Reti Wireless e Mobili

Indice

1. Lezione 01 [25/02] 3
1.1. Principi di Teoria della Trasmissione 3
2. Lezione 02 [26/02] 5
2.1. Ancora basi di teoria della trasmissione 5
2.2. Multiplexing 6
2.3. Comunicazione wireless 6
3. Lezione 03 [04/03] 8
3.1. Codifica e trasmissione dei dati 8
4. Lezione 04 [05/03] 11
4.1. Esercizi 11
4.2. OFDM [Orthogonal Frequency Division Multiplexing] 11
4.3. Spread Spectrum 12
4.3.1. Frequency Hopping Spread Spectrum 12
4.3.2. Direct Sequence Spread Spectrum 12
5. Lezione 05 [11/03] 14
5.1. WPAN 14
5.1.1. Personal Area Network [bluetooth] 15
6. Lezione 06 [12/03] 17
7. Lezione 07 [18/03] 19
7.1. Ancora BT 19
8. Lezione 08 [19/03] 22
8.1. ZigBee + Matter & Thread 22
8.1.1. ZigBee 22
8.1.2. Matter & Thread 25
9. Lezione 09 [25/03] 26
9.1. WLAN 26
10. Lezione 10 [26/03] 29
10.1. Problema del terminale nascosto 29
10.2. Frammentazione 29
10.3. Infrastruttura 29
11. Lezione 11 [01/04] 31
12. Lezione 12 [02/04] 34
12.1. Sicurezza in WiFi 35
12.2. Eduroam 35
12.3. Ultimi WiFi 36

1. Lezione 01 [25/02]

1.1. Principi di Teoria della Trasmissione

Tipicamente è uno schema del tipo

$$d(t) \to \text{trasmettitore} \to s(t) \to \text{channel} \to s(t) \to \text{receiver} \to d(t)$$

con dati analogici/digitali che vengono passati al trasmettitore (ho una sequenza di bit). s è segnale, d è dato.

Questo schema però è utopico, non è mai cosi: infatti, il canale è soggetto a

- rumore
- attenuazione (certa potenza che piano piano si perde, si affievolisce)
- interferenze

Ci esce un $s'(t)$ che esce dal canale. Ci saranno casi di s' impossibile da riconoscere oppure casi di s' che partono da un s cosi robusto da poterlo sistemare.

Segnale analogico:

- ha una variazione continua e non ci sono interruzioni/discontinuità

Segnale digitale:

- mantiene un livello di segnale costante per un determinato intervallo, con un rapido (quasi istantaneo) cambio di livello

I grafici sono nel dominio del tempo, ovvero come varia la misurazione nel tempo

Il segnale analogico, se periodico, è una sinusoidale

$$s(t) = A\sin(2\pi ft + \phi)$$

con 3 parametri sui quali giochiamo:

- A ampiezza, massimo livello o forza del segnale nel tempo (volt)
- f frequenza quanti cicli fa al secondo (Hertz)
- ϕ fase posizione relativa all'interno del periodo, dove parte

Abbiamo anche il periodo T inverso della frequenza, tempo impiegato per un ciclo. Infine anche la lunghezza d'onda λ che è la distanza occupata da un singolo ciclo, ed è tale che $\lambda = \frac{c}{f} = Tc$ con c velocità della luce, lunghezza spaziale.

Metti 4 esempi

Nel dominio delle frequenze, ogni segnale ragionevolmente periodico può essere scomposto in una serie di segnali periodici (onde seno e coseno) con ampiezza, frequenza e fase differenti. Idea di Fourier ad inizio 1800. Una serie di Fourier è tale che

$$s(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

dove $f = \frac{1}{T}$ è la frequenza fondamentale ($n = 1$), a_n e b_n sono le ampiezze delle singole componenti dette armoniche e c è una costante che è il valore medio del segnale. Partendo dalla f fondamentale, ogni armonica avrà un multiplo di questa frequenza fondamentale.

Dato un grafico, come facciamo a determinare le ampiezze di ciascuna componente? Con quale frequenza dobbiamo campionare il nostro segnale?

Teorema 1.1.1 (Teorema del campionamento di Shannon): La frequenza di campionamento deve essere almeno il doppio della frequenza massima del segnale in ingresso.

Per passare dal dominio del tempo al dominio delle frequenze usiamo la FFT (Fast Fourier Transform), ovvero passiamo il campionamento fatto alla FFT e mi genera le frequenze. La Inverse FFT passa dalle frequenze al tempo.

Quando tutte le frequenze sono multipli interi di una frequenza base f (frequenza fondamentale, le altre sono kf armoniche), il periodo del segnale $s(t)$ è il periodo della frequenza fondamentale. Lo **spettro** (spectrum) del segnale è il range di frequenze che lo contiene. La absolute bandwidth è l'ampiezza dello spettro (max - min)

ESEMPIO

Trasmettiamo due bit per ogni due bit, quindi il data rate è di 2f bits. Maggior parte energia concentrata nelle prime frequenze (kf –> ampiezza 1/k), effective bandwidth

La capacità del canale è il massimo bit rate alla quale è possibile trasmettere dati su un canale di comunicazione in determinate condizioni. Il noise è un segnale NON VOLUTO che si combina al segnale trasmesso che lo altera o distorce. L'error rate, o tasso di errore, a questo livello si intende bit error rate.

Esempio che non capisco

Considerazioni: impulso rettangolare ha banda infinita, noi vogliamo usare una banda finita. Banda minore ha maggiore distorsione

Scelgo la banda finita più ampia? Ho costi economici e limitazioni del dispositivo

Nyquist bandwidth

Dato un canale noise-free (ideale) la bandwidth limita il data rate

Ovvero, la Nyquist capacity ha un binary signals (2 livelli di voltaggio) quindi C=2B o ha un multilevel signaling C=2B log_2(M) (con M numero di segnali discreti o livelli di voltaggio)

Il rumore è un segnale non voluto che si combina al segnale trasmesso che lo altera e distorce. Può essere:

- thermal noise
- intermodulation noise
- cross talk
- impulse noise

2. Lezione 02 [26/02]

2.1. Ancora basi di teoria della trasmissione

Rumore termico: agitazione delle molecole. Intermodulation noise problemi tra le diverse modulazioni, ci si accavalla per trasmettere. Cross talk è più nel parlato. Impulse noise, impulso elettromagnetico specifico, distrugge il segnale che è attraversato.

Il decibel (dB) è una misura che rapporto tra due potenze (scala logaritmica), ovvero

$$\left(\frac{P_1}{P_2}\right)_{dB} = 10\log_{10}\left(\frac{P_1}{P_2}\right).$$

Fare un +-3 fa doppio/metà.

Il decibel-milliWatt (dBm) è l'unità di misura del rapporto tra una potenza arbitraria e una potenza di 1mW (milliWatt), ovvero

$$P_{dBm} = \frac{P}{1mW}.$$

Il rumore c'è sempre: il rapporto segnale rumore (signal to noise ratio SNR) è il rapporto tra la potenza del segnale trasmesso e la potenza del rumore, ovvero

$$(SNR)_{dB} = 10\log_{10}\left(\frac{\text{signal power}}{\text{noise power}}\right).$$

Più è alto più il segnale è forte rispetto al rumore

La Shannon Capacity Formula rappresenta la massima capacità teorica di un canale in bit al secondo in funzione del SNR, ovvero

$$C = B\log_2(1 + SNR)$$

dove B è la banda. Risultato puramente teorico e considera solo il thermal noise, tuttavia fornisce un limite superiore alla quantità di informazione (data rate) che può essere trasmessa senza errori.

In una determinata condizione di rumore (SNR) possiamo aumentare il data rate:

- aumentando la banda B ma il rumore termico è rumore bianco e maggiore è la banda e maggiore sarà il rumore che entrerà nel sistema
- aumentando la potenza del segnale, allora SNR++ ma sarà maggiore l'intermodulation e il cross talk noise

Esempio 2.1.1: Supponiamo di avere uno spettro tra $3MHz$ e $4MHz$ e SNR = 24dB. La banda vale quindi 1MHz e SNR è 251

La capacità di Shannon è C = 8Mbps

Ora facciamo inverso di Nyquist

Se $C = 2B\log_2(M)$ andiamo a ricavare $M = 16$

Esempio 2.1.2: Altro esempio

2.2. Multiplexing

In quasi tutti i casi la cpaacità del mezzo di trasmissione è superiore alla capacità richiesta da una trasmissione. Vogliamo combinare sullo stesso link più trasmissioni. Abbiamo un maggior data rate con un minore costo kbps. Le singole comunicazioni richiedono un data rate inferiore rispetto alla capacità del link.

FDM frequency division multiplexing, sfrutta il fatto che la banda disponibile sul mezzo di trasmissione eccede la banda richiesta da un singolo segnale. Divido la banda totale in sotto-bande, ognuna delle quali è canale parallelo.

TDM time division multiplexing sfrutta il fatto che il data rate del mezzo di trasmissione eccede il data rate richiesto da un singolo segnale. Sono robe pseudo-parallele

2.3. Comunicazione wireless

Trasmissione in banda base (baseband), ovvero ho dato digitale, che diventa analogico, canale, riconvertito, eccetera.

Per gestire sto segnale ho la banda B, dove parte? Dove arriva? Usiamo per semplicità 0 a B. Problemi:

- se tutti i dispositivi usano questo le comunicazioni interferiscono
- più è bassa la frequenza e più l'antenna deve essere grande
- ogni range di radio frequenze (RF) possiede diverse proprietà di propagazione e attenuazione

Soluzione è la banda traslata (o passa banda), ovvero ho sempre B ma ho una frequenza portante (frequency carrier) e il mio range di trasmissione è

$$f_c - \frac{B}{2} \rightsquigarrow f_c + \frac{B}{2}$$

Ora il trasmettitore, che prende il dato, lo codifica, lo modula con la portante f_c, fa il power control (amplificatore) e poi lo manda. Il bro invece fa de-modulazione e il decoding.

Ci chiediamo:

- quale spettro utilizzare (f_c)?
- come codifico i dati?
- come modulo il mio segnale in banda base sulla portante?

L'encoding symbol e symbol rate

Un simbolo è una forma d'onda, uno stato o una condizione significativa del canale di comunicazione che persiste per un intervallo di tempo fissato

Il symbol rate è il numero di simboli trasmetti al secondo, misurato in baud

In generale un simbolo può contenere più bit (codifica e modulazione), quindi symbol rate diverso da bit rate

Una data banda può supportare diversi data rate, a seconda dell'abilità del ricevente di distinguere 0 e 1 in presenza di rumore. Un simbolo può codificare più bit alla stessa frequenza.

La trasmissione che faremo noi è la radio Line of sight (LOS), ovvero sono in linea. Soffre di:

- free space loss & path loss (attenuazione del segnale dovuta alla distanza e all'ambiente in cui il segnale si propaga)
- rumore (disturbo che distorce il segnale)
- multipath (il segnale tra TX e RX può subire riflessioni, diffrazioni e scattering, causando la ricezione di più onde elettromagnetiche dello stesso segnale in tempi diversi)
- effetto Doppler (il segnale cambia a causa del movimento di TX, RX e ostacoli)

Il path loss è l'attenuazione del segnale radio in funzione della distanza tra TX e RX, ovvero

$$\frac{P_t}{P_r} = \left(\frac{4\pi}{\lambda}\right)^2 d^n = \left(\frac{4\pi f}{c}\right)^2 d^n$$

misurato in decibel. Questo è direttamente proporzionale alla frequenza (al quadrato), ad una potenza della distanza e n dipende dall'ambiente. Se free space ho praticamente una sfera, più sono lontano e meno ho segnale. Perdiamo sempre potenza, anche se non abbiamo rumore, e dipende tutto da quella formula.

3. Lezione 03 [04/03]

Se $n = 2$ nel free space loss allora

$$L_{dB} = 10 \log\left(\frac{P_t}{P_r}\right) = 20 \log\left(\frac{4\pi f}{c}\right)$$

A parità di distanza, maggiore è la frequenza e maggiore è il path loss. La potenza di trasmissione è regolamentata. A parità di potenza, maggiore è la frequenza e minore è il raggio di copertura (segnali sufficientemente forte da essere utilizzabile).

Antenne sono isotropiche (ideali), ovvero sono sfere. Un'altra ideale è quella direzionale, tipo ellisse. Il gain (guadagno) dell'antenna è definito come il rapporto tra l'intensità della radiazione elettromagnetica in una data direzione e l'intensità che si avrebbe se si usasse un'antenna isotropica. Il gain è misurato in dBi (isotropic)

Il path loss, con antenna gain, è

$$\frac{P_t}{P_r} = \left(\frac{4\pi f}{c}\right)^2 d^n = \frac{(4\pi f)^2}{G_{t_X} G_{r_X} c^2} d^n$$

e quindi

$$L_{dB} = 10 \log_{10}\left(\frac{P_t}{P_r}\right) = 20\left(\log_{10}\left(\frac{4\pi f}{c}\right) - \log_{10}\left(G_{t_X}\right) - \log_{10}\left(G_{r_X}\right)\right)$$

Vediamo il multipath: io sto mandando in LOS, ma ho interazioni con l'ambiente, tipo:

- riflessione
- scattering (se $\lambda \sim$ oggetto)
- diffrazione (se $\lambda \ll$ oggetto, effetto sui bordi)

Uno degli effetti è il **fading** (evanescenza), dovuto a interferenze distruttive tra più onde elettromagnetiche; le interferenze sono variabili nel tempo, perché siamo in un ambiente dinamico, e dipende anche dalla mobilità del dispositivo (entrambi ciao). Un altro è l'**interferenza Inter-Simbolo** (ISI Inter-symbol interference) ovvero la ricezione sovrapposta di simboli adiacenti a causa del ritardo di ricezione delle onde dei diversi percorsi. La durata è del simbolo è $\sim=$ o $<$ la max differenza dei tempi di arrivo.

Nel fading, il coherence time è la scala temporale in cui si possono considerare le caratteristiche del segnali costanti. Si calcola con

$$T_c = \frac{1}{f_D}.$$

La frequenza doppler dipende dalla velocità di movimento e dalla frequenza (oltre che da c) ed è

$$f_D = \frac{v}{c} f_c$$

Usiamo il MIMO (Multiple Input Multiple Output), che può essere di diversi tipi

3.1. Codifica e trasmissione dei dati

Dati utente –> forward error correction (FEC) ovvero encoder –> modulation e coding con la frequenza portante –> power amplifier (amplificatore) e lo mandiamo. Quando riceviamo

abbiamo de-modulazione (demodulation) e decoding –> forward error correction (FEC) e decoder

Schema di modulazione e codifica. Sappiamo che

$$s(t) = A\sin(2\pi f_c t + \phi)$$

ed esistono diverse tecniche per codificare dati digitali in segnali analogici.

Diversi livelli di ampiezza per diversi bit (o gruppi) parliamo di Amplitude-shift keying (ASK)

Diverse frequenze per diversi bit (o gruppi) parliamo di Frequency-shift keying (FSK)

Diverse fasi per diversi bit (o gruppi) parliamo di Phase-shift keying (PSK)

Il simbolo è una forma d'onda, uno stato o una condizione significativa del canale di comunicazione che persiste in un intervallo di tempo fissato. Il symbol rate è il numero di simboli trasmessi al secondo [baud]

In generale, un simbolo può contenere più bit, quindi symbol rate diverso da bit rate

Metti esempi vari

Tecniche che permettono più di un bit per simbolo:

- MFSK multilevel frequency-shift keying ($L = \log_2(M)$)
- QPSK quadrature phase-shift keying (2)
- X-QAM quadrature Amplitude modulation ($L = \log_2(X)$)

Vediamo ora QPSK. Usa la fase per determinare ...

Siamo nello spazio complesso (viva Edu) ma usiamo le coordinate polari. Il segnale è

$$s(t) = \frac{1}{\sqrt{2}}...$$

Ogni punto codifica una coppia di bit. Sono 4 fasi differenti, distanziate di 90 gradi. Usiamo 2 bit per simbolo, usando una codifica Gray per punti adiacenti.

Vediamo QAM. Cambia un po', ma combina variazioni di ampiezza e fase, ad esempio 16-QAM usa 4 bit per simbolo e la costellazione è più densa.

Bit error rate curve: le curve di BER rappresentano la probabilità di errore di un bit in funzione del rapporto tra la densità di energia del segnale per bit ed il livello del rumore, ovvero

$$BER = func\left(\frac{E_b}{N_0}\right)$$

La formula analitica (verificata poi sperimentalmente) è una stima ottimistica rispetto al caso reale, ovvero

$$BER = \frac{4}{n}\left(1 - \frac{1}{\sqrt{M}}\right) erfc\left(\sqrt{\frac{3nE_B}{(M-1)N_0}}\right)$$

con n bit per simbolo, M numero di simboli diversi (costellazione) e erfc funzione degli errori di Gauss complementare, ovvero

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2}\,\mathrm{d}t$$

AMC è adaptive modulation and coding

Il forward error correction aggiunge bit ai dati, così il ricevente li può usare per vedere se ci sono stati errori. Se la error detection vede un errore il blocco di dati viene ritrasmesso usando lo schema ARQ. Nelle trasmissioni wireless la probabilità di errore di un bit è elevata. Definiamo code redundancy come

$$\frac{n-k}{k}$$

mentre la coding rate come

$$\frac{k}{n}$$

A seconda delle condizioni del canale wireless il trasmettitore sceglie lo schema di modulazione e codifica opportuno

4. Lezione 04 [05/03]

4.1. Esercizi

Abbiamo SNR = 8 dB e un obiettivo che il canale deve garantire di BER = 10^-2 (sbagliare un bit ogni 100)

Abbiamo anche una tabella dei coding rate (k/n vedi Shannon)

SNR	BPSK	QPSK	16-QAM
$< 6dB$	0.6	0.4	0.2
$6 - 10dB$	0.8	0.6	0.5
$> 10dB$	0.9	0.8	0.7

Poi abbiamo un grafico con SNR sulle x e BER sulle y, di solito in scala

I simboli al secondo sono 1000 syb/s

Noi siamo a 8 dB quindi siamo sulla linea centrale. Noi vorremmo un BER uguale a 10^-2, quindi scegliamo BPSK. La QPSK invece non va bene, faccio troppi errori. Guardando la tabella, selezioniamo 0.8 vista la zona e la codifica.

Facciamo quindi syb/s * bit/syb * CR [ad], ovvero

$$1000 \cdot 1 \cdot 0.8 = 800 \text{ bit } /s$$

Se avessi chiesto 10^-1 prendevo anche QPSK, facevo conti e prendevo il migliore. Basta prendere tutto quello che è meglio di quello richiesto.

4.2. OFDM [Orthogonal Frequency Division Multiplexing]

Abbiamo già visto TDM e FDM con divisione in frequenza e tempo in base al segnale.

La tecnica OFDM permette di inviare uno stream di bit usando frequenze differenti per inviare porzioni dello stream. Offriamo canali differenti usando una divisione in frequenza. Vogliamo garantire stesso data rate in TDD. Qua manteniamo fissa la banda ma garantendo lo stesso data rate Qui ho N stream paralleli, uno per ogni frequenza, e ho R/N bps di durata N/R. Stesso data rate in entrambi, ma qui abbiamo tanti sotto stream su tutte le frequenze disponibili

Come lo si implementa:

- dobbiamo fare una conversione seriale -> parallelo
- mandiamo R/N bit ad ogni frequenza diversa detta subcarrier (sotto-portanti)
- ogni stream viene modulato indipendentemente usando lo stesso schema di modulazione codifica MCS
- l'onda trasmessa è la combinazione di tutti i subcarrier modulati

Partiamo da una frequenza base e poi la spostiamo

Come troviamo la f_b? Nel caso di FDM classico viene lasciato uno spazio di guardia per evitare interferenze. In questo caso, i subcarrier sono ortogonali tra di loro e non interferiscono. La distanza tra i subcarrier è studiata in modo da evitare interferenze

Ortogonali non ho interferenze.

Come garantiamo l'ortogonalità?

La scelta dipende dalla durata del simbolo T, ovvero

$$f_b = \frac{1}{T}$$

ovvero più il simbolo è breve e più devo distanziare, più il simbolo è lungo meno devo distanziare.

Considerazioni:

- più robusto riguardo ad interferenze che riguardano solo alcuni subcarrier; nel caso di sx rompe le palle a tutto, nel caso di dx solo un bit (o R/N) sarebbe interessato
- più robusto rispetto ai problemi di multipath perché la distanza tra un simbolo e l'altro è maggiore (inter-symbol interference (ISI) ridotto)

Multiple access: condividere il canale di comunicazione tra più utenti. In generale MA diverso da multiplexing. Ora abbiamo:

- TDMA slot temporali diversi
- FDMA frequenze diverse per gli utenti
- CDMA codificare l'informazione [3g e satellite]
- CSMA controllare il canale
- FHSS frequenze diverse saltando random
- OFDMA subcarrier [4g e 5g]

4.3. Spread Spectrum

Spread Spectrum (spettro espanso) consiste nel trasmettere il segnale di informazione su uno spettro di frequenze più ampio di quella del segnale

Ho input, poi encoder, il modulator prende uno pseudonoise generator oppure uno spreading code (deciso), canale, de-modulatore e poi fine

Motivazioni:

- immunità a diversi tipi di rumore e distorsioni multipath
- utilizzato per nascondere e cifrare il segnale. Solo TX e RX sono a conoscenza del codice di spreading
- molti utenti possono usare indipendentemente la stessa banda più ampia con pochissima interferenza, usata da CDMA

4.3.1. Frequency Hopping Spread Spectrum

In FHSS il codice di spreading determina quale frequenza usare per trasmettere il segnale. Ad ogni intervallo di tempo prestabilito, la frequenza viene cambiata (Frequency Hopping). Sequenza nota a TX e RX

Ci si mette d'accordo su due parametri: ogni quanto fare hopping (anche pubblico) e pseudonoise bit source, il seed della sequenza da generare

Cosa possiamo dire:

- più resistente al rumore e al jamming
  - jamming su una frequenza compromette solo quella
  - jamming su tutta la banda spread ha meno efficacia
- un altro ricevitore che si sincronizza con il trasmettitore può solo leggere alcuni pezzi di messaggi perché non conosce la sequenza di frequency hopping

4.3.2. Direct Sequence Spread Spectrum

Data una sequenza di bit D, ogni bit della sequenza viene rappresentato da un insieme di bit usando un codice di spread

1 bit di informazione diventa da N ottenuti da una sequenza casuale

I bit della sequenza di spread sono più piccoli (durano 1/N dei bit di informazione) e sono denominati chip

Vogliamo mantenere lo stesso data rate, quindi abbiamo bisogno di N volte la banda utilizzata per l'informazione

Esempio 4.3.2.1: Devo trasmettere D = 101 e ho un fattore $N = 3$. Per ogni bit di D uso 3 bit casuali. Faccio XOR (bit per ogni bit della sequenza) e poi mando.

Un bit di informazione va in xor con i bit del chip

5. Lezione 05 [11/03]

Multiplexing a livello fisico: ho 1 canale e lo divido in n sotto-canali. A livello 2 invece ho il multiple access: permetto a più utenti di accedere contemporaneamente, è il livello MAC che, in base ai canali, vede cosa fare. Se voglio livello MAC devo avere il livello fisico

Finiamo spread spectrum: ci manca CDMA (Code division multiple access)

Data una sequenza di bit D, ogni bit della sequenza viene convertito in un insieme di k chip usando un pattern prefissato detto codice. Un chip è una sequenza di 1 e -1. Vogliamo lo stesso data rate, quindi ci serve k volte la banda. Ogni utente ha un codice diverso e produrrà chip diversi.

Abbiamo:

- sequenze Walsh: creano un insieme di codici ortogonali (sono in numero limitato, non interferiscono l'uno con l'altro)
- sequenze PN, Gold, Kasami: creano codici non ortogonali ma in un numero molto maggiore (permettono leggera interferenza)

Se trasmettiamo 1 il codice rimane identico, se voglio trasmettere uno 0 cambio ogni segno del codice.

Posso mandare tutto assieme, modulando comunque sulle varie portanti, ma posso tutto assieme e recuperare, con i codici, le varie cose. Come?

Noi sappiamo il codice e quanto è lungo. Calcoliamo

$$S_u(d) = \sum_{i=1}^{k} d_i \times c_i$$

dove d_i è quello ricevuto e c_i è il codice.

Perché funziona? Perché se ho mandato un 1 ho delle moltiplicazioni che sommano solo cose positive, e la somma vale k. Se invece ho mandato uno 0 ottengo una somma $-k$. Quindi il bro che riceve, quando calcola moltiplicazioni e somme, deve ottenere k per 1 e $-k$ per 0. Questo in quelli ortogonali. Se usiamo il codice di un altro utente devo ottenere 0 in quelli ortogonali, quindi so che non mi ha mandato dati un certo utente.

Se non sono ortogonali i codici, ottengo una cosa diversa da 0 se altro utente ma non è abbastanza alto per essere considerato corretto.

Che succede se ho un segnale combinato? CDMA mi permette di mandare tutti assieme senza problemi. Ad esempio se mandiamo in 2 abbiamo 2 0 -2 come valori possibili. Prendiamo il codice del primo, moltiplicazione+somma. Il risultato, se è più alto (non ortogonali) allora il bro ha mandato un 1.

Più utenti vogliamo gestire, più il codice deve essere ampio

CDMA soffre del Near-Far problem, ovvero tutti trasmettono con la stessa potenza, gli utenti più lontani sono più difficili da interpretare. Quindi chi è lontano deve mandare più forte, ma consuma molta più batteria

5.1. WPAN

ISM band [industrial, scientific and medical] è una porzione di spettro riservato per usi industriali, scientifici e medici

Ad esempio, il forno a microonde lavora a 2.45GHz, l'ipertermia oncologica (con altre tecniche) su 434MHz e 915MHz

Spettro usato senza licenza, agire senza interferenze

Inoltre, abbiamo il Pulse Code Modulation (PCM) ed è una codifica del segnale audio con due aspetti:

- frequenza di campionamento (per unità di tempo)
- numero di livelli di quantizzazione (do i bit)

5.1.1. Personal Area Network [bluetooth]

Siamo nelle wireless personal area network

Lo standard IEEE 802.15 comprende un insieme di tecnologie per la comunicazione a corto raggio

Bluetooth è .1 come codice. Abbiamo delle reti piconet (molto piccole), e all'interno della rete non c'è uguaglianza. Ovvero, un dispositivo fa da master e una serie di slave che sono sotto il controllo del master, controlla la piconet

Il bluetooth è short range (10-50m nei casi d'uso tipici e a seconda della classe di potenza del dispositivo). Usa la banda ISM 2.4 GHz. Ha un data rate di 2.1-24 Mbps (non pensato per elevato data rate). Utilizzato per:

- punto di accesso per dati e voce (dati limitati)
- sostituzione di cavi (no tastiere mouse ecc, es. periferiche wireless)
- comunicazione ad hoc con altri dispositivi BT

BLU: core protocols, ci sono in tutti i dispositivi BT, la parte del core, se uno è BT complaint ci devono essere

ROSSI/BLU SCURO: ci sono solo se quel dispositivo offre quel servizio

Partiamo dal basso

Bluetooth radio: specifica l'interfaccia radio, ovvero radio frequenze, gestione del frequency hopping, schema di modulazione e utilizzo della potenza di trasmissione

Baseband: livello banda base, si occupa di stabilire la connessione con la piconet, gestire l'indirizzamento (no MAC, specifico dello stato), formattazione di pacchetti, sincronizzazione e tempistiche di comunicazione (TDD & TDMA) e gestisce la potenza di trasmissione (indicazioni passate poi al tempo radio)

Link Manager Protocol (LMP) configura dei collegamenti tra dispositivi, gestione di collegamenti attivi e funzionalità di sicurezza e cifratura. Svolte un compito di controllo

Punto di rottura: sotto ho dentro il chip bluetooth, sopra ho software o firmware

Logic link control and adaptation protocol (L2CAP) adatta i protocolli di livello superiore al livello baseband e offre ai livelli superiori servizi connectionless e connection-oriented. Fa da interfaccia

Service discovery protocol (SDP) gestisce le info del dispositivo, tipo servizi disponibili, caratteristiche disponibili. Possiamo interrogare per stabilire connessioni tra dispositivi.

Radio frequency communication (RFCOMM) è una porta seriale che mi astrae il bluetooth per permettere la comunicazione. Bla bla bla vedi slide

Sopra abbiamo un sacco di robe, intende riutilizzare il maggior numero di protocolli esistenti. Lo standard Bluetooth specifica dei profili che indicano un particolare modello di utilizzo dell'architettura

Piconet & scatternet

Una piconet ha un master, degli active slave (AS) (membri arrivi della piconet) che hanno un active member address [AMA] di 3 bit (il master è 0). Quindi ho 2^3 dispositivi disponibili, tolto il master, quindi max 7 active slave

I parked slave (PS) sono membri che devono aspettare che uno degli AS cambi stato e hanno un parked member address [PMA] su 8 bit (0 master) e quindi ho $2^8 - 1$ possibili

Ci sono poi i standby slave (SS), sono stati riconosciuti ma sono nel chill, senza indirizzo quindi numero infinito

La piconet è molto master-centrica: appartengo e mi coordino con il master, ma un dispositivo può stare in più piconet. Se un AS sta in più piconet otteniamo una scatternet. I due master sono entità separate, le due piconet sono totalmente indipendenti, ognuno per sé, ma una delle AS sta in entrambe le reti.

6. Lezione 06 [12/03]

Frequenze pari master parla, frequenze dispari slave parla. Non sono mai slot separati: parla master, subito dopo parla slave.

Gli slot per parlare consecutivi sono 1,3 o 5. Sempre dispari per la divisione in time division duplex. Se fossero pari andremmo a parlare anche negli slave. Da 7 in poi sono troppi. Questo vale sia per master che per slave. Il FH va in base agli slot: nell'esempio passiamo da f_2 a f_5 perché ho uno slot da 3, ho fatto 3 salti, non vado in f_3. Inoltre, nella stessa finestra di trasmissione (n dispari slot) uso sempre la stessa frequenza.

Tutti gli slave connessi alla piconet hanno questo clock ben sincronizzato con il master. Quindi scelgo FH uguale in tutta la rete, TDD per fare le parlate MS e SM e infine TDMA per far scegliere al master con chi parlare

La scatternet deve aggiungere altro

Ogni master ha la propria FH e si ha un disallineamento dei tempi, quindi ogni piconet è sfasata e non abbiamo vincoli che le leghino

FH decisa sempre dal master e condivisa nella piconet, ognuna con una sequenza diversa. Avendo 79 canali può capitare una sovrapposizione. Come si sistema:

- FH su un numero ridotti di canali (scegliamo robe diverse), riduce ma non risolve
- si usa CDMA per risolvere, ovvero evita interferenze tra piconet. Ogni master dà un codice ortogonale per tutti gli elementi della piconet (CDSMA scatter). Il MA sono le piconet

Non abbiamo veramente risolto, ma cosi riduciamo di molto perché i codici ortogonali sono molto pochi

Cosa offre la baseband come servizi (2 canali):

- synchronous connection-oriented link (SCO) point-to-point
  - canale audio/voce di 64 kbps bidirezionali
  - il master riserva una coppia di slot adiacenti ad intervalli regolari (MS e SM per arrivare a 64kbps)
  - previsti al massimo 3 canali SCO attivi contemporaneamente
  - traffico real time come la voce (delay non c'è)
- asynchronous connectionless link (ACL) point-to-multipoint
  - canali ACL occupano gli slot rimanenti, ciò che non è SCO
  - traffico dati con ciascuno degli slave (varie dimensioni)
  - un solo ACL contemporaneo tra master e uno slave
  - traffico best effort (non garanzie di delay)

Due canali logici offerti

Come sono formati i frame (pacchetti) a livello baseband?

Abbiamo:

- 68 (o 72) bit di access code, usato per ... che possono essere:
  - channel access code (CAC) identifica la piconet (48 bit dell'indirizzo HW del master)
  - device address code (DAC) derivato dall'HW dello slave ed è usato dal master per chiamare (paging) il dispositivo
  - inquiry address code (IAC) usato per trovare l'indirizzo di un dispositivo vicino (durante la fase di inquiry)
- 54 bit di packet header

    - 3 bit di AMA
    - 4 bit di tipo (tipo del pacchetto, formato di ACL)
    - 1 bit flow (controllo di flusso), vale 1 se stop, altrimenti 0 resume (usiamo per gli ACL, gli SCO sono cadenzati)
    - 1 bit di ARQN (automatic RQ number)
    - 1 bit di SEQN (sequence number modulo 2)
    - Ultimi due usati per il controllo degli errori
- 0-2744 bit di payload
    - SCO 30 byte (230 bit) perché abbiamo 30*8*1600/6 ovvero 64 kbps
    - ACL da 0 a 343 byte

Link Manager Protocol (LMP) è una macchina a stati

- si parte dalla standby mode, il dispositivo è accesso ma non è in nessuna piconet, quindi minimo consumo
- entro in ...

In standby non sono a conoscenza di niente. Come faccio a collegare? Non ho nessun coordinamento, ma c'è un concetto di «presentazione di qualcuno», ma non è lo slave che si annuncia al master (quello dal 4.0 in poi), qua è il master che si presenta allo slave. Il master fa discovery e manda pacchetti con IAC su 32 frequenze standard dove li mandiamo uno dopo l'altro. Gli slave sanno che devono ascoltare qua

I tempi di collegamento sono diversi: avendo un TDMA dobbiamo avere culo a prendere quando il master sta per mandare su quelle frequenze.

Quindi:

- mando su 32 canali wake-up un IAC packet (32 consecutivi) e i bro slave ascoltano per vedere se qualcuno ha mandato un IAC, tutto non coordinato però. Visto che spreco ad ascoltare, ascolto per 11.25 ms e aspetto. Tra una scansione e l'altra passano 1.28/2.56s
- quando si beccano dobbiamo dire chi siamo (48bit del MAC e la classe) con un random backoff per evitare le collisioni

Master passa da standard a inquiry, mentre slave da standby a inquiry-scan. Ci siamo allineati con il metronomo del master, manca solo una cosa: la FH. Non la sappiamo per ora, la dobbiamo sapere.

Uso 16 frequenze standard dei 32 di prima per mandare un DAC (access code) con il FH da usare e il suo active member address. Ora sappiamo come sincronizzarci, mando un DAC con un ACK

Passiamo poi negli stati PAGE e infine CONNECTED

7. Lezione 07 [18/03]

7.1. Ancora BT

Digressione sul near far: stessa potenza perché devo essere in grado di decodificare, se troppo debole il segnale si perde via

Due blocchi da 16 frequenze sulle 32 disponibili (divise in modo equo su tutto lo spettro). Lo slave seleziona UNO dei 32 canali di wake-up, perché non sa dove la sta mandando ora ma sa che la può mandare in 32 canali. Poi dopo random mando la risposta, il master ascolta le 16 frequenze

Un dispositivo accesso in standby mode non è membro di alcuna piconet, ho minimo consumo

Entro in inquiry mode per:
- creare una piconet
- periodicamente per vedere se sono stati mandati dei messaggi con IAC

Questa operazione di inquiry non è coordinata, ovvero non c'è sincronia dei clock

In page mode il master crea la piconet interrogando gli slave sui profili che possiedono. Transmit consuma, connected uguale ma meno

Master promuove e degrada gli slave in stati di power saving:
- sniff (consuma molto) ascolta ma non tutti gli slot (mantiene AMA)
- hold (consuma medio) con ACL sospesi e solo SCO (mantiene AMA)
- park (consuma meno) rimane membro della piconet ma lascia l'AMA per un PMA; periodicamente ascolta i messaggi del master in broadcast (non sulle 32/16 di prima, sanno dove sono, siamo nella piconet) a tutti i membri parked

Abbiamo visto la parte fisica, ora andiamo nel software

Logical Link Control and Adaptation Protocol (L2CAP) come se fosse il livello IP, non più firmware e hardware. Sempre presente da standard, siamo ad un livello superiore, funzionalità di alto livello

Non viene utilizzato per l'audio, è tutto nel livello dopo

Supporta solo canali ACL e offre 3 canali logici:
- connectionless: unidirezionale (broadcast tra master e slave)
- connection-oriented: bidirezionale con supporto QoS (qualità di servizio, tipo TCP)
- signaling: bidirezionale usato per messaggi di controllo master/slave

Come sono fatti i pacchetti [METTI FOTO]

Notiamo come i payload siano molto più grandi: infatti, sono >> baseband, mentre qua sono in byte. Viene fatta una segmentazione in messaggi baseband. In ricezione poi assembliamo.

Abbiamo lunghezza per sapere la lunghezza del messaggio, CID (connectionless 2 connection-oriented >= 64 signaling 1)

Ultimo pezzo è SDP: protocollo client-server dove si ha un server con le info e un client che fa
- ricerca di un servizio
- browser di servizi (listare i servizi di un dispositivo)

Client è il master, che chiede ai server (slave) i servizi o altro

FINE BT 2.1

Bluetooth Low Energy (BLE) balzo in avanti dal 2.1, siamo almeno nel 4.0 (credo)

Motivazioni:
- ridurre il consumo energetico sui dispositivi
- utilizzo nel mondo degli smart sensor
- necessità di un sistema più snello per la comunicazione
- compatibilità con disponibili Bluetooth
- richiesta di nuove funzionalità come positioning o presence

[IMMAGINE] a sx < 4.0 ho solo master + slave, banda e basta, 1MHz per ogni canale, a dx siamo nel mondo 4.0 e abbiamo, oltre alla stella, anche una struttura broadcast (senza una piconet rigida, chi è nel raggio GG sennò suca) e mesh, con anche servizi di device positioning (misura di presenza di dispositivi, distanza tra dispositivi e direzione). Stesso spettro ma i canali sono di meno 40 (non più 79) e quindi sono un pelo più larghi e resistenti all'interferenza

Perdiamo data rate, le versioni dopo cercano di aumentarlo

[IMMAGINE]

Livello BLE radio (PHY) ho sempre radio a 2.4 GHz ISM

Banda divisa in 40 canali, i primi 37 usati come data packets e i canali 37 38 39 usati come canali di advertising

Facciamo FHSS con hops determinati dalla formula

$$\text{channel} = (\text{current\_channel} + \text{hop}) \bmod 37$$

dove hop è stabilito all'atto della connessione

Usiamo la Gaussian Frequency Shift Keying (GFSK) bla bla bla

Advertising è lo slave che si annuncia al master per entrare nella piconet. Initiating lo fa il master, se si becca con advertising si crea la connection. Altri stati (iso e scanning) che sono messi li nello standard per i nuovi casi d'uso:
- iso è un broadcast periodico, che mette info in giro
- scanning fa ascolto di quello che c'è in giro

Advertising si fa su 3 canali, VEDI IMMAGINE

Si entra in stato advertising, si mandano sui 3 canali con un ADVInterval, multiplo di 0.625ms ma nel range 20ms-10.24s (determina anche uso batteria, subito –> molto lento). Per evitare allineamento che causi collisione (non siamo coordinati) ho un advDelay, pseudo-random in 0ms e 10ms

Generic Attribute Profile non ho capito cosa sia ma va bene

General Access Protocol (GAP) è un modulo software che trasforma gli stati del dispositivo:
- broadcaster (spedisce advertising packets, trasmissione i dati connectionless come eventi di adv)
- observer (riceve adv packets, riceve dati in connectionless)
- peripheral (periferico), device slave che opera in advertiser mode a LL
- central è un device master (Initiator) mode a LL

Vediamo una unicast peer-peer: opposto di quello che avveniva prima, master ascolta e gli slave fanno richiesta per collegarsi ad una piconet. Quando il master ha ascoltato passa in initiator

e manda una connection request sullo stesso canale. Poi si passa all'effettiva comunicazione master-slave

Connessione broadcast: abbiamo un broadcaster che manda dati sui canali 37 38 39 agli observer (nel raggio di comunicazione, non mi frega chi c'è o chi no, io devo solo trasmettere)

Possiamo avere un passive scanning: uno sniffer, ascolto periodicamente su quei canali quello che arriva, sempre sui 37 38 39 (id)

Oppure un active scanning: è sempre e solo sul 37 38 39 ma facciamo richieste su questi canali con una request + response. Scanner fa richiesta, advertiser fa la response. Questo deve avvenire in un advertising scan interval. La richiesta sono tipo cosa sai fare, dammi le tue coordinate, dove sei. Possiamo vederlo come broadcast + unicast quando faccio le richieste, mi sincronizzo per parlare con quel bro

Indice

1. Lezione 01 [25/02] 3
1.1. Principi di Teoria della Trasmissione 3
2. Lezione 02 [26/02] 5
2.1. Ancora basi di teoria della trasmissione 5
2.2. Multiplexing 6
2.3. Comunicazione wireless 6
3. Lezione 03 [04/03] 8
3.1. Codifica e trasmissione dei dati 8
4. Lezione 04 [05/03] 11
4.1. Esercizi 11
4.2. OFDM [Orthogonal Frequency Division Multiplexing] 11
4.3. Spread Spectrum 12
4.3.1. Frequency Hopping Spread Spectrum 12
4.3.2. Direct Sequence Spread Spectrum 12
5. Lezione 05 [11/03] 14
5.1. WPAN 14
5.1.1. Personal Area Network [bluetooth] 15
6. Lezione 06 [12/03] 17
7. Lezione 07 [18/03] 19
7.1. Ancora BT 19
8. Lezione 08 [19/03] 22
8.1. ZigBee + Matter & Thread 22
8.1.1. ZigBee 22
8.1.2. Matter & Thread 25
9. Lezione 09 [25/03] 26
9.1. WLAN 26
10. Lezione 10 [26/03] 29
10.1. Problema del terminale nascosto 29
10.2. Frammentazione 29
10.3. Infrastruttura 29
11. Lezione 11 [01/04] 31
12. Lezione 12 [02/04] 34
12.1. Sicurezza in WiFi 35
12.2. Eduroam 35
12.3. Ultimi WiFi 36

8. Lezione 08 [19/03]

8.1. ZigBee + Matter & Thread

Siamo sempre nell'802.15 ovvero nel corto raggio con un dispendio energetico ridotto

8.1.1. ZigBee

Standard 802.15.4 delle low-rate WPAN

Con BT e BLE volevamo una riduzione del consumo di batteria e una complessità che si abbassava. In ZigBee estremizziamo questi concetti con anche altri requisiti:

- affidabilità
- basso costo
- lunga durata della batteria (molto più del BT)
- bassa complessità (pensato per sensori)
- utilizzo delle bande ISM (sia 2.4GHz che 915MHz e 868MHz)
- scalabilità (alto numero di nodi ma con strutture anche particolari)
- interoperabilità tra vendors
- sicurezza

Utilizzi un botto, guardali da solo (automation, personal care, periferiche, sicurezza, smart, eccetera)

Le topologie di rete che abbiamo sono:

- stella (BT like)
- albero
- mesh

Possiamo anche inserire del routing con particolari nodi

Abbiamo due macro-classi:

- full function device [FFD] tutte le funzionalità
- reduced function device [RFD] una parte delle funzionalità

Tra i FFD ne abbiamo due particolari:

- un solo coordinatore, detto PAN coordinator, unico all'interno della rete, che la deve creare e mantenere le informazioni (tipo chiavi di sicurezza)
- router, nodi che hanno la capacità di inoltrare dati tra i vari dispositivi ZigBee

I RFD sono invece gli end device, hanno solo la capacità di parlare con un router/coordinatore, e hanno ridotta complessità ed elevato risparmio energetico. Sono proprio gli attuatori

Cerchiamo di mettere pochi FFD e tanti RFD per diminuire al minimo il dispendio energetico. Vogliamo cambiare le batterie il minimo possibile

I ZigBee li distinguiamo per tipologie di invio di dati:

- dati periodici (tipo sensori, intervallo di trasmissione fissato)
- dati intermittenti (asincroni, stimoli esterni o dell'applicazione, tipo interruttore, in base ad un evento)
- dati ripetitivi e a bassa latenza (tipo mouse, allocazione di time slot con un certo servizio, vogliamo in tempo reale)

IMMAGINE ARCHITETTURA azzurro solo quelli della ZigBee alliance (tolta da Thread & Matter), rossi sono dipendenti dai singoli sviluppatori

Partiamo dal lato fisico: lo standard specifica la tipologia di modulazione e di spread spectrum per le 3 bande (FDM), cifratura per interferenze

Andiamo al livello MAC: esso deve

- gestisce l'invio dei beacon (se siamo PAN coordinator)
- sincronizzazione con i beacon del coordinatore (router & end)
- associazione/dissociazione alla PAN ascoltando i beacon
- accesso al canale tramite CSMA/CD

- MAC address (16 o 64 bit)
- gestione del duty-cycle del dispositivo
- gestisce la trasmissione diretta tra dispositivo e coordinatore ambo i lati
- gestisce la trasmissione indiretta da coordinatore a dispositivi

Abbiamo due modalità di trasferimento:
- unslotted CSMA-CA senza beacon
- slotted CSMA-CA con beacon

Slotted CSMA-CA beacon mode

Si basa sull'invio di beacon, messaggi con informazioni su come è organizzata la piconet, inviati dal coordinatore ed eventualmente inoltrata dai router

Il coordinatore invia periodicamente i beacon per:
- sincronizzare gli altri dispositivi
- organizzare i periodi di trasmissione per le diverse tipologia di trasmissione (periodiche, asincrone e bassa latenza), deve capire come dividere i bro
- gestione della trasmissione indiretta:
  - il coordinatore mantiene in una lista le frame non ancora mandate ai dispositivi
  - nei beacon frame trasmette anche i dispositivi che hanno frame pendenti (i bro sapranno se hanno qualcosa per me)
  - i dispositivi che ascoltano i beacon sanno se c'è qualcosa per loro

Definiamo i superframe: è l'intervallo tra un beacon e l'altro, momento di attività e altri di inattività

Il duty cycle è l'alternarsi tra periodi di attività (radio accesa) e inattività. Se devo prendere qualcosa dal beacon ok, sennò mi spendo e mi riaccendo al prossimo superframe

Abbiamo il beacon interval BI e superframe duration SD. L'unità base è aBaseSuperframeDuration di 960 simboli. Avremo multipli di questo parametro

Ci serve poi
- BO (beacon order) che determina il beacon interval tra 0 e 14
- SO (superframe order) che determina la durata del superframe 0-14
- duty cycle $= \frac{2^{\mathrm{SO}}}{2^{\mathrm{BO}}}$

Mentre il nostri BI si calcola come

$$\mathrm{BI} = \mathrm{aBaseSuperframeDuration} \cdot 2^{\mathrm{BO}} \text{ sym}$$

960 simboli sono circa $15.3ms$ con banda 2.4

Il beacon frame [IMMAGINE] GTS (guaranted ...), nel primo blocco, tiene tutte le informazioni

Il superframe, dentro il beacon, mi da info sui tempi di attività:
- contention access period (CAP) accetto con CSMA-CA
- contention free period (CFP) (da 0 fino a 7 slot)m comunicazione con banda riservata tramite guardanteed time slot (GTS)

Come funziona la trasmissione? **IMMAGINE**

All'inizio faccio CCS (verifico che sia libero) per brevi periodi (8 simboli, poca batteria)

Non posso andare oltre il CAP, deve essere atomico l'operazione, per forza dentro li

Unslotted invece più semplice, siamo in non-beacon mode, quindi accediamo al canale con CSMA/CA senza i vincoli degli slot, no sincronizzazione (cordinatore e router RX sempre attivi), il tempo è continuo e non discreto come in beacon e il controller è più semplice

Andiamo al livello di rete, facciamo indirizzamento, gestione della rete join and leave, sincronizzazione e routing (star, tree, mesh AODV)

Ogni dispositivo è programmato per una specifica funzione (potrei avere più robe)

ZigBee Device Object definisce il ruolo del dispositivo, scoperta di nuovi dispositivi e delle loro funzionalità, interfaccia con le applicazioni definite dai manufacturer

8.1.2. Matter & Thread

Nuovo standard, sempre 802.15.4 ma viene montato Thread da parte a ZigBee e sopra Matter

Fisico e MAC siamo uguali a ZigBee, ma Thread abbiamo delle funzionalità più conosciute:

- 6LoWPAN
- IP routing
- UDP

Con anche robe di sicurezza, ...

Cambia le rete Thread

Abbiamo i routing full thread device:

- router: effettua routing e fornisce servizi di accesso e sicurezza (NoSleep, degradabile a router-eligible end device REED)
- leader: router con funzionalità aggiuntive che può eleggere/destituire REED

E abbiamo anche i non-routing full thread device:

- REED (prima) non lo sono ma possono esserlo
- full end device (FED) non possono essere router

Infine abbiamo i non-routing minimal thread device, hanno HW minori e:

- minimal end device: comunicazione solo con il router genitore e radio sempre attiva
- sleepy end device: comunica solo con il router genitore con duty-cycle
- synchronized sleepy end device: comunica solo con il router genitore e duty-cycle con intervalli schedulati

Ci sono anche i border router che fanno routing verso l'esterno, in ZigBee non ce l'avevamo

9. Lezione 09 [25/03]

9.1. WLAN

Siamo nell'802, livello fisico e MAC

In questo caso, siamo 802.11 per le WLAN

Obiettivi:

- throughput, uso efficiente del canale radio per elevato data rate
- elevato numero di nodi, non su singolo AP ma su più celle, centinaia di nodi gestiti da più celle
- connessione verso la dorsale (backbone) cablata
- raggio 100-300 metri
- uso efficiente della batteria (meno estremo di ZigBee e BT), ma da wifi6
- più WLAN possono coesistere
- operare nelle bande unlicensed
- configurazione dinamica

La più comune rete wifi (Wireless Fidelity) è [IMMAGINE], rete con uno o più access point e la rete viene coordinata con Point Coordination Function (punto di coordinamento, access point). In più, basic service set identifica la cella (tipo eduroam)

Un'altra versione sono reti ad-hoc e sono distributed coordination function, non si ha un vero punto di coordinamento, con un independent basic service set (ambito veicolare questo)

Livello fisico [metti IMMAGINE]

Cosa offre il servizio Logical Link Control (LLC):

- unacknowledged connectionless service
  - trasmetto ma consegna non garantita
  - datagram indipendenti
  - no controllo errori
  - no controllo di flusso
- connection-mode service (link affidabile, perché canale wireless è inaffidabile per definizione)
  - canale punto-punto
  - correzione degli errori
  - controllo di flusso
- acknowledged connectionless
  - datagram indipendenti
  - acknowledge datagram

Vediamo il sottolivello MAC

Il canale radio è sensibilmente più inaffidabile di un canale cablato, quindi la frame di MAC 802.11 è più complessa dell'Ethernet 802.3:

- in 802.3 il payload è di 1500-1518B
- in 802.11 al massimo è 2304B

Il livello MAC offre due servizi:

- servizio dati asincrono: best effort e con delay variabile
- servizio time-bounded: offre garanzie sul delay

Il time-bounded è disponibile solo in presenza di un coordinatore (AP)

Distributed coordination function: opera con CSMA/CA

L'accesso al canale radio deve essere regolato aspettando del tempo per poter trasmettere. 802.11 prevede diversi tempi di attesa a seconda della tipologia di dati da trasmettere

Ci sono standard sul numero di slot, ma ognuno parte quando vuole ad aspettare un certo tempo

Abbiamo 4 definizioni:

- slot time: tiene conto di ritardo di propagazione e del trasmettitore (un quanto di tempo che il dispositivo sa che deve attendere)
- short inter-frame spacing [SIFS]: intervallo più breve di attesa usato per messaggi ad alta priorità
- DCF inter-frame spacing [DIFS]: intervallo di tempo più lungo usato per messaggi a bassa priorità best-effort SIFS + 2*slot-time
- PCF inter-frame spacing [PIFS]: intervallo di tempo intermedio per time-bounded SIFS + slot-time

Usati per gestione, che ogni dispositivo in modo arbitrario e privato, del proprio tempo

Come avviene accesso al canale? È sempre in contesa

CANALE LIBERO NO ACK

No tempo random, iniziamo ad ascoltare subito. Ascoltiamo un tempo uguale a DIFS (più lungo), e durante la durata radio accesa per ascolto del canale (tutto il tempo, non spengo come ZigBee)

No ACK se il frame è corrotto, non ho modo di saperlo

CANALE LIBERO CON ACK

Non faccio carrier sense per l'ack. Dopo che finiamo di trasmettere, uso un tempo SIFS dopo aver mandato in modo atomico il mio frame, perché il frame è di controllo (ack). Aspettando tempo minore, sono sicuro che chi sta aspettando di trasmettere non decide di farlo e non fa interferenza

CANALE LIBERO CON ACK MA NON RICEVUTO

Se il frame è corrotto, il trasmettitore sta aspettando il SIFS. Se non riceve automaticamente assume che trasmissione non è andata a buon fine, a prescindere dall'errore. Cosa fa? Rimanda subito, ho preso il canale in maniera esclusiva. Viene fissato un numero massimo di tentativi. Ack viene mandato subito, tempo di switchare l'antenna

CANALE OCCUPATO

Sento un altro segnale, il CCA mi dà rosso perché uno sta trasmettendo. Cosa faccio? Tengo radio accesa (ecco perché dispendio alto di batteria) fino a quando non sentiamo la fine della trasmissione. Non possiamo trasmettere immediatamente, potrebbe manca un ack. Inoltre, noi non siamo da soli, non siamo gli unici ad aver trasmesso. Facciamo un periodo di contesa con un random backoff:

- si attende il SIFS/PIFS/DIFS dopo il CCS (fine trasmissione dell'altro bro, è un evento che bene o male sincronizza tutti i dispositivi di rete) in base alla priorità del messaggio che si deve mandare

Numero di slot time da attendere, durante il periodo noi facciamo CS

Se ci va ancora male? Sincronizzazione, aspetto DIFS (non ho manco ack), random backoff ma uno va prima di me. Opzioni:

- riparto dalla contesa, come se non fosse mai avvenuto, ma questo è un problema di attesa infinita –> interrompo il conteggio, e nel turno successivo riparto da quello

Problema del terminale nascosto

[IMMAGINE]

Se A fa CS, non sente nessuno che parla, quindi inizia a spedire. In modo analogo, D fs CS, non sente nessuno che parla, quindi inizia a spedire. Entrambi hanno ok dal livello fisico e iniziano a parlare

Cosa riceve B? Collisione non evitata, viola il CSMA/CD

Ho terminali nascosti, ovvero il raggio non mi permette la percezione delle trasmissioni degli altri.

10. Lezione 10 [26/03]

Perché aspetto DIFS dopo che mi sono sincronizzato? Devo vedere se arriva l'ack [IMMAGINE1]

10.1. Problema del terminale nascosto

Come funziona terminale nascosto

CSMA/CA funziona solo se tutti quelli che vogliono comunicare sono nel raggio

Soluzioni?

A chiede a B il permesso. Nel messaggio RTS (request to send) si mette il MAC del bro a cui voglio mandare e anche il mio. Network Allocation Vector (NAV) tempo trasmissione + «ack» viene messo dentro. Uno che riceve un frame non suo sa che deve aspettare tutto quel tempo, inutile che cerchiamo di accedere al canale.

Ora D e F non sanno quello. L'unico che fa la concessione è B: hanno richiesto me, se nessun altro ha richiesto di comunicare con me, mando il CTS (clear to send) con sorgente B destinazione A e ancora un tempo NAV (poco meno).

Il CTS viene sentito da A D F, cosi A inizia a trasmettere mentre D e F sanno che un altro nodo al di fuori del loro raggio di copertura vuole dialogare con B

Aspetto sempre SIFS per il CTS e per il primo frame da A a B

10.2. Frammentazione

Permettiamo di frammentare in pezzi più piccoli, canale radio molto più sensibile all'interferenza e al rumore

Considerando la dimensione bla bla bla

10.3. Infrastruttura

Vediamo la rete con infrastruttura: abbiamo qualcosa di più

Abbiamo:

- basic service set (BSS) insieme di stazioni controllate da un singolo coordinatore (AP) [una sola cella]
- extended service set (ESS) insieme di più BSS interconnessi tramite un sistema distribuito a livello LLC [eduroam]

Il portale è un router/bridge che collega il sistema distribuito alla LAN

ESS viene visto come un unico BSS a livello LLC per funzionalità di roaming tra AP diversi (overlapping per almeno 10% continuità)

In presenza di un AP tutti i frame passano per l'AP, non si fa ponte

Questa si chiama point coordination function, con servizi time-bounded possibili perché prima avevamo un backoff che non mi dava garanzie sul delay

Nella modalità PCF [AP] l'accesso point controlla l'accesso al canale radio:

- tutto il traffico passa da AP
- le stazioni associate ad AP usano DCF con tempistiche SIFS e DIFS per accedere al canale
- AP usa PIFS

Quindi AP si impossessa del canale prima delle stazioni in attesa

L'AP manda messaggi periodi (10-100s) detti beacon frame che sono frame di gestione:

- parametri operativi a livello fisico (bit rate e modulation coding scheme)
- sincronizzazione (usato nelle prime 802.11 che usavano FHSS)
- supporto a PCF con le relative informazioni
- invito per le nuove stazioni che non sono ancora associate

L'intervallo tra due beacon è detto superframe ed è diviso in 2:
- senza contesa (opzionale) ma necessario se vogliamo time-bounded, la gestisce tutta l'AP
- accesso a contesa (sempre presente), si usa CSMA/CA

Se canale radio è occupato oltre il limite del superframe questo tempo non verrà recuperato, si mangia tempo del pezzo dopo, molto più flessibili

Come funziona PCF

AP colleziona chi deve trasmettere cosa e a chi devono essere trasmettere cosa

Li raccolgo tutti e organizzo la trasmissione:
- devo allocare senza contesa
- inizio con canale occupato, smette, tutti iniziano con il CS, tutti aspettano DIFS mentre AP aspetta PIFS e prende il lock
- manda DDx con un NAV agli altri che non servono
- aspetto UDx se serve
- mando un CF end per dire fine del periodo contention-free

È un time division multiple access, con un tempo continuo

Indice

1. Lezione 01 [25/02] ... 3
1.1. Principi di Teoria della Trasmissione ... 3
2. Lezione 02 [26/02] ... 5
2.1. Ancora basi di teoria della trasmissione ... 5
2.2. Multiplexing ... 6
2.3. Comunicazione wireless ... 6
3. Lezione 03 [04/03] ... 8
3.1. Codifica e trasmissione dei dati ... 8
4. Lezione 04 [05/03] ... 11
4.1. Esercizi ... 11
4.2. OFDM [Orthogonal Frequency Division Multiplexing] ... 11
4.3. Spread Spectrum ... 12
4.3.1. Frequency Hopping Spread Spectrum ... 12
4.3.2. Direct Sequence Spread Spectrum ... 12
5. Lezione 05 [11/03] ... 14
5.1. WPAN ... 14
5.1.1. Personal Area Network [bluetooth] ... 15
6. Lezione 06 [12/03] ... 17
7. Lezione 07 [18/03] ... 19
7.1. Ancora BT ... 19
8. Lezione 08 [19/03] ... 22
8.1. ZigBee + Matter & Thread ... 22
8.1.1. ZigBee ... 22
8.1.2. Matter & Thread ... 25
9. Lezione 09 [25/03] ... 26
9.1. WLAN ... 26
10. Lezione 10 [26/03] ... 29
10.1. Problema del terminale nascosto ... 29
10.2. Frammentazione ... 29
10.3. Infrastruttura ... 29
11. Lezione 11 [01/04] ... 31
12. Lezione 12 [02/04] ... 34
12.1. Sicurezza in WiFi ... 35
12.2. Eduroam ... 35
12.3. Ultimi WiFi ... 36

11. Lezione 11 [01/04]

Beacon usati per scoprire una cella. Frequenza si configura sull'AP. Specificati i parametri di questa cella. Stazioni non presenti usano il periodo «contention period»

Formato del frame MAC: info principali sono messe come header, all'inizio

- in rosso tutto quello sempre
- in blu ci sono solo in certi tipi/sotto-tipi

Prim pezzo sono 2 byte FC di frame control:

- protocol version (versione usata del protocollo)
- tipo
- sotto-tipo
- toDS / fromDS verso il distributed system o da (celle del sistema distribuito), combinazione danno informazioni sugli indirizzi che ci sono
- MF more fragment (usato per riassemblare)
- RT rifare trasmissione
- PM attivo o no
- resto per sicurezza

Nei primi due byte abbiamo quindi protocollo e tipo del frame, quindi sappiamo poi cosa fare

Il secondo gruppo di due byte si ha la duration o la connection ID, qua ha lo durata del NAV

Poi abbiamo indirizzo destinazione (per chi è il frame, indirizzo MAC)

Quindi già in 10 byte sappiamo se questo è per noi o no

Vediamo frame control: ci sono tre tipi e sono per le tre macro funzionalità del sistema:

- 00 management (gestione cella)
- 01 controllo
- 10 dati

Per una roba più specifica basta guardare il sottotipo

Il frame può tenere sino a 4 indirizzi, il loro utilizzo e significato dipende dai valori dei campi TO DS e FROM DS

Se non 00 devo fare routing tra celle

Se from DS il frame arriva dal DS verso un AP all'interno della cella che contiene un indirizzo segnato nel secondo indirizzo

Se 10 sto mandando al DS

Ultimo comunicazioni dentro il DS, unico caso in cui si hanno 4 indirizzi attivi

In wifi6 si usa OFDMA Orthogonal Frequency Division Multiple Access

OFDM suddivide la bandwidth in canali usando frequenze differenti opportunamente distanziate, che erano tutte per un singolo utente

Con OFDMA diamo gruppi di canali di OFDM a utenti differenti. Nello stesso momento posso servire più utenti.

Ci serve qualcosa in più nell'AP: prima davo tutte le frequenze a tutti, ora devo fare uno scheduling delle frequenze più complicato, tempo e frequenza da assegnare. Inoltre, serve definire quanto e in quale modo io posso raggruppare le sotto-frequenze

Ogni sotto-portante è separata da 78.125 kHz

Abbiamo le resource unit (RU) gruppi di frequenze (solitamente adiacenti) che sono allocabili ad un utente

Dimensione RU variabile e dipende dalla banda disponibile e come AP vuole allocare le risorse agli utenti

Non tutta la banda viene usata: abbiamo intervalli di guardia. Inoltre, alcune sotto-portanti sono usate come pilot (bontà del canale). Segnale standard ben definito per correggere il canale e stimare quanto il canale è buono

Come comunico la suddivisione della banda?

AP utilizza frame di controllo, alcuni frame sono nuovi per supportare le nuove funzionalità, altri sono frame che erano già presente

Come associo le RU ai vari utenti?

Ad ogni trapezio si dà un indice di 7 bit, codice univoco

Assegnamento delle sotto-portanti di una RU sono esclusive per l'utente che le prende

Le informazioni di allocazione delle RU sono usate da PHY e MAC e vengono inviate

Come comunico quali sotto-portanti devono usare?

Come gestisco DL-OFDMA e UL-OFDMA (downlink da AP al disp e uplink viceversa)?

DL

Multi-user RTS che fa RTS e assegnazione delle RU per i dati che arriveranno. La RTS va alle stazioni che devono trasmettere, le altre allocano il NAV e non ascoltano. Ora che tutti hanno dei codici ortogonali, tutti rispondono con CTS paralleli, che essendo ortogonali non si sovrappongono mai

Dopo CTS possiamo trasmettere in parallelo, ogni stazione usa le frequenze dedicate e legge solo quello che interessa

Infine, si manca BAR (Block ACK request) con un block ACK da tutti in parallelo, sempre con un tempo SIFS per far finire l'AP di parlare (sta mandando in parallelo), non può ricevere se sta trasmettendo

UL

Un pelo più complicato, non è prevedibile se la rete è grande. Dobbiamo avere trasmissione sincronizzata e dire ad ogni utente quando trasmettere e dove

Più step:

- BSRP buffer status report poll, chiedo chi ha dati da trasmettere [primo trigger]
- BSR buffer status report, stazioni informano che hanno dei dati
- AP colleziona le richieste, assegna RU in base alle risposte e comunico con MU-RTS [secondo trigger]
- abbiamo il CTS da parte delle stazioni
- trigger per sincronizzare gli uplink e farli partire tutti assieme, così che AP riceva in blocco tutto (su risorse diverse) [terzo trigger]
- viene mandato UL-PPDU (con padding per arrivare alla durata massima)
- infine, se servono ACK si mandano Multi-STA Block ACK (multi-station)

Indice

1. Lezione 01 [25/02] ... 3
1.1. Principi di Teoria della Trasmissione ... 3
2. Lezione 02 [26/02] ... 5
2.1. Ancora basi di teoria della trasmissione ... 5
2.2. Multiplexing ... 6
2.3. Comunicazione wireless ... 6
3. Lezione 03 [04/03] ... 8
3.1. Codifica e trasmissione dei dati ... 8
4. Lezione 04 [05/03] ... 11
4.1. Esercizi ... 11
4.2. OFDM [Orthogonal Frequency Division Multiplexing] ... 11
4.3. Spread Spectrum ... 12
4.3.1. Frequency Hopping Spread Spectrum ... 12
4.3.2. Direct Sequence Spread Spectrum ... 12
5. Lezione 05 [11/03] ... 14
5.1. WPAN ... 14
5.1.1. Personal Area Network [bluetooth] ... 15
6. Lezione 06 [12/03] ... 17
7. Lezione 07 [18/03] ... 19
7.1. Ancora BT ... 19
8. Lezione 08 [19/03] ... 22
8.1. ZigBee + Matter & Thread ... 22
8.1.1. ZigBee ... 22
8.1.2. Matter & Thread ... 25
9. Lezione 09 [25/03] ... 26
9.1. WLAN ... 26
10. Lezione 10 [26/03] ... 29
10.1. Problema del terminale nascosto ... 29
10.2. Frammentazione ... 29
10.3. Infrastruttura ... 29
11. Lezione 11 [01/04] ... 31
12. Lezione 12 [02/04] ... 34
12.1. Sicurezza in WiFi ... 35
12.2. Eduroam ... 35
12.3. Ultimi WiFi ... 36

12. Lezione 12 [02/04]

La banda del WiFi viene divisa in canali (quelli che scegliamo sull'AP), e ogni canale viene diviso in sotto-portanti con quello che definisce lo standard

Possiamo scegliere 3 canali che non sono sovrapposti: ad esempio, 1 6 11, oppure 3 8 13. Identificato il canale troviamo la nostra banda e lo spettro che copriamo

12.1. Sicurezza in WiFi

Il canale radio è molto più esposto. Tutti ascoltano e inviano, quindi il canale è naturalmente broadcast. Inoltre, abbiamo la necessità di cifrare il canale a livello data-link

Prime versioni usavano WEP (Wired Equivalent Privacy):

- opzionale quindi lol
- algoritmo RC4 di cifratura
- assenza di un sistema di gestione delle chiavi
- unica chiave usata per cifrare tutto il traffico di tutti i dispositivi (chiave non password WiFi, ma ricavata da quello)
- tutto il traffico cifrato con la stessa chiave

Per sopperire alle lacune è stato introdotto un emendamento allo standard 802.11 detto 802.11i, che definisce la sicurezza del protocollo 802.11

[IMMAGINE]

Servizi offerti:

- access control: impone l'utilizzo dei protocolli di sicurezza e assiste lo scambio di chiavi
- authentication: definisce lo scambio tra utente e authentication server e genera le chiavi temporanee per la comunicazione
- privacy with message integrity: il payload MAC cifrati con aggiunta di un messaggio per il controllo dell'integrità

[IMMAGINE]

Abbiamo fasi:

- discovery: no cifratura, tramite beacon AP annuncia la sua presenza, STA ascolta e capisce quali servizi può usare leggendo dal beacon, associazione con accordo su che sicurezza utilizzare (anche negata se non si rispettano certi livelli);
- authentication e gestione chiavi: AS può essere anche nell'AP (ora sono collassate assieme, Eduroam no, gay), STA richiede ad AP l'autenticazione, che passa tramite un AS (esterno o meno), generazione delle chiavi in modo sicuro (master key, usata per generare tutte le altre che sono richieste in seguito). Come facciamo:
  - abbiamo la chiave di sessione e la chiave broadcast (usata per comunicare con tutti, non sto a cifrare ogni volta diverso, uso una chiave di gruppo)
  - generiamo nonce (number once, una sola volta)
  - cinque componenti (due numeri, mac address, master key che è psw wifi o generata da quella), generata dal client, che poi passa nonce all'AP
  - mando chiave di gruppo cifrando con quella di sessione, mando ack
- protezione dati: ho due alternative:
  - TKIP (WPA): integrità aggiunge un codice a 64 bit usando MAC dst e src, la confidenzialità si ha con RC4 e i cambiamenti sono solo software rispetto a WEP
  - CCMP (WPA-2): integrità fatta con cifratura cipher-block-chaining, confidenzialità con AES 128-bit per integrità e confidenzialità, nuova implementazione hardware

Il MIC è message integrity check

12.2. Eduroam

SSID eduroam, ha privacy con WPA2 enterprise, fase1 di autenticazione è PEAP mentre fase2 è MSCHAPv2, le credenziali sono pazze e si ha un certificato CA con la sua chiave pubblica

WPS al posto di mettere la password andiamo a usare un PIN (vedi slide nuove)

12.3. Ultimi WiFi

Con 802.11e si ha EDCA (Enhances Distributed Channel Access) parte con contesa, viene migliorata perché avevamo SIFS DIFS PIFS (e simili), ora per decidere le qualità di servizio si hanno dei parametri di accesso al canale:

- CWmin: congestion window minima, minima dimensione
- CWmax: congestion windows massima, massima dimensione
- AIFSN: numero di SIFS + N slot time (tempo di attesa, ma mai sotto il tempo di un AP)
- Max TXOP: massimo tempo nel quale una stazione può trasmettere più frame senza rilasciare il canale, per quanto tempo tengo il comando