

Domande Reti Wireless e Mobili

Massimo Perego

Indice

1	Trasmissione Wireless	2
2	WPAN	5
3	WiFi	8
4	AODV	10
5	4G LTE	12
6	5G	14
7	Comunicazione satellitare	15

1 Trasmissione Wireless

1. Descrivere le tecniche di multiplexing TDM, FDM e OFDM. Data la stessa ampiezza di banda, quali sono i vantaggi di OFDM rispetto a FDM?

Solution: Tutte e tre le tecniche servono per far passare più comunicazioni sullo stesso canale, ma lo fanno in maniera diversa:

- **Time Division Multiplexing TDM:** tutte le comunicazioni usano la stessa portante in frequenza, ma ognuna ha uno slot di tempo ciclico in cui può trasmettere. Ogni comunicazione ha accesso esclusivo al canale per breve tempo. Può essere usata quando il data rate del canale è molto maggiore del data rate richiesto da una singola comunicazione; richiede una precisa sincronizzazione
- **Frequency Division Multiplexing FDM:** ogni comunicazione ha una sotto-banda assegnata a uso esclusivo, permettendo la trasmissione in simultanea di tutti i canali. Si può usare quando la banda a disposizione è molto maggiore di quella richiesta da un singolo canale; ha una bassa efficienza spettrale dovuta all'uso di guardie tra le fasce di frequenze, necessarie per evitare interferenze
- **Orthogonal Frequency Division Multiplexing OFDM:** la banda viene divisa in sotto-portanti ortogonali, frequenze vicine che non causano interferenze tra loro in quanto durante il picco di una frequenza il contributo delle altre è a zero; più robusto a interferenze che riguardano solo alcune sotto-portanti e a problemi di multipath in quanto la distanza tra simboli è maggiore

Considerando la stessa ampiezza di banda, OFDM permette una maggiore efficienza spettrale, non richiedono guardie di frequenza inutilizzata tra un canale e l'altro; allo stesso tempo presenta una maggiore resistenza ai fenomeni di fading e multipath.

2. Molte tecnologie wireless codificano e trasmettono le informazioni utilizzando una tecnica denominata Adaptive Modulation and Coding AMC. Descrivere il funzionamento di questa tecnica e vantaggi rispetto a una tecnica di modulazione e codifica statica.

Solution: La tecnica AMC permette di adattare dinamicamente lo schema di modulazione e tasso di codifica in base alle condizioni del mezzo di trasmissione, altamente variabili in ambito wireless.

In generale, viene misurata la qualità del canale (spesso tramite l'invio di segnali standard) e in base a questa vengono scelti:

- Schema di modulazione: il modo in cui i bit vengono mappati sul segnale analogico, ad esempio QPSK, QAM, ...; in generale, migliore è il canale maggiore la quantità di bit per simbolo della modulazione, permettendo data rate migliore, ma potenzialmente più suscettibile a errori
- Tasso di codifica: il rapporto tra il numero di bit utili e i bit totali trasmessi dopo la fase di Forward Error Correction; si aggiunge una ridondanza per far rimanere il segnale distinguibile anche in caso di distorsioni, in base alla qualità del canale va deciso quanta ridondanza inserire

La misurazione del canale viene ripetuta a intervalli regolari. Per sapere ogni quanto campionare le condizioni del canale si definisce un Coherence time, lasso di tempo in cui il canale sicuramente non potrà subire cambiamenti significativi

$$T_C = \frac{1}{f_D}$$

dove f_D è la frequenza di Doppler, dipende dalla velocità di movimento tra trasmettitore e ricevitore.

AMC permette quindi di massimizzare l'utilizzo della capacità del canale, adattandosi a condizioni anche mutevoli, ad esempio passando a uno schema più robusto quando il canale si degrada. In generale permette un throughput migliore rispetto a tecniche statiche, al costo di una maggiore complessità di gestione del sistema.

3. Un transceiver è in grado di trasmettere 500 simboli al secondo. Il livello fisico implementa il meccanismo di Adaptive Modulation And Coding Scheme. Date le seguenti curve di BER e la tabella di coding rate, si determinino:

1. Le codifiche ammissibili
2. Il data-rate massimo (in media) indicando la codifica utilizzata

Caso 1:

$$SNR = 9dB, \quad \text{target } BER = 10^{-3}$$

Caso 2:

$$SNR = 13dB, \quad \text{target } BER = 10^{-4}$$

Non posso riportare il grafico, ma fidati che:

- BPSK: BER 10^{-3} per $SNR \geq 6.5$ e BER 10^{-4} per $SNR \geq 8$
- QPSK: BER 10^{-3} per $SNR \geq 8$ e BER 10^{-4} per $SNR \geq 9.5$
- 16-QAM: BER 10^{-3} per $SNR \geq 11$ e BER 10^{-4} per $SNR \geq 12.5$

Coding rate:

SNR	Coding rate		
	BPSK	QPSK	16-QAM
$< 5dB$	0.5	0.3	0.1
$5dB-9dB$	0.7	0.6	0.5
$> 9dB$	0.9	0.8	0.7

Solution: Per il **caso 1** si può vedere che le codifiche ammissibili sono BPSK e QPSK.

BPSK, con coding rate 0.7 e 1 bit per simbolo:

$$500 \frac{sim}{s} \cdot 1 \frac{bit}{sim} \cdot 0.7 = 350 \frac{bit}{s}$$

QPSK, con coding rate 0.6 e 2 bit per simbolo:

$$500 \frac{sim}{s} \cdot 2 \frac{bit}{sim} \cdot 0.6 = 600 \frac{bit}{s}$$

Per il **caso 2**, tutte e tre le codifiche sono ammissibili.

BPSK, con coding rate 0.9 e 1 bit per simbolo:

$$500 \frac{sim}{s} \cdot 1 \frac{bit}{sim} \cdot 0.9 = 450 \frac{bit}{s}$$

QPSK, con coding rate 0.8 e 2 bit per simbolo:

$$500 \frac{sim}{s} \cdot 2 \frac{bit}{sim} \cdot 0.8 = 800 \frac{bit}{s}$$

16-QAM, con coding rate 0.7 e 4 bit per simbolo:

$$500 \frac{sim}{s} \cdot 4 \frac{bit}{sim} \cdot 0.7 = 1400 \frac{bit}{s}$$

2 WPAN

1. Nel protocollo 802.15.4 (Livello PHY e MAC di ZigBee) viene introdotto il concetto di “Duty-Cycle”. Descrivere in cosa consiste e che vantaggi porta rispetto a 802.11 (Wi-Fi) per l'utilizzo in ambito IoT.

Solution: Il coordinatore di una rete ZigBee invia a intervalli regolari dei beacon, utilizzati per sincronizzare i dispositivi e organizzare i periodi di trasmissione. Il tempo tra un beacon e l'altro si divide in una prima parte di attività e una di inattività, per tutti i dispositivi.

Con duty cycle si intende l'alternarsi di periodi di attività e inattività, a radio spenta. Questo permette di ridurre significativamente i consumi rispetto ad altri standard, come 802.11, che richiedono di mantenere la radio sempre accesa.

In ambito IoT, in generale, i dati da trasmettere sono in quantità limitata e si dà la priorità a un basso consumo energetico. In questo caso tenere la radio spenta per la maggior parte del tempo può essere vantaggioso (i.e., non bisogna cambiare spesso la batteria ai sensori).

2. Cosa si intende per Scatternet in una rete Bluetooth? Come viene gestita rispetto a una Piconet?

Solution: Una rete composta da un singolo master e diversi slave è definita Piconet. Se uno o più dispositivi appartengono a più piconet contemporaneamente si crea una Scatternet.

Le due (o più) piconet rimangono completamente indipendenti, clock, sequenza di hopping e slot di tempo completamente differenti, sta al dispositivo collegato a entrambe gestire la complessità aggiuntiva che questo porta.

Sui 79 canali che Bluetooth usa per fare frequency hopping potrebbe capitare una sovrapposizione all'interno della scatternet, per evitare interferenze si usa CDMA (il master fornisce un codice ortogonale a ogni dispositivo).

3. Descrivere il funzionamento della modalità di accesso al canale Slotted CSMA/CA utilizzata dal livello MAC dello standard 802.15.4 (usato da ZigBee e Thread).

Solution: La modalità CSMA/CA si fonda sull'invio di beacon da parte del coordinatore, usati per sincronizzare i dispositivi e organizzare i periodi di trasmissione. All'interno del superframe (divisione, logica, del tempo di trasmissione data dal coordinatore) sono presenti slot con diverso tipo di accesso:

- Contention Access Period CAP: accesso al canale a contesa, usando CSMA/CA
- Contention Free Period CFP: intervallo di tempo per le comunicazioni con banda riservata

Nella modalità a contesa, un dispositivo, prima di trasmettere, verifica che il canale sia libero.

Per verificare la condizione del canale:

- Viene deciso un valore casuale di backoff $[0, 2^{BE} - 1]$, dove il Backoff Exponent BE è un parametro, e aspetta tale numero di slot (ognuno dura 20 simboli)
- Dopo l'attesa del numero casuale di slot vengono fatti un numero CW (Contention Window, parametro) di CCA ravvicinati tra loro
- Se il canale è risultato libero in tutti i CCA il dispositivo comincia a trasmettere
- Se il canale è occupato, vengono incrementati di 1 BE e NB (Numero di Backoff, inizialmente 0), prima di ritentare; dopo 4 tentativi il livello MAC dichiara transmission failure

In qualsiasi caso, la trasmissione deve terminare nel numero di slot dedicati al CAP. Se il numero di slot non è sufficiente per la trasmissione viene rimandata al superframe dopo; similmente, se il conteggio durante il random backoff eccede il numero di slot, riprende al superframe successivo.

4. In Bluetooth, la comunicazione all'interno della piconet utilizza FHSS, TDD e TDMA. Descrivere, usando uno schema temporale, come vengono utilizzate queste tre tecniche per la comunicazione tra master e slave all'interno di una Piconet Bluetooth.

Solution: In Bluetooth la comunicazione è divisa in slot da $625\mu s$ e le tecniche utilizzate portano a:

- Time Division Duplex TDD: la comunicazione alterna master e slave, negli slot pari comunica il master, in quelli dispari gli slave
- Time Division Multiple Access TDMA: ogni slot dedicato agli slave viene indirizzato a uno slave specifico
- Frequency Hopping Spread Spectrum FHSS: la banda viene divisa in 79 canali (40 per BLE) e la frequenza da utilizzare per ogni messaggio è determinata dal numero dello slot di tempo e da una sequenza pseudo-casuale condivisa

dal master. Viene generata una sequenza casuale di frequenze e allo slot di tempo n viene usata la n -esima frequenza. I messaggi possono durare 1, 3 o 5 slot, ma la frequenza utilizzata per un singolo messaggio non cambia durante la trasmissione

5. Descrivere, utilizzando un diagramma di sequenza, la procedura di Inquiry e Paging di Bluetooth. Si assuma che sia il dispositivo master e che il dispositivo slave siano nello stato iniziale di standby. Indicare inoltre in quale momento il dispositivo slave viene a conoscenza della specifica sequenza di frequency hopping del master.

Solution: In inquiry mode, il master invia periodicamente uno IAC packet su 32 canali standard. Gli slave ascoltano periodicamente su una delle 32 frequenze di wake up. Una volta che lo slave riesce a sentire una trasmissione del master:

- Conoscendo il clock del master, fa un random backoff per poi rispondere con il proprio device address e classe
- Il master risponde con il Device Address Code DAC, sequenza per il frequency hopping e l'Active Member Address AMA
- Lo slave risponde con DAC e ack

La fase di inquiry permette di individuare i dispositivi, il paging serve a stabilire definitivamente la connessione, si ha uno scambio di pacchetti per la sincronizzazione per poi passare alla piconet, usando tutti i 79 canali e la sequenza di hopping completa.

3 WiFi

1. Descrivere lo schema di accesso del protocollo 802.11 (Wi-Fi) CSMA/CA. Discutere, inoltre, che “accorgimento” viene aggiunto al meccanismo di backoff per evitare che una stazione attenda un tempo indefinito per accedere al canale.

Solution: Il sistema Carrier Sense Multiple Access/Collision Avoidance CSMA/CA richiede di aspettare “del tempo” prima di poter trasmettere. Definizioni delle unità di tempo:

- Slot time: unità base di tempo, dipende dal trasmettitore fisico usato
- SIFS: intervallo più breve, usato per messaggi ad alta priorità
- DIFS: intervallo più lungo, usato per messaggi a bassa priorità, pari a SIFS+2 slot time
- PIFS: intervallo di tempo intermedio, usato per servizi time-bounded, SIFS+slot time

Per trasmettere, un dispositivo:

- Verifica che il canale sia libero tramite un Clear Channel Assessment CCA
- Ascolta per tempo DIFS il canale
- fa un altro CCA

Se il canale è risultato libero entrambe le volte, può cominciare a comunicare.

Se il canale è occupato: il dispositivo aspetta il termine dell'altra trasmissione, per poi attendere tempo DIFS più un numero random di slot time (random backoff). Viene fatto carrier sense durante tutto il periodo di backoff, se il canale risulta libero può cominciare a trasmettere.

Se durante il periodo di contesa il canale torna occupato, al turno successivo il dispositivo riprende il conteggio degli slot dal valore a cui era arrivato.

Se necessario ack, il dispositivo attende tempo SIFS per riceverlo al termine della sua trasmissione, prima di presupporre che il frame sia stato corrotto e ritrasmettere.

2. Descrivere, con un esempio, il problema del terminale nascosto in una rete Wi-Fi che adotta il protocollo CSMA/CA per l'accesso al canale radio condiviso. Quali modifiche vengono introdotte al protocollo CSMA/CA per risolvere questo problema?

Solution: Se due terminali A e B, fuori dal rispettivo raggio di copertura, volessero trasmettere a B, vedrebbero il canale libero contemporaneamente, in quanto il meccanismo di carrier sense funziona solo se l'altro dispositivo che comincia a trasmettere può essere rilevato.

Per risolvere il problema, il sender, dopo aver fatto carrier sense, invia una Request to Send RTS, contenente origine, destinazione e durata stimata della comunicazione da inviare, in questo modo tutti i terminali che ricevono la RTS senza esserne destinatari possono allocare un Network Allocation Vector NAV per la durata della comunicazione, in cui sanno che il canale verso la destinazione indicata sarà occupato.

Il destinatario del messaggio risponde con un messaggio di Clear to Send CTS, anch'esso contenente origine, destinazione e durata stimata (rimanente) del messaggio. In questo modo anche i terminali all'interno del raggio di copertura del destinatario possono allocare un NAV per la durata della comunicazione.

4 AODV

1. In quali casi un nodo intermedio (non destinazione) che utilizza il protocollo AODV può rispondere con RREP alla ricezione di una RREQ? Che cosa deve fare il nodo se nel messaggio RREQ il flag Gratuitous è impostato a 1 (Assumendo che possa rispondere)?

Solution: Un nodo intermedio può rispondere a una RREQ nel caso in cui

- Possiede un percorso valido verso la destinazione
- La flag D è a 0
- Il SN della entry per il percorso non è minore del SN presente all'interno della RREQ

Per rispondere imposta hop count e lifetime pari a quelli presenti nella entry, invia la RREP sul percorso reverse in unicast, drop della RREQ. Se la flag G è alzata, invia una RREP anche verso la destinazione della RREQ originale, per indicare il percorso verso l'origine, quindi con hop count, lifetime, SN pari a quelli presenti nella RREQ, la destinazione è l'origine della RREQ e viceversa. In questo modo “simula” una richiesta di RREQ da parte della destinazione verso il nodo originale, in modo da completare il percorso tra i due.

2. Si consideri il caso in cui un nodo “X”, che utilizza AODV, riceva una RREQ dal nodo “Z”, descrivibile come

RREQ Ricevuta da Z			
Destination	C	Destination_Only	0
Destination SN	100	Gratuitous	1
Originator	A	Hop count	4
Originator SN	200		

e in quel momento la sua tabella di routing contenga

Routing table X			
DST	NEXT	HOP	DST SN
C	G	2	120
G	G	1	99
Z	Z	1	200

Indicare

- il tipo e i campi del/dei messaggio/i che invia il nodo X (quello che riceve la RREQ)

- come cambia la tabella di routing del nodo X

Solution: Dato che

- Il nodo X possiede un percorso per la destinazione della RREQ C
- Il SN del percorso è \geq del SN indicato nella RREQ
- Il flag Destination_only è a zero

il nodo X può rispondere alla RREQ, con una RREP contenente:

- SN = 120, pari a quello della entry
- Hop count = 2, come nella entry
- Lifetime pari a quello della entry

Dato che il flag Gratuitous è alzato, invierà un'altra RREP verso la destinazione della RREQ, ovvero C, con

- Hop count = 4, come nella RREQ
- Destinazione = A, l'originator della RREQ
- SN della destinazione = 200, come nella RREQ
- Origine = C
- Lifetime pari alla entry verso l'origine della RREQ

“Simula” una RREQ da C verso A.

Il nodo X aggiunge alla sua tabella di routing il percorso verso l'originator della richiesta A, con hop count 4 e next hop Z.

5 4G LTE

1. Descrivere il funzionamento del protocollo GTP (GPRS Tunneling Protocol) utilizzato nella rete mobile. Inoltre, discutere le motivazioni che hanno portato all'introduzione di questo protocollo e quali problemi risolve.

Solution: Il protocollo GTP è stato introdotto per gestire in modo efficiente la mobilità dei dispositivi. Lo User Equipment UE è libero di muoversi all'interno della rete, potenzialmente cambiando il punto di accesso alla rete (eNodeB e S-GW), cambiare le tabelle di routing di conseguenza sarebbe troppo dispendioso.

L'indirizzo IP del dispositivo dovrebbe rimanere unico per tutta la sessione, quindi GTP aggiunge ai pacchetti un header contenente un identificativo della sessione: Tunnel ID TEID.

In questo modo la sessione dello UE è identificata all'interno della rete operatore tramite il TEID, l'handover, anche a livello di S-GW, può essere gestito in maniera trasparente all'utente e alla rete esterna, il nodo di destinazione deve solo aggiornare le associazioni del TEID.

2. Descrivere i 3 principali approcci di riutilizzo delle bande di frequenza nelle reti cellulari per ridurre l'interferenza tra celle adiacenti.

Solution: I 3 approcci principali per il riutilizzo delle frequenze sono:

- La più intuitiva è usare frequenze diverse per celle adiacenti, la gestione è semplice ma viene sprecata molta banda in quanto effettivamente ne viene usata solo una porzione per volta
- Per non consumare più banda, una soluzione è usare tecniche di codifica per evitare interferenze tra celle vicine, come ad esempio CDMA (ogni utente ha il suo codice univoco, le trasmissioni sono distinguibili grazie a quello)
- L'ultima soluzione è utilizzare l'intera banda disponibile al centro della cella e ai bordi usare frequenze diverse per celle adiacenti; porta a un migliore uso della banda ma richiede un coordinamento più sofisticato tra le BS, oltre che riuscire a posizionare in maniera abbastanza precisa i dispositivi all'interno della cella

3. Che vantaggi porta il protocollo SCTP rispetto a TCP all'interno del control-plane di 4G LTE?

Solution: SCTP ha diversi vantaggi all'interno per l'utilizzo all'interno del control-plane 4G, tra cui

- Ammette ordinamento parziale: in TCP, se un segmento viene perso, tutti quelli successivi non vengono inviati ai livelli superiori, ma in 4G si ha la necessità di inviare dati relativi a tante connessioni indipendenti, quindi si aggiunge a ogni pacchetto uno Stream ID e la perdita di un pacchetto è bloccante solo rispetto ad altri pacchetti con lo stesso Stream ID
- SCTP è message oriented, al contrario di TCP che è stream oriented e richiede di inserire marcatori per delimitare i singoli messaggi
- SCTP permette il multi-homing: sorgente e destinazione della connessione non devono obbligatoriamente essere indirizzi singoli, possono essere multipli

4. In LTE 4G esistono due tipologie di handover: Seamless e Lossless. Come funzionano e in quali casi vengono usati.

Solution: In 4G LTE esiste solo hard handover (il dispositivo non è mai collegato a più BS contemporaneamente), ma gli handover si possono distinguere in due classi:

- Seamless handover: latenza minore, ha come obiettivo far percepire il meno possibile l'handover, anche a costo di un (breve) buco nella connessione; viene usato per applicazioni real time, ad esempio traffico VoIP
- Lossless handover: maggiore latenza, ma ha come obiettivo non perdere nessun pacchetto; viene usato quando la ritrasmissione sarebbe troppo lenta, come ad esempio per traffico HTTP/FTP. Per evitare di perdere pacchetti in downlink, il flusso in download continuerà a mandare pacchetti alla vecchia BS, che li inoltrerà tramite interfaccia X2 alla BS di destinazione, la quale farà il buffer dei dati fino al termine dell'handover

6 5G

1. Domanda

Solution: Risposta

7 Comunicazione satellitare

1. Domanda

Solution: Risposta