TREBALL DE FI DE CARRERA

TÍTOL DEL TFC: Detecció d'atacs DoS amb inhibidors de freqüències sobre xarxes IEEE 802.11

TITULACIÓ: Enginyeria Tècnica de Telecomunicació, especialitat en Sistemes de Telecomunicació

AUTOR: Moisés Gómez Díaz

DIRECTOR: Eduard García Villegas

DATA: 11 de Maig de 2009

Títol: Detecció d'atacs DoS amb inhibidors de freqüències sobre xarxes IEEE 802.11

Autor: Moisés Gómez Díaz

Director: Eduard García Villegas

Data: 11 de Maig de 2009

Resum

Les xarxes sense fils són sensibles a atacs DoS (*Denial of Service*) mitjançant inhibidors de freqüència, o dit d'una altra manera, basats en les tècniques de *jamming*. Aquest atac consisteix en la transmissió per part d'un atacant d'un senyal de gran potència en la mateixa banda freqüencial utilitzada per la víctima (en aquest cas, un canal de la banda ISM de 2,4 o 5 GHz). El senyal atacant interfereix en la comunicació, degradant la SINR. Aquest efecte pot donar-se accidentalment entre diferents dispositius que operen en la mateixa banda de freqüència, com els microones, altres xarxes Wi-Fi, aparells *bluetooth* o telèfons sense fils.

En les xarxes IEEE 802.11 l'accés al medi es basa en CSMA/CA, és a dir, abans de transmetre, una estació comprova si el medi està lliure. A causa de la naturalesa de CSMA/CA, les tècniques de *jamming* poden impedir totalment la comunicació en xarxes IEEE 802.11, ja que el medi sempre serà considerat com a ocupat per les estacions atacades si la potència detectada supera un determinat llindar.

Les defenses contra aquests atacs consisteixen en migrar les comunicacions a un canal no interferit pel *jammer*. No obstant, si el *jammer* emet en una banda molt ampla de freqüència, cap defensa és efectiva.

El treball d'aquest TFC inclou un estudi sobre els efectes de la presència d'un *jammer*. Els resultats d'aquest estudi serviran per decidir els criteris en base als quals es decideix la detecció d'un atac. Finalment, es desenvoluparà un petit programa en un entorn Linux que, mitjançant la monitorització dels paràmetres adients, proporcioni una alarma quan detecti la presència d'un atac amb inhibidors de freqüència.

Title: Detection of DoS attacks with jammers on IEEE 802.11 networks

Author: Moisés Gómez Díaz

Director: Eduard Garcia Villegas

Date: May, 11st 2009

Overview

Wireless networks are highly sensitive to DoS (*Denial of Service*) attacks caused by *jammers*. These attacks consist in the transmission of a high-power signal over the same frequency spectrum used by the victim (in this case, a channel of the ISM band of 2,4 or 5 GHz). The attacking signal jams the communication, degrading the SINR. This effect can be caused accidentally by different devices operating in the same frequency band, such as microwave ovens, or other wireless networks, e.g. *bluetooth* devices, wireless telephones, etc.

In IEEE 802.11 networks, medium access control is based on CSMA/CA, which senses the medium for idle periods before transmitting. Because of the CSMA/CA nature, jamming techniques can block absolutely the communications in IEEE 802.11 wireless networks, because the wireless medium will be considered as busy by the attacked stations if the detected power exceeds a determined threshold.

These attacks can be avoided by moving all communications to a channel not interfered by the jammer. However, if the jammer emits in a wide band of frequencies, there is no way of avoiding that jamming.

This TFC includes a review of the effects of a wide-band jammer. The conclusions of this review will suggest the criteria that can be used to detect a jamming attack. According to those criteria, a simple yet effective algorithm is developed under a Linux environment in order to, through the monitoring of the proper parameters, set an alarm whenever it detects the presence of a jamming attack.

A Crist, perquè m'ha permès arribar on sóc i m'ha ajudat durant aquest any. Perquè "amb Déu és la sabiduria" (Job 12:13) i sense ell mai ho hauria pogut aconseguir.

Al meu marit Sergio, qui m'ha recolzat en tot moment en fer aquest TFC i m'ha perdonat no poder-li haver dedicat tot el temps necessari.

"Déu inspira activitats particulars a cadascú, d'acord amb la seva vocació" (Joan Calví, Institució de la Religió Cristiana, Llibre II, Cap. II, 17)

ÍNDEX

INTRODUCCIÓ

Les xarxes locals sense fils són producte de l'evolució de les xarxes convencionals Ethernet. El seu origen es remunta a l'any 1991, quan IBM va dissenyar-ne una a una fàbrica amb un enllaç infraroig.

Les *Wireless Local Area Network* (WLAN) tenen molts avantatges, però també tenen inconvenients respecte les xarxes locals cablejades.
Les primeres faciliten la mobilitat dels usuaris, cosa que minimitza el cost d'instal·lació i augmenta la flexibilitat en el seu ús. El seu principal inconvenient és la seva sensibilitat a les interferències, cosa que les fa poc robustes en cas que la qualitat del canal sigui baixa.

És precisament per aquest motiu pel qual aquest tipus de xarxes són tan vulnerables als inhibidors de freqüències o *jammers*. Aquests són aparells que emeten un senyal a la mateixa banda freqüencial que la seva víctima i poden arribar a causar la caiguda total de la xarxa.
El sistema d'accés al medi CSMA/CA, emprat per l'estàndard IEEE 802.11, impedeix que dos clients transmetin simultàniament al mateix canal. Per aquest motiu, si un *jammer* està encès cap client pot enviar dades mentre aquest segueixi emetent, cosa que provoca que el nombre de bits per segon transmesos baixi, i la connexió en ocasions caigui.

L'objecte d'aquest Treball de Final de Carrera ha estat la detecció d'atacs de denegació del servei (*Denial of Service*, DoS) amb origen a un *jammer* i amb un o més clients de víctimes.

A fi de realitzar aquesta detecció, en primer lloc, s'ha analitzat la influència de l'inhibidor de freqüències en l'enllaç ràdio que s'estableix a una xarxa local sense fils, tenint en compte l'existència de diferents escenaris i de variables que modifiquen significativament el grau d'influència del mateix: el protocol, la distància, la modulació emprada o la longitud de paquet, entre d'altres.

La magnitud de referència per conèixer la influència del *jammer* a la xarxa sense fils és la diferència entre el *throughput* quan hi ha *jammer* respecte del *throughput* quan no n'hi ha. La caiguda varia en funció de les variables anteriorment mencionades, cosa que ens ajuda a detectar quines són aquelles que s'han de tenir més en compte a l'hora de la detecció.

El *driver* hostap mostra diferents paràmetres des del punt de vista d'un AP, tals com els intents d'enviament total els paquets i els bits enviats i rebuts, els paquets rebuts amb errors o els paquets enviats a una modulació diferent de la modulació per defecte. Experimentalment s'ha comprovat que els intents d'enviament per paquet, que és la relació entre els intents d'enviament total i el nombre de paquets, és el paràmetre que millor reflecteix la presència d'un *jammer* atacant. Posteriorment, amb ajuda d'aquest paràmetre i d'altres, s'ha desenvolupat una aplicació que, mitjançant un algorisme, és capaç de detectar la presència d'un inhibidor de freqüències.

Aquesta aplicació, a més d'haver detectat el *jammer* en totes les ocasions en què s'ha testejat, és capaç de detectar-lo des d'una distància mínima de 50 metres sense cap obstacle intermig. Que la distància mínima de detecció en aquestes condicions sigui tan alta permet prendre precaucions per tal de no perdre informació important a transmetre, donat que un *jammer* a 50 metres no influeix pràcticament en el *throughput* de la xarxa.

L' estructura del Treball de Final de Carrera està formada per cinc capítols:

Al Capítol 1 s'expliquen les característiques tècniques del protocol IEEE 802.11 així com el seu ús de les capes física i d'enllaç del model OSI.

Al Capítol 2 es poden trobar les principals problemàtiques i amenaces a què estan subjectes aquestes xarxes, així com les solucions que actualment s'implementen per tal d'evitar-les.

Al Capítol 3 s'analitzen les mesures fetes a diversos escenaris a fi de conèixer quina és la influència del *jammer* al *throughput* d'un enllaç sense fils.

Al Capítol 4 s'estudia la variació dels valors dels paràmetres ràdio proporcionats pel *driver* hostap segons diferents situacions de l'inhibidor de freqüències.

Al Capítol 5 s'explica l'aplicació que, amb l'anàlisi de les dades dels capítols anteriors, detectarà la presència de *jammers* i es verifica l'acompliment dels seus objectius.

Per últim, l'annex està dividit en tres seccions:

Al primer annex trobem alguns detalls del funcionament del protocol IEEE 802.11.

Al segon es troben tots els resultats de totes les mesures realitzades, a partir de les quals s'ha pogut desenvolupar l'aplicació de detecció de *jammers*.

A l'últim annex es troba el codi en C del programa desenvolupat.

CAPÍTOL 1. IEEE 802.11

IEEE 802 especifica les característiques de la capa física i de la capa d'enllaç del model OSI (*Open System Interconnection*) relatives a les connexions a xarxes d'àrea local (*Local Area Networks*) i metropolitana (*Metropolitan Area Networks*). La capa física s'encarrega dels detalls de la transmissió i la recepció, mentre que la capa d'enllaç coordina l'accés al medi.

Les especificacions individuals de l'IEEE 802 s'identifiquen per un segon nombre. Dos exemples d'aquestes són la IEEE 802.2, que especifica la capa d'enllaç *Logical Link Control* (LLC) i pot ser emprada per qualsevol especificació IEEE 802; i IEEE 802.3, que fa referència a la especificació de CSMA/CD (*Carrier Sense Multiple Acces network with Collision Detection*), emprada per Ethernet.

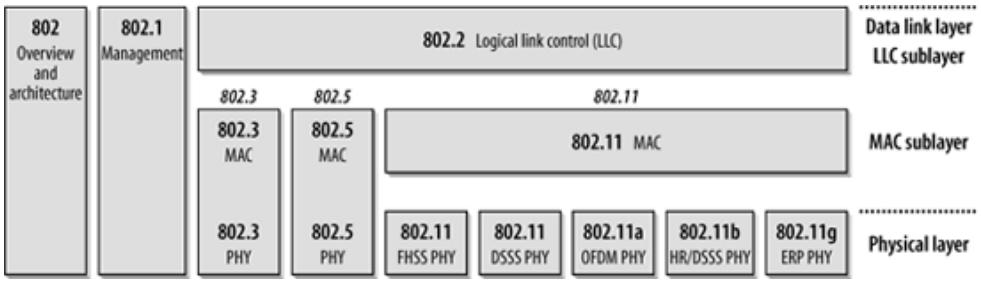


Figura 1.1. Relacions entre la família 802 i el model OSI

1.1. Estàndards IEEE 802.11

L'IEEE ha publicat diverses esmenes des del llançament del primer estàndard 802.11 l'any 1997.

IEEE 802.11 va veure la llum al 1997, amb unes taxes de transmissió d'1 i 2 megabits per segon (Mbps) a la banda de 2,4 GHz. També definia una capa física basada en infrarojos.

Al 1999 va ser alliberada una nova versió, 802.11b, proporcionant taxes d'1, 2, 5,5 i 11 Mbps. En funció de la taxa de transmissió variava la modulació a la capa física (DBPSK a 1, DQPSK a 2 Mbps i CCK amb DQPSK per 5,5 i 11 Mbps).

En aquest mateix any va ser publicat també el 802.11a, que proporcionava taxes de fins a 54 Mbps a la banda de 5 GHz. El fet que aquesta versió operés en una banda diferent de l'espectre radioelèctric va provocar problemes de compatibilitat amb les anteriors versions, quelcom que es va solucionar amb 802.11g, llançat al juny del 2003, el qual assolia les mateixes taxes que 802.11a i operava a les mateixes freqüències que 802.11 i 802.11b.

L’esmena 802.11d permet l’adaptació de l’estàndard als requisits tècnics de diversos països i regions. Així, permet variar les freqüències permeses, els nivells de potència i l’amplada de banda en funció de l’Estat en què s’empri l’especificació.

802.11e ofereix prioritització de dades, veu, transmissió de vídeo i *Quality Of Service* (QoS).

802.11h intenta resoldre les interferències de 802.11a, especialment amb radars, sistemes militars i aparells mèdics.

802.11i proveeix millores en l’encriptació, amb *Temporal Key Integrity Protocol* (TKIP) i *Advanced Encryption Standard* (AES).

802.11j permet l’ús de 802.11 al Japó, adaptant-se als requeriments legals, com al nombre de canals o la potència de sortida, entre d’altres.

802.11k facilita la realització de mesures de paràmetres ràdio en una xarxa sense fils. Aquestes mesures poden fer-se localment o bé sol·licitar-les a altres estacions. Les capes superiors podran accedir a elles a fi de gestionar els recursos de ràdio.

Finalment, l’esmena 802.11n permet velocitats de fins 600 Mbps, fiabilitat a les comunicacions i l’augment de la distància permesa entre les estacions i el punt d’accés (AP).

1.1.1. Topologies

802.11 permet dos tipus de topologies: el mode infraestructura (també anomenat *Infraestructure Basic Service Set*) i el mode *ad hoc* (o *Independent Basic Service Set*). Un BSS (*Basic Service Set*) és un conjunt d’estacions organitzades segons una de les dues topologies anteriors.

El mode infraestructura consisteix en diversos dispositius mòbils coordinats per un punt d'accés (*Access Point*). A través del punt d'accés passen totes les comunicacions, tant aquelles que es realitzen entre les estacions com entre les estacions i la resta de la xarxa cablejada.

A les xarxes amb aquesta topologia totes les estacions mòbils han d'estar en l'àmbit d'abast del punt d'accés, però no hi ha cap restricció de distància entre elles sempre i quan estiguin a l'àmbit de cobertura de l'AP.

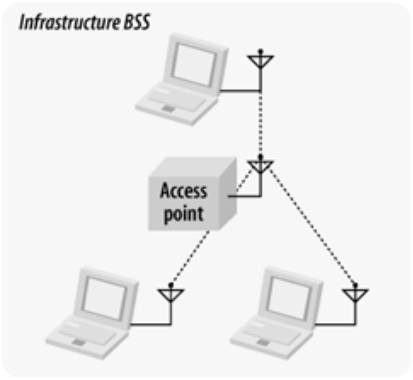


Figura 1.2. Xarxa amb topologia d'infraestructura.

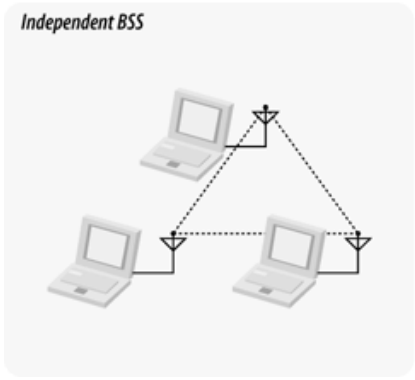


Figura 1.3. Xarxa amb topologia *ad hoc*.

D'altra banda, el mode *ad hoc* el formen aquelles xarxes de dispositius mòbils que no disposen de punts d'accés, sinó que es connecten entre ells mateixos mitjançant les seves pròpies targetes de xarxa.

Normalment aquest tipus de xarxes tenen un propòsit eventual i específic, com la connexió momentània entre diferents ordinadors. Per aquesta raó se'ls ha donat aquest nom, que significa literalment "per això".

Degut a que les BSS donen cobertura a zones de dimensions reduïdes, es pot configurar la xarxa mitjançant la unió de diversos BSS per tenir un abast major. Això es pot fer amb una configuració anomenada d'àrea estesa o *Extended Service Area*, que consisteix en la unió de diferents AP, que donen servei a àrees reduïdes, mitjançant una xarxa troncal (*backbone network*), anomenada sistema de distribució (DS). En aquest cas, totes les comunicacions entre estacions pertanyents a diferents BSS passarien sempre pel DS, mitjançant els AP corresponents a l'origen i a la destinació.

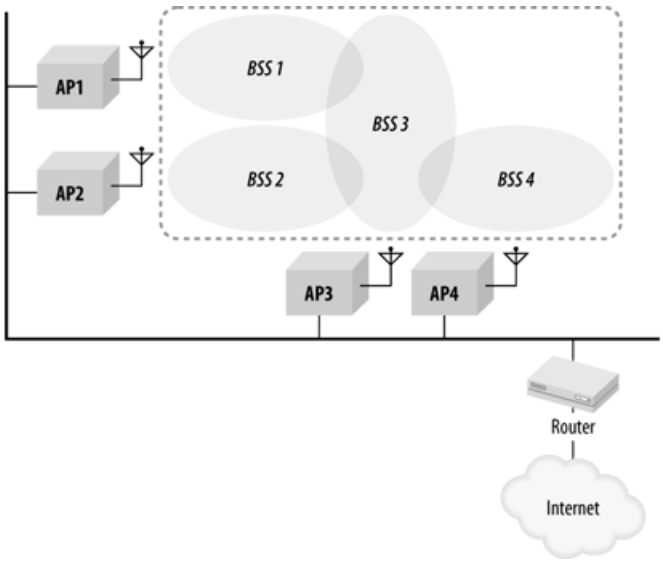


Figura 1.4. Xarxa d'àrea estesa.

1.1.2. Bandes ISM

802.11 opera a les bandes ISM (*Industrial, Scientific and Medical*), les quals estan regulades de diverses maneres en funció de la legislació de cada país.

L'ample de banda, una vegada eixamplat l'espectre, és de 20 MHz, amb una separació entre portadores de 5 MHz. Això fa que es necessitin almenys 5 canals de separació per garantir que dues transmissions simultànies no interfereixin entre elles. Això fa que per al 802.11b i 802.11g, que opera a 2,4 GHz, hi hagin només 3 canals de 13 que no se solapen (11 a USA), com es mostra a la Figura 1.5. A 802.11a, que treballa a 5 GHz, hi ha 19 canals disponibles (12 als EUA) que no se solapen.

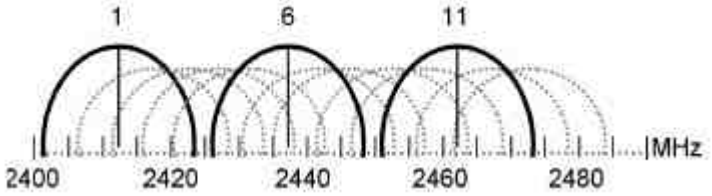


Figura 1.5. Canals a la banda ISM de 2,4 GHz

A Espanya aquesta banda està regulada pel Ministeri d'Indústria a través del *Cuadro Nacional de Atribución de Frecuencias* (CNAF).

La UN 85 [1] del CNAF, que s'encarrega de la banda freqüencial de 2,4-2,4835 GHz, estableix que aquest marge freqüencial només pot ser emprat en entorns de curt abast tant d'interior com d'exterior i amb una PIRE màxima de 20 dBm.
La UN 128 [1] s'encarrega de regular la banda de 5 GHz. Aquesta banda està dividida en dues sub-bandes: la primera banda 5,150-5,350 GHz, que només es pot emprar en entorns d'interior amb menys de 23 dBm de potència. A més a més, des de 5,250 GHz fins 5,350 GHz han de tenir mecanismes de control de potència; en cas contrari, la potència queda reduïda a un màxim de 20 dBm.
La segona banda, 5,470-5,725 GHz, pot ser emprada a exteriors i interiors amb una PIRE màxima de 30 dBm; 27 dBm en cas que no hi hagi mecanismes de control de potència.

1.1.3. Operacions de gestió

El protocol IEEE 802.11 gestiona els clients de cada xarxa mitjançant les operacions de gestió, les quals controlen totes les operacions des de la detecció del punt d'accés fins l'associació d'un client.

1.1.3.1. *Escanneig*

El procés pel qual una estació identifica punts d'accés propers als quals connectar-se s'anomena escanneig. En la cerca de xarxes l'estació pot especificar diversos paràmetres (veure Annex I), tot i que algunes implementacions incorporen alguns valors per defecte.

A continuació s'expliquen els dos tipus d'escanneig que contempla IEEE 802.11: l'actiu i el passiu.

1.1.3.1.1. *Escanneig actiu*

En aquest tipus d'escanneig l'estació cerca activament estacions a les quals connectar-s'hi, enviant a cada canal trames *Probe Request*. El procediment és el següent:

1. L'estació es mou a un canal i espera la recepció de qualsevol trama, ja que això indicaria que aquest canal s'està emprant. En cas que es rebi una trama, es demanaria accés al medi mitjançant CSMA/CA.
   Si no es rebés cap trama, després d'un temps igual a l'establert a *ProbeDelay*, es passaria a un altre canal.

2. Una vegada s'ha accedit al medi, s'estarà com a mínim un temps *MinChannelTime* i com a màxim un temps *MaxChannelTime* a cada canal. Si després del temps màxim el canal està buit, es mourà l'estació al següent canal. Durant aquest estat s'envien els *Probe Request* i s'esperen els *Probe Response*.

Les trames *Probe Response* son emeses únicament per una estació (l'AP) a cada BSS, i només quan aquesta ha rebut un *Probe Request*. Els camps més rellevants de les trames *Probe Request* i *Probe Responde* poden ser consultats a l'Annex I.

1.1.3.1.2. *Escanneig passiu*

A l'escanneig passiu l'estació escombra canal a canal a fi de rebre una trama *Beacon* enviada per algun punt d'accés. Aquestes trames *Beacon* faciliten tots els paràmetres que necessita una estació per connectar-s'hi a una xarxa.

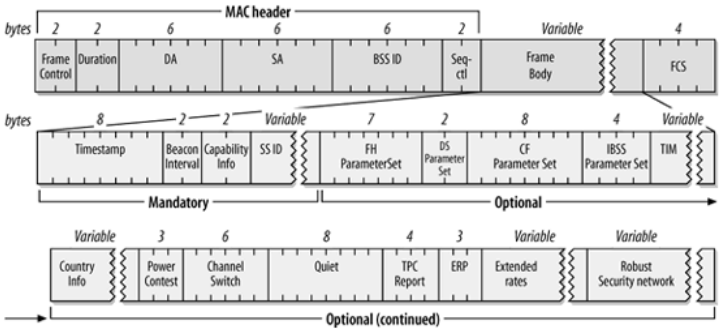


Figura 1.6. Camps d' una trama *Beacon.*

1.1.3.2. *Joining*

Després d'haver recopilat totes les xarxes sense fils disponibles segons els paràmetres de cerca, i abans d'associar-se definitivament a la xarxa, hi ha una etapa intermitja anomenada *joining*.

Una de les tasques més importants en aquesta etapa és la de la sincronització entre l'estació mòbil i la resta de la xarxa. A més a més, s'estableixen paràmetres tècnics de la capa física.

1.1.3.3. *Autenticació*

L'especificació 802.11 estableix que una estació ha d'identificar-se abans de poder enviar trames i que l'autenticació sempre és de l'estació i mai del punt d'accés, donat que aquest ja forma part de la xarxa.

1.1.3.3.1. *Open System Authentication (OSA)*

Open-System Authentication (OSA) és l'únic mètode d'autenticació requerit per l'estàndar 802.11. De fet, en l'especificació no es descriu com a tal, però el seus objectius el permeten descriure com un sistema d'autenticació, ja que obliga a identificar-se l'estació que vol connectar-se a la xarxa. Malgrat això, no és estrictament un sistema d'autenticació i, en conseqüència, no afegeix cap tipus de seguretat per impedir l'entrada d'intrusos a la xarxa sense fils.

Aquest mètode d'autenticació està format per dues etapes:

1. L'estació mòbil envia una trama a l'AP identificant-se, com a Ethernet, amb la seva MAC. El segon camp de la trama, que s'anomena *Authentication Algorithm Identification* està a 0, per indicar que el mètode OSA està en ús. El tercer camp de la trama és *Authentication Transaction Sequence*, que indica el nombre de trames que ha enviat l'estació mòbil, en aquest cas, el valor és 1.

2. A la segona etapa, l'AP processa la trama enviada i respon en conseqüència. A la trama de resposta hi ha tres parts importants: a la primera, al camp *Authentication Algorithm Identificacion* està a 0 per indicar que OSA està en ús. Al segon camp, *Authentication Transaction Sequence* està al valor 2, que indica que és la segona trama des de l'inici de la connexió entre l'AP i l'estació a autenticar-se. Per últim, el camp *Status Code* indica la resposta a la petició d'autenticació.

1.1.3.3.2. *Autenticació de clau compartida:WEP*

Els mètodes d'autenticació de clau compartida, com WEP (*Wired Equivalent Privacy*), operen en quatre seqüències:

1. Primerament, l'estació demana l'autenticació. Per això, envia una trama que conté informació per identificar l'algoritme d'autenticació i el número de seqüència. A més, el camp *Authentication Algorithm Identification* té el valor de 1, per indicar que s'està emprant una autenticació de clau compartida.

2. El destinatari respon amb una trama que refereix el tipus d'autenticació (*Authentication Algorithm Identification* amb el valor d'1), el número de seqüència (2 en aquest cas), l'*Status Code* (amb un valor de 0), que indica que no s'ha rebutjat l'autenticació, i un text de desafiament que l'estació receptora ha de xifrar.

3. L'estació respon de nou indicant el tipus d'autenticació, el número de seqüència i amb el missatge de desafiament xifrat amb la clau WEP.

4. Per últim, el receptor desencripta el missatge rebut i el compara amb el missatge de desafiament. Si són iguals, envia una trama indicant que l'autenticació s'ha produït. En cas contrari, l'*Status Code* indicarà que no ha estat satisfactòria.

1.1.3.3.3. *WPA*

Wi-Fi Protected Access (WPA) és una tecnologia desenvolupada en resposta a l'alta vulnerabilitat de WEP. Oficialment s'integrà la versió WPA2 a l'esmena 802.11i a IEEE 802.11.

WPA empra un xifrat de clau dinàmic, on la clau canvia constantment; a diferència de WEP, on la clau no varia.

Hi ha dues versions de WPA, en funció de en quin entorn s'utilitzi:

- Ús personal domèstic: Empra *Temporal Key Integrity Protocol* (TKIP), que és un mecanisme emprat per crear el xifrat de clau dinàmica i autenticació mútua.

- Ús empresarial: Empra la tecnologia 802.1X per autenticar els usuaris mitjançant un servidor RADIUS (*Remote Authentication Dial-In User Server*).

IEEE 802.11 defineix WPA2, la segona generació de WPA. Aquesta empra l'algoritme *Advanced Encryption Standard* (AES), que augmenta la seguretat respecte la primera generació.

1.1.3.4. *Associació*

L'associació d'una estació a un punt d'accés és el procés pel qual, una vegada completada l'autenticació, l'estació es connecta a la xarxa 802.11 tenint un accés complet a aquesta. A més a més, l'estació queda registrada a l'AP a fi que les trames enviades arribin correctament a l'estació de destinació.

Els clients sempre inicien el procés i són els punts d'accés els encarregats d'acceptar o no aquesta associació en funció de diversos paràmetres, com la seguretat o la distància. L'associació és exclusiva des del punt de vista de l'estació: una estació només pot estar associada a un punt d'accés, mentre que un punt d'accés pot estar associat a més d'una estació.

Malgrat que l'especificació no explicita cap límit quant a clients associats a un AP, a la pràctica sí que hi és degut a motius tècnics, com la impossibilitat de mantenir un número de comunicacions il·limitat i la disminució del *throughput* a mesura que augmenta el número d'associats.

El procediment d'associació és el següent:

1. L'estació envia un *Association Request* a l'AP, el qual li respondrà amb un *Association Response* en cas que l'associació es pugui portar a terme, o amb un *Deauthentication* si l'estació encara no s'ha autenticat.

2. Si el procés d'associació és correcte, l'AP respon amb un *Status Code* 0 i amb el *Association ID* corresponent. En cas que no es pugui fer l'associació, la trama únicament inclou l'*Status Code* on s'explica el motiu de la decisió negativa.

1.1.3.5. *Reassociació*

La reassociació és el procés pel qual una estació s'associa a una de nova. En el moment en què una estació detecta un punt d'accés que li ofereix un senyal de millor qualitat, s'inicia aquest procés.

El procés es divideix en les següents etapes:

1. L'estació envia un *Reassociation Request* al nou punt d'accés sol·licitant la reassociació des de l'antic AP. El nou AP s'ha de comunicar amb l'antic (la direcció del qual es proveeix a la trama de reassociació) per

verificar que l'antiga associació ha existit. En cas que per qüestions de compatibilitat (e.g.: l'antic AP empri sistemes propietaris que no compleixin l'estàndard), el nou punt d'accés denegarà l'associació per la impossibilitat de fer la verificació.

2. A continuació, i només en cas que s'hagi pogut realitzar la verificació, el punt d'accés processa la petició i envia una trama amb l'*Association ID* i amb el camp *Status Code* amb un valor de 0. En cas que no s'acceptés, l'AP només envia el motiu del rebuig a l'*Status Code*.

3. El nou punt d'accés contacta amb l'antic per finalitzar el procés de reassociació. Aquest últim envia els *frames* que es troben al seu *buffer* al nou punt d'accés per fer-los arribar a l'estació. Aquestes comunicacions són part de l'*Inter-Acces Point Protocol* (IAPP) o 802.11f, que governa les transmissions entre estacions i punts d'accés.

4. Per últim, l'estació deixa d'estar associada amb l'antic AP i comença a estar-ho amb el nou.

1.1.4. IEEE 802.11 MAC

IEEE 802.11 no es va crear del no-res, sinó que és una adaptació d' Ethernet a enllaços de ràdio. Així, mentre que Ethernet utilitza CSMA/CD, 802.11 empra *Collision Avoidance* (CSMA/CA).

En dissenyar l'accés al medi de l'especificació, es va acordar per raons econòmiques la incorporació d'un sol transceptor ràdio (és a dir, només podia o emetre o rebre, no emetre i rebre simultàniament). Per tant, no podia, com CSMA/CD, detectar col·lisions, però sí evitar-les (CA). També, com a Ethernet, no té cap controlador centralitzat i totes les estacions accedeixen al medi mitjançant el mateix mètode. Malgrat tot, la principal diferència entre un i altre es troba sota la capa d'enllaç, a la capa física.

Com d'altres protocols d'enllaç, 802.11 empra missatges positius de recepció de paquets. Així, qualsevol paquet ha d'ésser confirmat per l'estació receptora. En cas que l'emissor no rebés aquesta confirmació ACK (*acknowledgment*), el paquet seria reenviat.

1.1.4.1. *CSMA*

CSMA (*Carrier Sense Multiple Access)* és un mètode per accedir al medi que es basa en escoltar abans de parlar. Totes les estacions poden accedir al medi (accés múltiple), però han d'estar segurs que el recurs al qual volen accedir no està ocupat (detecció de portadora).

IEEE 802.11 té dos modes operatius, DCF (*Distributed Coordination Function*) i PCF (*Point Coordination Function*). Aquest últim és opcional i no és obligatoria la seva implementació. DCF està basat en CSMA/CA.

Les dues variacions més populars de CSMA són CSMA/CD i CSMA/CA.

- Si una estació que treballa amb CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) emet una trama i detecta que el medi està ocupat, deixa d'enviar el *frame*, envia un senyal que indica que deixa el medi buit i espera un tremps aleatori fins tornar a enviar la trama. Abans, però, d'enviar la trama, torna a escoltar el medi a fi de comprovar que no està ocupat. La principal diferència amb CSMA/CA és que, mentre envia el missatge, l'estació escolta el medi i, en cas que detecti presència al medi, pararà immediatament l'enviament.

- Una estació que empra CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), abans de començar a transmetre una trama, escolta el medi durant un temps IFS (*InterFrame Spacing*). En cas que el medi estigui ocupat, s'ajorna l'enviament durant un temps de *backoff*, triat aleatòriament entre tots els valors d'una finestra d'entre 0 i *Contention Window*. Aquest *timer* es pausa si el medi està ocupat o es decrementa si el medi està lliure durant un temps superior a DIFS (*Distributed InterFrame Space*). Quan arriba a 0, la trama s'envia.

  En cas que la trama no s'enviï correctament, la CW es dobla, triant de nou un temps aleatori de la finestra i repetint el procés anterior.

  Opcionalment, i per tal de reduir l'efecte del node ocult (veure Capítol 2), l'estàndard defineix un mecanisme d'accés basat en l'intercanvi de nous missatges RTS/CTS, que consisteix en l'enviament, per part de l'emissor, d'un missatge *Request To Send* (RTS), el qual serà respost amb un *Clear To Send* (CTS) per totes les estacions receptores. Aquest CTS silencia totes les estacions que el reben i permet l'accés al medi a l'estació que va enviar el RTS.

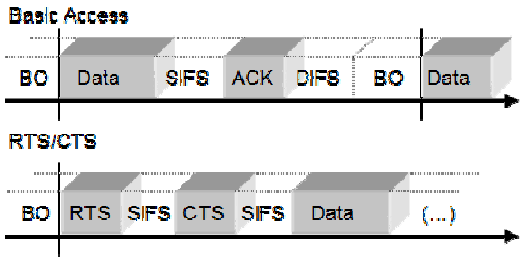


Figura 1.7. Seqüència de missatges per l'accés CSMA/CA bàsic i CSMA/CA amb RTS/CTS

1.1.5. Capa física

IEEE 802.11 defineix vàries tècniques d'eixamplat d'espectre (*spread spectrum*), però al mercat les dues més emprades són DSSS (*Direct Sequence Spread Spectrum*) i OFDM (*Orthogonal Frequency Division Multiplexing*). Aquestes tècniques són molt útils per a disminuir les interferències provocades, donat que la potència es distribueix en un amplada de banda major, no quedant concentrada en poques freqüències. D'altra banda, al repartir la informació en una porció més gran de l'espectre, s'aconsegueix major robustesa davant d'interferències de banda estreta.

A DSSS, l'ample de banda s'eixampla després de combinar el senyal inicial amb una seqüència de freqüència molt elevada. Una tècnica semblant és emprada per IEEE 802.11b, que introdueix *Complementary Code Keying* (CCK).

Tècnica	Modulació	Taxa [Mbps]
DSS	DBPSK	1
DSS	DQPSK	2
CCK	CCK/DQPSK	5,5
CCK	CCK/DQPSK	11
OFDM	BPSK	6
OFDM	BPSK	9
OFDM	QPSK	12
OFDM	QPSK	18
OFDM	16-QAM	24
OFDM	16-QAM	36
OFDM	64-QAM	48
OFDM	64-QAM	54

Taula 1.1. Taxes per modulació i tècnica d'eixamplat.

IEEE 208.11a i 802.11g especifiquen una capa física OFDM que divideix la informació en 52 subportadores. 4 de les subportadores s'empren com a referència per ignorar els desplaçaments en freqüència i fase. A les 48 subportadores restants, modulades, s'envien les dades de forma paral·lela. La separació de les subportadores és de 132,5 kHz i l'ample banda total és de 20 MHz (encara que només estan realment ocupats 16,6 MHz). D'aquesta manera, es redueix la influència de la propagació multicamí (*multipath*) i es guanya eficiència espectral.

A mesura que la modulació empra més símbols la taxa de transmissió augmenta. Així, BPSK obté com a màxim 9 Mbps, mentre que 64-QAM arriba fins els 54 Mbps.

CAPÍTOL 2. PROBLEMÀTIQUES I AMENACES

IEEE 802.11 té algunes problemàtiques i amenaces inherents a la seva naturalesa sense fils que impedeixen l'aprofitament total de totes les seves prestacions.

2.1. El problema del node ocult

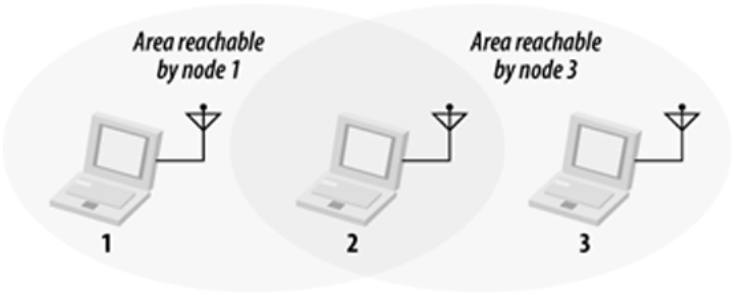


Figura 2.1. Els nodes 1 i 3 no es detecten entre sí.

A la Figura 2.1 els nodes 1 i 3 no es poden comunicar directament entre ells, ja que les seves respectives àrees de cobertura no cobreixen l'altre node. Si els dos nodes intentessin comunicar-se amb el node 2 simultàniament, ambdós podrien accedir al medi, doncs no es detecten, però hi hauria una col·lisió al node 2 i la informació es perdria, ja que l'estació no pot rebre paquets de més d'un node simultàniament.

En cas que tots dos nodes tinguessin cobertura un sobre l'altre, no es donaria mai el cas en què tots dos intentessin enviar un paquet al node 2 simultàniament, perquè el mètode d'accés al medi CSMA/CA els ho impediria. Com en aquest cas no es detecten entre ells, l'especificació 802.11 permet corregir aquest problema amb les instruccions RTS/CTS, que impedeixen la col·lisió de paquets.

Si l'estació 1 vol enviar un missatge a l'estació 2, la primera enviarà primer un missatge *Request To Send* (RTS) i la segona estació respondrà amb un *Clear To Send* (CTS). Amb aquests dos missatges, ambdues estacions silencien totes les estacions que es troben en el seu àmbit de cobertura, en conseqüència, si l'estació 1 envia un RTS a la 2, aquesta respon amb un CTS que impedeix que l'estació 3 transmeti res fins que passi un temps SIFS (*Short Interframe Space*).

Malgrat tot, aquestes trames que solucionen la problemàtica del node ocult consumeixen molta capacitat; per tant, només s'activen quan les trames a enviar són més grans que un llindar establert per l'administrador de la xarxa.

2.2. Problema del terminal exposat

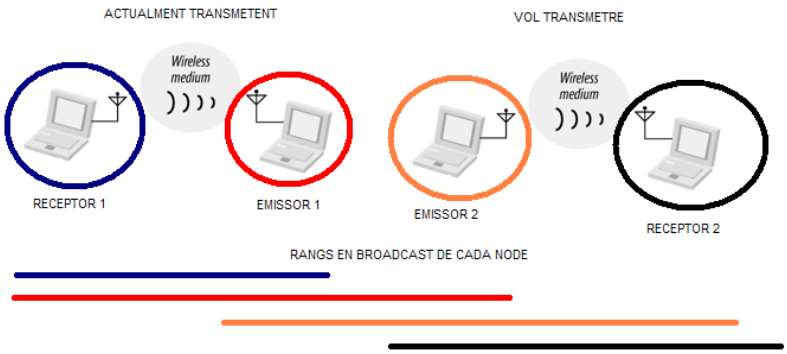


Figura 2.2. Situació en la qual es produeix el problema del terminal exposat.

Aquest problema provoca que una estació no emeti perquè, erròniament, creu que pot provocar una col·lisió.

Considerem dues estacions emissores: E1 i E2; i dues estacions receptores: R1 i R2.

Si E1 emet una trama amb destinació R1, E2 no enviarà res a R2 mentre duri aquesta comunicació, ja que creu que fent-ho provocaria una col·lisió amb les trames enviades per E1. Ara bé, R2 no està dins de l'abast d'S1, per tant, cap enviament des de E2 cap a R2 provocaria una col·lisió ja que el medi es troba lliure.

2.3. Qualitat de l'enllaç ràdio

L'ús de bandes sense llicència va ser un desafiament pels dissenyadors de l'especificació 802.11, ja que això suposava un gran nombre de potencials interferències. Ja no es podia assumir, com amb les connexions per cable, que cada paquet que un ordinador enviava a un altre era rebut. A més d'això, s'afegia el *clàssic* soroll blanc que afecta a tot l'espectre electromagnètic.

La qualitat de l'enllaç produeix un augment de la taxa d'error, la qual, per la seva banda, causa una disminució del *throughput* (Figura 2.3).

A més distància entre l'emissor i el receptor, pitjor relació senyal/soroll (SNR) i relació senyal/interferències i soroll (SINR), a més de menor velocitat.
Com es pot veure a la Figura 2.3, amb SNR baixes s'aconsegueix més *throughput* amb modulacions més robustes (per exemple, 1 Mbps) que amb les més sensibles (per exemple, 11 Mbps). Amb SNR altes, però, és més adient emprar modulacions més sensibles, perquè són les que poden proporcionar més *throughput* quan la qualitat de l'enllaç és bona.

L'espectre electromagnètic és un recurs escàs, per això s'ha de compartir. Les interferències produïdes pels dispositius poden classificar-se en dos tipus:

- Interferència co-canal: produïda pels aparells que empren el mateix canal.
- Interferència pel canal adjacent: produïda per transmissions en canals adjacents o solapats (veure Figura 1.5).

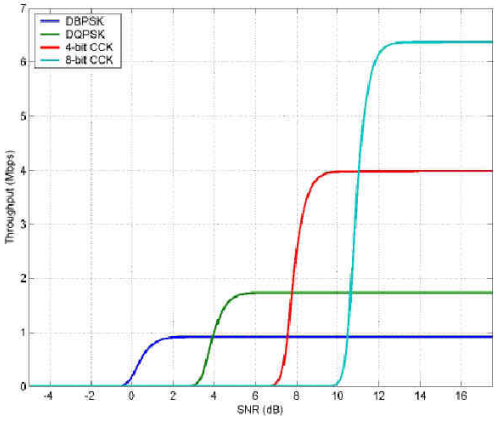


Figura 2.3. *Throughput* vs SNR a 802.11b.

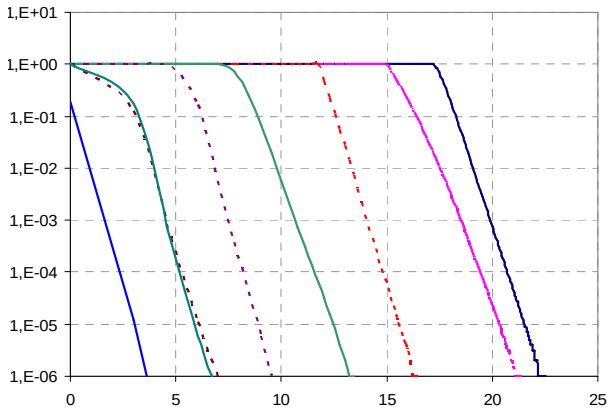


Figura 2.4. BER vs SINR a 802.11a/g.

2.4. *Jamming*

Les xarxes sense fils són sensibles a atacs DoS (*Denial of Service*) basats en les tècniques de *jamming.* Aquest atac consisteix en la transmissió per part d'un atacant d'un senyal de gran potència a la mateixa banda freqüencial utilitzada per la víctima (en aquest cas, la banda 2,4 GHz-2,4835 GHz). El senyal atacant interfereix en la comunicació, degradant la SINR (*Signal to Interference and Noise Ratio*).

A les xarxes sense fils IEEE 802.11 l'accés al medi es basa en CSMA/CA, que permet tenir més *throughput* que Aloha o altres versions de CSMA. Degut a la naturalesa de CSMA/CA, les tècniques *jamming* impedeixen totalment la comunicació, ja que el medi sempre serà considerat com ocupat si la potència detectada per l'estació supera un valor llindar. En conseqüència, no és necessària la emissió de grans potències per a llençar un atac efectiu.

Els atacants volen reduir el *throughput* de la xarxa i, a la vegada, emprar la menor energia possible. Això s'aconsegueix atacant paquets crítics, com els CTS o els ACK.

Aquest efecte pot donar-se accidentalment entre diferents dispositius que operen en la mateixa banda freqüencial, com els microones, altres xarxes sense fils Wi-Fi, aparells *bluetooth* o telèfons sense fils.

A les noves esmenes de 802.11 com 802.11h i 802.11k s'estan proporcionant nous mecanismes a fi de reduir la influència dels *jammers*. Per exemple, la gestió automàtica dels canals. Aquesta consisteix en la mesura sistemàtica de les condicions de cada canal, especialment pel que fa a senyals interferents. En cas que en el canal en ús hi hagués un senyal interferent, el punt d'accés coordinaria la migració de totes les comunicacions a un canal amb millors prestacions.

2.4.1. Tipus de *jammers*

D'acord amb [2] els *jammers* es poden classificar en quatre categories, en funció de la seva capacitat de sensar el medi i de la seva resposta a l'estat del medi.

- *Channel-Oblivious & memoryless*: No tenen capacitat per escoltar el canal i són independents de les seves accions passades. Dins aquesta categoria hi ha dos tipus: 1) en temps continu, els polsos *jamming* arriben segons una distribució de Poisson; 2) en temps discret, el *jammer* té una probabilitat P d'emetre un pols cada *slot* de temps.
- *Channel-Oblivious & stateful*: No escolten el canal, però les seves accions sí que depenen de les seves anteriors accions. Per exemple, un *jammer* periòdic. Aquest pot aconseguir que l'estació atacada no emeti, ja que el temps de *backoff*, a mesura que es detecta el medi ocupat, va augmentant progressivament.
  Per tant, l'estació pot arribar a tenir uns temps d'espera molt grans, en els quals no emet, permetent al *jammer* estalviar bateria (i guanyar, per tant, eficiència).
- *Channel-Aware & memoryless*: Emeten els polsos amb una taxa diferent segons l'estat del canal (ocupat, lliure...).
- *Channel-Aware & stateful*: Hi ha dos tipus: el reactiu i l'omniscient. Ambdós només ataquen quan els *frames* no han col·lisionat amb cap altre. L'omniscient, a diferència del reactiu, envia un puls *jamming* amb una probabilitat que depèn del temps de *backoff* de l'emissor.

2.4.1.1. *Eficiència dels jammers*

D'acord amb [2], els *jammers* sense memòria són els menys eficients de tots quatre tipus, tant a una xarxa poc saturada com a una saturada. Els periòdics són menys eficients que els omniscients i els reactius, per paquets petits, poques sessions i xarxes no saturades. Els omniscients són un 25% més eficients reduint el *throughput* que els reactius, especialment a xarxes petites amb poques sessions, les més típiques.

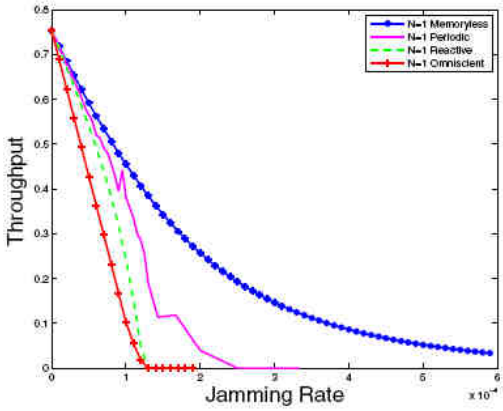


Figura 2.5. Comparació dels quatre *jammers*. Paquet de 500 bytes, 1 sessió.

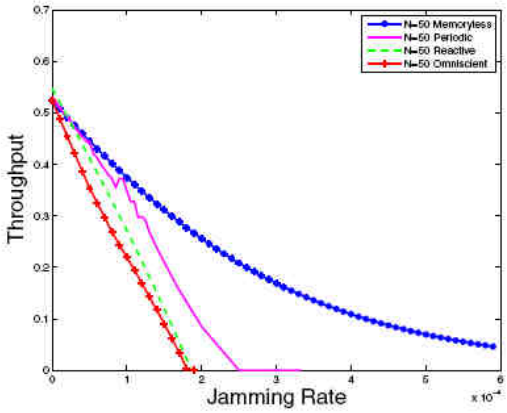


Figura 2.6. Comparació dels quatre *jammers*. Paquet de 500 bytes, 50 sesions.

2.4.1.2. *Disminució de la influència dels jammers*

Per reduïr la influencia de l'atac *jamming*, la víctima pot canviar a un canal on l'atacant no emeti. Evidentment aquesta solució no serà factible si l'atacant emet a tots els canals.

2.4.1.2.1. *Tipus de channel hopping*

El canvi de canal de l'estació legítima pot fer-se una vegada s'ha detectat que el canal que s'està emprant està patint un atac *jamming* o bé canviar de canal cada un cert temps aleatori. L'avantatge de la primera opció és que es fan menys canvis de canals, que evita temps morts en els quals la targeta de xarxa s'ha de reconfigurar a fi d'emetre per la nova freqüència. Però la segona opció s'estalvia comprovar cada cert temps que el canal no està sent utilitzat per un *jammer*, que és una operació bastant lenta, la qual pot durar fins-i-tot uns quants segons.

A la pràctica, segons [2], a la segona opció disminueix el *throughput* de forma mínima en absència de *jammers* respecte a la primera, però en cas d'atacs *jamming* la disminució del *throughput* es menor que quan l'estació verifica periòdicament que el canal no està sent atacat.

CAPÍTOL 3. MESURES DE *THROUGHPUT*

Les mesures de *throughput* tenen com a objectiu conèixer la influència del *jammer* a un enllaç sense fils 802.11 establert entre dues estacions en funció de la distància, de la modulació i de la grandària de paquet, entre d'altres variables.

3.1. L'escenari

L'estructura de totes les mesures serà la indicada a la Figura 3.1.

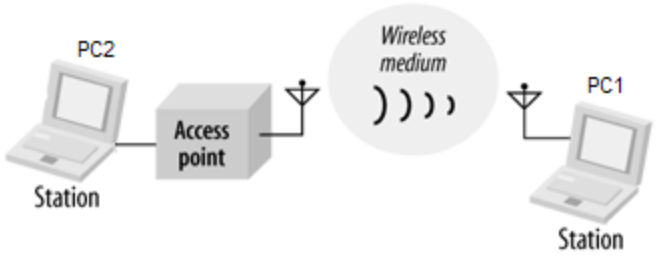


Figura 3.1. Escenari general de les mesures.

L'esquema està format per dos PC connectats entre ells mitjançant un AP Linksys WRT54G. A les mesures fetes a l'Escenari 1 (veure Figura 3.2) els PC són LG Pentium III, mentre que a les fetes a l'Escenari 2 (veure Figura 3.3) són dos PC portàtils Acer Pentium Centrino.

La targeta sense fils emprada pel PC1 és una 3com OfficeConnect Wireless 54 Mbps Compact USB Adapter.

Per a fer les mesures, un ordinador (client) enviarà paquets a l'altre (servidor) indicant, si s'escau, altres paràmetres, com la longitud del paquet i l'ample de banda a emprar. Per fer això s'utilitzarà el programa Iperf [4] o la seva versió gràfica Jperf [5], que és una eina que permet analitzar el comportament de la xarxa: mesurar l'ample de banda màxim amb *Transmission Control Protocol* (TCP) i *User Datagram Protocol* (UDP) i les pèrdues de datagrames.

Per a comprovar quina és la influència del lloc on es fan les mesures s'ha decidit fer-les en dos escenaris diferents:

El primer escenari (veure Figura 3.2) serà una aula de grandària mitjana (uns 35 m^2), que permetrà observar el comportament del *jammer* en un espai tancat.

El segon escenari (veure Figura 3.3) serà el soterrani de l'Escola. La configuració és la mateixa que al primer escenari, amb la diferència que el *jammer* es pot allunyar desenes de metres havent-hi línia de visió directa entre aquest i el PC1 en tot moment. Aquest escenari ens ajuda a veure la influència

de la distància que separa el *jammer* i un transmissor/receptor sobre el *throughput* en unes condicions on la propagació multicamí (*multipath*) és molt gran.

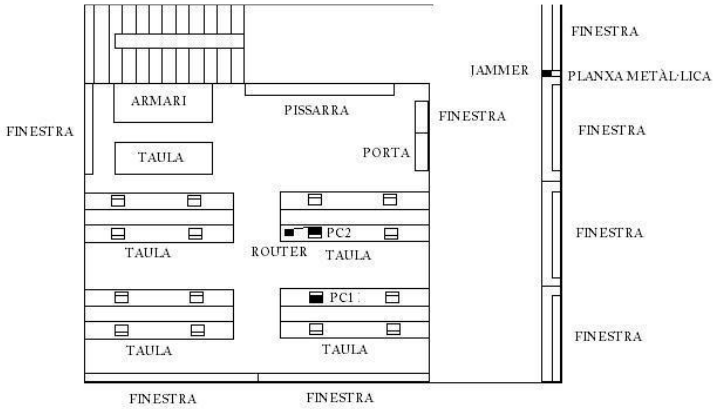


Figura 3.2. Croquis de planta del primer escenari.

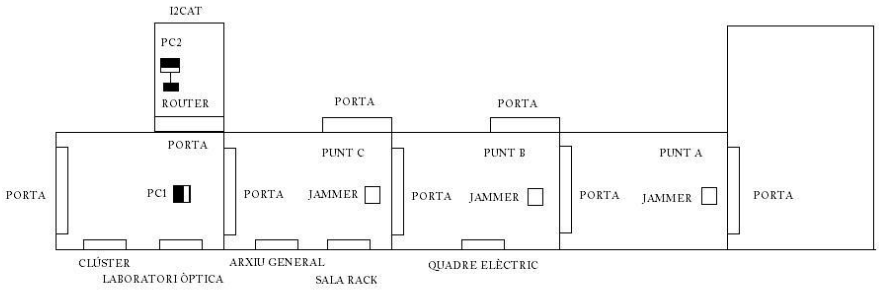


Figura 3.3. Croquis de planta del segon escenari.

3.1.1. El *jammer*

El *jammer* emprat a les mesures (Figura 3.5) emet a les bandes freqüencials de diverses tecnologies: 802.11b i 802.11g, *bluetooth* i GSM 900.
L'espectre freqüencial mostrat a la Figura 3.4 permet veure les seves emissions a les freqüències de GSM (900 MHz) i a la banda ISM de 2,4GHz

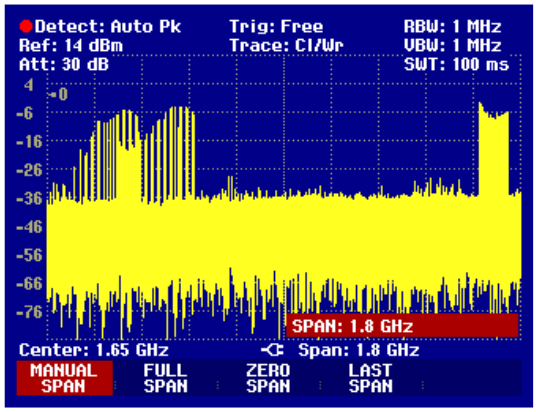


Figura 3.4. Espectre freqüencial amb *jammer*.

Segons les especificacions, l'inhibidor té una cobertura d'uns 10 metres de radi i emet una potència total de 450 mW. Experimentalment, però, s'ha verificat que el radi d'influència del *jammer* és molt superior.

Figura 3.5. *Jammer*

Per veure la seva influència a l'espectre freqüencial s'ha emprat un analitzador d'espectres Rohde & Schwarz Handheld Spectrum Analyzer amb una antena omnidireccional.

A les Figures 3.6 i 3.7 es pot veure com influeix l'inhibidor a l'espectre freqüencial. A la primera, el nivell mitjà de potència rebuda per l'analitzador és molt baix. En canvi, una vegada encès el *jammer*, la potència rebuda augmenta de forma espectacular.

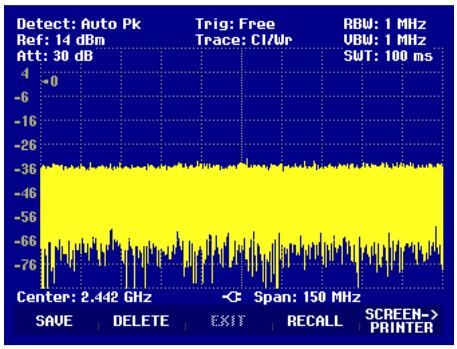


Figura 3.6. Espectre en absència del *jammer*.

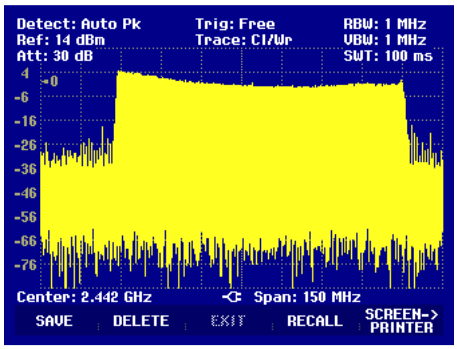


Figura 3.7. Espectre en presència del *jammer*

La potència rebuda amb el *jammer* a una distància d'un metre és de -16,7 dBm des dels 2412 MHz (canal 1) fins els 2477 MHz (canal 14) (veure Figura 3.9). La diferència entre la potència amb *jammer* i sense *jammer* és de 40,4 dB.

La potència rebuda deguda al *jammer* disminueix amb l'augment de la distància del *jammer* amb l'enllaç sense fils i amb l'increment del temps en què el *jammer* es troba encés (ja que la bateria disminueix i, en conseqüència, també la potència emesa).

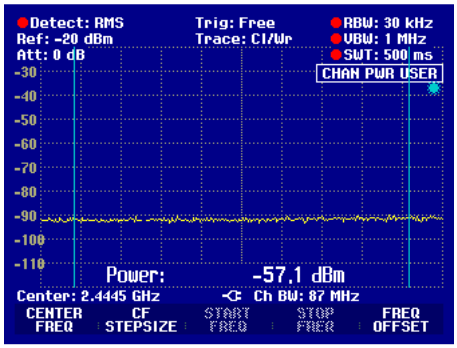


Figura 3.8. Potència a la banda de 802.11b sense *jammer*.

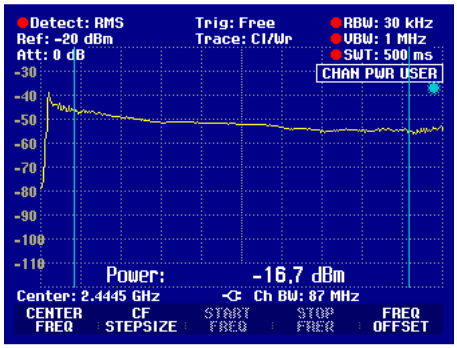


Figura 3.9. Potència a la banda de 802.11b amb *jammer*.

Al canal 11 la potència rebuda varia amb el temps segons la gràfica de la Figura 3.10. La variació no és molt significativa fins els primers 90 minuts. En canvi, a partir d'aquest punt, disminueix ràpidament fins arribar als -60 dBm, que és la potència del canal en absència de *jammer.*

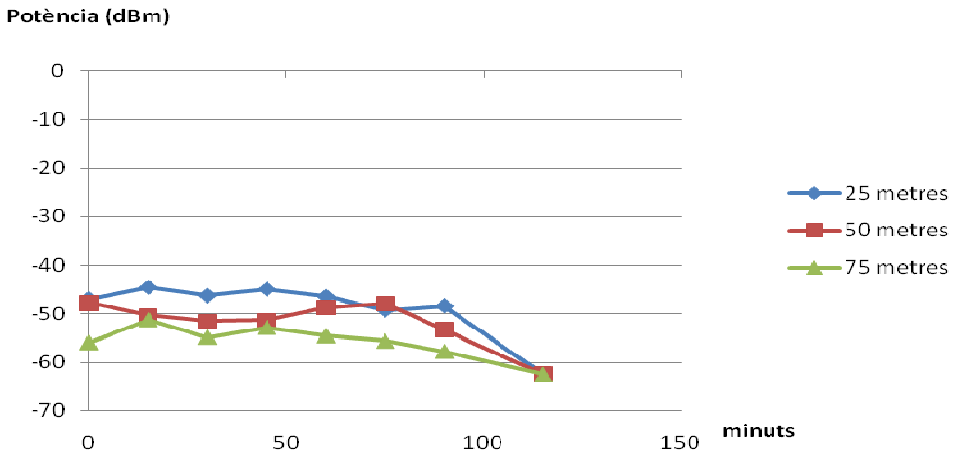


Figura 3.10. Potència al canal 11 en funció del temps i la distància amb el *jammer*.

Com s'ha vist a les captures de l'espectre freqüencial, la potència emesa per l'inhibidor és molt alta. Aquest fet provoca que, en cas que el *jammer* es trobi prop d'un enllaç sense fils, aquest caigui i no es pugui tornar a establir la connexió fins que l'inhibidor deixi d'emetre.

La Figura 3.11 mostra aquest fet. El *jammer* s'encén mentre PC1 està enviant paquets a PC2. La connexió passa de 6 Mbps a 0 Mbps en dos segons i no tornarà a recuperar-se fins que s'apagui o s'allunyi el *jammer*.

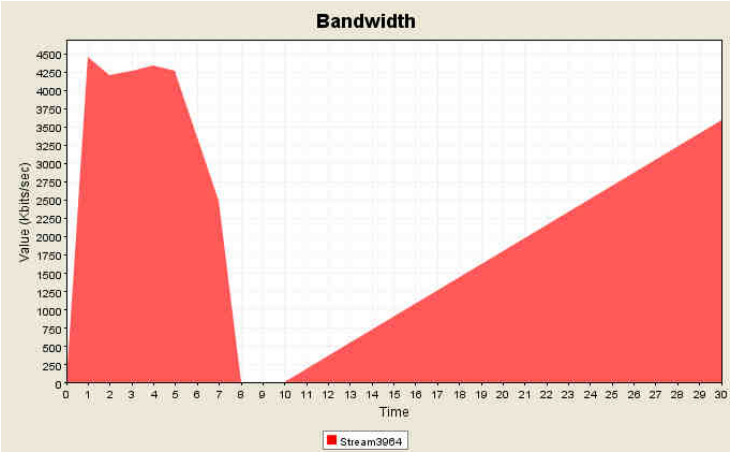


Figura 3.11. Variació de la taxa a nivell de transport en encendre un *jammer*.

El lent increment del *throughput* que mostra la Figura 3.11 després que el *jammer* hagi interromput la connexió es deu al control de congestió de TCP. Sempre que TCP detecta una pèrdua de paquets ho interpreta com a congestió (encara que no sempre sigui així, com no ho és quan hi ha un *jammer* proper). El mecanisme de control de congestió de TCP (*congestion avoidance*) funciona

incrementant la mida de la finestra de forma lineal, cosa que produeix un augment també lineal de la taxa a nivell d'enllaç, com mostra la Figura.

3.2. Metodologia

La metodologia per assolir els objectius constarà de dues etapes:

A la primera, es verificarà quin és el *throughput* que, sense cap inhibidor, assoleix l'enllaç ràdio.

A la segona, els resultats obtinguts donaran a conèixer la variació del *throughput* causada per la influència del *jammer*.

En ambdues etapes s'analitzarà la influència d'altres variables en els resultats, com són la distància amb el *jammer*, la modulació, la mida de les trames o el protocol de la capa de transport.

D'altra banda, totes les taxes (T) que a continuació es presentaran són a nivell d'enllaç. Donat que Iperf només proporciona valors a nivell de transport, en ocasions s'ha hagut d'emprar el següent factor de conversió:

$$T_{enllaç} = T_{transport} \frac{Longitud\ trama}{Longitud\ paquet}$$

Així, la longitud del paquet serà la longitud de la trama menys la capçalera a nivell d'enllaç. Aquesta varia en funció del protocol emprat: si és TCP és 40 bytes, en canvi, a UDP és de 28 bytes.

3.3. Resultats

A continuació es presenten els resultats de les mesures fetes als dos escenaris.

3.3.1. Primer escenari

Les mesures al primer escenari es subdivideixen en mesures sense *jammer* i mesures amb *jammer*.

3.3.1.1. Mesures sense jammer

Les mesures al primer escenari s'han fet amb dues taxes físiques, dos protocols i tres grandàries de trames diferents.

La taxa física més lenta i més robusta és 1 Mbps, mentre que la més ràpida i sensible al soroll i les interferències és la que ofereix 11 Mbps.
Els protocols emprats són TCP i UDP. El primer té control d'errors i congestió, el qual converteixen el tràfic en una font elàstica. El segon, en canvi, no té cap control sobre el tràfic, la qual cosa el fa més ràpid però menys fiable.

S'han triat tres mides de trama diferents, a fi de poder conèixer el comportament del *throughput* en funció de la variació del nombre de bytes de cadascuna.

Els resultats presentats a la Taula 3.1 són les mitjanes de quatre mesures fetes en cada cas. Aquestes quatre mesures consten de dues mesures de baixada i dues de pujada. Les dues primeres són els *throughputs* obtinguts en el sentit PC2→ PC1, mentre que les últimes són els obtinguts en el sentit contrari.

***Throughput*/Desviació típica**	**1 Mbps [Mbps]**		**11 Mbps [Mbps]**	
	TCP	**UDP**	**TCP**	**UDP**
200 Bytes	0,470 / 0,004	0,575 / 0,039	1,98 / 0,30	1,99 / 0,39
900 Bytes	0,770 / 0,001	0,837 / 0,005	3,84 / 0,40	5,21 / 0,24
1500 Bytes	0,842 / 0,017	0,865 / 0,005	5,32 / 0,21	5,72 / 0,16

Taula 3.1. Resultats de les mesures de *throughput* sense *jammer* al primer escenari.

La Taula 3.1 reflexa dos fets: Primer, que la taxa assolida amb UDP sempre és superior a la de TCP a les mateixes condicions. Segon, que a mesura que el paquet és més gran el *throughput* augmenta.

La desviació típica en termes percentuals és molt superior a 11 Mbps que a 1 Mbps, a causa de la major sensibilitat de la primera modulació.

Malgrat que no queda reflectit a la taula, hi ha dos fets importants a destacar. En primer lloc, s'han fet mesures amb una interfície de xarxa Avaya USB Wireless Client Gold obtenint uns resultats sensiblement diferents a totes les mesures, tot i que es desprenen les mateixes conclusions. També s'han fet mesures amb altres modulacions (veure Taula II.3 de l'Annex II) i s'han obtingut valors superiors al màxim teòric [3] (veure Taula 3.2 i 3.3). Aquest fet pot ser causat per la no conformitat dels diferents dispositius amb les especificacions de l'estàndard 802.11b.

La relació entre les mitjanes de les mesures fetes i el màxim teòric es pot veure a la Figura 3.12. Tot i que no hauria d'haver cap punt que superés el 100%, ja que això significaria que s'han obtingut taxes superiors a les que teòricament no es poden superar, 11 Mbps supera el màxim teòric amb paquets de 200 bytes a TCP i UDP en 28 punts percentuals.

Tècnica d'eixamplament d'espectre	Modulació	Taxa física [Mbps]	*Throughput* [Mbps]
OFDM	BPSK	6	5,37
	BPSK	9	7,78
	QPSK	12	10,00
	QPSK	18	14,12
	16-QAM	24	17,60
	16-QAM	36	23,73
	64-QAM	48	28,46
	64-QAM	54	30,80
DSSS/CCK	DBPSK	1	0,91
	DQPSK	2	1,71
	CCK	5,5	3,90
	CCK	11	6,10

Taula 3.2. *Throughput* màxim teòric d'un paquet de 1500 bytes amb un usuari.

Taxa física	Longitud [bytes]	*Throughput* màxim teòric [Mbps]
1 Mbps	200	0,595
	900	0,868
	1500	0,917
11 Mbps	200	1,55
	900	4,672
	1500	6,067

Taula 3.3. *Throughput* màxim teòric en funció de la longitud de paquet.

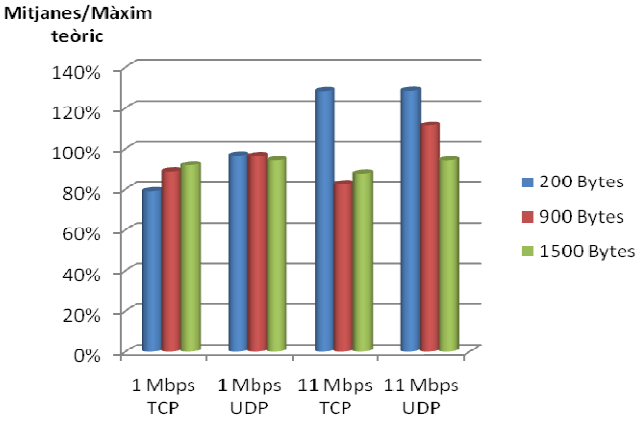


Figura 3.12. Percentatge del màxim teòric que suposa la mitjana de les mesures de *throughput* sense *jammer*.

3.3.1.2. Mesures amb jammer

Degut a les dimensiones de l'aula, no és possible fer cap mesura amb el *jammer* encès sense que la connexió caigui del tot. Per això, s'ha pensat que una alternativa per poder fer-les és situar el *jammer* darrere d'una planxa metàl·lica situada a dos metres de l'aula, a un metre i mig d'alçada, mantenint el punt d'accés protegit per la torre del PC2.

Els resultats (veure Taula 3.4), mostren, com en les mesures sense *jammer*, un millor comportament d'UDP i un major *throughput* a mesura que la longitud del paquet augmenta. La desviació típica és més gran en la pràctica totalitat dels casos que a les mesures sense *jammer*. La causa d'aquest fet és que l'aparell provoca unes interferències que, per la seva naturalesa, fan variar el *throughput* més que en el cas en què no hi ha inhibidor.

***Throughput*/Desviació típica**	**1 Mbps [Mbps]**		**11 Mbps [Mbps]**	
	TCP	**UDP**	**TCP**	**UDP**
200 Bytes	0,428/ 0,033	0,562/ 0,036	1,35 / 0,36	1,75 / 0,58
900 Bytes	0,729/ 0,013	0,842/ 0,011	2,77 / 0,85	4,40 / 0,46
1500 Bytes	0,784/ 0,022	0,873 / 0,003	3,50 / 1,34	4,86 / 0,57

Taula 3.4. Resultats de les mesures de *throughput* amb *jammer* al primer escenari.

Quan un *jammer* fa acte de presència prop d'una xarxa sense fils, el *throughput* entre els dos PCs disminueix de forma dràstica, però no en la mateixa magnitud sempre. Així, la Figura 3.13 mostra com la disminució és molt més gran a taxes físiques altes (més sensibles) que a taxes més robustes com 1 Mbps. A més a més, l'inhibidor de freqüències afecta a tots els paquets de forma similar, tant als més grans com als més petits.

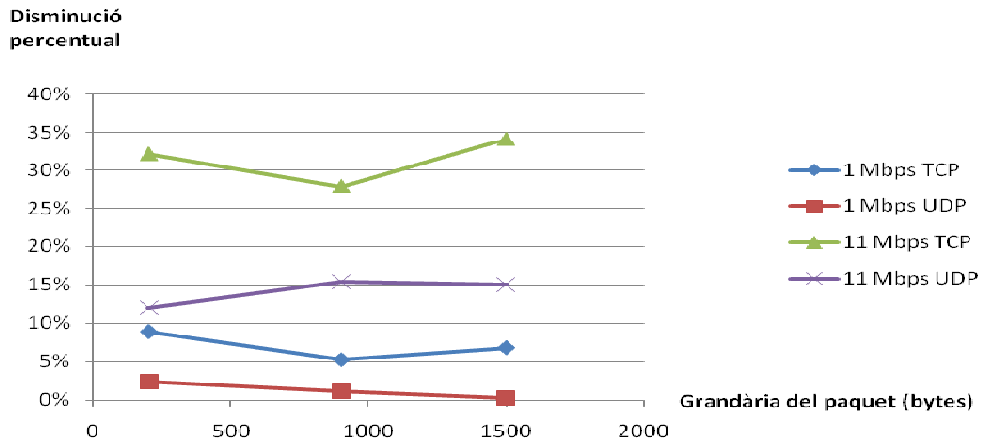


Figura 3.13. Disminució percentual del *throughput*.

Com mostra la Figura 3.14, UDP en tots els casos obté millors taxes a nivell d'enllaç que TCP. Aquest fet, en el cas d'1 Mbps és causat per la menor capçalera emprada per UDP. A mesura que la grandària de la trama augmenta, la importància de la capçalera disminueix, tot disminuint també per aquest motiu la diferència entre el *throughput* assolit emprant cadascun dels protocols.

A 11 Mbps hauria de succeir un fet similar teòricament però, a la pràctica, no ocórre. Això pot ser degut a la gran variació que sofreix el *throughput* d'aquesta modulació, la qual cosa impedeix poder verificar el fet teòric. Per tant, es pot dir que la longitud de les trames no influeix de forma decisiva en l'augment percentual del *throughput* d'UDP respecte TCP a 11 Mbps, tot i que sí que ho fa a 1 Mbps.

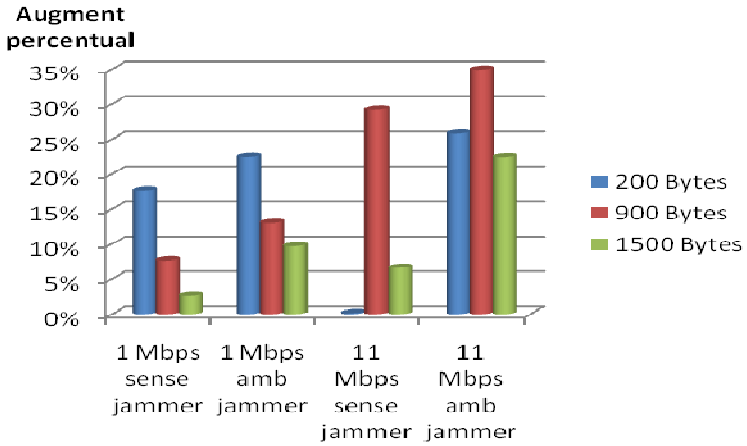


Figura 3.14. Augment percentual d'UDP respecte TCP.

La relació de les mitjanes de *throughput* amb el màxim teòric que mostra la Figura 3.15 segueix sent similar a quan no hi havia *jammer*. Ara 11 Mbps UDP supera el màxim teòric en 12 punts percentuals, mentre que sense l'inhibidor ho feia en 28. 11 Mbps TCP obté un *throughput* a 200 bytes del 87% del màxim teòric, quan abans obtenia un 128%. Per la seva banda, 11 Mbps UDP és el 112% del màxim teòric, quan abans ho era en un 128%.

El *jammer*, per tant, ha aconseguit disminuir el *throughput* considerablement, però tot i això hi ha una mesura de la modulació d'11 Mbps que segueix superant el màxim *throughput* teòric.

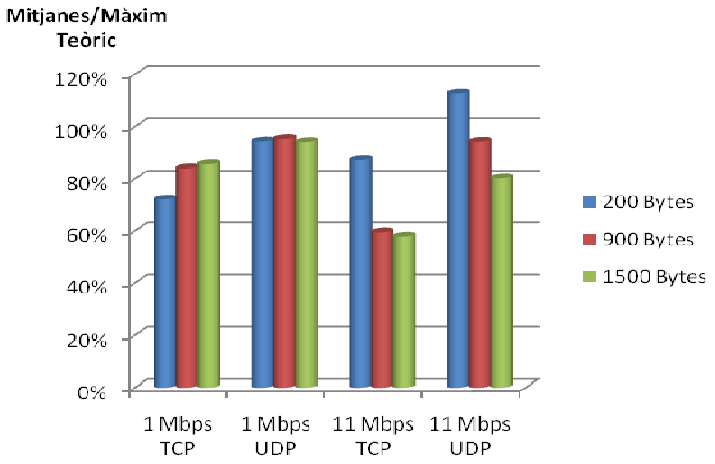


Figura 3.15. Percentatge del màxim teòric que suposa la mitjana de les mesures de *throughput* amb *jammer*.

3.3.2. Segon escenari

Les mesures al segon escenari s'han fet amb la modulació més sensible i la més robusta, emprant el protocol que més *throughput* aconsegueix assolir segons les mesures al primer escenari, UDP.

L'escenari, tal i com s'ha mostrat a la Figura 3.3, és el soterrani de l'Escola. Les mesures s'han fet situant el *jammer* a un mínim de 3 metres i a un màxim de 50 metres de l'enllaç sense fils.

3.3.2.1. Mesures sense jammer

Les mesures del segon escenari s'han restringit a les modulacions d'1 Mbps i 11 Mbps i al protocol UDP. No s'ha emprat TCP perquè al primer escenari ja es va poder comprovar que aquest protocol assoleix sempre taxes inferiors. La llargària de les trames és de 900 bytes.

	1 Mbps [Mbps]	**11 Mbps [Mbps]**
	UDP	
Mitjana	0,876	5,830
Desviació típica	0,021	0,160

Taula 3.5. Resultats de les mesures de *throughput* sense *jammer* al segon escenari.

Les mitjanes obtingudes no varien en gran quantitat amb els resultats de les mesures sense *jammer* a l'escenari 1 (veure Taula 3.1). En canvi, la desviació típica és molt superior en aquest escenari a la modulació més robusta, donat

que és molt més procliu a la propagació multicamí que el primer. La modulació més sensible no ha sofert aquest augment de la desviació típica perquè al primer escenari ja experimentava una gran variabilitat per la seva naturalesa molt més sensible.

3.3.2.2. Mesures amb jammer

A la Taula 3.6 es mostren les mitjanes de les mesures de baixada i de pujada amb *jammer* a l'escenari 2. Les mesures completes es poden consultar a l'Annex II.

	1 Mbps [Mbps]	**11 Mbps [Mbps]**
	UDP	**UDP**
Distància amb *jammer*	**5 metres**	
Mitjana	0,180	0,008
Desviació típica	0,181	0,015
Distància amb *jammer*	**10 metres**	
Mitjana	0,655	0,277
Desviació típica	0,111	0,272
Distància amb jammer	**25 metres**	
Mitjana	0,818	0,780
Desviació típica	0,008	0,785
Distància amb jammer	**30 metres**	
Mitjana	0,808	1,728
Desviació típica	0,008	1,670
Distància amb jammer	**40 metres**	
Mitjana	0,831	5,540
Desviació típica	0	0,311
Distància amb jammer	**50 metres**	
Mitjana	0,831	5,706
Desviació típica	0	0,107

Taula 3.6. Resultats de les mesures de *throughput* amb *jammer* al segon escenari.

Tal i com va passar a les mesures de l'escenari 1, la desviació típica és més gran a 11 Mbps que a 1 Mbps. Això és causat per la major sensibilitat d'aquesta modulació al *jammer* i perquè aquest escenari és més procliu a la propagació multicamí.

La relació senyal-soroll augmenta significativament a mesura que el *jammer* s'allunya. Així, a 10 metres és de 4 dB, a 25 metres 19 dB i a 40 metres 24 dB. Per tant, la distància entre l'inhibidor i l'enllaç sense fils és un factor molt important.

La influència al *throughput* de la distància que el separa del *jammer* és major a la modulació més sensible, on la diferència entre la taxa obtinguda a 5 metres i la obtinguda a 50 metres és d'un 99%, mentre que a 1 Mbps és d'un 77%.

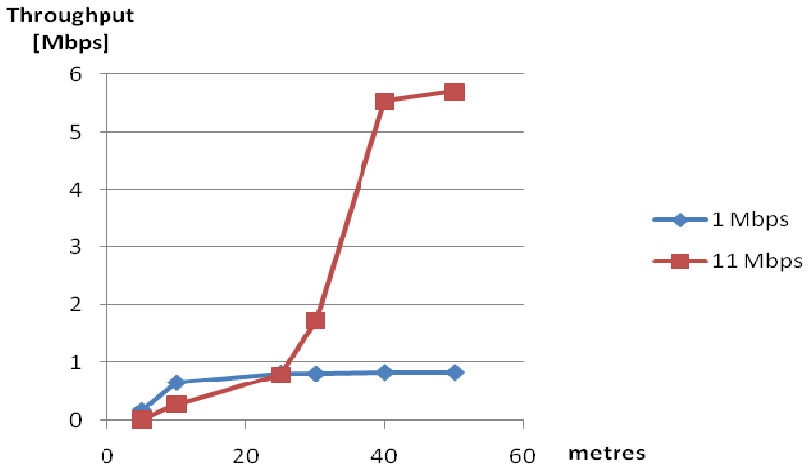


Figura 3.16. Variació del *throughput* en funció de la distància.

Com es pot observar a la Figura 3.16, 1 Mbps és molt més estable globalment –i, per tant, més robust- que 11 Mbps.
A menys de 25 metres 1 Mbps assoleix taxes superiors a les obtingudes per 11 Mbps. A partir d'aquesta distància 11 Mbps augmenta ràpidament tot arribant al seu màxim teòric als 50 metres, quan el *jammer* no exerceix cap influència a l'enllaç.

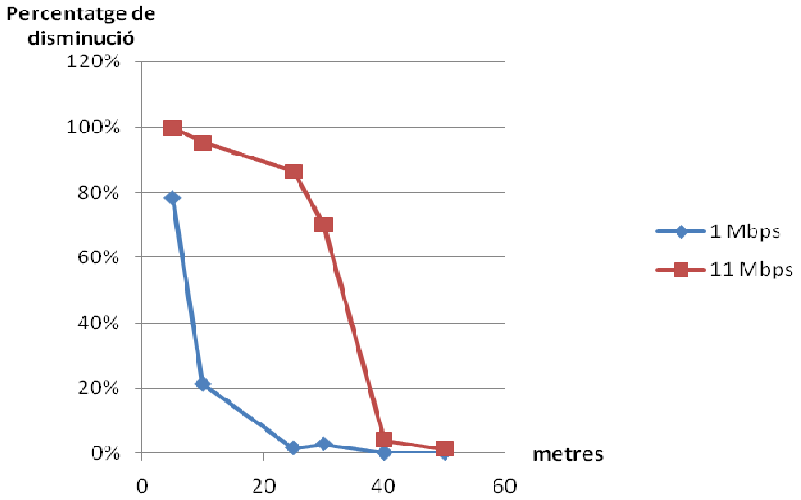
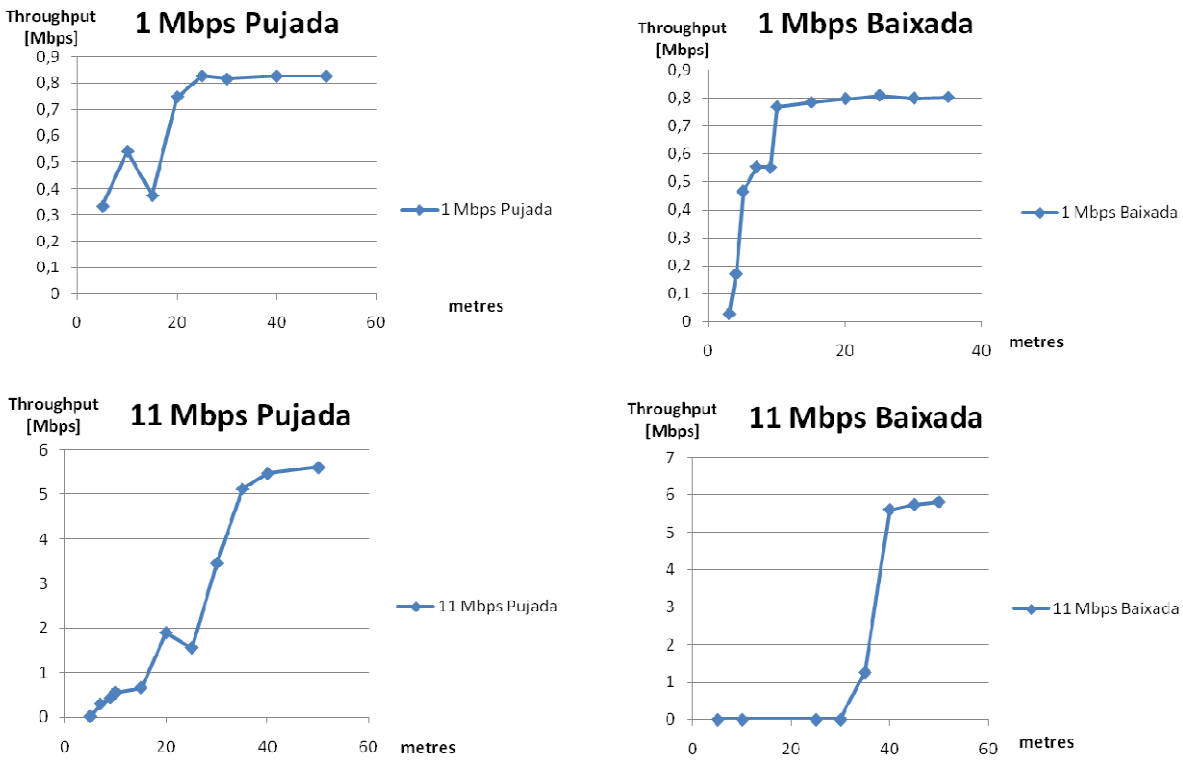


Figura 3.17. Disminució percentual del *throughput* amb *jammer* respecte al màxim experimental.

La disminució del *throughput* (Figura 3.17) respecte el màxim experimental és màxima a ambdues modulacions en distàncies petites (a 5 metres, el 78% a 1 Mbps i el 99% a 11 Mbps). A mesura que la distància del *jammer* augmenta, va disminuint fins el 0% d'1 Mbps a 50 metres i el 1,2% d'11 Mbps.



Figures 3.18. Gràfiques de pujada i baixada a 1 i 11 Mbps

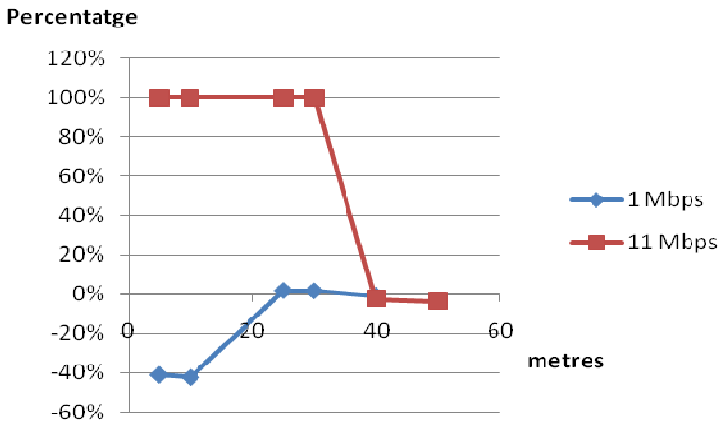


Figura 3.19. Augment percentual de la pujada respecte la baixada amb *jammer* a 1 i 11 Mbps UDP.

La modulació d'11 Mbps té un comportament millor a la recepció (pujada), mentre que la d'1 Mbps ho té en el de transmissió (baixada).

A la transmissió d'una trama, com es va explicar al Capítol 1, abans d'enviar un paquet es comprova que el canal no està ocupat. La potència a partir de la qual es considera que el canal està ocupat és superior a 11 Mbps que a 1 Mbps.

A la recepció el rendiment de cada modulació depèn de la SNR del canal, donat que el soroll rebut afecta a la capa física del model OSI. En canvi, en el cas de la transmissió, afecta a la capa d'enllaç.

En el sentit de baixada, 1 Mbps té un millor comportament perquè és més robust davant del soroll que 11 Mbps.

A la pujada, és 11 Mbps la modulació que obté millors resultats precisament perquè el punt d'accés, que es qui envia les trames, considera durant més temps que el canal no està ocupat. En aquest cas no influeix que la modulació d'1 Mbps sigui més robusta, ja que l'AP no està tan exposat a l'inhibidor com en el cas de la baixada (on el PC sí que està directament exposat al *jammer*), com es pot veure a la Figura 3.3.

3.4. Conclusions

Ambdós escenaris ens mostren que 1 Mbps és la modulació més estable i més resistent davant d'un potencial *jammer*, i que és aquest factor i no tant la grandària dels paquets, el més influent en la disminució del *throughput* en presència d'un *jammer*. Tot i això, 11 Mbps segueix sent la modulació que ofereix millor ample de banda, tot i ser més sensible a tot tipus d'interferències.

UDP és el protocol on més taxa a nivell d'enllaç podem obtenir, encara que sacrificant el control d'errors i de congestió, que només té TCP. A vegades s'han obtingut taxes superiors al màxim teòric amb aquest protocol, degudes segurament a detalls sobre l'implementació de l'estàndard 802.11 als equips emprats.

Per últim, l'efecte del *jammer* depèn en gran mesura de la modulació emprada i del sentit –pujada o baixada- de la comunicació. A 11 Mbps la pujada és millor que la baixada, mentre que a 1 Mbps és al revés. Això succeeix perquè, a la transmissió, el llindar de potència per considerar el canal ocupat és superior a 11 Mbps que a 1 Mbps; en canvi, a la recepció, el factor més important és la SNR, superior a la modulació més robusta.

CAPÍTOL 4. DETECCIÓ D'UN ATAC DE *JAMMING*

La detecció d'un atac per part d'un *jammer* es pot realitzar mitjançant la monitorització de diferents paràmetres estadístics característics dels enllaços sense fils. En aquest Capítol es pretèn analitzar aquests paràmetres a fi de trobar quin o quins poden indicar de forma més precisa la presència d'un inhibidor de freqüències.

4.1. Estadístiques bàsiques en la detecció de jamming

D'acord amb [6], les següents estadístiques poden indicar si un node està sent objecte d'un atac *jammer*:

4.1.1. Potència del senyal

La potència total a la banda freqüencial emprada pel receptor augmenta de forma considerable en presència d'un *jammer*. Per tant, la mesura de la potència a l'ambient pot ser una estadística que, correctament emprada, pot indicar si un node està sent víctima d'un atac *jamming*.

Per fer-ne ús s'han de recopilar estadístiques de la potència a la banda freqüencial en absència de *jammer*. Un tractament estadístic d'aquestes dades haurà de determinar un valor llindar a partir del qual es pot considerar que hi ha un atac *jamming*.

4.1.2. Temps de detecció de portadora

El protocol d'accés al medi CSMA/CA impedeix que un node legítim emeti mentre que un altre node –per exemple, un *jammer*- està ocupant el canal.

La mesura del temps d'accés al medi és una dada molt important que pot indicar que un node està sent víctima d'un atac *jamming* si el seu valor excedeix el valor típic obtingut mitjançant un mostreig estadístic en condicions normals d'aquesta magnitud.

Aquest criteri només és vàlid si el node legítim empra un llindar fix de potència del senyal per determinar si el canal està ocupat o no. En cas que el valor llindar sigui adaptatiu, el temps de detecció de portadora podria arribar a ser més petit amb *jammer* que sense *jammer* amb un valor llindar fix. Per tant, les estadístiques no seria homologables entre sí perquè variarien constantment en funció del canal.

4.1.3. *Packet Delivery Ratio*

Un *jammer* no només pot impedir l'enviament de paquets per un node legítim, sinó que també pot corrompre un paquet en transmissió.

Es defineix com a *Packet Delivery Ratio* (PDR) la relació entre els paquets correctament entregats al receptor i els paquets enviats correctament per l'emissor.

La PDR es pot calcular tant al receptor com a l'emissor. Al receptor és la relació entre els paquets rebuts amb un CRC correcte i tots els paquets rebuts. A l'emissor és la relació entre els ACK rebuts i els paquets enviats correctament.
Un mètode per detectar l'existència d'un *jammer* és la definició d'un valor màxim de PDR admissible, a partir del qual s'entén que un inhibidor està afectant la integritat dels paquets transmesos.

D'acord amb [7] un receptor pot reconèixer que se l'està atacant pels patrons d'energia que rep. No obstant, això necessita un processat digital de senyal (DSP) disponible només a àmbits militars; per això, els autors creuen que és millor emprar tècniques heurístiques. Mitjançant l'heurística es podria calcular el valor de la "utilitat" de les comunicacions establertes o rebudes i un valor llindar sota el qual es consideraria com a comunicació de poca utilitat molt sospitosa de ser un atac *jamming*.

Els factors que es consideren en el càlcul del valor llindar de la "utilitat" són:

- Impossibilitat reiterada d'accés al medi sense fils
- Trames incorrectes
- Errors als *checksums*
- Valors il·legals a adreces o altres camps
- Violació de protocols (e.g.: ACK no enviats)
- Excessiu nivell de senyal rebut
- Baixa SNR
- Col·lisions repetides
- Duració d'aquestes condicions

Aquestes dades han de ser recollides al hardware local, capa d'enllaç, de xarxa o qualsevol altre mitjà disponible.

4.2. *Driver* hostap i obtenció d'estadístiques

Un altre mètode per detectar un atac *jamming* és la monitorització de diversos paràmetres amb el *driver* hostap.

El *driver* hostap permet visualitzar paràmetres estadístics els quals, amb un correcte processament, permeten la detecció de la presència d'un inhibidor de freqüències.

Aquests paràmetres estan dividits en dos arxius accessibles a través del sistema de fitxers /proc a Debian:

- Arxiu d'estadístiques de cada client: Cada client té un arxiu anomenat amb la seva MAC. Els paràmetres més importants que conté són:

    - *Tx_packets*: Nombre de paquets enviats.
    - *Rx_packets*: Nombre de paquets rebuts.
    - *Tx_bytes*: Nombre de bytes enviats.
    - *Rx_bytes*: Nombre de bytes rebuts.
    - *Tx[modulació]*: Nombre de paquets enviats a cada una de les modulacions (1, 2, 5,5 i 11 Mbps).
    - *Rx[modulació]*: Nombre de paquets rebuts a cada una de les modulacions (1, 2, 5,5 i 11 Mbps).

- Arxiu d'estadístiques del punt d'accés: Anomenat "stats", conté estadístiques de l'AP. Les més importants són:

    - *TxDeferredTransmissions*: Nombre de paquets que han retardat el seu enviament per evitar una col·lisió al medi.
    - *TxUnicastFrames*: Nombre total de paquets transmesos la destinació dels quals és una adreça MAC *unicast*.
    - *TxMulticastFrames*: Nombre total de paquets transmesos la destinació dels quals és una adreça MAC *multicast*.
    - *TxUnicastOctets*: Nombre total d'octets transmesos formant part d'un paquet *unicast*.
    - *TxMulticastOctets*: Nombre total d'octets transmesos formant part d'un paquet *multicast*.
    - *RxFCSErrors*: Nombre de paquets rebuts amb errors de *Frame Check Sequence*.
    - *TxSingleRetryFrames:* Nombre de paquets correctament transmessos després d'una sola retransmissió.

4.2.1. Obtenció de paràmetres útils en la detecció de *jamming*

Aquest apartat té com a objectiu obtenir quins són els paràmetres proporcionats per hostap que indiquen millor la presència d'un inhibidor de freqüències.

4.2.1.1. *Escenari i metodologia*

L'equipament emprat a les proves per detectar els paràmetres que indiquen la presència d'un *jammer* són dos PC i un *jammer*.

Per realitzar les mesures s'ha emprat un ordinador amb Debian instal·lat, que fa de punt d'accés, amb el *driver* hostap [8]. Al client s'utilitza Iperf sobre Windows XP.

Per comprovar la influència del *jammer* en els paràmetres s'han fet les mesures en quatre escenaris diferents (de baixada i de pujada):

- Sense *jammer.*
- Sense *jammer* amb obstacles: S'ha emprat per esbrinar si els paràmetres que varien per la presència del *jammer* varien també en cas que entre els dos ordinadors hi hagi una distància considerable (uns 20 metres) i obstacles entre ells (portes, parets).
- Amb *jammer* amb obstrucció total: El *jammer* es troba entre els dos PC, afectant de la mateixa manera a ambdós.
- Amb *jammer* amb obstrucció parcial: El *jammer* afecta més al PC que fa d'AP.

Les mesures s'han fet, com al capítol anterior, emprant Iperf. Una vegada el client ha acabat d'enviar paquets s'han guardat les estadístiques per analitzar posteriorment els paràmetres. Tots els valors es troben a l'Annex II.

4.2.1.2. *Resultats*

Les mesures s'han realitzat amb tràfic, tant en baixada com en pujada, i sense tràfic.

4.2.1.2.1. Baixada

En les transmissions en sentit de baixada (AP → client) el paràmetre més significatiu és *TxDeferredTransmissions*.

Aquest paràmetre expressa el número de vegades que s'ha retardat l'enviament d'un paquet per evitar una col·lisió. En condicions normals el seu valor és baix, ja que el medi no sempre està ocupat. En canvi, si un *jammer* està emetent, el seu valor és molt alt, tal i com mostra la Figura 4.1.

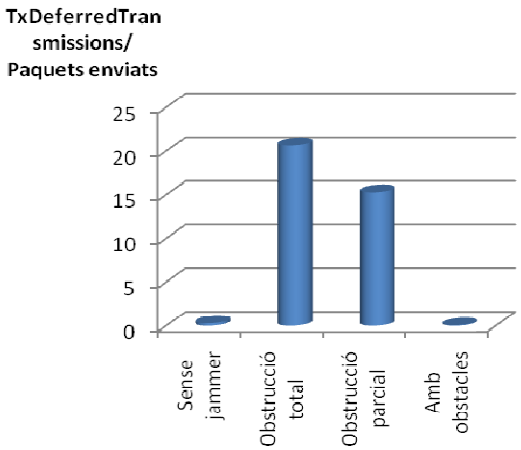


Figura 4.1. Intents de transmissió per cada paquet, a la baixada.

Tant a "sense *jammer*" com a "amb obstacles" els valors són molt baixos. En les situacions en què l'inhibidor està present el valor es dispara fins els 20 intents de transmissió per paquet. El nombre de transmissions és superior a "obstrucció total" que a "obstrucció parcial" perquè l'exposició de l'enllaç ràdio al *jammer* també és major al primer cas que al segon.

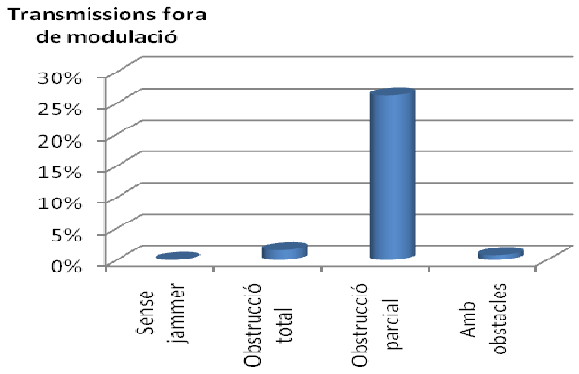


Figura 4.2. Transmissions fora de modulació per cada cent paquets, a la baixada.

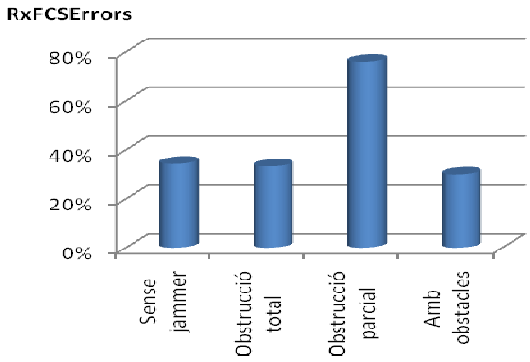


Figura 4.3. Errors FCS per cada cent paquets rebuts, a la baixada.

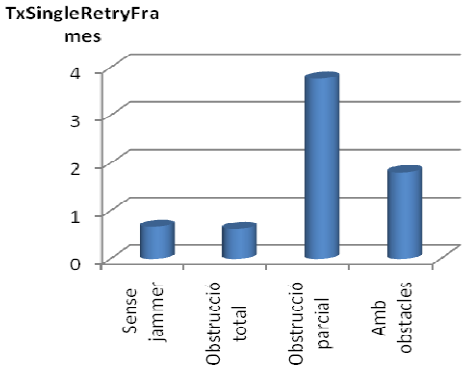


Figura 4.4. Número de paquets transmessos després d'una sola retransmissió, a la baixada.

Quan la presència del *jammer* només causa una obstrucció parcial augmenten el número de transmissions fora de la modulació per defecte (veure Figura 4.2). Així, mentre que les mesures s'han fet a una modulació per defecte d'11 Mbps, en el cas d'obstrucció parcial hi ha hagut una gran part de paquets que s'han enviat a 1, 2 i 5,5 Mbps.
Si el medi té molt de soroll (la SNR és baixa) 802.11 permet enviar els paquets a altres modulacions més robustes a fi de minimitzar la probabilitat d'error. No es pot aplicar en moltes ocasions en cas d'obstrucció total, ja que la SNR és tan baixa que ni amb la modulació més robusta el paquet podria no patir cap error. En canvi, en el cas d'una obstrucció parcial la SNR no és tan baixa com perquè no es pugui enviar.

Els errors en la recepció de paquets són més alts també en cas d'una obstrucció parcial que en cas d'obstrucció total (Figura 4.3). Això succeeix perquè, tot i que haurien de ser superiors en el segon cas, aquests paquets no s'arriben a rebre mai (a diferència de la situació d'obstrucció parcial); per tant, no es compatibilitzen com a paquets rebuts erronis i *RxFCSErrors* acaba sent inferior.

El paràmetre *TxSingleRetryFrames* (Figura 4.4) expressa el número de paquets que han estat transmesos després d'una sola retransmissió. En el cas d'un medi de molt baixa qualitat, com és la obstrucció total, aquest paràmetre serà molt baix perquè necessita molts més intents per poder enviar un paquet, en cas que ho pogui aconseguir.

4.2.1.2.2. Pujada

A la pujada, a diferència de la baixada, el paràmetre *TxDeferredTransmissions* no és representatiu de l'existència d'un *jammer*. Com mostra la Figura 4.5, per les quatre situacions el valor és molt similar.

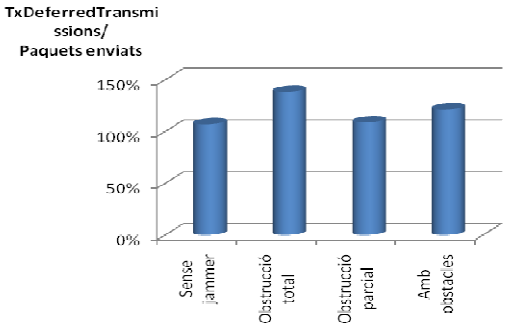


Figura 4.5. Relació entre *TxDeferredTransmissions* i els paquets enviats a la pujada.

Un paràmetre molt important és el nombre de paquets rebuts. A la Figura 4.6 es pot veure el seu nombre per totes les situacions assajades. En cas que hi hagi un atac d'un *jammer* el nombre de paquets rebuts baixa sobtadament, mentre que en condicions normals és molt més alt.

Si *TxDeferredTransmissions* és similar per totes les situacions no és possible distinguir a la pujada, tenint en compte només aquest paràmetre, si el canal està sent atacat per un *jammer* o si es troba en una situació d'alta ocupació.

Amb el nombre de paquets rebuts aquesta dificultat pot quedar resolta. En cas que hi hagi un *jammer* atacant, el nombre de paquets rebuts serà molt baix, mentre que si el canal té una alta ocupació el seu nombre serà molt més alt.

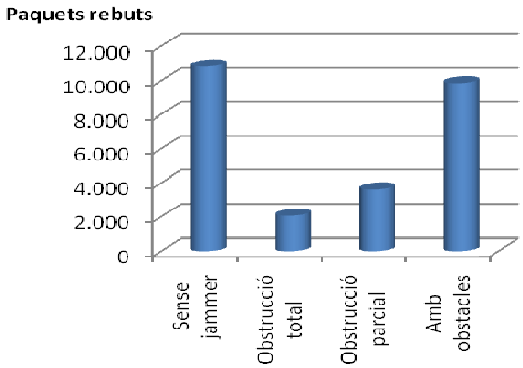


Figura 4.6. Nombre de paquets rebuts a la pujada.

En cas que un inhibidor no afectés directament el punt d'accés però sí als seus clients, el nombre de paquets rebuts seria també menor que en condicions normals, donat que els clients no podrien enviar ni rebre cap paquet de l'AP.

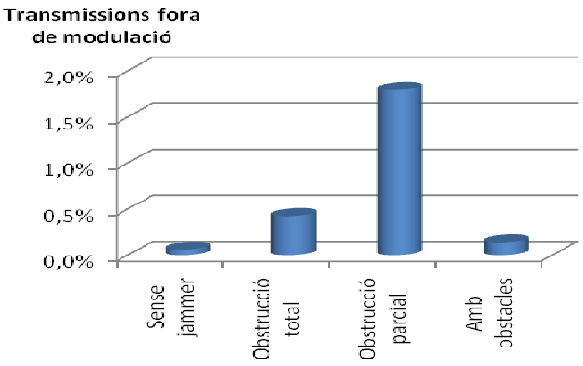


Figura 4.7. Transmissions fora de modulació, a la pujada.

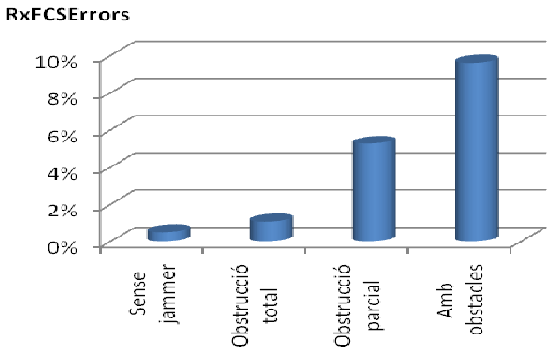


Figura 4.8. Errors FCS als paquets rebuts, a la pujada.

A la pujada, de la mateixa manera que a la baixada, les transmissions fora de la modulació per defecte són superiors també a "obstrucció parcial" (Figura 4.7). En canvi, els errors de recepció són superiors a "amb obstacles" (Figura 4.8), a diferència de la baixada, on era superior a "obstrucció parcial".

4.2.1.2.3. Sense tràfic

El nombre de transmissions per paquet també ens indica la presència d'un inhibidor en cas que no hi hagi tràfic. El valor de *TxDeferredTransmissions* pot ser fins a deu vegades superiors amb *jammer* que sense *jammer,* com es pot veure a la Figura 4.9, degut a la influència de l'inhibidor en l'enviament de les trames *Beacon* o *Probe Responses*.

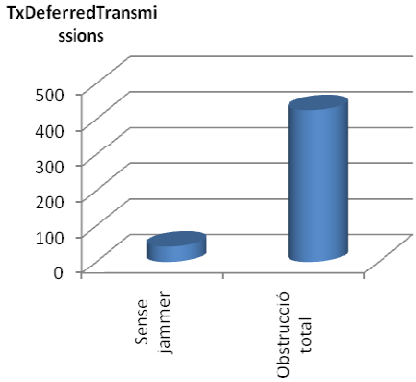


Figura 4.9. Intents de transmissions per paquet en un AP sense tràfic.

4.2.1.3. *Conclusions*

Els paràmetres que ajuden a detectar la presència d'un *jammer* varien en funció del tipus d'influència d'aquest a l'enllaç ràdio.

En cas que l'inhibidor obstrueixi totalment la comunicació, el número de transmissions per paquet és el paràmetre més afectat. Però només en el sentit de baixada, perquè a la pujada en aquesta situació la estadística que varia més en presència d'un *jammer* és el número de paquets rebuts.

Si l'inhibidor obstrueix parcialment la comunicació, els paràmetres que s'han de tenir més en compte a la baixada són el número de paquets enviats a una modulació menor a 11 Mbps i el número de paquets enviats correctament després d'una sola retransmissió. A la pujada el més important és també el nombre de paquets rebuts a una modulació menor d'11 Mbps.

En cas que no hi circuli tràfic a través d'un AP, el nombre de transmissions per paquet és molt superior en presència d'un *jammer* que en la seva absència.

Com es pot veure, hi ha una casuística molt complexa: per cada sentit del tràfic i situació de l'atacant hi ha un o més paràmetres que poden reflexar la presència d'un *jammer*. Detectar un atac en aquestes condicions és molt difícil, pel qual es proposa al següent apartat tenir en compte altres paràmetres, a més d'alguns estudiats en aquest, per realitzar la detecció.

4.2.2. Mètode de detecció d'un atac *jamming*

Un altre mètode per realitzar la detecció de *jamming* és la obtenció del temps d'ocupació del canal on s'ha establert un enllaç sense fils.
El temps d'ocupació del canal (en %) ens indica el percentatge de temps en què el canal està sent ocupat per tràfic de dades des del punt de vista de l'AP i en sentit de pujada (client → AP). Així, si no hi ha *jammer* el temps d'ocupació

del canal serà alt si hi ha tràfic de dades, mentre que si s'està rebent un atac serà molt baix perquè aquest impedeix que hi hagi tràfic de dades cap al punt d'accés.

A continuació, s'hauria d'obtenir el nombre d'intents de transmissió per paquet llindar (1) segons una caracterització del canal feta en condicions normals (sense *jammer)*, que relacioni el temps d'ocupació amb el nombre d'intents de transmissió per paquet. Aquest número serà la referència per detectar la presència d'un atacant.

Per últim, s'hauria de calcular el nombre d'intents de transmissió per paquet del canal en el moment de l'execució de l'aplicació (2) mitjançant els paràmetres del *driver* hostap.

Si (2) és superior a (1) el nombre d'intents de transmissió per paquet reals és superior al nombre d'intents de transmissió per paquet llindar (el nombre que correspon a la ocupació del canal) i, per tant, en aquest cas hi ha *jammer*. En cas contrari, no n'hi ha.

4.3. Conclusions

En aquest Capítol s'ha pogut comprovar l'existència de moltes tècniques per detectar inhibidors de freqüències, tot i que no totes són factibles i algunes són més fiables que d'altres.

En el nostre cas, s'ha decidit emprar una solució al nostre parer més fiable i que no depèn de la casuística de sentits de la transmissió (baixada i pujada) i posició relativa del *jammer* (obstrucció total o parcial), sinó que només ho fa d'uns pocs paràmetres que indiquen de forma directa i clara la presència d'un atacant.

CAPÍTOL 5. IMPLEMENTACIÓ D'UN PROGRAMA DETECTOR DE *JAMMERS*

A partir dels resultats de l'anterior Capítol, es proposa desenvolupar una aplicació amb la finalitat de detectar un *jammer*.

5.1. Caracterització del canal

La caracterització del canal és necessària per saber quins són els valors llindar en condicions normals d'intents de transmissió per paquet corresponents a un temps d'ocupació donat.

5.1.1. Metodologia

S'han mesurat el número de transmissions per paquet de manera experimental amb diferents modulacions, tràfics oferts i longituds del paquet.

Els intents de transmissió per paquet s'ha calculat segons la següent equació:

$$Intents\ per\ paquet = \frac{TxDef - TxDefOld}{TxMultFram - TxMultFramOld + TxUniFram - TxUniFramOld}$$

La variable *Intents per paquet* s'ha obtingut amb un programa que, en primer lloc, captura els paràmetres proporcionats pel *driver* hostap i després els guarda a *TxDef* (1), *TxMultFram* (2) i *TxUniFram* (3).

Un temps "t" després es copien aquests últims valors a unes altres variables (*TxDefOld*, *TxMultFramOld* i *TxUniFramOld*) i, a continuació, es tornen a capturar els nous valors a les variables (1), (2) i (3).

Finalment, els intents d'accés al medi per paquet, es calculen segons l'equació anterior.

5.1.2. Resultats

A les següents Figures estan representats els resultats de les mesures fetes en diferents condicions per obtenir els intents per paquet característics del canal.

En presència de dos clients, pràcticament per a qualsevol tràfic ofert i en totes les figures, el nombre d'intents per paquet és superior al que hi ha amb el mateix tràfic ofert amb un client. Això és causat perquè quan hi ha més d'un client connectat a un AP ambdós poden intentar accedir al medi simultàniament

i, per tant, la probabilitat de retardar l'enviament d'un paquet per evitar una col·lisió augmenta.

A mesura que la taxa física augmenta, també ho fa el nombre d'intents per paquet. Així, mentre que a 1 Mbps el màxim és 159 (Figura 5.1), a 5,5 Mbps és de 221 (Figura 5.2) i a 11 Mbps és de 434 (Figura 5.3).

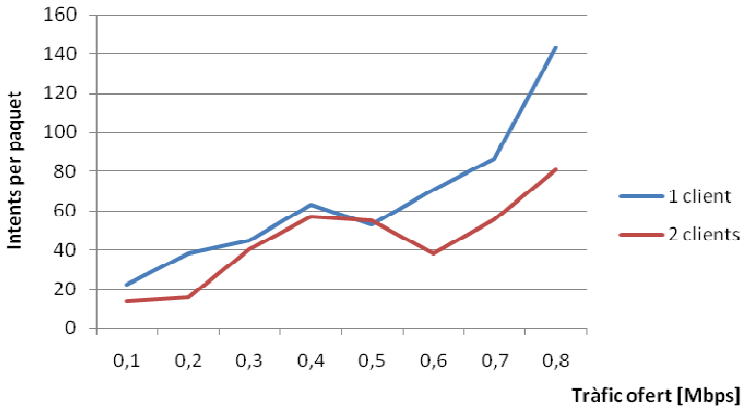


Figura 5.1. Intents per paquet en pujada, a 1 Mbps i 1000 bytes.

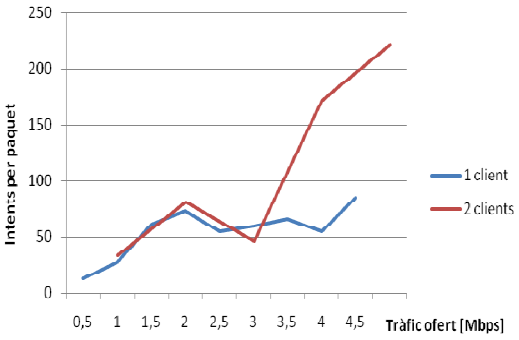


Figura 5.2. Intents per paquet en pujada, a 5,5 Mbps i 1000 bytes.

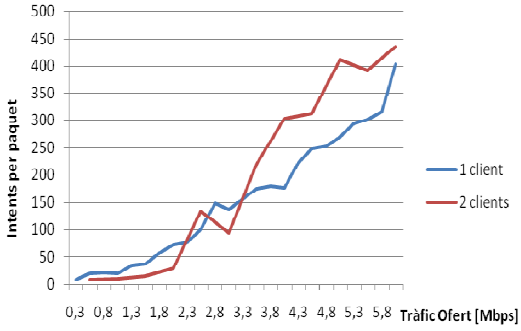


Figura 5.3. Intents per paquet en pujada, a 11 Mbps i 500 bytes.

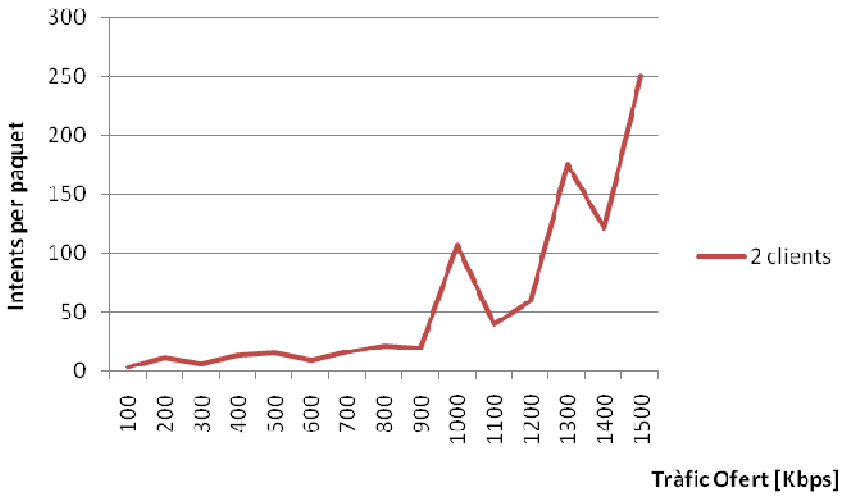


Figura 5.4. Intents per paquet en pujada amb l'AP a 11 Mbps, amb un client a 1 Mbps i un altre client a 11 Mbps. Longitud de paquet de 1000 bytes.

A la Figura 5.4 l'AP establia l'enllaç a 11 Mbps, mentre que un client ho feia amb 1 Mbps i l'altre amb 11 Mbps també. Amb aquesta combinació no és possible superar teòricament els 1500 Kbps entre els dos clients, i s'obté un màxim de 251 intents per paquet.

5.1.3. Gràfica característica del canal

A la Figura 5.5 es representen totes les mesures anteriors. Estan representades en funció del percentatge del medi que està ocupat. Així, amb un client d'1 Mbps enviant 450 Kbps tindrem un 50% d'ocupació (donat que un client a 1 Mbps pot arribar a enviar 900 Kbps). En el cas d'un client amb una modulació d'11 Mbps aquesta ocupació s'aconseguiria amb un tràfic ofert de 3 Mbps (donat que pot injectar fins a 6 Mbps).

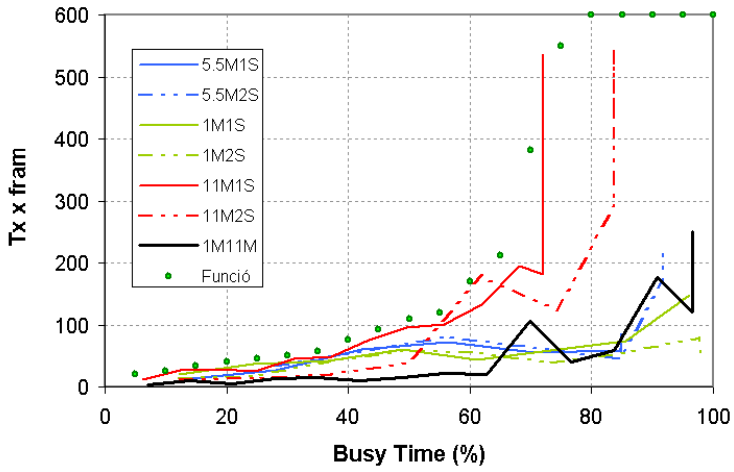


Figura 5.5. Intents per paquet en funció de la ocupació del canal.

El programa desenvolupat calcularà, mitjançant aquesta caracterització del canal, el nombre d'intents de transmissió per paquet llindar a partir del temps d'ocupació del canal (en %).

5.2. Programa de detecció de jammer

El programa ha estat desenvolupat en C i fa ús d'estructures dinàmiques per gestionar de forma més eficient la memòria. El codi es pot consultar a l'Annex III.

L'ordinador que exerceix de punt d'accés de la xarxa on s'ha executat aquest aplicatiu és un Toshiba Intel Centrino de 1400 MHz amb una memòria RAM de 760 MB.

5.2.1. Visió global del funcionament

El programa detector de *jammers* guarda els paràmetres estadístics necessaris de cada client a variables internes fent dues captures preses amb *t* segons de diferència. Una vegada estan carregades, calcula els valors mitjans de la taxa física, el *throughput*, la relació senyal-soroll i la longitud de paquet tenint en compte el temps entre ambdues preses de dades.

Els valors calculats se li passen a un programa que analitza la càrrega d'una cel·la IEEE 802.11 des del punt de vista d'un AP a partir de mesures de tràfic cursat. Mitjançant l'algorisme presentat en [9], aquest codi és capaç de calcular, entre d'altres coses, el temps d'ocupació del canal (en %).

Per últim, una vegada obtinguda la ocupació del canal, es busca quin és el valor llindar d'intents per paquet per a l'actual valor d'ocupació del canal, segons la caracterització del canal. Si el valor obtingut pel *driver* hostap en el moment de la execució del programa és superior a l'obtingut mitjançant la caracterització del canal (Figura 5.5) hi ha *jammer*, en cas contrari, no n'hi ha.

5.2.2. Pseudocodi

```
Struct sta
Struct staList
Struct stats
Integer t
Float Llindar, Txdef

UpdateMAC(staList)
UpdateAP(stats)
While (true)
      Sleep(t)
      UpdateMAC(staList)
      UpdateAP(stats)
      Llindar  = ComputeTxDef(staList)
      TxDef    = ComputeTxDefMeas(stats)
      If TxDef  > Llindar
            sendAlarm()
      End If

End while
```

staList conté una llista de les estacions *sta* associades. *Sta* conté variables que emmagatzemen les dades estadístiques referents a cada client associat, facilitades per hostap.

stats conté els paràmetres estadístics capturats per hostap a l'arxiu *stats*. Aquestes estadístiques es refereixen al propi AP. Entre d'altres paràmetres, inclou la variable *TxDeferredTransmissions*

TxDef conté el número d'intents que s'ha d'enviar un paquet, mentre que *Llindar* conté el número d'intents llindar a partir del qual es considera que hi ha present un *jammer*, calculat a partir del temps d'ocupació i d'acord amb la caracterització del canal.

El procés de detecció del *jammer* és el següent:

En primer lloc, es criden les funcions *UpdateMAC* i *UpdateAP*.

La primera obre el fitxer *maclist* i llegeix les dades estadístiques sobre el tràfic de cadascún dels clients associats a l'AP, emmagatzemades a */proc/net/hostap/wlan0/MAC* on MAC és la MAC de cada client. *UpdateAP* fa el mateix amb les dades emmagatzemades a */proc/net/hostap/wlan0/stats*.

Per cada client associat es genera una variable del tipus *sta* i els seus valors s'omplen amb els valors llegits dels fitxers *MAC*. L'estructura *staList* conté la llista de variables *sta* amb els clients associats a l'AP.

A continuació, després d'un temps *t*, es tornen a capturar i es guarden a les mateixes estructures.

Amb aquestes dades i el temps *t* es calculen el *throughput*, la taxa física, la longitud mitjana de paquet i la SNR de cada client.

A continuació, *ComputeTxDef* imprimeix els paràmetres estadístics dels clients a l'arxiu *decisio*, per passar-ho posteriorment a un programa que retorna el temps d'ocupació del canal per tràfic de dades, segons l'algorisme de [9]. Amb les dades de la caracterització del canal obtingudes prèviament obtenim quin és el número d'intents per paquet llindar corresponent al temps d'ocupació.

Posteriorment, després d'haver calculat el nombre d'intents per paquet amb les dades d'*stats* a la funció *ComputeTxDefMeas*, es compara aquest últim amb el nombre d'intents per paquet llindar. En cas que el nombre d'intents per paquet sigui superior al nombre d'intents per paquet llindar, *sendAlarm* alerta de la presència d'un *jammer*.

5.3. Avaluació del sistema

L'aplicació ocupa poca memòria (14 kB) i requereix poca capacitat de procés (menor del 2% de la CPU) de manera que pot ser executat en APs comercials amb capacitats limitades.

Experimentalment s'ha trobat que el *driver* hostap actualiza les dades estadístiques cada 11 segons. Per tant, el temps mínim necessari per detectar la presència d'un *jammer* no pot ésser inferior a aquest valor.

A continuació s'explica la metodologia emprada, l'escenari en què s'ha provat i els resultats obtinguts a l'avaluació.

5.3.1. Metodologia i escenari

L'escenari de les mesures ha estat el soterrani de l'EPSC (veure Figura 5.6), com també ho va ser de les realitzades al Capítol 3.

Les mesures s'han realitzat en unes condicions (modulació i longitud de paquet) favorables a un número d'intents per paquet alt. Aquest fet perjudica l'aplicació avaluada, donat que compara constantment el número d'intents per paquet llindar amb el número d'intents per paquet experimental. Si afavorim l'augment d'aquest últim, estem fent l'avaluació en el pitjor cas possible.

Les proves s'han fet en el sentit de pujada de la transmissió (client → AP), amb un i dos clients. La longitud de paquet emprada és de 1500 bytes i la modulació ha estat la més dèbil, 11 Mbps.

El procés de detecció ha estat el següent:

La distància entre el *jammer* i els dispositius atacats es redueix de cinc en cinc metres des del punt més llunyà possible fins que el programa el detecta. A aquesta distància l'anomenem distància mínima de detecció per un determinat tràfic ofert. Posteriorment es torna a realitzar el mateix procés augmentant aquesta vegada el tràfic ofert.

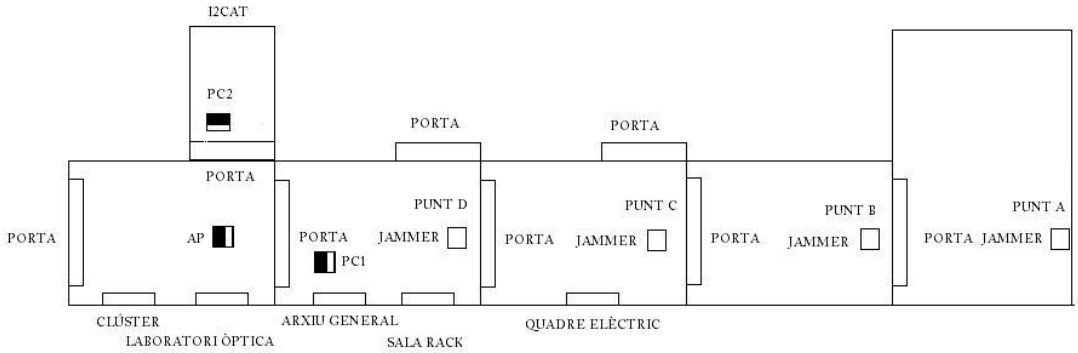


Figura 5.6. Croquis de planta de l'escenari de les mesures.

5.3.2. Resultats

1 client						
Tràfic ofert	**1 Mbps**	**2 Mbps**	**3 Mbps**	**4 Mbps**	**5 Mbps**	**6 Mbps**
Distància mínima de detecció [m]	60	60	60	60	50	50
2 clients						
Tràfic ofert	**1 Mbps**	**2 Mbps**	**3 Mbps**	**4 Mbps**	**5 Mbps**	**6 Mbps**
Distància mínima de detecció [m]	60	60	60	60	50	50

Taula 5.1. Resultats de l'avaluació de l'aplicació.

La distància mínima de detecció és la mateixa tant amb un client com amb dos, tot i que cada client envia la meitat del tràfic en el segon cas.

A mesura que augmenta el tràfic ofert disminueix la distància mínima de detecció. Si el tràfic enviat és molt baix, la influència del *jammer* a l'enllaç és més alta (és a dir, es detecta des de més lluny), en canvi, si el tràfic enviat és

més alt, el detector és menys sensible i no es percata de la presència de l'inhibidor fins que aquest és més a prop.

La Taula 5.1 ens mostra que la distància mínima és constant des d'1 Mbps fins els 4 Mbps, per un i dos clients. Per més de 5 Mbps i fins el màxim teòric de 11 Mbps (que és 6 Mbps) és 50 metres.

5.3.3. Conclusions

Els resultats mostren l'efectivitat del programa desenvolupat en la detecció de *jammers* des d'una distància gran. En el pitjor cas, com a mínim, es pot arribar a detectar quan el *jammer* es troba a 50 metres de la xarxa sense fils.
Al Capítol 3 es va mostrar que el *throughput* no variava més d'un 1,2% en presència d'un inhibidor a 50 metres de l'enllaç emprant una modulació d'11 Mbps. Tot i això, aquesta aplicació és capaç de detectar-lo en aquestes condicions.

Que la detecció es produeixi com a mínim a una distància en què la disminució del *throughput* pel *jammer* és pràcticament imperceptible garanteix que no s'hauran perdut les dades enviades una vegada ja s'hagi detectat l'inhibidor de freqüències.

Per tant, aquesta aplicació ens permet detectar l'atacant alhora que ho fa abans que pugui provocar cap mal a les dades que s'estan transmetent.

CONCLUSIONS

En el desenvolupament d'aquest Treball de Final de Carrera s'han estudiat en profunditat els efectes d'un inhibidor de freqüències sobre un enllaç sense fils. Després d'un seguit de mesures, on s'han detectat els paràmetres més afectats pel mateix, s'ha realitzat el disseny d'una aplicació que, funcionant des de l'AP, és capaç de detectar un *jammer*. Posteriorment, s'ha comprovat la seva efectivitat detectant inhibidors de freqüències a grans distàncies.

Les mesures realitzades per comprovar la influència d'un *jammer* indiquen que aquesta varia principalment en funció de la longitud de paquet, el protocol i la distància.

El *throughput* obtingut, tant sense com amb *jammer*, augmenta si s'incrementa la longitud de paquet. Tot i això, la disminució del *throughput* en presència d'un inhibidor és molt similar per una mateixa modulació per totes les longituds analitzades. Així doncs, tot i que la probabilitat d'error augmenta amb la longitud de paquet, la *Packet Error Rate* (PER) és compensada per un menor *overhead.* A modulacions sensibles, però, aquesta compensació de la PER amb l'*overhead* és molt menor, degut a que la *Packet Error Rate* és més alta a les modulacions sensibles que a les modulacions robustes.

UDP sempre obté un *throughput* superior que TCP, donat que no posseeix ni control d'errors ni control de congestió. Aquest factor, però, tendeix a ser menys important a mesura que la longitud de paquet augmenta, ja que la capçalera, que es manté constant en número de bytes, perd importància vers la longitud total, cosa que disminueix la diferència que hi ha entre el *throughput* obtingut amb UDP i amb TCP.

La distància és, sens dubte, la variable que més afecta a la influència d'un inhibidor de freqüències. Així, la disminució del *throughput* respecte al seu màxim experimental amb un *jammer* a una distància de 5 metres arriba al 99% a 11 Mbps, mentre que a 50 metres només és d'1,2%.

També l'escenari en què es troba l'inhibidor és important per a conèixer la seva influència. En un escenari sense obstacles, la desviació típica del *throughput*, tant sense com amb *jammer*, és superior a la d'un escenari més petit i amb obstacles, donat que el primer és més procliu a la propagació multicamí. Fora d'aquesta, no hi ha cap altra diferència significativa entre els escenaris.

Hi ha diversos paràmetres ràdio que ens poden indicar l'existència d'un atac *jamming* des del punt de vista d'un punt d'accés (AP). Els més significatius són els intents d'enviament per paquet (o la relació entre el nombre d'intents d'enviament fets i el nombre de paquets efectivament enviats) i el nombre de transmissions fora de modulació (o nombre de paquets enviats a una modulació diferent de la modulació per defecte).

En cas que el *jammer* obstrueixi totalment la comunicació i el tràfic tingui origen a l'AP (baixada), el nombre d'intents d'enviaments és molt més alt que sense

jammer. Si el tràfic té com a destinació l'AP (pujada), el paràmetre més significatiu és el nombre de paquets rebuts.
El protocol d'accés al medi, CSMA/CA, impedeix la transmissió per part de dos estacions de forma simultània. Un client no pot transmetre mentre un *jammer* també ho està fent, per tant, si ho intenta, el nombre d'intents d'enviament per paquet d'aquest client augmentarà. Per la seva banda, l'AP rebrà molt pocs paquets i, en conseqüència, l'augment del nombre de paquets rebuts per aquest últim serà molt més baix que en cas que no hi hagués *jammer*.

Si el *jammer* obstrueix parcialment la comunicació els paràmetres més significatius són uns altres. Així, si la modulació és d'11 Mbps hi haurà un nombre molt alt de paquets enviats a modulacions més robustes que si no hi ha un inhibidor present. De la mateixa manera, a la pujada també és el paràmetre que indica millor l'existència d'una obstrucció parcial.

S'ha de tenir en compte que en tot cas hi ha tràfic de baixada, donat que l'AP envia constantment trames *Beacon*, *Probe Responses* i ACKs. Per tant, el nombre d'intents d'enviament per paquet és el paràmetre que indica millor la presència d'un inhibidor de freqüències, tant quan és l'AP qui transmet com quan és el receptor.

L'aplicació programada ha estat desenvolupada a Linux amb C i permet detectar un *jammer* periòdicament. En cas que ho faci, avisa mitjançant un missatge en pantalla.

Per a realitzar la detecció, el programa compara els número d'intents d'enviament per paquet reals amb el número d'intents d'enviament per paquet llindar. Aquest últim nombre s'obté de la caracterització del canal feta anteriorment, que relaciona el percentatge de temps en què el canal està ocupat i el nombre d'intents d'enviament per paquet en condicions normals.

Les proves realitzades per verificar el funcionament de l'aplicació han donat un resultat satisfactori en tots els casos. La distància mínima a partir de la qual es detecta el *jammer* disminueix a mesura que augmenta l'ample de banda enviat. Tot i això, el programa aconsegueix detectar un *jammer* des d'una distància mínima de 50 metres, una distància en què la influència d'aquest en el *throughput* és pràcticament inexistent segons les mesures realitzades.

Impacte ambiental

Les ones electromagnètiques emeses pels dispositius IEEE 802.11 tenen un impacte ambiental molt reduït, donat que compleixen la normativa internacional sobre emissions radioelèctriques i radiacions no ionitzants. El *jammer*, en canvi, excedeix els límits de potència establerts pel CNAF per a la seva banda freqüencial.

D'altra banda, en el desenvolupament de l'aplicació detectora de *jammers* s'han emprat estructures dinàmiques, a fi de minimitzar el cost energètic de l'execució del programa.

Línies d'investigació futura

Tot i l'esforç fet fins ara, encara queda molt de treball per fer al voltant dels inhibidors de freqüències.

Actualment es coneixen tècniques per evitar la influència dels *jammers* que operen a un dels canals de la banda ISM de 2,4 GHz, però no n'hi ha cap quan l'atacant ocupa tot l'ampla de banda.

La localització de l'atacant mitjançant la triangulació del mateix amb diversos APs tampoc està gens desenvolupada, tot i que els coneixements similars en altres àmbits sí que ho estan, com la localització de telèfons mòbils mitjançant estacions base o el sistema de posicionament global GPS mitjançant satèl·lits.

Hi ha xarxes sense fils en què un client té cobertura de més d'un AP. Si un *jammer* té al seu abast un dels seus APs el client només canviarà de punt d'accés en cas que la connexió sigui d'una qualitat molt baixa, però en cas contrari seguirà amb l'AP víctima tot i tenir a l'abast un punt d'accés de molta més qualitat. En aquest cas, l'AP hauria de comunicar als seus clients que està sent objecte d'un atac *jamming*, amb l'objectiu que canviessin de punt d'accés. Aquests mecanismes de control de càrrega no eviten l'atac d'un *jammer*, però sí que podrien minimitzar el seu impacte.

BIBLIOGRAFIA

[1] Cuadro Nacional de Asignación de Frecuencias. Disponible a http://www.mityc.es/NR/rdonlyres/90141458-B3FC-4E12-8E8C-3C13AB45D04B/0/4atribuciones.pdf

[2] E. Bayrataroglu, C. King, X. Liu, G. Noubir, and B. Thapa (2008). "On the Performance of IEEE 802.11 under Jamming", in Proceedings of IEEE Infocom'08

[3] Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function", IEEE Journal on Selected Areas on Communications, vol. 18, no. 3, pp. 535–547, March 2000.

[4] Iperf. Disponible a http://sourceforge.net/projects/iperf/

[5] Jperf. Disponible a http://dast.nlanr.net/projects/jperf/

[6] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proc. 11th Ann. International Conference. Mobile Computing and Networking, ACM Press, 2005, pp. 46–57.

[7] A. D. Wood, J.A. Stankovic, S.H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", Proc. 24th IEEE Intl. Real-Time System Symposium, 2003, pp. 286-297

[8] Hostap. Disponible a http://hostap.epitest.fi/

[9] E. Garcia, D. Viamonte, R. Vidal, and J. Paradells. "Achievable Bandwidth Estimation for Stations in Multi-Rate IEEE 802.11 WLAN Cells". In 8th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM'07, pages 1-8, June 2007.

[10] Vishnu Navda, Aniruddha Bohra, Samrat Ganguly, Dan Rubenstein. "Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks", IEEE INFOCOM Mini-Symposium, 2007, Anchorage, Alaska.

[11] Garcia Villegas, E.; López-Aguilera, E.; Vidal, R.; Paradells, J. "Effect of adjacent channel interference in IEEE 802.11 WLANs", In Proc. of the 2nd Intl. Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom '07), Aug. 2007.

[12] Garcia Villegas, E. "Introducción al futuro estándar IEE 802.11k".

[13] Gast, Matthew S., 802.11 wireless networks the definitive guide. 2nd edition, Beijing: O'Reilly, 2005.

ACRÒNIMS

ACK: *Acknowledgement*
AP: *Access Point*
BSS: *Basic Service Set*
CSMA: *Carrier Sense Multiple Access*
DCF: *Distributed Coordination Function*
DIFS: *Distributed Interframe Space*
IEEE: *The Institute of Electrical and Electronics Engineers*
ISM: *Industrial, Scentific and Medical*
Mbps: Megabits per segon
OSI: *Open System Interconnection*
PCF: *Point Coordination Function*
SINR: *Signal to Interference-plus-Noise Ratio*
SNR: *Signal-to-Noise Ratio*
TCP: *Transmission Control Protocol*
UDP: *User Datagram Protocol*
WLAN: *Wireless Local Area Network*

ANNEXOS

TÍTOL DEL TFC: Detecció d'atacs DoS amb inhibidors de freqüències sobre xarxes IEEE 802.11

TITULACIÓ: Enginyeria Tècnica de Telecomunicació, especialitat en Sistemes de Telecomunicació

AUTOR: Moisés Gómez Díaz

DIRECTOR: Eduard García Villegas

DATA: 11 de Maig de 2009

ANNEX I. Paràmetres del protocol IEEE 802.11

Els següents són els paràmetres amb possibilitat d'ésser especificats durant l'escanneig per part d'un client d'una xarxa sense fils a la qual connectar-se:

- *BSSType*: Especifica la topologia de la xarxa a la qual vol connectar-se (*ad hoc*, infraestructura o qualsevol de les dues).

- *BSSID*: Indica si es vol cercar una estació en concret (individual) o qualsevol estació (*broadcast*). En cas que es triï aquest últim cas, apareixeran totes les estacions que es troben en l'àrea de cobertura de l'estació mòbil.

- *SSID*: Aquest paràmetre és el nom de la xarxa. L'estació mòbil pot cercar una xarxa especificant-ne el seu nom.

- *ScanType*: Hi ha dos tipus d'escanneigs: l'actiu i el passiu. En el primer tipus de cerca l'estació mòbil envia una trama *broadcast* anomenada "*Probe Request*" tot esperant una trama "*Probe Response*" procedent d'un punt d'accés. En el segon tipus l'estació espera únicament trames "*Beacon*" procedents d'un punt d'accés. El principal avantatge que té el mode passiu és que estalvia energia i tràfic.

- *ChannelList*: Aquest paràmetre permet a una estació especificar en quin canal vol escoltar les trames *Beacon*.

- *ProbeDelay*: Indica el temps, en microsegons, que l'estació triga en enviar un *Probe Request*.

- *MinChannelTime* i *MaxChannelTime*: Són el temps mínim i màxim, respectivament, durant el qual l'estació està escannejant un canal.

Els camps d'un *Probe Request* i d'un *Probe Response* són els següents:

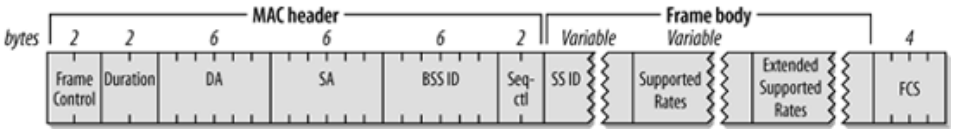


Figura I.1. Camps d'una trama *Probe Request.*

Alguns dels camps més rellevants d'aquesta trama són:

- *BSS ID* (*Basic Service Set Identifier*): Inclou un codi que identifica la xarxa a la qual pertany la trama.
  A les xarxes amb topologia d'infraestructura s'anomena ESS ID (*Extended Service Set Identifier*).

- *Supported Rates*: Indica quines taxes suporta l'estació mòbil. Aquest camp és emprat per les estacions que el reben per decidir si l'estació pot associar-se a la xarxa.

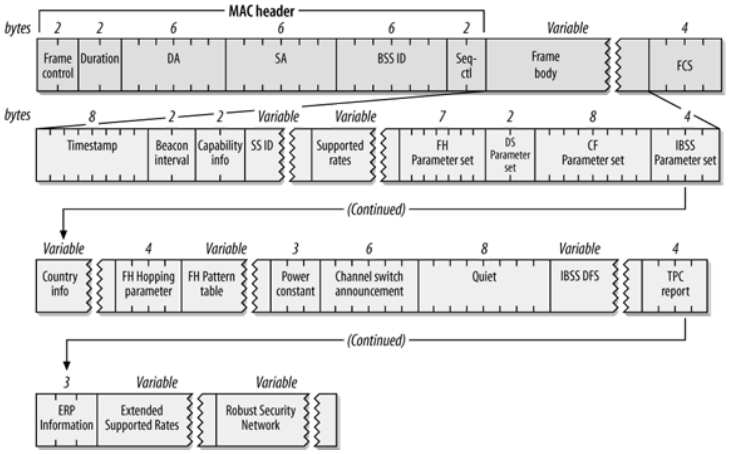


Figura I.2. Camps d'una trama *Probe Response.*

Tot i que no s'ha estès, l'estàndard 802.11h afegeix els següents camps a la trama Probe Response, per a facilitar la gestió de potència i freqüència.

- *Channel switch announcement*: Indica la intenció de l'estació emissora de canviar el canal en què es fa la comunicació a un on les condicions siguin millors.
- *TPC report*: Inclou la potencia transmesa per l'emissor.

ANNEX II. Resultats de les mesures realitzades

A continuació es detallen els resultats de les mesures realitzades.

Throughput	1 Mbps [Kbps]					
	TCP			UDP		
	200 Bytes	900 Bytes	1500 Bytes	200 Bytes	900 Bytes	1500 Bytes
Baixada	465	769	869	537	832	873
Baixada	466	768	824	535	832	859
Pujada	475	773	846	613	843	867
Pujada	475	770	830	615	841	862
Mitjana	**470,31**	**770,64**	**842,52**	**575,65**	**837,39**	**865,82**
Desviació típica	**4,212**	**1,94**	**17,36**	**39,16**	**5,19**	**5,35**
	11 Mbps [Mbps]					
	TCP			UDP		
	200 Bytes	900 Bytes	1500 Bytes	200 Bytes	900 Bytes	1500 Bytes
Baixada	1,71	3,52	5,12	2,42	4,97	5,58
Baixada	1,65	3,34	5,11	2,37	4,95	5,53
Pujada	2,275	4,23	5,53	1,60	5,47	5,90
Pujada	2,31	4,28	5,55	1,60	5,45	5,88
Mitjana	**1,98**	**3,84**	**5,32**	**1,99**	**5,21**	**5,72**
Desviació típica	**0,30**	**0,40**	**0,21**	**0,39**	**0,24**	**0,16**

Taula II.1. Mesures a l'escenari 1 sense jammer.

Throughput	1 Mbps [Kbps]					
	TCP			UDP		
	200 Bytes	900 Bytes	1500 Bytes	200 Bytes	900 Bytes	1500 Bytes
Baixada	433	708	745	522	824	861,53
Baixada	455	726	800	528	826,06	862,54
Pujada	372	740	793	602	830,18	868,6
Pujada	452	743	799	595	832,24	863,55
Mitjana	**428,43**	**729,82**	**784,89**	**562,02**	**828,12**	**864,055**
Desviació típica	**33,31**	**13,93**	**22,82**	**36,70**	**11,3712**	**3,1916**
	11 Mbps [Mbps]					
	TCP			UDP		
	200 Bytes	900 Bytes	1500 Bytes	200 Bytes	900 Bytes	1500 Bytes
Baixada	1,05	1,61	1,65	2,38	4,92	5,36
Baixada	1,10	2,45	4,91	2,20	4,84	5,42
Pujada	1,26	3,96	4,67	1,29	4,05	3,98
Pujada	1,90	3,08	2,80	1,14	3,84	4,72
Mitjana	**1,35**	**2,77**	**3,50**	**1,75**	**4,40**	**4,86**
Desviació típica	**0,36**	**0,85**	**1,34**	**0,58**	**0,46**	**0,57**

Taula II.2. Mesures a l'escenari 1 amb jammer.

	UDP
	5,5 Mbps [Mbps]
Baixada	4,30
Baixada	4,30
Pujada	4,26
Pujada	4,25
Mitjana	4,27
Desviació típica	0,02

Taula II.3. *Throughput* amb una taxa de transmissió de 5,5 Mbps emprant el protocol UDP.

	UDP 1 Mbps [Mbps]		
	5 metres		**10 metres**
	0,043569		0,57268
	0,38316		0,50882
	0,309	**Mitjana**	0,54075
	0,43157	**Desviació típica**	0,03193
	0,49028		
Mitjana	0,3315158		
Desviació típica	0,155759018		
	15 metres		**20 metres**
	0,33372		0,58504
	0,40891		0,65302
	0,37698		0,82606
Mitjana	0,37320333		0,81885
Desviació típica	0,03081213		0,78589
			0,82297
		Mitjana	0,74863833
		Desviació típica	0,09464315
	25 metres		**30 metres**
	0,82915		0,8137
	0,82091		0,81988
	0,82915		0,81988
	0,82606		0,80752
Mitjana	0,8263175	**Mitjana**	0,815245
Desviació típica	0,00336725	**Desviació típica**	0,00512419
	40 metres		**50 metres**
	0,824		0,82503
	0,82709		0,82606
Mitjana	0,825545	**Mitjana**	0,825545
Desviació típica	0,001545	**Desviació típica**	0,000515

Taula I.4. *Throughput* de pujada a 1 Mbps a l'escenari 2.

	UDP 1 Mbps [Mbps]		
	3 metres		**4 metres**
	0,029458		0,11742
Mitjana	0,029458		0,1854
Desviació típica	0		0,21218
		Mitjana	0,171666667
		Desviació típica	0,039885818
	5 metres		**7 metres**
	0,17201		0,4429
	0,103		0,70452
	0,7828		0,70967
	0,13905		0,47689
	0,515		0,4429
	0,55311	**Mitjana**	0,555376
	0,50882	**Desviació típica**	0,12450889
	0,50676		
	0,69937		
	0,69216		
Mitjana	0,467208		
Desviació típica	0,23335318		
	9 metres		**10 metres**
	0,54693		0,76632
	0,55929		0,79207
Mitjana	0,55311		0,73542
Variació	0,00618		0,78177
		Mitjana	0,768895
		Desviació típica	0,02138956
	15 metres		**20 metres**
	0,78177		0,7931
	0,79001		0,80443
Mitjana	0,78589	**Mitjana**	0,798765
Desviació típica	0,00412	**Desviació típica**	0,005665
	25 metres		**30 metres**
	0,81164		0,79928
	0,80855		0,80237
Mitjana	0,810095	**Mitjana**	0,800825
Desviació típica	0,001545	**Desviació típica**	0,001545
	35 metres		
	0,80237		
	0,80649		
Mitjana	0,80443		
Desviació típica	0,00206		

Taula II.5. *Throughput* de baixada a 1 Mbps a l'escenari 2.

	UDP 1 Mbps [Mbps]		
	5 metres		**7 metres**
	0,031827		0,28634
	0		0,31003
Mitjana	0,0159135	**Mitjana**	0,298185
Desviació típica	0,0159135	**Desviació típica**	0,011845
	9 metres		**10 metres**
	0,42127		0,46247
	0,43981		0,64684
Mitjana	0,43054	**Mitjana**	0,554655
Desviació típica	0,00927	**Desviació típica**	0,092185
	15 metres		**20 metres**
	0,78692		1,3905
	0,52118		1,1433
Mitjana	0,65405		0,92494
Desviació típica	0,13287		4,017
			1,648
			2,2454
		Mitjana	1,89485667
		Desviació típica	1,03660203
	25 metres		**30 metres**
	1,2257		4,738
	1,8952		2,1527
Mitjana	1,56045		1,545
Desviació típica	0,33475		4,6041
			4,429
			3,2651
		Mitjana	3,45565
		Desviació típica	1,24467804
	35 metres		**40 metres**
	5,047		5,4693
	5,2015		5,4796
Mitjana	5,12425	**Mitjana**	5,47445
Desviació típica	0,07725	**Desviació típica**	0,00515
	50 metres		
	5,5929		
	5,6135		
Mitjana	5,6032		
Desviació típica	0,0103		

Taula II.6. *Throughput* de pujada a 11 Mbps a l'escenari 2.

	UDP 1 Mbps [Mbps]		
	5 metres		**10 metres**
	0		0
Mitjana	0	**Mitjana**	0
Desviació típica	0	**Desviació típica**	0
	25 metres		**30 metres**
	0		0
Mitjana	0	**Mitjana**	0
Desviació típica	0	**Desviació típica**	0
	35 metres		**40 metres**
	0,8858		5,8504
	1,4626		5,8504
	1,4317		5,7268
Mitjana	1,26003333		4,8925
Desviació típica	0,26492344		5,7062
		Mitjana	5,60526
		Desviació típica	0,36143462
	45 metres		**50 metres**
	5,7783		5,768
	5,6856		5,8504
Mitjana	5,73195	**Mitjana**	5,8092
Desviació típica	0,04635	**Desviació típica**	0,0412

Taula II.7. *Throughput* de baixada a 11 Mbps a l'escenari 2.

	Baixada 1	Baixada 2	Baixada 3	Mitjana	% respecte paquets totals
TxDeferredTransmissions	1581	5507	1506	2864,66667	29,0524323
TxSingleRetryFrames	42	140	13	65	0,659206923
TxMultipleRetryFrames	1	32	3	12	0,12169974
TxRetryLimitExceeded	14	0	4	6	0,06084987
RxFCSErrors	45	54	40	46,3333333	34,40594059
Discarded packets: retry	20	1	6	9	0,091274805
Paquets totals enviats	11047	9553	8981	9860,33333	
Paquets totals rebuts	143	143	118	134,666667	
	Pujada 1	**Pujada 2**	**Pujada 3**	**Mitjana**	
TxDeferredTransmissions	330	597	357	428	10700
TxSingleRetryFrames	0	0	0	0	0
TxMultipleRetryFrames	0	0	0	0	0
TxRetryLimitExceeded	8	5	5	6	150
RxFCSErrors	41	99	21	53,6666667	0,494836489
Discarded packets: retry	12	7	5	8	200
Paquets totals enviats	4	4	4	4	
Paquets totals rebuts	10457	11043	11036	10845,3333	
Amb jammer					
Obstrucció total					
	Baixada 1	**Baixada 2**	**Baixada 3**	**Mitjana**	
TxDeferredTransmissions	100446	94517	109641	101534,667	2065,81214
TxSingleRetryFrames	9	45	37	30,3333333	0,617158359
TxMultipleRetryFrames	0	20	10	10	0,2034588
TxRetryLimitExceeded	756	662	778	732	14,89318413
RxFCSErrors	12	15	15	14	33,33333333
Discarded packets: retry	766	738	856	786,666667	16,00542557
Paquets totals enviats	4908	5695	4142	4915	
Paquets totals rebuts	47	26	53	42	
	Pujada 1	**Pujada 2**	**Pujada 3**	**Mitjana**	
TxDeferredTransmissions	696	707	674	692,333333	13846,66667
TxSingleRetryFrames	0	0	0	0	0
TxMultipleRetryFrames	0	0	0	0	0
TxRetryLimitExceeded	10	3	5	6	120
RxFCSErrors	24	22	19	21,6666667	1,051950154
Discarded packets: retry	15	5	9	9,66666667	193,3333333
Paquets totals enviats	5	5	5	5	
Paquets totals rebuts	649	2957	2573	2059,66667	

Obstrucció parcial					
	Baixada 1	**Baixada 2**	**Baixada 3**	**Mitjana**	
TxDeferredTransmissions	58403	35801	48923	47709	1528,644665
TxSingleRetryFrames	90	158	104	117,333333	3,7594788
TxMultipleRetryFrames	79	70	78	75,6666667	2,424436612
TxRetryLimitExceeded	381	230	328	313	10,02883691
RxFCSErrors	219	172	199	196,666667	76,12903226
Discarded packets: retry	433	396	321	383,333333	12,28238812
Paquets totals enviats	1848	4066	3449	3121	
Paquets totals rebuts	265	240	270	258,333333	
	Pujada 1	**Pujada 2**	**Pujada 3**	**Mitjana**	
TxDeferredTransmissions	1039	732	1276	1015,66667	10882,14286
TxSingleRetryFrames	0	0	0	0	0
TxMultipleRetryFrames	0	0	2	0,66666667	7,142857143
TxRetryLimitExceeded	3	7	6	5,33333333	57,14285714
RxFCSErrors	203	230	138	190,333333	5,256858774
Discarded packets: retry	3	7	3	4,33333333	46,42857143
Paquets totals enviats	3	12	13	9,33333333	
Paquets totals rebuts	2892	4153	3817	3620,66667	
Amb obstacles					
	Baixada 1	**Baixada 2**	**Baixada 3**	**Mitjana**	
TxDeferredTransmissions	439	664	853	652	6,314769976
TxSingleRetryFrames	132	190	234	185,333333	1,794995964
TxMultipleRetryFrames	30	31	55	38,6666667	0,374495561
TxRetryLimitExceeded	6	88	12	35,3333333	0,342211461
RxFCSErrors	34	47	34	38,3333333	29,79274611
Discarded packets: retry	7	88	14	36,3333333	0,351896691
Paquets totals enviats	10756	9563	10656	10325	
Paquets totals rebuts	131	135	120	128,666667	
	Pujada 1	**Pujada 2**	**Pujada 3**	**Mitjana**	
TxDeferredTransmissions	496	502	459	485,666667	12141,66667
TxSingleRetryFrames	0	0	0	0	0
TxMultipleRetryFrames	0	0	0	0	0
TxRetryLimitExceeded	2	5	1	2,66666667	66,66666667
RxFCSErrors	848	1130	866	948	9,622086139
Discarded packets: retry	2	5	2	3	75
Paquets totals enviats	4	4	4	4	
Paquets totals rebuts	9838	9934	9785	9852,33333	

Taula II.8. Paràmetres ràdio de hostap.

Trafic ofert [Mbps]							**Promig**
0,5	8	7	10	24	14	14	12,8333333
1	24	18	25	13	22	59	26,8333333
1,5	31	50	32	47	72	135	61,1666667
2	91,5	63	79	64	91	50	73,0833333
2,5	57	63	51	53	54	52	55
3	65	63	63	61	73	32,5	59,5833333
3,5	70	72	69	59	58	70	66,3333333
4	83	71	26,66	39	44,5	65	54,86
4,5	104	83	85	81	80	77	85

Taula II.9. Transmissions per paquet en pujada a 5,5 Mbps amb 1 client amb una longitud de paquet de 1000 bytes.

Trafic ofert total (suma dels dos clients) [Mbps]							**Promig**
1	49	16	10,5	52	38	35	33,4166667
1,5							
2	107	83	100	38,66	101	57	81,11
2,5							
3	84	39	42,75	25,18	19,33	66,33	46,0983333
3,5							
4	284	299	68,75	42	36	298	171,291667
4,5							
5	376	339	120	50,71	115,5	327	221,368333

Taula II.10. Transmissions per paquet en pujada a 5,5 Mbps amb 2 clients amb una longitud de paquet de 1000 bytes.

Trafic ofert total [Mbps]				Promig
0,1	12	42	28	27,3333333
0,2	32	62	37	43,6666667
0,3	59	42	52	51
0,4	67	79	58	68
0,5	72	76	84	77,3333333
0,6	109	103	100	104
0,7	123	119	128	123,333333
0,8	143	150	87	126,666667

Taula II.11. Transmissions per paquet en pujada a 1 Mbps amb 1 client amb una longitud de paquet de 1000 bytes.

Trafic ofert total (suma dels dos clients) [Mbps]								Promig
0,1	11	13	17					13,6666667
0,2	19	12,5	11,66					14,3866667
0,3	27	30	75	29				40,25
0,4	39	52	89	75	19			54,8
0,5	65	67	49	47	47			55
0,6	55	50	48	79	53	54		56,5
0,7	69	52	51	46	59			55,4
0,8	20,33	57	62	87	54	58	58	56,6185714
0,9	59	25,75	60	54	102	30,66	57	55,4871429

Taula II.12. Transmissions per paquet en pujada a 1 Mbps amb 2 clients amb una longitud de paquet de 1000 bytes.

Trafic ofert [Mbps]							Promig
0,1	13	21	17	14	14	26	17,5
0,2	53	34	18	29	37	25	32,6666667
0,3	42	43	46	44	38	14,66	37,9433333
0,4	51	55	59	73	35	75	58
0,5	28	21,5	20	29,66	33,33	35,66	28,025
0,6	20,28	49,33	48,66	31,5	32	40,25	37,0033333
0,7	41,8	44,25	39,33	38,42	56,75	75,33	49,3133333
0,8	91	184	164	157	86	275	159,5

Taula II.13. Transmissions per paquet en pujada a 1 Mbps amb 1 client amb una longitud de paquet de 1000 bytes.

Trafic ofert total (suma dels dos clients) [Mbps]							Promig
0,1							
0,2	29	31	16	5,14	11	11,66	17,3
0,3							
0,4	109	55	67	101	10,125	10,16	58,7141667
0,5							
0,6	20,66	16,83	34	9,72	9,27	29,66	20,0233333
0,7							
0,8	37,33	29,71	35,25	23,28	335	178	106,428333

Taula II.14. Transmissions per paquet en pujada a 1 Mbps amb 2 clients amb una longitud de paquet de 1000 bytes.

Trafic ofert total (suma dels dos clients) [Kbps]								Promig
100	3,83	3,8	1,85	2,8	2			2,856
200	2,85	9,5	24,66	10	6	15,75	4,5	10,4657143
300	3,18	6,5	4,85	3,33	11,33	6,8	3,44	5,63285714
400	13	7,66	27,5	22	7,83	8,57	5,1	13,0942857
500	31	16,8	11	14,75	11,5	13,75	8	15,2571429
600	5,21	7,44	12	10	7,62	13,25	9,71	9,31857143
700	20	11,83	29,66	11	12,55	9,66	15,66	15,7657143
800	19,83	19	33	16,83	21,75	20,2	19	21,3728571
900	20,8	28	23,6	21	18,25	15	9,41	19,4371429
1000	102	52,33	75,66	144	178	36,66	158	106,664286
1100	23	10,64	26,8	33	25,16	28,2	130	39,5428571
1200	65	111,66	89	32,66	54	37,5	27,42	59,6057143
1300	57,25	230	241	213	220	60	209,5	175,821429
1400	128,33	155	91	210,5	83,33	72,2	103,66	120,574286
1500	297,5	237	196	150,75	484	252,5	139,33	251,011429

Taula II.15. Transmissions per paquet en pujada amb l'AP a 11 Mbps, un client a 1 Mbps i l'altre a 11 Mbps. Longitud de paquet: 1000 bytes.

Trafic ofert [Mbps]				Promig
0,25	8	12	13,33	8,395
0,5	18	14	47	19,875
0,75	27	40	19	21,6875
1	23	25	26	18,75
1,25	45	46	44	34,0625
1,5	51	48	47	36,875
1,75	68	100	58	56,9375
2	138	40,5	107	71,875
2,25	93	114	96	76,3125
2,5	123	121	154	100,125
2,75	179	187	220	147,1875
3	166	178	203	137,5
3,25	241	192	188	156,0625
3,5	250	239	208	175,125
3,75	230	239	249	180,4375
4	269	287	145	176,25
4,25	302	296	290	223,0625
4,5	305	335	347	247,875
4,75	334	341	328	251,9375
5	361	345	368	269,75
5,25	381	382	405	293,3125
5,5	409	385	410	302,375
5,75	473	380	404	315,6875
6	576	567	464	403,25

Taula II.16. Transmissions per paquet en pujada a 11 Mbps amb 1 client amb una longitud de paquet de 500 bytes.

Trafic ofert total (suma dels dos clients) [Mbps]										**Promig**
0,25										
0,5	14,33	11,42	9,62							8,9675
0,75										
1	12,27	17	12,62							10,7225
1,25										
1,5	15,12	29,2	16,75							15,6425
1,75										
2	38,6	29,5	49							29,775
2,25										
2,5	93	147	296							134,625
2,75										
3	137,66	125,33	111							94,2475
3,25										
3,5	127	409	336							218,875
3,75										
4	520	296	390							302,5
4,25										
4,5	383	369	497							313,375
4,75										
5	479	652	504							410
5,25										
5,5	183,75	103,75	631	681	628	290	561	196,75	640	392,075
5,75										
6	545	403	625	255,5	549	397	632	462	470	434,45

Taula II.17. Transmissions per paquet en pujada a 11 Mbps amb 2 clients amb una longitud de paquet de 500 bytes.

ANNEX III. Codi de l'aplicació detectora de *jammers*

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>

#define TEMPS 10
#define MAX 101



/**
 * Tipus de dades amb informació i estadístiques d'una STA associada
 */
typedef struct {
        char mac[18]; //Adreça MAC
      //txB = Bytes tx; rxB = Bytes rx
      //tx1 = pack. enviats a 1 Mbps; etc.
      int tx1, rx1, tx2, rx2, tx5, rx5, tx11, rx11, txB, rxB, rxp,
txp, signal, silence;
      int tx1o, rx1o, tx2o, rx2o, tx5o, rx5o, tx11o, rx11o, txBo,
rxBo, rxpo, txpo;
      double txfm, lm, v;
      int snr;
} sta;

/**
 * Tipus de dades que conte una llista de STAs
 */
typedef struct {
        int size; //Num de STAs associades
        sta **v; // Llista de STAs associades
} staList;

typedef struct {
      int txd, txs, rxfcs, snr, txuo, txmo, txuf, txmf;
      double taxa, lm, txfm;
      int txuoo, txmoo, txufo, txmfo, txdo;
} stats;

staList staL;
stats stat;


/**
  * Retorna la posició d'una MAC
  * @staList: Estructura amb les estadístiques de tots els clients
  * @buffer: String que conté la MAC a trobar
  *
  */
int ismac (staList* s, char* buffer) {
      int i;
      for (i=0; i<s->size; i++) {
            if (strncmp (s->v[i]->mac, buffer, 17) == 0)
                  return i;
      }

      return (-1);
}
```

```
/**
  * Constructor que inicialitza dues variables
  *
  */
int getmacconstructor () {
      staL.v = NULL;
      staL.size = 0;
}

/**
  * Funció que elimina la posició "pos" d'staList
  * @staList: Estructura amb les estadístiques de tots els clients
  * @pos: Posició d'staList a eliminar
  *
  */
int elimina (staList* s, int pos) {

      int z;

      for (z=pos; z<s->size; z++) {
            s->v[z]=s->v[z+1];
      }

      free(s->v[s->size]);
      s->size = s->size--;
}


/**
  * Funció que detecta si un client s'ha desconnectat
  *
  * @staList: Estructura amb les estadístiques de tots els clients
  *
  */
int detectaposicio (staList* s) {

      int i, z;
      char buffer[18];
      FILE* arxiu;

      // Crea el fitxer maclist, on hi haurà les MAC associades

       system("ls /proc/net/hostap/wlan0/ | grep : >
/root/Desktop/maclist");

      if((arxiu=fopen("/root/Desktop/maclist", "r"))==NULL) {
                  perror("Error obrint fitxer maclist");
            return (-1);
      }

      else {
            for (i=0; i<s->size; i++) {

            /*Compara les MAC d'staList amb les de maclist. Si una MAC
no es troba
            a maclist, l'esborra*/

                  z=1;
                  rewind(arxiu);
                  while(fgets(buffer, 18, arxiu)!= NULL) {
```

```
                        buffer[17]='\0';
                        if (strncmp (s->v[i]->mac, buffer, 18) == 0) {
                              z=0;
                        }
                  }
                  if (z==1) {
                        elimina(s, i);
                        i--;
                  }
            }
      }
}

/**
  * Funció que guarda les estadístiques
  * de cada client des de l'arxiu amb el nom
  * de la MAC corresponent
  *
  */
int getmac(void) {

        FILE *fin, *fin2;
        int i=0, j, z;
        char buffer[25], buffer2[80];

      //Es deixen lliures les variables per a dades "actuals"
      //però el seu valor es guarda a les variables per a dades velles
("old")

      for (j=0; j<staL.size; j++) {
            staL.v[j]->tx1o = staL.v[j]->tx1;
            staL.v[j]->rx2o = staL.v[j]->rx2;
            staL.v[j]->tx5o = staL.v[j]->tx5;
            staL.v[j]->tx11o = staL.v[j]->tx11;
            staL.v[j]->txBo = staL.v[j]->txB;
            staL.v[j]->rxBo = staL.v[j]->rxB;
            staL.v[j]->txpo = staL.v[j]->txp;
            staL.v[j]->rxpo = staL.v[j]->rxp;
            staL.v[j]->rx1o = staL.v[j]->rx1;
            staL.v[j]->rx2o = staL.v[j]->rx2;
            staL.v[j]->rx5o = staL.v[j]->rx5;
            staL.v[j]->rx11o = staL.v[j]->rx11;
      }

      // Al fitxer maclist hi ha la llista de MACs associades

     system("ls /proc/net/hostap/wlan0/ | grep : >
/root/Desktop/maclist");

      //Obrim fitxer amb llista de MACs

        if((fin=fopen("/root/Desktop/maclist", "r"))==NULL) {
                perror("Error obrint fitxer maclist");
            return (-1);
        }

      //Llegim dades de cada STA

        while(fgets(buffer, 25, fin)!= NULL) {
            buffer[17]='\0';//conte una MAC de maclist
```

```
            // Si es la primera MAC, o es nova: ampliem memòria

            if (staL.size == 0 || ismac(&staL, buffer) == (-1)) {
                  staL.size++;
                  z = staL.size-1;

                  staL.v = (sta **) realloc(staL.v,
staL.size*sizeof(sta *));
                  staL.v[z] = (sta *)malloc(sizeof(sta));
                  strcpy(staL.v[z]->mac, buffer);
            }

            // Si la MAC de maclist ja està a staL, ismac retorna
            // la posició de MAC a staL.

            if (ismac (&staL, buffer) != (-1)) {
                  z = ismac (&staL, buffer);
            }

            //Concatenem la ruta amb la MAC
            strcpy(buffer2, "/proc/net/hostap/wlan0/");
            strcat(buffer2, buffer);

            //Obrim les estadístiques del client

            if((fin2=fopen(buffer2, "r"))==NULL) {
                  perror("Error obrint fitxer MAC");
                  return (-1);
            }

            //Llegim les estadístiques i guardem a la sta corresponent

            while(fgets(buffer2, 80, fin2)!= NULL) {
                  if(strncmp("rx_bytes", buffer2, 8)==0)
                        sscanf(buffer2, "rx_bytes=%d", &(staL.v[z]-
>rxB));
                  if(strncmp("tx_bytes", buffer2, 8)==0)
                        sscanf(buffer2, "tx_bytes=%d", &(staL.v[z]-
>txB));
                  if(strncmp("tx[1M]", buffer2, 6)==0)
                        sscanf(buffer2, "tx[1M]=%d", &(staL.v[z]-
>tx1));
                  if(strncmp("tx[2M]", buffer2, 6)==0)
                        sscanf(buffer2, "tx[2M]=%d", &(staL.v[z]-
>tx2));
                  if(strncmp("tx[5.5", buffer2, 6)==0)
                        sscanf(buffer2, "tx[5.5M]=%d", &(staL.v[z]-
>tx5));
                  if(strncmp("tx[11M", buffer2, 6)==0)
                        sscanf(buffer2, "tx[11M]=%d", &(staL.v[z]-
>tx11));
                  if(strncmp("rx[1M]", buffer2, 6)==0)
                        sscanf(buffer2, "rx[1M]=%d", &(staL.v[z]-
>rx1));
                  if(strncmp("rx[2M]", buffer2, 6)==0)
                        sscanf(buffer2, "rx[2M]=%d", &(staL.v[z]-
>rx2));
                  if(strncmp("rx[5.5", buffer2, 6)==0)
                        sscanf(buffer2, "rx[5.5M]=%d", &(staL.v[z]-
>rx5));
                  if(strncmp("rx[11M", buffer2, 6)==0)
```

```
                        sscanf(buffer2, "rx[11M]=%d", &(staL.v[z]-
>rx11));
                  if(strncmp("tx_packets", buffer2, 10)==0)
                        sscanf(buffer2, "tx_packets=%d", &(staL.v[z]-
>txp));
                  if(strncmp("last_rx: silence=-100 dBm signal",
buffer2, 16)==0)
                        sscanf(buffer2, "last_rx: silence=-100 dBm
signal=%d", &(staL.v[z]->signal));
                  if(strncmp("last_rx: silence", buffer2, 16)==0)
                        sscanf(buffer2, "last_rx: silence=%d",
&(staL.v[z]->silence));
                  if(strncmp("rx_packets", buffer2, 10)==0)
                        sscanf(buffer2, "rx_packets=%d", &(staL.v[z]-
>rxp));
            }
            fclose(fin2); //Fitxer de MAC
        }
        fclose(fin); //Fitxer maclist

      return;


}

/**
  * Funció que llegeix i guarda estadístiques
  * del fitxer "stats"
  *
  */
int getstats ()
{
      int j=0;
      char buffer[80];
      FILE *fitx;

      //Els paràmetres actuals es guarden a una variable de
      //paràmetres antics (old)

      stat.txdo = stat.txd;
      stat.txuoo = stat.txuo;
      stat.txmoo = stat.txmo;
      stat.txufo = stat.txuf;
      stat.txmfo = stat.txmf;

      fitx=fopen("/proc/net/hostap/wlan0/stats", "r");

      if (fitx==NULL)   {
            perror("Error obrint el fitxer stats\n");
            return (-1);
      }
      else  {
            while(fgets(buffer, 40, fitx)!=NULL) {

                  //Es guarden estadístiques del fitxer "stats"

                  if(strncmp("TxUnicastFrames", buffer, 15)==0)
                        sscanf(buffer, "TxUnicastFrames=%d",
&stat.txuf);
                  if(strncmp("TxMulticastframes", buffer, 17)==0)
```

```
                        sscanf(buffer, "TxMulticastframes=%d",
&stat.txmf);
                  if(strncmp("TxUnicastOctets", buffer, 15)==0)
                        sscanf(buffer, "TxUnicastOctets=%d",
&stat.txuo);
                  if(strncmp("TxMulticastOctets", buffer, 17)==0)
                        sscanf(buffer, "TxMulticastOctets=%d",
&stat.txmo);
                  if(strncmp("TxDeferredTransmissions", buffer, 23)==0)
                        sscanf(buffer, "TxDeferredTransmissions=%d",
&(stat.txd));
                  if(strncmp("TxSingleRetryFrames", buffer, 19)==0)
                        sscanf(buffer, "TxSingleRetryFrames=%d",
&stat.txs);
                  if(strncmp("RxFCSErrors", buffer, 11)==0)
                        sscanf(buffer, "RxFCSErrors=%d", &stat.rxfcs);

            }
      }

      fclose(fitx);

      return 0;
}

/**
  * Funció que retorna el número de transmissions
  * per paquet en funció de la ocupació del canal
  *
  * @ocupacio: Enter amb la ocupació del canal.
  *
  */

double grafica (int ocupacio) {

      double v_ocupacio[MAX];

      v_ocupacio[5] =  20.0;
      v_ocupacio[10] = 25.0;
      v_ocupacio[15] = 34.3;
      v_ocupacio[20] = 40.6;
      v_ocupacio[25] = 45.1;
      v_ocupacio[30] = 51.1;
      v_ocupacio[35] = 56.7;
      v_ocupacio[40] = 75.6;
      v_ocupacio[45] = 93.1;
      v_ocupacio[50] = 110.0;
      v_ocupacio[55] = 120.0;
      v_ocupacio[60] = 170.1;
      v_ocupacio[65] = 212.1;
      v_ocupacio[70] = 380.8;
      v_ocupacio[75] = 550.0;
      v_ocupacio[80] = 600.0;
      v_ocupacio[85] = 600.0;
      v_ocupacio[90] = 600.0;
      v_ocupacio[95] = 600.0;
      v_ocupacio[100] = 600.0;

      return v_ocupacio[ocupacio];

}
```

```
/**
  * Funció que determina si hi ha un jammer present.
  *
  */

int deteccio_jammer() {

      int i, ocupacioint;
      float ocupacio, paquetstotals=0.00;
      char buffer[40];
      double txfm = 0.0, intentspkt=0.0, txdef;
      FILE* arxiu2;
      FILE* arxiu3;


      //Es crida al constructor que inicialitza les variables
      getmacconstructor();

      //Es llegeixen i guarden les estadístiques dels clients
      getmac();

      //Es llegeixen i guarden les estadístiques de l'arxiu "stats"
      getstats();

      //Si un client s'ha desconnectat, s'esborren les seves dades
      detectaposicio(&staL);


      for (i=0; i<staL.size;i++) {

            sleep(TEMPS);

            /*Es tornen a llegir les estadístiques de cada client i de
l'arxiu "stats".
            Amb aquesta segona lectura, i tenint en compte la primera i
el temps entre
            les dues preses, es calculen els valors de la velocitat,
taxa física, longitud
            mitjana i SNR*/

            getmac();
            getstats();

            /*Dades de cada client*/
            //Velocitat en kps
            staL.v[i]->v=(double)((staL.v[i]->rxB)-(staL.v[i]-
>rxBo))*8/(TEMPS*1000);

            //Taxa física mitjana en kbps
            staL.v[i]->txfm = 1000.0*(double)((staL.v[i]->rx1 -
staL.v[i]->rx1o) * 1 + (staL.v[i]->rx2 - staL.v[i]->rx2o) * 2 +
(staL.v[i]->rx5 - staL.v[i]->rx5o) * 5 + (staL.v[i]->rx11 + 1 -
staL.v[i]->rx11o) * 11)/ (double)(staL.v[i]->rxp +1 - staL.v[i]-
>rxpo);

            //Longitud mitjana. Se suma 1 per evitar que lm sigui
infinit.
            staL.v[i]->lm = (double)((staL.v[i]->rxB) - (staL.v[i]-
>rxBo))/(double)((staL.v[i]->rxp)-(staL.v[i]->rxpo)+1);
```

```
            //SNR
            staL.v[i]->snr = (staL.v[i]->signal) - (staL.v[i]-
>silence);
            }

            if((arxiu2=fopen("/root/Desktop/decisio", "w"))==NULL) {
                  perror("Error escribint al fitxer de decisio");
            return (-1);
      }
      else {
            //Impressió de les dades de cada client
            for (i=0; i<staL.size; i++) {
                  fprintf (arxiu2, "%f %d %f %f\n", staL.v[i]->txfm,
staL.v[i]->snr, staL.v[i]->lm, staL.v[i]->v);
            }

      }
      fclose(arxiu2);

      //Es passa l'arxiu "decisio" a "Executable"  i es copia el valor
de la
      //ocupació del canal a l'arxiu "tmp"

      system("/root/Desktop/Executable decisio | grep L | cut -d\" \"
-f 3 > tmp");


      if((arxiu3=fopen("/root/Desktop/tmp", "r"))==NULL) {
                  perror("Error llegint el fitxer tmp");
            return (-1);
      }
      else {
                  fscanf(arxiu3, "%f", &ocupacio);
      }

      fclose(arxiu3);

      /*S'arrodoneix a l'alça al múltiple de 5 més pròxim el valor de
la ocupació del canal*/

      ocupacioint = (int) ocupacio;

      if (ocupacioint % 5 < 0)
            ocupacioint = 5;
      else if (ocupacioint % 5 == 0)
            ocupacioint = (int) ocupacio + 5;
      else if (ocupacioint % 5 == 1)
            ocupacioint = (int) ocupacio + 4;
      else if (ocupacioint % 5 == 2)
            ocupacioint = (int) ocupacio + 3;
      else if (ocupacioint % 5 == 3)
            ocupacioint = (int) ocupacio + 2;
      else if (ocupacioint % 5 == 4)
            ocupacioint = (int) ocupacio + 1;
      else {
            printf ("El valor de la ocupació del canal no es pot
aproximar\n");
            return (-1);
      }
```

```
      //S'obté el número d'intents per paquet llindar a partir de la
ocupació del canal
      txdef = grafica(ocupacioint);

      //Intents de transmissió per paquet al canal segons les
estadístiques de hostap
      intentspkt = 1.0 + (double)(stat.txd -
stat.txdo)/(double)(stat.txmf-stat.txmfo+stat.txuf-stat.txufo+1);


       for (i=0; i<staL.size; i++) {
            printf("--------Client %d\n", i);
            printf("MAC: %s\n-----Recepció: Modulació: %f Kbps, Tràfic
ofert: %f Kbps, SNR: %d dB, Mida paquet: %f bytes\n", staL.v[i]->mac,
staL.v[i]->txfm, staL.v[i]->v, staL.v[i]->snr, staL.v[i]->lm);
      }
      printf("-----Transmissió: Modulació: %f Kbps, Tràfic ofert: %f
Kbps, SNR: %d dB, Mida paquet: %f bytes\n", stat.txfm, stat.taxa,
stat.snr, stat.lm);
      printf ("Temps d'ocupació del canal: %f%, Intents per paquet:
%f, Intents per paquet llindar: %f\n", ocupacio, intentspkt, txdef);

      /*Si el número de transmissions per paquet del canal és superior
al número de transmissions per paquet
      llindar, hi ha jammer. En cas contrari, no n'hi ha*/

      if (intentspkt > txdef)
            printf ("Hi ha jammer\n");
      else
            printf ("No hi ha jammer\n");
}

/**
  * Main del programa, on s'executa la funció
  * que detecta la presència d'un jammer
  */
int main(int argc, char *argv[])
{
      int i=0;

      /*S'executa la funció deteccio_jammer() indefinidament
      a fi de detectar l'existència d'un jammer*/

      for (;;) {
      deteccio_jammer();


      //Alliberem la memòria
      for(i=0; i<staL.size; i++)
            free(staL.v[i]);

      free(staL.v);
      }
      return;
}
```