

INDICE

INTRODUZIONE

CAPITOLO 1 - Le Comunicazioni Wireless

1.1-Caratteristiche generali.....	1
1.2 WPAN: Bluetooth, Zigbee e UWB.....	3
1.3 Reti Locali Wireless (WLAN): 802.11.....	8
1.3.1 Vantaggi e svantaggi dell'approccio wireless.....	9
1.3.1.1 Mobilità.....	10
1.3.1.2 Allocazione delle frequenze.....	10
1.3.1.3 Interferenza e affidabilità.....	11
1.3.1.4 Riservatezza dei dati.....	11
1.3.1.5 Consumo di potenza.....	12
1.3.1.6 Sicurezza degli utenti.....	12
1.3.1.7 Throughput.....	12
1.3.2 La propagazione del segnale.....	13
1.3.3 Antenne ed amplificatori.....	14
1.3.4 Controllo d'accesso e topologie di rete.....	15
1.4 HIPERLAN e MMAC-HiSWAN.....	20
1.5 Il sistema telefonico mobile.....	21
1.5.1 Storia.....	23

CAPITOLO 2 - Il Protocollo IEEE 802.11

2.1 Introduzione.....	28
2.2 Architettura della rete.....	29
2.3 Panoramica dei servizi.....	31
2.4 Il livello fisico (PHY).....	35
2.4.1 Architettura del PHY.....	35
2.4.2 Bande di frequenza senza licenza: l'ISM.....	35
2.4.3 Spread Spectrum.....	36
2.4.4 Tecniche di modulazione.....	37
2.4.4.1 FH-SS (Frequency Hopping Spread Spectrum).....	37
2.4.4.2 DS-SS (Direct Sequence Spread Spectrum).....	42
2.4.4.3 OFDM (Orthogonal Frequency Division Multiplexing).....	48

CAPITOLO 3 - IEEE 802.11: Il Livello MAC

3.1 Introduzione.....	51
3.2 DCF: la modalità d'accesso distribuita.....	54
3.2.1 Livelli di priorità d'accesso: IFS (Inter Frame Space).....	54

3.2.2	Il meccanismo base d'accesso e la procedura di backoff.....	55
3.2.3	Il meccanismo RTS/CTS e il Net Allocation Vector (NAV).....	60
3.2.4	Frammentazione e riassetto.....	61
3.2.5	Procedure di recupero.....	62
3.2.6	Relazione tra le costanti temporali della DCF.....	63
3.3	PCF: la modalità d'accesso centralizzata.....	64
3.3.1	Struttura e temporizzazione del CFP.....	64
3.3.2	Il meccanismo di "polling".....	64
3.3.3	Il meccanismo di "reservation" e la "polling list".....	67
3.4	Formato dei frame.....	69
3.4.1	Formato generale del frame.....	69
3.4.1.1	Frame Control.....	70
3.4.1.2	Campi di tipo "Address".....	72
3.4.1.3	Sequence Control.....	74
3.4.1.4	FCS (Frame Check Sequence).....	75
3.4.2	Descrizione di alcuni frame importanti.....	75
3.4.2.1	Formato del frame RTS.....	75
3.4.2.2	Formato del frame CTS.....	76
3.4.2.3	Formato del frame ACK.....	76
3.4.2.4	Frame di tipo dati.....	77
3.4.2.5	Frame di tipo management.....	78

CAPITOLO 4 – QoS (Quality of Service)

4.1	Introduzione.....	80
4.2	La Qualità del Servizio (QoS).....	80
4.2.1	Principi fondamentali per la regolazione del traffico.....	82
4.2.2	Meccanismi di scheduling.....	84
4.2.2.1	First In First Out (FIFO).....	85
4.2.2.2	Accodamento prioritario.....	85
4.2.2.3	Round robin.....	86
4.2.2.4	Weighted Fair Queuing (WFQ).....	86
4.2.3	Meccanismi di policing: il Token Bucket.....	87
4.3	Architetture per la QoS.....	88
4.3.1	Integrated Services (IntServ).....	88
4.3.2	Differentiated Services (DiffServ).....	91
4.3.3	Vantaggi e svantaggi di IntServ e DiffServ.....	92
4.4	Limitazioni per la QoS nel protocollo 802.11 in una WLAN.....	94
4.4.1	Limitazioni della DCF.....	94
4.4.2	Limitazioni della PCF.....	95
4.5	Miglioramenti per la QoS per WLAN 802.11.....	96

CAPITOLO 5 – IEEE 802.11e: Il Livello MAC

5.1	Introduzione.....	98
5.2	Descrizione dei servizi MAC.....	99
5.2.1	Servizio Dati.....	99

5.2.1.1	Determinazione dell'UP.....	100
5.2.1.2	Interpretazione del parametro "Priorità" nelle primitive del servizio MAC.....	100
5.2.1.3	Interpretazione del parametro "classe di servizio" nelle primitive del servizio MAC in una QSTA.....	101
5.2.2	Ordinamento delle MSDUs.....	102
5.2.3	Architettura del servizio dati MAC.....	103
5.3	Formato del frame.....	104
5.3.1	Formato del frame MAC.....	104
5.3.1.1	Formato generale del frame.....	104
5.3.2	Formato di alcuni tipi di frame.....	114
5.3.2.1	Request To Send (RTS).....	114
5.3.2.2	Clear To Send (CTS).....	115
5.3.2.3	Acknowledgement (ACK).....	116
5.3.2.4	Block Ack Request (BlockAckReq).....	116
5.3.2.5	Block Ack (BlockAck).....	117
5.3.2.6	Frame Dati.....	118
5.3.2.7	Beacon.....	120
5.4	Architettura MAC.....	120
5.4.1	Hybrid Coordination Function (HCF).....	121
5.4.1.1	HCF Contention-Based Channel Access (EDCA).....	122
5.4.1.2	HCF Controlled Channel Access (HCCA).....	124
5.4.2	Coesistenza di DCF, PCF e HCF.....	125
5.4.3	Frammentazione/Deframmentazione.....	125
5.5	DCF (Distributed Coordination Function).....	126
5.5.1	Interframe Space (IFS).....	126
5.5.1.1	Arbitration IFS (AIFS).....	127
5.5.2	Rilevazione e recupero dei duplicati.....	127
5.6	HCF (Hybrid Coordination Function).....	128
5.6.1	EDCA (HCF Contention-Based Channel Access).....	129
5.6.1.1	Implementazione di riferimento.....	129
5.6.1.2	EDCA TXOPs.....	129
5.6.1.3	Ottenere una EDCA TXOP.....	130
5.6.1.4	Procedura di backoff EDCA.....	132
5.6.1.5	Procedure di ritrasmissione.....	133
5.6.2	HCCA (HCF Controlled Channel Access).....	134
5.6.2.1	Generazione CFP.....	134
5.6.2.2	Generazione CAP (Controlled Access Phase).....	135
5.6.2.3	Struttura e temporizzazione delle TXOP.....	135
5.7	Block Acknowledgment (BlockAck).....	136

CAPITOLO 6 – Analisi e valutazione della PER e della TXOP

6.1	Packet Error Rate (PER): Caratteristiche generali.....	139
6.2	Codici convoluzionali ed eventi di errore.....	140
6.3	Distribuzione EEL e PER nei codici convoluzionali.....	141
6.3.1	Derivazione della Packet Error Rate.....	143
6.4	Calcolare la TXOP (Transmission Opportunity).....	145

6.4.1 Schema di scheduling basato sulla “data rate”.....	147
6.5 Adeguare la TXOP in base alla PER.....	150

CONCLUSIONI E SVILUPPI FUTURI

BIBLIOGRAFIA

Introduzione

Scopo del presente lavoro di tesi è lo studio ed il confronto tra alcuni standard di comunicazione wireless nell'ambito della realizzazione di reti locali di computer (*Wireless LAN*), in particolare ci si è soffermati su due protocolli sviluppati dall'*Institute of Electrical and Electronics Engineers* (IEEE): IEEE 802.11 e IEEE 802.11e. Lo studio è stato effettuato a livello di protocollo e l'attenzione è stata rivolta al sottolivello MAC ("*Medium Access Control*").

Le comunicazioni wireless, ed in particolare il *Wireless Networking*, rappresentano una tecnologia in rapida espansione che consente all'utente un accesso a reti e servizi senza necessità di cablaggi. Possiamo pensare, ad esempio, ad un utente provvisto di una serie di dispositivi, generalmente indipendenti l'uno dall'altro, quali il telefono cellulare, il computer portatile, il PDA e così via ed immaginare una situazione in cui questi dispositivi possano interagire fra di loro, ad esempio per condividere documenti presenti sul proprio computer portatile durante una riunione oppure per ricevere la posta elettronica sul PDA invece che sul computer fisso e tutto ciò senza necessità di alcun cablaggio. Possiamo pensare ad operazioni più "quotidiane" come entrare in un centro commerciale e veder comparire sul nostro PDA le ultime novità e le offerte del giorno oppure scaricare sul computer portatile mappe ed informazioni turistiche mentre si passa un casello autostradale o si sosta in una stazione di servizio. Tutto questo oggi è già possibile dal punto di vista tecnologico e le sperimentazioni sono già state avviate con successo in molte parti del mondo, Italia compresa. Le reti locali wireless sono senza dubbio uno dei possibili fulcri dell'attuale e futura innovazione tecnologica.

Ovviamente l'approccio wireless nella realizzazione di reti di computer presenta dei vantaggi ma anche degli svantaggi rispetto al classico approccio cablato. In via teorica, gli utenti di una rete locale wireless vogliono usufruire degli stessi servizi e vorranno disporre delle stesse potenzialità a cui una rete cablata li ha abituati. In pratica, l'equivalenza tra i due approcci wireless e wired, è una sfida aperta. In particolare l'approccio wireless, a fronte di innegabili vantaggi, è soggetto ad alcuni limiti non presenti nell'approccio cablato.

Le wireless LAN (WLAN) trasmettono e ricevono dati via etere, minimizzando il bisogno di collegamenti cablati, combinando, così, la connettività e la mobilità degli utenti, i quali possono accedere ad informazioni condivise, senza cercare un luogo per collegarsi in rete; gli amministratori del sistema, inoltre, possono implementare o ingrandire una WLAN senza installare o trasportare fili (tali opportunità di mobilità e di servizio non sono possibili con reti cablate). Altri vantaggi possono essere la velocità d'installazione, l'elevata scalabilità e i costi di gestione ridotti. Uno dei principali svantaggi di questo tipo di reti è l'utilizzo di onde radio, come mezzo trasmissivo delle informazioni, che risente dei disturbi elettromagnetici (interferenze varie) e della presenza di ostacoli composti da materia non perfettamente penetrabile dalle onde radio. Perciò la propagazione delle onde radio è molto complicata sia in ambiente indoor che outdoor, perché il segnale può arrivare al ricevitore attraverso molti cammini, in quanto nel suo percorso dal trasmettitore al ricevitore il segnale sarà soggetto a riflessioni e rifrazioni. Questo fenomeno, noto come *multi-path*, causerà la ricezione di segnali di intensità diversa in istanti temporali differenti (dell'ordine di 10-100 ms). I segnali giungono perciò con fasi differenti e ciò può provocare un annullamento a causa della sovrapposizione di segnali sfasati di 180 gradi. La risposta in frequenza ottenuta mostra spesso dei picchi negativi in corrispondenza della frequenza selezionata. E' il fenomeno del *multi-path fading*. Un altro svantaggio, dovuto all'uso di onde radio, riguarda tutte le problematiche relative alla limitatezza di banda e al riuso delle frequenze.

Le caratteristiche del mezzo fisico hanno notevole impatto anche sulle topologie e sulle tecniche d'accesso multiplo che vengono utilizzate nelle reti locali wireless. Come nelle reti locali cablate, anche nelle reti locali wireless il collegamento tra diverse stazioni avviene tramite l'uso di un unico canale di comunicazione condiviso, sul quale le comunicazioni sono di tipo broadcast: uno trasmette e tutti gli altri sentono. Ciò significa che quando una stazione trasmette, essa occupa una parte o addirittura la totalità di una risorsa limitata e condivisa, la banda disponibile. Occorre quindi coordinare l'azione delle stazioni in modo che in ogni istante non ve ne sia più di una che trasmette: altrimenti si verifica una collisione, che generalmente comporta la distruzione, al ricevitore, dell'informazione contenuta in tutti i segnali trasmessi.

Di qui la necessità dei protocolli d'accesso multiplo, implementati in quella parte del sistema di comunicazione nota con il nome di MAC (*“Medium Access Control”*), che hanno il compito di garantire, tramite tecniche di accesso casuale, ordinamento, segnalazione, l'uso dinamico, efficiente ed equo da parte di più stazioni dell'unica risorsa di comunicazione.

L'*Institute of Electrical and Electronic Engineers* (IEEE) ha costituito il gruppo di studio 802.11 con l'incarico di definire uno standard internazionale per reti locali radio. Lo scopo è quello di fornire le specifiche per il livello fisico delle trasmissioni (*PHY* - *“Physical Layer”*) e per i protocolli di controllo d'accesso al mezzo (*MAC*). Il *MAC* è progettato in modo da essere indipendente dalla scelta del *PHY* sottostante. Il nostro interesse è focalizzato sul livello *MAC*, in particolare nella sua parte centrale, che tratta dei servizi di scambio di dati fra le stazioni della rete, e sui meccanismi di accesso al mezzo previsti per eseguirli.

Trattandosi di una rete locale, la possibilità di accesso alla rete e la mobilità sono confinate in un'area limitata, la cui estensione dipende dalle potenze trasmesse, dalla capacità dei ricevitori, dai livelli di rumore ed interferenza, dalle caratteristiche dell'ambiente fisico. Quest'area è denominata con il termine *“Basic Service Area”* (*BSA*), e l'insieme delle stazioni che possono comunicare fra loro al suo interno è il *“Basic Service Set”* (*BSS*). Il *BSS* è il blocco di base con cui si possono costruire delle reti 802.11. Per estendere l'accesso e la mobilità oltre i confini di una *BSA*, è necessario interconnettere più unità *BSS*, formando così un *“Extended Service Set”* (*ESS*) che si estende su una *“Extended Service Area”* (*ESA*). Per questo motivo, lo standard prevede due distinte architetture di rete: *Ad-Hoc Network*, costituita da una sola *BSS* indipendente, e *Infrastructure Network*, costituita da più *BSS* interconnessi in un *ESS*. La connessione dei *BSS* all'interno di un *ESS* è fornita dal *“Distribution Service”* (*DS*) attraverso entità denominate *“Access Point”* (*AP*). Ogni *BSS* in un *ESS* possiede il proprio *AP*. Un *AP* è una stazione che possiede anche funzionalità di comunicazione con gli *AP* degli altri *BSS*. Lo standard dice esplicitamente che il mezzo fisico utilizzato per connettere gli *AP* nel *DS* (denominato *DSM*, *“Distribution Service Medium”*) è logicamente distinto dal mezzo fisico utilizzato all'interno di una *BSS* (indicato con *WM*, *“Wireless Medium”*).

Il servizio fondamentale che una rete 802.11 deve svolgere è quello del trasferimento di pacchetti fra le stazioni della rete. Questi pacchetti sono denominati MSDU (“*MAC Service Data Unit*”) e costituiscono le unità dati che vengono scambiate dai livelli LLC (“*Logical Link Control*”) delle stazioni, attraverso l’uso dei servizi forniti dal MAC. A sua volta il MAC, per trasferire gli MSDU, si appoggia ai servizi forniti dal livello fisico. Per far questo, si scambiano delle unità denominate trame (in inglese “*frame*”) o MPDU (“*MAC Protocol Data Unit*”).

Il livello fisico è suddiviso in due sottolivelli: il PLCP (“*Physical Layer Convergence Procedure*”) e il PMD (“*Physical Medium Dependent*”). Il PLCP è la colla tra i frame del MAC e le trasmissioni radio nell’aria. Aggiunge un proprio header ad ogni frame, in modo da aiutare la sincronizzazione delle trasmissioni. Il PMD è addetto alla trasmissione dei bit, ricevuti dal PLCP, nell’aria tramite l’uso di un’antenna. Il PHY incorpora la funzione CS/CCA (“*Carrier Sense/Clear Channel Assessment*”), che indica al MAC quando il segnale è percepito.

L’approccio classico per le comunicazioni radio è quello di confinare i segnali in una banda ristretta e fornirgli la massima potenza possibile. L’utilizzo dello spettro RF (“*Radio Frequenza*”) non è libero, ma è regolato da alcuni istituti (FCC, ERO, ETSI, ITU), che emettono le varie licenze di trasmissione, stabilendo banda e potenza del segnale. Esistono delle bande che non necessitano di licenza e sono dette ISM (“*Industrial, Scientific and Medical*”), in quanto sono riservate ad apparecchiature industriali, scientifiche e mediche. Chiunque può sfruttare queste bande, perciò un problema delle bande ISM è l’inquinamento causato dall’alto numero di sistemi che vi operano (ad esempio i forni a microonde o i telecomandi dei garage operano a queste frequenze). Inoltre le onde sono ostacolate dalle molecole d’acqua, perciò la comunicazione in caso di pioggia o nebbia è molto difficoltosa e quindi non può estendersi su lunghe distanze. Anche se le bande ISM sono libere, sono state stabilite alcune regole fondamentali per il loro utilizzo: la massima potenza trasmessa (1W per FCC e 100mW per ETSI) e l’uso della tecnica di *Spread Spectrum*. Questa tecnica consiste nel diffondere il segnale nel più largo range di frequenza possibile tramite l’uso di funzioni matematiche. Il ricevitore esegue l’operazione inversa ricostruendo il segnale da più segnali a banda ristretta, per cui i relativi rumori hanno poca influenza sul segnale totale.

Il livello fisico di 802.11 usa tre tecniche diverse di Spread spectrum: FH-SS (*“Frequency Hopping Spread Spectrum”*), DS-SS (*“Direct Sequence Spread Spectrum”*) e OFDM (*“Orthogonal Frequency Division Multiplexing”*).

Il sottolivello MAC del protocollo L’802.11 prevede due modalità d’accesso multiplo distinte per operare all’interno di un BSS: la *Distributed Coordination Function* (DCF), modalità d’accesso distribuita basata sulla tecnica CSMA/CA e la *Point Coordination Function* (PCF), modalità d’accesso centralizzata basata su un meccanismo di “reservation+polling”. La modalità d’accesso principale è la DCF. Essa deve essere supportata obbligatoriamente da tutte le stazioni. La PCF è una modalità d’accesso opzionale, che è implementata sulla base della DCF. Una rete 802.11 può operare esclusivamente con la DCF, ma non esclusivamente con la PCF: se quest’ultima è presente, deve essere presente anche la prima. Il modo con cui DCF e PCF coesistono quando usati entrambi è quello dell’alternanza periodica nel tempo. La struttura periodica logica in cui coabitano è detta *SuperFrame*, ed ha una durata costante. Ogni *SuperFrame* è diviso in due parti: nella prima, detta *Contention Free Period* (CFP), la modalità d’accesso utilizzata è la PCF; nella seconda, la *Contention Period* (CP) la DCF. Il punto di separazione fra le due parti ha una posizione variabile all’interno del *SuperFrame*, che viene decisa dal Point Coordinator.

La *“Distributed Coordination Function”* è la modalità d’accesso distribuita del MAC dell’802.11, basata sulla tecnica d’accesso multiplo casuale nota sotto il nome di *“Carrier Sense Multiple Access/Collision Avoidance”* (CSMA/CA). La tecnica CSMA/CA può essere sommariamente descritta spiegando i singoli termini dell’acronimo: nel CSMA prima di trasmettere, una stazione testa il canale (*“Carrier Sensing”*) e se lo trova libero trasmette; nel CA in caso negativo, dopo che il canale si libera, per evitare collisioni con eventuali altre stazioni in attesa (*“Collision Avoidance”*), ogni stazione seleziona un ulteriore tempo d’attesa casuale (*backoff*) all’interno di una certa finestra temporale (*“Contention Window”*). Quella che ha scelto il backoff più piccolo trasmette, le altre rinviando ulteriormente la trasmissione al termine di quella in corso. La DCF prevede due meccanismi distinti di trasmissione di un pacchetto. Un meccanismo standard, di tipo “2-way handshaking”, nel quale al pacchetto trasmesso dalla stazione mittente, segue, in caso di ricezione corretta, un breve trama di riscontro positivo

("Acknowledgement", ACK) inviata dalla stazione destinataria; e un meccanismo opzionale, di tipo "4-way handshaking", noto con il nome di *RTS/CTS*, nel quale alla trasmissione del pacchetto vero e proprio si fa precedere lo scambio di due speciali trame di prenotazione del canale: la richiesta di trasmissione ("*Request To Send*", RTS) da parte della stazione mittente, e la conferma alla disponibilità a ricevere ("*Clear To Send*", CTS) da parte della stazione destinataria.

Il protocollo CSMA/CA impone che vi sia un intervallo di tempo specificato tra le trasmissioni di due frame successivi. Questo intervallo viene genericamente chiamato IFS ("*Inter Frame Space*"). Una stazione che vuole trasmettere dovrà assicurarsi che il mezzo trasmissivo risulti libero per l'adeguato IFS prima di provare a trasmettere. Se al contrario il mezzo viene rilevato come "occupato", la stazione deve rimandare la trasmissione fino al termine di quella in corso. Dopo questo ritardo e anche immediatamente dopo una qualsiasi trasmissione avvenuta con successo, una stazione deve compiere la cosiddetta procedura di *backoff*. Questa procedura consiste nel selezionare un ritardo casuale (*random backoff interval*) con il quale si inizializza un count-down timer. Il timer è decrementato finché il canale rimane libero, congelato quando viene rilevata una trasmissione sul canale, e riattivato, a partire dal valore a cui si trovava quando è stato fermato, quando il canale viene di nuovo rilevato libero per più di un IFS. La stazione trasmette quando il suo backoff timer arriva a 0.

E' tuttavia prevista dallo standard una modifica al meccanismo di accesso base, che prevede lo scambio di due piccoli frame di controllo RTS e CTS prima di ogni trasmissione dati, essenzialmente pensata per ridurre ulteriormente le collisioni e ridurre i problemi derivanti dalle situazioni di tipo "nodi nascosti" (ciò è una stazione non riesce a sentire la trasmissione di un'altra). Quando la stazione destinataria riceve l'RTS, risponde con un CTS. La stazione sorgente può quindi trasmettere il suo pacchetto dopo corretta ricezione del CTS. Inoltre, i pacchetti RTS e CTS portano l'informazione relativa alla durata della trasmissione che sta per avvenire. Questa informazione è utilizzata per implementare, presso tutte le stazioni che siano state in grado di udire almeno una delle due trame, una funzionalità di *carrier-sense virtuale*: ognuna di queste stazioni utilizza l'informazione relativa alla durata della trasmissione prossima per aggiornare un "*Net Allocation Vector*" (NAV) contenente l'informazione sul periodo di tempo in

cui il canale rimarrà occupato. Una stazione considera quindi il canale occupato quando almeno uno fra il carrier-sense fisico e il carrier-sense virtuale fornisce indicazione in tal senso.

Il MAC IEEE 802.11 prevede un metodo di accesso opzionale chiamato “*Point Coordination Function*” (PCF), che può essere usato però solo nelle reti con infrastruttura. Questo metodo di accesso prevede che un’entità logica detta “*Point Coordinator*” (PC), che risiede nell’AP della BSS, stabilisca istante per istante mediante un’operazione di *polling* quale stazione sia autorizzata a trasmettere. Il PCF utilizza un meccanismo di carrier-sense virtuale insieme ad un meccanismo d’accesso basato su priorità. Il metodo d’accesso fornito dal PCF può dunque essere utilizzato per realizzare un accesso di tipo *contention-free* (CFP, Contention Free Period), ovvero il PC controlla integralmente la trasmissione delle stazioni in modo tale da eliminare la contesa di queste ultime per il mezzo trasmissivo. Il PC acquisisce il controllo del mezzo trasmissivo all’inizio di ogni CFP, e tenta di mantenere questo controllo per tutta la durata del CFP usando un IFS minore di quello usato dalle stazioni che operano secondo le regole del DCF. Ogni CFP inizia con una trama di sincronizzazione, detta *beacon*, inviata dal PC. La durata del CFP è decisa dal PC. Essa non può superare un certo valore limite (*CFP-Max-Duration*) specificato dal protocollo. In ogni trama di beacon il PC inserisce in un apposito campo (*CFP-Dur-Remaining*) il tempo che manca alla fine del CFP se questo dovesse avere la durata massima consentita. Questa informazione è usata dalle stazioni per mantenere il NAV sul valore “occupato” fino alla fine nominale del CFP. Il PC termina un CFP tramite un’esplicita trama (*CF-End*), che può essere trasmessa anche prima della fine nominale del CFP determinata dalla *CFP-Max-Duration*. Le stazioni che ricevono questa trama rimettono il loro NAV sul valore “libero”. Il trasferimento di trame sotto la PCF consiste tipicamente nell’alternarsi di trame inviate dal PC e trame inviate al PC. L’ordine delle trasmissioni e la stazione che è autorizzata a trasmettere in ogni momento, sono controllati dal PC tramite l’invio di particolari frame (come i CF-Poll). L’802.11 prevede che il PC mantenga una lista delle stazioni da interrogare, la cosiddetta “*polling list*”.

La rete Internet è in grado di fornire un servizio *best-effort* a tutte le applicazioni e non fa alcuna promessa sulla *qualità del servizio* (QoS) che un’applicazione riceve, infatti essa riceverà qualsiasi livello di prestazioni che la

rete è in grado di offrire in quel momento. L'internet attuale non permette alle applicazioni multimediali (sensibili al ritardo) di richiedere alcun trattamento speciale perchè nei vari router i pacchetti sono trattati tutti allo stesso modo, compresi quelli sensibili al ritardo. I modelli di *QoS* per IP sono stati introdotti proprio per cambiare questa situazione e per dare la possibilità agli utenti (eventualmente paganti) di richiedere alla rete determinate prestazioni garantite.

Una rete è in grado di garantire un fissato livello di *QoS* in due modi: *Overprovisioning* e *Admission Control*. Inoltre si può garantire la *QoS* o per *flusso* o per *aggregati* (o *classi*) di flussi. Nella rete internet attuale i pacchetti sono trattati tutti allo stesso modo, infatti vengono memorizzati nelle code dei router e spediti in ordine FIFO. Quindi, ad esempio, i pacchetti FTP e quelli audio sono trattati allo stesso modo e una raffica di pacchetti FTP può causare un ritardo non tollerabile nella consegna di quella audio. Per ovviare a ciò si può pensare di dare una priorità ai diversi pacchetti in modo che quelli a più alta priorità vengano spediti prima di quelli a più bassa. Ciò implica che un flusso a più alta priorità potrebbe occupare in modo intensivo il canale impedendo così la trasmissione agli altri flussi, quindi è desiderabile avere un qualche grado di isolamento tra i vari flussi di traffico. Per garantire questo isolamento si possono seguire due approcci: sorvegliare i flussi di traffico o assegnare ai flussi canali logici separati. Il tutto deve essere fatto cercando di sfruttare al massimo le risorse della rete. Ad un flusso che richiede una certa *QoS*, la rete deve garantire quelle risorse affinché lo stesso sia ritenuto utilizzabile, perciò prima di accettarlo bisogna eseguire un processo di ammissione che fa sì che un flusso dichiari i suoi requisiti di *QoS* e che indichi alla rete di accettare il flusso oppure di bloccarlo. Tale processo è detto ammissione della chiamata.

I pacchetti che giungono ad un router sono memorizzati in buffer e il modo in cui sono selezionati per la trasmissione è detto *modalità di scheduling del link*. Esistono diverse politiche di scheduling, alcune delle più importanti sono: First In First Out (FIFO), Accodamento Prioritario, Round Robin, Accoramento Equamente Pesato. Il processo di regolazione della velocità a cui ad un flusso è permesso di immettere pacchetti sulla rete è detto *meccanismo di policing*. Il più utilizzato è il *token bucket*, il quale consiste in un contenitore che può includere fino a *b* token. Al flusso è permesso spedire dati solo quando c'è almeno un token nel contenitore.

Esistono due architetture fondamentali per la QoS e si distinguono in base al servizio offerto: *Integrated Services* (Servizi Integrati) e *Differentiated Services* (Servizi Differenziati). L'IntServ mira a fornire garanzie per-flusso a sessioni di applicazioni individuali, definendo nuove classi di servizio da affiancare al best effort, e la comunicazione è orientata alla connessione. Si basa su due concetti fondamentali: l'applicazione richiedente "prenota risorse" sufficienti a garantire la propria QoS e quindi "chiede a ogni router" del percorso di comunicarle le risorse già impegnate; in questo modo si instaura una connessione. Ogni richiesta di prenotazione ha al suo interno un oggetto attraverso cui l'host sorgente specifica la QoS richiesta ed identifica il flusso di dati cui riservare quella QoS. Tale oggetto è detto *flow descriptor* costituito da un *flowspec*, in cui si specifica la QoS richiesta, e un *filter spec*, che indica a quale flusso riservare le risorse. A questo punto attraverso un processo di *admission control* si va a verificare se la richiesta può essere soddisfatta e attraverso il *policy control* si verifica che l'host sorgente sia autorizzato ad inoltrare tale richiesta (memorizzando informazioni per la tariffazione). L'IntServ ha classificato le applicazioni in 2 topologie: *elastic traffic* e *real time traffic*. La prima tipologia supporta il best effort, la seconda necessita di un trattamento preferenziale perché è necessario un *delay bound* da non superare affinché i pacchetti ricevuti siano ancora validi.

DiffServ mira a risolvere i problemi di IntServ, in quale è adatto per piccole reti IP e non per una rete così grande come Internet. Perciò si forniscono garanzie per aggregati di flussi e non per il singolo flusso. Aggregati di diverse connessioni con comportamenti analoghi sono detti *behavior aggregate* (BA). Dal lato gestore, gli aggregati con stesso BA sono trattati allo stesso modo ma contemporaneamente è necessario rispettare le garanzie date all'utente singolo. Nell'architettura prevista dai DiffServ si distinguono due regioni: una ai margini della rete (*edge*) e una al centro della rete (*core*). I pacchetti provenienti dagli host si raggruppano in zone edge e vengono marchiati in base alla loro priorità, indipendentemente dall'host a cui appartengono. Si evita così che un singolo flusso debba prenotare risorse, poiché i flussi simili sono comunque trattati allo stesso modo. Il trattamento differenziato del traffico è assolto da modalità di inoltro chiamate *Per Hop Behavior* (PHB) sui nodi lungo il percorso. Il PHB permette di aggregare tutti i pacchetti nell'edge e di marcarli per classe di priorità in modo da fornire un

servizio efficiente nel core. Il vantaggio di DiffServ è quello di poter trattare più comunicazioni contemporaneamente.

Garantire i requisiti di QoS richiesti da un utente in una rete wireless 802.11 è molto difficoltoso perché il protocollo non prevede meccanismi utili allo scopo. Perciò il consorzio IEEE ha istituito un gruppo di lavoro che ha sviluppato il protocollo 802.11e. Il livello MAC dello standard IEEE 802.11e fornisce la funzionalità QoS (Quality of Service) ed è quindi in grado di gestire le applicazioni che richiedono il supporto QoS in una WLAN. Si forniscono due meccanismi per supportare le applicazioni che richiedono QoS: *Enhanced Distributed Channel Access* (EDCA), che gestisce la consegna del traffico tramite l'utilizzo di priorità differenziate, definite come *user priorities* (UPs), e *Hybrid Coordination Function (HCF) Controlled Channel Access* (HCCA), che si basa sulla prenotazione di "opportunità di trasmissione", *transmission opportunities* (TXOPs), attraverso l'utilizzo di un coordinatore ibrido, *hybrid coordinator* (HC).

Il livello MAC 802.11 non prevede la gestione di frame con differente priorità, infatti tutte le stazioni hanno uguale probabilità di ottenere l'accesso al canale. Però uguali probabilità di accesso non sono desiderabili fra stazioni che hanno differente priorità dei frame. Per far ciò il livello MAC 802.11e introduce un *identificatore di traffico* (TID, "*Traffic Identifier*") per specificare servizi differenziati per ogni MSDU. Nelle QSTAs ("*QoS Station*") associate in un QBSS ("*QoS BSS*"), il MAC usa un set di regole per spedire prima le MSDUs con più alta UP ("*User Priority*") rispetto a quelle con più bassa UP.

Per supportare la QoS il protocollo 802.11e include una funzione di coordinazione addizionale detta *Hybrid Coordination Function* che è solo utilizzabile nelle configurazioni di rete che supportano QoS (QBSS). La HCF sarà implementata in ogni QSTAs. La HCF combina funzioni della DCF e PCF con alcune innovazioni, meccanismi di QoS specifici e sottotipi di frame per consentire un set uniforme di sequenze di scambio da essere usate per trasferimento di dati QoS sia durante il CP (Contention Period) che il CFP (Contention Free Period). L'HCF utilizza il meccanismo *Enhanced Distributed Channel Access* (EDCA) per il trasferimento basato sulla contesa e quello *HCF Controlled Channel Access* (HCCA) per il trasferimento senza contesa. Sotto HCF, l'unità base che determina il diritto di trasmettere sul WM è la *TXOP* ("*Transmission Opportunity*"). Ogni

TXOP è definita da un tempo di partenza e da una durata massima e può essere ottenuta da una QSTA che vince un'istanza di contesa EDCA durante il CP o da una non-AP QSTA che riceve un frame QoS (+)CF-Poll durante il CP o il CFP.

Il meccanismo EDCA fornisce accesso differenziato e distribuito al mezzo wireless per QSTAs che utilizzano 8 differenti UPs. Definisce quattro categorie di accesso (*ACs*, “*Access Categories*”) che forniscono supporto per la consegna del traffico con UPs alle QSTAs. Per ogni AC si definisce un IFS, temporizzato in maniera tale che l'AC con maggiore priorità abbia più probabilità di ottenere una TXOP. Il meccanismo HCCA usa un coordinatore centralizzato, chiamato *Hybrid Coordinator* (HC), e opera sotto regole che sono differenti dal PC e dalla PCF. L'HC differisce dal PC usato nel PCF in molte caratteristiche significative, sebbene può opzionalmente implementare le funzionalità di un PC. La caratteristica più importante è che le sequenze di scambio frame possono essere usate fra QSTAs associate in un QBSS sia durante il CP che il CFP. L'HC garantisce alle non-AP QSTA una “polled” TXOP con durata specificata in un frame QoS(+)CF-Poll. L'HC può anche operare come un PC, fornendo (non-QoS) CF-Poll alle stazioni associate secondo le stesse regole e formati di un PC. Durante una TXOP, una QSTA può cominciare la trasmissione di uno o più frame, ognuno spedito dopo un intervallo SIFS. Tutte le trasmissioni, inclusi i frame di risposta, entro una TXOP sono considerate parte della TXOP e l'HC ne terrà conto al momento del settaggio del limite della stessa.

Uno dei maggiori problemi che si incontra nelle reti wireless è l'elevato tasso di errori causati dal rumore presente sul canale, se paragonato a quello delle reti wired. Tutti i pacchetti spediti contengono un campo definito CRC (“*Cyclic Redundancy Check*”), la cui funzione è quella di correggere gli eventuali bit in errore ricevuti. Se però il numero di bit errati è molto alto allora neanche il CRC è in grado di correggerli e quindi il pacchetto sarà perso. Se il canale è molto rumoroso allora il numero di pacchetti persi può causare un degradamento delle prestazioni tale che non si riesce a garantire più il rispetto dei parametri di QoS. Perciò analizzare e comprendere come il rumore influisce sulla qualità dei bit ricevuti è fondamentale per progettare e tarare al meglio i vari meccanismi che consentono l'ottenimento di una data QoS. Un primo passo è quello di analizzare in che modo e con che frequenza si presentano questi errori, perciò dei parametri che

ci forniscono informazioni sul grado di affidabilità del canale sono: la *Bit Error Rate* (BER) e la *Packet Error Rate* (PER). La PER è principalmente derivata usando la BER e supponendo che gli errori sono uniformemente distribuiti, ma ciò fornisce una sovrastima della stessa. Un altro metodo per descrivere i processi di errore prevede l'utilizzo di un modello di Markov, ma questo approccio non riesce a fornire una formula chiusa basata sui parametri di codice utilizzati nei sistemi di comunicazione. Il modello analizzato nella tesi si basa sulla distinzione tra eventi di errore e periodi senza errori. Un evento di errore comincia con la ricezione di un simbolo di errore e finisce dopo una sequenza di v bit ricevuti senza errori. La derivazione della distribuzione (EEL, "*Error Event Length*") degli eventi di errore è la base su cui si fonda il calcolo della PER. Alcuni lavori in letteratura hanno dimostrato che la distribuzione della EEL è simile per i codici che hanno le stesse caratteristiche. Si può assumere che la lunghezza dei periodi senza errori e quella con errori sono indipendenti, ma questa assunzione non è corretta per SNR bassi. Si definisce *epoca di decodificazione o di errore* l'intervallo fra due eventi di errore consecutivi, perciò essa consiste di un periodo senza errori seguito da un evento di errore. La lunghezza di un evento di errore è indipendente da quella di un'epoca di errore, quindi la distribuzione delle epoche di errore possono essere facilmente derivate usando una distribuzione geometrica senza memoria.

Utilizzando un'approssimazione lineare si può stabilire la lunghezza media dell'evento di errore e quella del periodo di decodificazione. Da ciò si ricava la lunghezza media del periodo senza errori. Per alto SNR è possibile assumere che la lunghezza del periodo senza errori segue una distribuzione geometrica con parametro $\lambda(s)$, da cui supponendo che il decodificatore è resettato all'inizio di ogni pacchetto ricevuto, si ricava la probabilità che un pacchetto contenga un evento di errore. E' stato dimostrato che con questo approccio la stima della PER è nettamente più vicina ai valori reali.

Il protocollo IEEE 802.11e fornisce uno scheduler in grado di garantire le minime performance richieste dai vari utenti. Il metodo utilizzato è l'allocazione di una TXOP all'utente, perciò il calcolo della durata di questa TXOP è fondamentale per raggiungere gli obiettivi prefissati. Per calcolare la TXOP allocata ad uno specifico stream di traffico un QAP (QoS Access Point) usa i seguenti parametri: la velocità media di produzione dei dati, la lunghezza nominale di una MSDU,

l'intervallo di servizio schedulato (intervallo tra due TXOP consecutive), la velocità di trasmissione del livello fisico e gli overhead introdotti dal protocollo per la gestione. Per evitare la creazione di code il QAP deve allocare una TXOP di lunghezza tale da garantire che siano trasmessi tutti i pacchetti giunti durante l'intervallo di servizio schedulato. Inoltre la TXOP deve essere calcolata tenendo conto anche delle code dei vari stream di traffico, cercando di offrire lo stesso trattamento a tutti i vari tipi di traffico. Si è analizzato un metodo che cerca di predire qual'è l'ammontare di traffico che giunge durante l'intervallo di servizio e quindi si è tenuto conto anche di queste informazione nel calcolo della TXOP. Altri parametri che influiscono sono gli eventuali intervalli di tempo in eccesso che possono essere ridistribuiti ai vari flussi e l'introduzione di un token bucket che sorvegli il traffico, limitando i flussi a durata più lunga. Tenendo conto di tutti questi parametri si può determinare un metodo di calcolo della TXOP che generi dei risultati migliori rispetto ad altri scheduler standard (HCCA e FHCF).