Università degli Studi di Padova
Facoltà di Ingegneria

Corso di Laurea Triennale in Ingegneria Elettronica

Tesi di laurea Triennale

Analisi di reti IEEE 802.11n per applicazioni in ambito industriale

Candidato:
Enrico Tonetto
Matricola 595777

Relatore:
Stefano Vitturi

Anno Accademico 2011–2012

SOMMARIO

Lo scopo di questa tesina è quello di analizzare gli aspetti innovativi introdotti nelle wireless LAN da 802.11n al fine di poterli utilizzare in ambito industriale. Per poter capire appieno le caratteristiche di questo standard è stato necessario conoscere gli standard della famiglia 802.11 e cosa miravano ad ottenere.
Dopo una breve introduzione (capitolo 1) nel capitolo 2 sono trattati alcuni aspetti peculiari delle trasmissioni wireless e in particolare in ambiente industriale. Nel capitolo 3 vi è una descrizione dei principali protocolli della famiglia 802.11 che hanno portato allo sviluppo dell'attuale 802.11n. Nei capitoli 4 e 5 sono descritte le innovazioni apportate da 802.11n per quanto riguarda il livello fisico e il controllo di accesso al mezzo. Sempre nel capitolo 5 vi è una breve presentazione di 802.11e protocollo mirato a garantire QoS.
Infine nel capitolo 6 vi è un'analisi degli aspetti introdotti nei capitoli precedenti con riferimento ad un utilizzo in reti in ambiente industriale.

ABSTRACT

The purpose of this work is to analyze the newest IEEE 802.11 wireless LAN standard to use it in industrial environment.
A brief introduction, chapter 1, is followed, in the second chapter (2), by an overview about wireless transmission and more particularly industrial wireless transmission. In chapter 3 there is a presentation of the set of standard 802.11 and the basic concepts for 802.11n standard development. In the chapters 4 and 5 there are the innovations about the 802.11n physical and data link layer. In chapter 5 there is also an overview of 802.11e as regards "quality of service" (QoS).
Finally in chapter 6 there are an analysis of the aspects of 802.11n that can have a significant impact on the future design of wireless industrial communication network.

INDICE

ELENCO DELLE FIGURE

ELENCO DELLE TABELLE

1 INTRODUZIONE

Lo scopo di questa tesi è quello di analizzare gli aspetti innovativi del protocollo 802.11n. Tale tecnologia è nata come realizzazione di WLAN acronimo di *Wireless Local Area Network* ovvero reti caratterizzate da un'estensione relativamente piccola paragonabile a singoli uffici, abitazioni ma spesso ampliate a interi palazzi. Tali reti sfruttano tecnologie wireless per connettere tra loro gli Access Point, di seguito AP, con dispositivi di vario genere quali computer, telefoni o apparecchiature che comunque interfacciano lo standard 802.11. La versatilità di connessione e quindi di far parte di una rete senza la necessità di cablare il dispositivo ha cominciato ad avere grande notorietà e diffusione con la nascita di dispositivi portatili quali laptop e telefoni che sfruttano l'accesso ad internet degli AP collegati alla rete tramite tale tecnologia.
Molteplici sono i vantaggi per i quali le WLAN hanno avuto nell'ultimo decennio una sempre maggiore diffusione rispetto alle LAN cosiddette *cablate*; come primo aspetto vi è appunto il fatto che non è richiesta la connessione fisica tra un utente ed un altro all'interno della rete, quindi non vi è necessità di cablaggio. Questo aspetto è molto rilevante in quanto per un'azienda o anche per un uso domestico, il cablaggio di tutti i dispositivi comporta costi nettamente maggiori rispetto a connessioni wireless a causa dei costi di posa dei cavi e dei connettori oltre a quelli di configurazione della rete stessa presenti necessariamente in tutti i tipi di rete; infine sempre per quanto riguarda la posa di cavi, non tutti gli ambienti si prestano alla realizzazione di una rete via cavo. Esempi di questo possono essere palazzi storici oppure ambienti pubblici quali aereoporti o stazioni. Infine tale rete si presta bene ad installazioni temporanee utili ad esempio in luoghi adibiti a fiere o per test su dispositivi. Un altro aspetto caratteristico di questa tipologia di reti è che l'ingresso di un nuovo utente all'interno della rete stessa avviene in modo quasi automatico o al massimo con l'istallazione di un nuovo AP se necessario.
C'è da dire che tale tecnologia non ha solo vantaggi ma come si può facilmente dedurre, la natura fisica del mezzo stesso introduce alcune problematiche sulle quali vi sono molti studi in

letteratura. Il fatto di utilizzare le onde radio porta al problema dell'interferenza dovuta alle trasmissioni che possono interessare luoghi vicini a dove ha sede la rete WLAN. Ulteriori elementi di disturbo sono rappresentati da pareti, oggetti e persone in movimento o il rumore presente in tutte le trasmissioni e che assume un certo rilievo in presenza di impianti industriali. Tali fattori possono compromettere notevolmente l'affidabilità delle trasmissioni a tal punto da non permettere al ricevitore di risalire al segnale originale o a parte di esso. Altri problemi che possono insorgere sono dovuti alla sicurezza dei dati in quanto tra un utente ed un altro può esserci qualcuno intenzionato a intercettare o a corrompere le informazioni trasmesse. Per ovviare a questo vi è l'utilizzo di metodi di crittografia che da un punto di vista portano ad un miglioramento dell'affidabilità ma dall'altro introducono ulteriore complessità nella realizzazione delle parti di trasmissione/ricezione interessate dalla codifica. Infine, almeno per ora, le WLAN non riescono ad ottenere velocità di trasmissione equiparabili a quelli della tradizionali LAN via cavo. Come si può dedurre, il tema delle reti wireless è oggetto di ricerca in tutti i suoi aspetti sia per porre rimedio ai problemi sopracitati sia per migliorare le prestazioni aumentando, ad esempio, la velocità di trasmissione. La maggior parte dell'attenzione è mirata allo studio e all'implementazione di 802.11 all'interno di ambienti quali uffici, case o all'utilizzo come hotspot pubblici. Ciò che verrà affrontato invece in questa tesina sarà un'approccio mirato all'utilizzo di reti IEEE 802.11 ed in particolare di IEEE 802.11n per quanto riguarda l'ambito industriale. L'obbiettivo è quello di analizzare le peculiarità dello standard e capire quali caratteristiche rispondono ai requisiti di una trasmissione industriale e quali invece potrebbero rivelarsi critiche.

2 TRASMISSIONI IN AMBIENTE INDUSTRIALE

Realizzazioni di reti non cablate come sopraevidenziato presentano numerosi problemi legati alla tipologia fisica del mezzo stesso. Inoltre in ambienti di tipo industriale ci sono dei requisiti che vanno rispettati e che verranno presentati nella sezione 2.2.

2.1 TRASMISSIONI WIRELESS

Le reti wireless sono soggette a problemi di trasmissione che nelle classiche reti cablate non sono presenti. Tale tecnologia è nota essere incline ad una elevata probabilità di errore sul bit e di conseguenza sui pacchetti. Oltre ai problemi di sicurezza, che espongono le reti wireless a maggior vulnerabilità (si tratta di un mezzo aperto), vi sono degli aspetti tecnici che nessitano un'analisi approfondita quali ad esempio il fading.
Con il termine *fading* vengono indicati diversi effetti della propagazione del segnale, in particolare la sensibile variazione del canale nel tempo e come diretta conseguenza la variazione dei parametri che vanno a definire il modello di canale.
Solitamente vengono indacati due tipi di fading:

- **Fast Fading** si tratta di variazioni rapide della potenza ricevuta con conseguente riduzione di SNR dovute a cammini multipli e movimenti di ricevitori, trasmettitori o di entrambi. Tali situazioni danno luogo a cambiamenti rapidi dei parametri caratteristici del segnale come ad esempio l'interferenza mutua e possono dar luogo a copie dello stesso segnale che presentano ritardo e fase diversa rispetto al segnale originale. In figura 1 vi è un semplice schema di propagazione multicanale dove si può notare che al ricevitore giungono molti campioni del segnale originale sfasati. Si nota che solamente introducendo una differenza di cammini ottici si hanno degli sfasamenti.

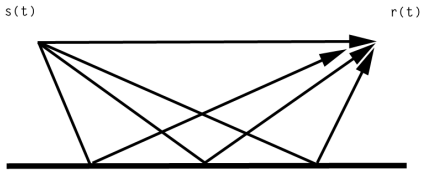

Figura 1: Schema riflessioni

In linea del tutto generale dato un segnale trasmesso:

$$s(t) = Re\left\{u(t)e^{j2\pi f_c t}\right\} \tag{1}$$

avremo in ricezione un segnale $r(t)$ funzione dei diversi percorsi k, dell'attenuazione e del ritardo dell'n-esimo percorso rispettivamente $\alpha_n(t)$ e $\tau_n(t)$.

$$r(t) = Re\left\{\sum_{n=0}^{k} \alpha_n(t)u(t-\tau_n(t))e^{j(2\pi f_c(t-\tau_n(t)))}\right\} \tag{2}$$

Senza prendere in considerazione l'eventuale effetto doppler che può presentarsi e complicare ulteriormente il segnale al ricevitore.

- **Slow Fading** altrimenti noto con il termine di *shadow fading* indica la variazione di intensità del segnale ricevuto a causa di spostamenti di oggetti all'interno del cammino di propagazione provocando un cambiamento, in media, della potenza ricevuta.

Due ulteriori problemi che si riscontrano all'interno di reti wireless sono il problema della stazione nascosta (*hidden node problem*) e il problema della stazione esposta. Con il primo si indica l'impossibilità da parte di una stazione di rilevare alcune stazioni presenti sulla rete a causa della ridotta portata del canale radio. Con riferimento alla figura 2 se C vuole trasmettere a B sente il canale libero anche se nello stesso momento A sta tresmettendo, C comincerà a trasmettere andando in collisione.

Con problema della stazione esposta si intende in un certo senso il problema contrario rispetto al Hidden node. Con riferimento alla figura 3, supponiamo che B stia trasmettendo ad A e C voglia trasmettere a D. Se C fa un controllo sul canale rileverà la trasmissione tra B e A e deciderà di non trasmettere. Tuttavia la stazione C poteva trasmettere lo stesso in quanto la ricezione all'interno della rete sarebbe compromessa solo nella zona

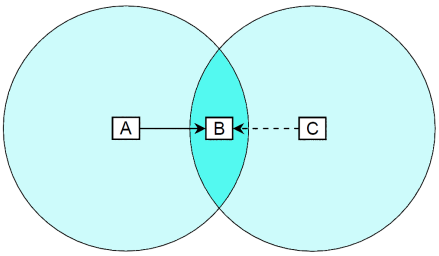

Figura 2: Stazione nascosta.

compresa tra B e C e quindi D avrebbe ricevuto correttamente i dati da C.

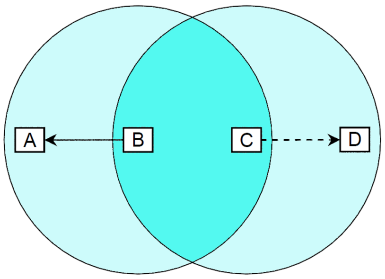

Figura 3: Stazione esposta.

Infine vi è una rigida normativa che va rispettata in fatto di utilizzo di frequenze radio. Vi è un ente che gestisce le frequenze delle trasmissioni in base a normative nazionali e internazionali. Tale argomento verrà trattato nel capitolo 3 per quanto riguarda le frequenze utilizzate da 802.11.
Nel caso di frequenze libere vi sono molti protocolli che vengono sviluppati nella stessa banda e questo si presenta come rumore aggiunto in ricezione.

2.2 TRASMISSIONI IN AMBIENTE INDUSTRIALE

La trasmissione in ambiente industriale richiede particolare attenzione dovuta al fatto che il rumore prodotto è nettamente maggiore rispetto a quello di ambienti quali abitazioni o uffici oppure di spazi aperti.
Come si vedrà di seguito ogni ambiente di produzione è soggetto a fenomeni di disturbo propri e caratteristici e quindi lo studio effettuato, ad esempio, su una centrale di distribuzione dell'energia elettrica porterà a conclusioni diverse da quelle

risultanti da uno studio in un'acciaieria. In [5] sono stati effettuati dei test al fine di delineare alcuni parametri caratteristici dell'ambiente di trasmissione con lo scopo di tracciare la risposta impulsia del canale $h(\tau)$. Per far questo è stato analizzato il power-delay-profile (PDP) che indica la potenza ricevuta in funzione del tempo a partire da un impulso trasmesso. Si puo vedere dal grafico in figura 4 che vi è la presenza di picchi che si distribuiscono come una Gaussiana. La causa di un grafico di questo genere è da ricercare nella differenza di tempi di propagazione dovuta a lunghezze di percorso diverse determinate delle riflessioni dell'ambiente circostante.

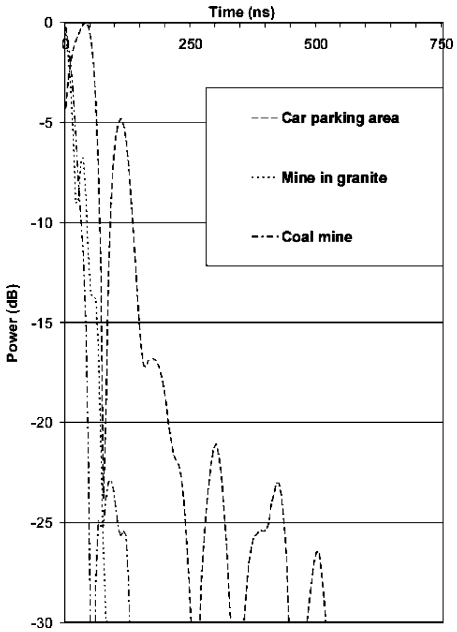

Figura 4: Power delay profile

Sempre in [5] si è cercato di determinare alcuni parametri caratteristici per definire i canali posti sotto esame, definendo la potenza totale P_T:

$$P_T = \sum_k P(\tau_k) \tag{3}$$

si è poi analizzata la media, rispetto al tempo, del ritardo $\bar{\tau}$ e la deviazione standard σ,

$$\bar{\tau} = \frac{1}{P_T} \sum_k \tau_k P(\tau_k) \tag{4}$$

$$\sigma = \sqrt{\frac{1}{P_T} \sum_k (\tau_k - \bar{\tau})^2 P(\tau_k)} \tag{5}$$

Infine un altro parametro caratteristico determinato è la larghezza di banda coerente (*coherence bandwidth*) che rappresenta un parametro legato anch'esso al ritardo di diffusione; tale valore indica la larghezza di banda per la quale si ha una correlazione di circa 0,9 . Da [8] è definita come:

$$B_{0.9c} \approx \frac{1}{50\sigma} \tag{6}$$

I risultati dei test condotti su diversi siti industriali sono riportati in tabella 1.

Tabella 1: Parametri siti

Site	$\bar{\tau}$ [ns]	σ [ns^2]	$B_{0.9c}$ [KHz]
Petrochemical plant	38	88	526
Transformer station	85	7954	227
Manufacturing plant	44	561	455
Carpark	74	11388	263
Mine in granite	16	68	1250
Coal mine	23	81	870

Come si può intuire tali paramentri variano sensibilmente da luogo a luogo e possono variare anche solo modificando la posizione di ricevitori e trasmettitori. Da ciò si può concludere che un'analisi di questo tipo non potrà mai essere esaustiva ma al contempo può dare un punto di partenza dal quale progettare un'eventuale rete.
Ciò che emerge dall'analisi fatta in [5] emerge anche in [2] dove vengono condotti diversi test per caratterizzare i distubi dovuti a macchine per la lavorazione, all'ambiente che presenta per la maggior parte parti metalliche e all'interferenza di altri sistemi di comunicazione wireless.

A prescindere dal mezzo fisico utilizzato le reti industriali presentano delle specifiche particolari in termini di Quality of Service (QoS). Con tale termine si fa riferimento alle caratteristiche che la rete deve avere al fine di garantire un certo tipo di servizio agli utilizzatori, in questo caso i dispositivi saranno sensori e ricevitori che andranno ad elaborare i dati presenti nella rete. Come specifica fondamentale che una rete industriale deve realizzare c'è quella di essere real-time, garanzia dal punto di vista della trasmissione dei pacchetti per quanto concerne la consegna di un pacchetto entro un tempo stabilito. Tale

caratteristica sembra scontata ma in trasmissioni di tipo broadcast o file sharing non è garantita.
Come fa notare [14] le reti industriali oltre alla caretteristica real-time devono essere affidabili ed utilizzare per la trasmissione pacchetti di breve durata. Infine devono garantire del cosiddetto *traffico urgente* necessario per notificare situazione di allarme ed avviare eventuali procedure di sicurezza. Per implementare tali specifiche solitamente le reti utilizzano diversi tipi di approcci tra questi, uno chiamato *master-slave model* dove si prevede che una o più stazioni attive dette *master* vadano ad interrogare ad una ad una le stazioni *slave* presenti in una lista di interrogazioni, *polling list*.
La seconda tecnica utilizzata è prevista nelle reti di tipo *producer-consumer* dove vi è un nodo il quale produce i dati che vengono trasmessi ad uno o più nodi (consumatori) che necessitano di tali dati. All'interno della rete vi è un nodo coordinatore che ha il compito di avvisare i nodi (produttori) di quali dati e in che tempi devono essere prodotti.

3 IEEE 802.11

Lo standard IEEE 802.11n fa parte di un progetto di sviluppo che è nato inizialmente come 802.11 e che si è sviluppato in diversi protocolli compatibili tra loro che interagiscono nello stesso tipo di rete. Tali protocolli si collocano ai livelli *Physical* e *Data Link* dello stack protocollare ISO/OSI visibile in figura 5; in particolare con il primo vengono descritte le specifiche fisiche della trasmissione del segnale sul mezzo quali le caratteristiche del mezzo trasmissivo, le modulazioni, la durata di un singolo bit, vincolando quindi la costruzione del trasmettitore e del ricevitore ma anche la massima lunghezza di un link oppure le frequenze da utilizzare.

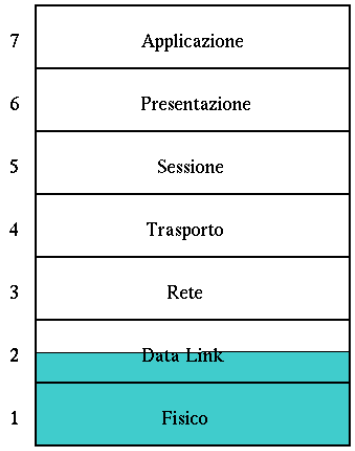

Figura 5: Modello di Riferimento OSI.

Il livello *Data Link* invece si occupa del trasferimento dei dati provenienti dai livelli superiori del modello OSI tra due utenti attraverso lo stesso livello fisico. E' compito del data link frammentare i dati in pacchetti e di inviarli in modo sequenziale, inoltre a questo livello si opera rilevamento ed eventuale correzione d'errore implementando *Automatic Repeat Request*(ARQ) oppure *Foward Error Correction* (FEC). Infine è possibile implementare un controllo di flusso per non saturare le risorse al trasmettitore e al ricevitore.
Il livello *Data Link* per quanto riguarda il protocollo 802.11 viene diviso in due parti: MAC *(Medium Access Control)* responsa-

bile del controllo di accesso al canale e quindi al mezzo condiviso e LLC *(Logic Link Control)* che si occupa dell'interazione tra i livelli superiori quali network, transport... con il sottolivello MAC.

Il progetto 802.11n fa parte di un gruppo di standard rilasciati a partire dal 1997 riguardanti le trasmissioni tramite onde radio nelle frequenze ISM (industrial scientific and medical). Tali frequenze possono essere usate liberamente e sono regolate dell'ente ETSI (European telecommunication standard istitute). L'utilizzo di tali frequenze è libero ma la costruzione di dispositivi è soggetta a licenze.
A diverse versioni di IEEE 802.11 corrisponde un diverso utilizzo del mezzo fisico e di trasferimento dati, garantendo comunque la compatibilità con le precenti versioni.

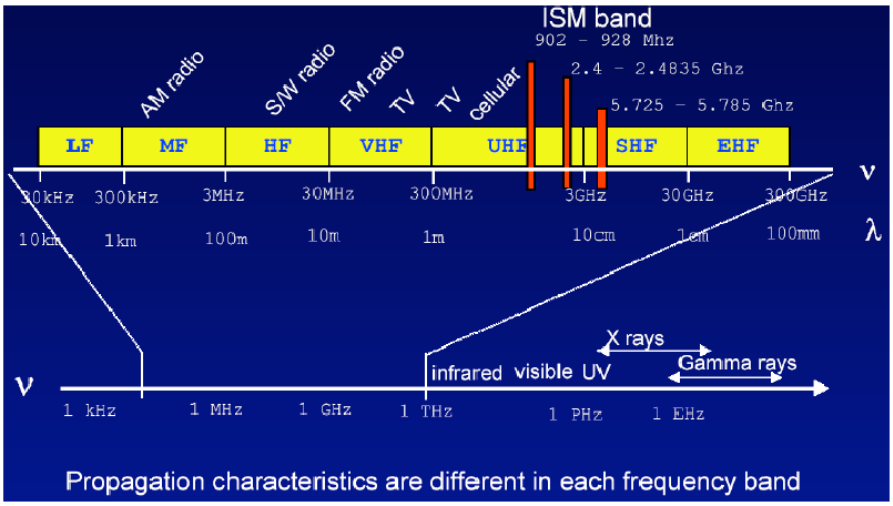

Figura 6: Diagramma di utilizzo delle frequenze

IEEE 802.11 Prevedeva la scelta di 3 differenti tecniche di trasmissione delle quali però solamente la *direct sequence spread spetrum* DSSS è stata implementata a livello commerciale prevedendo l'utilizzo di due diverse modulazioni che raggiungevano 1Mbit/s e 2Mbit/s, DBPSK e QBPSK rispettivamente.
Sono stati definiti 11 canali nella banda dei 2,4 GHz ISM per un totale di 80 Mhz di larghezza di banda. Degli undici canali disponibili però venivano utilizzati solamente i canali 1, 6 e 11 in quanto ogni canale occupa 22 MHz e, a causa dell'interferenza tra i canali, è necessario una separazione tra essi di almeno 25 MHz.

IEEE 802.11B Con tale standard l'obiettivo era quello di aumentare il bit rate con il risultato di ottenere bit rate di 5,5 Mbit/s e 11 Mbit/s trasmettendo sempre nella banda dei 2,4 Ghz. Il numero di canali, la larghezza di banda per canale e le tecniche di accesso al mezzo rimasero invariate. Era previsto inoltre il ritorno alla trasmissione a 1 e a 2 Mbit/s in condizioni del mezzo non favorevoli (fall back rate).

IEEE 802.11A Dopo la liberalizzazione da parte degli enti di gestione delle frequenze della banda ISM attorno ai 5 GHz (figura 6) si sviluppò questo standard appunto per lavorare con frequenze attorno ai 5 GHz e per incrementare ulteriormente il rate fisico di trasmissione portandolo ad un massimo di 54 Mbit/s con fall-back rate di 48, 36, 24, 18, 12, 9 e 6 Mbit/s. Questo è possibile tramite l'utilizzo dell' OFDM.
Sono supportati 8 canali non sovrapposti che possono operare nella stessa area geografica; tramite OFDM si suddivide la banda B in N sottocanali che occupano B/n Hz; nel caso di 802.11a ciascun canale a 20 MHz è suddiviso in 64 sub-carriers di 312,5 KHz ciascuna, la particolarità di tale tecnica è che permette di utilizzare, per ogni subcarriers, diverse tipologie di modulazione (BPSK, QPSK, 16QAM, 64QAM). Dei 64 sotto-canali disponibili ne vengono utilizzati solamente 48 per la trasmissione dei dati, i rimanenti vengono utilizzati per ridurre l'interferenza tra canali adiacenti e per la stima del canale. La tecnica di trasmissione OFDM verrà presentata nella sezione 4.1.

IEEE 802.11G Implementa le stesse caratteristiche di 802.11a estendendole alla banda ISM dei 2,4 GHz ottenendo 54 Mbit/s utilizzando un massimo di 3 canali.

Per quanto concerne il livello MAC, vi sono due tipologie di trasmissione o tipologie di rete realizzabili con il protocollo 802.11:

- IBSS (*indipendent basic service set*) non prevede una struttura di rete prefissata. Tramite IBSS ogni utente può comunicare con qualsiasi altro utente direttamente, sfruttando anche un terzo utente o più, nel caso di *hidden node*. Come si può intuire quest'ultima tipologia è soggetta a problemi legati al fatto che la topologia della rete non è nota a

priori infatti una stazione potrebbe spegnersi improvvisamente e scollegare degli utenti, inoltre possono insorgere dei problemi a causa dell'ambiente dinamico.

- BSS *basic service set* o reti ESS *exentended service set* dove vi è un AP fisso che gestisce i diversi utenti presenti nella rete. Si è soliti includere nella trattazione anche un DS *distribution system* termine con il quale ci si riferisce per indicare la rete di collegamento tra diversi AP solitamente con tratte Ethernet che possono fornire l'accesso a internet.La gestione avviene in modo strutturato supportando due diverse modalità operative:
  - DCF *Distributed coordination function* utilizza un protocollo simile a quello utilizzato da Ethernet (802.3) detto CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*);
  - PCF *Point coordination function* affida all'AP la coordinazione di tutte le stazioni nella sua cella;

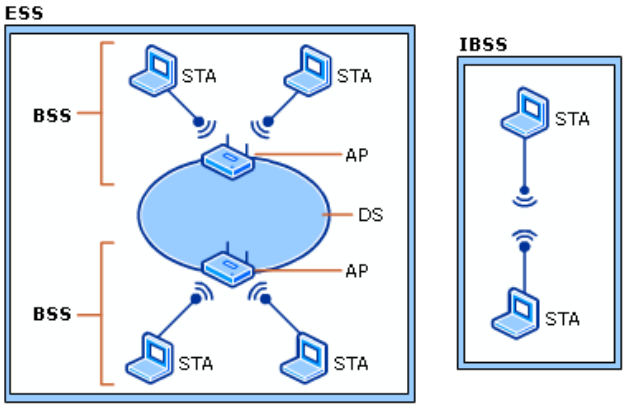

Figura 7: BSS e IBSS

Tutte le tecniche di accesso al mezzo verrano esposte ed analizzate nel capitolo 5. In particolare verrà presentato il protocollo **IEEE 802.11e** nel paragrafo 5.2. Tale protocollo è stato introdotto per garantire QoS, in particolare prevede l'introduzione di due tecniche di accesso opzionali: EDCA e HCCA.

3.1 802.11N

Lo standard 802.11n nasce da un progetto sviluppato da *High Throughput Task Group* (TGn) che si proponeva come scopo l'incremento del througput intervenendo sia sul *physical layer* (PHY) e sia sul *medium access control layer* (MAC). Con throughput si definisce l'informazione utile trasmessa dal sistema e, utilizzandolo come sistema di misura, per quanto concerne sistemi 802.11a/g essi raggiungevano un througput massimo di circa 25 Mbps.

Il TGn si pone come obbiettivo quello di realizzare un sistema che raggiungesse un througput di almeno 100 Mbps garantendo:

- una vasta distribuzione sul mercato
- compatibilità rispetto alle architetture 802.11 già esistenti
- realizzazione dal punto di vista tecnico
- realizzazione dal punto di vista economico

La realizzazione di tali specifiche verranno trattate nei due successivi capitoli.

4 PHYSICAL LAYER

Lo standard 802.11n introduce diverse tecniche mirate ad aumentare il throughput massimo. Come già introdotto per quanto riguarda 802.11a e successivamente standardizzato anche in 802.11g vi è l'utilizzo di *Orthogonal Frequency Division Multiplexing* OFDM. Le novità introdotte sono invece l'utilizzo di tecniche MIMO *Multiple Input Multiple Output* e la presenza di canali a 40 Mhz.

4.1 ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING

OFDM è un tipo di modulazione che prevede di soddisfare le richieste di alto bit rate in canali a banda larga. L'idea di fondo è quella di suddividere il canale in N sottocanali (portanti) tra loro ortogonali. Tale tipo di trasmissione permette la ripartizione del flusso informativo su molte portanti in modo da ridurre sensibilmente l'interferenza tra simboli (ISI), problema che si presenta nel caso di utilizzo di una sola portante in canali selettivi in frequenza. Inoltre l'ortogonalità delle portanti consente di garantire un'elevata efficienza spettrale (bit/s per unità di banda) e consente di ridurre di molto l'interferenza tra le portanti (ICI).
In figura 8 è rappresentata la risposta in frequenza di un generico canale $G_{Ch}(f)$ si vede come è possibile suddividere il canale in modo da ottenere dei sottocanali che presentano un guadagno in ampiezza quasi piatto.

Il bit rate dell' informazione in ingresso R_b viene trasmesso nel canale in *blocchi* di $N \cdot m$ bit dove N indica il numero delle portanti e m il numero di bit degli $M = 2^m$ simboli della modulazione. Per ogni portante è previsto l'utilizzo di una modulazione digitale a M segnali (ad esempio BPSK $m = 2$, QPSK $m = 4$, 64-QAM con $m = 6$). Per ottimizzare le prestazioni si può pensare di utilizzare m variabile ma generalmente si lascia m costante.
Definendo il tempo di bit $T_b = 1/R_b$ trasmettendo in parallelo

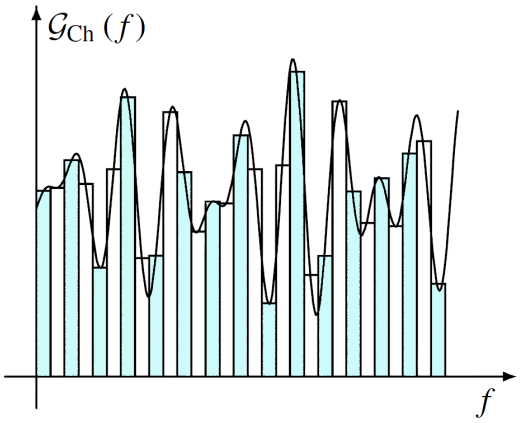

Figura 8: Suddivisione del canale in sottocanali

su N portanti, il tempo di simbolo OFDM T_s e symbol rate R_s risultano:

$$T_s = (N \cdot (T_b \cdot m)) \qquad R_s = \frac{1}{T_s} = \frac{R_b}{Nm} \tag{7}$$

Il symbol-rate complessivo tenendo conto degli N canali sarà:

$$R_{s\Sigma} = R_s \cdot N = \frac{R_b}{m} \qquad simboli/s \tag{8}$$

Come è possibile notare nella formula 8 scegliendo m sufficientemente elevato si riesce a trasmettere elevati bit-rate mantenendo su ogni portante un symbol-rate basso. In tale modo si può limitare l'ISI anche nell'eventualità di canali selettivi. In canali radio per ridurre ulteriormente l'ISI viene inserito un intervallo di guardia (GI) tra due segnali OFDM adiacenti.
Per quanto riguarda il segnale OFDM quest'ultimo è il risultato della trasformata di fuorier inversa dei simboli α_n

$$g(t) = \sum_n \alpha_n e^{j2\pi f_n t}, \tag{9}$$

dove $\quad 0 \leqslant t \leqslant T_s, \quad f_n = \frac{n}{T_s} \quad e \quad 0 \leqslant n \leqslant N-1.$

Il risultato in frequenza nel caso di 4 portanti è raffigurato in figura 9.

In 802.11a vi sono 64 sottocanali ricavati da un canale ampio 20 MHz e risulta $\Delta_f = 312,5kHz$. Presenta quindi 64 valori FFT/IFFF (Fast Fourier Transform/Inverse Fast Fourier Transform), il periodo di simbolo T_s risulta essere pari a 3.2µs.
Dei 64 sottocanali solo 52 vengono utilizzati ed inoltre sono previsti 0.8µs di intervallo di guardia.

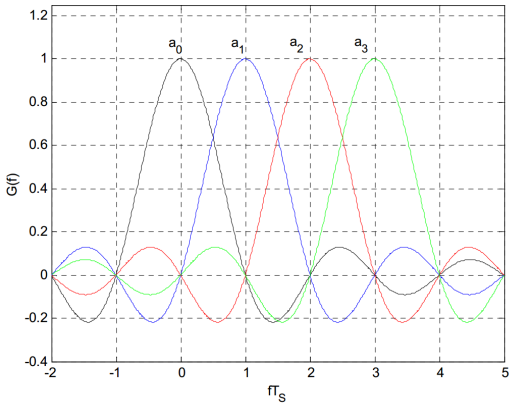

Figura 9: Esempio di segnale OFDM in frequenza con quattro portanti

4.2 MULTIPLE INPUT MULTIPLE OUTPUT

Una delle innovazioni introdotte da questo nuovo standard è il fatto di poter trasmettere utilizzando le tecniche MIMO *Multiple-input Multiple-output* ovvero l'utilizzo di trasmissioni basate su antenne multiple sia in trasmissione che in ricezione. Il concetto di fondo per l'utilizzo di MIMO è lo *spatial division multiplexing* SDM ovvero la trasmissione di stream di dati indipendenti su differenti antenne.
Quindi per una coppia di antenne (trasmettitore e ricevitore) è permesso trasmettere stream dati diversi rispetto alle altre coppie realizzando così link di tipo $2x2, 3X3$. Inoltre sono previste tecniche di trasmissione che prevedono in modo del tutto generale MxN MIMO/SDM.
Tramite MIMO/SDM il rate massimo del sistema aumenta pro-

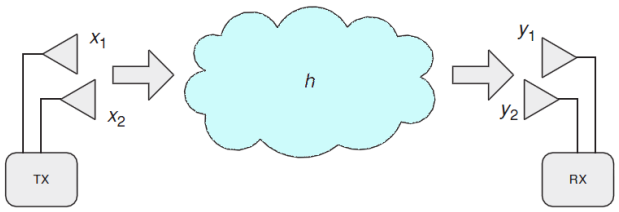

Figura 10: Esempio sistema SDM

porzionalmente al numero di stream dati indipendenti.

Per aumentare ulteriormente il rapporto segnale rumore (SNR) sono previste delle tecniche di trasmissioni e di codifica che si differenziano per risultati ottenuti e per complessità di realizzazione:

TRANSMIT BEAMFORMING (TXBF) tramite tale tecnica si da un peso agli stream in trasmissione per aumentare l'SNR in ricezione. Questo è possibile tramite la conoscenza da parte del trasmettitore del canale trasmissivo (channel state information, CSI). L'informazione sul canale da parte del trasmettitore è fornita dal dispositivo ricevitore in quanto nel preambolo del pacchetto di trasmissione i bit sono noti ad entrambi i dispositivi e a seconda di come vengono ricevuti il trasmettitore modificherà i pesi attribuiti ai segnali. Il tutto tramite una tecnica di feed-back.

SPACE TIME BLOCK CODING (STBC) è un tipo di codifica che introduce della ridondanza all'interno della trasmissione per ottenere un livello di diversità dove non si ha informazioni sul canale trasmissivo. L'aggiunta di ridondanza implica una riduzione del throughput ma in compenso una notevole riduzione della probabilità d'errore. Questo tipo di codifica si basa su un idea che ha sviluppato Alamouti in [1] per un numero arbitrario di antenne. La codifica di Alamouti prevede due antenne in trasmissione e una in ricezione (2x1); con la particolarità che le due antenne per due intervalli di simbolo consecutivi trasmettono i segnali C_1 e C_2 come in tabella 2. In figura 11 vi è lo schema tramettitore-ricevitore.

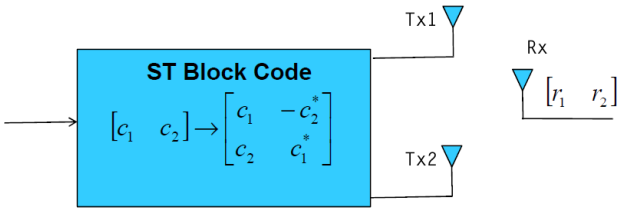

Figura 11: Schema di Alamouti

Un codice STBC è definito da una matrice NxT dove T rappresenta il numero di intervalli di simbolo consecutivi che costituiscono il blocco da trasmettere e N il numero di antenne in trasmissione.

Tabella 2: Codifica e sequenza di trasmissione 2x1 secondo Alamouti

	antenna 1	antenna 2
time t	c_1	c_2
time t+T	$-c_2*$	c_1*

SPATIAL EXPANSION è una tecnica utilizzata quando si hanno a disposizione più antenne rispetto agli *spatial streams*, al fine di utilizzare al meglio la potenza disponibile ed evitare beam forming involontario. SE anche chiamato *cyclic delay diversity* opera inviando copie del segnale con le antenne addizionali in modo che in presenza di un canale caratterizzato da flat fading vi sia una buona ricezione del segnale.

LOW DENSITY PARITY CHECK CODE (LDPC) è una codifica avanzata che appartiene alla classe dei codici blocco lineari caratterizzata da una matrice prevalentemente composta da zeri e solo qualche elemento presenta uni. Tale codifica di avvicina molto alla capacità di shannon definita in [9] dove si dimostra che esiste un valore, detto appunto *capacità del canale*, dove per rate inferiori a tale capacità le trasmissioni risultano affidabili e di conseguenza tale cosa non è possibile per rate superiori. Un ulteriore vantaggio è che l'implementazione di tale tipo di codifica richiede una bassa complessità di decodifica. I vantaggi dell'utilizzo di tale codifica rispetto al BCC (*binary convolutional code*) si possono notare nel grafico in figura 12 dove vi sono descritte le caratteristiche del *packet error rate* (PER) in funzione dell'SNR utilizzando una trasmissione MIMO 2x2 in un canale di 20 MHz tratto da [7].

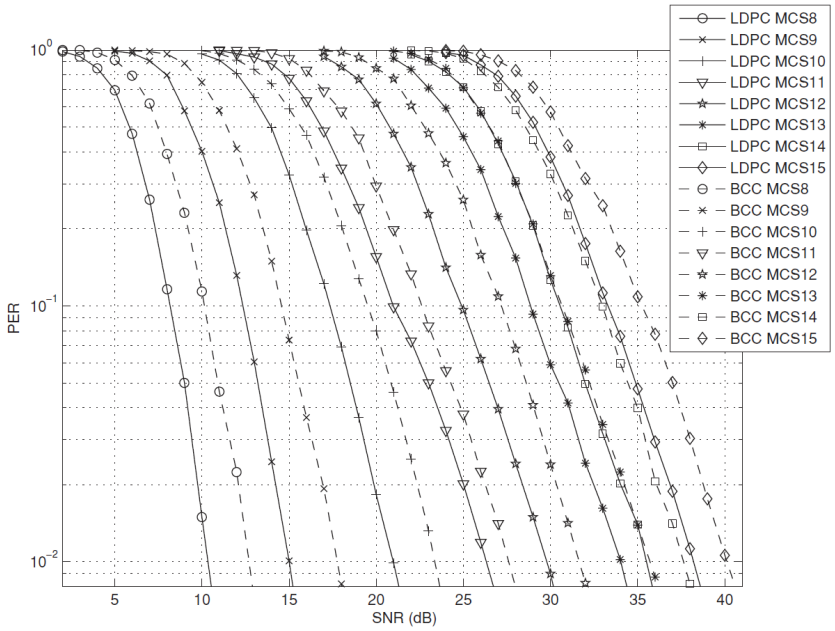

Figura 12: Confronto tra LDPC e BCC, 2x2 in un canale a 20 MHz.

4.3 CANALI A 40 MHZ

Oltre all'utilizzo di MIMO con 802.11n si è introdotta la possibilità di utilizzare canali a 40 MHz quindi raddoppiando la larghezza di banda rispetto agli standard precedenti. I canali a 40 Mhz sono previsti sia per le frequenze attorno ai 2.4 GHz e sia per quelle riguardanti i 5 Ghz. Sono previsti 128 sottoportanti di 312 KHz di ampiezza di cui ne vengono utilizzate 108 per i dati; si può notare quindi che rispetto ai 52 previsti, per HT (*High througput*) il potenziale bit rate è più che raddoppiato come si può notare dalle tabelle 3 e 4 dove volutamente sono stati omessi tutti gli altri MCS previsti dallo standard.

Tabella 3: Schema modulazione e codifica (MCS) per canali a 20 MHz

Indice MCS	Modulazione	R	Data rate (Mbps)
8	BPSK	1/2	13.0
9	QPSK	1/2	26.0
10	QPSK	3/4	39.0
11	16-QAM	1/2	52.0
12	16-QAM	3/4	78.0
13	64-QAM	2/3	104.0
14	64-QAM	3/4	117.0
15	64-QAM	5/6	130.0

Tabella 4: Schema modulazione e codifica (MCS) per canali a 40 MHz

Indice MCS	Modulazione	R	Data rate (Mbps)
8	BPSK	1/2	27.0
9	QPSK	1/2	54.0
10	QPSK	3/4	81.0
11	16-QAM	1/2	108.0
12	16-QAM	3/4	162.0
13	64-QAM	2/3	216.0
14	64-QAM	3/4	243.0
15	64-QAM	5/6	270.0

4.4 INTERVALLO DI GUARDIA RIDOTTO

Per limitare l'interferenza intersimbolo (ISI) si è introdotto un tempo di guardia tra due succesivi simboli OFDM, come si può notare in figura 13.
L'intervallo di guardia va quindi ad aggiungersi al tempo di simbolo.

In ricezione la parte relativa al tempo di guardia non viene

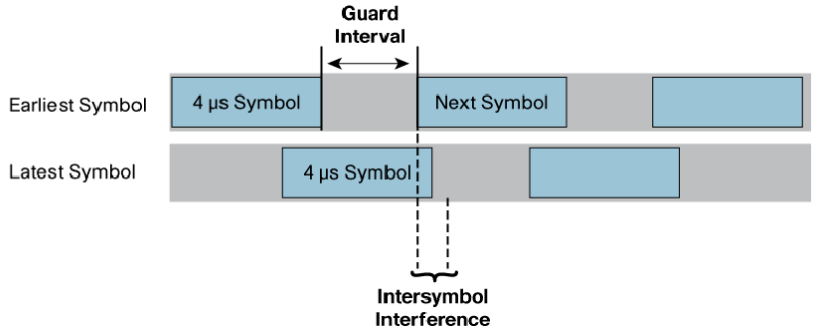

Figura 13: Esempio di intervallo di guardia errato.

considerata al fine di demodulare il simbolo in quanto è la parte che subisce maggiore interferenza dal simbolo precedente.
802.11n utilizza un intervallo di guardia di 800ns che andando ad aggiungersi ai 3.2µs di dati porta ad un periodo di simbolo di 4µs. In alternativa a questo è previsto l'utilizzo di un GI di 0.4ns e quindi un periodo di simbolo di 3.6µs con conseguente aumento di data rate massimo a 289 Mbps per canali a 20 MHz e 600Mbps per quelli a 40MHz. L'utilizzo di tale GI è da considerarsi proibitiva in presenza di canale soggetto ad elevato ritardo [11].

5 MEDIUM ACCESS CONTROL

5.1 PRINCIPALI CARATTERISTICHE MAC

Le stazioni, di seguito STA, devono garantire alcuni servizi di base che devono essere implementati in entrambi i modi operativi descritti nel capitolo 3. Tali servizi hanno come scopo quello di controllare l'accesso alla rete, la consegna dei dati provenienti dagli strati superiori per la comunicazione tra stazioni sul mezzo radio e la protezione dei dati. In particolare i primi servizi sono detti servizi di stazione e devono essere garantiti da tutte le stazioni invece i successivi sono detti servizi di distribuzione e sono forniti dall'AP.

SCANNING una stazione che vuole entrare nella rete scopre un BSS e i relativi parametri legati a tale BSS tramite rilevamento di un pacchetto detto *Beacon*.
Il Beacon è un pacchetto che l'AP invia ad intervalli regolari per rendersi visibile. All'interno vi sono informazioni riguardanti le funzionalità e le caratteristiche del BSS e IBSS in cui è inserita la stazione.

AUTENTICATIONE processo tramite il quale si stabilisce se un client ha il permesso di accedere alla rete attraverso il quale si andrà ad attuare alcune verifiche di sicurezza prima di entrare nella rete.

DEAUTENTICAZIONE processo inverso rispetto al precedente tramite il quale una STA fa richiesta all'AP di essere deautenticata.

TRASMISSIONE scambio di frame a livello MAC tra due stazioni.

SEGRETEZZA questo servizio permette di non poter utilizzare i dati presenti nel mezzo fisico da terzi non autorizzati. Questo è possibile tramite, ad esempio, crittografia dei dati.

ASSOCIAZIONE servizio utilizzato per informare l'AP della presenza della STA all'interno del raggio d'azione dell'AP stesso.

RIASSOCIAZIONE permette ad una stazione di effettuare una transizione di AP all'interno della stessa ESS (vedi fig.7).

DISASSOCIAZIONE processo per terminare un'associazione, è realizzabile sia dalla stazione, che vuole disassociarsi e sia dall'AP nel caso in cui una stazione non sia più raggiungibile.

DISTRIBUZIONE operazione tramite la quale l'AP suddivide i frame e li invia alle stazioni di sua competenza oppure agli altri AP attraverso il sistema di distribuzione

INTEGRAZIONE permette la conversione dei frame dello standard 802.11 in frame appartenenti ad altri standard della famiglia 802. Tale servizio permette, ad esempio, l'interfacciamento di un AP con una LAN cablata che implementa Ethernet (IEEE 802.3).

In figura 14 vi è lo schema di scambio servizi offerti tra livelli dello stack protocollare. Come si può notare all'interno dello stesso utente rappresentato in questo caso con tramite STA1 oppure STA2 i servizi sono forniti tramite lo scambio di SDU (*service data unit*) ed in particolare MSDU (*MAC SDU*) tra LLC e MAC e PSDU (*Physical Layer SDU*) tra MAC e Physical Layer.

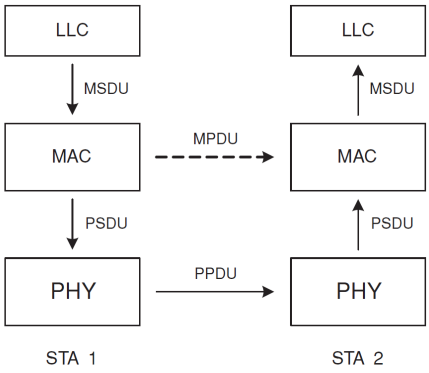

Figura 14: Scambio di SDU e PDU all'interno dello stack protocollore.

Per quanto riguarda lo scambio di informazioni tra livelli uguali ma di utenti diversi questo avviene tramite le PDU (*pro-*

tocol data unit) che come avveniva per le SDU prendono nomi diversi a seconda dei livelli interessati.

5.1.1 Acknowledgement

Il canale wireless è incline a errori e per rendere la trasmissione affidabile è previsto un sistema di acknowledgement.

Una stazione che riceve un frame corretto invierà a sua volta un frame ACK al mittente del frame ricevuto. Quest'ultimo all'effettiva ricezione avrà conferma che la trasmissione è avvenuta in modo positivo. Se la stazione non riceve nessun frame di ACK ritrasmette il pacchetto in quanto assume che non sia stato ricevuto.
In figura 15 vi è un esempio della procedura base di acknowledgement.

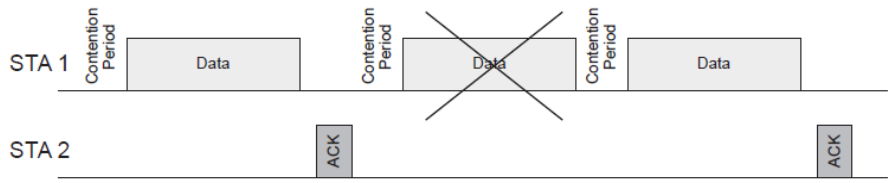

Figura 15: Esempio di sequenza temporale di scambio pacchetti data e ACK.

5.1.2 Frammentazione

L'invio di pacchetti di grande durata può impiegare il mezzo trasmissivo per parecchio tempo soprattutto utilizzando modulazioni che impiegano bassi rate di trasmissione come BPSK o QPSK. In questo modo il pacchetto è soggetto ad un elevato errore e di conseguenza si va ad aumentare il numero di ritrasmissioni, infine la durata maggiore del tempo dedicato ad un pacchetto porta a variazioni sensibili per tutta la durata della trasmissione di quest'ultimo. Per risolvere questo problema si è deciso di frammentare i pacchetti in pacchetti di minore durata con conseguente riduzione della probabilità di errore, infine con tale tecnica in caso di ricezione di pacchetto errata, basta trasmettere solamente la parte corrotta dell'intero pacchetto originale e non tutto il frame. Questa tecnica però porta a dei peggioramenti in fatto di thoughput dovuto a un aumento del-

l'overhead dovuto al fatto che le sezioni del frame di partenza verranno inviate tramite diverse MPDU e incapsulate in diverse PPDU.

5.1.3 Time Slot e IFS

All'interno della rete sono definiti degli intervalli di tempo multipli di un tempo detto di slot t_{slot} che quindi rappresenta l'unità temporale del sistema e dipende dalla realizzazione del livello fisico.
Gli intervalli di tempo definiti IFS *Interframe Space* possono essere di quattro tipi che in ordine di durata sono: SIFS, separa le trasmissioni di uno stesso dialogo; PIFS offre priorità al PDF per eventuali operazioni a maggior priorità; DIFS usato dalle stazioni che attendono il canale libero e infine EIFS usato al posto di DIFS dalle stazioni che hanno ricevuto un frame incomprensibile per il quale non è possibile effettuare l'aggiornamento del NAV (sezione 5.1.4).

5.1.4 Procedure di base per l'accesso al mezzo

Quando una stazione vuole trasmettere dedica un tempo DIFS per effettuare il *sense* sia fisico (rilevando le trasmissioni) e sia a livello MAC tramite una procedura che va a consultare il NAV (tale procedura verra spiegata nel seguito del capitolo).

Se il canale risulta libero vi sono due metodi con i quali può avvenire la trasmissione:

- ***DCF base:*** se il canale è libero una stazione può inviare il frame e solo dopo aver atteso un tempo SIFS riceverà dall'AP l'ACK. Se la stazione trasmettitrice ha frammentato il pacchetto potrà inviare i successivi frame dopo aver atteso solamente uno SIFS per ogni frame, garantendo in questo modo priorità alla trasmissione in atto. Un nodo che sente il canale occupato setta un contatore NAV *Network allocation vector*. Tale contatore è impostato per tutto il tempo della durata della comunicazione e si decrementa automaticamente, il canale è libero quando il NAV ha valore 0.

- ***DCF con handshaking:*** nel caso vi siano molte stazioni all'interno della rete e, in presenza di terminali nascosti,

tramite questo metodo si effettua una prenotazione del canale per evitare collisioni. Vengono utilizzati due pacchetti, *request to send* (RTS) per richiedere l'utilizzo del canale e *clear to send* (CTS) di risposta a un RTS. Dopo l'invio da parte di una stazione di un RTS, la stazione o l'AP al quale era indirizzato il RTS risponde con un CTS.
Le stazioni che non partecipano a questa sequenza settano il loro NAV per tutta la durata della trasmissione.

Per quanto riguarda il settaggio del NAV da parte delle stazioni in ascolto esso avviene tramite il rilevamento del parametro *Duration* nell'header del MAC.
Il meccanismo del rilevamento delle collisioni avviene dopo la verifica del CRC nel pacchetto dati da parte della stazione ricevente.
Quando la trasmissione di una stazione collide viene scelto casualmente un valore da una finestra fra $[0, CW_{min}]$ (*finestra di backoff*) e tale valore viene moltiplicato per t_{slot}. Tale intervallo di tempo (*backoff*) sarà il tempo che una stazione dovrà attendere prima di effettuare nuovamente il sense del canale e avviare quindi la procedura di trasmissione. Nell'eventualità che la la stazione collida per più di una volta l'intervallo della finestra di backoff varierà per un tempo compreso tra o e CW_i dove quest'ultimo valore è $CW_i = [2 \cdot (CW_{i-1} + 1)] - 1$ dove i rappresenta il numero di tentativi. Come si può notare utilizzando questa tecnica ad ogni tentativo avremo un raddoppio della finestra di backoff con conseguente dimezzamento della probabilità di andare a collidere nuovamente.

Come anticipato nel capitolo 3 vi è un'infrastuttura di rete opzionale: la PCF (*point coordination function*) che garantisce alle stazioni che la implementano una priorità di traffico rispetto a quelle che utilizzano DCF.
Tramite PCF vi è un controllo centralizzato coordinato dal *point coordinator* PC che stabilisce un periodo *contention free period* CFP dove è lui che regola l'accesso al mezzo. Tale controllo è permesso in quanto vi è l'utilizzo di PIFS, intervallo di tempo più breve rispetto al DIFS.

Durante il CFP viene settato il NAV al massimo del suo valore per impedire la trasmissione alle stazioni e il trasferimento di dati è basato su un protocollo di polling appunto controllato da PC. Infine è previsto che una stazione alla quale sono destinati dei dati possa mettere l'ACK in coda ad eventuali dati

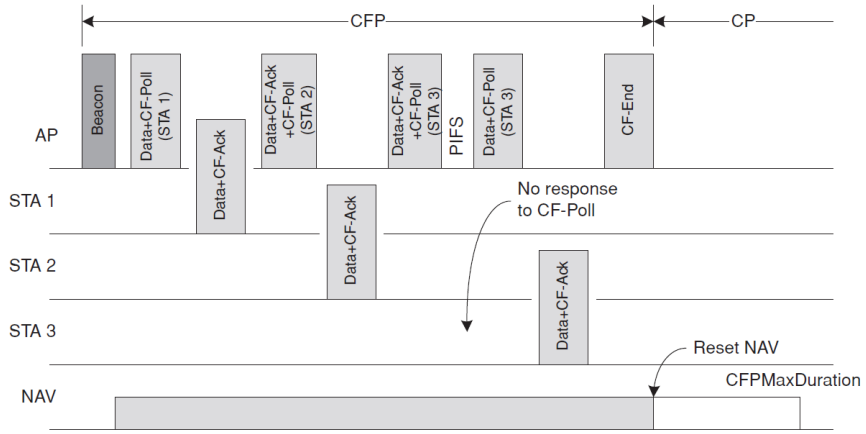

Figura 16: Sequenza di trasferimento dati in Contention Free Period.

di risposta. In figura 16 vi è un esempio di trasferimento dati durante CFP. Solitamente è l'AP che svolge la funzione di point coordinator ed ha il compito di resettare il NAV se eventualmente termina il CFP prima della durata massima stabilita precedentemente. Dopo di questo riprendono le trasmissioni DCF all'interno del *contention period* CP.

5.2 IEEE 802.11E

Ulteriori funzioni disponibili a livello mac sono introdotte da 802.11e e più in particolare in termini di QoS [6] . Tramite questo protocollo è introdotta una funzione che opera al di sopra della DCF l' *hybrid coordination function* (HCF).
In modo molto simile a quanto avveniva per il PCF vi è un *hybrid coordinator* (HC) con funzioni di coordinazione al quale le stazioni chiedono di entrare a far parte del *transmit opporunities* (TXOP).
Il TXOP è uno spazio di tempo riservato dove una stazione può trasmettere uno o più frame all'interno della rete senza interruzioni da parte di trasmissioni provenienti dalle altre stazioni. Tale procedura è possibile anche in modo periodico dove l'HC invita la stazione a trasmettere preservando eventuali accessi da parte degli altri utenti. Il protocollo introduce due differenti schemi di accesso:

EDCA *enhanced distributed coordination access*: tramite questa tecnica vi è la creazione di classi di accesso utilizzando AIFS[i] *arbitration inter frame space* al posto di DIFS dove i indica la classe di appartenenza. Quest'ultima determina diffe-

renti valori di CW_{min} e CW_{max} nella contention window. In questo modo vi è una distinzione per quanto riguarda la priorità d'accesso ed inoltre la stazione che vince la contesa ottiene un TXOP dove può inviare più di un pacchetto per un periodo di tempo prefissato.

HCCA *hybrid coordination function controlled channel access*: tramite tale tecnica di accesso l'HC, dopo aver verificato che il canale sia libero per almeno uno PIFS e senza aspettare ulteriore periodo di backoff, può allocare TXOPs in modo da ottenere maggiore priorità rispetto all'utilizzo di EDCA. In questo modo l'HC può richiedere dati alle stazioni presenti nella rete tramite CF-Poll. L'HC è responsabile anche di determinare i parametri riguardanti TXOP quali la massima durata e il tempo di inizio. E' prevista inoltre un'ulteriore funzione di polling da parte dell'HC la quale richiede delle informazioni di feedback da parte delle stazioni attraverso un meccanismo di contesa controllato basato sulla categoria di traffico di appartenenza.

5.2.1 Block ACK

Un'ulteriore tecnica introdotta da 802.11e è quella del *Block ACK*, meccanismo che consente di trasmettere più frame di dati separati da SIFS prima ancora di ricevere alcun ACK. Sono previsti due tipi di Block ACK: *immediato* e *ritardato*. Nel primo caso dopo una sequenza di frame inviati vi è la richiesta di un block ack al quale il destinatario deve rispondere all'interno dello stesso TxOP. Per quanto riguarda invece il Block ACK ritardato alla richiesta del block ack la stazione alla quale era destinata la sequenza di pacchetti risponde con un semplice ACK all'interno dello stesso TxOP; in un altro TxOP quest'ultima invierà l'effettivo Block ACK e la stazione sorgente risponderà con un

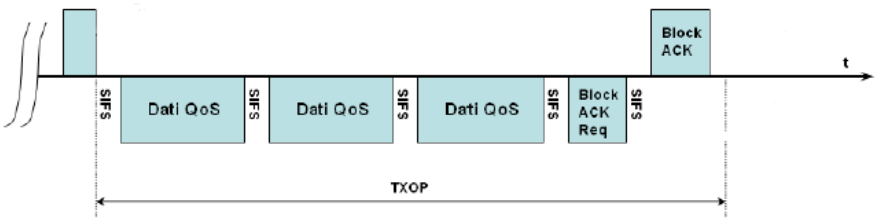

Figura 17: Sequenza di trasferimento dati tramite Block ACK Immediato.

semplice ACK, tale tecnica introduce latenza per permettere al ricevitore di verificare i dati ricevuti. Le due differenti tecniche sono riassunte nelle figure 17 e 18. L'utilizzo della tecnica di Block ACK necessita di un processo di negoziazione e setup tra le stazioni che intendono utilizzarla.

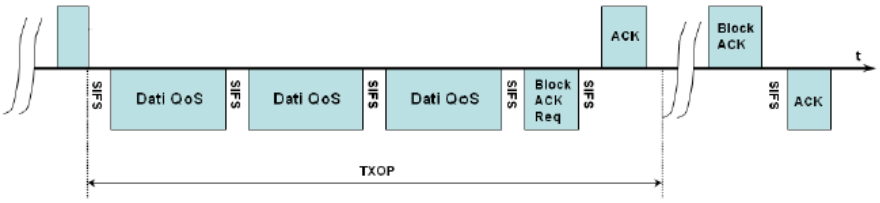

Figura 18: Sequenza di trasferimento dati tramite Block ACK Ritardato.

5.3 MAC 802.11n

I miglioramenti portati dal livello fisico per quanto riguarda il rate di trasmissione non vengono sfruttati al massimo senza modificare anche il livello MAC. Come si può notare in figura 19 il throughput aumenta linearmente per valori bassi di rate fisico per poi andare ad aumentare molto più lentamente per valori elevati di quest'ultimo. Tale comportamento è da attribuire al fatto che l'overhead necessario da supporto al MIMO è nettamente superiore rispetto alle precedenti versioni di 802.11. Con lo scopo di aumentare il throughput sono state introdotte delle tecniche quali l'aggregazione di frame e modifiche al block ack che hanno portato ad un aumento lineare del throughput in funzione del rate fisico.

Per quanto riguarda il block ACK i miglioramenti introdotti da 802.11n sono mirati alla riduzione dello spazio inter-frame, si è arrivati alla conclusione che la durata di uno SIFS è eccessiva e si reputa necessario solamente attendere un intervallo di tempo affinche il ricevitore sia disponibile a ricevere il pacchetto successivo. Ulteriori miglioramenti sono possibili eliminando lo spazio interframe, eliminando la richiesta di block ACK (BAR) e riducendo la dimensione del BA. I miglioramenti della tecnica di Block ACK introdotti da 802.11n sono riassunti in figura 20.

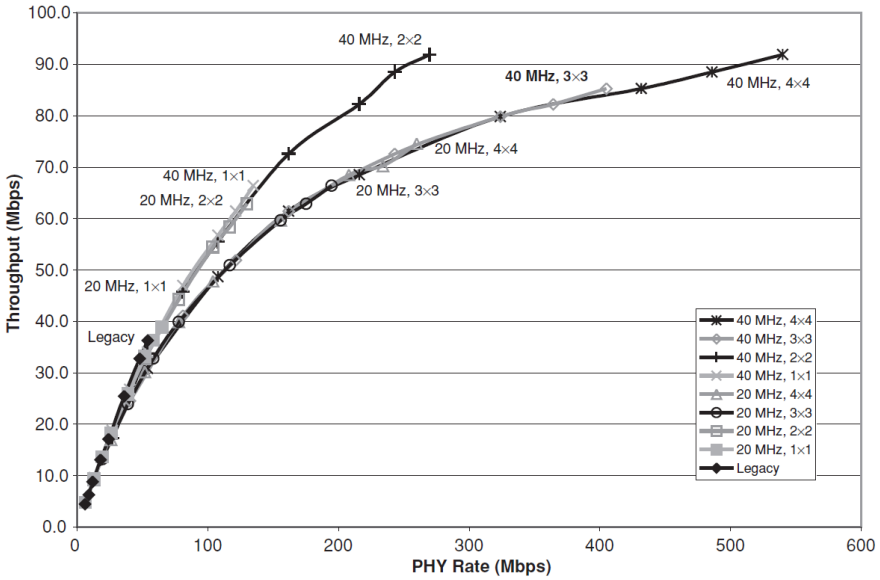

Figura 19: Throughput in funzione del rate fisico senza modifiche al livello MAC.

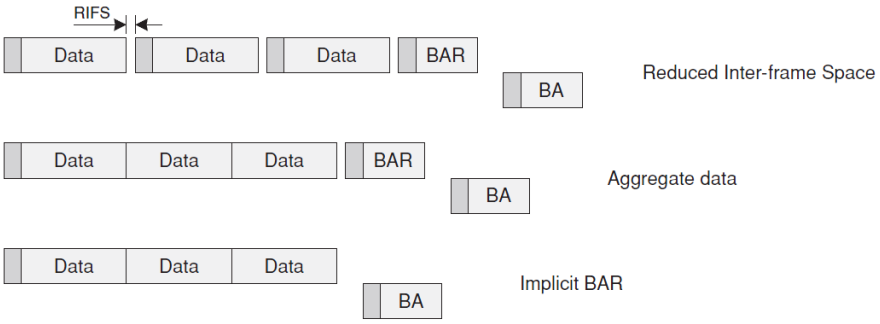

Figura 20: Miglioramenti al meccanismo di Block ACK in 802.11n

5.3.1 Aggregazione

I miglioramenti apportati al meccanismo di block ACK non erano sufficienti a migliorare in modo consistente il throughput complessivo del sistema e quindi 802.11n ha introdotto delle tecniche di aggregazione dei pacchetti. Ciò può sembrare contraddittorio rispetto alla tecnica della frammentazione discussa nel paragrafo 5.1.2 ma come si può intuire tale tecnica in presenza di rate fisici elevati porta solamente piccoli miglioramenti quasi trascurabili.
Facendo riferimento alla figura 14 vi sono due tipi di aggregazione che vanno ad interessare MSDU e MPDU che sono definiti rispettivamente A-MSDU e A-MPDU.
Nel caso di A-MSDU le MSDUs ricevute da LLC appartenenti

allo stessa categoria di servizio e indirizzate allo stesso destinatario vengono inserite in un unico MPDU. Tutto ciò porta a una riduzione di bit da inviare a parità di dati reali e, come conseguenza di questo, vi è un aumento di throughput.
Nel caso invece di A-MPDU esso porta ad un incapsulamento dei pacchetti in modo da preparare un unico PPDU inserendo quindi un unico preambolo radio. In figura 21 si può notare come dopo le varie modifiche al livello ora il thruoghput aumenti linearmente anche con il rate fisico.

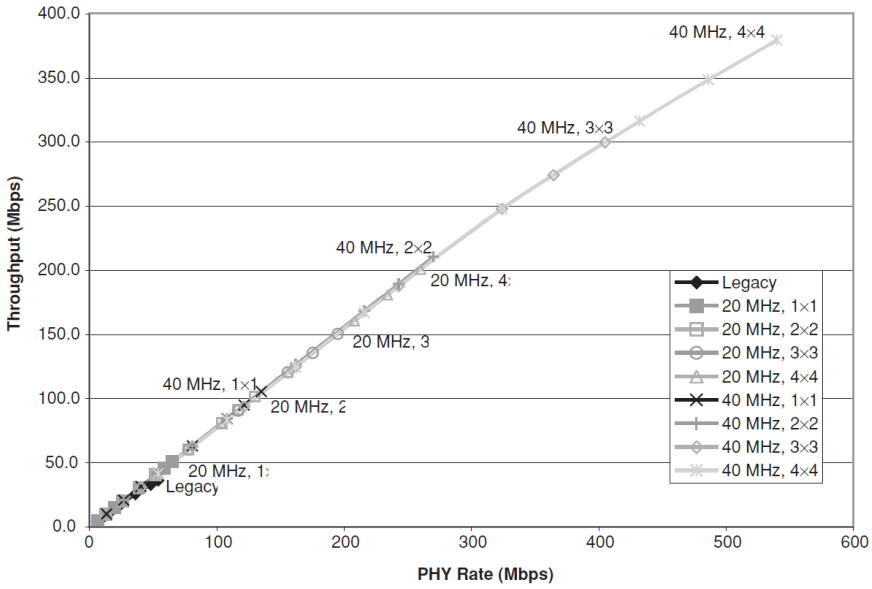

Figura 21: Thruoghput in funzione del rate fisico dopo i miglioramenti al livello MAC

5.3.2 Power-save multi poll

Power-save multi poll (PSMP) è una tecnica di ottimizzazione di accesso al mezzo che lavora assieme al HCCA. E' un meccanismo di polling tramite il quale l'AP inizia le trasmissioni inviando uno schema dei tempi riservati. Un esempio di questo sono i tempi destinati al downlink oppure all'uplink, in modo tale che il client può determinare quando deve rimanere attivo e operare quindi tecniche di risparmio energetico.

6 ASPETTI DI 802.11N PER APPLICAZIONI INDUSTRIALI

In questo capitolo verranno proposte delle idee per l'applicazione dello standard 802.11n per applicazioni industriali. L'analisi delle novità introdotte da questo standard rispetto ai precedenti porta ad alcune considerazioni per un'eventuale implementazione.
Secondo i criteri presentati nel capitolo 2 emerge come fondamentale punto di partenza l'implementazione di MIMO. Diverse sono le tecniche presentate nel paragrafo 4.2 per quanto concerne il livello fisico. Alcune richiedono delle capacità di calcolo non indifferenti come ad esempio LDPC che prevede una codifica piuttosto pesante dei dati da trasmettere anche se la decodifica è semplice, altre invece come TxBF richiedono una conoscenza del canale (feedback) per poter regolare la trasmissione secondo quest'ultimo.
Un interessante sviluppo potrebbe riguardare la spatial expansion, tecnica che richiede invece l'impiego di molte antenne. Questo potrebbe essere sfruttato dagli access point piuttosto che delle singole stazioni in quanto in ambiente industriale queste ultime sono rappresentate il più delle volte da sensori/attuatori. Infine STBC potrebbe essere sfruttato per aggiungere ridondanza ai segnali trasmessi in modo da garantire maggior efficienza portando quindi ad una diminuzione di ritrasmissioni. Un'ulteriore modifica al livello fisico portata da 802.11n è l'intervallo di guardia ridotto che però va evitato in presenza di canali particolari [7] come nel caso industriale.
Le tecniche di accesso al mezzo introdotte vanno a migliorare le novità introdotte da 802.11e. Le modifiche apportate alla tecnica del block ACK andrebbero applicate facendo alcune distinzioni: in [13] si distinguono due tipi di trasmissioni *traditional industrial traffic* che riguarda lo scambio di dati caratteristico dell'automazione industriale e *industrial multimedia traffic* che riguarda invece il trasferimento di dati come il controllo video il quale richiede, rispetto al precedente, una quantità di dati nettamente maggiore.

La tecnica del block ACK potrebbe venire utilizzata nel caso di industrial multimedia traffic in modo da occupare per meno tempo il canale trasmissivo. Con il traffico tradizionale tale tecnica non potrebbe essere nemmeno utilizzata in quanto richiede da parte del trasmettitore la presenza di molti dati da trasmettere cosa che solitamente non avviene nel caso di reti di sensori in quanto il traffico generato è rappresentato da pochi dati molto spesso costituito anche da un solo parametro.
La tecnica dell'aggregazione presentata nel paragrafo 5.3.1 necessita anche quella di un traffico elevato proveniente da un sola stazione e quindi anche per questo si possono trarre le stesse conclusioni risultate dall'utilizzo di Block ACK.
In ambiente industriale si opera tramite reti di sensori che oltre a presentare un flusso di dati molto basso, hanno a disposizione poca potenza di trasmissione. Inoltre ad un certo punto si è costretti a valutare tra consumo energetico, impiego di potenza di calcolo o l'aggiungere ridondanza tramite codifica. La diversità spaziale introdotta da MIMO da un lato aumenta notevolmente l'efficienza ma dall'altro richiede un consumo dovuto alla complessità computazionale.
Infine come evidenziato da [13] non vi è alcun riferimento a tecniche di adattamento di rate o meglio vi è indicata la possibilità di modificare i rate di trasmissione (*fall back rate*) ma lo standard non definisce come operare in tal senso. Quindi affianco alle innovazioni introdotte data la natura del mezzo fisico si dovranno sviluppare delle tecniche di ARF (*automatic rate fallback*) per andare a contrastare le variazioni del canale ed ottenere delle trasmissioni che soddisfino le specifiche evidenziate nel capitolo 2.

7 CONCLUSIONI

Le innovazioni sviluppate da 802.11n erano mirate ad aumentare il throughput massimo per equiparare o almeno avvicinarsi ai rate di trasmissione tipici di 802.3 proponendo però modulazioni difficilmente applicabili in ambito industriale. Inoltre le tecniche di trasmissione MIMO applicate a sensori che il più delle volte contengono pochissimo hardware andrebbero analizzate sia da un punto di vista economico e sia per quanto riguarda il risparmio energetico che assume una rilevante importanza in tale ambito.
Nonostante tutto, l'introduzione di MIMO è un punto di partenza per migliorare in modo radicale le trasmissioni aumentandone l'efficienza e migliorare quindi la qualità del servizio fornita. Inoltre come tutti i protocolli della famiglia 802.11 è importante il fatto che, come è avvenuto con i precedenti, anche con questo protocollo si sia mantenuta la compatibilità con le versioni preesistenti in modo da poter utilizzare hardware già presente in impianti o comunque in commercio.
Per la stesura di tale tesina è stata volutamente omessa la trattazione del formato dei pacchetti, lunghezza e composizione, in quanto tale approfondimento esula dagli scopi di questo lavoro. Per eventuali riferimenti completi si fa riferimento allo standard stesso oppure una trattazione completa è presente in [7].

BIBLIOGRAFIA

[1] Siavash Alamouti. "A simple Transmit Diverity Tecnique for Wireless Communications". In: *IEEE JOURNAL ON SELECT AREAS IN COMMUNICATION* (1998).

[2] *Sources of Disturbances on Wireless Communication in Industrial and Factory Environment*. Asia-Pacific International Symposium on Electromagnetic Compatibility. 2010.

[3] Nevio Benvenuto e Michele Zorzi. *Principles of Communications Networks and Systems*. Wiley, 2011.

[4] Mario Fossi. "Elementi di modulazione OFDM". 2009.

[5] Andrew H. Kemp e Edmund B. Bryant. "Channel Sounding of Industrial Sites in the 2.4 GHz ISM band". In: *Wireless Personal Communications* 31 (2004), pp. 235–248. URL: http://dx.doi.org/10.1007/s11277-004-4169-z.

[6] Stefan Mangold et al. "IEEE 802.11e Wireless LAN for Quality of Service". In: *XXX* (20XX).

[7] Eldad Perahia e Robert Stacey. *Next generation wireless LANs*. Cambridge University press, 2008.

[8] Theodore Rappaport. *Wireless Communications: Principles and Practice*. 2nd. Prentice Hall PTR, 2001.

[9] C. Shannon. "A mathematical theory of communication". In: *The Bell System Technical Journal* (1948).

[10] A.U.H. Sheikh e Y.D. Al-Moallem. "On the design of a wireless network in an industrial environment". In: *Communication Systems (ICCS), 2010 IEEE International Conference on*. 2010, pp. 756 –760.

[11] Michael Speth et al. "Optimum receiver design for wireless Broad Band system using OFDM". In: *IEEE TRANSACTION ON COMMUNICATIONS* (1999).

[12] Andrew S. Tanenbaum. *Computer Networks* 4^{th} *edition*. Prentice Hall PTR, 2002.

[13] S. Vitturi et al. "On the Rate Adaptation Techniques of IEEE 802.11 Networks for Industrial Applications". In: *Industrial Informatics, IEEE Transactions on* PP.99 (2012), p. 1. ISSN: 1551-3203. DOI: 10.1109/TII.2012.2189223.

[14] A. Willig, K. Matheus e A. Wolisz. "Wireless Technology in Industrial Networks". In: *Proceedings of the IEEE* 93.6 (2005), pp. 1130 –1151.

[15] Andreas Willig. "Recent and Emerging Topics in Wireless Industrial Communication: A Selection". In: *IEEE TRANSACTION ON INDUSTRIAL INFORMATICS* (2008).

[16] Andreas Willig et al. "Measurement of a wireless link in a industrial environment using an IEEE 802.11 - Compliant Physical layer". In: *IEEE TRANSACTION ON INDUSTIAL ELECTRONICS* (2002).