Riassunto RWM

Massimo Perego

Indice

1 Teoria della Trasmissione

Si vogliono trasmettere informazioni su un mezzo analogico: non perfetto, questo può introdurre **rumore**, **interferenze** o **attenuare** il segnale.

Un segnale può essere rappresentato:

- Nel dominio del **tempo**, vedendolo come un segnale periodico sinusoidale; rappresentazione "classica"
- Nel dominio delle **frequenze**, ogni segnale ragionevolmente periodico può essere scomposto in una serie di segnali periodici (sin e cos), detti armoniche, ognuna con il relativo contributo rispetto al segnale originale

Quando tutte le armoniche sono multiple di una frequenza base, questa si chiama **frequenza fondamentale**.

Teorema del campionamento di Shannon: Il segnale analogico va campionato, la frequenza di campionamento deve essere almeno il doppio della frequenza massima del segnale in ingresso.

Relazione tra banda e data rate: Per trasmettere perfettamente onde come composizioni di sinusoidali serverebbe banda infinita, quindi si usa un'approssimazione.

La quantità di informazioni inviata dipende dalla banda, per trasmetterne di più o si aumenta la banda o si peggiora l'approssimazione (usare meno armoniche).

Teorema di Nyquist sulla banda: Dato un canale noise-free, il limite della quantità di informazioni è dato dalla formula

$$C = 2B \log_2 M$$

Dove

- B è la banda
- M il numero di livelli del segnale (binario ne ha 2)

La capacità del canale aumenta con banda e numero di livelli del segnale, ma questo è solo un limite teorico in assenza di rumore.

Decibel: Unità di misura del rapporto di potenze, in scala logaritmica:

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

Rapporto segnale rumore SNR: Per quantificare il rumore su un canale, e quindi il suo impatto sulla trasmissione

$$SNR_{dB} = 10 \log_{10} \frac{P_{\text{signal}}}{P_{\text{noise}}}$$

Tanto più il rapporto è alto, tanto più il segnale si distingue dal rumore.

Formula della capacità di Shannon: La capacità di un canale dipende anche dal rumore

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

Questa formula fornisce una massima teorica per la trasmissione senza errori sul canale.

Partendo dalla capacità data da Shannon si può trovare il numero di livelli da usare con un dato canale tramite l'inverso della formula data dal teorema di Nyquist:

$$M = 2^{\frac{C}{2B}}$$

Trasmettere un numero maggiore di livelli è inutile, il rumore sarebbe troppo alto.

1.1 Multiplexing

Con "multiplexing" si intende la capacità di far passare più comunicazione all'interno dello stesso canale.

Frequency Division Multiplexing FDM: Con una banda larga, la si può dividere in sotto-bande, ognuna con una comunicazione diversa.

Time division Multiplexing TDM: Se il data rate è molto superiore a quello richiesto da una singola trasmissione, si possono creare n slot di tempo ciclici.

1.2 Comunicazione Wireless

Le comunicazione wireless non possono avvenire in banda base (spettro $[0, B]$): ci sarebbero interferenze, le antenne richieste sarebbero troppo grandi, ogni range di frequenza ha delle proprietà specifiche.

Si usa quindi la banda traslata, si sposta il range a $[f_c - B/2, f_c + B/2]$, ovvero la stessa banda attorno a una frequenza portante f_c.

Il trasmettitore deve quindi codificare e modulare (attorno a f_c) il segnale prima di inviarlo.

Simbolo: Uno stato significativo del canale di comunicazione che persiste per un tempo prefissato. In generale un simbolo può contenere più bit.

Tipi di antenne: Una antenna può essere:

- Omnidirezionale: potenza emessa ugualmente in tutte le direzioni
- Direzionale: il segnale si propaga principalmente in una sola direzione

Il gain è il rapporto tra l'intensità della radiazione in una direzione rispetto all'intensità che si avrebbe con un'antenna isotropica/omnidirezionale, misurato in dBi.

Propagazione onde radio: Esistono diversi tipi di propagazione delle onde radio, sopra i $30MHz$ la più comune è la Line of Sight LoS, che richiede una linea diretta tra RX e TX.

Problemi con la trasmissione LoS:

- Path loss: attenuazione dovuta alla distanza e ambiente in cui il segnale si propaga; misurato in dB

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

  dove n dipende dall'ambiente in cui si propaga il segnale (free space con $n = 2$)
- Rumore: disturbo che può distorcere il segnale
- Multipath: riflessi di un segnale giunti al RX dopo aver già ricevuto l'originale, dovuti a riflessioni, rifrazioni o scattering; i percorsi "alternativi" sono più lunghi, le riflessioni vengono ricevute dopo. Inter-

Symbol-Interference ISI: simboli successivi devono tener conto del multipath dei segnali precedenti

- Effetto doppler: il segnale cambia a causa del movimento di RX o TX

1.2.1 Modulazione e Codifica

L'obiettivo di codifica e modulazione è quello di ottenere una forma d'onda con un determinato significato.

Per la codifica si può agire su ognuno dei 3 parametri di una sinusoidale: Amplitude Shift Keying ASK, Amplitude Shift Keying ASK, Amplitude Shift Keying ASK.

Differential Phase-Shift Keying (DPSK): Accorgersi di una differenza è più facile che misurare un livello, si codifica l'1 con un cambio di fase.

Quadrature Phase-Shift Keying QPSK: Si usa la fase per determinare i bit. Ci sono 4 fasi differenti (90° tra ognuna), di conseguenza 2 bit per simbolo.

Quadrature Amplitude Modulation QAM: Oltre alla fase si modifica l'ampiezza. Più parametri permettono più valori e una costellazione più densa. Si mappa prima in fase, poi in frequenza.

1.2.2 Bit Error Rate BER Curve

La curva BER rappresenta la probabilità che un bit venga alterato, in funzione del rapporto tra la densità di energia del segnale e il livello di rumore.

La probabilità di sbagliare a leggere una codifica, diminuisce all'incrementare del SNR. Tanto più una codifica ha una costellazione di valori densa più è facile sbagliare un simbolo (i valori sono vicini).

Adaptive Modulation and Coding AMC: Si può adattare la codifica in base alla qualità del canale; si definisce un lasso di tempo ogni quanto misurare la qualità del canale e adattare la codifica di conseguenza.

1.2.3 Forward Error Correction

Servono tecniche di correzione dell'errore, molto probabile in ambito wireless. Viene aggiunta ridondanza ai dati inviati: ogni sequenza di bit lunga n diventa una codeword lunga k ($k > n$) secondo una tabella prefissata, rendendo la trasmissione più resiliente agli errori.

In AMC va scelta anche la coding rate, ovvero la proporzione tra bit di dati e bit di ridondanza.

1.2.4 Orthogonal Frequency Division Multiplexing OFDM

Multiplexing usando una divisione in frequenza con bande ortogonali tra loro (separate dal reciproco della durata del simbolo), in quanto bande ortogonali non possono causare interferenze a vicenda.

Si ha una portante f_0 e tante sotto-portanti multiple di f_b, scelta come

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

dove T è la durata di un simbolo.

Questo metodo

- permette di usare più banda rispetto a FDM in quanto non più necessaria una guardia (banda libera) tra le frequenze
- è più robusto a interferenze che riguardano solo alcune subcarrier
- è più robusto ai problemi di multipath perché la distanza tra un simbolo e l'altro è maggiore (ridotta ISI)

1.2.5 Spread Spectrum

Trasmettere il segnale occupando deliberatamente uno spettro più ampio del necessario, in modo da rendere il segnale più robusto, nascondere il segnale e permettere accesso multiplo.

Frequency Hopping Spread Spectrum FHSS: Si genera pseudo-casualmente un codice di spreading, usato per determinare quale frequenza usare all'interno di una certa ampiezza di banda. La frequenza viene cambiata ogni intervallo di tempo prestabilito.

Generalmente resistente a rumore e jamming (compromettere tutte le frequenze è più difficile), nasconde parzialmente il segnale (è difficile leggere il messaggio senza sapere il codice di spreading).

Direct Sequence Spread Spectrum DSSS: Ogni bit di una sequenza viene rappresentato da un insieme di bit, ottenuti da una sequenza casuale. Ogni bit trasmesso, chiamati "chip", dura $1/n$ del tempo dei bit di informazione, dove n è il numero di chip che compongono un bit.

Per mantenere lo stesso data rate è necessaria n volte la banda.

Generalmente, si invia uno `xor` tra bit di informazioni e sequenza di spread (si manda la sequenza originale per uno 0, invertita per 1).

Code Division Multiple Access CDMA: Ogni bit della sequenza da inviare viene codificato con un codice lungo $k \geq 1$ chip, unico per ogni utente. L'idea è che tutti gli utenti possono parlare assieme e le informazioni rimangono distinguibili. I chip usano 1 e -1 (al posto dello 0).

Un 1 viene codificato tramite il codice stesso, 0 con l'inverso. Il ricevitore moltiplica i bit ricevuti con il relativo bit all'interno del codice: se la somma di tutti questi è positiva è stato trasmesso un 1, 0 altrimenti.

Usando un codice non corretto per decifrare il risultato della sommatoria sarebbe inconcludente (vicino allo 0); il valore risultante deve essere abbastanza alto.

Più è alto il numero di utenti, più lo spreading factor deve essere alto; può essere modulato in funzione del numero di utenti.

Questo sistema funziona bene se i vari segnali ricevuti hanno circa la stessa potenza. **Near-far problem:** utenti più lontani avranno potenza minore. La soluzione è modulare la potenza in base alla distanza.

2 WPAN

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

2.1 Bluetooth

Standard 802.15.1. Si compone di reti chiamate **piconet**, all'interno della rete si ha un **master** che controlla la piconet e uno o più **slave** controllati.

Si tratta di comunicazione short range (10-50m), usa la banda ISM $2.4GHz$, data rate $2.1Mbps$-$24Mbps$.

2.1.1 Piconet & Scatternet

Una piconet è composta da **master** e

- **Active Slave AS:** membro attivo della piconet, con un Active Member Address AMA di 3 bit assegnato dal master
- **Parked Slave PS:** membro della piconet temporaneamente disattivato, con un Parked Member Address PMA di 8 bit
- **Standby Slave SS:** membro non sconosciuto ma scollegato, senza indirizzo

Scatternet: Un dispositivo può appartenere a più piconet differenti, portando a una scatternet. Le due piconet rimangono completamente autonome. Nel caso le due piconet usino la stessa frequenza per comunicare, si ha CDMA per evitare interferenze.

2.1.2 Architettura dei protocolli

Ci sono dei protocolli definiti *core*, ovvero necessariamente implementati all'interno di tutti i dispositivi Bluetooth.

Bluetooth radio: Livello fisico, specifica l'interfaccia radio: quali frequenze usare, gestisce il frequency hopping, schema di modulazione e potenza di trasmissione.

Per gestire le scatternet si usa FH-CDMA, anche in caso usino la stessa frequenza si ha il CDMA.

Per comunicare all'interno di una piconet vengono usate:

- Frequency Hopping FH: frequenza decisa dal master, determinata in base al numero di slot passati
- Time Division Duplex TDD: la comunicazione è a slot alternati master-slave, ogni $625\mu s$; la dimensione dei messaggi è di 1, 3 o 5 slot, per mantenere l'alternanza
- Time Division Multiple Access TDMA: per gestire più dispositivi nello stesso momento; il master decide chi può comunicare in quale slot di tempo

Baseband: Si occupa di stabilire la connessione con la piconet, gestire l'indirizzamento, formattazione dei pacchetti, gestire le tempistiche di comunicazione e potenza di trasmissione.

Offre due tipologie di servizio (canali logici):

- **Synchronous Connection-Oriented Link (SCO)** point-to-point: canale bidirezionale $64kbps$, tipicamente audio/voce; il master riserva una coppia di slot adiacenti a intervalli regolari; fino a 3 canali SCO attivi contemporaneamente; traffico real time. Garantiscono un bit rate fisso, per casi delay-sensitive.
- **Asynchronous Connectionless Link (ACL)** point-to-multipoint: occupano tutti gli slot rimanenti, traffico best effort; qualità maggiore senza nessuna garanzia

Alcuni dei campi all'interno dei pacchetti:

- Accesso code 72 bit: utilizzato per sincronizzazione e identificazione. Può essere di 3 tipi: Channel Access Code (CAC, identifica la piconet), Device Address Code (DAC, indirizzo dello slave), Inquiry Address Code (IAC, usato per trovare l'indirizzo di un dispositivo vicino)
- AMA: indirizzo del membro attivo
- Type: tipo del pacchetto
- ARQN: 1 ack, 0 nack
- SEQN: 1 bit di sequence number

ARQN e SEQN sono 2 bit e sufficienti per il controllo degli errori. La sequenza di invio tipica è:

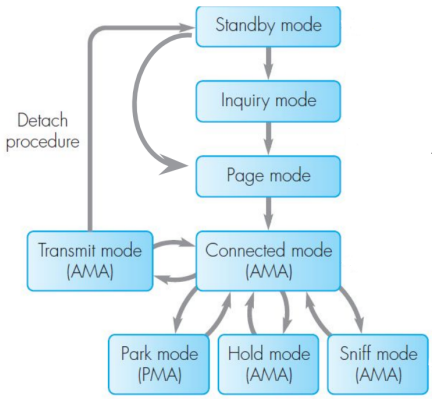
- master invia un pacchetto con SEQN s
- lo slave risponde con ACK e SEQN s

Per la trasmissione successiva si inverte il SEQN. Problemi possibili:

- slave non riceve il pacchetto: risponde con SEQN corretto e NACK; il master re invia il pacchetto
- master non riceve ack: ritrasmette con lo stesso SEQN, lo slave capisce che deve ritrasmettere l'ack dato che il SEQN è uguale al precedente

Link Manager Protocol: "Manager" del collegamento, si occupa di configurare i collegamenti tra dispositivi, gestire i collegamenti attivi e funzionalità di sicurezza e cifratura. Protocollo solamente di controllo, niente dati.

Transizioni di stato:



Appena acceso il dispositivo entra in **standby mode**, nessuna piconet, minimo consumo.

Il master invia periodicamente 32 messaggi consecutivi su canali standard, i quali contengono un IAC packet. Gli slave in **inquiry mode** ascoltano periodicamente i canali aspettando un IAC packet.

Ogni slave ascolta sulle frequenze di wake-up, una volta trovata una trasmissione si può sincronizzare al clock del master, fare random backoff di qualche slot, per poi rispondere. Il master risponde con DAC, AMA e sequenza per il FH, su 16 dei 32 canali. Lo slave risponde con DAC e ACK.

In fase di **paging**, il master invia messaggi di paging per richiamare il dispositivo target, fornire tutti i dati di sincronizzazione necessari e stabilire definitivamente la connessione.

Altri stati: un dispositivo può essere:

- Connected mode: connesso senza trasmettere
- Transmit mode: quando deve trasmettere
- Sniff mode: non ascolta tutti gli slot, mantiene AMA
- Hold mode: ascolta solo canali SCO, mantiene AMA
- Park mode: rilascia l'AMA, rimane membro della piconet, riceve un PMA. Ascolta periodicamente messaggi in broadcast, rimane sincronizzato

Le ultime 3 sono modalità di power saving.

Logical Link Control and Adaptation Protocol L2CAP: Primo livello implementato a livello software. Si occupa di adattare i protocolli di livello superiore al livello baseband e astrarre le feature esposte dai livelli inferiori.

Supporta solo canali ACL e offre 3 tipi di canali logici:

- **Connectionless:** unidirezionale, senza connessione
- **Connection-oriented:** bidirezionale, orientato alla connessione, supporta QoS
- **Signaling:** bidirezionale, usato per messaggi di controllo

Gestisce anche segmentazione e ricostruzione dei frame inviati a livello baseband.

Il tipo di pacchetto viene identificato dal campo Channel Identifie CID: $= 1$ signaling, $= 2$ connectionless, ≥ 64 connection-oriented.

Service Discovery Protocol SDP: Protocollo client-server, il client può richiedere al server:

- ricerca di un servizio
- browse dei servizi disponibili sul dispositivo

Generalmente master chiede, slave risponde.

2.2 BLE

Vuole ridurre i consumi, semplificare il sistema di comunicazione.

Introduce nuove strutture di comunicazione:

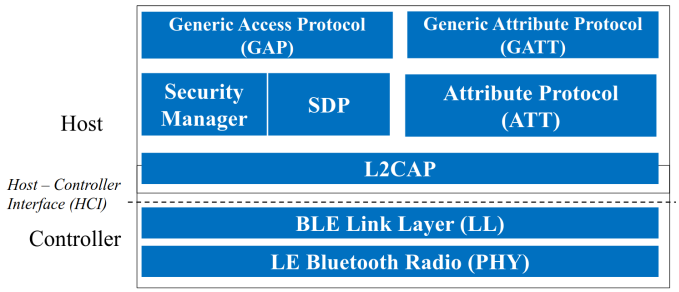
- **Broadcast**: chi è in range ascolta un broadcaster
- **Mesh:** ogni dispositivo può essere connesso a molteplici altri

Aggiunge servizi di positioning, permette di rilevare presenza, distanza e direzione di un dispositivo.

Stessa banda ISM $2.4GHz$, ma 40 canali al posto che 79.

2.2.1 Architettura

Il fisico cambia, il resto è equivalente a BT 2.1.



BLE Radio (PHY): 37 canali usati per data, ultimi 3 per advertising.

Generic Attribute Profile GATT: Permette scambio di dati strutturati tra client che richiedono e server che offrono servizi tramite profili. I ruoli non sono fissi, ogni profilo ha dati e caratteristiche associate.

General Access Protocol GAP: Un'applicazione può decidere uno dei ruoli fondamentali definiti da GAP:

- **Broadcaster:** spedisce dati in modo connectionless come pacchetti di advertising
- **Observer:** riceve pacchetti di advertising connectionless

- **Peripheral:** opera in slave (advertiser) mode a livello di link layer
- **Central:** opera in master (initiator) mode a livello di link layer

Creazione connessione unicast: Il master ascolta, lo slave è l'advertiser, vuole essere trovato mandando advertising packets. Una volta che il master (initiator) ascolta un messaggio, invia una connection request nello slot di tempo successivo, contenente anche le informazioni per il FH.

Connessione broadcast: Per quando un broadcaster ha solo interessa a inviare dati. Gli observer ascoltano i canali di advertising per i messaggi del broadcaster.

Lo scanning può essere passivo oppure attivo, in cui vengono richiesti dati in unicast al dispositivo di broadcast tramite i canali di advertising.

2.2.2 BLE State Machine

Tutti partono dallo **standby**, possono andare a:

- **Advertising:** lo slave si annuncia per cercare la piconet, non è più il master che cerca
- **Initiating:** vengono ascoltati i messaggi di advertising
- **Isochronous broadcasting:** periodico broadcasting di informazioni
- **Scanning:** il dispositivo si mette in ascolto

Advertising: Ogni certa quantità di tempo, viene inviato un advertising event su uno o più dei canali di advertising. Il tempo è determinato da due parametri: `advInterval` stabilito e `advDelay` più breve e casuale.

2.3 ZigBee

Standard 802.15.4, cerca principalmente affidabilità, basso costo e complessità, bassissimo consumo, scalabilità. Usa le bande $2.4GHz$ e $915/868MHz$.

Topologia di rete: Si possono avere topologie a stella, albero o mesh, quindi anche multi-hop (serve routing).

Classi di nodi: Ci sono due macro classi di nodi:

- **Full Function Device FFD:** Un coordinatore e uno o più router, possono fare instradamanto
- **Reduced Function Device RFD:** end device, possono solo comunicare e ricevere dati; ridotta complessità e consumo

Tipologie di dati: In base al caso d'uso:

- **periodici:** inviati dopo un intervallo di trasmissione fissato
- **intermittenti:** comunicati in base a un evento; asincroni
- **ripetitivi e a bassa latenza:** allocazione di time slot

2.3.1 Architettura

Livello PHY: Vengono specificati tipo di modulazione e spread spectrum per ognuna delle 3 bande possibili.

Multiplexing sui canali all'interno della banda, spread spectrum DSSS per la comunicazione. I data rate sono sempre molto limitati.

Livello MAC: Si occupa di

- gestire l'invio dei beacon per il coordinatore, sincronizzazione con i beacon del coordinatore per gli altri
- (dis)associazione alla PAN ascoltando i beacon
- accesso al canale tramite CSMA/CA
- MAC Address
- gestione del duty cycle

Si possono avere due tipi di trasmissioni:

- diretta: bidirezionale dispositivo e coordinatore
- indiretta: solo da coordinatore verso il dispositivo

Modalità di trasferimento: Sono due possibili:

- **Unslotted CSMA/CA**, senza l'ausilio di beacon; i dispositivi accedono usando CSMA/CA, senza vincoli di slot; si ripete la fase di backoff finché non riesce a trasmettere
- **Slotted CSMA/CA**, con beacon

Slotted CSMA/CA: Si fonda sull'invio di beacon da parte del coordinatore; vengono usati per

- sincronizzare i dispositivi
- organizzare i periodi di trasmissione
- gestire la trasmissione indiretta, nei beacon viene trasmessa la lista di dispositivi che hanno frame pendenti

Il tempo totale tra un beacon e l'altro è detto **superframe**, rappresenta l'organizzazione logica della comunicazione. Si ha un duty cycle, si alternano periodi di attività e inattività, in cui viene spenta la radio.

L'**intervallo tra beacon** è

$$aBaseSuperframeDuration \cdot 2^{BO}$$

simboli, dove $aBaseSuperframeDuration = 960$ simboli e il Beacon Order BO va da 0 a 14.

La **durata del superframe** invece è

$$aBaseSuperframeDuration \cdot 2^{SO}$$

dove il Superframe Order SO è sempre un valore 0-14.

Il rapporto tra i due fornisce il duty cycle.

Il superframe viene di viso in slot con diversi tipi di accesso:

- **Contention Access Period CAP:** accesso al canale usando CSMA/CA. Canale a contesa, per capire lo stato del canale:
  - viene scelto un intero casuale nell'intervallo $[0, 2^{BE} - 1]$, dove il Backoff Exponent BE è un parametro, e viene atteso quel numero di slot (20 simboli); se il conteggio viene interrotto, riprende al superframe successivo
  - Dopo l'attesa, vengono fatti CW Clear Channel Assessment, dove Contention Window CW è un parametro

  - Se dopo i CCA il canale è libero comincia a trasmettere
  - Se il canale risulta occupato, si allarga la finestra del random backoff incrementando di 1 BE e il numero di backoff NB
  - Se $NB = 4$: transmission failure

- **Contention Free Periodo CFP:** intervallo per le comunicazioni con banda riservata tramite Guaranteed Time Slot (campo del beacon)

3 WiFi 802.11

Si ha una rete con uno o più Access Point AP, coordinata da Point Coordinator Function PCF (un solo punto di coordinamento, l'AP). Un Basic Service Set BSS indica la cella o rete WiFi.

Alternativamente, si può avere una rete ad hoc, senza PCF ma con una Distributed Coordination Function DCF, con un Indipendent Basic Service Set IBSS.