localización), y por tanto es necesario complementar las medidas con otras.

Pruebas en exteriores

Para complementar los resultados previos en interior, se considera que puede ser importante hacer lo mismo en exteriores, al ser un medio y unas condiciones diferentes. Con ello, podemos analizar qué resultados presenta nuestra propuesta de aplicación de localización combinada con las anteriores propuestas cuando se cuenta con un mayor número de AP de referencia. Para ello, hemos utilizado el AP Asus RTAC66U (SSID: APTest24 MAC: E0:3F:49:0A:62:88) ubicado en la ventana del despacho 223 (con sus antenas dirigidas hacia el exterior) y el MiniAP de la marca *Tenda* (SSID: Tenda_F09538, MAC: C8:3A:35:F0:95:38) sujeto a una palmera en frente de la ubicación anterior. En la Figura 125 se muestra una imagen de la ubicación de cada uno de ellos. Estos dos AP nos van a servir como AP principales de referencia para nuestras pruebas.

Figura 125. Ubicación de AP para pruebas en exteriores

Para la creación de la BD de localización (fase de aprendizaje) nos vamos a ceñir a solo una parte de la calle entre ambos AP. Para simplificar la misma hemos definido un área de unos 320 m^2, rectángulo de unos 40 m de largo y 8 m de ancho. Además hemos usado una superficie en forma de cuadrícula para la toma de medidas. Los nodos de la

cuadrícula están separados 10 m en los lados mayores y unos 4 m en los lados menores. Esto lo hemos hecho así, ya que se ha comprobado que hacerlo para menores distancias (por ejemplo 1 m o similar) es ineficiente por ser inapreciables los cambios en los niveles de señal para esas distancias. En la Figura 126 se muestra de forma aproximada dicha cuadrícula sobre la calle. Hemos identificado cada nodo de la cuadrícula (círculo en la Figura 125) con las coordenadas relativas al origen (0,0 bajo APTest24), ubicados en la recta que une ambos AP (01), (04) y (08) y los extremos más alejados, a unos 40 m (posiciones (40,1), (40,4) y (40,8)). Tenemos que resaltar que el AP con SSID Tenda_F09538 se encuentra a 1,5 m del suelo (sobre la palmera) y APTest24 se encuentra a unos 8-9 m de altura (borde de ventana). Esta diferencia puede ser relevante para discernir posiciones por los diferentes niveles de señal recibidas de un AP o del otro.

El proceso consiste en ubicarnos en cada nodo de la cuadrícula y realizar 100 medidas mediante un rastreo (scanning) de los diferentes AP detectables y sus niveles de señal (dBm) o RSSI equivalente. La BD patrón de localización incluye por cada AP detectado y posición (zona) el número de medidas: los valores máximo, mínimo, promedio y desviación típica.

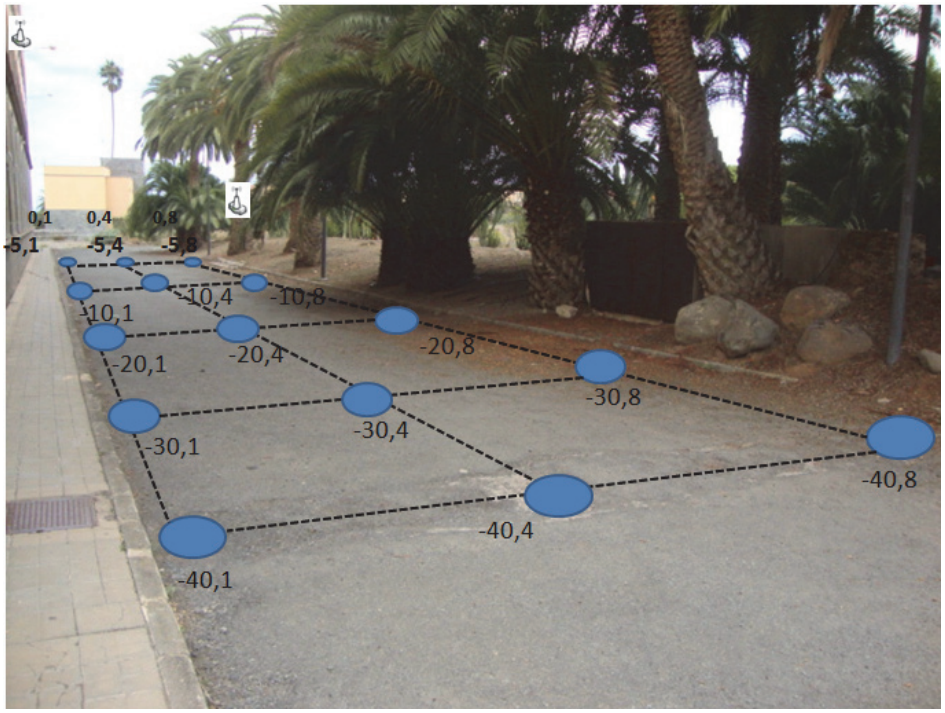


Figura 126. Cuadrícula para BD de localización en exteriores

En la Tabla 41 se muestra solo una parte de la BD de forma simplificada. Hemos definido zona, al contorno de cada posición (nodo). Si se analiza ligeramente dicha Tabla 40, podemos apreciar que en el caso de la zona 01, el AP-3 es detectado en 15 ocasiones con el mismo valor (-87 dBm) y los AP-2, AP-4, AP-5 y AP-6 que no superan las 32 medidas de las 100 posibles. Si de 100 posibles solo se detectan en un 30% es un dato representativo.

Tabla 41. Valores obtenidos en fase de aprendizaje zona cercana (01, 04, 08)

ZONA	AP	MAC	N. MEDIDAS	Min.	Media	Max.	Std.
01	1	00:0F:24:EC:FA:40	96	-88	-82	-79	2.3
	2	00:12:01:B5:49:A0	30	-87	-83	-82	1.6
	3	00:12:01:B5:61:F0	15	-87	-87	-87	0
	4	00:12:01:B5:62:90	33	-84	-82	-81	0.9
	5	00:12:01:B5:62:D0	23	-84	-82	-81	1.4
	6	00:12:01:B5:69:70	32	-92	-84	-82	3.8
	7	00:15:F9:6C:93:C0	96	-92	-84	-80	3.1
	8	00:1D:45:9E:9C:60	96	-84	-76	-66	3.8
	9	68:7F:74:AA:EA:7B	17	-84	-83	-82	1.02
	10	98:FC:11:76:A4:85	----------				
	11	C8:3A:35:F0:95:38	96	-70	-57	-52	3.47
	12	E0:3F:49:0A:62:88	96	-73	-67	-62	2.2
04	1	00:0F:24:EC:FA:40	100	-86	-70	-69	1.8
	2	00:12:01:B5:49:A0	84	-92	-85	-81	3
	3	00:12:01:B5:61:F0	----------				
	4	00:12:01:B5:62:90					
	5	00:12:01:B5:62:D0	24	-88	-86	-85	1.27
	6	00:12:01:B5:69:70	73	-92	-88	-87	1.5
	7	00:15:F9:6C:93:C0	90	-94	-86	-82	2.8
	8	00:1D:45:9E:9C:60	100	-84	-74	-66	4.2
	-	00:80:48:4E:AC:A2	----------				
	9	68:7F:74:AA:EA:7B	58	-92	-83	-79	2.7
	10	98:FC:11:76:A4:85	98	-92	-85	-80	2.8
	11	C8:3A:35:F0:95:38	100	-69	-58	-47	4.7
	12	E0:3F:49:0A:62:88	100	-67	-60	-56	1.7
08	1	00:0F:24:EC:FA:40	70	-86	-80	-78	1.42
	2	00:12:01:B5:49:A0	96	-90	-82	-77	2.4
	3	00:12:01:B5:61:F0	88	-91	-87	-84	1.9
	4	00:12:01:B5:62:90	----------				
	-	00:12:01:B5:5E:70	2	-87	-87	-87	0
	5	00:12:01:B5:62:D0	96	-94	-86	-80	3.22
	6	00:12:01:B5:69:70	96	-94	-85	-79	3.7
	7	00:15:F9:6C:93:C0	----------				
	8	00:1D:45:9E:9C:60	96	-82	-74	-65	3.6
	9	68:7F:74:AA:EA:7B	2	-85	-85	-85	0
	10	98:FC:11:76:A4:85	11	-88	-87	-84	1.6
	11	C8:3A:35:F0:95:38	96	-61	-54	-45	2.6
	12	E0:3F:49:0A:62:88	96	-70	-61	-57	2.2

El AP-9 presenta pocos valores en la posición 01, pero al compararlos con las otras posiciones (en zona 04 aparece con 58 valores y en zona 08 con solo 2), se observa que es una característica diferencial para este AP-9 en la zona 08. En la zona 08 solo el AP-5 presenta un elevado número de medidas de las 100 posibles frente a las otras zonas. Por último en la zona 08, el AP-9 y AP-10 presentan igualmente un reducido número de valores.

En la Tabla 42, se muestran los datos obtenidos para la zona de la cuadrícula (-301 y -308), más alejada de los dos AP principales de referencia. Destacamos una diferencia entre los valores promedio para AP-11 y AP-12, así como una menor desviación típica.

Tabla 42. Valores obtenidos en fase de aprendizaje zona alejada (-301,-308)

ZONA	AP	MAC	N. MEDIDAS	Min.	Media	Max.	Std.
-301	1	00:0F:24:EC:FA:40	96	-90	-78	-72	2.6
	2	00:12:01:B5:49:A0	75	-91	-84	-79	3
	3	00:12:01:B5:61:F0	46	-89	-87	-85	1.2
	4	00:12:01:B5:62:90	----------				
	-	00:12:01:B5:5E:70	36	-88	-86	-84	1.4
	5	00:12:01:B5:62:D0	96	-94	-88	-81	3.1
	6	00:12:01:B5:69:70	89	-95	-86	-80	3.3
	7	00:15:F9:6C:93:C0	----------				
	8	00:1D:45:9E:9C:60	96	-92	-83	-79	3
	9	68:7F:74:AA:EA:7B	26	-87	-85	-84	0.9
	10	98:FC:11:76:A4:85	96	-91	-84	-81	2.3
	11	C8:3A:35:F0:95:38	96	-61	-54	-51	1,5
	12	E0:3F:49:0A:62:88	96	-83	-75	-71	2.3
-308	1	00:0F:24:EC:FA:40	100	-87	-72	-68	2.6
	2	00:12:01:B5:49:A0	100	-93	-83	-77	3.2
	3	00:12:01:B5:61:F0	100	-95	-86	-82	2.6
	4	00:12:01:B5:62:90	----------				
	-	00:12:01:B5:5E:70	98	-93	-86	-82	3.4
	5	00:12:01:B5:62:D0	100	-97	-86	-80	3.4
	6	00:12:01:B5:69:70	100	-95	-84	-77	4
	7	00:15:F9:6C:93:C0					
	8	00:1D:45:9E:9C:60	100	-84	-76	-71	3.0
	9	68:7F:74:AA:EA:7B	----------				
	10	98:FC:11:76:A4:85	100	-93	-84	-79	2.7
	11	C8:3A:35:F0:95:38	100	-79	-68	-62	2.9
	12	E0:3F:49:0A:62:88	100	-76	-66	-64	2

En la Figura 127 se muestran todas las medidas del AP-12 (APTest24) para las zonas 01, 04 y 08 (línea más cercana). Se observa que se obtienen peores niveles de señal del APTest24 al estar más cerca que al estar alejado. Esto no parece un resultado lógico, salvo que se relacione con que justamente debajo del AP no hay visión directa

con sus antenas y que el diagrama de radiación se ve afectado por ello o por su cercanía de la pared. Esto no sucede a 4 m y a 8 m (zona 04 y 08). El caso de la señal del AP-11 (Tenda_F09538) en las mismas posiciones anteriores se muestra en la Figura 128.

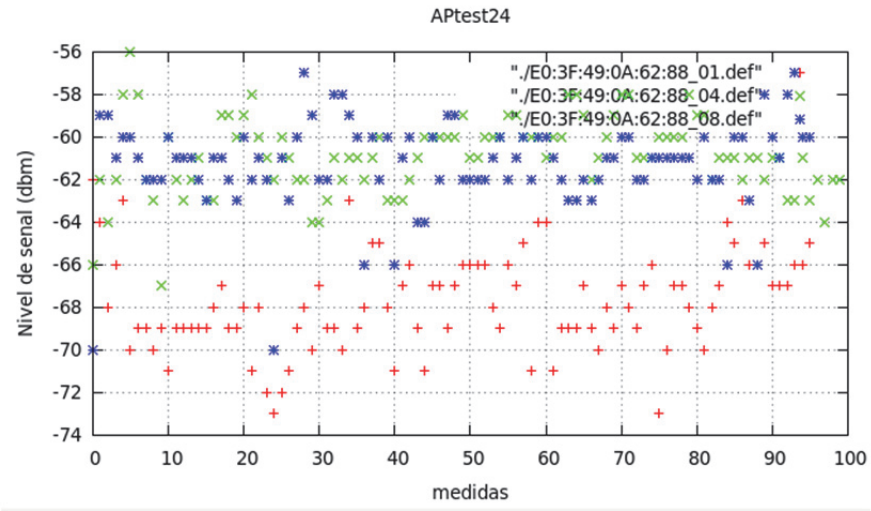


Figura 127. Niveles de señal de APTest24 en 1ª línea (posiciones 01, 04, 08)

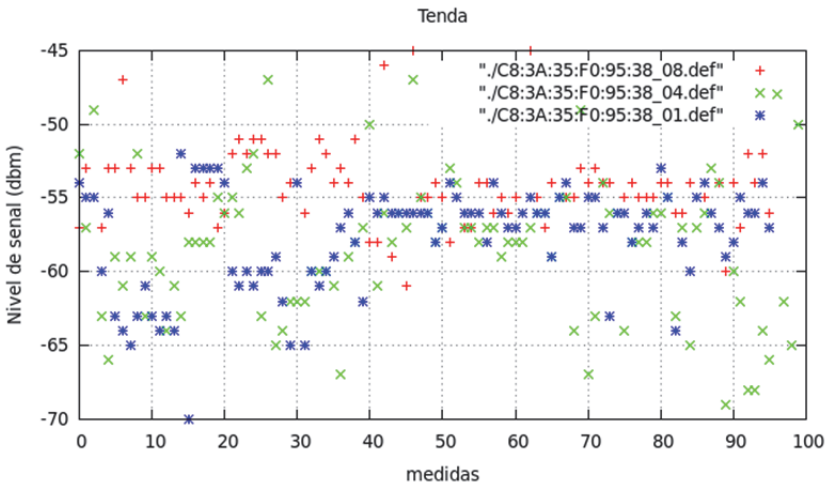


Figura 128. Niveles de señal de Tenda_F09538 en 1ª línea (posiciones 08, 04, 01)

En la Figura 127 observamos que discernir por el valor de nivel de señal recibido si el terminal se encuentra en el punto 01, 04 o 08 para este AP es prácticamente imposible, dado que cualquiera de los valores puede presentarse en cualquiera de los casos. Además destacamos la gran desviación típica para el zona 04 (>4).

Asimismo, en la Figura 129 se muestra la variación de los niveles de señal de AP-11 (Tenda_F09538) desde la posición más cercana (08) hasta la más alejada (-408). Este caso es bastante interesante por la agrupación de valores (menor desviación típica) y diferenciación bastante apreciable entre las diferentes posiciones (incrementos de 10

m), salvo los casos 08 y 208, que nuevamente presentan unos resultados inesperados. El razonamiento que sacamos es que la posición 08 esta justamente debajo del AP-11 con lo cual, sucede lo mismo que para el APTest24 en la posición 01.

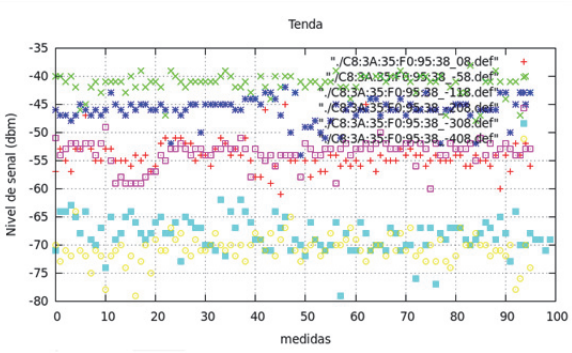


Figura 129. Niveles de señal de AP-11 en línea longitudinal (08,..,408)

Otros valores muy interesantes son los mostrados en la Figura 130 y 131. En la primera de ellas mostramos los valores medidos para los AP de referencia en la posición 301 y 308, respectivamente. Mientras en el primer caso parece que las diferencias son notables y representativas, en el segundo caso son poco útiles.

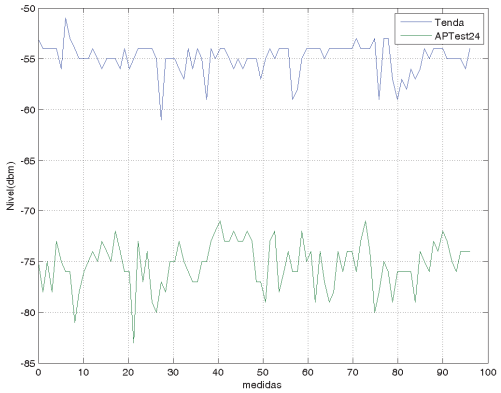


Figura 130. Niveles de señal de AP-11 y AP-12 en posición 301

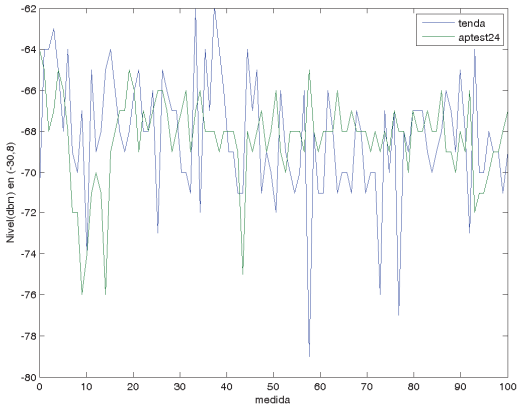


Figura 131. Niveles de señal de AP-11 y AP-12 en posición 308

Como sucede en interiores, una vez realizado el proceso de aprendizaje se detecta una elevada similitud de los niveles de señal para cada AP detectable para posiciones cercanas (del orden de decenas de metros). Esto representa un problema importante a la hora de la diferenciación durante el proceso o fase de búsqueda y comparación. En el caso de comparación directa de nivel de señal recibida, los resultados son poco precisos. En ciertas posiciones de la cuadrícula, solo es posible conseguir una estimación de localización con un grado aceptable de exactitud gracias a la existencia de señales de otros AP y no por diferencias apreciables en las medidas. Por el contrario, se detecta un elevado número de AP que están presentes en todas las zonas y, justamente, este aspecto va a ser determinante a la hora de realizar la localización como concluimos previamente en el caso de interiores.

Una vez realizada la captura tenemos que hacer las siguientes consideraciones:

- El número de medidas o valores detectados de cada AP es una variable importante para mejorar la precisión.
- En algunos puntos se detectan más de 15 AP, APTest24, Tenda_F09538, TELEMATICA_1, TELEMATICA_2 y otros tantos AP con SSID ULPGC y su correspondiente SSID virtual *eduroam* que físicamente se encuentran en otras plantas del pabellón C, zonas de tránsito entre edificios o en el edificio anexo (pabellón B). Esto puede ser positivo para una más eficiente estimación de posición si hay suficientes diferencias relativas entre los valores de cada uno de ellos, ya que si no fuese así, no se consigue una mayor precisión y solamente ralentiza el proceso durante la fase de localización.
- La variabilidad de nivel de señal no es apreciable en rangos inferiores a 20-30 m para muchos de los AP por su lejanía y tampoco son los suficientemente diferentes para AP cercanos en rangos de 4 u 8 m.
- Para que la BD de localización sea un patrón o referencia más viable, sería recomendable aplicar algún proceso de filtrado o calibración para eliminar aquellos valores que generen imprecisión por duplicidades de los mismos para dos ubicaciones distintas.

Tras las diferentes pruebas experimentales realizadas para esta zona de pruebas y con los datos contenidos en la BD de referencia, detectamos que la precisión en los

resultados, considerando solo promedio de niveles de señal es bastante baja en la mayoría de los casos. También la aparición de falsos positivos se producen por la cantidad de elementos repetidos en todos los puntos. Esto, como se comentó, está directamente relacionado con utilizar un patrón *raw* sin un procesado de los datos. Además la ineficiente ubicación de muchos de los AP detectados, cuya instalación no se realizó necesariamente para su uso en localización, limita algo más el proceso.

Considerando como referencia, no el promedio incluido en la BD (que es lo habitual para esta técnica (*fingerprint*)), sino los valores máximos, mínimos, e incluso aplicando el valor de nivel de señal que tiene más frecuencia de aparición para la búsqueda y comparación, nos da peores resultados frente a los anteriores.

Por tanto, como resumen podemos decir que es necesario recurrir a diferentes métricas y tratamiento de datos para mejorar los resultados, consistentes en:

- Considerar el número de AP detectados como un criterio complementario.
- Poner umbrales regulables de valores extremos (suavizado).
- Eliminar AP con reducido número de medidas (p. e. menos de 10 sobre 100).
- Descartar valores muy bajos que puedan introducir elementos distorsionadores. Recordemos que sensibilidades de -90 dBm, solo son considerados válidos para algunos AP operando a 1 Mbps, pero siempre mantenidos en el tiempo, y no para solo unos pocos beacons detectados.

Con la aplicación de esta propuesta de localización en la plataforma multifuncional se evidencia que la precisión de la misma es altamente dependiente de la zona escogida (patrón de referencia), la ubicación de los AP, y especialmente, del número de ellos, pues la alta variabilidad de la señal recibida y reducida variación para cortas distancias hace complejo conseguir precisiones elevadas.

Para el método que hemos implementado, de huella digital o mapa (*fingerprint*), la mayoría de estos aspectos son determinantes durante la fase de aprendizaje. Incluso, si bien la duración de la ejecución de las aplicaciones no es motivo de estudio en esta tesis doctoral, consideramos importante que, desde un punto de vista de procesado, el tiempo de respuesta durante la búsqueda es altamente dependiente del tamaño de la BD y cuanto depurado o calibrado estén los datos contenidos en la misma.

Además se constata que, en la fase de toma de medidas de campo por parte del agente, se deben realizar múltiples medidas. Al igual que sucede para interiores, tras

diferentes pruebas realizadas, detectamos que con solo una o dos medidas de rastreo (scanning), por parte de los terminales, en la mayor parte de los casos no es suficiente. Por tanto consideramos necesario hacerlo un mayor número de veces. Los resultados obtenidos se mejoran bastante cuando el terminal obtiene al menos 5 medidas, con ellas el agente las promedia y las envía al gestor para que realice el proceso de búsqueda en la BD y estime la posición.

Por último, como se constata en la literatura existente, la aplicación de localización en exteriores basada solo en WiFi presenta grandes dificultades, y lo más habitual es encontrarnos con soluciones híbridas GPS – WiFi para mejorar la estimación. Implementaciones propietaria como [197] garantizan unos 40 m de precisión, lo cual parece que es solo de aplicación para grandes zonas (calles, parkings,..), nunca para entornos muy cercanos.

Ante todo esto y como análisis final indicar que la localización sigue siendo una línea muy importante de investigación especialmente en interiores, dado que tiene una gran dependencia de factores, que no son muy tenidos en cuenta, como son la correcta planificación o despliegue de los AP. Ante este hándicap, parece cada vez más habitual hacer uso de *WiFi Tag* [198] o redes de sensores como complemento al uso de datos obtenidos de la propia red WiFi. En el caso de exteriores, diferentes propuestas y soluciones propietario han sido desarrolladas, como por ejemplo en [199]; orientadas muchas de ellas hacia la localización de hotspots.

La aplicación del conocimiento lo más exacto posible de la ubicación de los terminales complementa perfectamente a las otras funcionalidades. Ayuda en la estimación de la localización de un terminal en el ámbito de las coberturas de los AP utilizados. Con esta información se sugieren reubicaciones físicas y, asimismo, complementa perfectamente los traspasos con la información que aporta tras su utilización.

Capítulo 6. Conclusiones

En este capítulo exponemos una visión general de las conclusiones extraídas tras la realización de la presente tesis doctoral, destacando que los objetivos planteados han sido alcanzados de forma aceptable así como las propuestas o aportaciones surgidas del mismo. Además se exponen algunas líneas futuras de investigación que pueden ser continuación de los trabajos aquí realizados de forma directa o relacionada.

6.1 Conclusiones finales

Una vez alcanzado este punto de la presente tesis procede realizar una exposición de las conclusiones alcanzadas tras la realización de la misma. Antes de ello, creemos conveniente recordar que como se indica en la introducción, como usuarios de las redes WiFi nos solemos encontrar, quizás de forma más habitual de lo deseable, con ciertos acontecimientos que pueden ser inaceptables. En algún caso nos hemos encontrado con que se produce una desconexión de forma espontánea del terminal. En otras ocasiones, ubicados en un lugar con conectividad no se consigue asociar al mismo. También suele ser demasiado habitual encontrarnos reproduciendo un video on-line y se detiene repentinamente, y en muchos casos, es necesario reiniciar la sesión. En casi todos los casos, solo contamos con una información visual muy básica del sistema operativo del terminal utilizado, generalmente en forma de *vumeter digital o icono en modo diagrama de barras* y, por ello, nos suele generar un mayor desconcierto.

Por todo lo anterior, nos propusimos analizar estos hechos e investigar sus causas, y si fuera posible, proponer mejoras. Hemos evidenciado con la experimentación y contrastado con la gran cantidad de literatura existente, que las redes WiFi no garantizan un caudal mínimo para cada conexión, ni gestionan el mantenimiento eficiente de los enlaces, y en especial, no gestionan un reparto según los requisitos del servicio. Para mejorar esto se incorporan múltiples soluciones e incluso se desarrolla el estándar IEEE 802.11e, diseñado específicamente en la línea de priorizar unos flujos frente a otros. Como demuestran otros autores, cada servicio hace uso del canal lo más que pueda lo más pronto que pueda, sin conocer que otros servicios de otros terminales hacen uso del mismo canal. Técnicamente hablando, este efecto es intrínseco al modo de operación *best-effort*, que presenta grandes ventajas a la hora de implementar un método de acceso al medio eficaz, pero por otro lado, tiene estos otros inconvenientes. En este tipo de tecnologías, y en general en cualquier red de comunicaciones, el creciente aumento de usuarios y las exigencias cada vez mayores de los mismos, no pueden ser garantizados completamente. Es evidente que en otras tecnologías, la existencia de mecanismos de multiplexación si permiten hacer repartos más ajustados a necesidades, generalmente mínimo ancho de banda, máximo retraso aceptable, máximo jitter... A todo esto hay que unir la tendencia a crecer en el número de AP desplegados, denominadas ya como redes

WiFi densas, en las que los solapes de canales pueden ser cada vez mayores. También el creciente número de usuarios/terminales y la cada vez mayor demanda de servicios de alta calidad, podrían llevar a una reducción de la disponibilidad de los mismos. Por ello, es necesaria una eficiente planificación de canales y ubicación de los AP y, además, se combine con nuevas tecnologías (antenas inteligentes, radio cognitiva, diversidad espacial,…). Por tanto parece evidente, que bajo ciertas circunstancias, es necesario que en redes WiFi se apliquen mecanismos eficientes de planificación de canales y potencias de emisión, autoregulación y priorización de tráficos, reparto de recursos... En general, el estado de los AP y sus canales sean considerados de forma prioritaria a la hora de tomar decisiones, especialmente a la hora de asociarse a uno de ellos.

Tras esta reflexión o análisis final podemos concluir que es indispensable no solo aumentar la capacidad de las tecnologías sino añadir mecanismos de control a diferentes niveles y se considere, de manera especial, el estado de los canales y AP relacionados. Para ello consideramos que analizando los valores de aquellas variables o parámetros que pueden relacionarse con el funcionamiento de WiFi, se puede realizar una optimización paramétrica que consiga mejorar sus prestaciones. Estas prestaciones no son otras que mejorar la calidad de servicio ofrecida, visto desde una mejor percepción de las comunicaciones, mayor eficiencia y mayor mantenimiento de las mismas.

Por tanto, bajo nuestro punto de vista las propuestas realizadas en esta tesis, a la vista del estudio de las tecnologías implicadas y las evidencias empíricas obtenidas tras múltiples experimentaciones son bastante aceptables. La implementación real de las mismas en una plataforma de pruebas combinada y los resultados obtenidos podemos indicar que con su incorporación entre las funciones del AP y terminales conseguimos una mejora evidente frente al caso de no aplicarlas. Esto es especialmente importante cuando hacemos uso de servicios dependientes del tiempo, como son multimedia, dado que al ser servicios muy demandantes de ancho de banda pueden verse muy afectados cuando otros servicios/usuarios comparten el uso del canal.

Además algunas líneas de actuación propuestas por nosotros, coinciden con las planteadas por otros autores con resultados equivalentes aunque ninguno de ellos, lo hacen como lo hacemos nosotros, de forma conjunta. Este conjunto de iniciativas combinadas y complementarias entre sí, presentan la ventaja de conjugar diferentes cambios de comportamiento frente al modelo estándar. Este modelo de operación estándar de las redes WiFi podríamos decir que es bastante pasivo frente al que proponemos aquí. Bajo nuestro punto de vista, se propone una participación más activa

de los terminales y, especialmente de los AP convirtiéndolos en verdaderos gestores o controladores del uso que hacen dichos terminales de sus canales.

Haciendo un breve recordatorio, indicar que propusimos que los terminales deben regular la tasa de inserción de tráfico al canal RF según las indicaciones del AP para limitar sus efectos sobre otros tráficos. Complementariamente, si las condiciones de uso de un canal son limitadas, el AP puede requerir un cambio de AP/canal para liberar su carga; realizar un balanceo de carga mediante re-asociación de terminales, y por último, proponer a un terminal, desde el AP en combinación con dicho terminal, para la selección de otro AP que pueda ofrecer mejores resultados, o que de su cambio se libere la carga generada por dicho terminal.

Creemos importante resaltar una serie de hechos que durante la realización de esta tesis se han ido sucediendo en el tiempo y han constituido grandes avances en la evolución de los estándares WiFi:

- Antes de que se desarrollará el estándar *WiFi-Direct,* ya proponíamos que la conectividad en modo infraestructura resultaba ineficiente para conexiones entre terminales en el mismo canal. Ya planteábamos mantener conectividad directa como solución y solo la redirección hacia el AP se produjese para tráfico de salida. Obviamente la solución de nodos ocultos no estaba contemplada.
- Antes de que se desarrollará el estándar 802.11f, conocido como IAPP, que no ha tenido el éxito esperado y ha quedado como opcional, que especifica que los AP deben intercambiar información de estado de forma *multicast*, ya considerábamos que información de estado del canal intercambiada entre los AP podría ser bastante útil. De esta manera permitimos o habilitamos lo que denominamos "traspaso", pudiendo mejorar las prestaciones ofrecidas por los AP al hacer una elección más eficiente por parte de los terminales, como corroboran los artículos presentados.

Como reflexión final indicar que el auge de las redes WiFi y su creciente uso y demanda ha sido fomentado por la elevadísima cantidad de investigadores, gran cantidad de aportaciones en sus diferentes aspectos y literatura científica relacionada existente, que indudablemente ha llevado a una evolución exponencial de la misma y que permanecerá abierta indefinidamente.

6.2 Otras líneas de investigación abiertas

Dado que las posibilidades que se abren son enormes, consideramos que en la línea de seguir mejorando las prestaciones de las redes WiFi en particular, y quizás muchas de ellas se pueden generalizar para otras redes inalámbricas, como son redes de sensores, redes vehiculares... estamos realizando ya diferentes acciones. Concretamente una de ellas dentro del grupo de investigación, se relaciona con la estimación de valores de RSSI para una toma de decisión óptima, dado que de dicho valor pueden depender muchas acciones como la localización, *handover* horizontal o vertical, control de desconexión por límite de cobertura, control de movilidad, sincronización de datos offline u on-line,... Ya estamos realizando medidas experimentales y modelando el comportamiento para proponer variantes a las ya existentes de otros autores.

Otra línea ya iniciada consiste en considerar que los *beacons* emitidos por cada AP pueden ser utilizados como transporte de información de estado y de control del canal, reduciendo con ello el *overhead* creado por el tráfico de control requerido para las propuestas ya presentadas. Los primeros resultados analíticos y experimentales ya están siendo obtenidos y en proceso de presentación en congresos o publicación en revistas de prestigio.

Otra línea de trabajo transversal, se relaciona con el proceso de guiado y seguimiento de terminales para favorecer, que durante la movilidad de un terminal se habilite y garantice que no sufra pérdidas de conexión entre los diferentes AP.

Por último, consideramos muy importante, como ya lo hacen otros autores, es aunar esfuerzos en el tema tan importante en las redes inalámbricas que es el consumo energético. Este lo vemos desde dos vertientes: la parte de los terminales, dada su limitada duración e importancia para el peso y otros factores, como para los AP, donde su constante consumo requiere de iniciativas para reducir el mismo. En esta línea se requieren iniciativas orientadas hacia aumentar la durabilidad de la batería de los equipos, reducir el coste económico por el consumo eléctrico a usuarios y, de manera especial, aumentar el ahorro energético.

Bibliografía

[1] V. Bharghavan, «Performance Analysis of a Medium Access Protocol for Wireless Packet Networks,» *IEEE Performance and Dependability Symposium,* 1998.

[2] J. L. Sobrinho y A. S. Krishnakumar, «Quality-of-service in ad hoc carrier sense multiple access wireless networks,» *IEEE Journal on Selected Areas in Communications,* vol. doi:10.1109/49.779919, p. 1353–1368, 1999.

[3] R. M. D. Lang y D. T. Sharad Ramanthan, «Measuring Performance of ad-hoc Networks using Timescales for Information Flow,» *INFOCOM,* 2003.

[4] J. Jangeun, P. Pushkin y S. Mihail, «Theoretical Maximun Throughput of IEEE 802.11 and its Applications,» pp. 249-256, 2003.

[5] P. T. Hasler y O. Dousse, «Connectivity in ad-hoc and hybrid networks,» *Proc. INFOCOM,* 2002.

[6] L. Benyuan, L. Zhen y D. Towsley, «On the Capacity of Hybrid Wireless Networks,» *Infocom,* 2003.

[7] J. Maniyeri, «A Linux Based Software Router Supporting QoS, Policy Based Control and Mobility,» *IEEE Computer Society. ISCC'03,* 2003.

[8] M. H. Prihandoko y A. B. Habaebi, «Adaptive call admission control for QoS provisioning in multimedia wireless networks,» *Computer Communications,* vol. 26 , pp. 1560-1569, 2003.

[9] Y. Fang y Y. Zhang, «Call admission control schemes and performance analysis in wireless mobile networks,» *ISSN: 0018-9545,* vol. 51, p. 371–382, 2002.

[10] C. K. Toh, M. Delwar y D. Allen, «Evaluating the communication performance of an ad_hoc wireless network,» *IEEE Transactions on Wireless Communications,* vol. 1, nº doi:10.1109/TWC.2002.800539, p. 402–414, 2002.

[11] Y. Xiao, «IEEE 802.11e: QoS Provisioning at the MAC layer,» *IEEE Wireless communications,* 2004.

[12] P. Boggia, L. A. Camarda y S. M. Grieco, «Feedback-based bandwidth allocation with call admision control for providing delay guarantees in IEEE802.11e networks,» 2004.

[13] S. Vinnakote, S. Naresh y S. Pasupuleti, «New-MAC protocol for enhancement of QoS performance in wireless LAN,» *IFIP International Conference on Wireless and Optical Communications Networks. ISBN: 1-4244-0340-5,* 2006.

[14] N. Qiang, «Performance analysis and enhancements for IEEE 802.11e wireless networks. ISSN: 0890-8044,» *IEEE Communication,* vol. 19, nº 4, p. 21–27, 2005.

[15] L. Zhao, G. Yao y J. W. Mark, «Mobile positioning based on relaying capability of mobile stations in hybrid wireless networks,» *IEEE Proced. communications,* vol. 153, nº 5 , p. 762–770, 2006.

[16] D. Munoz, F. Bouchereau, C. Vargas y R. Enriquez, «Position techniques and Applications,» *Academic Press (Elsevier),* 2009.

[17] L. Meng, A. Zipf y S. Winter, «Map-based Mobile Services Design, Interaction and Usability,» *Lecture Notes in Geoinformation and Cartography (Springer Verlag),* 2008.

[18] H. A. Karimi, Handbook of research in Geoinformatics, IGIC GLobal, 2009.

[19] T. Akiyama, Y. Teranishi, S. Okamura y S. A. Shimojo, «Consideration of the precision improvement in WiFi positioning system.,» *International Conference on Complex, Intelligent, and Software Intensive Systems. IEEE Press,* pp. 1112-

1117, 2009.

[20] W. Ching, T. Jing, L. Rue y C. Rizos, «Uniwide Wifi based positioning system.,» *IEEE International Symposium on Technology and Society (IEEE Press),* pp. 180-189, 2010.

[21] L. Song, D. Kotz, R. Jain y H. Xiaoning, «Evaluating location predictors with extensive Wi-Fi mobility data,» *Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies - IEEE Press. INFOCOM.,* vol. 2, p. 1414–1424, 2004.

[22] J. Rodrigues, S. Fraiha, J. Araujo, H. Gomes, C. Frances y G. Cavalcante, «Empirical study of the QoS parameters behavior of a VoIP application in wi-fi networks,» *Microwave and Optoelectronics Conference (IMOC). SBMO/IEEE MTT-S Int.,* vol. 3, nº ISSN: 1679-4389, pp. 257-261, 2009.

[23] C. Liu, T. Wang y R. Chang, «Cross-layer handoff via predictive multiples pre-registrations for QoS of mobile multimedia applications,» *IEEE International Conference on Wireless Communications, Networking, and Information Security. IEEE Press,* 2010.

[24] H. Y. Starsky, H. Y. Wong, S. Lu y V. Bharghavan, «Robust rate adaptation for 802.11 wireless networks,» *ACM 12th Annual International Conference on Mobile Computing and Networking. Los Angeles, CA: ACM Press,* 2006.

[25] Y. Shoham y K. Leyton-Brown, «Multiagent systems algorithmic, game-theoretic, and logical foundations,» *Cambridge, England: Cambridge University Press,* 2009.

[26] V. H. Silva, E. I. Salgado y F. R. Quintana, «AWISPA: An awareness framework for collaborative spontaneous networks,» *In ASEE/ IEEE Frontiers in Education Conference. IEEE Press.,* pp. 1-6, 2006.

[27] M. A. Zarki y M. E. Visser, «Voice and data transmission over an 802.11 wireless network,» *In Proceedings of PIMRC-95, Toronto, Canada,* pp. 648-652, 1995.

[28] J. L. Krishnakumar y A. S. Sobrinho, «Real-time traffic over the IEEE 802.11 medium access control layer,» *Bell Labs Technical Journal,* pp. 172-187, 1996.

[29] D. Chang y R. J. Deng, «A priority scheme for IEEE 802.11 DCF access method,» *IEICE Transactions on Communications, VE82-B,* pp. 96-102, 1999.

[30] N. H. Vaidya, P. Bahl y S. Gupta, «Distributed fair scheduling in a wireless LAN,» *In Proceedings of ACM MOBICOM 2000, Boston, MA. IEEE TRANSACTIONS ON MOBILE COMPUTING, NOVEMBER/DECEMBER 2005,*

vol. 4, nº 6, 2000.

[31] A. Lindgren, A. Almquist y O. SchelŽen, «Quality of Service Schemes for IEEE 802.11 Wireless LANs An Evaluation,» *In Special Issue of the Journal on Special Topics in Mobile Networking and Applications (MONET),* vol. 8, pp. 223-235, 2003.

[32] L. Vollero y G. Iannello, «Frame Dropping a QoS mechanism for multimedia communications in WiFi hot spots,» *Proceedings of the 2004 International Conference on Parallel Processing Workshops (ICPPW- 04),* pp. 1530-2016, 2004.

[33] K. V. Rezende y J. F. De-Cardoso, «Increasing throughput in dense 802.11 networks by automatic rate adaptation improvement,» *Wireless Networks, Springer,* 2012.

[34] S. Nishimaki, H. Yamamoto y K. Yamazaki, «Wifi concierge at home network focusing on streaming traffic,» *IEICE Communications Express,* vol. 4, nº 2, pp. 67-72, 2015.

[35] R. Chandra, V. Bahl y P. Bahl, «MultiNet: Connecting to multiple IEEE 802.11 networks using a single wireless card,» *In Proceedings of INFOCOM,* 2004.

[36] S. Shakkottai, E. Altman y A. Kumar, «Multi- homing of users to access points in WLANs: A population game perspective,» *IEEE Journal on Selected Areas in Communications,* vol. 25, nº 6, p. 1207–1215, 2007.

[37] A. Cassell, T. Alperovich, M. Wellman y P. Noble, «Access point selection under emerging wireless technologies,» 2011.

[38] A. Kumar y V. Kumar, «Optimal Association of Stations and APs in an IEEE 802.11 WLAN,» *In Proceedings of the National Conference on Communications (NCC), IIT Kharagpur.,* 2005.

[39] D. Giustiniano, E. Goma y A. R. P. Lopez, «WiSwitcher: An efficient client for managing multiple APs,» *In Second ACM SIGCOMM Workshop on Programmable Routers for Extensible Services of Tomorrow,* p. 43–48, 2009..

[40] A. Croitoru, D. Niculescu y C. Raiciu, «Towards Wifi Mobility without Fast Handover,» *University Politehnica of Bucharest,* 2015.

[41] A. J. Nicholson, Y. Chawathe, M. Chen, B. Noble y D. Wetherall, «Improved access point selection,» *in Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, MobiSys 06. ACM,* pp. 233-245, 2006.

[42] S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose y D. Towsley, «Facilitating access point selection in IEEE 802.11 wireless networks,» *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurements. USENIX Association.,* pp. 26-26, 2005.

[43] O. Karimi, J. Liu y J. Rexford, «Optimal collaborative access point association in wireless networks,» *Proc. IEEE INFOCOM,* 2014.

[44] A. Miu, H. Balakrishnan y C. Koksal, «Improving loss resilience with multi-radio diversity in wireless networks,» *Proceedings of the 11th annual international conference on Mobile computing and networking. ACM, Mobicom,* p. 16–30, 2005.

[45] I. Savage y S. Ramani, «SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks,» *Proceedings of INFOCOM.,* 2005.

[46] Y. Bejerano, S. Han y L. Li, «Fairness and load balancing in wireless LANs using association control,» *Proceedings of ACM Mobicom,* 2004.

[47] S. Shah, K. Chen y K. Nahrstedt, «Available bandwidth estimation in IEEE 802.11-based wireless networks,» *Proceedings of 1st ISMA/CAIDA Workshop on Bandwidth Estimation. (BEst),* 2003.

[48] A. Baid, M. Schapira, I. Seskar, J. Rexford y D. Raychaudhuri, «Network cooperation for client-AP association optimization,» *IEEE In International Workshop on Resource Allocation and Cooperation in Wireless Networks,* 2012.

[49] P. B. Padmanabhan y N. Venkata, «RADAR: An In-Building RF-based User Location and Tracking System,» *Infocom IEEE,* nº ISSN 0743-166X, 2000.

[50] Y. Huang, J. Zheng, Y. Xiao y M. Peng, «Robust Localization Algorithm Based on the RSSI Ranging Scope,» *Hindawi Publishing Corporation. International Journal of Distributed Sensor Networks.,* vol. 2015, p. 8 , 2015.

[51] P. Hetal, N. Mistry y H. Mistry, «RSSI based Localization Scheme in Wireless Sensor Networks: A Survey,» *2015 Fifth International Conference on Advanced Computing & Communication Technologies,* nº 2327-0659/15, 2015.

[52] T. I. Chowdhury, M. M. Rahman, S.-A. Parvez, A. Alam, A. Basher, A. Alam y S. Rizwan, «A Multi-step Approach for RSSI-Based Distance Estimation Using Smartphones,» *IEEE,* nº 978-1-4799-8126-7/15, 2015.

[53] B. Mukhopadhyay, S. Sarangi y S. Kar, «Performance Evaluation of Localization Techniques in Wireless Sensor Networks Using RSSI and LQI,» *IEEE,* nº 978-1-4799-6619-6/15, 2015.

[54] R. Jin, Z. Che, H. Xu, Z. Wang y L. Wang, «An RSSI-based localization algorithm for outliers suppression in wireless sensor networks,» *Springer Science+Business Media New York,* nº DOI 10.1007/s11276-015-0936-x, 2015.

[55] S. Sen, J. Lee, K.-H. Kim y P. Congdon, «Avoiding Multipath to Revive Inbuilding WiFi Localization.,» *ACM. MobiSys'13,* nº 978-1-4503-1672-9/13/06, 2013.

[56] G. Lui, T. Gallagher, B. Li, A. G. Dempster y C. Rizos, «Differences in RSSI Readings Made by Different Wi-Fi Chipsets: A Limitation of WLAN Localization,» *IEEE,* nº 978-1-61284-4577-0188-7/11, 2011.

[57] «Real Academia de la Lengua,» [En línea]. Available: http://lema.rae.es/drae/?val=multimedia. [Último acceso: 19 Agosto 2015].

[58] ITU, «International Telecommunication Union,» [En línea]. Available: http://www.itu.int/en/about/Pages/default.aspx. [Último acceso: 10 Marzo 2015].

[59] N. G*, «International Telecommunication Union,» [En línea]. Available: http://www.itu.int/rec/T-REC-G/en. [Último acceso: 10 Marzo 2015].

[60] G.729, «International Telecommunications Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-G.729/es. [Último acceso: 10 Marzo 2015].

[61] ISO, «Coding of audio, picture, multimedia and hypermedia information,» JTC1/SC29, International Organization for Standardization/I. E. Commission, [En línea]. Available: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45316. [Último acceso: 10 Marzo 2015].

[62] ISO/IEC, «International Standards Organization,» [En línea]. Available: http://www.iso.org/iso/home.html. [Último acceso: 10 Marzo 2015].

[63] H2*, «International Telecommunications Union,» Normas ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-H/es. [Último acceso: 10 Marzo 2015].

[64] H.261, «International Telecommunication Union,» [En línea]. Available: http://www.itu.int/rec/T-REC-H.261-199303-I/es. [Último acceso: 20 Febrero 2015].

[65] H.263, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-H.263/en. [Último acceso: 20 Febrero 2015].

[66] H.264, «International Telecommunication Union,» ITU-T, [En línea]. Available:

http://www.itu.int/rec/T-REC-H.264. [Último acceso: 20 Febrero 2015].

[67] H.265, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-H.265-201410-I/en. [Último acceso: 20 Febrero 2015].

[68] Codecs, «Intenational Standards Organization,» ISO, [En línea]. Available: http://www.iso.org/iso/iso_technical_committee?commid=45316. [Último acceso: 20 Febrero 2015].

[69] IETF, «Internet Protocol (RFC),» International Engineering Task Force, [En línea]. Available: https://www.ietf.org/rfc/rfc791.txt. [Último acceso: 25 Marzo 2015].

[70] L. Hanzo, F. C. Somerville y J. Woodard, Voice and Audio Compression for Wireless Communications. Second Edition, Wiley, 2007.

[71] L. Hanzo, P. Cherriman y J. Streitf, Video Compression and Communications. From Basics to H.261, H263, H264, MPEG4 for DVB and HSDPA-Style Adaptative Turbo-Transceivers. Second Edition., Wiley, 2007.

[72] W. Simpson, Video over IP. IPTV. Internet Video, H.264, P2P, Web TV and Streaming: A complete guide to understanding the technology. Second Edition, Focal Press Elsevier, 2008.

[73] A. Ganz, Z. Ganz y K. Wongthavarawat, Multimedia Wireless Networks. Technologies, Standards and Qos., Prentice Hall, 2004.

[74] 3GPP, «The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations,» [En línea]. Available: http://www.3gpp.org/. [Último acceso: 10 Marzo 2015].

[75] GSM/GPRS, «ETSI,» [En línea]. Available: http://www.etsi.org/search-results?q=GSM&typeOfSearch=articles.. [Último acceso: 10 Marzo 2015].

[76] UMTS, «ETSI,» [En línea]. Available: http://www.etsi.org/technologies-clusters/technologies/mobile/umts. [Último acceso: 10 Marzo 2015].

[77] 4G-LTE, «ETSI,» [En línea]. Available: http://www.etsi.org/search-results?q=LTE&typeOfSearch=articles.. [Último acceso: 10 Marzo 2015].

[78] Wimax, «Wimax Forum,» [En línea]. Available: http://www.wimaxforum.org/. [Último acceso: 10 Marzo 2015].

[79] 802.16, «Wimax (IEEE),» [En línea]. Available: http://www.ieee802.org/16/.

[Último acceso: 10 Marzo 2015].

[80] 802.16, «Institute of Electrical and Electronics Engineers,» IEEE 802.16, [En línea]. Available: http://standards.ieee.org/about/get/802/802.16.html. [Último acceso: 10 Marzo 2015].

[81] C. Smith, LMDS Local Multipoint Distribution Service, MacGrawHill, 2000.

[82] Wifi, «Alianza Wifi,» [En línea]. Available: http://www.wi-fi.org/. [Último acceso: 10 Marzo 2015].

[83] 802.11, «Estándares WiFi,» [En línea]. Available: http://standards.ieee.org/about/get/802/802.11.html). [Último acceso: 10 Marzo 2015].

[84] «Estadísticas connexiones a Internet,» [En línea]. Available: http://www.internetlivestats.com/internet-users/. [Último acceso: 19 Marzo 2015].

[85] «Cisco. (2012). Cisco Visual Networking Index: Global mobil,» [En línea]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html. [Último acceso: 22 Marzo 2015].

[86] ChromeCast, «Google ChromeCast,» [En línea]. Available: https://www.google.es/chrome/devices/chromecast/. [Último acceso: 10 Marzo 2015].

[87] Bluetooth, «Estándar Bluetooth,» [En línea]. Available: http://www.bluetooth.com/Pages/How-It-Works.aspx.. [Último acceso: 10 Marzo 2015].

[88] 802.15.4, «Estandar IEEE 802.15.4 (2003),» [En línea]. Available: http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.. [Último acceso: 10 Marzo 2015].

[89] 802.15.4, «Estándar IEEE WSN (2006),» [En línea]. Available: http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf. [Último acceso: 10 Marzo 2015].

[90] W. Mardini, Y. Khamayseh, R. Jaradatand y R. Hijjawi, «Interference Problem between ZigBee and WiFi,» *IPCSIT IACSIT Press, Singapore,* vol. 30, 2012.

[91] D. T. Mangir, L. Sarakbi y H. Younan, «Analyzing the Impact of Wi-Fi Interference on ZigBee Networks Based on Real Time Experiments,» *International Journal of Distributed and Parallel Systems (IJDPS),* vol. 2, nº 4,

2011.

[92] C.-J. M. Liang, N. B. Priyantha, J. Liu y A. Terzis, «Surviving Wi-Fi Interference in Low Power ZigBee Networks,» *ACM,* nº 978-1-4503-0344-6, 2010.

[93] 802.11b, «IEEE 802.11,» Institute of Electrical and Electronics Engineers, [En línea]. Available: http://standards.ieee.org/about/get/802/802.11.html-. [Último acceso: 10 Marzo 2015].

[94] 802.11ac, «IEEE 802.11ac-2013 PDF,» Institute of Electrical and Electronics Engineers, [En línea]. Available: http://standards.ieee.org/about/get/802/802.11.html. [Último acceso: 10 Marzo 2015].

[95] 802.11s, «Amendment 10: Mesh Networking,» IEEE Standard for Information Technology-Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 2006. [En línea]. Available: www.ieee802.org/802_tutorials/06.../802.11s_Tutorial_r5.pdf.

[96] M. Ma, M. K. Denko y Y. Zhang, Wireless Quality of Service. Techniques, Standards and Applicatons, CRC Press, 2009.

[97] D. Gong, M. Zhao y Y. Yang, «Distributed channel assignment algorithms for 802.11n WLANs with heterogeneous clients,» *Elsevier,* 2014.

[98] K. Ratnam y I. Matta, «Effect of Local Retransmission at Wireless Access Points on the Round Trip Time Estimation of TCP,» *IEEE,* 1998.

[99] M. Heusse, F. Rousseau, G. Berger-Sabbatel y A. Duda, «Performance Anomaly of 802.11b,» *IEEE,* nº 0-7803-7753-2/03/, 2003.

[100] E. Velayos y H. Pelletta, «Performance measurements of the saturation throughput in IEEE 802.11 access points,» *IEEE,* nº 0-7695-2267-X, 2005.

[101] S. Kouhbor, J. Ugon, A. Rubinov, A. Kruger y M. Mammadov, «Coverage in WLAN with Minimum Number of Access Points,» *IEEE,* nº 0-7803-9392-9/, 2006.

[102] 802.11f, «802.11F-2003 - IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability Via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation,» [En línea]. Available: https://standards.ieee.org/findstds/standard/802.11F-2003.html. [Último acceso: 10 Marzo 2015].

[103] RAI, «Real Academia de Ingeniería,» [En línea]. Available: http://diccionario.raing.es/es/lemas?title=Calidad+de+Servicio&title_op=contains&tid=All. [Último acceso: 20 Febrero 2015].

[104] Wikipedia, «Calidad de Servicio,» [En línea]. Available: http://es.wikipedia.org/wiki/Calidad_de_servicio. [Último acceso: 19 Agosto 2015].

[105] Y. Bernet, Networking Quality of Service and Windows Operating Systems, New Rifers Publishing, 2001.

[106] G.114, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.114-200305-I!!PDF-E&type=items. [Último acceso: 19 Marzo 2015].

[107] P.800, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-P.800-199608-I/es. [Último acceso: 11 Marzo 2015].

[108] PEVQ, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-J.247/en. [Último acceso: 11 Marzo 2015].

[109] PEAQ, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/R-REC-BS.1387-1-200111-I/en. [Último acceso: 11 Marzo 2015].

[110] PESQ, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-P.862-200102-I/en. [Último acceso: 11 Marzo 2015].

[111] POLQA, «International Telecommunication Union,» ITU-T, [En línea]. Available: http://www.itu.int/rec/T-REC-P.863-201409-P/en. [Último acceso: 11 Marzo 2015].

[112] Minetur, «Gobierno de España,» [En línea]. Available: http://www.minetur.gob.es/telecomunicaciones/es ES/Servicios/CalidadServicio/Paginas/Calidad.aspx. [Último acceso: 11 Marzo 2015].

[113] «WiFi,» [En línea]. Available: http://www.wi-fi.org/. [Último acceso: 15 Marzo 2015].

[114] «Optimizing Enterprise Video Over Wireless LAN,» [En línea]. Available: http://www.cisco.com/c/en/us/products/collateral/wireless/5508-wireless-controller/white_paper_c11-577721.html. [Último acceso: 27 Marzo 2015].

[115] RSVP, «IETF,» RFC2205, [En línea]. Available: http://tools.ietf.org/html/rfc2205. [Último acceso: 14 Marzo 2015].

[116] Diffserv, «IETF,» [En línea]. Available: http://tools.ietf.org/html/rfc2474. [Último acceso: 14 Marzo 2015].

[117] IPTV, «Paper IPTV,» Internet Protocol TeleVision, [En línea]. Available: https://ritdml.rit.edu/bitstream/handle/1850/11668/FHuArticle2007.pdf?sequence=1. [Último acceso: 14 Marzo 2015].

[118] «IGMP - RFC3376,» [En línea]. Available: http://tools.ietf.org/html/rfc3376. [Último acceso: 14 Marzo 2015].

[119] L. codecs, «Codecs,» [En línea]. Available: http://www.codecguide.com/links.htm. [Último acceso: 14 Marzo 2015].

[120] «Network Simulator NS-2,» [En línea]. Available: http://www.isi.edu/nsnam/ns/. [Último acceso: 27 Marzo 2015].

[121] linssider, «Sourceforge,» Software scan, [En línea]. Available: http://sourceforge.net/projects/linssid/. [Último acceso: 30 Marzo 2015].

[122] U. Linux, «Wireless Tools for Linux,» Configuración WiFi, [En línea]. Available: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html. [Último acceso: 10 Abril 2015].

[123] iperf, «Herramientas medir prestaciones de red,» [En línea]. Available: https://iperf.fr/. [Último acceso: 30 Marzo 2015].

[124] D. Marrero, «seritel,» Documentación complementaria, 2015. [En línea]. Available: http://seritel.teleco.ulpgc.es/personal/tesis. [Último acceso: 6 Octubre 2015].

[125] Airview, «Spectrum Analyzer 2.4 GHz,» Ubiquity, [En línea]. Available: https://www.ubnt.com/. [Último acceso: 10 Noviembre 2014].

[126] VideoLAN, «VLC,» [En línea]. Available: http://www.videolan.org/vlc/. [Último acceso: 14 Marzo 2015].

[127] ASUS, «AP Router RTAC66U,» [En línea]. Available: http://www.asus.com/es/Networking/RTAC66U/. [Último acceso: 14 Marzo 2015].

[128] «Sniffer Tcpdump,» [En línea]. Available: http://www.tcpdump.org/. [Último acceso: 31 Marzo 2015].

[129] «Traffic Control. Functions tc.,» [En línea]. Available: http://tldp.org/HOWTO/Traffic-Control-HOWTO/intro.html. [Último acceso: 10 Abril 2015].

[130] D. Marrero, «Software para injección de tráfico broadcast configurable en C para unix/linux,» ULPGC, 2012.

[131] «Traffic Control. Modulo netem,» [En línea]. Available: http://www.linuxfoundation.org/collaborate/workgroups/networking/netem. [Último acceso: 10 Abril 2015].

[132] T. Instrument, «TI,» LQI, [En línea]. Available: https://e2e.ti.com/support/wireless_connectivity/w/design_notes/calculation-and-usage-of-lqi-and-rssi. [Último acceso: 1 Julio 2015].

[133] W. Fan, «Study of Smart Multi-antenna and Multi-channel for Smart Distribution Grid Based on Mesh Networks,» *iiicec-15, Advances in Computer Science Research,* nº ISSN: 2352-538x, 2015.

[134] Z. Ding, C. Zhong, D. Ng y M. Peng, «Application of smart antenna technologies in simultaneous wireless information and power transfer,» *Communications Magazine, IEEE. ISSN : 0163-6804,* vol. 53, pp. 86-93, 2015.

[135] P. Patel, V. Patel y M. Snehal, «Cognitive Radio Future of Wireless Communication,» *Scientific Essay,* p. 7, 2015.

[136] A. Saleem, A. Ghulan, D. Baksh y F. Qureshi, «CRANs (Cognitive Radio Ad Hoc Network) a Survey,» *Proc. of International Conference on Communication Information Technology and Robotics. N&N Global Technology,* nº DOI: 08.ICCITR.2015.1.15, 2015.

[137] K. Kumar, K. Annapurna y B. SeethaRamanjaneyul, «Supporting Real-Time Traffic in Cognitive Radio Networks,» *Dept of ECE, K L UNIVERSITY,* 2015.

[138] Linksys, «Cisco System,» [En línea]. Available: http://www.linksys.com/es/. [Último acceso: 7 Julio 2015].

[139] DD-WRT, «AP linux,» [En línea]. Available: http://www.dd-wrt.com/site/index. [Último acceso: 07 Julio 2015].

[140] Ubuntu, «Linux,» Versión 12.04 LTS, [En línea]. Available: http://cdimage.ubuntu.com/netboot/12.04/. [Último acceso: 7 Julio 2015].

[141] Tenda, «MiniAP,» [En línea]. Available: http://www.tenda.cn/uk/product/A6.html. [Último acceso: 1 Julio 2015].

[142] IETF, «MPTCP,» Desarrollo MPTCP, [En línea]. Available: http://datatracker.ietf.org/wg/mptcp/documents/. [Último acceso: 19 Junio 2015].

[143] IEEE, *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.,* ANSI/IEEE Standard 802.11.

[144] IEEE, *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY),* Specifications, Nov 1997. P802.11..

[145] IEEE, «Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Higher Speed Physical Layer Extension in the 2.4 GHz Band,„» 1999.

[146] «WiFi-Direct.,» [En línea]. Available: https://www.wi-fi.org/discover-wi-fi/wi-fi-direct. [Último acceso: 17 Febrero 2015].

[147] «MANET (Mobile Ad-Hoc Networks).,» [En línea]. Available: https://tools.ietf.org/html/rfc2501.. [Último acceso: 17 Febrero 2015].

[148] «IP-Tables / NAT (Network Address Translation),» [En línea]. Available: http://www.iptables.org, http://www.netfilter.org. [Último acceso: 17 Febrero 2015].

[149] R. Droms, «Dynamic Host Configuration Protocol,» [En línea]. Available: http://www.ietf.org/rfc/rfc2131.txt. [Último acceso: 17 Febrero 2015].

[150] DNS, «RFC1035, RFC1034,» Domain Name Server, [En línea]. Available: http://tools.ietf.org/html/rfc1035.. [Último acceso: 17 Febrero 2015].

[151] «RADIUS (Remote Authentication Dial In User Service),» [En línea]. Available: http://tools.ietf.org/html/rfc2865. [Último acceso: 17 Febreo 2015].

[152] IEEE, *IEEE 802.11a-1999 (8802-11:1999/Amd 1:2000(E)), IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control.*

[153] IEEE, *IEEE 802.11g-2003 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY.*

[154] D. Marrero, A. Suárez y E. Macías, «Dynamic Interconnection of Ad-hoc Nodes Based on the Type of Service to be Accessed,» de *International Conference on Wireless Networks (ICWN),*, Las Vegas (EEUU), 2005.

[155] DLINK, «WNIC. Technology Wifi Turbo,» [En línea]. Available: www.dlink.com. [Último acceso: Marzo 2015].

[156] I. 802.11n, *PIEEE 802.11N (D2) Draft STANDARD for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (P.*

[157] Apple, «AppleTV, Technical specification,» [En línea]. Available: https://www.apple.com/es/appletv/. [Último acceso: 3 Abril 2015].

[158] I. 802.11e, *IEEE 802.11e-2005, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PH.*

[159] calsoftlabs, «Qos extreme-to-extreme,» [En línea]. Available: http://www.calsoftlabs.com/downloads/w_qos-wireless-lan.pdf. [Último acceso: 4 Abril 2015].

[160] «Eduna. Controlador de red,» [En línea]. Available: http://www.e-duna.com/. [Último acceso: 21 Febrero 2015].

[161] «Programming with pcap,» [En línea]. Available: http://www.tcpdump.org/pcap.htm. [Último acceso: 21 Febrero 2015].

[162] «Netfilter/Iptables Project Homepage,» [En línea]. Available: http://www.netfilter.org/. [Último acceso: 21 Febrero 2015].

[163] «Linux Advanced Routing y Traffic Control,» [En línea]. Available: http://www.lartc.org, http://tcng.sourceforge.net/. [Último acceso: 21 Febrero 2015].

[164] Cisco, «Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide,» Cisco Press, 2013.

[165] IEEE, «IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—,» Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2012 (Rev. 2007).

[166] A. Suarez, J. A. Santana, E. Macías, V. Mena, J. Canino y D. Marrero, «RSSI Prediction in WiFi Considering Realistic Heterogeneous Restrictions,» *Network Protocols and Algorithms,* nº ISSN 1943-3581, 2014.

[167] J. Schiller, Mobile Communications, Addison Wesley, 2003.

[168] skyhook. [En línea]. Available: http://www.skyhookwireless.com/. [Último acceso: 4 Abril 2015].

[169] Ekahau, «RTLS,» [En línea]. Available: http://www.ekahau.com/real-time-location-system/technology. [Último acceso: 4 Abril 2015].

[170] Cisco, «Wireless Location,» [En línea]. Available: http://www.cisco.com/c/en/us/products/wireless/wireless-location-appliance/index.html. [Último acceso: 4 Abril 2015].

[171] M. Quintana, D. Sánchez, D. Marrero y J. Navarro, «Localización en WLAN utilizando distribuciones de probabilidad con reducción de cómputo por trilateralización,» de *Jitel2009*, Cartagena, 2009.

[172] IEEE, «802.11k RSSI,» Received Signal Strength Indication, [En línea]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4544755&tag=1. [Último acceso: 4 Abril 2015].

[173] A. R. Prieto Bernárdez y A. Suárez-Sarmiento, *Aplicación Gráfica para la localización de puntos de acceso en interiores de entornos poco cambiantes,* PFC EUITT-ULPGC, 2009.

[174] N. Kawaguchi, «WiFi Location Information System for Both Indoors and Outdoors,» *Springer Berlin / Heidelberg,* nº ISBN 978-3-642-02480-1.

[175] Compaq, WL110. PCMCIA Compaq, [En línea]. Available: www.compaq.com. [Último acceso: 12 Agosto 2015].

[176] RedHat, S.O. Linux. Distribution RedHat 9.0, [En línea]. Available: www.redhat.com. [Último acceso: 15 Agosto 2015].

[177] Slackware, «Linux,» Operating System, [En línea]. Available: www.slackware.com. [Último acceso: 15 Agosto 2015].

[178] Compaq, «WL310,» Adapter PCI-PCMCIA + NIC WL110 Compaq, [En línea]. Available: http://www.compaq.com.

[179] RealTek, NIC Ethernet Realtek 10/100 Mbps, [En línea]. Available: www.realtek.com. [Último acceso: 15 Agosto 2015].

[180] Dlink, «Network Devices,» DWL900+. Access Points Dlink. DWL900+, [En línea]. Available: www.dlink.com.

[181] Genius, HUB 8 port Genius, [En línea]. Available: www.geniusnet.com.tw. [Último acceso: 15 Agosto 2015].

[182] Die, «ICMP,» ping, [En línea]. Available: http://linux.die.net/man/8/ping. [Último acceso: 18 Mayo 2015].

[183] ICMP, «IETF,» [En línea]. Available: http://tools.ietf.org/html/rfc792. [Último acceso: 18 Mayo 2015].

[184] Netperf, «Network Performance Benchmarch,» Hewlett Packard. Information Networks Division, February 1995. [En línea]. Available: http://www.netperf.org/netperf/. [Último acceso: 18 Mayo 2015].

[185] FTP, «IETF,» File Transfer Protocol, [En línea]. Available: http://tools.ietf.org/html/rfc959. [Último acceso: 18 Mayo 2015].

[186] IETF, «NAT,» Network Address Translation, [En línea]. Available: http://tools.ietf.org/html/rfc3022. [Último acceso: 18 Mayo 2015].

[187] IETF, «RFC2131,» Dynamic Host Configuration Protocol, [En línea]. Available: http://tools.ietf.org/html/rfc2131. [Último acceso: 18 Mayo 2015].

[188] DNS, «IETF,» Domain Name Service, [En línea]. Available: http://tools.ietf.org/html/rfc1035, http://tools.ietf.org/html/rfc1034. [Último acceso: 18 Mayo 2015].

[189] hostapd, «Kernel Linux,» [En línea]. Available: https://wireless.wiki.kernel.org/en/users/documentation/hostapd#wireless_interface. [Último acceso: 08 Junio 2015].

[190] J. Tourrilhes, «Hewlett Packard,» [En línea]. Available: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html. [Último acceso: 8 Junio 2015].

[191] hostpad. [En línea]. Available: http://w1.fi/hostapd/. [Último acceso: 08 Junio 2015].

[192] Handover, «Handover-Interoperatibility,» 802.21, [En línea]. Available: http://www.ieee802.org/21/. [Último acceso: 20 Agosto 2015].

[193] IETF, «RFC3244,» MobileIP, [En línea]. Available: http://tools.ietf.org/html/rfc3344. [Último acceso: 08 Junio 2015].

[194] Ubuntu, «Linux,» Versión 8.10, [En línea]. Available: www.ubuntu.com. [Último acceso: 18 Mayo 2015].

[195] Atheros, Chip set, [En línea]. Available: https://www.atheros.cz/. [Último acceso: 18 Mayo 2015].

[196] MadWifi, «Wireless NIC,» Madwifi (driver), [En línea]. Available: http://madwifi-project.org/. [Último acceso: 18 Mayo 2015].

[197] Combain, «Positioning Systems,» [En línea]. Available: https://combain.com/. [Último acceso: 1 Octubre 2015].

[198] Ekahau, «WiFi Tag,» [En línea]. Available: http://www.ekahau.com/real-time-location-system/technology/wi-fi-tags. [Último acceso: 1 Octubre 2015].

[199] Google, «Indoors-Outdoors Patents,» [En línea]. Available: http://www.seobythesea.com/2012/04/google-acquires-indooroutdoor-wireless-location-patents/. [Último acceso: 1 Octubre 2015].

ANEXO

En este apartado se relaciona la documentación complementaria de la tesis doctoral, concretamente los archivos media obtenidos como evidencias y descritos en el documento, así como la sección de análisis de capacidad de diferentes AP disponibles, indicados en el capítulo 3, que no se incluyen en el documento para hacerlo más manejable.

Documentación Complementaria

Los archivos que a continuación se relacionan están accesibles en el sitio web [124] y se ubican en las carpetas:

/media

Nombre	Tamaño	Descripción
Countdown_with_Sound_mpHD.mpg	4 MB	Video original de pruebas
prop_Countdown_with_Sound_mpHD.html	53 KB	Características de archivo de video Countdown_with_Sound_mpHD
captura_loss1pc.mp4	21 MB	Video con efecto 1% de pérdidas
captura_loss2pc.mp4	21 MB	Video con efecto 2% de pérdidas
captura_loss4pc.mp4	26 MB	Video con efecto 4% de pérdidas
captura_loss10pc.mp4	28 MB	Video con efecto 10% de pérdidas
captura_1M.mp4	24 MB	Video con efecto de canal limitado a 1 Mbps
captura_3M.mp4	28 MB	Video con efecto de canal limitado a 3 Mbps
captura_5M.mp4	22 MB	Video con efecto de canal limitado a 5 Mbps
captura_10M.mp4	25 MB	Video con efecto de canal limitado a 10 Mbps
captura_delay_2s.mp4	31 MB	Video con efecto de retraso de 2 s
captura_delay_4s.mp4	37 MB	Video con efecto de retraso de 4 s
simulacion_wifi_ns2.mp4	125 MB	Video con simulación en NS-2
Counter_down_2_ch3_inj_1u.mp4	26 MB	Efectos de congestión al inyectar tráfico en canal con transmisión de video activa.
Counter_down_10_ch3_inj_5-10.mp4	23 MB	
Counter_down_10_ch3_inj_100ms_nro8.mp4	22 MB	
Counter_down_10_ch3_inj_10ms_nro6.mp4	22 MB	

/anexo

medidas_velocidades_ap1-2-3.pdf	Medidas de velocidad obtenidas en cada canal para los otros 3 AP comerciales de diferentes fabricantes.