Domande Reti Wireless e Mobili

Massimo Perego

Indice

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:

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

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

4. Cosa definisce il teorema di Shannon è perché è importante nella trasmissione di informazioni su canale radio.

Solution: Il teorema di Shannon definisce la capacità di un canale, tenendo conto dell'ampiezza di banda e del rumore presente sul canale (definito tramite Signal to Noise ratio).

La formula per la capacità del canale è:

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

Importante in quanto permette di stabilire il limite teorico superiore di informazioni inviabili su un certo canale in un determinato istante, massimizzando l'efficienza spettrale.

5. Supponendo di avere uno spettro tra 2 e $4MHz$ e un $SNR_{dB} = 20dB$, quanti livelli di segnale servono per raggiungere la capacità teorica, tenendo in considerazione il rumore?

Solution: La banda a disposizione è

$$B = 4 - 2MHz = 2MHz$$

Il valore del SNR in dB vuol dire che

$$SNR_{dB} = 10 \log_{10}(SNR) \implies SNR = 10^{20/10} = 100$$

il segnale è circa 100 volte superiore al rumore.

La capacità secondo Shannon dice che

$$C = B \cdot \log_2(1 + SNR) = 2 \cdot 10^6 \cdot \log_2(101) \approx 13.32Mbps$$

Possiamo quindi ricavare il numero di canali sapendo che

$$C = 2B \log_2 M \implies M = 2^{C/2B} = 10$$

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.

6. Descrivere le funzioni svolte dal Link Layer di BLE negli stati Advertising e Scanning, spiegando anche perché non è prevista una transizione di stato da Scanning a Connection.

Solution: Il Link Layer in BLE si occupa della trasmissione e ricezione dei pacchetti radio, anche sui canali di advertising.

Nello stato di Advertising, uno slave si annuncia periodicamente, usando i canali di advertising. Se un master vuole raccogliere informazioni riguardanti i dispositivi vicini entra nello stato Scanning, in cui ascolta i pacchetti inviati sui canali di advertising.

Non è prevista una transizione da Scanning a Connection in quanto lo stato di Scanning è solo per la raccolta dati, una volta che il master vuole collegarsi a un dispositivo entra nello stato Initiator.

7. Spiegare come vengono gestiti più dispositivi Slave all'interno di una piconet Bluetooth. In particolare, descrivere come vengono gestiti duplex e multiple access?

Solution: All'interno di una piconet Bluetooth, più dispositivi slave vengono gestiti tramite i meccanismi di:

- Time Division Duplex TDD: il master trasmette e i dispositivi ascoltano negli slot pari, viceversa negli slot dispari
- Time Division Multiple Access TDMA: il master decide, per ogni slot dedicato agli slave, quale di questi può comunicare

8. Che tipi di servizi supporta la baseband Bluetooth?

Solution: La baseband Blouetooth supporta due tipi di servizio:

- Synchronous Connection Oriented Link SCO: connessione punto-punto con garanzie su bitrate minimo e delay, un canale riservato per casistiche real time; al massimo 3 in contemporanea
- Asynchronous Connectionless Link ACL: traffico best effort, occupa tutti gli slot rimanenti; permette qualità maggiore, ma senza garanzie

9. Descrivere lo schema di error control adottato da Bluetooth.

Solution: All'interno dei pacchetti Bluetooth sono presenti solo 2 bit usati per il controllo degli errori, ARQN e SEQN, rispettivamente un ack/nack e numero di sequenza per il pacchetto.

In una trasmissione tipica:

- Il master invia un pacchetto con SEQN s
- Lo slave risponde con ack e SEQN s
- Nello slot successivo si ripete, con SEQN $\neg s$

I possibili errori sono:

- Lo slave non riceve il pacchetto: risponde con un nack e SEQN s, il master sa che deve ritrasmettere grazie al nack
- Il master non riceve l'ack: in caso di ack perso il master ritrasmette sempre, lo slave si accorge della ritrasmissione in quanto il SEQN è pari a quello precedente

10. Cos'è un superframe in ZigBee? Come viene definito e come è composto.

Solution: A livello MAC si possono avere due modalità di trasferimento dati, sempre con CSMA/CA, ma possono essere slotted o unslotted.

La modalità slotted utilizza i beacon: pacchetti di controllo, inviati dal coordinatore, contenenti informazioni per sincronizzare gli altri dispositivi, organizzare i periodi di trasmissione e gestire le trasmissioni di frame ancora pendenti.

L'organizzazione logica del tempo di comunicazione è detta "superframe", questa viene definita dal coordinatore e condivisa agli altri dispositivi attraverso i beacon.

Il superframe viene diviso in slot con diverso tipo di accesso:

- Contention Free Period CFP: periodo senza contesa, in cui il coordinatore garantisce la possibilità di comunicare ad alcuni dispositivi che lo necessitano
- Contention Access Period CAP: periodo a contesa, l'accesso al canale viene fatto usando CSMA/CA

11. Spiegare la procedura di accesso al canale tramite CSMA/CA in ZigBee.

Solution: Nel periodo di trasmissione slotted CAP, l'accesso al canale viene regolato tramite CSMA/CA, quindi, per poter trasmettere, un dispositivo:

- Aspetta un numero di slot di tempo random, nell'intervallo $[0, 2^{BE}]$, dove il Backoff Exponent BE è un parametro
- Effettua un numero CW di Clear Channel Assessment CCA ravvicinati, dove il valore di Contention Window CW è un parametro
- Se il canale è risultato libero durante tutti i CCA può cominciare a trasmettere
- Se il canale è risultato occupato, aumenta il valore di BE e NB (Numero di Backoff, inizialmente 0) prima di riprovare

Se il conteggio degli slot durante la contesa viene interrotto da una trasmissione o dalla fine del periodo CAP, riprende dal valore a cui era arrivato all'occasione successiva, per evitare possibili attese infinite.

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, contenete 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.

3. Data una rete WiFi che opera in moodalità DCF, descrivere la politica di backoff usata da una stazione che perde la contesa per l'accesso al canale.

Solution: Per ottenere l'accesso al canale in CSMA/CA una stazione deve effettuare due Clear Channel Assessment CCA a distanza DIFS.

Se durante uno di questi il canale è occupato, il dispositivo aspetta fino al termine della trasmissione in corso (facendo carrier sense), per poi aspettare tempo DIFS/PIFS/SIFS (in base alla priorità) e un numero di slot random (periodo di contesa). Se il canale è ancora libero dopo il periodo di contesa allora può cominciare a trasmettere.

Se il canale torna occupato durante il periodo di contesa, il conteggio viene interrotto e ripreso al termine della trasmissione successiva (non riparte per evitare che una stazione aspetti indefinitivamente).

4. Spiegare il processo di Downlink e Uplink tramite OFDMA in WiFi 6.

Solution: In WiFi 6 viene introdotto Orthogonal Frequency Division Multiple Access OFDMA per la suddivisone della banda tra più utenti.

In downlink, l'Access Point conosce la lista di destinatari e deve comunicare l'assegnamento delle risorse ai vari dispositivi, invia dunque una Multi-User Request to Send MU-RTS, per notificare ai dispositivi interessati l'assegnamento delle risorse e l'intento di comunicare.

Dopo la MU-RTS, i dispositivi rispondono con una Clear to Send CTS, di seguito l'AP è libero di inviare in parallelo i dati a tutti i dispositivi.

Se necessario, l'AP invia anche un Block Acknowledgment Request BAR e i dispositivi rispondono con un Block ack.

Per l'uplink è necessario sincronizzare tutti i dispositivi, quindi:

- L'AP invia un Buffer Status Report Poll BSRP, a cui i dispositivi rispondono con un Buffer Status Report BSR, usato per comunicare chi ha da trasmettere qualcosa
- L'AP invia la MU-RTS contenente l'allocazione delle risorse, i dispositivi rispondono con CTS
- Dopo un ulteriore trigger di sincronizzazione da parte dell'AP i dispositivi possono cominciare a trasmettere (padding se la trasmissione è troppo corta)
- Se necessario, l'AP invia un Multi-Station Block ack

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.

3. Qual è la principale funzione del Sequence Number SN nel protocollo AODV? Quali nodi possono modificare il valore del SN?

Solution: La funzione principale del Squence Number SN nel protocollo Ad Hoc Distance Vector AODV è quello di contatore monotono crescente, usato per determinare la freschezza dell'informazione riguardante un nodo. Se più alto, l'informazione è più recente.

Il SN di un nodo può essere modificato solo dal nodo stesso, in particolare viene incrementato di uno quando genera una RREQ o risponde a una RREQ destinata al nodo stesso.

4. In AODV, un nodo Originator O riceve RREP in tempi diversi e da cammini diversi per la stessa RREQ. In base a quali parametri di RREP il nodo O sceglie il cammino migliore?

Solution: Un nodo Originator che ha inviato una RREQ, riceve più RREP in tempi diversi, i parametri per determinare il cammino migliore sono:

- Numero di hop: all'interno della richiesta viene segnato il numero di inoltri effettuati, un percorso più breve è (solitamente) migliore
- Sequence Number SN: il SN codifica la freschezza dell'informazione, un SN più alto significa avere informazioni più recenti

Prima viene guardato il SN, poi l'hop count, il presupposto di AODV è che la rete sia dinamica, quindi un'informazione più recente è migliore. Nel caso entrambi i valori sono pari potrebbe essere guardato il lifetime rimanente.

5. Descrivere le attività svolte da un nodo AODV quando riceve una RREQ.

Solution: Quando un nodo riceve una RREQ:

- Controlla se l'ID di richiesta e IP di origine sono già noti: se già visti, ignora la richiesta
- Aggiorna il percorso verso l'originator, se il SN dell'origine è maggiore della eventuale entry già presente
- Se non può rispondere, inoltra il messaggio ai vicini, incrementando l'hop count
- Se il flag destination only è a 0, e il nodo possiede una entry valida verso la destinazione con SN maggiore di quello all'interno della richiesta, allora può rispondere con una RREP
- Se ha risposto e il flag Gratuitous è alzato, invia una RREP anche al nodo destinazione della RREQ

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

5. Dato il seguente sequence diagram della procedura di handover:
    1. Quale interfaccia di comunicazione viene utilizzata?
    2. In quali casi è possibile?
    3. Descrivere i vari passi della procedura a partire dal punto 4 (la decisione di effettuare l'handover è stata presa)

Solution: L'interfaccia di comunicazione utilizzata è l'interfaccia X2,un canale di comunicazione diretto tra eNodeB.

Questo tipo di handover è possibile solo nel caso il trasferimento sia effettuato tra celle appartenenti allo stesso MMU, i.e., cambia il bearer radio ma non il bearer S1.

Dopo che è stata presa la decisione di handover:

- La source eNodeB manda una richiesta di handover all'eNodeB di destinazione
- La eNodeB di destinazione alloca le risorse prima di rispondere con un ack alla richiesta
- Una volta che le risorse sono state allocate viene mandato il comando di handover dalla source eNodeB allo UE
- Viene trasferito lo stato della sessione in esecuzione sullo UE alla eNodeB di destinazione (per garantire continuità di servizio)
- Nel caso di lossless handover si ha una comunicazione su interfaccia X2 per trasferire i dati ricevuti in downlink dalla eNodeB sorgente durante il trasferimento
- Una volta che il trasferimento è completato, lo UE invia un messaggio di handover completato alla target eNodeB
- La target eNodeB invia una path switch request all'MME, ovvero una richiesta per cambiare l'indirizzamento dei dati relativi allo UE che è stato spostato; unica comunicazione con il CN, chiede di spostare il path dei dati
- L'MME risponde con un path switch ack
- Una volta terminato tutto, la target eNodeB invia un messaggio alla source eNodeB per rilasciare le risorse

6. Descrivere le funzionalità dei moduli principali (MME, SGW, PGW) in una rete LTE.

Solution: I moduli principali in una rete LTE sono:

- Mobility Management Entity MME: si occupa di tutto il traffico di controllo e segnalazione all'interno della rete (tutto ciò che non è dati utente), come ad esempio gestione della mobilita, della tracking area, del paging, …
- Serving Gateway SGW: il nodo all'interno della CN che si occupa del traffico user; il punto di gestione per tutti i dati utente, con assegnato un gruppo di eNodeB

- Packet Data Network Gateway PDW: il punto di accesso tra rete LTE e le reti esterne, si occupa di cose come l'assegnamento dell'IP allo UE, garantisce le policy autorizzate per un certo utente, filtra i pacchetti per garantire QoS usando bearer diversi

7. Quali sono le tre caratteristiche in base a cui può essere deciso un handover?

Solution: Il parametro principale secondo cui viene deciso se fare handover o meno è la potenza di trasmissione:

- Si può guardare solo la potenza relativa: quando la potenza di una BS è minore di un'altra si cambia; questo può portare a un continuo cambio (inutile) sui bordi delle celle e a un "rimbalzo" tra diverse BS
- Si può guardare anche una soglia di segnale: se il segnale è sufficiente, ancora "abbastanza buono", non viene fatto l'handover; il problema è definire queste soglie
- Aggiungere isteresi: l'handover viene fatto se la potenza relativa è maggiore e il segnale sotto una certa soglia, ma per effettuare il cambio la differenza di potenza deve essere significativa

Per determinare l'handover si combinano queste tre idee.

8. Come può essere gestito il duplex in 4G LTE? Cosa si intende per Uplink Timing Advance?

Solution: All'interno di LTE, il duplex può essere:

- Frequency Division Duplex FDD: vengono assegnate frequenze diverse per uplink e downlink
- Time Division Duplex TDD: una sola frequenza, ma vengono assegnati slot di tempo ciclici diversi per uplink e downlink; la percentuale di tempo dedicato a ogni fase è configurabile in base alla necessità

In TDD, dopo il downlink si ha un periodo di guardia per tenere conto dell'Uplink Timing Advance: un anticipo della trasmissione durante il periodo di uplink dei dispositivi, dovuto al tempo fisicamente necessario per far arrivare la trasmissione all'AP; la trasmissione si può anticipare solo se il canale è libero, quindi si ha una guardia.

9. Spiega le fasi dell'handover S1.

Solution: Quando l'handover richiede di cambiare sia BS che MME bisogna cambiare il bearer S1. La procedura è:

- La eNodeB sorgente notifica la richiesta di handover al suo MME
- L'MME sorgente manda una Forward Relocation Request all'MME destinazione
- L'MME destinazione comunica la richiesta di handover alla eNodeB destinazione, la quale prepara le risorse necessarie
- Dopo il setup delle risorse, l'eNodeB destinazione risponde al suo MME con un handover request ack
- L'MME destinazione risponde alla relocation request dell'MME sorgente
- L'MME sorgente invia alla sua eNodeB il comando di handover, inoltrato poi allo UE
- Viene fatto il trasferimento di stato per mantenere la sessione dello UE tra le eNodeB
- Se lossless handover si ha una comunicazione su canale X2 per l'inoltro dei pacchetti
- Lo UE invia la conferma di avvenuto handover
- La eNodeB di destinazione notifica l'avvenuto handover al suo MME
- I due MME si scambiano forward relocation complete e il relativo ack
- Lo UE invia all'MME l'update della tracking area
- Il vecchio MME indica alla eNodeB source di rilasciare le risorse

6 5G

1. Spiegare il concetto di Software Defined Networking SDN.

Solution: Una normale applicazione di rete contiene un singolo layer per flussi di controllo e dati, entrambi gestiti da tutti i dispositivi della rete.

Con SDN si astrae la parte di controllo, centralizzata in un SDN controller: il layer di controllo viene implementato a livello software in maniera centralizzata, al di sopra del data layer.

Questo rende il control plane programmabile in maniera software, risultando in maggiore flessibilità della rete, semplificazione nella gestione e si presenta la possibilità di configurare i meccanismi di controllo in base alle condizioni della rete.

Allo stesso tempo, gli SDN Controller diventano un single point of failure per la rete, con le relative problematiche di sicurezza (controllare il controller vuol dire controllare la rete), inoltre la possibilità di adattare le regole real-time porta una complessità aggiuntiva alla gestione.

Si vuole andare verso un'architettura con anche data plane programmabile, implementato a livello software e adattabile secondo le condizioni della rete.

2. Spiegare il concetto di Network Function Virtualization NFV, funzionamento, architettura e implementazione per la rete mobile.

Solution: Con la NFV, le componenti passano da necessitare hardware dedicato a essere implementazioni software, installabile su hardware standard; si separano le funzionalità hardware e software.

Per capire cosa deve implementare un determinato servizio si ha una Service Function Chain SFC: catena delle funzionalità necessarie per una determinata applicazione.

L'architettura si divide in:

- NFV Infrastructure, contenente le risorse virtualizzate, sulla base della quale vengono montate le Virtual Network Function VNF, ognuna delle quali con il relativo Element Management System EMS per tenere traccia dello stato di funzionamento
- NFV Management and Orchestration MANO, parte "di controllo" interfacciata alla rete operatore, contiene
  - VNF Manager VNFM: gestisce le VNF istanziate
  - VNF Infrastructure Manager VIM: definisce le risorse disponibili

– NFV Orchestrator: coordina NFM e VIM, collegato alla rete operatore per ricevere e gestire le richieste all'interno della rete; contiene template per possibili funzionalità necessarie e vengono istanziate secondo la SFC

La NFV permette di avere maggiore flessibilità e scalabilità della rete, proprietà intrinseche alla virtualizzazione, ottimizzando l'uso delle risorse e facilitando modifiche ai servizi (l'hardware rimane sempre uguale, basta modificare il software).

Di contro, le prestazioni dell'hardware devono essere adeguate allo scopo, anche considerando l'overhead di virtualizzazione, la gestione delle risorse può essere complicata, l'introduzione di software porta possibili problemi di sicurezza e bisogna pensare alla fase di transizione tra funzionalità hardware e software, le due devono poter coesistere.

L'architettura di una eNodeB è composta da Remote Radio Head RRH e Baseband Unit BBU che si occupano, rispettivamente, della parte radio e di gestire la comunicazione secondo il protocollo usato.

Per facilitare la densificazione della rete, vengono separate le due parti, si aggiungono solo RRH dove serve segnale, la BBU diventa una Virtual BBU vBBU, posizionata in remoto, con tutte le tecnologie necessarie (anche multi-tenant).

Questo permette di virtualizzare e ottimizzare la gestione della parte di controllo delle BS, migliorando le prestazioni e permettendo una densificazione delle celle in maniera più sostenibile (installare solo RRH è più facile).

3. Cosa sono e a cosa servono le Network slices in 5G?

Solution: Il concetto di "Network slicing" modifica il paradigma della rete da statico a dinamico, reti logiche vengono create on demand, secondo il caso d'uso e lo scopo richiesto. Viene costruito un overlay di rete ad hoc per ogni servizio, rendendo più flessibile la gestione della rete.

Le Network Slices 5G permettono di classificare diversi casi d'uso e per ognuno di questi vengono stabilite le caratteristiche del servizio e la composizione delle network function per tali caratteristiche. Vengono "confezionate" diverse strutture di reti logiche per diversi possibili casi d'uso.

Per identificare una slice si usa uno slice identifier a 32 bit:

- I primi 8 identificano il tipo di slice ("caso d'uso", la categoria)
- I rimanenti identificano la specifica istanza

Lo slice identifier viene poi inserito all'interno dei pacchetti.

4. In cosa consiste e a cosa serve lo standard 5G New Radio NR.

Solution: Per ridurre la latenza, una possibile soluzione è ridurre la durata dei simboli. Lo standard 5G NR definisce quindi 5 diverse durate, chiamate numerology, e due possibili intervalli di frequenza.

Per una numerology μ si ha una distanza tra le frequenze in OFDMA Δf

$$\Delta f = 2^{\mu} \cdot 15kHz$$

Aumenta la distanza tra le portanti, raddoppiare la banda permette di dimezzare la durata dei simboli.

All'interno dello scheduling si possono allocare resource block con numerology diverse, permettendo latenze diverse per utenti differenti, magari anche in base alla network slice utilizzata.

7 Comunicazione satellitare

1. Quali sono le possibili orbite satellitari? Quali sono vantaggi e svantaggi di ognuna?

Solution: Le tre principali orbite satellitari sono:

- Geostationary Earth Orbit: A circa 35k km dalla superficie terreste, il periodo dell'orbita è circa 24h, apparendo quindi fisso rispetto alla superficie terreste
  - Vantaggi: ampia copertura, angolo di elevazione fisso, visibilità permanente, permette di usare antenne fisse sul terreno, semplificando la gestione
  - Svantaggi: alto delay, bassa qualità del segnale, elevata potenza richiesta per raggiungere il satellite
- Low Earth Orbit LEO: Periodo dell'orbita di 1.5/2h, con una visibilità di 15/20 minuti prima di oltrepassare l'orizzonte, l'orbita più bassa utilizzabile
  - Vantaggi: basso delay, bassa potenza di trasmissione richiesta, miglior utilizzo dello spettro e qualità del segnale
  - Svantaggi: copertura limitata, gestione complessa per tracciamento e handover, richiedono costellazioni numerose per una copertura significativa
- Medium Earth Orbit MEO: A metà delle orbite precedenti, periodo dell'orbita di 5-10h, 2-8h di visibilità per passaggio
  - Vantaggi: significativamente minore delay e potenza richiesta rispetto a GEO, RTT nelle decine di ms; le caratteristiche sono "nel mezzo" e dipendono dall'altezza del satellite
  - Svantaggi: potenza e delay maggiori di LEO

  Usati da GNSS, per scaricare solamente dati non ci sono problemi.

2. Quali sono i 3 segmenti che compongono l'architettura per la comunicazione satellitare?

Solution: I 3 segmenti sono:

- Space segment: i satelliti e le relative costellazioni, si possono avere anche link inter-satellitari (radio o anche ottici)
- Ground segment: la parte di stazioni a terra che permettono il controllo del sistema, include gateway e tutto ciò che connette i satelliti al terreno, inclusi telemetria e tracking

- User segment: utilizzatori del servizio, possono essere mobili o fixed

3. Quali sono le possibili architetture e opzioni di integrazione per includere i satelliti nelle reti 5G/6G?

Solution: Le possibili architetture per includere i satelliti sono:

- Relay: il satellite funge da ripetitore per le comunicazioni, aumentando la qualità del canale
- Backhaul: raggiungere una zona tramite la rete di backhaul potrebbe essere complicato, quindi viene rimpiazzata dai satelliti
- Direct Access: l'utente può collegarsi direttamente al satellite ed è a conoscenza della presenza di quest'ultimo

Le possibili opzioni di integrazione sono:

- NTN Transparent Payload: il satellite rimpiazza il livello fisico, il gateway dialoga con le BS; soluzione più semplice da implementare
- NTN Regenerative Payload: il satellite implementa lo stack di una BS e ne svolge le funzionalità, il gateway è collegato alla core network
- NTN Regenerative Payload with functional split: il satellite svolge solo le funzioni del modulo distributed unit di una gNodeB, implementa solo una parte dello stack di una BS

Il satellite può quindi implementare: solo il livello fisico, tutta la BS, una parte della BS.