UNIVERSITA' DEGLI STUDI DI PISA

FACOLTA' DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Specialistica in Tecnologie Informatiche

Analisi qualitativa di reti wifi attraverso l'individuazione di parametri significativi e la rilevazione dello spostamento degli utenti

Relatore:

Prof. Luca Deri

Prof. Maurizio Bonuccelli

Controrelatore:

Prof.ssa Laura Ricci

Tesi di Laurea di:

Davide Marini

Matr. N. 237298

Anno Accademico 2007/2008

....

Indice

Elenco delle figure

Elenco delle tabelle

Abstract

.....

Capitolo 1

Introduzione

La tecnologia WIFI si sta diffondendo rapidamente in ogni ambito lavorativo e si stima che nell'arco del prossimo decennio tutti i dispositivi IT saranno dotati di una qualche capacità Wireless. Aziende e privati hanno accolto questa tecnologia con entusiasmo e stanno iniziando a utilizzarla per le applicazioni più svariate; ad esempio, in edifici di vecchia costruzione e in tutte le situazioni dove può essere difficoltoso, dispendioso o impossibile installare i cavi come aeroporti, locali pubblici, grandi magazzini, ecc.. Il continuo sviluppo tecnologico ha aumentato l'interesse per queste reti e le ha rese competitive rispetto alle reti tradizionali, rappresentando di fatto il futuro delle reti locali e garantendo una maggiore flessibilità e portabilità dei sistemi all'interno delle reti aziendali e domestiche.

Tali tecnologie sono, inoltre, particolarmente adatte per consentire a computer portatili di connettersi a una rete locale, aumentando la mobilità dell'utente e di conseguenza la sua produttività. Le reti wireless sono molto semplici, rapide da installare ed utilizzare, e apportano benefici immediati.

Oramai questa tecnologia è la chiave per raggiungere l'*Internet everywhere*, l'Internet ovunque, che è una delle premesse per arrivare a una *società dell'informazione*, nella quale le informazioni sono ovunque, disponibili rapidamente e a un costo minimo. In questa ottica si può pensare anche ad applicazioni non immaginabili sino a ieri. All'estero ed in certe realtà anche nel nostro paese, ad esempio, molte amministrazioni locali hanno provveduto ad attrezzare con il Wi-fi le piazze più frequentate, i parchi ed altri luoghi pubblici, diffondendo quello che viene chiamato *Hot Spot*.

Di conseguenza, questa rapida e capillare diffusione delle reti Wireless ha di fatto generato la necessità, da parte degli amministratori di rete, di monitorarne l'utilizzo per offrire servizi efficienti, in termini di affidabilità e velocità di connessione, ad un numero sempre più crescente di utenti.

Attualmente, il monitoraggio di reti WIFI è sostanzialmente rivolto alla identificazione di reti e alla cattura ed analisi dell'intero traffico via etere, mediante tecniche passive. A tale scopo, le principali informazioni base raccolte sono:

- Nome della Rete (Wireless Network Name - SSID)
- Numero canale
- Intensità segnale
- Tipo encription
- Tipo di rete
- Numero pacchetti

Tali informazioni sono contenute in *pacchetti* che, talvolta, sono i*nteramente* catturati e resi disponibili per possibili analisi.

La tesi discute il problema nei suoi aspetti tecnici e propone uno studio per il monitoraggio *informativo* e *qualitativo* di una rete WIFI, costituitia da almeno due Access Point (AP), ponendosi una serie di obiettivi, sia sul piano degli approfondimenti teorici che su quello di proposte realizzative.

1.1 Obiettivi prefissati

Gli obiettivi che il presente lavoro si è prefissato sono molteplici:

- precisare il concetto di *qualità* di una rete WIFI, oltre alla naturale rispondenza agli standard previsti
- individuare i parametri significativi e le loro correlazioni per valutare tale idea di qualità
- fornire un approccio metodologico e proporre uno strumento di Amministrazione per
  - ottimizzare l'utilizzo delle risorse della rete
  - migliorare e/o preservare nel tempo le prestazioni della rete
  - rispondere in maniera efficace a cambiamenti intervenuti nella "geografia" della rete medesima

mediante soluzioni generate da algoritmi dedicati alla elaborazione degli specifici parametri qualitativi individuati.

1.2 Caratteristiche principali

Allo scopo del raggiungimento degli obiettivi prefissati (in particolar modo di quello inerente la salvaguardia degli aspetti prestazionali di una rete wifi) si è privilegiato l'approfondimento della tematica relativa alla rilevazione degli spostamenti dell'utente, rivelatisi specificatamente significativi per valutare le necessità di riconfigurazione della rete.

L'individuazione delle informazione "Livello del Segnale", così come "Numero del Canale" in termini di frequenza e "Allocazione del Canale" in termini di banda da rendere disponibile agli Utenti e la loro analisi concorrono ad effettuare tale valutazione, attraverso uno strumento di supporto decisionale per l'Amministratore della rete.

La progettazione di questo strumento, pur sostanzialmente non sfociata in una sua completa realizzazione, ci pare costituisca un apporto utile allo sviluppo della tematica della Gestione di reti WIFI, costituendo un primo passo nella direzione di un approccio non solo teorico alla materia.

1.3 Organizzazione del documento

Il presente documento è articolato come segue:

- il **Capitolo 1** introduce brevemente la tecnologia WIFI ed esplicita gli obiettivi prefissati nonchè la peculiarità del lavoro effettuato;
- il **Capitolo 2** riguarda la descrizione teorica dello standard IEEE 802.11 utilizzato per la comunicazione WIFI;

- il **Capitolo 3** precisa il concetto di qualità nelle reti WIFI, discute brevemente la rilevanza dei principali parametri e grandezze significative utili per l'analisi e descrive l'applicazione che rileva tali informazioni;

- il **Capitolo 4** approfondisce la discussione sui parametri significativi "Numero Canale" e "Allocazione del Canale", evidenziando le motivazioni delle scelte compiute; descrive le analisi effettuate sui dati forniti dai test, traendone opportune conclusioni e confrontando tali risultati con quelli attesi; inoltre, discute un possibile studio sull'utilizzo "commerciale" della banda del canale;

- il **Capitolo 5** approfondisce il tema della rilevazione dello spostamento degli utenti, giustificandone l'importanza e proponendo un algoritmo adatto a tale scopo; è descritta la relativa applicazione software;

- il **Capitolo 6** descrive in maniera completa l'ambiente di test, realizzato ad-hoc, per dimostrare la fattibilità dell'algoritmo di rilevazione dello spostamento degli utenti proposto e per visualizzare i parametri significativi discussi al capitolo 3;

- il **Capitolo 7** Conclusioni e possibili sviluppi futuri ipotizzabili

Capitolo 2

IEEE 802.11 : Lo Standard

2.1 Introduzione

Il wireless ha iniziato a diffondersi negli anni 80, quando l'idea di condividere dati tra computer diventava indispensabile. La prima tecnologia utilizzata fu quella dei ricetrasmettitori a raggi infrarossi che a causa della grave limitazione dei raggi nell'attraversare la maggior parte dei materiali, non ebbe un grande sviluppo. Il mercato richiedeva una tecnologia pulita, con la possibilità di attraversare ostacoli, da poter essere utilizzata in qualsiasi ambiente di lavoro. Nacque così una tecnologia wireless basata su segnale radio che incominciò a prendere piede negli inizi degli anni '90, quando la capacità di calcolo dei processori risultò sufficiente a gestire la ricetrasmissione via radio.Una prima implementazione che si creò si dimostrò costosa e di proprietà e non permetteva di comunicare con nessun altro sistema, difatti le reti non compatibili si dimostrarono un fallimento.

A quel punto l'attenzione si focalizzò sul neonato standard creato dagli

esperti volontari IEEE (Institute of Electrical and Electronics Engineers) [1] appunto l'802.11. Lo scopo iniziale di questo progetto era quello di creare uno standard globale per reti operanti in una banda libera senza la necessità di utilizzare alcuna licenza.

2.2 WLAN Contesto e motivazioni

Con il termine "WLAN" (Wireless Local Area Network) si indica un sistema di comunicazione tra apparecchiature elettroniche che utilizza onde-radio al posto delle tradizionali infrastrutture di cavi "cablati". Solitamente, dove questo sistema è utilizzato, rappresenta l'ultimo anello di congiunzione fra "la rete" e l'utente finale. Di conseguenza possiamo vedere come un'infrastruttura di tipo "Wireless" ed una di tipo "Wired" (cablata) possano coesistere nella stessa rete senza problemi; anzi, questo è addirittura consigliato, in quanto si può in tal modo beneficiare dei vantaggi che i due sistemi possono portare. Inoltre, la possibilità di utilizzare una WLAN diventa essenziale in quegli ambienti dove è impraticabile, per diversi motivi, l'implementazione di una tradizionale rete cablata. Ad esempio per questioni di costi, o, ancora, per motivi di non-intrusione in un eco-sistema preesistente.

Nella presente trattazione ci si soffermerà sulle caratteristiche del protocollo 802.11 [2][3], base dell'implementazione delle reti WLAN, standardizzato a livello internazionale dall'IEEE e presente in diverse tipologie, ad esempio lo standard 802.11b, che permette velocità massime di 11Mbps.L'aderenza dei vari prodotti commerciali al protocollo, nonché gli argomenti non trattati dallo standard, infine, sono discussi da un consorzio di produttori di reti

WLAN nel WECA: "Wireless Ethernet Compatibility Alliance" [4], con altresì lo scopo di certificare e garantire l'interoperabilità fra apparecchiature di diversi produttori. Lo "step" finale del lavoro di questo consorzio è la certificazione di un apparato come "Wi-Fi" (Wireless Fidelty) [5].

2.3 Componenti dell'architettura 802.11

Una 802.11 WLAN è basata su una architettura cellulare in cui l'area dove deve essere distribuito il servizio viene suddivisa in celle proprio come accade nei sistemi di distribuzione per servizi di telefonia GSM[6]. Ciascuna cella (chiamata Basic Service Set o BSS nella nomenclatura) è controllata da una stazione base denominata Access Point, o più semplicemente AP.

Gli AP sono bridge che collegano la sottorete wireless con quella cablata, mentre i Device Mobile(DM) sono i dispositivi che usufruiscono dei servizi di rete. Gli AP possono essere implementati in hardware (dispositivi dedicati), ma anche in software, appoggiandosi, ad esempio, ad un PC o notebook, dotato sia dell'interfaccia wireless, sia di una scheda Ethernet. I DM possono essere di qualunque tipo: notebook, palmari, PDA, cellulari, apparecchi che interfacciano standard IEEE 802.11. Vediamo di seguito un esempio di sistema:

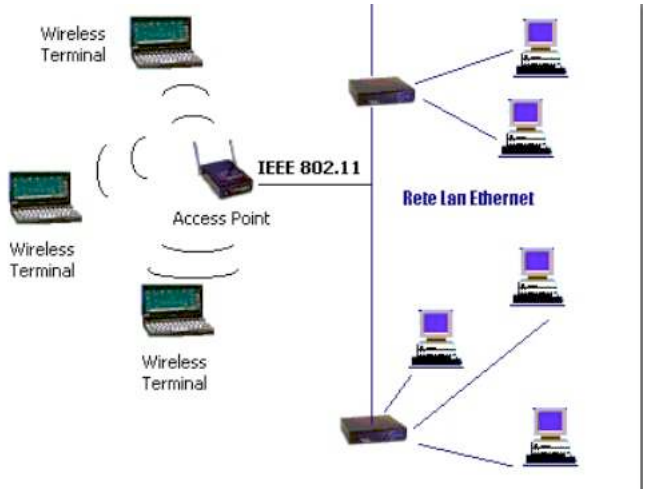

Figura 2.1: Una esempio di WLAN

Il primo modo di funzionamento che vediamo, sebbene di scarso utilizzo pratico, è il cosiddetto ad-hoc mode (o Indipendent Basic Service Set: IBSS) , nel quale non esistono AP e ciascun terminale mobile DM comunica con gli altri senza un controllo centralizzato. Una struttura di tal genere, peer-to-peer, è però utile solo per situazioni temporanee in quanto si perde la possibilità di connettersi ad una rete Wired, ed inoltre le distanze fra i vari DM devono essere ridotte per avere velocità di comunicazione efficienti.

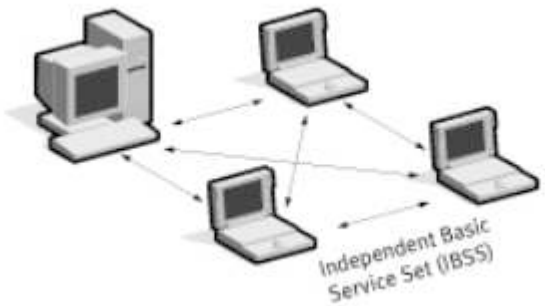

Figura 2.2: WLAN 802.11 in configurazione ad-hoc

Per quanto riguarda i modi di funzionamento mediante l'uso di una infrastruttura, sebbene una WLAN possa essere formata da una singola cella, con un singolo AP, la maggior parte delle installazioni sarà formata da una molteplicità di celle dove i singoli AP sono interconnessi attraverso un qualche tipo di rete di distribuzione (che normalmente viene definita Distribution System o DS). La rete di distribuzione è normalmente costituita da una dorsale Ethernet e in certi casi è wireless essa stessa. In tali casi i terminali DM sono programmati in modo "managed", in modo cioè da vedere solo gli AP, e non gli altri terminali. Saranno poi gli AP che permetteranno la comunicazione fra i diversi dispositivi.

Il complesso delle diverse WLAN interconnesse, comprendenti differenti celle, i relativi AP e il sistema di distribuzione, viene visto come una singola rete 802 dai livelli superiori del modello OSI ed è noto nello standard come Extended Service Set (ESS). In figura 1.3 è mostrato lo schema di una tipica rete WLAN basata sul protocollo 802.11 comprendente i componenti descritti sopra.

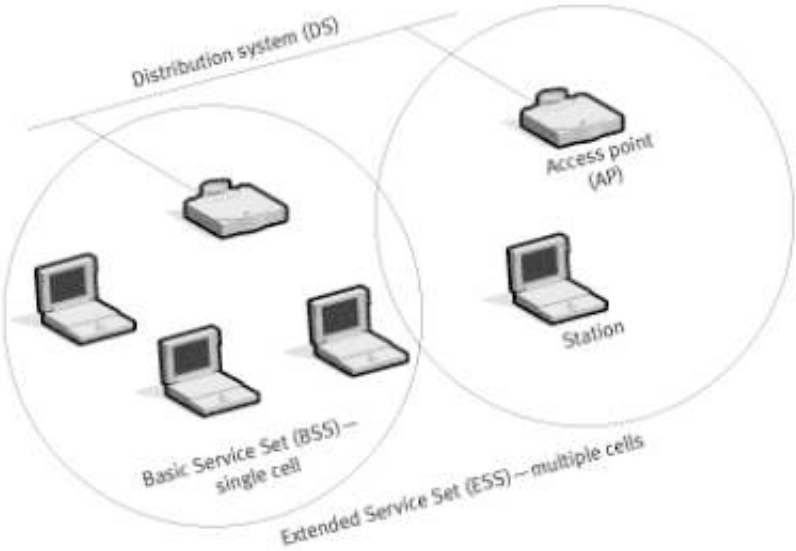

Figura 2.3: Una tipicaWLAN 802.11

Ovviamente il numero e la disposizione degli AP è di cruciale importanza al fine di ottenere, infine, una rete perfettamente funzionante e performante. Un planning per la progettazione delle celle è indispensabile, e, soprattutto, è dipendente dallo specifico ambiente in cui la rete deve essere collocata. Questo a causa del mezzo trasmissivo utilizzato (onde radio) sensibili a pareti, sorgenti elettromagnetiche, ostacoli in genere. Un periodo di set-up è quindi praticamente indispensabile.

2.4 Descrizione degli strati dell'IEEE 802 e 802.11

Lo standard 802.11 è afferente alla famiglia di standard 802.x [7], che consiste in una "suite" di protocolli utilizzati in contesti diversi ma tutti rivolti alla standardizzazione delle reti locali LAN e metropolitane MAN. Questa fami-

glia di standard è basata, o meglio, implementa, i livelli di "Physical Layer" e "Data Link Layer" del modello ISO/OSI [SNMP1], come è possibile notare dalla seguente figura:

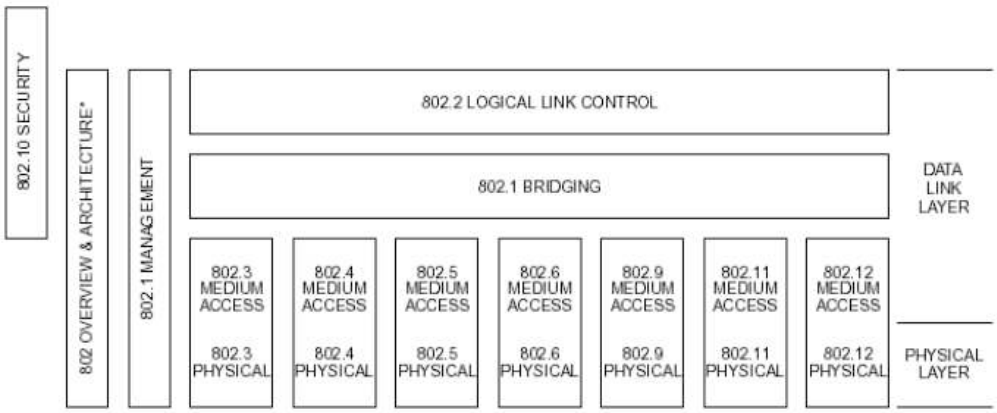

Figura 2.4: Insieme degli standard 802.x

In generale, parlando dello standard 802.11x, le specifiche definiscono un singolo livello MAC che può interagire con i seguenti tre livelli fisici PHY (vedi figura 1.6), operanti a velocità variabili:

- *Frequency Hopping Spread Spectrum* (FHSS) nella banda ISM 2,4GHz;
- *Direct Sequence Spread Spectrum* (DSSS) nella banda ISM 2,4GHz;
- Trasmissione infrarossa (IR).

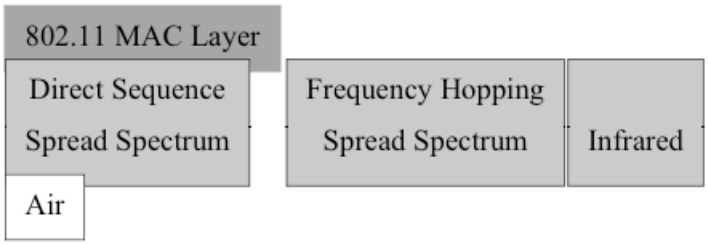

Figura 2.5: Stack IEEE 802.11

Rispetto al modello di riferimento delle reti ISO/OSI, la posizione all'interno di essa del protocollo in esame è la seguente:

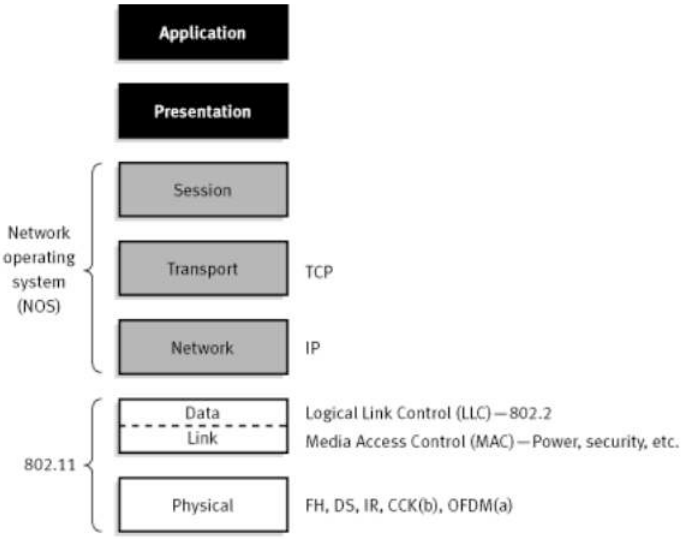

Figura 2.6: modello di riferimento ISO/OSI e collocazione del protocollo 802.11

Oltre alle funzionalità standard usualmente fornite dai livelli di MAC dei protocolli 802.x, il MAC 802.11 supporta delle funzionalità aggiuntive, tipiche dei livelli superiori dello stack protocollare, come la gestione della frammentazione delle Protocol Data Unit, la ritrasmissione dei pacchetti e la gestione dell'acknowledge.

2.4.1 Rassegna degli standard 802.11

IEEE 802.11 o Wi-Fi definisce uno standard per le reti WLAN sviluppato dal gruppo dell' IEEE 802.11 Questo termine viene usualmente utilizzato per

definire la prima serie di apparecchiature 802.11 sebbene si debba preferire il termine 802.11 legacy. Questa famiglia di protocolli include tre protocolli dedicati alla trasmissione delle informazioni (a, b, g) mentre la sicurezza è stata inclusa in uno standard a parte l'802.11i. Gli altri standard della famiglia (per esempio c, d, e, f, h) riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Il primo protocollo largamente diffuso è stato il *b*; in seguito si sono diffusi il protocollo *a* e soprattutto il protocollo *g*. L' 802.11b e 802.11g utilizzano lo spettro di frequenze libero da licenze nella banda dei 2.4 Ghz. L' 802.11a utilizza la banda di frequenze di 5 Ghz. Operando in bande di frequenze libere, i dispositivi b e g, possono essere influenzati da telefoni cordless, trasmettitori mobili e in genere da tutti gli apparecchi che utilizzano quella banda di frequenze.

2.4.1.1 802.11 Legacy

La prima versione dello standard 802.11 venne presentata nel 1997 e viene chiamata 802.1y, specificava velocità di trasferimento comprese tra 1 e 2 Mbit/s e utilizzava i raggi infrarossi o le onde radio nella frequenza di 2.4 Ghz per la trasmissione del segnale. La trasmissione infrarosso venne eliminata dalle versioni successive dato lo scarso successo. La maggior parte dei costruttori infatti non aveva optato per lo standard IrDA, preferendo la trasmissione radio. Il supporto di questo standard per quanto riguarda la trasmissione via infrarossi è incluso nelle evoluzioni dello standard 802.11 per ragioni di compatibilità. Poco dopo questo standard vennero introdotte da due produttori indipendenti delle evoluzioni dello standard 802.1y che una volta riunite e migliorate portarono alla definizione dello standard 802.11b

2.4.1.2 802.11b

802.11b, approvato nel 1999, ha la capacità di trasmettere al massimo 11Mbit/s e utilizza il CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess con **C**ollision **A**voidance) come metodo di trasmissione delle informazioni. Una buona parte della banda disponibile viene utilizzata dal CSMA/CA. In pratica il massimo trasferimento ottenibile è di 5.9 Mbit/s in TCP e di 7.1 Mbit/s in UDP. Metallo, acqua e in generale ostacoli solidi riducono drasticamente la portata del segnale. Il protocollo utilizza le frequenze nell'intorno dei 2.4Ghz. Utilizzando antenne esterne dotate di alto guadagno si è in grado di stabilire delle connessioni punto a punto del raggio di molti chilometri. Utilizzando ricevitori con guadagno di 80 decibel si può arrivare a 8 chilometri o se le condizioni del tempo sono favorevoli anche a distanze maggiori ma sono situazioni temporanee che non consentono una copertura affidabile. Quando il segnale è troppo disturbato o debole lo standard prevede di ridurre la velocità massima a 5.5, 2 o 1 Mbit/s per consentire al segnale di essere decodificato correttamente. Sono state sviluppate delle estensioni proprietarie che utilizzando più canali accoppiati consentono di incrementare la velocità di trasmissione a scapito della compatibilità con le periferiche prodotte dagli altri produttori. Queste estensioni normalmente vengono chiamate 802.11b+ e portano la banda teorica a 22, 33 o addirittura a 44 Mbit/s. Il primo produttore commerciale a utilizzare il protocollo 802.11b è stata Apple Computer con il marchio AirPort. Il primo produttore per IBM compatibili è stato Linksys, l'attuale leader di questi prodotti.

2.4.1.3 802.11a

Nel 2001 venne ratificato il protocollo 802.11a presentato nel 1999 ma approvato solo nel 2001. Questo standard utilizza lo spazio di frequenze nell'intorno dei 5 Ghz e opera con una velocità massima di 54 Mbit/s, sebbene nella realtà la velocità reale disponibile all'utente sia di circa 20 Mbit/s. La velocità massima può essere ridotta a 48, 36, 34, 18, 9 o 6 se le interferenze elettromagnetiche lo impongono. Lo standard definisce 12 canali non sovrapposti, 8 dedicati alle comunicazioni interne e 4 per le comunicazioni punto a punto. Quasi ogni stato ha emanato una direttiva diversa riguardante questo standard, per regolare le frequenze ma dopo la conferenza mondiale per la radiocomunicazione del 2003 l'autorità federale americana ha deciso di rendere libere le frequenze utilizzate dallo standard 802.11a. Questo standard non ha riscosso i favori del pubblico dato che l' 802.11b si era già molto diffuso e in molti paesi l' uso delle frequenze a 5 Ghz è tuttora riservato.

2.4.1.4 802.11g

Nel giugno del 2003 venne rattificato lo standard 802.11g. Utilizza le stesse frequenze del *b* cioè la banda di 2.4 Ghz e fornisce una banda teorica di 54 Mbit/s che nella realtà si traduce in una banda netta di 24.7 Mbit/s, simile a quella dello standard 802.11a. E' totalmente compatibile con lo standard *b*, ma quando si trova a operare con periferiche di tipo *b* deve ovviamente ridurre la sua velocità. Prima della ratifica ufficiale dello standard 802.11g avvenuta nell' estate del 2003 vi erano dei produttori indipendenti che fornivano delle apparecchiature basate sulle specifiche non definitive dello standard. I

principali produttori preferirono comunque aspettare le specifiche ufficiali e quando furono disponibili molti dei loro prodotti vennero resi compatibili con il nuovo standard. Alcuni produttori introdussero delle ulteriori varianti chiamate g+ o Super G nei loro prodotti. Queste varianti utilizzavano l'accoppiata di due canali per raddoppiare la banda disponibile anche se questo portava interferenze con le altre reti e non era supportato da tutte le schede. Il primo grande produttore a rilasciare schede con le specifiche ufficiali 802.11g fu nuovamente Apple che presentò i suoi prodotti AirPort Extreme. Cisco decise di entrare nel settore acquistando Linksys, e fornì i suoi prodotti con il nome di Aironet.

2.5 Livello MAC dell'IEEE 802.11

Il livello di MAC definisce due differenti metodi di accesso che verranno descritti singolarmente nei successivi paragrafi: *Distributed Coordination Function* e *Point Coordination Function*.

2.5.1 Metodo di Accesso Base: CSMA/CA

Il meccanismo di accesso base, denominato *Distributed Coordination Function*, è basato sul meccanismo di accesso multiplo con rilevamento della portate e prevenzione delle collisioni (Carrier Sense Multiple Access con Collision Avoidence o in forma più compatta CSMA/CA). I protocolli CSMA sono ben noti nell'industria e il più popolare è sicuramente l'Ethernet che però è basato su un meccanismo di rilevamento delle situazioni di collisone sul canale di comunicazione (Collision Detection o CD). Un protocollo CSMA lavora

nel modo seguente. Quando una stazione vuole trasmettere, testa il canale di trasmissione. Se il canale è occupato (una delle altre stazioni connesse sul medesimo mezzo sta trasmettendo) la stazione deferisce la trasmissione ad un momento successivo. Se invece si rileva che il mezzo è libero, alla stazione è consentito trasmettere.

Questi tipi di protocolli sono molto efficienti se il mezzo di trasmissione non è pesantemente caricato, in quanto le stazioni possono trasmettere con il minimo ritardo. Vi è però la possibilità che più stazioni, rilevando contemporaneamente che il mezzo trasmissivo è libero, comincino a trasmettere simultaneamente. In questo caso, ovviamente, si verifica una situazione di collisione sul mezzo radio. Questa situazione di collisione deve essere rilevata in modo che i pacchetti possano essere ritrasmessi direttamente dal livello di MAC, senza interessare i livelli superiori dello stack protocollare, cosa questa che produrrebbe significativi ritardi a livello di trasmissione dei singoli pacchetti.

Nel caso dell'Ethernet, questa situazione di collisione è rilevata dalla stazione trasmittente, la quale entra in una fase di ritrasmissione basata su un algoritmo di posticipo della trasmissione denominato Exponential Random Backoff Algorithm; questo algoritmo fissa un tempo di ritrasmissione arbitrario al termine del quale viene testato il mezzo trasmissivo e, se è ancora occupato, il tempo di ritrasmissione viene aumentato con logica esponenziale.

Mentre questo meccanismo di rilevamento della collisione è un'ottima idea nel caso di Wired LAN, è assolutamente esclusa la sua adozione nel caso in cui il mezzo trasmissivo sia il canale radio; questo per due ragioni principali:

- l'implementazione di un meccanismo di rilevamento della collisione richiederebbe l'immediata implementazione di capacità di trasmissione e ricezione full-duplex e ciò porterebbe ad un significativo incremento del prezzo degli apparati;

- in un ambiente wireless non è possibile assumere che una stazione sia in grado di sentire l'attività di tutte le altre (questa ipotesi è alla base dello schema di rilevamento della collisione). In quest'ottica se una stazione che vuole trasmettere rileva la non occupazione del mezzo, non necessariamente significa che il mezzo sia libero attorno all'area di ricezione.

Allo scopo di superare questi problemi, l'802.11 utilizza un meccanismo di collision avoidance unito ad uno schema di positive acknowledge, il cui funzionamento è il seguente:

- Una stazione che vuole trasmettere testa il mezzo trasmissivo. Se il mezzo è occupato la trasmissione verrà deferita. Se il mezzo è libero, ed è libero per un certo tempo, denominato Distributed Inter Frame Space (DIFS) nello standard, la stazione effettua la trasmissione.

- La stazione ricevente controlla il CRC del pacchetto ricevuto e invia un pacchetto di acknowledgement (ACK). La ricezione di questo pacchetto indica alla stazione trasmittente che non si è verificata nessuna situazione di collisione. Se la stazione che ha iniziato la trasmissione non riceve l'acknowledgement, allora ritrasmetterà il pacchetto fino a che non riceve un pacchetto di acknowledge. E' comunque fissato un nu-

mero massimo di ritrasmissioni oltre il quale il pacchetto viene buttato via.

2.5.2 Virtual Carrier Sense

Allo scopo di ridurre la probabilità che si verifichi una situazione di collisione tra due stazioni a causa della impossibilità di ciascuna stazione di sentire tutte le altre, lo standard definisce un meccanismo denominato Virtual Carrier Sense:

Una stazione che vuole trasmettere, innanzitutto procede alla trasmissione di un breve pacchetto di controllo denominato RTS (Request To Send), che contiene l'identificativo della sorgente e della destinazione, oltre alla durata della successiva trasmissione relativa al pacchetto RTS e al rispettivo ACK. La stazione di destinazione risponde (se il mezzo è libero) con un pacchetto di controllo denominato CTS (Clear To Send), con la stessa informazione relativa alla durata di trasmissione.

Tutte le stazioni ricevendo sia un RTS sia un CTS, settano l'indicatore Virtual Carrier Sense (chiamato NAV che sta per Network Allocation Vector), per un certo tempo ed utilizzano questa informazione insieme con il Physical Carrier Sense al momento in cui vanno a effettuare la rilevazione di occupazione del mezzo.

Questo meccanismo riduce la probabilità di collisione su un'area di ricezione che è nascosta all'interno dell'intervallo di tempo necessario alla trasmissione dell'RTS, poiché la stazione sente il CTS e definisce il mezzo come occupato fino alla fine della trasmissione. L'informazione relativa al tempo

di trasmissione protegge inoltre l'area del trasmettitore dalle collisioni durante l'invio dell'ACK da parte di quelle stazioni che sono fuori dall'area di visibilità della stazione che deve fornire l'ACK stesso.

2.5.3 Point Coordination Function

Oltre alla funzione base di coordinazione, denominata Distributed Coordination, è prevista una Point Coordination Function, che può essere usata per implementare servizi che hanno requisiti temporali stringenti, come le trasmissioni audio o video. Questa funzione fa uso dell'elevata priorità che l'AP può guadagnare attraverso l'utilizzo di un breve Inter Space Frame (PIFS). Utilizzando questa elevata priorità di accesso, l'AP emette, secondo un meccanismo di polling, delle richieste alle stazioni per la trasmissione dati, quindi controlla l'accesso al mezzo. Allo scopo di consentire alle stazioni regolari di accedere al mezzo trasmissivo, è prevista la norma in base alla quale l'AP deve lasciare abbastanza tempo per il Distributed Access all'interno della PCF.

2.5.4 Metodo di indirizzamento

Al fine di mantener compatibilità con i precedenti standard 802, l'802.11x prevede un indirizzamento a livello MAC di 48 bit. In tal modo anche l'interoperabilità con soluzioni wired di tipo Ethernet è garantita.

2.6 Metodi di accesso ad una BSS

Primadi utilizzare un network bisognerebbe prima "*trovarlo*". Nel caso di una rete cablata è semplice, basta collegare il cavo, ma nel caso di una reteWireless le cose si complicano moltissimo. Nell'ambito Wireless il processo di scoperta ed identificazione della rete è detto scanning. I diversi parametri che sono utilizzati inquesta procedura possono essere specificati dall'utentema molti sono di *default* presenti nei driver delle schede Wireless. I parametri più importanti sono:

Tipo BSS, indentifica se la rete è Ad Hoc oppure Infrastructured BSS

- *SSID*, Assegna una stringa di bit ad un ESS. Molti produttori identificano il SSID con il nome del network
- *BSSID*. identifica se l'SSID è inviato o no in broadcast
- *Scan Type*, è *attivo* se la stazione invia pacchetti per identificare la rete, *passivo* se rimane in ascolto dei pacchetti beacon inviati dall'Access Point o dalle altre stazioni
- *Channel list*, invio della lista dei canali disponibili sui quali tentare una connessione oppure rimanere in ascolto per identificare quale sia il canale utilizzato.

Nello *scanning passivo* la stazione rimane in ascolto dei pacchetti di beacon dell'AccessPoint. Nei pacchetti di beacon vi sono i parametri necessari ad una stazione al finedi collegarsi al network: tipo di BSS, SSID, timer per la sincronizzaione e canale da utilizzare. Nello *scanning attivo*, una stazione

piuttosto che ascoltare trasmette dei pacchetti, canale per canale, richiedendo l'accesso ad uno specifico ESS.

Al termine dello scan, *attivo* o *passivo*, la stazione ha l'insieme dei parametri necessari a connettersi alla rete: tipo di BSS, SSID e canale da utilizzare. A questo punto la stazione può passare all'autenticazione. Nell'802.11 i metodi di autenticazione usati sono l'*open system* e la *shared key*:

- Open System, l'AccessPoint accetta la connessione da qualunquestazione senza verificarne l'identità. L'unico parametro identificativo preso in considerazione è il MAC address sul quale è possibile eseguire delle regole di filtraggio.

- Shared Key, viene utilizzato l'autenticazione di tipo *WEP* (Wired Equivalent Privacy) ed implica che ogni stazione abbia il *WEP* attivo ed utilizzi una *shared key*. In questa procedura viene introdotto un meccanismo di controllo della *shared key* tramite l'utilizzo della stessa per criptare un 'challenge text' e la sua decriptazione che può avvenire solo se le due *shared key* sono uguali.

Una volta che l'autenticazione è stata completata la stazione può associarsi ad un AccessPoint o riassociarsi ad un nuovoAccess Point nel caso di *roaming*. L'*associazione* è una procedura di registrazione della identità della stazione in modo che il sistema di distribuzione sappia sempre dove la stazione si trova per indirizzare correttamente i frame. Dopo che l'associazione è stata completata l'Access Point deve registrare la stazione nella rete cablata in modo che i frame destinati alla stazione siano corettamente inviati all'AccessPoint. Un metodo di registrazione è associare il MAC della stazione alla porta dello

switch dove l'Access Point è collegato tramite il protocollo ARP. Dopo che la stazione è autenticata sull'AP viene inviato un pacchetto di *association request*. L'Access Point processa l'*association request* e se l'associazione è andata a buon fine l'Access Point comincia a far transitare i *frame* da e per la stazione.

2.7 Roaming

Il *Roaming Connection-Less* è il processo che consente lo spostamento di una stazione da una cella (o BSS) ad un'altra senza perdita di connessione. Questa funzione è simile a quella che viene realizzata nei sistemi di telefonia cellulare, con due differenze fondamentali:

- Su un sistema *LAN* basato sulla tecnica di trasmissione a pacchetti, la transizione da una cella all'altra deve essere realizzata tra la trasmissione di un pacchetto e quella del successivo, al contrario di quanto accade in un sistema per telefonia in cui il processo deve avvenire durante lo svolgimento di una comunicazione. In base a ciò, quindi, in una LAN il processo risulta sicuramente di più semplice implementazione.

- Il rovescio della medaglia si trova nel fatto che, su un sistema per il trasferimento della voce, una temporanea disconnessione può non avere un effetto significativo, mentre in un ambiente basato sul pacchetto questa momentanea interruzione della connessione porta ad una significativa riduzione delle prestazioni, in quanto è necessario operare delle ritrasmissioni, gestite, però, dai livelli superiori dello stack protocollare.

Lo standard 802.11 non definisce come il roaming debba essere realizzato, ma definisce un modo di funzionamento base, secondo il quale la stazione in movimento, attraverso il meccanismo di Passive Scanning o quello di Active Scanning, rileva quali AP sono disponibili per la connessione. A quel punto, in funzione del livello del segnale ricevuto dagli AP decide a quale è più conveniente associarsi e attraverso un meccanismo di re-associazione, definito dallo standard, può eliminare l'associazione dal vecchio AP e associarsi a quello nuovo.

Il processo di *riassociazione* è il permette l'associazione da un vecchio Access Point ad uno nuovo. Se nel raggio di azione di una stazione vi è un altro AP con lo stesso ESS, la stazione ne monitorizza la qualità del segnale. Quando la stazione decide che questo nuovo Access Point è una scelta migliore, inizia la procedura di riassociazione: invia una richiesta di riassociazione al nuovo AP specificando quale era il suovecchio AP, il nuovoAccess Point comunica con il vecchio, tramite il protocollo *IAPP* (Inter−Access Point. Protocol), verificando che la stazione fosse realmente a lui associata. In caso positivo accetta la associazione comunicandola al vecchio Access Point il quale forwarda al nuovo Access Point gli eventuali pacchetti bufferizzati da inviare alla stazione e termina l'associazione della stazione. La procedura è conclusa e la stazione ha cambiato Access Point in modo del tutto trasparente all'utente.

2.8 Mantenimento della Sincronizzazione

Le stazioni hanno inoltre la necessità di mantenere la sincronizzazione, che è necessaria per mantenere la sincronizzazione nei salti di frequenza e per la realizzazione di altre funzioni come il risparmio energetico. In una infrastruttura basata su BSS questo è ottenuto provvedendo all'aggiornamento del clock delle singole stazioni, in accordo con il seguente meccanismo. L'AP trasmette periodicamente un Beacon Frame. Questo frame contiene il valore dell'orologio interno dell'AP al momento della trasmissione. Da notare che questo rappresenta il momento in cui la trasmissione viene realizzata e non il momento in cui il frame viene inserito nella coda di trasmissione. Poiché anche questo frame viene trasmesso utilizzando la regola CSMA, la trasmissione può essere significativamente ritardata. La stazione ricevente controlla il valore del proprio orologio al momento della ricezione del segnale e lo corregge mantenendo la sincronizzazione con l'orologio dell'AP. Questo meccanismo è di fondamentale importanza perché previene lo slittamento del clock che si può verificare dopo alcune ore di funzionamento del sistema.

2.9 Livello PHY dell'IEEE 802.11

Il livello fisico del protocollo 802.11, come detto, comprende 3 differenti tipi di tecnologie utilizzabili indistintamente: FHSS, DSSS e IR. L'uso di queste tecnologie è simile all'utilizzo nelle LAN Ethernet di tipi di mezzi di comunicazione quali 10BASE-2 o 10BASE-T.

Come ovvio, apparati che utilizzano PHY diversi non possono appartenere

alla stessa WLAN, in quanto totalmente incompatibili.

FHSS e DSSS sono basate sulla tecnologia "Spread Spectrum", con il significato che, in modi diversi, la potenza del segnale è distribuita ("spread") su uno spettro più ampio, quest'ultimo definito a partire dal segnale in ingresso mediante uno "spreading code". Le caratteristiche fondamentali sono le seguenti:

- bassa densità di potenza del segnale (in quanto viene distribuita su ampi spettri);
- ridondanza, che fa si che il segnale sia presente su diverse frequenze allo stesso tempo. In tal modo si può avere una correzione degli errori;

Vediamo le caratteristiche fondamentali di queste varianti

2.9.1 DSS

- Banda 2.4 – 2.4835 GHz;
- Utilizza diverse bande, ciascuna di 22 MHz;
- Più costosa rispetto alle altre tecnologie;
- Tempi di risposta più rapidi;
- Data Rates di 1 , 2 e 11 Mbps, quindi più veloce rispetto alla FHSS;
- Molto sensibile a fenomeni quali "multipath fading", disturbi, "rumore"...

Probabilmente la più utilizzata fra le tre alternative, e di prestazioni superiori, DSSS è una forma di tecnologia per molti versi simile a quella utilizzata dal GPS (Global Positioning System).

Come descrizione sommaria, si può dire che il segnale contenente lo stream di dati è combinato mediante XOR con un sequenza di impulsi pseudo- casuali, in tal caso l' "11 chip Barker Code". Il risultato è un segnale digitale di, ad esempio, 11 Mbps, che può essere modulato in una banda di 20 Mhz. Ovviamente in ricezione bisognerà conoscere la sequenza "11 chip Barker Code" utilizzata. Per la modulazione si utilizza DBPSK per trasmissioni a 1Mbps e 11 Mbps, DQPSK per trasmissioni a 2Mbps. In tal caso lo "spreading code" è proprio l' "11 chip Barker Code".

2.9.2 FHSS

- Banda 2.4 – 2.4835 GHz;
- Utilizza una frequenza per ogni "time hop", scelto casualmente all'interno della banda disponibile;
- Implementazione più semplice e costi minori rispetto alla DSSS
- Migliore tolleranza ai disturbi, alle interferenze ed al "multipath fading" (ossia i "cammini multipli" di un segnale dal trasmettitore al ricevitore);
- Maggior numero di network intendenti collocabili sulla stessa area (26 contro i tre del DSSS);
- Data rates di 1 , 2 Mbps e tempi di risposta più lunghi rispetto al DSSS.

In tal caso l'approccio è totalmente differente, in quanto la portante di modulazione varia la sua frequenza da un canale all'altro all'interno della banda concessa al "data stream", mediante un ordine pre-ordinato anche in questo caso pseudo-casuale. Ovviamente i ricevitori dovranno essere sincronizzati con il trasmettitore, in modo da poter demodulare correttamente il segnale. Il sistema utilizza la modulazione 2FSK a 1Mbps e 4FSK a 2Mbps. Le frequenze di modulazione sono distanziate di 1Mhz. Esistendo, per lo standard, 89 canali e 78 diverse sequenze ("hop sequences"), la possibilità di collisioni è drasticamente inferiore rispetto al sistema DSSS. Come contraltare, i tempi di risposta generali del sistema sono superiori, e, come detto, la velocità massima raggiungibile risulta essere soltanto di 2Mbps. In tal caso lo "spreading code" è proprio l' "hop sequence".

Capitolo 3

Identificazione e analisi dei parametri significativi

Finora, l'attenzione degli addetti ai lavori, in tema di reti WIFI, è stata concentrata sul problema, senz'altro strategico in talune situazioni, ma importante in ogni contesto, della *sicurezza* delle informazioni e quindi della rete stessa. Forse, il problema della *efficienza* della rete WIFI, del suo corretto dimensionamento e, soprattutto in relazione alla crescita del numero di utenti, del mantenimento nel tempo di standard qualitativi accettabili è stato meno sentito dalla comunità scientifica, preferendo, genericamente, potenziare la rete aumentando il numero di AP, piuttosto che affidarsi ad uno studio sistematico dei parametri sigificativi e ad una loro ottimizzazione al variare delle condizioni. Può essere interessante, viceversa, indagare come un diverso approccio al problema della *qualità della configurazione* possa aiutare nell'obiettivo di mantenere, o raggiungere, un' efficienza della rete.

Un interessante lavoro è riportato in [8] dove ci si concentra sulla ricerca

di metodi per il monitoraggio passivo di WLAN e su come tali rilevazioni debbano tenere conto di dati sulla localizzazione degli utenti e terminali giungendo alla realizzazione di vere e proprie mappe di copertura e qualità.

Sono stati già fatti un certo numero di studi sulle misurazioni[9]. Molte di queste ricerche sono state fatte su sottoreti wired. In [10] si discute che le misurazioni wireless sono più appropriate per catturare le caratteristiche di mezzi wireless ed il loro impatto sul flusso di traffico. Le misurazioni wireless permettono di acquisire informazioni più dettagliate sui mezzi wireless di quelle effettuate su sotttoreti wired. E' affermato che il monitoraggio wireless può efficientemente identificare le cause di perdite e ritardi .

In [11] è stato realizzato uno studio che dimostra come movimenti lenti degli utenti influenzino la qualità del link. In contrasto alle comuni assunzioni l'esperimento dimostra come la qualità aumenti all'aumentare della velocità dei movimenti e lo si valuta dal fatto che il numero di pacchetti persi e la varianza, misurata dopo la ritrasmissione a livello link, diminuscono. Le misurazioni mostrano anche che la qualità del link è influenzata principalmente dal tipo di modulazione, dal massimo numero di ristrasmissioni, dal settaggio sperimentale e anche dalla qualità della alimentazione elettrica. In [12]la pianificazione della rete è indicata come una nuova area applicativa per la tecnologia della localizzazione mobile. In particolare, si valutano tecniche di localizzazione UMTS e la loro capacità di favorire la pianificazione di reti. La conoscenza del livello del segnale ricevuto come una funzione della localizzazione è un compito chiave nella pianificazione delle reti. Il livello del segnale è usato per pianificare la copertura, per l'analisi delle interferenze e la pianificazione di ciò che sta attorno. Un considerevole risparmio dei co-

sti lo si ottiene se le misure in campi dedicati possono essere rimpiazzati da report di misure forniti da usuali telefoni mobili. Il documento parla dell'accuratezza della valutazione del livello del segnale. In [13] e [14] è presentato il Sistema di Copertura Adattativi (ACS - Adaptive Coverage System) del progetto IST-CELLO. Si tratta di un sistema per localizzare l'area in reti a celle dove è necessaria una maggior capacità e per fare rilevanti cambiamenti nella configurazione della rete. Il concetto è di utilizzare le informazioni sulla localizzazione per affinare adattivamente le antenne per raggiungere un incremento della capacità della rete e la stabilità.

E' opportuno sottolineare che come l'efficienza è *uno* dei criteri per stabilire la qualità di una rete WIFI, così l'efficienza stessa può essere meglio definita come un insieme di caratteristiche, tra le quali particolare attenzione meritano l'*affidabiltà*, i *tempi di risposta*, la s*oddisfazione delle richieste degli utenti.* E' significativo, quindi, individuare parametri che influenzino tali fattori e progettare algoritmi che, elaborando questi parametri, diano risultati nel senso di fornire un supporto alle decisioni per raggiungere, o mantenere, gli obiettivi di efficienza voluti.

Riassumendo:

valutiamo la qualità di una rete WIFI non solo in termini di ovvia rispondenza agli standard previsti, ma anche in termini di affidabilità, tempi di risposta e, non secondario, il grado di soddisfazione degli Utenti che vedono rispettate le proprie aspettative.

3.1 Sistema di Monitoraggio dei Parametri Significativi

Il contenuto del presente capitolo consiste nell'analisi e progettazione di massima di un Sistema di Monitoraggio per una rete WIFI costituita da almeno due AP. L'utente amministratore, mediante l'utilizzo di una applicazione (sia di tipo locale che usufruibile tramite WEB), tiene sotto controllo lo stato della rete, visualizzando tutte le informazioni necessarie al monitoraggio e agli interventi di ottimizzazione della rete medesima.

I dati di monitoraggio raccolti vengono salvati in file, in formato *.pcap* [15], e successivamente analizzati dall'applicazione.

Dalle informazioni presenti sono ricavati i parametri, ritenuti di maggiore utilità per i motivi di seguito illustrati, che forniscono indici di qualità sulla configurazione della rete WIFI:

- Numero e allocazione di canale
- Tipo di modalità 802.11 a/b/g
- Livello Segnale e conseguente rilevazione degli spostamenti dell'utente nella rete

Monitorando l'utilizzo della rete, e visualizzando opportunamente i parametri sopra elencati, sono generati messaggi all'amministratore di rete, al fine di consigliare possibili modifiche per l'ottimizzazione della rete stessa. Ogni parametro ha un suo peso nell'ottimizzazione e per ognuno viene descritta una soluzione ad hoc per un suo opportuno dimensionamento, facendo riferimento al Sistemna di Monitoraggio ipotizzato.

3.1.1 Numero e allocazione del canale

Come noto, i canali usati dai vari AP nella stessa rete, non devono essere gli stessi tra celle adiacenti, potendosi generare, in questo caso, fenomeni di *interferenze* tra i vari AP con relativa decrescita esponenziale della *performance*. Di conseguenza, è opportuno richiedere una adeguata distribuzione dei canali. Tutto ciò porta a considerare tale parametro (numero canale) significativo per valutare la qualità della rete.

In presenza di una rete dotata di un AP, che venga interessata dall"'ingresso" di un nuovo Access Point, si evidenzia nella Sezione 4.1.1, attraverso l'analisi dei risultati di test appropriati, l'importanza dell'assegnamento del numero di canale, al fine di limitare la degradazione delle comunicazioni.

L'applicazione proposta, acquisendo il numero del canale di tutti gli AP rilevati, è in grado di avvisare l'Amministratore della nuova situazione e di suggerire eventuali modifiche del parametro.

Una diversa situazione, ma un ulteriore motivo di interesse è rappresentato dall'aspetto "commerciale" dell'utilizzo del parametro Canale. Una situazione di allocazione dello stesso, suddividendolo tra Utenti che richiedono un servizio di connessione in rete, è affrontata, seppure solo in maniera teorica senza alcun aspetto realizzativo, nella sezione 4.2.

3.1.2 Tipo di modalità 802.11g/b

Tale parametro, visualizzato dall'applicazione proposta (sezione 3.3), risulta importante ai fini della qualità delle comuncazioni perchè condiziona sensibilmente la banda di comunicazione dei Device Mobili.

Infatti, gli AP settati per comunicare con protocolli 802.11b accettano esclusivamente clienti predisposti a dialogare con il medesimo protocollo; lo stesso dicasi per AP settati per protocolli 802.11g. Gli AccessPoint settati in modalità *mixed* (che accettano, cioè, sia 802.11b che 802.11g) possono associare clienti di entrambe le configurazioni; la presenza, in tali situazioni, di clienti in protocollo 802.11b, forza la commutazione di **tutto** il traffico di tipo 802.11g in modalità 802.11b, riducendo, di conseguenza, la banda ai potenziali utenti 802.11g.

Per questo motivo si decide di monitorare il numero di utenti in media presenti su un certo AP con una certa modalità e, nel caso in cui gli utenti in 802.11.b sia minimo si può segnalare all'amministratore l'opportunità di posizionare un ulteriore AP in *sola* modalità 802.11.g, oppure di riconfigurare uno degli AP presenti in modalità *mixed* in sola modalità 802.11g, rendendo così possibile agli utenti più veloci di usufruire appieno del servizio.

3.1.3 Livello segnale

Il livello del segnale (Vedi capitolo 4 per la descrizione della logica e l'implementazione software della soluzione proposta) è uno dei parametri fondamentali da monitorare ed è quello che viene preso maggiormente in considerazione nel presente lavoro, perchè condiziona sensibilmente il servizio e di conseguenza la qualità della rete WIFI.

Nella soluzione proposta (vedi capitolo 4) non si rileva con precisione la posizione degli utenti nella rete, ma si utilizza la logica del "metodo a propagazione" (illustrata nello stesso capitolo 4) per rilevare lo spostamento

(avvicinamento o allontanamento) del Device Mobile dall'AP per consentire di valutare, anche se approssimativamente, la posizione degli utenti nella rete, nel senso di essere o meno nella cella di un Ap.

A fronte di tali rilevamenti, viene mandato uno specifico messaggio che avvisa l'amministratore della presenza di un certo numero di utenti lontani dall'AP (suddivisi in "fasce" di distanza e di conseguente degrado del servizio) e della utilità di inserire un ulteriore AP nella loro direzione, oppure dell'installazione di un Amplificatore di segnale.

Inoltre, il rilevamento dello spostamento degli utenti fa capire, in tempo reale, verso quale direzione si dirigono e quindi se, sul nuovo AP su cui si associeranno, ci siano o meno risorse adeguate ai suoi servizi. Il monitoraggio della posizione degli utenti su ogni AP dà la possibilità all'amministratore di capire dove in media viene sfruttato maggiormente l'apparato o, viceversa, dove un AP viene sottoutilizzato ed eventualmente è conveniente la sua eliminazione.

A tale proposito, l'algoritmo di ottimizzazione di posizionamento degli AP indica all'Amministratore la classifica degli AP più *stressati* e può consigliare lo spostamento o l'aggiunta di uno o più AP per migliorare il servizio. I tipi di segnalazione, in relazione al livello di utilizzo dell'AP, e i relativi consigli di ottimizzazione, sono:

- *Alert di Alto utilizzo*, consiglio di aggiungere al più presto un AP nella stessa zona con una modalità di connessione di tipo WDS (Wireless Distribution System).

- *Warning di Medio utilizzo*, consiglio di rivedere la configurazione, ma-

gari aggiunendo un AP per aumentarne le prestazioni.

- *Warning di Basso utilizzo*, consiglio di eliminare l'AP oppure di spostarlo in una zona più densa di utenti.

3.2 Descrizione dell'applicazione software per la rilevazione dei parametri

Come ampiamente descritto nel capitolo 6, l'applicazione realizzata si occupa di processare i file *.pcap,* generati da *Kismet_Server* sul flusso, spedito da *Kismet_Drone*, dei pacchetti monitorati. Lo sniffing dei pacchetti è rivolto ai soli pacchetti di tipo IEE802.11, di cui nella figura seguente è illustrato un esempio di rappresentazione nel file *.pcap:*

```
0000  80 00 00 00 ff ff ff ff  ff ff 00 14 bf fa 30 2d  ........ ......0-
0010  00 14 bf fa 30 2d f0 bf  85 b1 20 25 00 00 00 00  ....0-.. .. %....
0020  64 00 11 04 00 06 57 49  46 49 44 33 01 08 82 84  d.....WI FID3....
0030  8b 96 24 30 48 6c 03 01  0b 05 04 00 01 00 00 2a  ..$0Hl.. .......*
0040  01 00 2f 01 00 32 04 0c  12 18 60 dd 06 00 10 18  ../..2.. ..`.....
0050  02 01 04 dd 18 00 50 f2  01 01 00 00 50 f2 02 01  ......P. ....P...
0060  00 00 50 f2 02 01 00 00  50 f2 02 00 00           ..P..... P....
```

Figura 3.1: Frame IEE802.11

Si è resa necessaria una interpretazione dei contenuti del pacchetto (fornito in codifica esadecimale), per identificarne le informazioni significative, utilizzando le specifiche dello standard di riferimento; in questo modo le informazioni ricavate sono state strutturate in maniera adatta alla loro successiva elaborazione, suddividendole, ad esempio, in ragione del tipo e sottotipo di frame (es.: tipo *management*, sottotipo *beacon*).

Nei paragrafi che seguono sono descritti, tra i formati previsti nello stan-

dard di riferimento, quelli che sono stati utilizzati nel presente lavoro, con la relativa descrizione dei rispettivi parametri e grandezze presenti.

Infine sono descritte, nella sezione 3.2.2., in particolare, le informazioni decodificate dall'applicazione proposta, tra cui le principali sono:

- Numero di Canale
- Modalità di Connessione (sia degli AP che dei DM)
- Tipo e Sottotipo di Pacchetto

3.2.1 Formato dei pacchetti IEEE 802.11

Ciascun pacchetto MAC (o frame come lo abbiamo chiamato finora), è composto dai seguenti componenti base:

1. *MAC Header*: che comprende informazioni di controllo, informazioni sugli indirizzi mittente e destinatario etc.
2. *Frame Body*: di lunghezza variabile, contiene informazioni relative al tipo di frame specificato nell'header (ad esempio, se il frame è di tipo *dati* il frame body conterrà i dati stessi, ovvero il *payload*).
3. *Frame Check Sequence* (FCS): è il CRC a 32 bit usato per rilevare gli errori di ricezione.

3.2.1.1 Formato generale dei frame

La seguente figura illustra il formato dei *frame MAC* del protocollo IEEE 802.11:

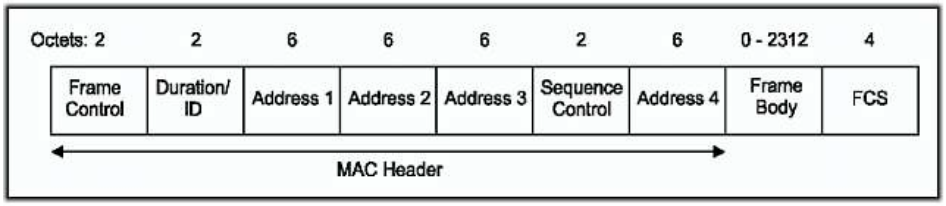

Figura 3.2: Formato generale del frame MAC

I campi: Address 1, Address 2, Address 3, Sequence Control, Address 4 e Frame Body sono presenti solo in alcuni tipi di frame.

3.2.1.2 Descrizione dei campi

Campo Frame Control

La seguente figura mostra il contenuto del campo *frame control* incluso nell'header:

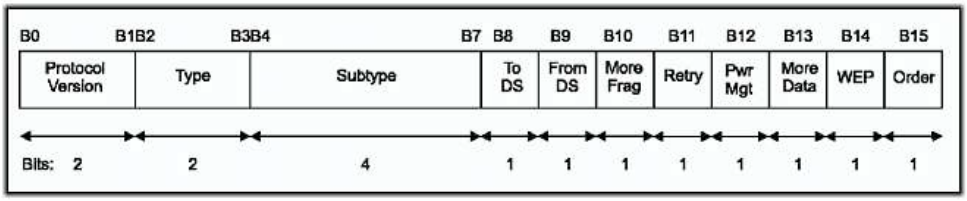

Figura 3.3: Formato del Frame Control Field

E' opportuno analizzare alcuni sotto-campi di maggiore importanza:

Type e Subtype

Lo standard prevede 3 tipi di frame: ***data, control e management***. Ciascuno dei tipi ha a sua volta molti sottotipi e questi possono essere riassunti nella seguente tabella:

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Tabella 3.1: Valori possibili dei campi Type e Subtype del frame control field.

ToDS e FromDS

Sono presenti solamente nel caso di Frame di tipo *dati*. Le diverse combinazioni dei campi *ToDS* e *FromDS* e i loro significati possono essere riassunti nella seguente tabella:

ToDS	FromDS	Significato
0	0	E' presente in un frame di tipo dati che va da una STA ad un'altra nella stessa IBSS, ed è presente in tutti i frame di tipo control e management
0	1	E' presente nei frame di tipo dati destinati al DS
1	0	E' presente nei frame di tipo dati provenienti dal DS
1	1	E' presente nei frame che transitano da un AP ad un altro Ap tramite il Wireless DS (WDS)

Tabella 3.2: Combinazioni dei campi To/From DS

Retry

Il bit retry è posto a 1 se il frame corrente rappresenta una *ritrasmissione* di un frame precedente. Questo è utile nella rilevazione dei frame duplicati, e di conseguenza di frame persi.

Campi di tipo Address

Nell'header dei pacchetti MAC IEEE 802.11 vi sono 4 campi dedicati agli indirizzi, ciascuno dei quali contiene un indirizzo a 48 bit conforme allo standard IEEE Std 802-1990. Un indirizzo MAC può essere di 2 tipi:

1. *Indirizzo individuale.* L'indirizzo associato ad una particolare STA nella rete.

2. *Indirizzo di gruppo.* Un indirizzo relativo a destinazioni multiple. Anche qui abbiamo 2 sottotipi:

    - *Multicast.* Un indirizzo associato, a livello superiore al MAC, ad un gruppo di STA della rete.

- *Broadcast.* Un particolare indirizzo multicast che indirizza tutte le STA appartenenti ad una specifica LAN. Quando i bit del campo Destination Address sono tutti pari a 1, questa situazione viene interpretata come un trasferimento broadcast.

I suddetti 4 campi dedicati agli indirizzi possono contenere una delle seguenti indicazioni:

- *BSSID (BSS Identifier),* rappresenta un indirizzo a 48 bit avente lo stesso formato degli indirizzi MAC IEEE 802, che identifica univocamente ciascuna BSS. Se quest'ultima possiede un'infrastruttura, ovvero è presente l'AP, il campo BSSID rappresenta l'indirizzo MAC della STA in cui risiede l'AP. In una IBSS, quest'indirizzo viene generato casualmente. Il valore pari a tutti 1, del campo BSSID, rappresenta una situazione di broadcast per tutte le BSS.

- *Destination Address (DA)*, contiene un indirizzo MAC (individuale o di gruppo) che identifica la (o le) entità MAC intese come destinataria (o destinatarie) finale della MSDU (o del singolo frammento MPDU) contenuto nel frame body.

- *Source Address (SA)*, contiene un indirizzo MAC individuale che identifica l'entità MAC dalla quale ha avuto origine la trsmissione della MSDU (o MPDU).

- *Trasmitter Address (TA)*, contiene un indirizzo MAC individuale che identifica la STA che ha trasmesso, relativamente al WM, la MPDU contenuta nel frame body.

- *Receiver Address (RA)*, contiene un indirizzo MAC (individuale o di gruppo) che identifica l'entità (o le entità) MAC che, relativamente al WM (Wireless Medium), sarà l'immediata destinataria del frame body corrente.

Alcuni frame possano non contenere alcuni dei campi d'indirizzo.

In alcuni casi, l'uso di un particolare campo d' indirizzo è direttamente collegato alla sua posizione (1-4) all'interno dell'header del frame MAC. Ad esempio, quando una STA vuole confrontare il proprio indirizzo con l'indirizzo destinazione di un frame, controlla sempre il contenuto del campo Address 1, oppure l'indirizzo del ricevente (ovvero della STA destinataria immediatamente successiva) dei frame CTS e ACK è sempre ottenuta dal campo Address 2 **(???)** nel corrispondente frame RTS o nel frame che si sta confermando con l'ACK.

3.2.1.3 Descrizione di alcuni frame importanti

Composizione dei frame di tipo Dati

La composizione di un frame di tipo dati non varia a seconda dei sottotipi, ed è definito dalla seguente figura:

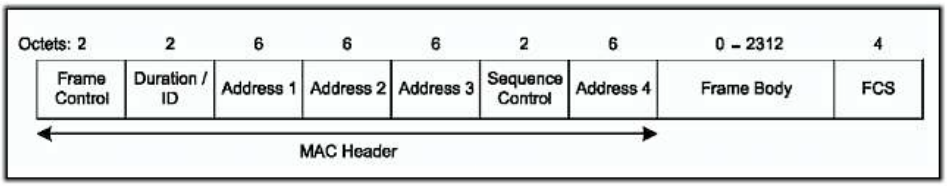

Figura 3.4: Composizione del frame di tipo Dati

Di seguito si mostra un esempio del frame di tipo Dati:

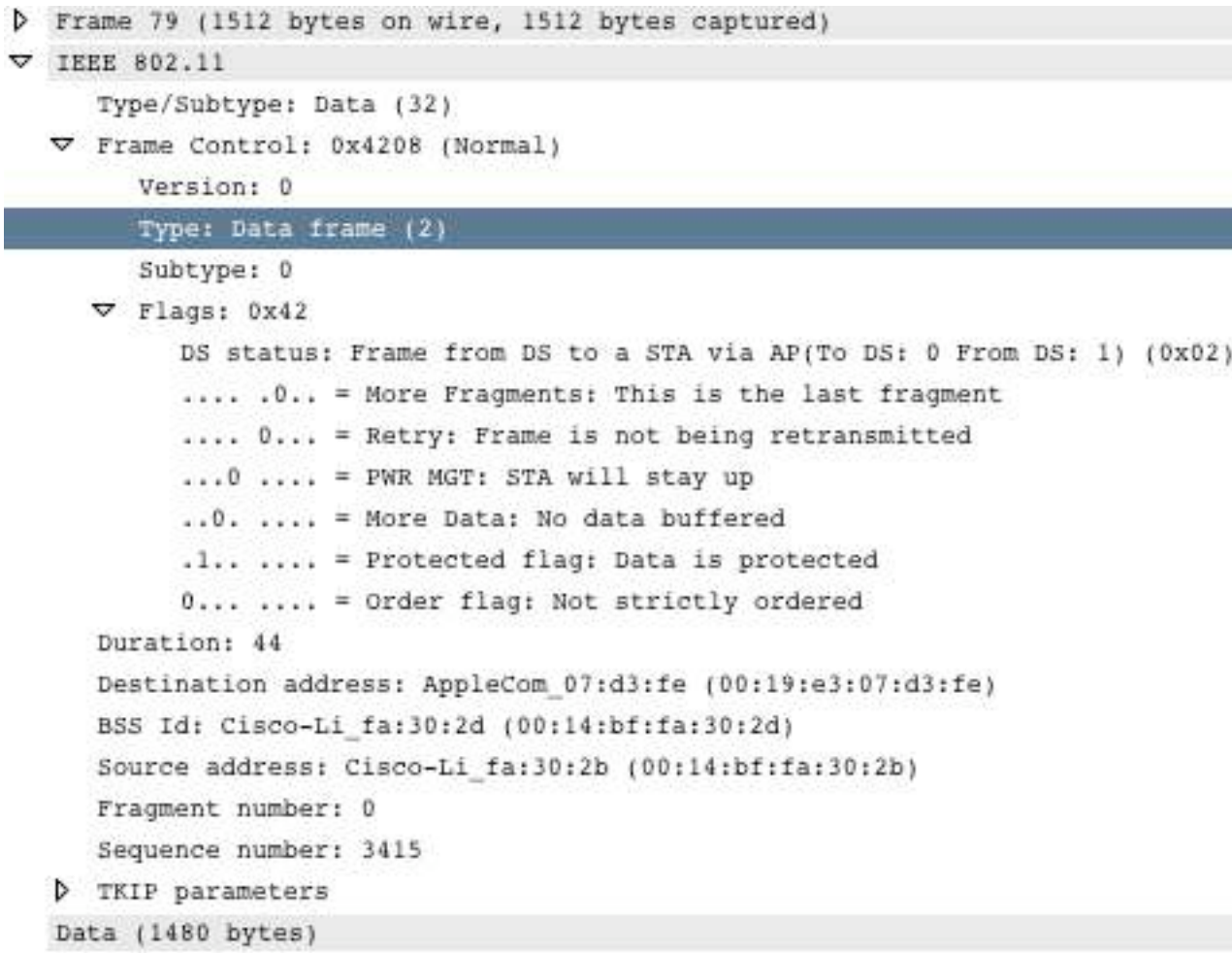

Figura 3.5: Esempio di frame di tipo Dati

Il contenuto dei campi indirizzo dipende dai valori dei campi ToDS e FromDS del campo *frame control* incluso nell'header, come si vede dalla tabella 3.2 precedentemente illustrata.

I valori ToDS e FromDS possono essere interpretati come di seguito:

Tabella 3.3: Relazione tra To/From DS e i campi Address in un frame dati

ToDs	FromDS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Quando il contenuto del campo è N/A, il campo stesso è omesso. Il campo Address 1 contiene sempre l'indirizzo MAC del destinatario del frame, mentre il campo Address 2 contiene sempre l'indirizzo MAC della STA che sta trasmettendo il frame.

Una STA usa il contenuto del campo Address 1 per capire se il frame è ad essa indirizzato. Nel caso in cui il campo Address 1 contenga un indirizzo di gruppo (multicast o broadcast), viene esaminato anche il valore BSSID per capire se il frame multicast o broadcast ha avuto origine nella stessa BSS della STA ricevente.

Una STA usa il contenuto del campo Address 2 per indirizzare il frame ACK, quando richiesto. RA è l'indirizzo MAC del'AP che nel sistema di distribuzione wireless è l'immediato destinatario del frame, o del frammento. TA invece è l'indirizzo MAC dell'AP che, sempre nel sistema di distribuzione wireless, è l'immediato mittente del frame o del frammento.

Il valore BSSID viene così interpretato:

- se la WLAN è di tipo "*con infrastruttura*", il BSSID coincide con l'indirizzo MAC della STA IEEE 802.11 che funziona da AP;

- se la WLAN è una rete *ad hoc* (IBSS), il BSSID è l'identificativo della IBSS (scelto casualmente).

Composizione generale dei frame di tipo Management

Anche la composizione dei frame di tipo *Management* non varia a seconda dei diversi sottotipi. La composizione è osservabile dalla seguente figura:

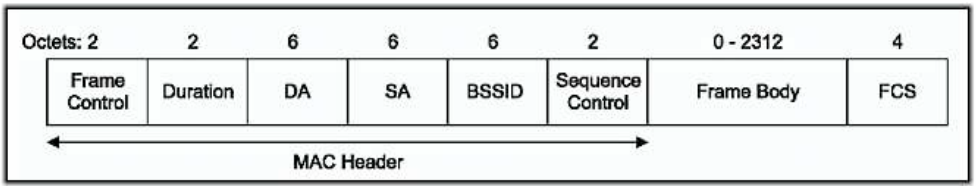

Figura 3.6: Composizione del Frame di tipo Management

Di seguito si mostra un esempio del frame di tipo Management:

```
▷ Frame 186 (109 bytes on wire, 109 bytes captured)
▽ IEEE 802.11
    Type/Subtype: Beacon frame (8)
  ▽ Frame Control: 0x0080 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 8
    ▷ Flags: 0x0
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Cisco-Li_fa:30:2d (00:14:bf:fa:30:2d)
    BSS Id: Cisco-Li_fa:30:2d (00:14:bf:fa:30:2d)
    Fragment number: 0
    Sequence number: 4079
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (12 bytes)
  ▷ Tagged parameters (73 bytes)
```

Figura 3.7: Esempio di frame Management

Il frame body è composto in parte da campi di dimensione fissata, ed in parte da elementi informativi, ovvero raggruppamenti di più dati che possono avere dimensione variabile. Alcuni campi o elementi informativi sono obbligatori ed è obbligatorio anche l'ordine in cui devono comparire all'interno del frame body; nell'esempio i suddetti campi sono rappresentati rispettivamente da *Fixed parameters* e *Tagged Parameters*.

3.2.2 L'Applicazione proposta

L'applicazione analizza i file *.pcap* e visualizza a schermo (o li salva in un apposito file di testo), i parametri significati ai fini della valutazione qualitativa della rete WIFI.

I tipi di pacchetto (campo subtype del frame control) identificati sono:

- Beacon
- Probe Request
- Probe Response
- Data

3.2.2.1 Beacon

,E' un tipo di pacchetto spedito dall'AP per "pubblicizzarsi", ossia notificare le sue caratteristiche alla rete, tra cui l'invio del timer (*timestamp*) per permettere la sincronizzazione ad un clock comune, in modo da permettere ai dispositivi interessati (DM) di "associarsi" alla sua cella.

Di seguito viene mostrato l'output dell'applicazione che rileva il pacchetto Beacon spedito dal'AP Router, a tempi costanti, per annunciare la sua presenza:

```
(Header) Management frame type
BSSID:00:14:bf:fa:30:2d DA:ff:ff:ff:ff:ff:ff SA:00:14:bf:fa:30:2d Beacon frame (WIFID3) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 11
```

Figura 3.8: Beacon Frame

Le informazioni necessarie, estratte dal pacchetto, sono:

- *BSSID*, il MAC dell'AP monitorato
- il *DA*, che in questo caso, con il valore: *ff:ff:ff:ff:ff:ff,* indica che il pacchetto Beacon è stato mandato in Broadcast.
- il SA dell'AP che ha trasmesso il Beacon.
- il *subtype* del *Frame*, cioè l'identificativo del Beacon Frame con la relativa lettura del *SSID* (*WIFID3*), che, in questo caso, appare visibile; altri casi può essere stato nascosto dall'AP (*SSID invisible*) a fronte di specifica decisione dell'Amministratore
- Il tipo di *Modalità di connessioni supportato*, che in questo caso rileva, con l'*array* di valori da 1.0 MBit a 54.0 Mbit, un AP settato in *modalità 802.11g.*
- *Numero canale*, CH 11.

3.2.2.2 Probe Request

Pacchetto spedito in broadcast dal Device Mobile (DM) per ottenere la sincronizzazione all'AP.

```
(Header) Management frame type
BSSID:ff:ff:ff:ff:ff:ff DA:ff:ff:ff:ff:ff:ff SA:00:05:5d:25:1d:fa Probe Request (WIFID3) [1.0 2.0 5.5 11.0 Mbit]
946685177:823252 (109)
```

Figura 3.9: Probe Request Frame

Le informazioni necessarie estratte dal pacchetto, evidenziano:

- il SA del DM che ha trasmesso la richiesta di associazione
- il SSID dell'AP a cui il DM vorrebbe associarsi
- La modalità di connessione supportata dal DM, che in questo caso appare di tipo 802.11b essendo i valori contenuti nell'array compresi tra 1.0Mbit a 11.0Mbit.

3.2.2.3 Probe Response

Pacchetto inviato dall'AP in risposta al Probe Request per permettere la sincronizzazione e la conseguente associazione alla cella di connessione.

```
(Header) Management frame type
BSSID:00:14:bf:fa:30:2d DA:00:05:5d:25:1d:fa SA:00:14:bf:fa:30:2d Probe Response (WIFID3) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 11
```

Figura 3.10: Probe Response Frame

Le informazioni necessarie estratte dal pacchetto, sono le stesse evidenziate nel Beacon con l'aggiunta, in questo caso, del DA, in riposta al DM che aveva chiesto di essere associato a quel determinato AP.

In questo particolare caso si può notare che, anche se l'AP lavora in modalità 802.11g, sarà costretto a commutarsi alla modalità 802.11b, portando la sua velocità massima teorica da 54Mbit a 11Mbit.

3.2.2.4 Data

Paccheto di tipo Data scambiato tra l'AP e il DM.

```
(Header) Data frame type
DA:00:19:e3:07:d3:fe BSSID:00:14:bf:fa:30:2d SA:00:14:bf:fa:30:2b
```

Figura 3.11: Data Frame

Capitolo 4

Gestione canali radio e allocazione dei canali agli utenti

Il primo dei parametri che si ritengono significativi, per le motivazioni illustrate in ciascuna sezione, è quello relativo al Numero di Canale (frequenza) ed alla Allocazione del Canale agli Utenti, in termini di suddivisione di banda.

4.1 Gestione dei canali radio

Quando, all'interno di un edificio, vengono installate connessioni con diversi access point, dovrebbero essere assegnati canali sufficientemente distanziati gli uni dagli altri in modo tale da minimizzare le interferenze.

Gli AP 802.11b/g spesso utilizzano i canali 1, 6, e 11, mentre gli AP 802.11a utilizzano i canali 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, e 161. La gamma più ampia di canali disponibili che non si sovrappongono è la ragione per cui è possibile fare installazioni AP più ravvicinate per quelli

che seguono lo standard 802.11a. Per esempio, se si sono configurati tre AP 802.11g al primo piano, dovreste assegnare il canale 1 (sinistra), 6 (in mezzo) e 11 (destra), utilizzando tutti lo stesso SSID in modo tale che i client si possano connettere all'AP a loro più vicino e possano passare liberamente dall'uno all'altro. Se metteste altri tre AP al secondo piano, dovreste assegnare i canali 11 (sinistra) 1 (in mezzo) e 6 (destra) in modo tale che nessuna coppia di AP prima/dopo utilizzi lo stesso canale.

Per una buona configurazione della rete si potrebbe pensare di:

- assegnare ad ogni AP un suo SSID differente ma ciò forzerebbe gli utenti a scegliere a quale AP connettersi provocando una conseguente riduzione della velocità e la degradazione del segnale quando l'utente si allontana dall'AP, anche se si sposta verso un altro AP che può offrire un servizio migliore. Dovreste assegnare diversi SSID solo se desiderate realmente segmentare la WLAN, facendo in modo che alcuni utenti si connettano ad una SSID (per esempio "guest"), mentre altri utenti si connettono a diversi SSID (per esempio, "company").

- assegnare lo stesso canale a tutti gli AP, questo provocherebbe una competizione tra gli utenti per la stessa identica banda di frequenza, distribuendo tra tutti la banda disponibile in un singolo canale a 22 MHz invece di perdere il resto dello spettro. Inoltre, le collisioni si verificherebbero tra utenti di AP adiacenti quando ognuno cerca di trasmettere sulla stessa frequenza nello stesso momento. Queste collisioni hanno come risultato degli errori che richiedono delle ri-trasmissioni,

riducendo, quindi, l'efficienza. Quando ciò accade, alcuni AP possono essere configurati per ri-sintonizzarsi su un canale con meno rumore.

L'assegnazione dei canali senza interferenze rappresenta un reale problema nelle installazioni Enterprise con molti AP. Ad ogni AP è assegnato un canale in grado di trasportare una quantità di traffico finita quindi, ogni AP è in grado di supportare solo un certo numero di utenti. L'aggiustamento manuale dei canali AP è impraticabile, specialmente nelle grandi installazioni, perchè correggere un problema ne può provocare un altro. Per questo è utile fare un assegnamento ottimizzato dei canali, utilizzando algoritmi ad hoc.

Nell'esempio:

Figura 4.1: Ricezione simultanea dello stesso traffrico tra AP e DM

Il traffico che l'utente invia potrebbe essere ricevuto da entrambi gli AP, così come l'utente potrebbe ricevere i beacon da entrambi gli AP; il risultato è la degradazione della performance e la bandwidth disponibile risulta inferiore,

per via del numero di beacon "inutili", quindi da scartare, che l'interfaccia di rete di un utente riceve dall'AP "intruso".

Se gli AP sono troppo vicini fra loro o il medesimo canale è assegnato ad AP adiacenti, le performance decrescono esponenzialmente; questo è dovuto alle *interferenze* fra canali analoghi.

Il fenomeno delle interferenze rappresenta la principale difficoltà per un uso efficiente dello scarso spettro radio dedicato alle comunicazioni senza fili; queste possono essere causate da trasmissioni simultanee senza vincoli (usando lo stesso canale o canali limitrofi, come già accennato), che si risolvono in comunicazioni danneggiate, da dovere ritrasmettere, portando ad un più alto costo del servizio.

Tutto ciò giustifica la decisione di considerare, al fine di questo lavoro, il parametro del Numero del Canale, come significativo per la valutazione della qualità della rete.

Le interferenze possono essere eliminate (o almeno ridotte) per mezzo di adeguate tecniche di assegnazione del canale, attraverso algoritmi che fanno uso delle caratteristiche di perdita della propagazione radio per incrementare l'efficienza del "riuso" dello spettro e, quindi, ridurre il costo totale del servizio.

Gli algoritmi di assegnamento del canale ripartiscono lo spettro radio disponibile in un insieme di canali disgiunti che possono essere usati simultaneamente dalle stazioni, dal momento che mantengono un accettabile livello di segnale radio.

Utilizzando la caratteristica fisica della perdita della propagazione radio, lo stesso canale può essere riusato da due stazioni, nello stesso tempo, senza

interferenze (stazioni *co-canali*), tenendo conto del fatto che le due stazioni sono dislocate sufficientemente lontano. La distanza minima alla quale i co-canali possono essere riutilizzati senza interferenze è chiamata *distanza di riuso di co-canali* σ. D'altrone, i fenomeni di interferenza possono essere così forti che anche differenti canali, usati in stazioni vicine, tra loro possono interferire se i canali sono troppo vicini.

Poiché non sono disponibili filtri perfetti, l'interferenza tra frequenze vicine rappresenta un problema serio che può essere gestito aggiungendo frequenze "di guardia" tra canali adiacenti, o imponendo la separazione del canale. In quest'ultimo approccio, largamente seguito ed in genere preferibile in termini di banda occupata, i canali assegnati a stazioni vicine devono essere separati da un "*gap*" sullo spettro radio - contato in un certo numero di canali - che è *inversamente proporzionale* alla distanza tra le due stazioni. Il problema che tratta tale situazione è detto *channel assignment problem with separation* (CAPS).

In altre parole, i canali *f(u)* e *f(v),* assegnati alle stazioni u e v a distanza i, con $i < \sigma$, devono essere tali che $|f(u) - f(v)| \geq \delta i$, quando è richiesta una *minima separazione* di canale δi tra stazioni a distanza i. Il proposito degli algoritmi di assegnazione del canale è di assegnare canali ai trasmettitori in modo tale che la distanza di riuso dei co-canali ed i vincoli di separazione del canale siano soddisfatti e la *differenza tra il canale più alto e quello più basso sia tenuta più piccola possibile.*

Finora le grandi dimensioni delle celle (ed il loro limitato numero nelle singole realtà), dovute al costo di ricerca del sito di istallazione, degli apparati, ecc., hanno consigliato di assegnare piccoli valori alla *distanza di riuso.*

Per esempio, per il noto caso di assegnazione del canale "Philadelphia", valori realistici di *distanza di riuso* sono 3 o 4, mentre attuali valori di separazione sono 2 per stazioni a distanza 1 e valori uguale a 1 per stazioni con $2 \leq$ *distanza* $\leq (\sigma - 1)$ [16]. Comunque, il decremento del costo delle infrastrutture e la necessità di grande larghezza di banda, porterà ad una limitazione della grandezza delle celle ed all'aumento del loro numero, ciascuna con significativa potenza. In tale scenario, una *distanza di riuso* piccola non sarà più fattibile e σ dovrà essere molto più grande [17].

In tutti i casi, le soluzioni ottime sono fornite per mezzo di efficienti algoritmi di assegnazione del canale, basati spesso su tecniche di ricerca su grafi non orientati (di diverse tipologie) nei quali sono rappresentati le stazioni (vertici) e la loro adiacenza (spigoli che uniscono i vertici)[18][19][20][21].

Per tutte le reti, un canale può essere assegnato a ciascun vertice in un tempo costante, dal momento che la posizione relativa del vertice nella rete è nota. Nel caso contrario, i canali possono essere assegnati in parallelo ai vertici dopo l'esecuzione di un semplice algoritmo di distribuzione delle posizioni dei vertici, che richiede un tempo ottimo ed un certo numero di messaggi di "broadcast" tra i vertici stessi.

Una possibile configurazione ottimizzata dei canali, potrebbe risultare la seguente:

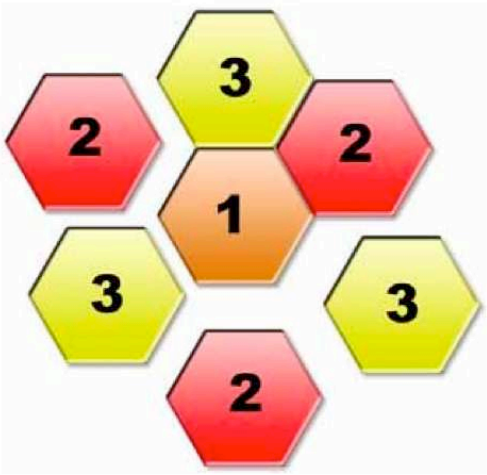

Figura 4.2: Esempio di assegnamento di canali

4.1.1 Test sul condizionamento della trasmissione WIFI

Al fine di trovare dei riscontri sperimentali a quanto affermato, si sono impostati 2 diverse serie di test, di seguito illustrati.

La situazione reale che si intende analizzare (Presenza di un nuovo AP in un ambiente di rete locale preesistene) è stata, ovviamente, simulata introducendo alcune ipotesi semplificative, per motivi di realizzabilità pratica, riguardanti il numero dei DM componenti la rete.

La simulazione è avvenuta, quindi, utilizzando la configurazione di seguito descritta, per ambedue i test (test-1 e test-2) descritti nei paragrafi successivi.

Sono state utilizzate due stazioni client così configurate:

- (Client1) PC Mac, con scheda WIFI AirPort Extreme (Atheros chipset)
- (Client2) PC Dell, D-Link DWL-660 WiFi 802.11b PCMCIA (ORINOCO chipset)

Ciascuna stazione è associata ad una rete WIFI di tipo 802.11b indipendente (AP 1 e AP 2) che rappresenta una la rete locale da monitorare, l'altra la nuova rete "aggiunta", configurata con i seguenti SSID:

- WIFID3, che rappresenta l'Acces Point 1 (AP1)
- OpenWrtDAV3, che rappresenta l'Acces Point 2 (AP2).

I router utilizzati per ciascuna delle due reti sono due Lynkys WRT54GS collegati, attraverso cavo ethernet (10/100), ciascuno ad un Server, realizzando, quindi, due reti locali indipendenti.

Più nello specifico la topologia di rete, creata ad hoc, per i due ambienti risulta la seguente:

Rete Locale 1:

Server Ubuntu (192.168.1.102) <–Ethernet–>AP1(192.168.1.4) <–WIFI–> Client Mac (192.168.1.100)

Rete Locale 2:

Server Ubuntu (192.168.1.101) <–Ethernet–>AP2(192.168.1.1) <–WIFI–>Client DELL (192.168.1.100)

La trasmissione del file utilizzato per generare traffico e monitorare i parametri voluti avviene utilizzando il Protocollo SSH e, nello specifico, il file trasmesso e relativa dimensione è il seguente:

32335300 Skype_2.6.0.184.dmg

I test sono avvenuti inviando, utilizzando *script* opportuni, simultaneamente sui due client verso il relativo server collegato alla rete più copie del file sopra citato.

Si sottolinea che le differenze di tempo di accesso su disco dei due client è da considerarsi scarsamente significative, quindi non influenzanti i riusltati delle prove.

Di seguito sono mostrate le frequenze adottate dai canali messi a disposizione, con le relative sovrapposizioni.

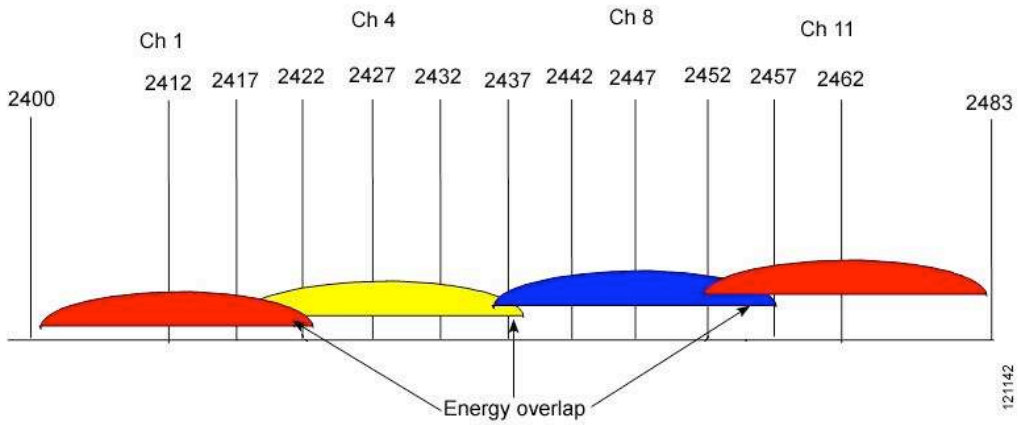

Figura 4.3: Frequenze canali con relative sovrapposizioni

4.1.1.1 Test1

Per valutare la degradazione delle comunicazioni si è considerato il tempo di trasmissione (ovvero la velocità) simultaneo dei file;

nella tabella che segue, per ciascun Client, sono indicati la velocità ed il tempo necessario per la trasmissione di 4 o più copie del medesimo file.

#Test	Client Mac	Client Dell	Note
1	**Ch 11** 671.9KB/s 00:47 686.5KB/s 00:46 686.5KB/s 00:46 686.5KB/s 00:46	**Ch 11** 493.4KB/s 01:04 493.4KB/s 01:04 493.4KB/s 01:04 501.2KB/s 01:03	Unico caso di send non simultanea, per mostrare la massima velocità di trasmissione raggiunta dai client
2	**Ch 11** 485.8KB/s 01:05 493.4KB/s 01:04 493.4KB/s 01:04 501.2KB/s 01:03	**Ch 11** 161.1KB/s 03:16 303.6KB/s 01:44 493.4KB/s 01:04 493.4KB/s 01:04	Nel client Dell il primo file viene condizionato interamente dall'invio del client MAC. Il secondo file viene invece condizionato solo in parte perchè intorno all'80% finisce l'invio del client Mac. I restanti file vengono inviati senza condizionamenti.
3	**Ch 1** 686.5KB/s 00:46 657.9KB/s 00:48 671.9KB/s 00:47 657.9KB/s 00:48 644.4KB/s 00:49 686.5KB/s 00:46	**Ch 11** 222.4KB/s 02:22 347.0KB/s 01:31 493.4KB/s 01:04 493.4KB/s 01:04	Condizionamento solo nel primo file inviato dal client DELL.
4	**Ch 2** 671.9KB/s 00:47 644.4KB/s 00:49 657.9KB/s 00:48 657.9KB/s 00:48 657.9KB/s 00:48	**Ch 11** 375.9KB/s 01:24 457.6KB/s 01:09 457.6KB/s 01:09 501.2KB/s 01:03	Lieve condizionamento solo nel client DELL.
5	**Ch 3** 657.9KB/s 00:48 657.9KB/s 00:48 644.4KB/s 00:49 631.6KB/s 00:50 607.3KB/s 00:52 671.9KB/s 00:47	**Ch 11** 328.9KB/s 01:36 478.5KB/s 01:06 501.2KB/s 01:03 501.2KB/s 01:03	Condizionamento nel client DELL e lieve condizionamento anche nel client MAC

6	**Ch 2** 287.1KB/s 01:50 319.0KB/s 01:39 306.6KB/s 01:43 261.0KB/s 02:01 239.2KB/s 02:12 319.0KB/s 01:39 281.9KB/s 01:52 265.4KB/s 01:59	**Ch 3** 58.2KB/s 09:03 83.3KB/s 06:19	Rilevante condizionamento su entrambi i Client
7	**Ch 3** 485.8KB/s 01:05 471.3KB/s 01:07 394.7KB/s 01:20 380.5KB/s 01:23 432.6KB/s 01:13 493.4KB/s 01:04 493.4KB/s 01:04 485.8KB/s 01:05	**Ch 3** 136.7KB/s 03:51 144.2KB/s 03:39	Si può osservare che, pur trovandoci a comunicare sul medesimo canale, il condizionamento appare meno rilevante rispetto a quello del test #6 dove l'assegnazione dei canali è differente.
8	**Ch 1** 535.2KB/s 00:59 563.9KB/s 00:56 574.1KB/s 00:55	**Ch 4** 6.1KB/s 1:18:10 ETA	Il client DELL, pur trovandosi su un canale differente, non riesce ad inviare il file.
9	**Ch 1** 415.5KB/s 01:16 332.4KB/s 01:35 332.4KB/s 01:35 335.9KB/s 01:34 358.8KB/s 01:28 493.4KB/s 01:04 485.8KB/s 01:05 444.8KB/s 01:11	**Ch 1** 82.0KB/s 06:25 168.9KB/s 03:07 162.8KB/s 03:14	Condizionamento su entrambi i client ma non così accentuato come nel test #8
10	**Ch 11** 671.9KB/s 00:47 644.4KB/s 00:49 619.2KB/s 00:51 657.9KB/s 00:48 631.6KB/s 00:50 619.2KB/s 00:51 619.2KB/s 00:51 631.6KB/s 00:50 701.7KB/s 00:45	**Ch 1** 235.7KB/s 02:14 464.4KB/s 01:08 493.4KB/s 01:04 493.4KB/s 01:04	Condizionamento solo durante l'invio del primo file nel client DELL.

11	**Ch 3** 471.3KB/s 01:07 444.8KB/s 01:11 464.4KB/s 01:08 380.5KB/s 01:23 385.1KB/s 01:22 363.0KB/s 01:27 358.8KB/s 01:28 371.5KB/s 01:25 354.8KB/s 01:29	**Ch 3** 121.5KB/s 04:20 105.3KB/s 05:00	Condizionamento su entrambi i client

Tabella 4.1: Test 1 sulla degradazione delle comunicazioni

Da notare come il Test #8 (ch1-ch4) risulti parecchio degradante per il client DELL che non riesce a spedire il file in tempi ragionevoli pur trovandosi ad una distanza (in termini di numero di canali) buona. Al contrario, nel Test #7 (ch3-ch3), pur avendo gli AP settati sul medesimo canale, il client DELL riesce ad inviare solamente due volte il file nello stesso tempo in cui l'altro client invia 8 copie del file.

Conclusioni Test-1

In primo luogo, si prende atto della migliore performance, a parità di standard della rete (802.11b), della scheda del client MAC in ragione dei driver ottimizzati e più recenti rispetto a quelli della scheda (ormai datata) del client DELL. Dai vari test effettuati (di cui sopra sono riportati i più significativi), si nota come sia evidente, in ogni caso, una degradazione delle comunicazioni anche con una distanza superiore a 3-4 canali e in, alcuni casi, l'assegnamento diverso dei canali non appare neppure come la scelta migliore.

Il miglior compromesso, dove è solo il client DELL a risentire, in un primo momento, dell'invio simultaneo dei file, è il caso dell'assegnamento ch1-ch11 con il client MAC che non risente di alcun condizionamento.

4.1.1.2 Test-2

In questo test è stata utilizzata la stessa configurazione di rete illustrata precedentemente, ma a differenza del test 1 (ove si valuta solo la velocità/ tempo di trasmissione del file), la degradazione è stata valutata intercettando i pacchetti di tipo "*Data*" trasmessi dal client Mac verso il Server Ubuntu e valutandone il tasso di ritrasmissione.

L'analisi è stata resa possibile apportando opportune modifiche al codice dell'applicazione *Kismet_ server*, per consentire il calcolo del numero dei pacchetti persi e della relativa percentuale sul totale della trasmissione.

Dai pacchetti intercettati si è analizzato il flag del frame IEEE 802.11 che indica appunto la ritrasmissione del pacchetto (Retry =1), nel caso in cui esso risulti perso:

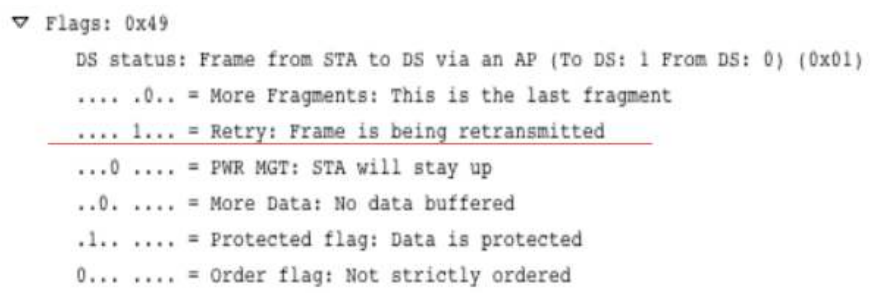

Figura 4.4: Flag del Retry Frame

Ai fini del test si sono monitorati:

- numero dei pacchetti totali trasmessi
- numero dei pacchetti ritrasmessi (numero di retry)
- tempo di trasmissione

ed è stata calcolata, di conseguenza, la percentuale dei pacchetti persi.

L'invio dei file dai due client (Mac e Dell) è avvenuto simultaneamente, come nel test precedente (Test-1), utilizzando un opportuno script.

In questo caso però, non si è reputato necessario mostrare nuovamente le degradazioni del client Dell ma si è preferito rilevare solamente quelle del client Mac, provvisto di scheda wifi con driver ottimizzati.

#Test	Mac send	Dati Pacchetti	Note - Ch
1	686.5KB/s 00:46 686.5KB/s 00:46 686.5KB/s 00:46 686.5KB/s 00:46	Trasmessi: 2069 Ritrasmessi: 14 Percentuale persi: **0.676655%** Tempo totale: **1.84** min	Unico caso di invio non simultaneo tra client Ch**11** Mac
2	478.5KB/s 01:06 471.3KB/s 01:07 471.3KB/s 01:07 478.5KB/s 01:06	Trasmessi: 2106 Ritrasmessi: 112 Percentuale persi: **5.31814%** Tempo totale: 4**.26** min	Ch **11** Mac- **11** Dell
3	607.3KB/s 00:52 686.5KB/s 00:46 686.5KB/s 00:46 686.5KB/s 00:46	Trasmessi: 1733 Ritrasmessi: 66 Percentuale persi: **3.63531%** Tempo totale: 1**.9** min	Ch **2 -11**
4	619.2KB/s 00:51 607.3KB/s 00:52 619.2KB/s 00:51 607.3KB/s 00:52	Trasmessi: 2242 Ritrasmessi: 255 Percentuale persi: **11.3738%** Tempo totale: 2**.06** min	Ch **3 - 11**
5	210.5KB/s 02:30 252.6KB/s 02:05 289.7KB/s 01:49 265.4KB/s 01:59	Trasmessi: 2893 Ritrasmessi: 686 Percentuale persi: **23.7124%** Tempo totale: **7.43** min	Ch **2 - 3**

6	315.8KB/s 01:40 464.4KB/s 01:08 444.8KB/s 01:11 350.9KB/s 01:30	Trasmessi: 1740 Ritrasmessi: 162 Percentuale persi: **9.31034%** Tempo totale: **4.89** min	Ch **3 - 3**
7	619.2KB/s 00:51 544.4KB/s 00:58 574.1KB/s 00:55 526.3KB/s 01:00	Trasmessi: 2092 Ritrasmessi: 44 Percentuale persi: **2.10325%** Tempo totale: **2.64** min	Ch **1 - 4**
8	426.7KB/s 01:14 457.6KB/s 01:09 332.4KB/s 01:35 335.9KB/s 01:34	Trasmessi: 2329 Ritrasmessi: 175 Percentuale persi: **7.51395%** Tempo totale: **4.92** min	Ch **1 - 1**
9	607.3KB/s 00:52 595.8KB/s 00:53 574.1KB/s 00:55 595.8KB/s 00:53	Trasmessi: 2282 Ritrasmessi: 282 Percentuale persi: **12.3576%** Tempo totale: **2.13** min	Ch **11 - 1**

Tabella 4.2: Test 2 sulla degradazione delle comunicazioni

Il grafico che segue mostra il livello di degradazione della comunicazione del client Mac, in relazione alla differente assegnazione dei canali nelle due reti indipendenti.

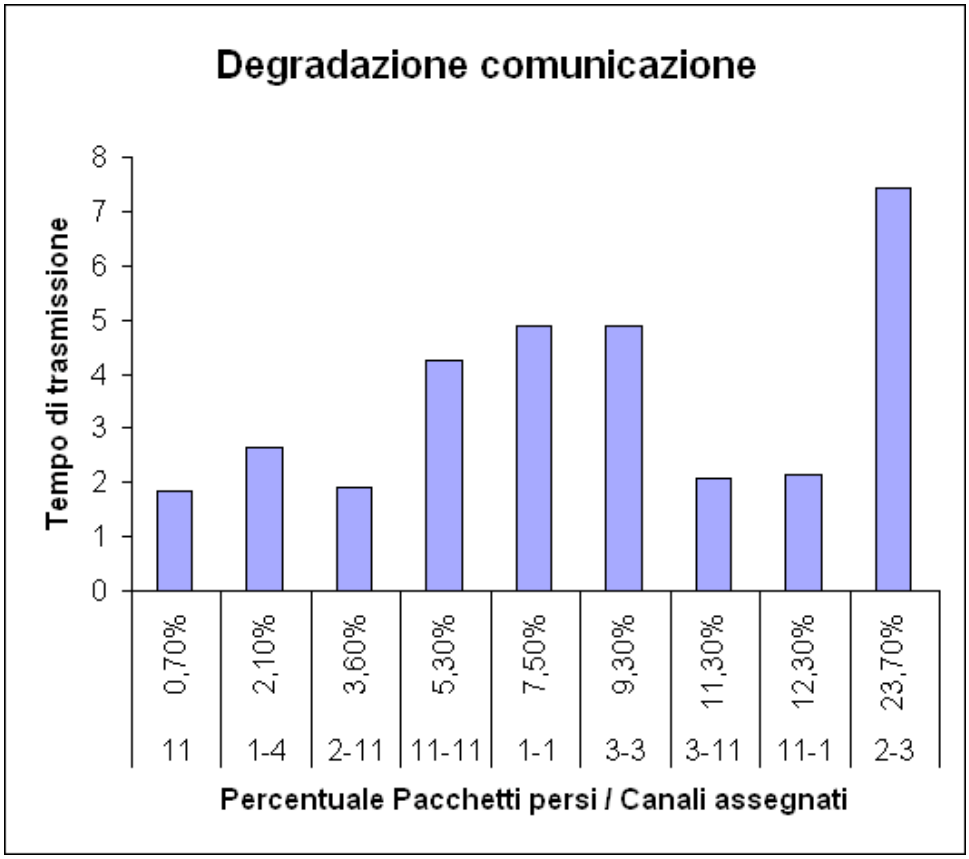

Figura 4.5: Grafico del livello di degradazione delle comunicazioni

Conclusioni Test-2

Come per il test precedente si nota che le degradazioni avvengono per ogni tipo di assegnamento, anche con distanze superiore a 4-5 canali. Inoltre si rileva come, anche in presenza di una perdita maggiore di pacchetti (caso 3-11 e 11-1) rispetto al caso di canali uguali o vicini, l'invio si dimostri più veloce, evidenziando l'importanza del parametro "assegnazione canale" (in termini di distanze tra canali). La maggior perdita di pacchetti non influenza molto sulla velocità di invio dei file se non in presenza di una percentuale molto alta di ritrasmissione e vicinanza di canali.

4.1.1.3 Conclusioni complessive sui test eseguiti

Alla luce dei due differenti test, si può affermare come ***non esista un assegnamento ottimo*** (privo di degradazioni) dei canali, sicuramente a causa della ristretta frequenza della *Banda ISM* (Industrial, Scientific and Medical) di 2.4 GHz e delle numerose interferenze (per ostacoli, rumore di fondo, rimbalzi del segnale, ecc.) presenti.

Importanza non secondatria la riveste, infatti, anche la qualità dell'harware e software della scheda di rete utilizzata, soprattutto per le loro capacità di filtraggio di rumori.

Si può concludere che, al fine del raggiungimento degli obiettivi prefissati dell'applicazione proposta e del presente studio:

per stabilire la natura ed i valori approssimati dei parametri significativi che suggeriscano all'amministratore una diversa politica di gestione della rete, a fronte del sopraggiungere di un nuovo attore AP

è indispensabile tenere conto di:

- numero canale
- percentuale pacchetti persi
- livello medio del segnale (che, come descritto nel capitolo 3 e specificatamente nel capitolo 6, rappresenta un buon elemento per giudicare le degradazioni della comunicazione) rilevato sui *beacon* inviati dall'AP esterno

per stabilire un

assegnamento del numero canale all'AP amministrato di una distanza di almeno 4-5 canali rispetto al "nuovo arrivato".

4.2 Allocazione dei canali agli utenti

Il problema dell'allocazione dei canali WIFI è stato affrontato anche in ambienti diversi dalla ricerca e dal settore tecnico-scientifico. Si può ipotizzare la situazione problematica di seguito descritta che, come illustrato successivamente, ha trovato anche pratiche attuazioni.

Un'attività commerciale vuole fornire ai suoi clienti la possibilità di usufruire di un'accesso WIFI. Poichè tale servizio è un valore aggiunto dell'attività, l'obiettivo è ottenere un alto livello di benessere sociale tramite uno schema di pagamenti che non sia esoso e che permetta a gran parte degli agenti (clienti), in relazione alle preferenze di ognuno di essi, di usufruirne. L' Access Point che fornirà il servizio ha, per ovvi limiti fisici, delle limitazioni al numero di connessioni contemporanee che può servire.

Tale problema è molto attuale ed è divenuto costume diffuso fornire servizi di collegamento WIFI in aereoporti, grossi centri commerciali, stazioni ferroviarie, etc. La fornitura di tale servizio non è l'attività primaria aziendale, per cui l'obiettivo non è esclusivamente ottenere il massimo profitto dai pagamenti che si e ricevono in cambio della fornitura del servizio, ma è soprattutto il far si che gli utenti siano soddisfatti. Nel caso di attività commerciali, il servizio WIFI costituisce uno di quei fattori denominato di "Surplus aziendale", ossia, quei servizi accessori che servono a rendere gradevole l'attesa o la permanenza degli agenti nelle attività commerciali e che

possono influenzare in maniera positiva la valutazione che i vari agenti hanno del servizio primario offerto.

Poichè il problema che stiamo affrontando nasce dal tentativo di trovare una soluzione ad una situazione reale si considerano, nella definizione del modello e nella ricerca della soluzione, vincoli che nella trattazione esclusivamente teorica non sono di fondamentale importanza: Tali vincoli sono:

- non si può supporre di utilizzare un qualche algoritmo che abbia un compito ben specifico, come fosse una "black box" e assumendo che esso esista e che abbia un certo tempo computazionale;
- i tempi d'esecuzione degli algoritmi proposti devono essere ragionevoli, poichè un tempo d'esecuzione troppo elevato avrebbe un effetto negativo per i clienti;
- il pagamento a cui deve essere sottoposto un utente dev'essere proporzionale al tempo di connessione ed alla banda ad esso allocata;
- l'algoritmo proposto deve essere a partecipazione volontaria, per cui un agente, disposto a pagare x per un'allocazione, paga un prezzo che è sicuramente inferiore o al più uguale ad x;

4.2.0.4 Descrizione del problema

L'obiettivo dell'algoritmo da progettare è la determinazione del prezzo da far pagare, ai vari utenti interessati al servizio, in relazione alla quantità di banda, ed alla durata dell'allocazione per essi determinata; le allocazioni e

i prezzi pagati per esse devono esser tali da rendere massimo sia il profitto, sia il benessere sociale dell'utente. Il problema diviene ancor più interessante, considerando che è divenuta una nuova moda fornire servizi Wi-Fi e, per molte attività commerciali, fornire o meno tale servizio può divenire un "surplus" necessario, ad esempio, per non essere emarginati dal mercato. Il servizio Wi-Fi è collaterale all'attività commerciale, ed il prezzo da fare pagare per esso non dev'essere esoso, poichè per essere un "surplus" dev'essere utilizzabile dai vari utenti ad un prezzo che sia adeguato ai loro interessi, e dev'essere tale che tutti gli utenti abbiano la possibilità di utilizzarlo evitando che vi siano agenti che monopolizzino un canale, rendendolo inutilizzabile a chiunque altro vi sia interessato. Nonostante ciò, non supporremo che le allocazioni siano preemptive, per cui ad un'agente non può essere revocato un canale, a lui allocato, in un momento arbitrario precedente al termine della durata di tale allocazione. L'arrivo degli utenti in un locale pubblico e, ancor di più, di quelli interessati alla connessione Wi-Fi è un evento prettamente casuale e non sono possibili assunzioni relative a distribuzioni di probabilità, differenti in funzione dei tempi di arrivo, che guidino il comportamento degli utenti. Poichè si vuole che ogni agente paghi un prezzo che sia legato in una qualche misura alla sua valutazione del servizio, e tale valutazione è differente per ogni agente, la determinazione del prezzo di vendita e del tempo di allocazione non può essere computata, senza una dichiarazione dell'agente circa la sua valutazione del servizio, ossia prima che esso non abbia effettuato un'offerta. Gli utenti interessati al servizio hanno un ampio range di possibili valutazioni, ovviamente conosciute solo a se stessi. Quando un utente decide di voler concorrere, per ottenere il collegamento Wi-Fi, effettua un'offerta e

l'algoritmo, che guida lo schema di allocazione dei canali gestibili dall'AP, ricevuta tale offerta, determina l'allocazione del canale all'agente (*durata temporale* e *pagamento*). Poichè gli agenti sono considerati *egoisti*, essi non necessariamente dichiarano un'offerta pari alla loro valutazione del servizio, se, mentendo, pensano di riuscire ad ottenere un qualche beneficio maggiore. L'obiettivo è fornire il servizio ai vari utenti in maniera tale che ogni agente massimizzi il proprio benessere, e la misura della loro soddisfazione dipende in maniera inscindibile dal prezzo pagato per il servizio. Quindi, la determinazione del prezzo di allocazione è fondamenetale per il conseguimento degli obiettivi da perseguire ed è necessario progettare un'algoritmo che induca gli agenti a dichiarare le loro reali valutazioni. L'algoritmo da progettare richiede un'impostazione online, poichè deve produrre risposte per ogni agente che si presenti, e le decisioni devono esser prese esclusivamente in virtù di ciò che è avvenuto precedentemente circa le allocazioni, senza alcuna conoscenza a priori sulle suddette che avverranno in un tempo successivo.

4.2.0.5 Soluzioni esistenti

Il problema è di natura pratica ed essendo diffusa, nell'ambito di varie tipologie di attività commerciali, la fornitura di connessioni Wi-Fi, esistono un'insieme di soluzioni già implementate per la realizzazione degli obiettivi illustrati. Le soluzioni, presenti sul mercato, al problema in analisi si possono riassumere in:

- **Servizio a Prezzo Fisso per unità di tempo**: le allocazioni sono

gestite in maniera indiscriminata ed i pagamenti sono basati su un prezzo fisso per unità di tempo.

- **Servizio gratuito**: le allocazioni sono analoghe a quelle precedenti ma il servizio non prevede pagamenti.

La *strategia a prezzo fisso per unità di tempo* non effettua considerazioni circa le valutazioni degli agenti, poichè questi pagano un prezzo fisso di connessione, indipendentemente dalle loro valutazioni. La determinazione del prezzo di connessione per unità di tempo è complessa, poichè se tale prezzo fosse troppo alto rischieremmo di mantenere inutilizzati molti dei canali a disposizione e se fosse troppo basso otterremmo un profitto basso.

Il *servizio gratuito* è, sicuramente, la soluzione che rende massimo il *benessere dell'utente*, ma rende complessa la gestione dei canali, perchè ogni agente, anche se poco interessato al servizio, tenterebbe di sfruttare la banda per il massimo tempo possibile. Inoltre, ciò richiederebbe una gestione preemptive delle allocazioni, con la possibilità di prelazionare il canale, deallocandolo ad un utente ed assegnandolo ad un diverso utente.

L'innovazione di *Starbucks* [22] (famosa catena di Coffe Bar presente negli Stati Uniti ed in diversi paesi Europei) è quella di aver definito una nuova strategia nella definizione dei prezzi di allocazione della banda. Non è stato definito un meccanismo che medi tra allocazione e pagamenti, ma l'innovazione consiste nel definire un insieme di possibili schemi di pagamento che incontrano le esigenze e i gusti delle varie tipologie di utenti che, potenzialmente, si può trovare a dover servire. Gli agenti, quindi, possono scegliere, tra un insieme di schemi di pagamento differenti, quello preferito ed utilizzare

tale schema per ottenere la connessione Wi-Fi. Lo schema di allocazione resta, comunque, indiscriminato e "non prelazionabile" quindi non si definisce alcuna tecnica per un'allocazione della banda che medi tra occupazione dei canali e desideri dei vari utenti. Inoltre, la banda è allocata, se disponibile, a qualunque utente si presenti in relazione allo schema di allocazione da esso scelto. L'idea base del sistema di pagamenti definito da Starbucks definisce una metodologia per la gestione dei pagamenti e delle allocazioni che si avvicini il più possibile alle esigenze dei vari agenti. In tale sistema, quindi, gli utenti (non effettuano delle offerte in base alle loro valutazioni, ma) utilizzano le valutazioni per scegliere uno tra gli schemi di pagamento disponibili all'interno dei piani tariffari determinati a priori. E' impensabile pensare di definire un insieme di schemi di pagamento che tenga conto dei gusti e delle valutazioni di tutti i possibili utenti, ma è previsto che qualcuno, comunque, si debba adattare a quanto presente. L'idea è la progettazione di un'*asta,* in cui ogni utente effettua un certo insieme di offerte ed, in base ad esse, si determina un'allocazione basata sulla disponibilità attuale di banda e sulle offerte degli altri utenti. Quindi, il problema si riconduce alla progettazione di un meccanismo d'asta che determini allocazione e pagamenti per i vari utenti partecipanti. Poichè gli agenti formulano le offerte in relazione alla loro valutazione del servizio e avendo supposto che tali utenti siano *egoisti*, il meccanismo dev'essere tale da costringere gli utenti a dichiarare le loro reali valutazioni quando concorrono all'allocazione della banda, e non siano incentivati a mentire, al fine di pagare un prezzo inferiore. L'obiettivo, quindi, si riduce alla progettazione di un meccanismo *truthful* e, più in particolare, un'*asta truthful,* riconducendo il problema alla progettazione di meccanismi

truthful online. Inoltre, ai nostri scopi, sarebbe interessante analizzare e considerare una definizione di *truthfulness* più forte, per la quale gli agenti devono essere incentivati a non mentire, sia circa le loro valutazioni, sia circa i loro tempi di arrivo.

4.2.0.6 Modello

Illustriamo, ora, le varie componenti del modello di riferimento che utilizzeremo per la ricerca della soluzione al nostro problema.

4.2.0.7 Condivisione della banda WiFi

L'accesso Wi-Fi, da un punto di vista prettamente fisico, non è assimilabile ad una connessione punto a punto, in quanto i dati, viaggiando nell'etere, non sono esenti da collisioni e ritardi; esso nella definizione del modello può essere considerato come un *multiplexing* di frequenze su di un link fisico. Il link fittizio a cui gli agenti possono connettersi è a disposizione di tutti, ma può accettare soltanto un numero limitato di connessioni contemporaneamente. La capacità del link e quindi il numero di connessioni contemporanee, può essere modellata in due differenti modi:

- come un insieme di k canali distinti e identici, con ogni agente interessato ad uno di essi
- come una quantitià $Q = 1$ infinitamente frazionabile (anche in misure diverse) ed ogni utente paga un prezzo proporzionale alla quantità di banda che il meccanismo decide di allocargli.

Le due formulazioni sono entrambe realistiche ed ampiamente sfruttate in letteratura per la definizione dei modelli relativi a problemi simili, anche se, in realtà, la prima formulazione è più diffusa perchè più semplice e realistica. Infatti, molti canali fisici non permettono che il multiplexing dei canali assegni quantità di banda differenti ai vari agenti, ma vincolano ad assegnare ad ogni agente una frazione identica della capacità del canale.

4.2.0.8 Valutazione degli utenti

I vari utenti hanno un insieme di valutazioni relative alle allocazioni dei canali e tali valutazioni sono conosciute solo a loro stessi. Le valutazioni possono essere viste come associazioni di prezzi a quantità di banda ricevute per un certo tempo.

4.2.0.9 Durata dell'allocazione

Poichè si desidera che la banda sia allocata, potenzialmente, a tutti gli agenti che sono interessati ad essa, è plausibile assumere che la durata delle allocazione sia limitata superiormente, e che non possa richiedersi banda per un tempo eccedente tale limite, definito dal gestore del meccanismo (l'AP). Denoteremo la durata di un'allocazione con Ti (i indica che tale tempo è relativo all'allocazione relativa all'i-esimo utente) , ed è tale che τ= [1,Tmax] e t $\in \tau$. Se la durata delle allocazioni viene considerata una quantità discreta avremo che τ = {1, . . . , Tmax }.

4.2.0.10 Gestione della banda

Un modello corretto per il meccanismo di risoluzione del nostro problema deve prevedere che, terminato il tempo di allocazione di un canale, esso torna disponibile per una successiva allocazione. Quindi, nonostante k sia una quantità finita, il ritorno in disponibilità, a fine allocazione, rende possibile considerarla alla stregua di una quantità illimitata. Considerando la banda come infinitamente frazionabile, indicheremo con q$i \in$ Q la quantità allocata all'i-esimo utente.

4.2.0.11 Notazione

Ogni utente effettua una o più offerte, esprimendo le sue preferenze circa l'allocazione, e, denoteremo con Vi l'insieme di valutazioni dell'utente i-esimo tale che Vi = {Vi (q1 , t1), . . . , Vi (qn , tn)} con Vi : Q x τ $\rightarrow\mathbb{R}+$ ad indicare la valutazione che l'agente i-esimo ha per una determinata quantità di banda allocatagli per un determinato tempo. Nel modello in cui la banda viene suddivisa in frazioni identiche della banda totale avremo Vi : τ $\rightarrow\mathbb{R}+$.

4.2.0.12 Offerte degli agenti

I vari utenti concorrono all'allocazione del canale attraverso delle offerte e, per determinare tali offerte, ricorrono alle loro personali valutazioni, conosciute solo da loro stessi. Denoteremo con bi il vettore di offerte dell'utente i-esimo tale che bi = {bi (q1 , t1), . . . , bi (qn , tn)} e, equivalentemente alle valutazioni bi : Q x τ $\rightarrow R+$ denoterà l'offerta dell'agente i-esimo per la

quantità di banda qj allocata per un tempo tj . Se la banda è suddivisa in k canali avremo bi : $\tau \rightarrow \mathbb{R}+$ in quanto la richiesta non dipende dalla quantità di banda allocata, poichè questa è suddivisa equamente tra i k canali e gli utenti effettuano offerte in maniera indistinta per uno qualunque di essi. Visto che siamo interessati ad aste di tipo truthful e, quindi, alla progettazione di meccanismi tali che le offerte fatte dall'agente i-esimo siano identiche alle sue reali valutazioni, abbiamo bi = vi.

4.2.0.13 Allocazione

Il meccanismo d'asta online dev'essere tale che, ricevuto il vettore d'offerta bi dall'agente i-esimo, decide se allocargli o meno un canale e, in caso affermativo, determina la durata di tale allocazione ed il pagamento da richiedere. Determinato il tempo di connessione dell'agente i-esimo, il canale viene allocato e diviene indisponibile per t istanti di tempo. Trascorso il tempo d'allocazione il canale torna disponibile e può essere assegnato ad una qualunque altro utente interessato. L'allocazione è denotata con Xi = (qi,* ti*, pi) o Xi = (t*i, pi), che sta ad indicare che all'utente i-esimo viene assegnato un canale (o una quantità di banda q*i) per un tempo t*i, ed il pagamento che tale utente deve effettuare è pi.

4.2.0.14 Considerazioni

Il problema modella una situazione in cui non vi sono strategie ottime di risoluzione e per la quale formalizzazioni differenti del modello possono portare a soluzioni diverse. Gli autori dell'articolo [23], infatti, analizzano tale difficoltà e, alla luce di essa non propongono soluzioni costruttive nuove, ma

"timidamente" affermano che l'unica soluzione plausibile è la ricerca di un'equilibrio *bayesiano di Nash*; essi però richiedono una cosa non da poco, cioè la conoscenza a priori della distribuzione di probabilità da cui sono derivate le valutazioni dei vari utenti. L'applicabilità di tale soluzione è. ovviamente, bassissima dal punto di vista concreto poichè non può assumersi, nella realizzazione di una qualche soluzione, nessuna distribuzione di probabilità che guidi il comportamento degli utenti, visto che si implicherebbe che gli utenti abbiano un comportamento pressocchè identico tra loro.

4.2.0.15 Soluzione proposta, K Aste identiche

Poichè la pratica di fornire l'accesso Wi-Fi come servizio accessorio è in notevole diffusione si potrebbe erroneamente pensare che la teoria delle aste stia trovando altissima applicazione in tale ambito. In realtà, la metodologia di tentare di far pagare per un bene un prezzo che sia adeguato al valore che l'utente associa col possedere tale bene non è ancora stata applicata in pratica. Le varie soluzioni adottate al problema, infatti, definiscono un prezzo fisso di connessione per unità di tempo (in genere il minuto) e tutti gli agenti interessati pagano quello stesso prezzo. La catena di bar Starbucks, è stata presa come punto di riferimento nell'analisi fatta precedentemente poichè è quella che ha dimostrato un maggior spirito d'innovazione, adottando uno schema di pagamenti versatile che permette di gestire le differenze tra i vari agenti, influenzando pagamenti e allocazioni per essi determinati. Ciò nonostante, tale approccio non è considerabile nell'ottica di un'asta e nessuno, allo stato attuale, ha adottato una soluzione che si ispiri alla teoria delle aste online.

Tale soluzione delle K aste identiche può essere pensata come un'evoluzione della soluzione a prezzo fisso e, ponendosi come obiettivo il perseguire una qualche forma di *benessere sociale* per l'utente, consiste nel definire un'asta per ognuno dei canali in cui il link *virtuale* tra l'AP e le stazioni mobili degli agenti è suddivisibile. Più in particolare, in tale impostazione il problema sta nel progettare un'asta per ogni possibile connessione l'AP possa accettare e, considerando k come il numero di canali messi a disposizione, definire k aste, una per ogni canale. Quando un utente è ammesso a partecipare ad un'asta, nel caso in cui vi sia un canale libero, l'agente effettua offerte utili alla determinazione del tempo di *allocazione* di quel canale ed al relativo pagamento da effettuare per una tale allocazione.

4.2.0.16 Algoritmo di Wrapping

Considerando il tempo una quantità discreta, quando l'utente i-esimo è interessato al canale non compete con altri agenti ma sottomette il suo vettore d'offerta bi, definito nella sezione 4.2.0.12. Tutte le offerte in esso contenute competono tra loro al fine di determinare un'allocazione (ti , pi), definito nella sezione 4.2.0.13. L'utente, quindi, è realmente e necessariamente disinteressato al comportamento degli altri partecipanti al gioco, poichè le sue offerte competono esclusivamente tra loro. L'algoritmo riportato di seguito definisce un semplice wrapper per la gestione delle k aste il cui unico compito è determinare un'associazione tra l'agente interessato ad un canale e una delle k aste, e determina il comportamento da seguire quando si presenta il vettore d'offerte dell'utente i-esimo. Tale algoritmo denota con $\boldsymbol{A}$ la generica asta per uno qualunque dei canali.

Algoritmo

if esiste almeno un canale libero **then**

esegui l'asta A sul vettore di offerte bi determinando (ti,pi). Alloca il canale dell'utente i-esimo per ti istanti di tempo e ricevendo un pagamento pi

else

rifiuta la richiesta di connessione e poni ti =0 e pi=0

end if

trascorsi i ti istanti di tempo di allocazione l'utente i-esimo rilascia il canale che torna disponibile per una nuova allocazione.

4.2.0.17 Asta a prezzo fisso

Si utilizza un qualunque meccanismo d'asta in cui viene fissato un prezzo fisso di connessione. Quindi, l'approccio consisterà nell'utilizzo di meccanismi online per la gestione dell'allocazione in cui il vettore d'offerta del singolo agente è visto per quello che esso realmente identifica, cioè una *singola richiesta di connessione*. In campo economico, le curve di fornitura e le curve di fornitura globale sono delle funzioni marginali, indipendenti dall'offerta, che determinano la quantità di beni da allocare ad un determinato utente ed il prezzo che per essi deve pagare. In un'ottica generale, tali curve sono adattive, poichè possono modificarsi in virtù delle allocazioni precedenti. Considerando, invece, un meccanismo in cui l'unico interesse è l'allocazione,

e, terminata essa, i beni tornano ad essere disponibili, otteniamo che l'adattività precedentemente menzionata non è necessaria e, una volta rilasciato il canale, per un agente che effettui una richiesta per ottenerlo può essere presentata la medesima curva di fornitura. Per cui, la curva di fornitura determina:

- se allocare o meno il canale all'utente
- per quanto tempo allocargli il canale
- il pagamento dovuto per una tale allocazione

Quindi, escludendo l'adattività dalle curve di fornitura, possiamo ottenere un meccanismo a prezzi fissi multipli efficiente e versatile.

4.2.0.18 Analisi

Poichè il fornitore del servizio (l'AP) ha interesse, nel tentativo di massimizzare profitto e benessere sociale, a far connettere il maggior numero di utenti possibile, può definire una curva di fornitura crescente, in modo tale che i primi minuti di connessione abbiano un prezzo di fornitura accessibile alla maggior parte degli utenti. Tra l'altro è perfettamente plausibile l'ipotesi che le funzioni d'offerta degli agenti siano decrescenti, supponendo un comportamento orientato a connettersi per pochi istanti di tempo, che sarebbe il comportamento plausibile di chi si connette ad Internet in un bar svolgendo le poche attività urgenti che gli necessitano. Poichè le k aste sono identiche e indipendenti l'una dall'altra, esse presentano, tutte e sempre, le stesse curve di fornitura. Per cui, per uno stesso vettore d'offerta $\mathbf{b}$ l'asta allocherà il

canale per il medesimo tempo e richiederà il medesimo pagamento. Quindi, il prezzo pagato da un offerente è indipendente dal tempo in cui arriva la richiesta, e quindi non vi è convenienza a ritardare un'offerta nella speranza di ottenere un'allocazione più vantaggiosa.

4.2.0.19 Considerazioni

Da quanto detto è semplice derivare vantaggi e svantaggi derivanti dall'applicazione di una tale metodologia. Il vantaggio principale deriva dal fatto che l'AP ottiene un profitto determinato esclusivamente dalla definizione della curva di fornitura e, quindi, dalla stima dell'interesse che gli utenti mostreranno verso il servizio che fornisce.

Lo svantaggio è evidente, e deriva dal fatto che non si è sviluppata un'asta vera e propria e, quindi, non si è creato un vero e proprio mercato. Per cui i prezzi non si adeguano in base alle precedenti allocazioni, e non tengono conto del livello di congestione della banda, considerando l'allocazione di un canale allo stesso modo, sia quando ve ne sono n occupati, sia quando sono tutti liberi, senza considerare le differenze che comporta una tale allocazione dal punto di vista trasmissivo; in realtà è solo la presenza di canali liberi a determinare la possibilità di fare *frequency hopping* nei link wireless, permettendoci di considerare la banda come un insieme di k canali distinti.

Capitolo 5

Rilevazione spostamento Utenti

In un ambiente di rete WIFI, in media, la banda varia in funzione della *lontananza* del DM (quindi dal suo spostamento determinato dall'analisi del livello del segnale) dall'AP; di conseguenza, all'aumentare di tale distanza, il servizio perde di efficienza e si va verso punti morti di bassa velocità o cessazione del servizio.

Ciò porta a considerare il livello del segnale, generalmente inversamente proporzionale alla grandezza *lontananza*, *come uno dei parametri fondamentali da monitorare ai fini dell'analisi qualitativa di una rete WIFI.*

Nelle sezioni che seguono sono descritte:

- alcune delle soluzioni, presenti in letteratura, che riescono a monitorare in maniera sufficientemente precisa lo spostamento degli utenti nella rete e la loro localizzazione;
- una proposta di soluzione personale, presente nell'Applicazione di Mo-

nitoraggio degli Spostamenti descritta e realizzata in alcune parti, di volta in volta evidenziate.

5.1 Tecniche di Localizzazione

Lo sviluppo delle architettetture WLAN si sta dirigendo verso velocità sempre più alte grazie all'utilizzo di schemi di modulazione sempre più complessi. La complessità di tali schemi rende la comunicazione sensibile alle interferenze causate dalla non idealità dell'ambiente esterno. Quest'ultimo può essere caratterizzato in due modi distinti:

- *Indoor*; rappresenta l'ambiente interno agli edifici, costituito da uffici, stanze, etc. In un ambiente di questo tipo le interferenze sono molteplici e di vario tipo a causa della variabilità dell'ambiente che può contenere oggetti caratterizzati da vari materiali e dimensioni.

- Outdoor; rappresenta l'ambiente esterno agli edifici, anch'esso caratterizzato da una estrema variabilità dovuta alla densità delle abitazioni, alla loro posizione, alla presenza di vegetazione e a tutti gli oggetti che possono essere incontrati all'esterno degli edifici.

I modelli che descrivono la propagazione del segnale possono essere fondamentalmente divisi in due categorie :

- *Large scale propagation models*, modelli che predicono il valor medio della potenza del segnale ricevuto, danno una stima della copertura del segnale radio da parte di un trasmettitore, viene infatti presa in

consideranzione, la potenza del segnale ricevuto su distanze e tempi grandi rispetto alla durata delle oscillazioni che possono essere presenti.

- *Small scale propagation models;* modelli che predicono le rapide fluttuazioni che la potenza del segnale può assumere quando viene fatta un'analisi o considerando piccole variazioni spaziali e/o temporali.

La differenza fra queste due famiglie risiede nella scala di osservazione della potenza del segnale ricevuto, i parametri di spazio e tempo su cui la media viene eseguita, risultano determinanti per la scelta del modello; i *large scale propagation models* adottano spazi e tempi di osservazione che assorbono le rapide fluttuazioni della potenza del segnale ricevuto, mentre i *small scale propagation models* prendono in considerazione spazi e tempi tali da permettere l'analisi delle rapide fluttazioni della potenza del segnale ricevuto.

Le soluzioni più diffuse per la localizzazione deglio utenti sono basate sull'elaborazione dell'intensità del segnale [24]. A tale proposito in campo scientifico esistono realizzazioni basate sul modello Empirico e sul modello a propagazione sopra citato.

- Il *modello empirico* è basato sulla memorizzazione a priori, in un database, di informazioni sul segnale (quale l'intensità del segnale dagli Access Point), relativi a diversi punti scelti in una cosiddetta "radio map", costruita prima che il processo di posizionamento inizi. Quando un dispositivo in una posizione sconosciuta richiede la localizzazione, si raccolgono le informazioni sul segnale dai vari AP e sono inviate al database per la comparazione. Un algoritmo opportuno ricerca l'entry

nel database con i valori più prossimi a quelli del dispositivo (eventualmente mediando i valori tra più entry trovate), dichiarandolo come posizione del dispositivo stesso. Un tale modello presenta due svantaggi principali: l'onere di costruire la radio-map (ed il relativo database) e la perdita di accuratezza del sistema allorché le condizione ambientali correnti sono diverse rispetto a quelle esistenti al momento della creazione del database (ad esempio per la presenza di oggetti nuovi, quali persone, ecc.). Una maggiore sofisticazione del modello può prevedere la creazione di diverse radio-map, in ragione di varie condizioni previste.

- Il *modello propagazione,* generalmente più flessibile rispetto al modello precedente, è basato sul fatto che quando un'onda radio viaggia in un ambiente perde segnale e l'intensità del segnale è dipendente dall'ambiente. La perdita di intensità di segnale può essere modellata utilizzando le teorie note sulla propagazione delle onde radio ed il "path loss". Secondo tali teorie, la distanza tra un dispositivo wireless ed un Acces Point può essere calcolata, dato il valore della perdita di intensità del segnale ricevuto. A questo punto, avendo la distanza di un device da tre o più access point, mediante metodi di triangolazione si ottiene la posizione del device stesso. Poiché la localizzazione è calcolata solamente utilizzando le distanze relative dagli Access Point circostanti, il sistema è in grado di lavorare in un qualunque ambiente in cui sono note a priori le posizioni degli access point stessi. Uno svantaggio di tale modello è relativo alla difficoltà di ottenere, da parte del sistema

di posizionamento, precisi valori di pathloss dagli *Access Point*; è necessario una accurata progettazione dei dispositivi hardware e software per limitare tale difficoltà. Un altro problema è relativo al fatto che l'accuratezza del posizionamento decresce con l'aumentare della distanza tra il device da posizionare ed il relativo *Access Point,* dovuto alla presenza di altri fattori (ad. Es: differenze di umidità) che influenzano il percorso di onde radio su lunghe distanze. Si può limitare tale problema ed aumentare l'accuratezza del posizionamento conferendo, ad esempio, maggior peso nell'algoritmo di triangolazione all'Access Point definito primario (ad esempio quello con il minore valore di path loss).

5.1.1 RADAR

Il *RADAR*[25] *Project* (finanziato da Microsoft) è uno dei primi progetti nato per la localizzazione della posizione degli utenti nelle reti Wireless LAN; basato sull' utilizzo di Radio Frequenze (RF), ha di fatto rappresentato il modello metodologico per i progetti venuti dopo. L'infrastruttura considerata è un WLAN, basata sullo standard 802.11/a/b/g. Le stazioni fisse e di posizione nota sono quindi gli AP mentre i terminati mobile sono dotati di una scheda WLAN.

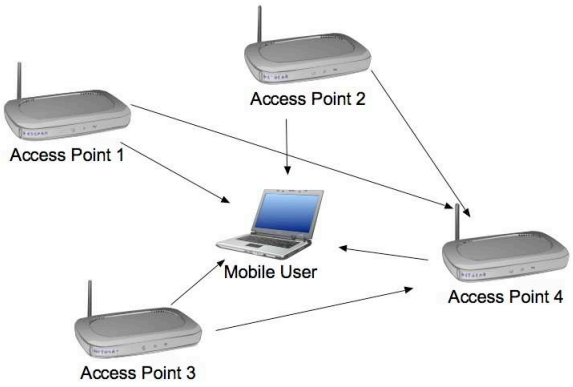

Figura 5.1: Radar

Questo sistema differisce da altri in quanto si prefigge di essere "nn invasivo" rispetto all'infrastruttura di comunicazione. In altre parole, non vi deve essere necessità di una strutturazione dell'ambiente confacente alle sue necessità, bensì deve essere adattabile al luogo nel quale si trova a lavorare.

Il Sistema combina due modelli, progettati separatamente, ma testati e comparati assieme:

Nel Modello Empirico, viene utilizzata l'informazione del livello del segnale e il rapporto Segnale-Rumore. I punti noti prescelti sulla "mappa radio" sono memorizzati in un database attraverso le loro coordinate (x e y) ma anche le direzioni (Nord, Sud, Est ,Ovest) rispetto le Base Stations. La posi-

zione dei punti sconosciuti si determina (applicando un algoritmo di ricerca dei k-nearest neighbour) confrontando con le posizioni conosciute presenti nel DataBase.

Nel Modello a Propagazione, si utilizza la Wall Attenuation Factor (*WAF)* per calcolare le distanze usando il "path loss" .

$$P(d)[dBm] = P(d_0)[dBm] - 10n\log(\frac{d}{d_0}) - \begin{cases} nW * WAF & ,nW < C \\ C * WAF & ,nW \geq C \end{cases}$$

dove:

- n indica il tasso al quale il path-loss aumenta con la distanza
- *P(d0)* è la potenza del segnale ad una certa distanza di riferimento *d0*
- d è la distanza tra il trasmettitore ed il ricevitore
- C è il numero massimo di ostruzioni fino al quale sono significative differenze del fattore di attenuazione
- nW è il numero di ostruzioni tra il tramettitore ed il ricevitore
- WAF è il fattore di attenuazione del muro che ostruisce

n e WAF dipendono dall'architettura dell'ambiente e dai materiali di costruzione utilizzati e sono stati derivati i maniera empirica. Sono stati scelti valori di n= 1,523 e p(d0)=58,48 dBm come valori simili per tre Access Point utilizzati, a prescindere della loro collocazione fisica. I risultati pubblicati indicano un errore di stima di 2,94 metri per il modelloempirico e di 4,3 metri per quello a propagazione.

5.1.2 Awp

L'*Advanced Wavelan Position Project* [26] è un progetto di un gruppo di studenti della Lulea University of Technology che ha lo scopo di sperimentare nuovamente, anche se con alcune modifiche, sia l'approccio sperimentale che quello a propagazione di RADAR. Nell'approccio empirico, l'unico parametro preso in considerazione è il livello del segnale, in quello a Propagazione si usa una versione semplificata dell'equazione della WAF. Interessante, nel progetto, la possibilità, tramite una interfaccia, di posizionare ostacoli o ambienti nella mappa. I risultati, nel modello a propagazione, sono stati di errori di posizionamento tra 2,8 e 7,3 metri.

5.1.3 Amulet

L'*Amulet* [27](Approximate Mobile User Location Tracking System) *Project* è un progetto che fa uso di modello empirico simile a quello proposto da RADAR. Realizzato da Blake M. Harris, nella Università di Rochester, USA, in ambiente Linux, è composto da moduli che interagiscono tra loro: l'Access Point Statistical Recorder (APSR) che memorizza continuamente le informazioni sul segnale dagli Access Point, il Nerest Neighbour Association Module (NNAM) che implementa il solito algoritmo k-nearest neighbour di RADAR sui dati passati da APSR, il Map GUI che semplicemente visualizza i punti della radio map e la locazione dei device. La "Signal Quality", le informazioni sul segnale raccolte durante la costruzione del database, hanno portato a posizionamenti con una risoluzione dai 3 ai 5 metri.

5.1.4 Halibut

Halibut [28]è un progetto della Stanford University (USA) che utilizza il modello a propagazione esclusivamente per il posizionamento; esso considera i vari fattori che influenzano la propagazione delle onde radio includendo l'attenuazione del segnale, la diffrazione, il multi-path fading ed una variabile random per una modellazione di tipo "log-normal shadowing", utilizzando una equazione simile al WAF usata nel RADAR project.

5.1.5 Ekahau

Ekahau Postioning Engine[29], risultato di dieci anni di ricerca, si tratta di un tool di posizionamento di LAN Wireless, commercializzato in ambiente Windows e su diverse altre piattaforme. Sfruttando la tecnica di triangolazione incrementale, consente ad una qualiasi rete Wireless a Stamdard 802.11a/b/g, implementata o in fase di implementazione, di trasformarsi in un vero e proprio sistema di localizzazione dinamico con un'accuratezza di un metro. L'alta accuratezza combinata con una bassa latenza ed un veloce aggiornamento permettono una ricerca affidabile nelle applicazioni che la richiedono. Attraverso questo potente strumento è possibile creare dei modelli di posizionamento, tracciare la posizione di dispositivi wifi associati alla rete oltre ad analizzare l'accuratezza delle coordinate.

Fa uso sia del modello empirico che di quello a propagazione ed è formato da tre moduli: Ekahau Client, Ekahau Manager e Positioning Engine. Viene utilizzata una tecnica Client-Server: il dispositivo mobile (Client) rileva le intensità dei segnali emessi dagli access point e li trasmette al dispositivo di

rete fisso, Ekahau Manager (server di localizzazione). Questo, ricevuti i dati dal dispositivo, utilizzando la Mappa Radio che ha in memoria, determina, mediante il modulo Positioning Engine , la posizione dell'utente con un errore di circa 1-2 metri e memorizza i dati di calibrazione. L'approccio basato sulla calibrazione della forza del segnale e' radicalmente differente dalle altre tecniche commerciali, che si basano soprattutto sulla propagazione del segnale e sul calcolo della triangolazione per calcolare la locazione.

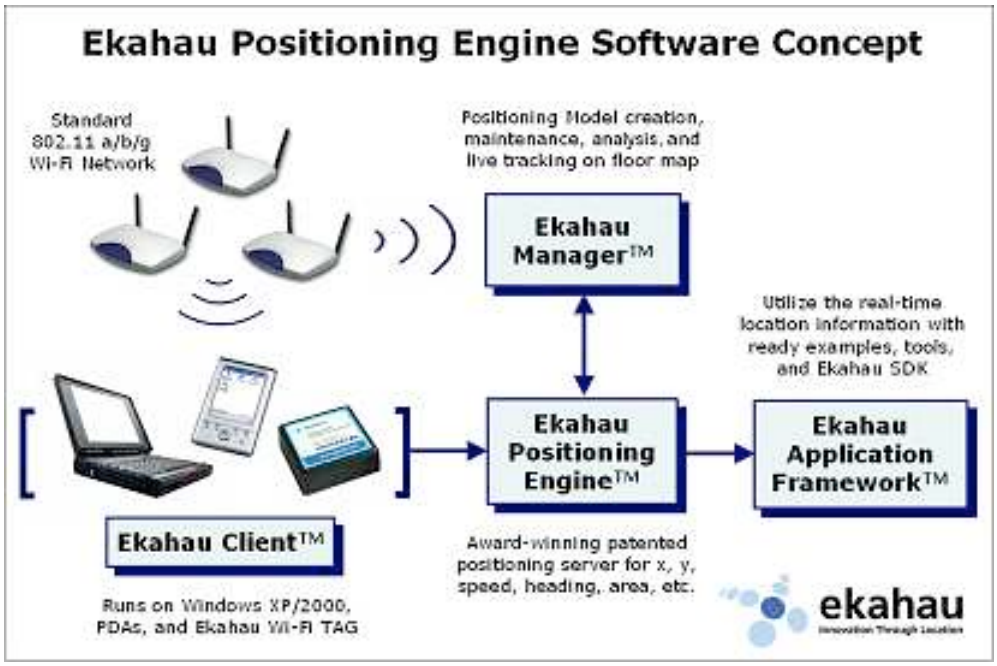

Figura 5.2: Ekahau

Compilando un form sul sito dell'Ekahau (http://www.ekahau.com) è possibile avere il trial gratis solo per sistemi operativi Microsoft Windows.

5.1.6 Skyhook

Shyhook è una società americana che da alcuni anni propone una valida alternativa urbana al GPS posizionando in rampa di lancio per il grande mercato Skyhook Wireless promettente software WPS, acronimo di Wireless Positioning System. Attraverso la triangolazione dei radiosegnali WiFi, Skyhook propone un metodo di localizzazione preciso ed esplicitamente pensato per le grandi città. Il suo funzionamento è facile e, vista la grandissima diffusione dei dispositivi WiFi, il successo del WPS sembra quasi garantito. Negli scorsi mesi la Skyhook ha creato dettagliate mappe di 25 tra le più grandi metropoli statunitensi: mappe particolarissime, che tengono conto delle coordinate geografiche di tutti gli hotspot 802.11 sparsi per i quartieri. La potenza del WPS sta tutta nella sempre maggiore diffusione del WiFi sul tessuto urbano americano: al momento del lancio, uno speciale client aggancia il segnale dei router wireless più vicini, ciascuno precedentemente registrato all'interno del databae Skyhook. Dalla comparazione tra la distanza dei vari hotspot, memorizzati singolarmente con un codice univoco, WPS riesce a triangolare la posizione geografica dell'utente. L'invenzione di Skyhook offre una precisione maggiore del GPS, che entra in crisi ovunque vi sia un'alta densità di edifici. Il segnale WiFi è molto più denso di quello satellitare e dovrebbe garantire un margine di precisione pari a circa 20 metri. Se WPS viene utilizzato in luoghi densamente abitati ed urbanizzati con una elevata concentrazione di punti d'accesso WiFi, la nuova tecnologia potrebbe fornire un'accuratezza senza pari.

5.2 Applicazione di Monitoraggio degli Spostamenti

La funzionalità di rilevare, attraverso l'algoritmo descritto, gli spostamenti degli utenti presenti nella rete WIFI diviene utile per due scopi:

- *informativo*; per capire dove un determinato utente si trova
- *qualitativo*; per valutare, tenendo traccia delle posizioni in media *preferite* dagli utenti, se aggiungere o rimuovere un AP.

L'algoritmo viene applicato tenendo presente due prerequisiti essenziali:

- conoscenza della posizione assoluta degli AP su una mappa data
- localizzazione in un ambiente ideale, senza ostacoli ed interferenze

Ogni AP monitora il livello del segnale di ogni DM presente nella sua area e invia l'informazioni al Server Centrale. L'applicazione progettata utilizza l'agoritmo di localizzazione degli spostamenti (realizzato e descritto nella sezione successiva) prendendo in input i dati sul livello del segnale del determinato DM, inviati da almeno due AP.

Essendo nota la posizione degli AP e analizzando il livello più o meno alto del segnale, si può ricavare la posizione relativa dello specifico DM.

Per esempio, se il dato sul livello del segnale inviato dall'AP1 risulta di volta in volta sempre più basso mentre quello dell"AP2 più alto, significa che il DM si sta spostando verso la zona dell"AP2 e viceversa. Più AP sono presenti più accurata è la localizzazione dell'utente (avendo a disposizione

più dati da confrontare), considerando sempre che l'utente si sta spostando verso l'AP che lo rileva con un livello di segnale più forte. Nell'analisi del problema si è evidenziato un caso particolare in cui, se entrambi gli AP rilevano un analogo innalzamento o abbassamento del livello del segnale, ci possiamo trovare in due differenti situazioni:

- non siamo in presenza di uno spostamento fisico del DM nell'ambiente, ma di una variazione del livello generato dallo stesso DM.
- due AP si trovano perfettamente in perpendicolare sul DM, di conseguenza entrambi rileveranno, durante il movimento del DM, la medesima variazione del livello del segnale.

5.3 Algoritmo di localizzazione degli spostamenti proposto

Come già illustrato i parametri qualititavi utilizzati dagli algoritmi proposti sono desunti dall'elaborazione dei file *.pcap* prodotti da *Kismet_Server*. Questo è valido per tutti i parametri utilizzati escluso quello riguardante il livello del segnale che, pur essendo rilevato da taluni AP (come descritto nella sezione 6.1), non viene salvato da *Kismet_Server* in formato *.pcap*.

E' stato quindi necessario modificare il codice di *Kismet_Server* (più precisamente il file *kismet_server.cc* - presente all'interno del *Server*), che riceve il flusso e processa i pacchetti ricevuti da *Kismet Drone* (presente all'interno della Fonera).

Le motivazioni della scelta dell'*AP Fonera* utilizzato sono esaurientemente descritte nel capitolo 6, dedicato alla descrizione dell'ambiente di test.

I pacchetti monitorati sono quelli diretti dal *DM* (*Device Mobile*) all'*AP Router*; la Fonera, posizionata accanto all'*AP Router*, inserisce in ogni pacchetto monitorato l'informazione sul livello del segnale che viene poi utlizzata dall' applicazione realizzata.

All'interno del sorgente *kismet_server.cc*, è stato intercettato il punto in cui vengono processate le informazioni sui singoli pacchetti ed estrapolato il dato sul livello del segnale.

L'analisi viene fatta sui Device Mobili (DM), identificati univocamente dal MAC, che l'amministratore vuole tenere sotto controllo e che vengono aggiunti nel file di configurazione *MacMobileInNetwork.xml* nel seguente il formato:

<ApInfo>

<mac>00:17:D3:07:D3:FE</mac>

<mac>00:19:E3:07:D3:FE</mac>

<mac>00:05:5D:25:1D:FA</mac>

</ApInfo>

Il file XML viene "parsato" una prima volta al lancio di *Kismet_Server* e la lista dei MAC dei DM da voler monitorare viene inserita nell'apposita struttura dati.

Ai fini dell'algoritmo, il livello del segnale viene estrapolato dai pacchetti di tipo DATA inviati dal DM verso L'AP router. Il router Fonera, adibito al monitoraggio, viene posizionato accanto al'AP router in modo tale che possa inserire l'informazione del livello del segnale rilevato del pacchetto più accurata possibile. La figura che segue mostra una parte dell'ambiente di test del sistema di monitoraggio che verrà poi descritto più diffusamente nel capitolo 6.

Figura 5.3: Posizionamento Fonera

Durante i test sul monitoraggio del livello del segnale, la prima cosa che si è evidenziata è stata l'enorme variabilità del valore del livello stesso. Per esempio, nel caso, apparentemente ottimo, in cui il DM è fermo e posizionato accanto all'AP (senza alcun ostacolo frapposto tra loro), i valori del segnale non sono apparsi costanti nel tempo (dell'ordine di alcuni secondi di traffico) o di poco diversi l'uno dall'altro, bensì, in maniera forse inaspettata, comprendenti significative variazioni tra loro.

Per esempio, una rilevazione tipica su 10 pacchetti inviati nelle condizioni suddette è stata:

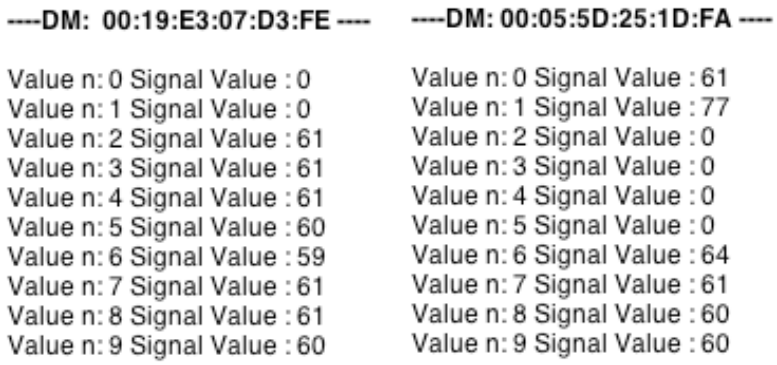

Figura 5.4: Esempio di valori del segnale anomali

La presenza di valori molto bassi, talvolta anche molto alti, che si discostano in maniera rilevante dai valori medi del segnale monitorato, ha portato alla necessità di progettare un algoritmo che limiti il più possibile questi fenomeni, limitandone quindi il condizionamento, per calcolare il conseguente spostameno, o meno, del DM su dati maggiormente affidabili.

In sintesi, la procedura di filtraggio dei valori rilevati proposta consiste nei seguenti punti:

- Rilevamento, tramite le opportune modifiche al codice di *Kismet_ Server,* del livello del segnale per ogni DM monitorato, inserendo le informazioni ottenute nella opportuna struttura dati

  Si è definito un buffer di tipo Vector formato da tanti elementi quanto sono i DM da monitorare, identificati dal loro MAC; ciascun elemento è formato da una struttura

  con un campo di tipo array, opportunamente definito, preposto a contenere i valori del segnale.

- Calcolo Mediana dei valori del livello del segnale, rilevati in un numero prefissato di pacchetti consecutivi

  La mediana di un insieme di valori ordinati, in modo crescente o decrescente, dà un'idea di quello chè è il valore "di posizione centrale", quindi più lontano da valori anomali, per eccesso o difetto. Il calcolo della mediana, attraverso la nota formula, risente meno, rispetto alla media aritmetica, di valori "errati".

  Il numero dei pacchetti considerati, parametrizzabile attraverso il file di configurazione .XML (nei test considerato uguale a 10), deve tenere conto del volume di traffico; un numero troppo elevato in presenza di poco traffico (e quindi pochi pacchetti nell'unità di tempo considerata) porta ad un "ritardo" elevato nella stima dello spostamento; viceversa, un numero troppo basso, sempre in presenza di poco traffico, rende i valori calcolati poco significativi. Il discorso diventa meno critco in presenza di volumi di traffico piè elevati, per i quali il parametro dei numero dei pacchetti può essere significativamente aumentato. E' ovvio che una situazione di elevato traffico migliora l'accuratezza della stima dello spostamento effettuata.

- Calcolo Percentuale di filtraggio (*deltavalue*)

  Sperimentalmente si è stimato che una percentuale del 20% (valore parametrizzabile nel file .XML di configurazione) di scostamento dalla mediana dei valori rilevati costituisce un buon criterio per filtrare i livelli del segnale.

- Calcolo dei valori da Filtrare

Una semplice formula, applicata ai valori rilevati e conservati nella opportuna struttura, consente di filtrare i dati ritenuti errati, dovuti ad interferenze o risposte particolari del driver dell'AP Fonera (ad esempio per i valori uguali a 0):

Per ogni Valore i

*se (abs(mediana - valore[i]) > deltavalue*k)*

allora RimozioneValore

altrimenti ValoreAccettato

Il fattore k può consentire una maggiore raffinamento del filtraggio.

- Calcolo Varianza e Media dei valori filtrati

  La varianza risulta essere una misura della dispersione degli n (con n<=10) valori rilevati e filtrati; ovvero maggiormente differenti sono i valori ottenuti e maggiore sarà il valore della varianza. Per l'appunto è chiamata anche indice di dispersione poiché offre una indicazione sull'addensamento dei valori della variabile attorno al valor medio. Se dunque abbiamo una varianza alta in un insieme di pacchetti, vuole dire che ci sono valori molto differenti fra di loro; ciò può essere considerato indicativo del fatto che il DM è in movimento. Viceversa se la varianza ha un valore basso, i valori ottenuti sono pressoché equivalenti, dunque i vari DM possono essere considerati non in movimento. Sperimentalmente, nelle condizioni ambientali specificate nel Capitolo 6, un valore di varianza minore di 3 (valore parametrizzabile nel solito modo) ci fa stimare i DM fermi.

- Identificazione possibile spostamento in relazione al valore della Varianza, in caso di Varianza sopra il limite considerato.

  In caso di varianza oltre il limite fissato, si stima la natura del movimento (in avvicinamento all'AP o in allontanamento) effettuando un confronto tra i valori medi dei segnali rilevati dei vari insiemi di pacchetti. Se tra un insieme ed il precedente la media dei valori risulta crescente, allora in quello settore temporale si identifica un movimento di avvicinamento del DM verso l'AP; viceversa siamo in presenza di un allontanamento.

Le informazioni di monitoraggio del livello del segnale e il conseguente risultato sul movimento o meno da parte dei DM, viene memorizzato in un apposito file di log.

Di seguito viene mostrato un frammeto di file con l'output generato dove sono evidenti i valori che portano alle conclusioni sopra descritte:

----DM: 00:19:E3:07:D3:FE ----

Value n: 0 Signal Value : 62
Value n: 1 Signal Value : 62
Value n: 2 Signal Value : 59
Value n: 3 Signal Value : 63
Value n: 4 Signal Value : 60
Value n: 5 Signal Value : 61
Value n: 6 Signal Value : 60
Value n: 7 Signal Value : 62
Value n: 8 Signal Value : 59
Value n: 9 Signal Value : 60

Varianza: 1.95556
Media livello segnale : 60.8
Il terminale mobile risulta:
FERMO

---DM: 00:05:5D:25:1D:FA ---

Value n: 0 Signal Value : 0
Value n: 1 Signal Value : 0
Value n: 2 Signal Value : 0
Value n: 3 Signal Value : 83
Value n: 4 Signal Value : 62
Value n: 5 Signal Value : 64
Value n: 6 Signal Value : 63
Value n: 7 Signal Value : 61
Value n: 8 Signal Value : 59
Value n: 9 Signal Value : 62

Varianza: 2.96667
Media Livello Segnale : 61.8333
Il terminale mobile risulta:
FERMO

----DM: 00:19:E3:07:D3:FE ----

Value n: 0 Signal Value : 60
Value n: 1 Signal Value : 61
Value n: 2 Signal Value : 59
Value n: 3 Signal Value : 60
Value n: 4 Signal Value : 60
Value n: 5 Signal Value : 62
Value n: 6 Signal Value : 60
Value n: 7 Signal Value : 60
Value n: 8 Signal Value : 60
Value n: 9 Signal Value : 60

Varianza: 0.622222
Media livello segnale : 60.2
Il terminale mobile risulta:
FERMO

---DM: 00:05:5D:25:1D:FA ---

Value n: 0 Signal Value : 58
Value n: 1 Signal Value : 63
Value n: 2 Signal Value : 63
Value n: 3 Signal Value : 63
Value n: 4 Signal Value : 61
Value n: 5 Signal Value : 62
Value n: 6 Signal Value : 61
Value n: 7 Signal Value : 59
Value n: 8 Signal Value : 59
Value n: 9 Signal Value : 59

Varianza: 3.73333
Media Livello Segnale : 60.8
Il terminale mobile risulta:
IN ALLONTANAMENTO

----DM: 00:19:E3:07:D3:FE ----

Value n: 0 Signal Value : 62
Value n: 1 Signal Value : 61
Value n: 2 Signal Value : 61
Value n: 3 Signal Value : 56
Value n: 4 Signal Value : 58
Value n: 5 Signal Value : 58
Value n: 6 Signal Value : 59
Value n: 7 Signal Value : 58
Value n: 8 Signal Value : 58
Value n: 9 Signal Value : 55

Varianza: 4.93333
Media livello segnale : 58.6
Il terminale mobile risulta:
IN ALLONTANAMENTO

---DM: 00:05:5D:25:1D:FA ---

Value n: 0 Signal Value : 62
Value n: 1 Signal Value : 62
Value n: 2 Signal Value : 61
Value n: 3 Signal Value : 57
Value n: 4 Signal Value : 58
Value n: 5 Signal Value : 62
Value n: 6 Signal Value : 57
Value n: 7 Signal Value : 59
Value n: 8 Signal Value : 58
Value n: 9 Signal Value : 64

Varianza: 6.22222
Media Livello Segnale : 60
Il terminale mobile risulta:
IN ALLONTANAMENTO

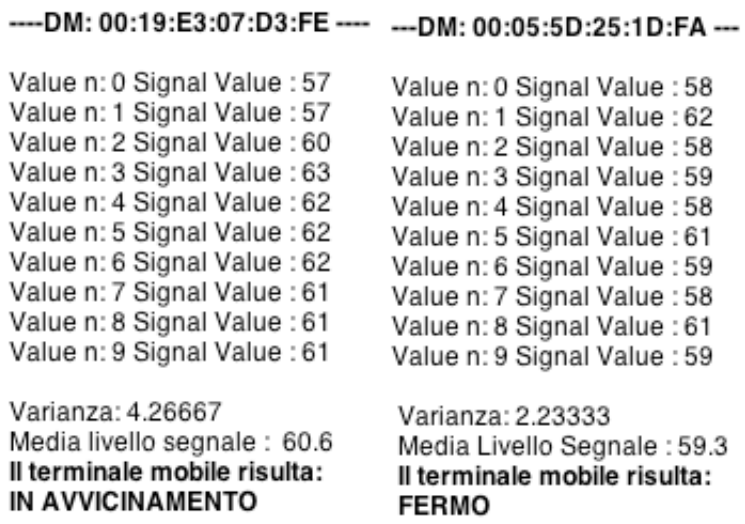

Figura 5.5: Esempio di output che indica i movimenti o meno dei DM

5.3.1 Considerazioni finali

Rispetto all'obiettivo dell'individuazione del parametro "spostamento" al fine di permettere una migliore configurazione della rete (posizionamento AP), possiamo dire che il risultato dell'algoritmo proposto è soddisfacente, pur risultando sempre condizionanti le condizioni ambientali e le relative interferenze indotte.

Capitolo 6

Ambiente di Test

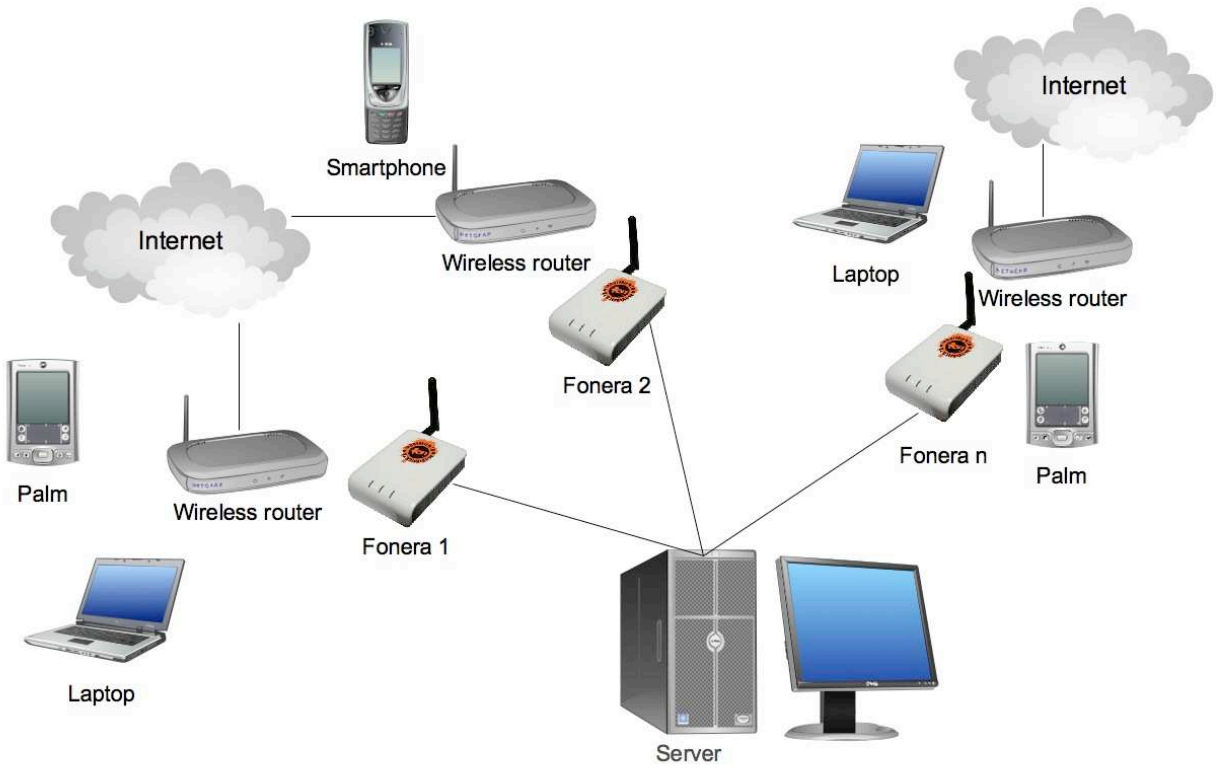

Figura 6.1: Ambiente di Test

Gli attori presenti sono:

- Access Point (Fonera), per lo sniffing dei pacchetti
- Server, per collezionare e visualizzare le informazioni di sniffing ricevuti dagli AP
- Device Mobile (DM), gli utenti collegati alla rete WIFI

6.1 Access Point - Fonera o Linksys WRT54GL?

Per la preparazione dell'ambiente di test si è dovuto ovviamente effettuare uno studio sulle caratteristiche degli AP disponibili sul mercato, in relazione ai seguenti fattori:

- possibilità di modificare e personalizzare il firmware presente sugli AP;
- disponibilità di chipser con driver che rilevasse i parametri di qualità ritenuti necessari;
- affidabilità e robustezza del sistema;
- rispondenza alle specifiche di compatibilità con gli standard 802.11b/g;
- diffusione del prodotto;
- prezzo accessibile in ragione della necessità di effettuare test con un certo numero significativo di esemplari.

La scelta iniziale è caduta sul Linksys WRT54GL, equipaggiato con il chipset Broadcam 4704, per l'estrema facilità delle operazioni di personalizzazioni del firmware necessarie per l'installazione dell'applicazione di monitoraggio. Uno studio più approfondito ha rilevato, però, l'impossibilità di monitorare uno dei parametri ritenuti maggiormente significativi (il livello del segnale), in quanto non rilevato dal driver del chipset.

L'AP Fonera, viceversa, fornisce questa possibilità pur essendo molto più difficoltosa la personalizzazione dell'aggiornamento del firmware, come illustrato nei successivi paragrafi.

6.1.1 Ap Fonera

La scelta dell'AP è caduta sul router della comunità WIFI FON [30] per le ottime caratteristiche mostrate dall'apparato equipaggiato col chip Atheros che rende possibile numerose operazioni grazie ai driver *madwifi* (http://madwifi.org/) . All'accensione dell'AP, è attivato il demone *"kismet_ drone"* che si occupa di "sniffare" i pacchetti scambiati, rilevati nell'etere, tra i DM e i Wireless Router. Il flusso di traffico rilevato dal demone viene inviato, a intervalli regolari e configurabili, al Server per poi essere, successivamente, processato dall'applicazione. Nella configurazione ottimale l'AP viene installato accanto ad ogni Wireless Router presente nella rete in modo tale che si possa avere il dato sul livello del segnale dei pacchetti ricevuti da un determinato DM il più affidabile possibile.

Successivamente viene descritta la procedura tecnica adottata passo per passo per adattare l'AP Fonera alle nostre esigenze di monitoraggio.

6.1.2 Modifica Router AP

Una volta collegato il cavo seriale della "fonera" al computer, per stabilire una connessione di console seriale è stato necessario usare un adeguato software, in relazione al tipo di sistema operativo.

Per esempio, con Windows si può usare "*Hyperterminal*", per sistemi Gnu/Linux *gtkterm* o per sistemi MacOSX *Zterm*.

In ogni modo, i parametri che devono essere settati, indipendentemente dall'applicativo usato, sono i seguenti:

- speed = 9600
- bits = 8
- stopbits = 1
- parity = none
- flow = none

Accesa la fonera e finito il boot, al prompt di Linux (**root@OpenWrt:**/#) si ha il controllo completo del router:

Figura 6.2: Accesso all'AP Fon via Seriale

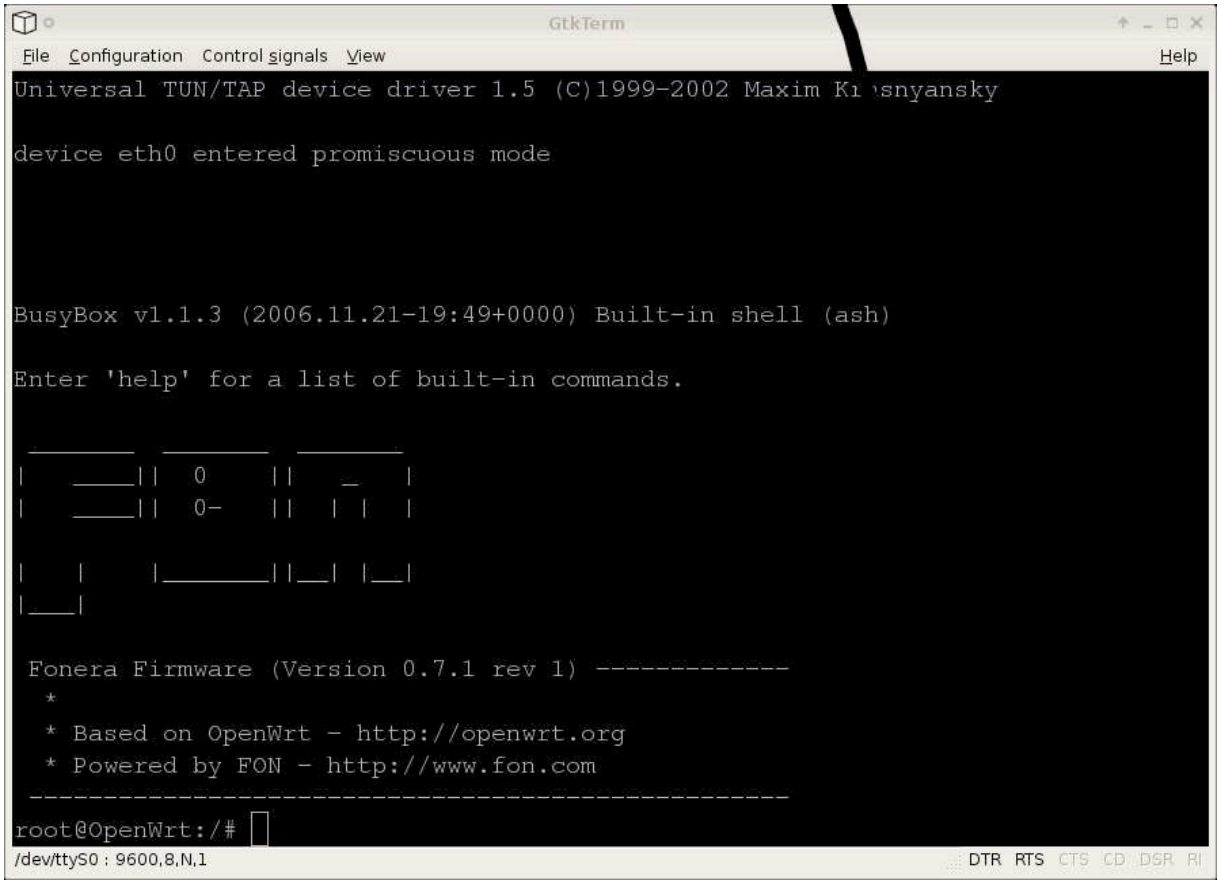

Figura 6.2 Accesso all'AP Fon via Seriale

Una volta entrati nel sistema, si apre la porta 22 relativa ad SSH con il relativo comando di *iptable*

:/# iptables -I INPUT 1 -p tcp –dport 22 -j ACCEPT

e si attiva il demone SSH presente:

:/# **/etc/init.d/dropbear**

Per far in modo che il demone SSH parta ad ogni avvio, si deve rinominare il file di avvio nel seguente modo:

:/# **mv /etc/init.d/dropbear /etc/init.d/S50dropbear**

A questo punto, si può accedere alla Fonera via SSH; l'*ip* preso dalla Fonera risulta il: 169.254.255.1, quindi, una volta configurata l'interfaccia di rete del computer utilizzato con l'adeguata classe di IP, si può accedere alla Fonera con *login: root e password: admin*. Ora è necessario settare le regole del firewall, caricate all'avvio, all'interno del file */etc/firewall.user* con un editor *vi*:

*:/#***vi /etc/firewall.user**

decommentiamo (togliendo "#") le seguenti righe per dare all'avvio la possibilità di accedere sulla porta 22 di *SSH*:

 # iptables -t nat -A prerouting_rule -i $WAN -p tcp ?dport 22 -j ACCEPT

 # iptables -A input_rule -i $WAN -p tcp ?dport 22 -j ACCEPT

Per evitare che la fonera faccia partire lo script che aggiorna in automatico il firmware della casa madre, si edita lo script */bin/thinclient* commentando l'ultima riga del file:

*:/#***vi /bin/thinclient**

aggiungendo "#" alla riga: ***. /tmp/.thinclient.sh***

A questo punto, si deve cancellare il vecchio firmware della *Fon* e inserire il nuovo e più performante *OpenWrt Kamikaze.* Per far questo è necessario accedere al *bootloader* del router, cioè a *RedBoot*. La configurazione di *RedBoot* è presente nella partizione "*RedBoot config*" della Fonera (*/dev/mtd6*). La configurazione del kernel presente nel firmware Fon non permette la scrittura. A tale proposito, bisogna sfruttare il fatto che il kernel, contenuto nella partizione "vmlinux.bin.17"(/dev/mtd4), è modificabile; si carica prima una versione modificata del kernel, compatibile con il firmware della Fonera, che permetta la scrittura nella partizione contenente la configurazione di RedBoot, successivamente si carica una configurazione di *RedBoot* che permetta il collegamento, via *telnet*, a RedBoot stesso ed avere la *shell* del bootloader.

I file necessari all'operazione si trovano all'indirizzo:

http://ww.dmarini.org/fonera/openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma

Ora si deve copiare il file appena scaricato all'interno della fonera nel seguente modo:

davide3@shadow:~$ **scp openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma root@169.254.255.1:/tmp/**

A questo punto, si accede, via SSH, alla fonera e per installare il nuovo kernel si usa il seguente comando, all'interno della dir */tmp* :

:~# **mtd -e vmlinux.bin.l7 write openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma vmlinux.bin.l7**

Il relativo output è:

Unlocking vmlinux.bin.l7 ...

Erasing vmlinux.bin.l7 ...

Writing from openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma to vmlinux.bin.l7 ... [w]

Completato il conseguente reboot del sistema, si può scrivere nella partizione di configurazione di RedBoot e, come è stato fatto precedentemente per il kernel, si copia il file *out.hex,* presente al link:

http://www.dmarini.org/fonera/out.hex

all'interno della dir */tmp:*

davide3@shadow:~$ scp out.hex root@169.254.255.1:/tmp/

Ora, per installare la nuova versione di RedBoot che ne attivi la shell via *telnet*, si esegue il solito comando precedentemente usato per installare il nuovo kernel; il tutto sempre all'interno della dir */tmp*:

root@OpenWrt:~# mtd -e "RedBoot config" write out.hex "RedBoot config"

l'output è:

Unlocking RedBoot config ...

Erasing RedBoot config ...

Writing from out.hex to RedBoot config ... [w]

e, dopo il nuovo conseguente reboot del sistema, ad ogni riavvio di *RedBoot*, prima di caricare il firmware, la Fonera si mette in ascolto, all'indirizzo 192.168.1.254, porta 9000, per fornire una shell via telnet. A questo punto, si deve disconnettere e ricconnetere la Fonera e collegarsi, via telnet, cambiando la classe di ip dell'interfaccia di rete del pc con la conseguente classe di ip: 192.168.1.166/24.

RedBoot, oltre ad accettare connessioni in telnet, rende possibile anche il download dei files dalla rete via *TFTP* (*T*rivial *F*ile *T*ransfer *P*rotocol), dando la possibilità di caricare le immagini del firmware che si vuole scrivere. A tale scopo, prima di connettersi a RedBoot, si scaricano i file da installare sulla Fonera; nel momento della stesura del presente documento è stata utilizzata l'ultima release di *Kamikaze*, cioè la 7.09:

Il root di *Kamikaze,* compilato per la Fonera:

http://downloads.openwrt.org/kamikaze/7.09/atheros-2.6/openwrt-atheros-2.6-root.jffs2-64k

L'immagine del Kernel compilato:

http://downloads.openwrt.org/kamikaze/7.09/atheros-2.6/openwrt-atheros-2.6-vmlinux.lzma

A questo punto, si passa a "flashare" la Fonera, nel seguente modo:

- Viene settato il pc con l'indirizzo IP nella classe 192.168.1.100/24
- Si esegue il server TFTP, fancedolo puntare alla cartella dove sono stati memorizzati i due file scaricati precedentemente

- Si riavvia la Fonera
- Ci si connette con Telnet all'indirizzo 192.168.1.254, porta 9000

Al prompt di RedBoot, si formatta la flash con:

RedBoot> fis init

Si comunica a RedBoot il suo indirizzo IP e quale è l'indirizzo del server TFTP da cui prendere le immagini con i comandi:

RedBoot> ip_ addr -h 192.168.1.100 -l 192.168.1.254/25

IP: 192.168.1.254/255.255.255.128,

Gateway: 0.0.0.0 Default server: 192.168.1.100

Si effettua il caricamento dell'immagine *OpenWrt*:

RedBoot>load -r -v -b %{FREEMEMLO} openwrt-atheros-2.6-root.jffs2-64k

Si crea la partizione di *OpenWrt* con la scrittura dell'immagine caricata (tale operazione richiede un tempo di circa 20 minuti):

RedBoot>fis create -f 0xA8030000 -l 0x006F0000 rootfs

Si carica l'immagine di Kamikaze con:

RedBoot>load -r -b %{FREEMEMLO} openwrt-atheros-2.6-vmlinux.lzma

e si crea la partizione per il kernel con la scrittura dell'immagine:

RedBoot>fis create -r 0x80041000 -e 0x80041000 vmlinux.bin.l7

Infine, si dice a RedBoot di caricare il nuovo kernel ed eseguirlo con:

RedBoot>fis load -l vmlinux.bin.l7

RedBoot>exec

A questo punto, si entra, via telnet all'indirizzo 192.168.1.1 si setta la password di root (attraverso il comando passwd) e successivamente si accede via **ssh** tramite il comando:

davide-marinis-computer:~davide3$ ssh -l root 192.168.1.1

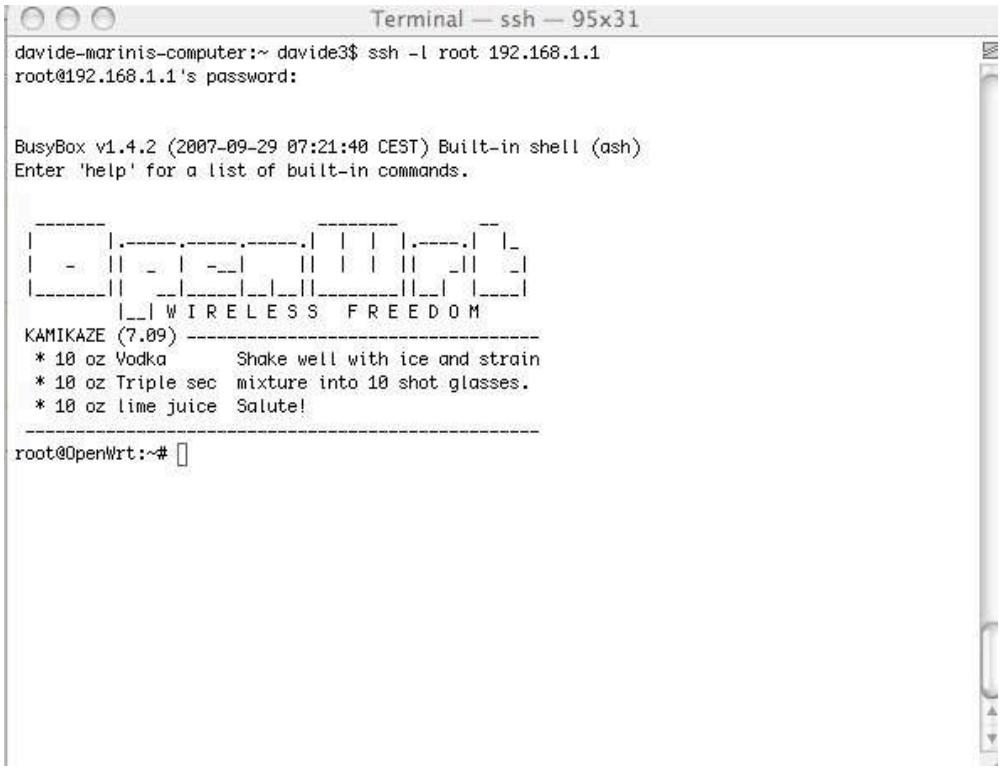

Figura 6.3: Accesso SSH alla Fonera con OpenWrt

Una volta configurati i dns in /etc/resolv.conf si può usufruire del *packet management* di OpenWrt, cioè **ipkg**, per installare i seguenti pacchetti:

- wireless-tools
- libpcap
- kmod-madwifi
- kismet-drone

tramite il comando:

root@OpenWrt:~# ipkg install nomepacchetto

Nel file di configurazione di Kismet_Drone */etc/kismet/kismet_drone.conf* si deve specificare rispettivamente, il tipo di device (nel caso del chipset Atheros **Madwifi_g**), l'interfaccia dove kismet riceve i pacchetti (**wifi0**) e il nome auto commentate della sorgente dei pacchetti:

source=Madwifi_g,wifi0,Atheros

Al lancio di Kismet_Drone si ottiene una schermata del tipo:

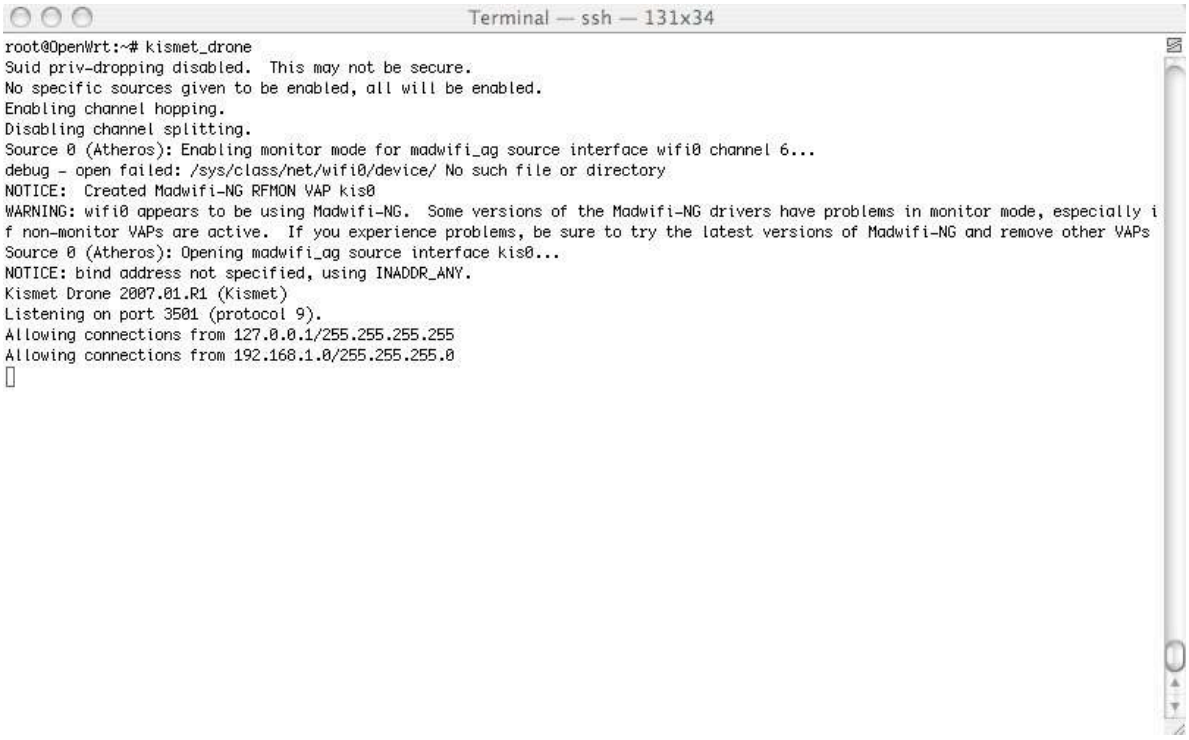

Figura 6.4: Lancio di *Kismet_ Drone* all'interno dell'AP Fonera

a questo punto il flusso è pronto per essere spedito e collezionato dal Server Centrale, come viene spiegato nella sezione successiva.

6.2 Server Centrale

Il Server Centrale è un nodo (computer del System Administrator), su cui è attivato *"kismet_ server"* che riceve il flusso dei pacchetti dall'AP a e li salva nel file in formato *".pcap"*.

Il software sviluppato si occupa di elaborare i dati ricevuti per ricavare le opportune informazioni di monitoraggio descritte nel capitolo 3.

6.3 Dispositivi Mobili (DM)

I device Mobili sono qualsiasi dispositivo con connessione WIFI come Laptop, PDA e SmartPhone, ognuno identificati dal proprio MAC address.

Capitolo 7

Conclusioni

Diverse sono le considerazioni che possono essere fatte al termine del lavoro.

Rispetto agli obiettivi prefissati, si può affermare che l'individuazione dei parametri ritenuti significativi per la valutazione qualitativa della rete WIFI ha dimostrato l'efficacia del parametro *Livello del Segnale,* che si è dimostrato affidabile, per i test effettuati, nel rilevamento dello spostamento del Device Mobile all'interno della cella dell'Access Point.

Un maggior grado di aleatorietà ha invece assunto il parametro *Numero Canale* (frequenza), che nei test ha dimostrato di risentire molto delle interferenze introdotte dall'ambiente e della qualità dell'hardware utilizzato, evidenziando la presenza di risultati dei test talvolta inaspettati, quali una maggior velocità nell'invio dei dati, anche in presenza di una percentuale di perdita di pacchetti maggiore. Da ciò appare evidente l'*impossibilità pratica* di una *ottimizzazione* dell'*assegnazione dei Canali*, testimoniata anche da talune prove in cui risulta che non sempre l'osservanza di una distanza minima tra canali assicura una migliore trasmissione.

Evidente, anche senza prova sperimentale, che l'utilizzo di Access Point che accettano sia connessioni di tipo 802.11b e 802.11.g risulta controproducente nel casi di presenza nella rete di Device Mobile di tipo 802.11b, che porterebbero ad un abbassamento di velocità anche per gli altri dispositivi di tipo 802.11.g. In questo caso, una politica di assegnazione "forzata" di modalità di connessione, aggiungendoAP di sola tipo 802.11b o 802.11.g, può aumentare la qualità complessiva della rete.

L'Applicazione Software denominata "*Sistema di Monitoraggio dei Parametri Significativi*", pensata come strumento di supporto alle decisione dell'Amministratore è stata solamente descritta, di volta in volta, nelle sezioni inerenti le singole grandezza da monitorare. Ne sono state sviluppate, in linguaggio C e C++, solamente le parti riguardanti la Visualizzazione dei Parametri Significativi (con relativo filtraggio) e quella del Rilevamento degli Spostamenti degli utenti, con l'intercettazione ed elaborazione del Livello del Segnale. Analogamente, è stata sviluppata la parte di Calcolo Pacchetti persi, utilizzata nella fase di test per la rilevazione delle degradazioni delle comunicazioni, nei vari casi di assegnamento dei Canali.

Da sviluppare interamente è la parte di raccolta di tali informazioni da più Access Point contemporaneamente e quella di presentazione dei vari messaggi informativi all'Amministratore, che poggi su una architettura applicativa di tipo WEB.

La costruzione dell'ambiente di test adatto è stata molto laboriosa, in ragione della necessità di modificare ad-hoc il firmware degli Access Point a me disponibili ed in ragione dell'utilizzo di un ambiente laboratoriale di tipo "casalingo".

Ringraziamenti

.

Bibliografia

[1] Institute of Electrical and Electronics Engineers, http://www.ieee.org.

[2] Gruppo di Lavoro 802.11, http://grouper.ieee.org/groups/802/11/.

[3] IEEE Std, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) specifications.

[4] Wireless Ethernet Compatibility Alliance, http://www.wirelessethernet.org.

[5] http://www.wirelessethernet.org/interoperability.asp.

[6] Gsm, http://www.gsmworld.com.

[7] Standard IEEE802, http://standards.ieee.org/getieee802/.

[8] B.Viken and L.Paquereau, Wireless LAN (IEEE 802.11) traffic monitoring: Using Location information for network monitoring purposes.

[9] A. Balachandran, G. M. Voelker, P.Bahl, adn P.V. Rangan, "Characterizing user behavior and network performance in a public wireless LAN",

in Proceedings of ACM SIGMETRICS'02, ISBN 1-58113-531-9, (Marina Del Rey, California), pp.195 205, ACM Press, 2002.

[10] J.Yeo, S.Banerejee, and A. Agrawala, Measuring traffic on the wireless medium: Experince and pitfalls," Tech. Rep. CS-TR 4421, Department of Computer Science, University of Maryland, dec 2002.

[11] C. Hoene, A. Gunther, and A. Wolisz "Measuring the impact of slow user motion on packet loss and delay over IEEE 802.11b wireless links" in Proceedings of IEEE LCN'03, ISSN 0742-1303, (Bonn, Germany), pp. 652-662, oct 2003.

[12] S. Ahonen, J. Lahteenmki, H. Laitinen, and S. Horshmanheimo, "Usage of mobile location techniques ofr UMTS network planning in Urban environment," in Proceedings of IST Mobile & Wireless Telecommunications Sumit 2002, (Thessaloniki, Greece), jun 2002.

[13] J. Rissanen, "Utilization of mobile network performance data for dynamic capacity reallocation." WAWC03 Conference, Lappeenranta, Finland, aug 2003.

[14] C. Dimitriadis et al., "Enhanced cellular network performance with adaptive coverage based on position location of mobile terminals," in Proceedings of IST Mobile & Wireless Telecommunications Sumit 2002, (Thessaloniki, Greece), jun 2002.

[15] Librerie Libpcap, `http://www.tcpdump.org/`.

[16] D.H. Smith, S. Hurley, and S.U. Thiel, "Improving Heuristics for the Frequency Assignment Problem," European J. Operation Research, 1998

[17] J. Zander, "Trends and Challenges in Resource Management Future Wireless Networks," Proc. IEEE Wireless Comm. and Networks Conf., 2000.

[18] I. Katzela and M. Naghshineh, "Channel Assignment Schemes for Cellular Mobile Telecommunication Systems: A Comprehensive Survey," IEEE Personal Comm, June 1996.

[19] I. Chlamtac and S.S. Pinter, "Distributed Nodes Organizations Algorithm for Channel Access in a Multihop Dynamic Radio Network," IEEE Trans. Computers, 1987.

[20] S.T. McCormick, "Optimal Approximation of Sparse Hessians and Its Equivalence to a Graph Coloring Problem," Math. Programming, 1983

[21] I. Katzela and M. Naghshineh, "Channel Assignment Schemes for Cellular Mobile Telecommunication Systems: A Comprehensive Survey," IEEE Personal Comm, June 1996.

[22] Starbucks Coffe, `http://www.starbucks.com/retail/wireless.asp`.

[23] E. Friedman e D. Parkes. Pricing WiFi at Starbucks - Issues in Online Mechanism Design. In Proc. Fourth ACM Conference on Electronic Commerce (2003).

[24] N. Lenihan, University of Limberick, ”WLAN POSITIONING”, `http://www.ul.ie/nlenihan/WLAN%20positioning.pdf`.

[25] Bahl, P. et al. Microsoft Corp. "RADAR: An In-Building RF-based User Location and Tracking System", http://research.microsoft.com/~padmanab/papers/infocom2000.pdf.

[26] Student Project at Lulea University Of Technology, "Advanced WaveLan Positioning", May 2001, http://web.media.mit.edu/~alisa/2001-05-23.pdf.

[27] Blake M. Harris, "Amulet: Approximate Mobile User Location Tracking System", http://darkfate.com/bmh/other/pubs/Amulet.pdf.

[28] Stanford University, "Halibut: An Infrastructure for Wireless LAN-based Location Tracking", http://fern2.stanford.edu/cs444n/.

[29] Ekahau, Inc., "Ekahau Technology and Products", http//www.vtt.fi/virtual/navi/expo2003/Ekahau030402.pdf.

[30] Comunita' Fon, http//www.fon.com