Tutte le domande
di
Reti e Sicurezza

Luca De Franceschi

Università degli studi di Padova

Indice

1 Capitolo Strato Fisico

1.1 Cosa si intende per serie di Fourier

Le informazioni possono essere trasmesse via cavo variando alcune proprietà fisiche, come la tensione e corrente. Fourier condusse alcuni studi ed arrivò alla conclusione che le informazioni trasmesse via cavo potevano essere rappresentate da una funzione $f(t)$. Questa funzione è composta da una serie infinita di somme di seni e coseni, ed è in grado di rappresentare un segnale periodico e regolare. La trasmissione però non è mai perfetta e c'è per forza attenuazione di linea. L'intervallo di frequenze trasmesse senza forte attenuazione è detto **banda passante**. Anche in un ipotetico canale perfetto, ovvero senza attenuazioni, la velocità di trasmissione non può essere troppo elevata; la massima velocità è data dall'equazione di Nyquist/Shannon:

$$V_{max} = \log_2 Vbit/sec$$

1.2 Bitrate e baudrate

Bitrate: Velocità di trasmissione si indica in bit/s. Il teorema di Nyquist mette in relazione il bitrate con la banda disponibile:

$$2H \log_2 V$$

Con H banda disponibile e V livelli di segnale (simboli) usati:

$$S/N = segnale/rumore,\ SNR = 10 \log_{10}(S/N)dB$$
$$Massimobitrate = 2 \log_2(1 + (S/N))$$

Baudrate: numero di imboli al secondo, un simbolo può valere più bit.

1.3 Descrivere i vari tipi di cavo e confrontarli

Principalmente esistono 3 tipi di cavo, il classico **doppino**, il **cavo coassiale** e la **fibra**.
Il doppino è composto da due conduttori di rame isolati, attorcigliati tra loro in modo elicoidale (DNA style), per evitare interferenze fra di loro. Il doppino è molto utile per la linea telefonica, dato che può percorrere molti km senza che il segnale si indebolisca, ovvero senza bisogno di un'amplificazione.
Il cavo coassiale è più grosso e può estendersi per distanze maggiori rispetto il doppino. La distanza maggiore è frutto di una maggior schermatura a cui è sottoposto il nucleo in rame del cavo che lo rende immune dal rumore.
Esistono due cavi coassiali, uno da 50 Ohm per le trasmissioni digitali e uno da 75 Ohm per quelle analogiche.
La fibra ottica è formata da 3 parti: sorgente luminosa, mezzo di trasmissione e rilevatore di luce. La sorgente di luce è rappresentata da LED oppure laser, anche se il secondo, oltre ad essere meno diffuso è anche più costoso. Il mezzo trasmissivo è la fibra, composta un nucleo di vetro di pochi micron, avvolta in una guaina di vetro rivestita a sua volta da una guaina di plastica. La luce che attraversa la fibra è riflessa al suo interno, da un'estremità all'altra del cavo. Nonostante si trasmetta alla velocità della luce, quest'ultima viene stroncata

dalla velocità di decodifica inferiore che avviene alle estremità. La fibra può contenere più raggi che si differenziano per l'angolo di riflessione. Questo tipo di fibra è detto multimodale. Se la trasmissione all'interno della fibra è unica, si ha una trasmissione in linea retta, detta monomodale.
Lo svantaggio della fibra rispetto al doppino e cavo coassiale è il costo maggiore e la difficoltà nell'unire vari pezzi di cavo, mentre per gli altri due tipi basta attorcigliare il nucleo di rame. Il vantaggio della fibra è la manutenzione, essendo vetro è pari a zero. Altro vantaggio è l'unione di più canali, che avviene tramite prismi.

1.4 Caratteristiche e confronto fra i vari tipi di satellite, GEO, MEO, LEO

Un satellite è un grande ripetitore di microonde posizionato in cielo. Ci sono tre tipi di satelliti che si differenziano per la loro distanza dalla superficie terrestre.
I satelliti più lontani sono detti **geostazionari** e sono posti in successione su un'orbita circolare al livello dell'equatore, ad una distanza minima di 2 gradi uno dall'altro(ps: immaginare tanti cerchi concentrici che hanno come primo cerchio il nostro equatore e tutti gli altri più grandi, i satelliti sono su uno di questi). Questi satelliti sono molto lontani dalla terra e per questo hanno un tempo medio di ritardo della trasmissione di 300 millisecondi, ma con uno di essi possiamo coprire quasi un terzo della superficie terrestre. I satelliti **LEO** distano circa 500 km dalla terra, hanno un tempo di latenza inferiore rispetto ai GEO, come il consumo energetico. Essendo vicini, per coprire tutta la terra, sono necessari molti satelliti. Si muovono velocemente. I satelliti **MEO** sono posti a un'orbita intermedia tra i LEO e GEO, hanno una velocità relativamente bassa, in quanto sono posti a 18 mila km dalla terra e il loro tempo di rivoluzione è di 6 ore.

1.5 Che cos'è la modulazione in frequenza (FM)? E in ampiezza(AM)?

La modulazione in frequenza è una delle tecniche di trasmissione utilizzate per inviare informazioni attraverso la variazione della frequenza dell'onda portante. La FM è una modulazione a onda continua, ovvero viene modulata la portante sinusoidale. Per riuscire a inviare dati in forma digitale è necessario un ampio spettro di frequenza, questo rende adatta la trasmissione in banda base solo a basse velocità e a distanze brevi. Nella modulazione a frequenza vengono utilizzate 2 o più frequenze.
Pro:

- Molto meno sensibile ai disturbi rispetto all'AM;
- Permette una trasmissione di miglior qualità;
- Efficienza energetica molto maggiore, cioè il segnale di informazione non richiede potenza aggiuntiva per essere trasmesso.
-

Contro:

- Necessità di circuiti molto più complessi;
- Occupa più banda;
-

Modulazione in ampiezza (AM): due diverse ampiezze sono usate per rappresentare 0 e 1. Utilizza per il segnale un segnale a radio frequenza come portante. L'AM modifica il segnale in modo proporzionale.
Pro:

- Semplice da mettere in pratica.

Contro:

- Molto sensibile a disturbi.

1.6 Che cos'è la modulazione delta (delta modulation)?

Questa tecnica è una differente tecnica di multiplexing (più conversazioni nello stesso mezzo fisico) a divisione di tempo. Ogni valore campionato differisce dal precedente di +1 o -1 sotto le condizioni che può essere trasmesso un singolo bit che dice se il nuovo campione è maggiore o minore del precedente.

1.7 Descrivere in dettaglio il GSM (Global System for Mobile connection)

Il GSM è una tecnologia simile al D-AMPS, appartenente alla seconda generazione di cellullari con qualche modifica. La prima sostanziale è il numero di canali, infatti il GSM ha 124 coppie di canali simplex ampi 200KH e supporta fino ad 8 connessioni contemporanee grazie al multiplexing a divisione di tempo. La trasmissione e la ricezione non avvengono nello stesso intervallo, poiché il sistema non è in grado di gestirlo. Il GSM è il protocollo che ha introdotto le SIM, le quali contengono IMSI e la chiave crittografia KI, diversa per ogni SIM. Il cellulare manda IMSI e KI in broadcast. L'operatore riceve entrambi e invia un numero casuale, che viene analizzato e rimandato con la firma del KI all'operatore.
La struttura a cella GSM: nel protocollo GSM ci sono 4 tipi di celle: macro, micro, pico e Umbrella. Le prime sono le più grandi, sono sopraelevate rispetto gli edifici e hanno un raggio massimo di 35 km. Le micro sono più piccole, coprono un'altezza pari agli edifici. Le pico sono molto piccole, usate in aree molto dense, tipicamente indoor. Umbrella è una piccola estensione, usata per coprire i buchi tra le varie celle sopracitate.

1.8 Si descriva la tecnica CDMA (Code Division Multiple Access), possibilmente con esempio

CDMA permette la trasmissione per tutto il tempo attraverso l'intero spettro. Queste trasmissioni multiple e simultanee vengono separate tramite tecnica di codifica. L'idea è che i segnali si sommino linearmente, ma ogni coppia lo fa in

lingua diversa. Per risalire a ciò che viene detto, basta togliere il rumore aggiunto dalle altre conversazioni utilizzando le matrici di Walsh. Vediamo un esempio.
Creando una matrice di Hadamard 4x4 posso gestire 4 lingue, invertendo ogni riga ottengo altre 4 parole, in modo da avere una coppia di parole per ogni lingua. Ognuno usa una parola, si sommano le coordinate di ogni parola ottenendo un unico vettore risultante che moltiplicato per una parola di una determinata lingua, fornisce un numero:

- **Zero**: se il dispositivo non ha trasmesso;
- **Positivo**: c'è una parola in quella lingua e la parola è la parola positiva;
- **Negativo**: c'è una parola in quella lingua e la parola è la parola negativa;

Es: Si costruisca una base trasmissiva (chip codes) per 18 stazioni in CDMA (volendo, usando le matrici di Hadamard). Basta fare la matrice di hadamard 32x32 e prendere solo 18 righe Il chip codes è una riga della matrice (di Hadamard) che viene assegnata alla singola stazione che trasmette quello per mandare un 1 o il complemento a 1 ($riga * -1$) per mandare uno 0. Ogni riga definisce una "lingua" diversa che è linearmente indipendente dalle altre (alias riga $S * T = S * (-1 * T) = 0$ se $S! = T$).

1.9 Il GPRS: cos'è, difetti e pregi

Il GPRS è un'evoluzione del GMS che permette la gestione del traffico a pacchetti. Al contrario del GSM non serve un servizio dedicato ma vi è un canale condiviso. Lo spreco di banda è inesistente e si utilizza una tariffa a traffico e non a tempo, come avviene per il GSM. IL GPRS aggiunge il supporto a PPP e IP. essendo una naturale evoluzione del GSM, ci furono differenti classi di cellulare, a seconda del supporto alla prima o seconda tecnologia.
Nei cellulari in classe C, l'utente deve selezionare quale comunicazione utilizzare, se GSM oppure GPRS. La classe B, permette di utilizzare entrambe le reti, ma se si sta scaricando un pacchetto e si riceve una chiamata, il download viene sospeso. Prima della classe A, esiste una pseudo classe A, in cui si possono usare contemporaneamente utilizzando una solo frequenza. La Classe A, permette di utilizzare sia una che l'altra tecnologia, contemporaneamente, è come avere due cellulari indipendenti.
La sicurezza è analoga al GSM, con l'aggiunta di una seconda chiave Kc(cipher key). Questa è generata ogni volta dalla Ki e da un numero casuale ogni volta che l'utente di autentica.

1.10 Handoff: che cos'è e i vari tipi

Nelle connessioni mobili, ogni telefono è connesso alla rete tramite una sola cella finché non si sposta. Quando ci si sposta, si deve cambiare la cella precedente con una più vicina, anche per evitare problemi dati dalla distanza. La disconnessione da una cella, può avvenire con due modalità:

- Hard handoff: quando il segnale è troppo debole, lo switching office chiede alle celle vicine quanta potenza ricevono dal cellulare. Queste gli rispondono e il cellulare viene riassegnato alla cella con più potenza. Quindi il cellulare viene mollato e poi riagganciato, in qualche caso è presente del lag che fa cadere la linea;
- Soft handoff: introdotto da GSM per ovviare al problema del lag, quando il cellulare ha poco segnale dalla cella, prima di lasciarla, si aggancia ad una nuova e poi abbandona la vecchia. Occorre che il cellulare gestisca due frequenze, cosa che 1G e 2G non supportavano.

1.11 FDM, TDM, CDM: algoritmi per la selezione della banda

FDM: sfrutta la trasmissione in banda passante per condividere un canale, divide lo spettro in bande di frequenza di cui ogni utente ha uso esclusivo per inviare il proprio segnale.
TDM: gli utenti fanno a turni secondo una politica round-robin e ognuno di loro, periodicamente prende possesso della banda completa per un tempo limitato.
CDM: comunicazione a spettro distribuito in cui un segnale a banda stretta viene sparso su una banda di frequenza più ampia. Ciò rende il segnale più tollerante alle interferenze e permette a più segnali di utenti diversi di condividere la stessa banda di frequenza, chiamato anche CDMA.

1.12 QAM e QAM16 (Quadrature Amplitude Modulation)

È un sistema di modulazione numerica sia analogica che digitale. Le portanti sono solitamente sinusoidali. Il termine quadratura indica che gli angoli differiscono di 90°. Il segnale può essere visto come la somma di due segnali modulati in fame.
QAM: Più immune al rumore si ottiene tramite i diagrammi a costellazione, quelli circolari sono quelli ideali ma sono più difficili sia da ottenere che da decodificare. QAM 16: Quando si voleva spingere sull'acceleratore, nella trasmissione di dati via cavo, si è pensato che il miglior approccio da utilizzare era combinare due tipi di modulazione assieme, l'ampiezza e la fase.
Da questa idea nasce il QAM-16. Grazie ad esso possiamo utilizzare un alfabeto più ampio e spedire un simbolo su 16 ogni unità di tempo con bitrate quadruplo.

2 Capitolo Strato Data Link

2.1 Che cos'è il byte stuffing?

Il byte stuffing è usato in PPP (Point-to-Point Protocol) ed è un metodo usato per capire dove inizia e finisce un frame. Il byte stuffing inserisce prima e dopo ogni frame un byte, chiamato flag byte. Quindi in caso di perdita di dati, basterà cercare l'ultimo flag byte caricato. Un possibile inconveniente è che dentro i dati ci sia un flag byte. In questo caso, basta che la sorgente inserisca un byte di Escape subito prima di ogni occorrenza e la destinazione provvederà a toglierli. Il controllo del frame è eseguito dallo strato Data Link, il quale prima di passa passare il frame allo strato successivo, elimina le sequenze escape e i flag byte.
Se trova una sequenza di escape nel frame, devo inserire a sua volte un altro escape per non far ignorare le successiva. Un difetto di questo metodo è legato all'uso di caratteri a 8 bit. Ad esempio Unicode usa una codifica a 16bit.

2.2 Descrivere il Bit stuffing

È analogo al byte stuffing, solo che è fatto a livello di bit, così viene aggirato il problema del byte stuffing e quindi si può scegliere la dimensione della flag. Ogni frame inizia e finisce con 01111110 (protocollo X.25). Ogni volta che lo strato datalink della sorgente incontra 5, uni di fila inseriscono uno zero. Il destinatario ogni volta che incontra 5 uni, elimina lo zero successivo. Questo metodo è usato anche per fare padding.

2.3 Numero di bit necessari per riconoscimento(correzione) degli errori di trasmissione

Esistono due strategie per la gestione degli errori:

- Codifica a correzione d'errore: vengono inclusi nel blocco trasmesso una quantità di informazioni ridondanti, che in caso di errore permettono di ricostruire e riparare il frame;
- Codifica a rilevazione di errori: introduce ridondanze in modo che il destinatario capisca se c'è un errore, ma NON è in gradi di correggerlo.

Dati m bit per il frame e r bit ridondanti: $m + r = n$, ovvero n è la lunghezza totale del messaggio inviato, chiamato codeword. Prendiamo ad esempio due codeword: 810001001 e 10110001. Come determino quanti bit corrispondenti sono differenti? Eseguo l'OR esclusivo ed ottengo 0011000. Il numero di bit corrispondenti diversi è detto distanza di Hamming: se due codeword sono a distanza di Hamming d uno dall'altra, sono necessari d errori su singoli bit per convertire una sequenza nell'altra. Per trovare d errori necessito di codifica con distanza d+1. Per correggere d errori necessito di codifica con distanza 2d+1.

2.4 Si descriva cos'è il CRC (Cycle redundancy check). Si calcoli inoltre il CRC di 10011101 usando il polinomio generatore di $x^4 + x + 1$.

Il cyclic redundancy check è un metodo per il calcolo di checksum. Il nome deriva dal fatto che i dati d'uscita sono ottenuti elaborando i dati di ingresso, i quali vengono fatti scorrere ciclicamente in una rete logica. Il controllo CRC è molto diffuso perché la sua implementazione binaria è semplice da realizzare, richiede conoscenze matematiche modeste per la stima degli errori e si presta bene a rilevare errori di trasmissione su linee affette da elevato rumore di fondo. 16) il generatore deve avere i bit di ordine più alto e più basso uguali a 1. per poter calcolare il checksum di un frame di m bit che corrisponde al polinomio M(x), il frame deve essere più lungo del polinomio generatore. Quando la destinazione riceve un frame prova a dividerlo per il polinomio generatore. Se la divisione ha un resto, c'è stato un errore nella trasmissione.

1. Posto r il grado di G(x), aggiungere r bit con valore zero dopo la parte di ordine piu' basso del frame. Così che adesso contenga m+r bit e corrisponda al polinomio $x^r M(x)$;
2. Dividere la sequenza di bit corrispondenti a G(x) per la sequenza corrispondente a $x^r M(x)$ usando la divisione modulo 2;
3. Sottrarre il resto dalla sequenza corrispondente a $x^r M(x)$ usando la sottrazione in modulo 2. Il risultato è il frame con checksum pronto per la trasmissione.

Dati due polinomi P e G (generatore) dobbiamo aggiungere alla destra di P tanti zeri quanto è il grado massimo di G e otteniamo il polinomio F. Poi si dive il polinomio ottenuto per G, si ottiene un resto che va sommato al polinomio F, infine si raggruppano i bit in gruppetti di 4 e si codifica in esadecimale.
Esempio: $P = 10011101$ e $G = x^4 + x + 1$, quindi abbiamo $G = 10011$,
$F = P = 100111010000$ e il resto è 1111.
Il polinomio finale è 100111011111 in esadecimale è $9DF$.

2.5 Descrivere Il protocollo stop and wait, pregi e difetti

Il protocollo S&W è un protocollo molto semplice per il controllo del flusso e si può utilizzare in canali simplex o half-duplex. Quando il mittente invia un blocco aspetta che il ricevente invii una conferma, un ACK (acknowledge). Lo svantaggio principale è l'attesa, ma in compenso non c'è bisogno di regolare la velocità.
Possono sorgere due errori: il frame non arriva mai a destinazione e il mittente aspetta e rinvia all'infinito: c'è bisogno di un tempo limite di rinvio. L'altro problema riguarda l'ACK: potrebbe non arrivare al mittente, il quale rinvia il pacchetto e al destinatario arriva più volte, ma per fortuna viene scartato, grazie al numero di messaggio.

2.6 Cos'è il piggybacking

La tecnica consiste nello sfruttare un messaggio del destinatario al mittente come passaggio per l'ACK, in modo da non perdere tempo e sfruttare al meglio il canale di comunicazione(un messaggio in meno da inviare). Il campo ACK è posto all'inizio del frame. Il problema principale è quando fare piggybacking: in attesa molto lunga può essere vana, poiché il mittente rinvia il frame. Quindi se il pacchetto arriva per il mittente è caricato e inviato in tempo breve si fa piggybacking, altrimenti s'invia l'ACK separatamente.

2.7 Si descriva la tecnica dello Sliding window

È un protocollo per il controllo di flusso. Utilizza la tecnica del piggybacking. Invia pacchetti e aspetta messaggio di conferma ACK. Sorge il problema di quando fare il piggybacking, un'attesa troppo lunga può rendere vano il tutto perché il mittente fa un rinvio del frame. Quindi se il pacchetto arriva velocemente viene fatto piggybacking sennò viene inviato separatamente.
L'essenza del protocollo è che ogni partecipante alla comunicazione deve tener sotto controllo 2 finestre, quella dei frame in entrata e quella dei frame in uscita. Ogni frame in usciata contiene un numero di sequenza e il destinatario deve tener traccia di questi per la ricezione mentre il mittente per l'invio.
Con lo sliding window a 1 bit, viene utilizzato il metodo stop and wait. Quando il mittente invia un frame, resta nella finestra finché non viene ricevuto l'ACK corrispondente prima di aggiornare la finestra. I frame inviati sono numerati con 1 o 0. Quando il destinatario riceve il frame, controlla che il numero sia uguale a quello che aspettava, se s'invia l'ACK. Se l'ACK contiene il numero che la sorgente si aspettava allora continua a inviare, altrimenti re invia quello segnato nel buffer. Si può utilizzare anche il pipelining, inviando più frame contemporaneamente prima di entrare in attesa. Il destinatario aggiorna la finestra non appena riceve il frame e invia l'ACK. Esistono 2 approccio: go back n e selective repeat.

2.8 Si descriva l'idea dei protocolli "go back N", indicandone pregi e difetti.

Questo protocollo è utilizzato con sliding window di ampiezza 1 in ricezione e maggiore di uno in invio. I pacchetti arrivano uno per volta e su di essi viene fatto un checksum, se si trovano errori vengono segnalati alla sorgente indicando il numero del pacchetto danneggiato. Per questo motivo la finestra deve essere capiente. Se la finestra sorgente si riempie prima che il timer di arrivo scatti, la pipeline viene svuotata. La destinazione intanto scarta i pacchetti successivi a quello in errore.
Questo approccio è efficacie contro la prevenzione di errori, ma occupa molta banda se la frequenza di errori è alta.

2.9 Si descriva cos'è la tecnica del selective repeat

La tecnica del selective repeat è una tecnica che si usa con il protocollo sliding window. In questo caso il buffer della destinazione deve essere più capiente. Infatti in caso di errori, viene inviato alla sorgente un NACK, indicandone il

pacchetto. Finché il pacchetto contenente l'errore non arriva al destinatario, i pacchetti successivi vengono mantenuti nel buffer. Una volta arrivato tutto, il messaggio viene passato allo strato network. Inoltre la sorgente dispone di un timer per cui, se il pacchetto è errato e non arrivasse un NACK il pacchetto sarebbe rinviato comunque.

3 Capitolo Sottostrato MAC

4 Capitolo Strato Network

5 Capitolo Strato Trasporto

6 Capitolo Strato Applicazione

7 Capitolo Sicurezza