Riassunto RWM

Massimo Perego

Premessa: Non si tratta di un documento completo, ho tirato a indovinare cosa possa essere più importante. Inoltre è pensato per essere letto conoscendo già l'argomento, non come fonte stand-alone.

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:

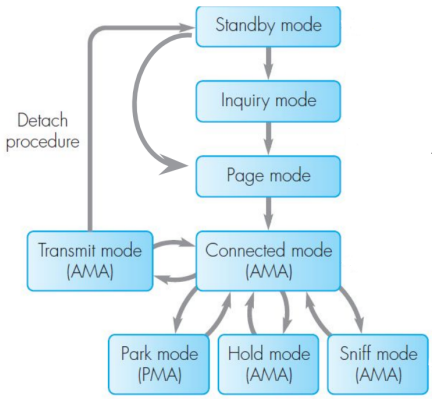
- master invia un pacchetto con SEQN s
- lo slave risponde con ACK e SEQN s

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:

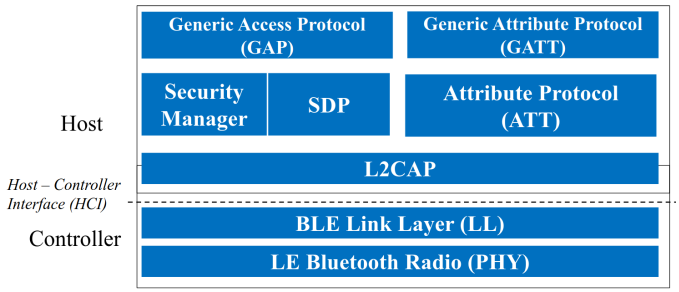
- **Broadcast**: chi è in range ascolta un broadcaster
- **Mesh:** ogni dispositivo può essere connesso a molteplici altri

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.

Al di sopra di PHY, MAC e PCF si ha un livello di **Logical Link Control LLC:** il quale offre principalmente 3 servizi:

- Unacknowledged connectionless service: consegna non garantita, senza connessione, niente controllo degli errori
- Connection-mode service: canale punto-punto affidabile
- Acknowledged connectionless: senza connessione, ma con ack

3.1 Senza infrastruttura

Canale molto inaffidabile, con frame da $2304B$. Il sottolivello MAC offre:

- Servizio dati asincrono: niente garanzie su delay o QoS, best effor
- Servizio time-bounded: garanzie sul delay, disponibile solo in presenza di AP

3.1.1 Distributed Coordination Function DCF

Opera in **CSMA/CA**: l'accesso al canale viene regolato aspettando del tempo prima di trasmettere. Diversi periodi di attesa possibili:

- **slot time:** unità base di tempo
- **Short Inter Frame Spacing SIFS:** intervallo breve
- **DCF Inter Frame Spacing DIFS:** SIFS + 2 slot time
- **PCF Inter Frame Spacing PIFS:** SIFS + slot time

Per trasmettere:

- il sender ascolta il canale

- fa un CCA
- ascolta per tempo DIFS
- fa un altro CCA

Se il canale è risultato sempre libero, allora il dispositivo può cominciare a trasmettere.

Se necessario l'ack, l'attesa di questo ha durata SIFS, per non andare in conflitto con i CCA. Al contrario, si presume frame corrotto se dopo SIFS non viene ricevuto ack.

Se il canale è occupato, il sender aspetta il termine della trasmissione, per poi aspettare uno dei periodi di tempo (in base alla priorità del messaggio), per poi avere un periodo di contesa, in cui il dispositivo aspetta un numero random di slot time da attendere. Se interrotto, il conteggio riprende alla contesa successiva

3.1.2 Problema del terminale nascosto

Il carrier sense funziona solo se il dispositivo che comincia a trasmettere è rilevabile. Se due dispositivi che non si vedono vogliono trasmettere allo stesso RX vedrebbero entrambi il canale libero nello stesso momento.

Per risolvere, il sender invia una Request to Send RTS, contenente sorgente e destinazione della richiesta, oltre che durata stimata.

Quando un terminale riceve un RTS:

- se non è il target del messaggio, alloca un Network Allocation Vector NAV, tempo in cui sa di non poter trasmettere a quel RX
- il destinatario risponde con un Clear to Send CTS, contenente sorgente, destinazione e tempo rimanente

Il CTS viene ricevuto da tutti i terminali nel raggio del destinatario, che allocheranno un NAV per il tempo indicato nel CTS.

Dopo il CTS, il sender aspetta SIFS prima di cominciare a inviare.

Frammentazione: Il frame a livello MAC è più piccolo di un frame Ethernet (troppi errori altrimenti), quindi un frame LLC viene suddiviso in frammenti, ognuno dei quali contiene informazioni riguardo il NAV per i dispositivi non direttamente coinvolti.

Frammentazione e correzione dei dati viene fatta a livello MAC, tra AP e terminale, per ridurre il ritardo di correzione.

3.2 Con Infrastruttura

Nel caso più semplice si ha un AP con relativo BSS; si possono anche avere più BSS connesse tramite un distributed system DS, formando un Extended Service Set ESS (comunque visto come un'unica rete).

3.2.1 Point Coordination Function PCF

In presenza di AP, tutti i frame passano per questo, permettendo di avere servizi time-bounded. AP usa tempo PIFS, per prevalere sulle stazioni che usano tempistiche DIFS e SIFS.

AP manda beacon frame periodici, contenenti:

- Parametri PHY (modulation and coding scheme)
- Sincronizzazione
- Supporto a PCF con le relative informazioni
- Invito per le nuove stazioni, non ancora associate

Una rete manda beacon per farsi scoprire e comunicare le proprie caratteristiche per nuove associazioni.

Il tempo è diviso in blocchi (superframe), con due periodi:

- Senza contesa, opzionale, per i servizi time bounded
- A contesa, sempre presente

Per il periodo senza contesa: l'AP aspetta PIFS al termine della comunicazione precedente, tutti gli altri aspettano DIFS, quindi prende possesso del canale e fornisce il permesso di trasmettere dove necessario, aspettando SIFS tra una trasmissione e l'altra. Al termine manda un Contention Free End.

3.2.2 Formato Frame MAC

Nell'header del frame si hanno obbligatoriamente

- Frame Control FC: 2 byte contenenti informazioni sul tipo di frame, inclusi tipo del messaggio e 2 bit che indicano se il messaggio è verso o dal DS
- Duration/Connection ID D/I: contengono la durata della trasmissione rimanente, usate per i NAV
- Indirizzo di destinazione e fino ad altri 3 indirizzi, il cui significato varia in base ai bit To DS e From DS; in generale sono sorgente e destinazione del messaggio, e l'eventuale "hop" in mezzo

3.3 Orthogonal Frequency Division Multiple Access OFDMA

WiFi 6, usa subcarrier per fornire connettività a più dispositivi contemporaneamente.

Vengono serviti più dispositivi contemporaneamente, assegnando gruppi di sotto-portanti a dispositivi diversi.

Le frequenze sono raggruppate in blocchi base asssegnabili a ogni utente, chiamati Resource Units RU. Ogni RU ha una sequenza unica di 7 bit che identifica univocamente il gruppo di sotto-portanti.

Alcune sotto-portanti sono usate come pilot, trasmettono onde standard usate per stimare la qualità del segnale.

3.3.1 Downlink

Per comunicare l'assegnamento delle risorse, l'AP

- invia una **Multi-User Request to Send MU-RTS**, ha la funzione di RTS
- le stazioni rispondono con un CTS in contemporanea
- l'AP invia gli assegnamenti delle RU
- l'AP invia un Block Acknowledgment Request BAR
- i dispositivi rispondono in parallelo con un Block ACK

Ogni operazione è intervallata da tempo SIFS.

3.3.2 Uplink

Meno prevedibile, richiede di sincronizzare i dispositivi che devono trasmettere. Tutto gestito dall'AP:

- l'AP invia **Buffer Status Report Poll BSRP**, chiede chi ha da dire qualcosa
- i dispositivi rispondono con un **Buffer Status Report BSR**, contenente le quantità di dati da trasmettere
- l'AP assegna risorse in base alle risposte delle stazioni, invia il **MU-RTS** indicando la suddivisione delle RU
- le stazioni rispondono con CTS
- l'AP invia un trigger aggiuntivo per sincronizzare tutti i dispositivi
- ogni stazione trasmette in parallelo sulle risorse allocate; se la trasmissione dura meno: padding
- se necessario: l'AP invia **multi-station block acknowledgment Multi-STA Block ack**

3.4 WLAN Security

802.11 definisce feature di sicurezza. Si vuole cifratura a livello di data link.

Wired Equivalent Privacy WEP: Cifratura RC4, non obbligatorio, stessa chiave per tutto il traffico.

Robust Security Network RSN: Per sopperire alle lacune di WEP; al suo interno ha diversi servizi:

- **Accesso control:** impone l'utilizzo di protocolli di sicurezza e assiste lo scambio delle chiavi
- **Authentication:** definisce lo scambio tra utente e AS, genera chiavi temporanee
- **Privacy with message integrity:** il payload MAC viene cifrato e viene aggiunto un controllo per l'integrità

Più fasi per le operazioni:

- **Discovery:** AP manda il beacon con i servizi disponibili, vengono negoziate le capabilities prima di decidere le funzioni di sicurezza da usare
- **Autenticazione e gestione chiavi:** STA richiede all'AP autenticazione tramite AS (remoto EAP o meno), vengono generate e consegnate le chiavi
- **Protected data transfer**
- Chiusura della connessione

Per generare le chiavi:

- AP $\rightarrow$ Client: Nonce
- Chiave di sessione K_S calcolata dal client, a partire da MAC address, nonce e master key
- Client $\rightarrow$ AP: nonce, assieme a un Message Integrity Check MIC_S, dipendente dalla sessione
- AP calcola la stessa K_S
- AP $\rightarrow$ Client: chiave di gruppo K_G, cifrata tramite K_S
- Client verifica che K_S dell'AP sia corretta
- Client $\rightarrow$ AP: ack cifrato con K_S
- AP verifica che K_S del client sia corretta

Lo standard 802.11i considera due alternative per la protezione dati:

- **TKIP (WPA):** RC4 con codice integrità di 64 bit, usando MAC sorgente e destinazione
- **CCMP (WPA-2):** integrità tramite CBC AES-128

3.5 802.11e EDCA Enhanced Distributed Channel Access

Quando i livelli superiori richiedono un certo QoS, si possono modificare dei parametri in base a profili prefissati. I parametri sono:

- CWMin: minima dimensione della contention window
- CWMax: massima dimensione della contention window
- AIFSN: numero di SIFS+N slot time, tempo di attesa

- Max TXPO: massimo tempo in cui una stazione può trasmettere senza lasciare il canale

Permette una definizione più granulare delle politiche di accesso al canale in contesa, riducendo i tempo per le applicazioni che lo necessitano.

4 Ad Hoc Distance Vector Routing Protocol AODV

Protocollo di routing per creare e riempire tabelle di instradamento, pensato per reti senza infrastrutture in cui ogni nodo è anche router. I percorsi vengono creati solo a necessità.

Gli obiettivi principali sono:

- Gestione dinamica della rete ad hoc
- Auto inizializzante
- Loop free
- Risposta rapida alla richiesta di rotta e alla rottura di link/cambio di topologia

Le funzionalità offerte sono:

- Scoprire e costruire percorsi
- Mantenere percorsi in modalità soft-state (scadono se non aggiornati)
- Riconoscimento errori e cancellazione percorsi

Protocollo a livello di applicazione (UDP 654), al di sopra ci sono i messaggi AODV, sotto stack IP con PHY e LL qualsiasi.

4.1 Tabelle di Routing

Ogni nodo mantiene una tabella con destinazioni conosciute e next hop per arrivarci. Ogni entry della tabella contiene:

- IP Destinazione
- Sequence Number SN della destinazione: in una dinamica, ogni entry possiede un SN che codifica la "freschezza" dell'informazione. Si tratta di un valore per ogni nodo, modificabile solo dal nodo stesso: incrementato di 1 quando un nodo inizia o risponde a una ricerca di percorso; gli altri nodi possono aggiornare il SN quando vengono ricevute informazioni più aggiornate
- Flag di validità del SN (disabilita temporaneamente il percorso)
- Stato del percorso
- Interfaccia di rete

- Hop count per arrivare alla destinazione
- Lista dei precursori: quali vicini utilizzano il router per arrivare alla destinazione
- Lifetime della entry: scadenza

4.2 Route Request RREQ

All'interno del pacchetto: Tipo 1. Ci sono delle flag:

- `D` Destination only: solo la destinazione può rispondere
- `U` Unknown SN: l'origine non conosce il SN della destinazione
- `G` Gratuitous: se risponde un nodo intermedio, questo deve creare il percorso bidirezionale

Oltre a questo contiene:

- Hop count: incrementato di 1 ogni inoltro, tiene traccia della distanza della richiesta
- RREQ ID: identificativo della richiesta, permette di riconoscere copie della stessa richiesta
- Destination IP Address e ultimo SN conosciuto
- Originator IP Address e SN

Una RREQ viene creata quando serve conoscere un percorso verso una destinazione. Per inviare:

- L'originator incrementa RREQ ID e il proprio SN
- Setta i flag come necessario
- Mantiene una copia per un tempo standard `PATH_DISCOVERY_TIME`, per evitare il riprocessamento e reinvio del pacchetto, se ricevuto nuovamente

Expanding Ring Search: Per evitare di propagare "inutilmente" una RREQ in tutta la rete, il TTL dell'header IP della RREQ viene aumentato iterativamente, espandendo la ricerca man mano (valori di inizio, incremento e fine sono parametri).

Senza conoscenze a priori si parte da un TTL standard, se ci sono informazioni riguardo la destinazione (percorso scaduto o interrotto), si usa l'hop count della vecchia entry come TTL.

Processamento e Inoltro: Quando un nodo riceve una RREQ:

- Controlla se ha già visto la richiesta: `RREQ_ID` e originator IP già noti
- Aggiorna il percorso verso l'originator: se il SN della richiesta è maggiore di quello posseduto, aggiorna la entry verso l'originator impostando come next hop il nodo da cui è arrivata la richiesta e hop count pari a quello dello RREQ
- Se non può rispondere con RREP, inoltra la richiesta in broadcast (livello IP) ai vicini incrementando di 1 l'hop count e ponendo il SN della DST al massimo tra quello della RREQ e quello presente all'interno della propria routing table

Il propagarsi di una richiesta permette ai nodi che la ricevono di costruire un percorso verso l'originator.

4.3 Route Reply RREP

Tipo 2, le flag sono:

- `A`: richiede ack, per prevenire link non affidabili

Inoltre contiene:

- prefix size: usato per subnet, indica la lunghezza del prefisso di rete dell'IP dst
- Destination IP Address, chi ha generato la risposta
- Destination SN
- Lifetime, in ms, tempo di validità della risposta

Creazione: Chi può generare la risposta:

1. La destinazione: quando riceve la RREQ
   - Incrementa il proprio SN di 1
   - Hop count = 0
   - Aggiorna lista dei precursori

- Imposta il campo lifetime, secondo parametro
- Invia RREP lungo il percorso reverse in unicast
- Drop della RREQ

2. Un nodo intermedio: con delle condizioni:
   (a) Avere una entry con percorso valido per la destinazione
   (b) Flag `D == 0`
   (c) DST SN della entry $\geq$ DST SN della RREQ

   Se tutte soddisfatte:
   - Hop count = hop count della entry
   - Aggiorna la lista dei precursori
   - Imposta campo lifetime, pari a quello della entry
   - Invia RREP lungo il percorso reverse in unicast
   - Drop della RREQ
   - Se flag `G == 1`, allora invia una RREP anche alla destinazione

Processamento e Inoltro: Quando un nodo riceve un messaggio RREP

- Aggiorna la entry nella tabella se: la corrente non è valida, DST SN della RREP maggiore di quello della entry o il numero di hop è minore
- Aggiorna
  - Entry marcata come valida
  - Next hop della entry = nodo da cui proviene RREP (DST della RREQ)
  - RREP hop count += 1
  - Lifetime della entry
  - Lista dei precursori

RREP con flag Gratuitous: Durante il ritorno della RREP, ogni nodo intermedio crea il path da se stesso alla destinazione originale della RREQ. Per creare il percorso bidirezionale anche tra nodo che ha risposto e destinazione serve la flag `G`.

Se un nodo intermedio riceve RREQ con flag `G` alzata, deve "costruire" anche il percorso verso la destinazione della RREQ. Il nodo invia quindi 2 RREP indipendenti:

1. Verso il nodo originator della RREQ
2. Verso la destinazione della RREQ, con parametri atti a "simulare" che la destinazione abbia fatto una RREQ verso l'originator, per completare il path bidirezionale

4.4 Hello Message

Messaggi broadcast con TTL=1, senza incremento di SN, per fornire informazioni riguardo la connettività ai propri vicini.

RREP speciale con:

- DST IP = IP del nodo stesso
- DST SN = SN del nodo
- Hop count = 0
- Lifetime = dato da parametri `ALLOWED_HELLO_LOSS * HELLO_INTERVAL`

Meccanismo facoltativo, usato se non si ricevono altri informazioni da un vicino.

4.5 Route Error RERR

Ogni nodo ha il compito di tenere traccia della connettività con i nodi indicati come "next hop" nella tabella di routing. Questa può essere controllata tramite qualsiasi pacchetto a livello di data link o rete (se ricevo informazioni il link funziona).

Quando un nodo **identifica un link interrotto/scaduto** parte di un percorso attivo:

- Vengono invalidati i percorsi esistenti

- Identifica le destinazioni per le quali viene usato come next hop il link interrotto
- Determina quali vicini nella lista dei predecessori possono essere affetti dal problema e invia un Route Error RERR

Tipo 3, le flag:

- `N` No Delete: indica alla destinazione di non eliminare la entry, il percorso è stato riparato localmente

Altri campi:

- Destination Count: indica il numero di destinazioni non più raggiungibili contenute nel messaggio
- Unreachable Destination IP Address
- Unreachable Destination SN

Quando viene inviato un messaggio RERR:

- Link interrotto trovato mentre si prova a inoltrare un pacchetto DATA (era il next hop verso una destinazione)
- Ricezione di pacchetto DATA per una destinazione sconosciuta (l'originator del pacchetto usa informazioni troppo vecchie)
- Ricezione di un pacchetto RERR da un vicino per uno o più percorsi attivi

Processamento e Inoltro: Quando un nodo riceve una RERR:

- Marca come invalide le entry della destinazione indicate nel RERR
- Ogni entry invalidata viene preservata per un tempo (parametro)
- Inoltra RERR ai predecessori

Local Repair: Se un nodo riceve un pacchetto per una destinazione "non troppo lontana" (distanza definita) il cui percorso è interrotto, allora il nodo prova a riparare il percorso tramite una RREQ con TTL tale da non raggiungere la sorgente del pacchetto DATA (hop count del percorso verso originator).

Due possibili esiti del tentativo di riparazione:

- procedura fallisce: manda RERR
- trova un percorso alternativo: aggiorna la propria entry

Se il percorso trovato è più lungo del precedente, invia una RERR con flag `N` alzata, sta alla sorgente decidere come procedere (la nuova lunghezza è accettabile o serve una RREQ?).

5 Mobile Network

L'idea è molteplici trasmettitori, area divisa in celle, ogni cella servita da una Base Station BS, la quale contiene trasmettitore, ricevitore e unità di controllo.

Le celle devono coprire "bene" l'area e avere una disposizione uniforme (comunque considerando vincoli dovuti alla situazione reale).

Riuso delle frequenze: Celle vicine non possono usare la stessa banda di frequenza. Tre soluzioni possibili:

- **Frequenze diverse tra celle vicine**: ogni cella ha la sua banda, servono più bande differenti (costano); usato da 2G
- Usare la **stessa frequenza ma tecniche di codifica** per evitare interferenze, come CDMA
- Usare **frequenze diverse ai bordi** delle celle, l'**intero spettro al centro**; permette banda maggiore ma richiede coordinamento tra le BS (da 4g e 5G)

Architettura: Si divide in due macro aree:

- **Radio Access Network RAN:** stazioni e collegamento radio che forniscono connettività ai dispositivi mobili (parte wireless)
- **Core Network:** parte responsabile di gestione e controllo della comunicazione

In generale, esistono 2 tipologie di canali e traffico:

- Canali di controllo: informazioni per la gestione delle operazioni; Control Plane
- Canali di traffico: voce e dati; Data Plane

La divisione tra i due piani è netta ed esplicita.

5.1 Operazioni

Inizializzazione: Quando un dispositivo vuole iniziare una comunicazione con la rete cellulare:

- Disponibilità dei canali radio con BS: ascolta le trasmissioni broadcast delle BS per individuare la migliore e quali parametri usare
- Traffico di controllo per iniziare la comunicazione: viene inoltrata la richiesta di comunicazione fino al MTSO, parte della CN che si occupa di autenticare l'utente, verificare permesse e risorse
- Creazione dei collegamenti su data plane: se la fase di controllo va a buon fne, vengono allocati canali fisici e logici necessari per il traffico dati

Paging: Quando *qualcosa* deve raggiungere il dispositivo, è compito della rete trovarne la posizione quando necessario. MTSO contatta le BS per trovare il dispositivo.

Chiamata accettata: I dati passano sempre per il CN, il dispositivo accetta la chiamata, MTSO crea un circuito e le BS impostano i canali radio data plane.

Handoff: Quando un dispositivo esce da una cella, deve collegarsi a un'altra. Le fasi per il cambio cella sono: decidere la nuova associazione, gestirla, riconfigurare i percorsi di comunicazione.

Il tutto deve avvenire in maniera automatica e trasparente al dispositivo.

La procedure può essere decisa in due modi:

1. solo dalla rete: in base al segnale in uplik
2. coinvolgendo il dispositivo: anche in base a feedback sul downlink

Vengono usate diverse metriche, ma il parametro principale è la potenza del segnale ricevuto. Possibili metodi per stabilire quando cambiare BS a cui il dispositivo è collegato:

- **Solo potenza relativa:** l'associazione viene fatta alla BS con il migliore segnale. Potrebbe portare a cambio continuo tra BS quando sui bordi delle celle e l'handover è costoso
- **Soglia di segnale:** L'handover viene fatto nel caso incui il segnale è peggiore di un'altra BS e allo stesso tempo sotto una certa soglia. Come si definiscono le soglie? (difficile)

- **Isteresi:** Per far partire l'handover deve esserci una differenza significativa di potenza, risolvendo il ping pong

La soluzione reale è combinare i metodi.

L'handover può essere:

- **Hard**: dispositivo associato a una sola BS alla volta, cambio immediato di frequenza
- **Soft**: il dispositivo mantiene connettività con entrambe le BS e ne rilascia una quando il segnale è chiaramente dominante; occupa più risorse

Duplex: Può essere gestito come:

- FDD: divisione in frequenza, minore delay, maggiori risorse richieste
- TDD: una sola frequenza e slot di tempo; maggiore ritardo dovuto all'attesa

6 4G LTE

Introduce una separazione più netta tra data e control plane. Le stazioni si chiamano ora eNodeB. Il dispositivo utente si chiama User Equipment UE.

La rete si divide in:

- **E-UTRAN**, parte wireless, che comprende:
  - **UE**
  - **eNodeB:** Fornisce connettività radio all'UE e lo collega alla CN; ha i compiti di una BS
- **EPC**, che contiene i moduli:
  - **MME Mobility Management Entity:** si occupa di tutto il traffico di controllo e segnalazione all'intero della rete, tra CN e UE usando protocolli NAS; si occupa di gestione del contesto UE tramite operazioni NAS, dei bearer, della mobilità, del paging, degli aspetti di sicurezza e cifratura; tra UE e MME transitano solo dati di controllo
  - **HSS Home Subscriber Server:** contiene le informazioni dell'utente riguardanti il profilo e la connessione
  - **P-GW Packet Data Network Gateway:** bordo tra rete LTE e reti esterne; gestisce l'assegnamento IP dell'UE, garantisce QoS, filtra pacchetti IP downlink in bearer differenti per QoS, gestisce la mobilità tra reti non-3GPP
  - **S-GW Serving Gateway:** Unico modulo data plane, responsabile della gestione del traffico user plane. Si occupa di gestire tutti i pacchetti IP degli utenti, gestione dei bearer in fase di handover (dentro la TA), funzionalità di buffering quando UE è IDLE-CONNECTED; si tratta del punto di gestione, con un sottogruppo di eNodeB assegnate.
  - **PCRF Policy Control and Charging Rules Function:** svolge funzioni di controllo e autorizzazioni per i singoli flussi a livello di P-GW, autorizza QoS secondo il profilo utente (da HSS); contiene le regole da applicare all'utente, tramite il P-GW

6.1 Modulazione e Codifica