
Appunti
di
Reti e sicurezza

Luca De Franceschi
Mirko Polato

Università degli studi di Padova

Indice

1	Introduzione	2
2	Lo strato fisico	3
2.1	Mezzi di Trasmissione	3
2.1.1	Basi teoriche della comunicazione dati	3
2.1.2	Mezzi Magnetici	3
2.1.3	Doppino	3
2.1.4	Cavo coassiale	4
2.1.5	Fibra Ottica	4
2.2	Trasmissioni Wireless	6
2.2.1	Lo spettro elettromagnetico	6
2.2.2	Trasmissioni radio	6
2.2.3	Trasmissione a microonde	6
2.2.4	Infrarossi	7
2.2.5	Trasmissioni a onde luminose (LASER)	7
2.3	Satelliti	8
2.3.1	Satelliti Geostazionari (GEO)	8
2.3.2	Satelliti su orbite medie (MEO)	9
2.3.3	Satelliti su orbite basse (LEO)	9
2.3.4	Satelliti o fibra?	9
2.4	Sistema Telefonico	10
2.4.1	Struttura della rete	10
2.4.2	Modem, ADSL, Wireless	10
2.4.3	Multiplexing	14
2.4.4	Commutazione	15
2.5	Sistema telefonico mobile	16
2.5.1	Cellulari di I generazione	16
2.5.2	Cellulari di II generazione	17
2.5.3	Cellulari di III generazione	19
2.5.4	Oltre al 3G	20
3	Lo strato data link	21
4	Il sottostrato MAC (<i>Medium Access Control</i>)	22
5	Lo strato network	23
6	Lo strato trasporto	24
7	Lo strato applicazione	25
8	Sicurezza delle reti	26
A	Glossario	26

B Domande degli appelli	26
B.1 Capitolo 2	26
B.1.1 Cosa si intende per serie di Fourier	26
B.1.2 Bitrate e baudrate	26
B.1.3 Descrivere i vari tipi di cavo e confrontarli	26
B.1.4 Caratteristiche e confronto fra i vari tipi di satellite, GEO, MEO, LEO	27
B.1.5 Che cos'è la modulazione in frequenza (FM)? E in am- piezza(AM)?	27
B.1.6 Che cos'è la modulazione delta (delta modulation)?	28
B.1.7 Descrivere in dettaglio il GSM (Global System for Mobile connection)	28
B.1.8 Si descriva la tecnica CDMA (Code Division Multiple Access), possibilmente con esempio	29
B.1.9 Il GPRS: cos'è, difetti e pregi	29
B.1.10 Handoff: che cos'è e i vari tipi	30
B.1.11 FDM, TDM, CDM: algoritmi per la selezione della banda	30
B.1.12 QAM e QAM16 (Quadrature Amplitude Modulation) . . .	30
C Capitolo 3	31
C.0.13 Che cos'è il byte stuffing?	31
C.0.14 Descrivere il Bit stuffing	31
C.0.15 Numero di bit necessari per riconoscimento(correzione) degli errori di trasmissione	31
C.0.16 Si descriva cos'è il CRC (Cycle redundancy check). Si calcoli inoltre il CRC di 10011101 usando il polinomio generatore di $x^4 + x + 1$	32
C.0.17 Descrivere Il protocollo stop and wait, pregi e difetti . . .	32
C.0.18 Cos'è il piggybacking	32
C.0.19 Si descriva la tecnica dello Sliding window	33
C.0.20 Si descriva l'idea dei protocolli "go back N", indicandone pregi e difetti.	33
C.0.21 Si descriva cos'è la tecnica del selective repeat	33
D Capitolo 4	34
E Capitolo 5	34
F Capitolo 6	34
G Capitolo 7	34
H Capitolo 8	34

1 Introduzione

2 Lo strato fisico

2.1 Mezzi di Trasmissione

2.1.1 Basi teoriche della comunicazione dati

Le informazioni posso essere trasmesse via cavo variando alcune proprietà fisiche (tensione/corrente). Rappresentando la tensione/corrente in una funzione $f(t)$ è possibile analizzare il segnale. Fourier dimostrò che un segnale di questo tipo, periodico e abbastanza regolare può essere descritto da una ideale somma infinita di seni e coseni (**Serie di Fourier**). Una funzione può essere ricostruita a partire dalla sua serie di Fourier. Analizziamo un segnale di trasmissione analogica e proviamo a ricostruirlo con Fourier. Dobbiamo tener conto che nessun canale trasmissivo è perfetto, per cui c'è sicuramente attenuazione. L'intervallo di frequenze trasmesse senza forte attenuazione è detto **banda passante**. Anche in un canale perfetto ci si accorge comunque che un segnale digitale non può essere trasmesso a velocità troppo elevate, esistono però alcuni schemi di codifica per aumentare la velocità di trasmissione.

Nyquist/Shannon dimostrò che la velocità massima di trasmissione è:

$$V_{max} = 2H \log_2 V_{bit/sec}$$

Mentre il livello di rumore si misura facendo il **rapporto segnale-rumore**. Solitamente viene indicata tale misura antedecendo $10\log_{10}$ e misurando in dB.

$$Segnale/Rumore = 10\log_{10} S/N \text{ dB}$$

Un risultato notevole ottenuto da Shannon fu:

$$MAX_{bit/s} = H \log_2(1 + S/N)$$

con H pari all'ampiezza di banda in Hz.

2.1.2 Mezzi Magnetici

Sistema molto semplice, utilizzato da sempre e basato su un funzionamento banale: si salvano i dati su nastri magnetici (dischi rimovibili) e si trasportano fisicamente a destinazione dove verranno letti. Se si pensa a un tir che trasporta un centinaio di HD da 1TB che percorre qualche Km per consegnare questi dischi si può intuire che la larghezza di banda è elevatissima e con un costo irrisorio. La cosa banalmente poco buona è l'enorme ritardo nella trasmissione dati.

2.1.3 Doppino

Il doppino è composto da 2 conduttori di rame isolati attorcigliati tra loro a forma elicoidale (stile DNA), questo per evitare interferenze tra di loro (risulterebbero un'ottima antenna). Viene largamente utilizzato nel sistema telefonico, questo perché il doppino può attraversare diversi Km senza bisogno di amplificare il segnale così dall'abitazione si può agevolmente arrivare alla centrale. Si possono usare per trasmettere dati Analogici o anche Digitali e la

larghezza di banda dipende dal diametro del cavo e dalla distanza percorsa. Esistono più categorie di questi cavi che differiscono sostanzialmente per il numero di spire per cm per ridurre le interferenze. Il doppino cat3 (usato sino al 1988) sono composte da 2 cavi isolati cavi attorcigliati. Il doppino cat5 sono come i cat3 ma utilizzano più spire per cm questo li rendono più adatti a trasmissione ad alta velocità. Il doppino può arrivare a una banda di 250-600MHz. Questi cavi sono detti anche UTP (*Unshielded Twisted Pair*).

2.1.4 Cavo coassiale

Essendo più schermato del precedente il cavo coassiale può estendersi per distanze maggiori. Esistono 2 tipi di cavi coassiali: da 50 Ohm per le trasmissioni digitali e da 75 Ohm per le analogiche. Composto da un nucleo di rame, rivestito da materiale isolante a sua volta rivestito da una calza conduttrice il tutto ricoperto da una guaina protettiva, il cavo coassiale è caratterizzato da un'eccellente immunità al rumore. L'ampiezza di banda di questi cavi arriva attorno a 1GHz e dipende dalla lunghezza, dalla qualità e dal rapporto segnale-rumore del segnale.

2.1.5 Fibra Ottica

Un sistema di trasmissione ottico è formato principalmente di 3 parti: sorgente luminosa, mezzo di trasmissione e rivelatore di luce. La sorgente di luce è rappresentata o da LED o semiconduttori laser. Il mezzo trasmissivo ovviamente è la fibra composta da un nucleo (core) di vetro di pochi micron avvolto in una guaina di vetro (cladding) con indice di rifrazione più basso e infine la solita rivestitura con guaina in plastica. La fibra si basa su un principio molto semplice, ovvero che la luce che la attraversa viene riflessa al suo interno fino ad arrivare all'altra estremità del cavo, questo avviene perché la luce immessa nel core incontra il cladding con indice di rifrazione minore e il raggio luminoso viene così riflesso (se possiede un'inclinazione corretta). La velocità di tale raggio è circa quella della luce infatti il limite di banda della fibra non è dovuto alla velocità di trasmissione ma di decodifica del segnale luminoso in impulso elettrico. Una fibra può contenere più raggi che si riflettono in essa l'importante è che il loro angolo di riflessione sia diverso. Questo tipo di fibre è detto **multimodale**. Le fibre che invece permettono la trasmissione di luce in linea retta sono le **monomodali** che non sono altro che guide d'onda ma possono raggiungere i 50Gbps per 100Km senza attenuazione. Un problema delle fibre è il collegamento tra 2 i esse che può avvenire in 3 modi:

1. Le fibre vengono inserite in apposite prese grazie a dei connettori con perdita di circa 10-20% della luce;
2. Le fibre vengono attaccate meccanicamente, messe di fronte una all'altra e poi viene avvolto in una macchina particolare per poi essere pinzate, con perdita comunque di circa il 10% della luce;
3. Le fibre vengono fuse tra loro. Una soluzione quasi ottimale, anche se difficile, genera una piccola attenuazione di segnale.

Le LAN basate sulle fibre ottiche solitamente sono ad anello con congiunzione a T per ogni pc o a stella passiva. La configurazione ad anello ha il difetto che se una congiunzione si guasta salta tutta la rete.

Tabella riassuntiva

		Mezzi Magnetici	Doppino	Coassiale	Fibra ottica
	Anno	1950	1980	1980	1980
	Tipo dati	-	A/D	A/D	A/D
	Banda(Hz)	Elevata	10M-600M	< 1G	1G - 10G (100G)
	Ritardo	Elevato	Accettabile	Basso	Quasi nullo
	Immunita Rumore	-	Eccellente	Eccellente	Eccellente
	Costo	Basso	Basso	Intermedio	Elevato
	Estensione	-	Diversi Km	Decine Km	100Km
	Interferenze	-			Immune
	Intrusione	-	Facile	Facile	Difficile

Figura 1: Riassunto caratteristiche dei mezzi trasmissivi.

2.2 Trasmissioni Wireless

2.2.1 Lo spettro elettromagnetico

Lo spostamento di elettroni crea campi magnetici. Questa osservazione fu fatta per la prima volta da Hertz. Il numero di oscillazioni al secondo di un'onda è chiamato **frequenza** e si misura in Hz. La distanza massima tra 2 picchi (o minimi) è chiamata **lunghezza d'onda**. Tutte le trasmissioni wireless si basano sul principio che un'antenna collegata a un circuito elettrico invia onde elettromagnetiche che possono essere captate da un ricevitore posto a una distanza appropriata. Le onde viaggiano nell'etere alla velocità della luce. Qui di seguito è visualizzato lo spettro elettromagnetico e la sua suddivisione.

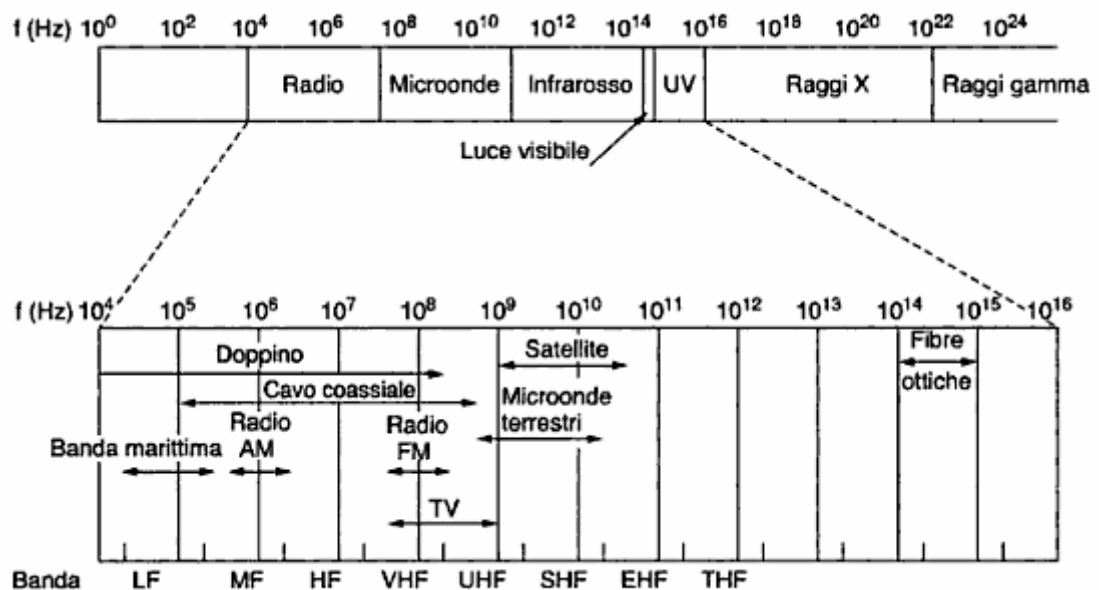


Figura 2: Spettro elettromagnetico.

2.2.2 Trasmissioni radio

Le onde radio sono onde omnidirezionali semplici da riprodurre e viaggiano per lunghe distanze attraversando gli edifici. Non necessita di alcun allineamento trasmettitore-ricevente. Nell'aria l'attenuazione delle onde con frequenze più basse è di circa $1/r^2$. Nelle bande VLF, LF, MF le onde seguono la forma del terreno e possono viaggiare per circa 1000 Km. Nelle alte frequenze invece le onde che riescono ad entrare nella ionosfera vengono riflesse e ritornano sulla terra permettendo così di percorrere distanze notevoli.

2.2.3 Trasmissione a microonde

Sopra i 100 MHz le onde viaggiano quasi in linea retta per cui è necessario un allineamento trasmettitore-ricevente. Concentrando l'onda in un piccolo raggio si ottiene un ottimo rapporto segnale/rumore. Il problema di queste

trasmissioni sta nelle lunghe distanze e dalla curvatura della terra, la quale porta alla necessità di ripetitori. L'utilizzo di antenne molto alte riduce l'effetto della curvatura. Alcune onde posso rifrangersi negli strati più bassi dell'atmosfera e arrivare in ritardo rispetto a quelle dirette e addirittura fuori fase causandone l'annullamento (**multipath fading**). Le microonde non attraversano gli edifici molto bene, e sono soggette alle condizioni climatiche. Comunemente si usano bande sopra i 10 GHz ma sopra i 40 GHz la pioggia comincia ad assorbire le onde. Acquisto e installazione di apparecchi per questo tipo di trasmissione è molto basso.

Divisione dello spettro elettromagnetico

Tutti vogliono un pezzo di spettro per aumentare la velocità di trasmissione e quindi bisogna regolarne tale divisione, se ne occupa l'ITU-T. In passato per compiere tale divisione sono stati utilizzati 3 modi:

1. Concorso di bellezza: ognuno di coloro che voleva spettro doveva dare un motivo per il quale doveva averlo proprio lui. Problemi: corruzioni e scelte arbitrarie senza senso.
2. Lotteria: veniva fatta una vera e propria lotteria per assegnare lo spettro. Problemi: partecipavano anche i non interessanti solo per guadagnare soldi dalla rivendita dello spettro.
3. Asta: vendita all'asta dello spettro. Problema: banca rotta delle aziende.
4. Libertà: approccio che non prevede assegnamento di spettro, lasciando trasmissione libera ma regolata. Ovvero la potenza doveva essere utilizzata in modo da limitare la portata per evitare interferenze.

2.2.4 Infrarossi

Sistema economico e facile da costruire con il difetto di non riuscire ad attraversare gli ostacoli. Queste onde, infatti, si avvicinano alle onde di tipo luminose. Sono più sicuri delle onde radio per la difficoltà di intercettazione, ma risentono molto degli ostacoli. Questo a volte può rappresentare anche un vantaggio (es. telecomandi tv). Per questi motivi sono usati per distanze brevi (collegamento pc-stampanti, telecomandi ecc.), e hanno un ruolo secondario nelle telecomunicazioni. Il sistema infrarosso non richiede alcuna licenza governativa.

2.2.5 Trasmissioni a onde luminose (LASER)

Sistema poco costoso che offre una banda molto elevata, facile da installare e non richiede licenze. La sua debolezza sta nel raggio molto sottile (e unidirezionale) e quindi difficile da indirizzare verso il bersaglio esatto. Per ovviare al problema a volte vengono inserite lenti per rendere il raggio meno focalizzato. Il raggio laser per di più non attraversa la pioggia e la nebbia ed è soggetto a fenomeni di convezione (turbolenza provocata da fonti di calore).

2.3 Satelliti

Un satellite può essere immaginato come un grande ripetitore di microonde collocato nel cielo, che contiene molti **trasponder** (ricetrasmittitori satellitari). I raggi verso la terra possono essere più o meno grandi, questa modalità è detta **bent pipe**. I satelliti hanno un periodo orbitale che dipende dalla loro altezza rispetto alla terra. Un problema è la presenza delle **fasce di Val Allen**, strati di particelle molto cariche, che distruggerebbero un satellite in poco tempo.

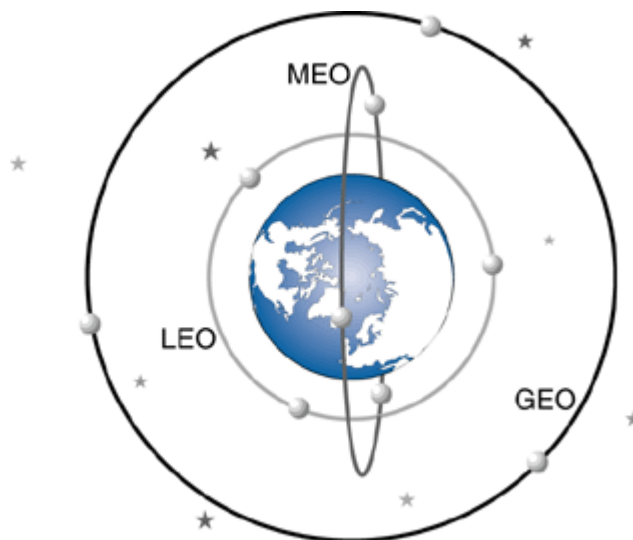


Figura 3: Posizione dei satelliti GEO, MEO e LEO

2.3.1 Satelliti Geostazionari (GEO)

Questi satelliti sono posti in orbite molto alte e con le tecnologie odierne non si possono collocare 2 satelliti GEO a meno di 2 gradi nel piano equatoriale, quindi con 180 satelliti si copre tutto. L'allocatione degli slot spaziali è gestito dall'ITU. L'ITU inoltre ha assegnato alcune bande di frequenza alle applicazioni satellitari in modo da non interferire con i sistemi a microonde preesistenti. I segnali inviati da questi satelliti viaggia alla velocità della luce, ma essendo molto lontani dalla terra hanno comunque un ritardo di circa 300 ms. I primi satelliti GEO con una singola emissione coprivano circa 1/3 della terra, chiamata **impronta**. Poi con lo sviluppo delle tecnologie si è cominciato a concentrare i raggi trasmissivi (spot) in aree geografiche più piccole (centinaia di Km). Un nuovo passo avanti nel settore delle comunicazioni satellitari si ebbe con le stazioni VSAT, piccole stazioni con una antenna da circa 1m che comunicano con i satelliti GEO e per le loro piccole dimensioni e potenza non essendo in grado di comunicare tra loro si è dovuto ideare alcune stazioni particolari più potenti per fare da ponte. Sono ovviamente mezzi di trasmissione broadcast e per quanto riguarda la sicurezza sono un disastro. Il costo della trasmissione satellitare non dipende dalla distanza, ma è costante. Hanno una reattività quasi istantanea e un ottimo tasso di errore.

2.3.2 Satelliti su orbite medie (MEO)

Questi satelliti si muovono sopra di noi a una velocità relativamente bassa percorrendo il giro del pianeta in circa 6 ore. Coprono un'area più piccola dei GEO e si possono raggiungere con mezzi meno potenti. I 24 satelliti GPS che orbitano a 18000 Km sono di tipo MEO.

2.3.3 Satelliti su orbite basse (LEO)

Si spostano molto velocemente e per realizzare un sistema completo sono necessari molti satelliti di questo tipo. Essendo vicini alla crosta terrestre le stazioni non hanno bisogno di molta energia per comunicare con poco ritardo.

Iridium

Lanciati nel 1997 i 66 satelliti LEO del progetto Iridium (Motorola) vennero acquistati da un investitore riprendendo il servizio nel marzo 2001, che era stato fermato nel 1999. Il progetto fornisce un servizio di telecomunicazione a livello mondiale basato su "cellulari" particolari. I satelliti Iridium sono collocati a 750 Km di altezza, con un satellite ogni 32 gradi. Le trasmissioni avvengono nello spazio: ogni satellite comunica con altri satelliti fino a destinazione.

GlobalStar

Basato su 48 satelliti LEO utilizzando uno schema diverso dal precedente. Il satellite che riceve la chiamata trasmette a una centrale terrestre che comunica con altre fino al satellite posto sulla cella del destinatario. La complessità resta quindi terrestre facilitandone la gestione.

Teledesic

Progetto mirato per gli utenti internet, con l'idea di offrire 100 Mbps in trasmissione e 720 in ricezione. Il sistema è composto da 32 satelliti LEO con un'impronta più grande. Basato sulla commutazione di pacchetto, con ogni satellite in grado di instradare ogni singolo pacchetto.

2.3.4 Satelliti o fibra?

E' ovvio che la comunicazione con le fibre sia molto veloce ma ci sono molti settori in cui i satelliti non possono essere rimpiazzati dalla fibra, come ad esempio la comunicazione mobile. Le comunicazioni broadcast per eccellenza sono satellitari. Un altro settore è la comunicazione in luoghi ostili, in cui le infrastrutture terrestri scarseggiano e la posa di cavi ottici non sarebbe il massimo. Inoltre anche le zone in cui i costi di posa sono elevati il satellite può essere un'ottima alternativa. In sostanza per la comunicazione terrestre è sicuramente migliore la fibra ma il satellite rimarrà indispensabile per altri settori.

2.4 Sistema Telefonico

2.4.1 Struttura della rete

Inizialmente il mercato dei telefoni prevedeva la vendita di 2 apparecchi e spettava all'utente tirare il cavo tra i 2 telefoni. Questo intuitivamente creò una struttura di rete troppo confusa. Bell notato questo particolare aprì il primo ufficio di commutazione nel 1878. Le chiamate quindi dovevano passare per la centrale nella quale un addetto si occupava di collegare con un cavo il chiamante al chiamato. La rete però, sebbene meno complessa, rimase ancora troppo confusa poichè non era pensabile collegare ogni ufficio di commutazione a una centrale. Vengono così ideati i livelli delle centrali di commutazione. Inizialmente con 2 livelli fino ad arrivare a 5. In generale una comunicazione avviene a più livelli:

1. La richiesta di chiamata arriva alla centrale locale del chiamante alla quale è collegato direttamente con 2 cavi di rame (doppino di categoria 3). Se il chiamato appartiene alla stessa centrale locale avviene il collegamento tra le parti;
2. La centrale locale è collegata a una centrale interurbana (con cavi in fibra/microonde/coassiale), e come per quella locale se la centrale locale del chiamato è collegata alla stessa centrale interurbana allora le parti si collegano;
3. Le centrali interurbane sono connesse a centrali intermedie e la trasmissione avviene analogamente alle precedenti.

Le trasmissioni sono preferibili in digitale per la non necessità di accuratezza, per il basso costo e per la semplicità di gestione. Si possono quindi individuare 3 componenti fondamentali del sistema telefonico:

1. Collegamenti locali: rappresentano il collo di bottiglia del sistema;
2. Linee: collegamenti in fibra tra le centrali;
3. Centrali di commutazione: che spostano le chiamate tra le linee.

2.4.2 Modem, ADSL, Wireless

Il modem ha la funzione di convertire i dati dalla forma digitale del pc alla forma analogica necessaria per inviare i dati attraverso un collegamento locale. Nella centrale poi i dati vengono ritrasformati in digitale e poi ritrasmessi in linee a lunga distanza. Dall'altro capo poi ci sarà il modem per la conversione inversa alla precedente. I problemi principali delle linee di trasmissioni sono 3:

1. Attenuazione: rappresenta la perdita di energia (in dB/Km) dalla propagazione del segnale. Tale perdita dipende dalla frequenza;
2. Distorsione: rappresenta la differenza di velocità tra le varie componenti del segnale;
3. Rumore: rappresenta energia indesiderata all'interno del segnale originale, causate da sorgenti di trasmissione esterne.

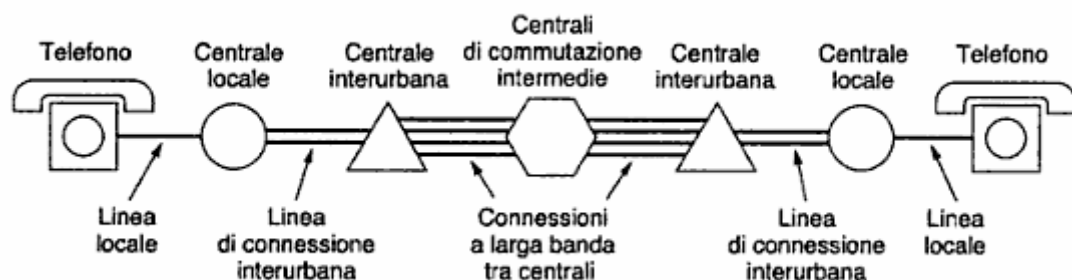


Figura 4: Percorso tipico di una chiamata a media distanza

Modem

Per riuscire a inviare dati in forma digitale è necessario un ampio spettro di frequenza questo rende adatta la trasmissione in banda base (DC) solo a basse velocità e distanze brevi. Il problema è aggirato utilizzando una trasmissione (AC) aggiungendo un segnale portante tra i 1000 e i 2000 Hz. Nella modulazione di ampiezza (ASK) sono utilizzate 2 diverse ampiezze 0 e 1, nella modulazione di frequenza (FSK) si utilizzano 2 o più toni. In quella di fase invece l'onda portante è spostata di 0 o 180 gradi a intervalli regolari.

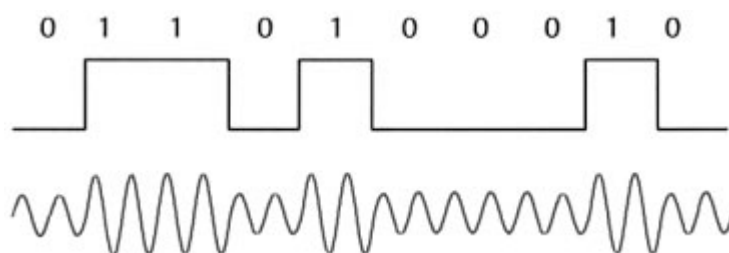


Figura 5: Modulazione d'ampiezza

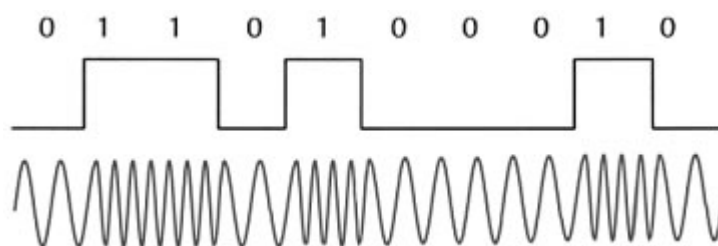


Figura 6: Modulazione di frequenza

Un apparecchio che utilizza uno di questi metodi per “tradurre” un flusso di bit in segnale analogico è detto modem. La maggior parte dei modem campiona 2400 volte al secondo. Il numero di campionamenti al secondo si

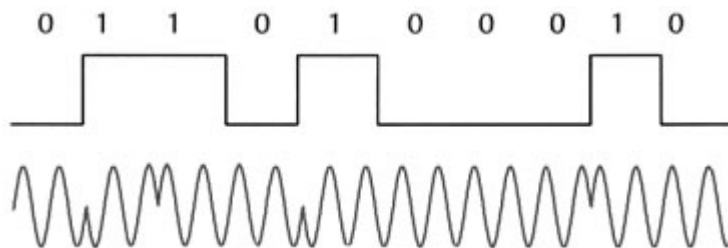


Figura 7: Modulazione di fase

misura in **baud**. Durante ogni baud è trasmesso un simbolo. Concetti da ricordare:

- Banda passante: intervallo di frequenza passante nel mezzo con un attenuazione minima(Hz);
- Baud rate: numero di campioni per secondo (=frequenza simboli);
- Modulazione: determina il numero di bit per simbolo;
- Frequenza di bit: quantità di (simboli/sec)*(bit/simbolo).

La trasmissione digitale è adatta in banda base (DC) a basse velocità. Per aggirare i problemi di tale banda si usa la trasmissione AC introducendo un segnale costante detto **portante d'onda sinusoidale**. La sua ampiezza, frequenza o fase posso essere modulate per inviare informazioni. Nella **modulazioni di ampiezza** vengono usate 2 ampiezze diverse per rappresentare 1 e 0 mentre in quella di **frequenza** (FSK) si utilizzano più toni. Infine nella **modulazione di fase** più semplice l'onda viene spostata di 0 o 180 gradi (schemi migliori utilizzano spostamenti più piccoli). I modem odierni utilizzano modulazioni ibride per avere un maggior baud rate. Un esempio è la QPSK (*Quadrature Phase Shift Keying*). Questa tecnica di modulazione prevede l'utilizzo di più fasi e più ampiezze, e in base al numero di combinazioni nascono i nomi QAM-16 (4 bit per simbolo utilizzando 4 fasi e 4 ampiezze, 9600 bps), QAM-64 (*Quadrature Amplitude Modulation*) e così via. Uno schema con costellazione molto fitta è soggetto a errori per questo i modem che li adottano utilizzano meccanismi di correzione degli errori, per esempio con un bit extra di parità. Gli standard utilizzati dai modem più conosciuti sono:

- V.32: trasmette 4 bit più 1 di parità a 2400 baud (9600 bps);
- V.32 bis: trasmette 6 bit più 1 di parità a 2400 baud (14400 bps);
- V.34: utilizza 12 bit per simbolo a 2400 baud (28800 bps);
- V.34 bis: utilizza 14 bit per simbolo a 2400 baud (33600 bps).

Una connessione che permette ai dati di viaggiare in entrambe i sensi è detta **full duplex**, mentre se lo permette ma solo uno alla volta è detta **half duplex** se invece è permesso un solo senso è **simplex**. In base quanto detto la

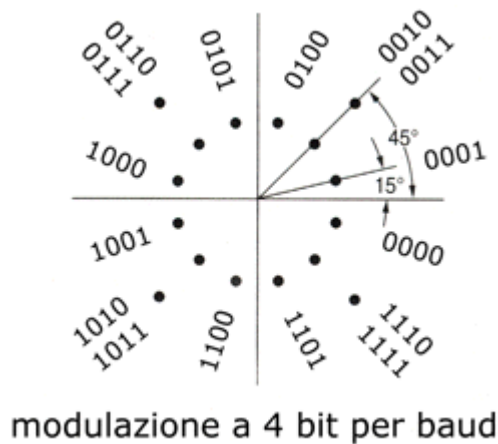


Figura 8: Diagramma costellazione QAM

velocità massima dei modem è 34 Kbps questo non è vero perché l'ampiezza del canale telefonico è 4 MHz quindi per Nyquist il numero di campioni massimo è 8000, per gli 8 bit per campione usato negli U.S. si hanno 64 Kbps! In realtà non è così perché 1 bit serve per il controllo per cui si riduce il tutto a 56 Kbps che è lo standard **V.90**.

Linee DSL

Servizi con banda maggiore a quella appena descritta sono detti a **banda larga**. Per ottenere questo aumento di banda viene usato un artificio che si basa sostanzialmente sulla rimozione del filtro che limitava la capacità del collegamento locale a 3100 Hz. Questi servizi, detti xDSL, sarebbero dovuti funzionare sui doppini già installati nelle abitazioni, senza creare problemi ai telefoni, con costi limitati e non legati al tempo di utilizzo e ovviamente dovevano velocizzare di molto quei 56 Kbps.

- Proposta AT&T: divisione dello spettro delle reti locali in POTS, upstream e downstream;
- DMT (*Discrete MultiTono*): lo spettro è diviso in 256 canali indipendenti. Il primo canale utilizzato per POTS, i 5 successivi non vengono utilizzati per limitare le interferenze e tutti gli altri per i dati, e chi fornisce il servizio decide come dividerli tra up e down (solitamente 10%-90%).

Quest'ultima idea fa nascere l'ADSL che può arrivare a circa 8 Mbps in ricezione e 1 Mbps in trasmissione. In realtà questi valori sarebbero maggiori ma il rapporto segnale/rumore non li permettono. Per usufruire dell'ADSL è necessario installare un **NID** e uno **splitter** spesso all'interno di uno stesso pezzo, questo per filtrare le bande e un modem. Se quest'ultimo non è interno al pc allora si deve collegare a esso con ethernet, USB o rete wireless.

2.4.3 Multiplexing

Per limitare i costi le aziende hanno ideato modi per convogliare più conversazioni nello stesso mezzo fisico, appunto il **Multiplexing**. Esistono sostanzialmente 2 categorie di quest'ultimi:

- FDM: Frequency Division Multiplexing;
- TDM: Time Division Multiplexing;

In FDM lo spettro di frequenze è diviso in bande e ogni utente ne possiede una. In TDM gli utenti si danno il cambio, tipo round-robin.

Multiplexing a divisione di frequenza

La banda è limitata dai filtri a 3.1 KHz, e nell'unione in multiplexing viene allocato uno spazio un po' superiore, 4 KHz per avere un po' di tolleranza. Poi ogni canale voce viene aumentato di una frequenza diversa e unito agli altri senza sovrapposizione. Nonostante questi accorgimenti 2 canali adiacenti avranno un po' di sovrapposizione che potrebbe tramutarsi in un po' di rumore nei 2 canali. Uno standard comune prevede 12 canali voce uniti in multiplexing nella banda tra 60-108 KHz. Questa unità è chiamata **gruppo** che possono essere uniti in multiplexing in un **supergruppo** e a loro volta ancora in un **mastergroup**.

Multiplexing a divisione di lunghezza d'onda

Utilizzato per i canali in fibra, il **WDM** (*Wavelength Division Multiplexing*) si fonda sul principio della combinazione e divisione di lunghezze d'onda. Più fibre vengono combinate convogliando ogni segnale in un unico canale nella cui estremità c'è uno splitter utile a ripristinare i segnali delle fibre di partenza. La differenza sostanziale rispetto all'FDM è il sistema ottico completamente passivo. Un sistema con molti canali e lunghezze d'onda ravvicinate è definito **DWDM** (Dense WDM).

Multiplexing a divisione di tempo

Gestita completamente da dispositivi elettronici digitali, per cui è necessaria una conversione da parte della centrale prima di trasmettere il segnale sulla linea di uscita. La centrale locale digitalizza il segnale analogico producendo numero a 8 bit (grazie al **codec**, *coder-decoder*), elaborano 8000 campioni al secondo. Questa tecnica è chiamata PCM e costituisce il cuore del sistema telefonico odierno. Nel mondo esistono molti schemi PCM diversi incompatibili tra loro. In Giappone e in Nord America si utilizza la portante T1 in altre zone del mondo quella E1. Una tecnica chiamata **differential pulse code modulation** al posto di inviare l'ampiezza digitalizzata invia la differenza rispetto alla precedente così da ridurre il numero di bit (da 7 a 5) utili supponendo che sia poco probabile il salto di ± 16 . Una variante di questa tecnica detta **modulazione delta** si basa su un principio simile: ogni valore campionato differisce dal precedente di ± 1 sotto le condizioni che può essere trasmesso un singolo bit che dice se il nuovo campione è maggiore o minore del precedente. Questa tecnica che ipotizza una bassa variazione di segnale può

avere problemi con bruschi cambiamenti di livello. Esistono altre tecniche dette **codifiche per ipotesi** che utilizzando pochi valori precedenti prevedono il successivo.

2.4.4 Commutazione

Commutazione di circuito

Quando viene avviata una telefonata l'apparecchio di commutazione del sistema telefonico prova a creare un percorso fisico tra il chiamante e il chiamato.

Commutazione di messaggio

Questa tecnica non prevede un collegamento fisico a priori ma si basa su un'idea diversa, ovvero un passo alla volta. Il messaggio viene inviato alla prima centrale di commutazione, la quale dopo averlo esaminato per vedere gli eventuali errori, lo ritrasmette alla successiva fino ad arrivare al destinatario. Questa tecnica è chiamata **store and forward**.

Commutazione di pacchetto

Questa tecnica è molto diversa dalle precedenti e si basa sull'idea di dividere i dati in pacchetti limitati i quali partono e possono arrivare anche in ordine sparso sarà compito del destinatario riordinarli. Non c'è bisogno di alcun collegamento predefinito e ogni pacchetto può percorrere strade diverse. E' più resistente agli errori della commutazione di circuito, poiché si possono aggirare commutatori bloccati passando per un altro percorso. Inoltre la commutazione di pacchetto non riserva alcuna ampiezza di banda per cui in linea generale è più efficiente. L'addebito dipende sia dal tempo che dalla distanza.

	Caratteristica	Com. Circuito	Com. Pacchetto
	<i>Instaurazione chiamata</i>	Richiesta	Non richiesta
	<i>Percorso fisico dedicato</i>	Si	No
	<i>Ogni pacchetto segue la stessa strada</i>	Si	No
	<i>I pacchetti arrivano in ordine</i>	Si	No
	<i>Il guasto dello switch è fatale</i>	Si	No
	<i>Banda disponibile</i>	Fissa	Dinamica
	<i>Istante di congestione</i>	Avvio connessione	A ogni pacchetto
	<i>Banda sprecata</i>	Si	No
	<i>Store and Forward</i>	No	Si
	<i>Trasparenza</i>	Si	No
	<i>Tariffa</i>	A minuto	A pacchetto

Figura 9: Confronto tra commutazioni

2.5 Sistema telefonico mobile

Esistono 3 generazioni di telefoni cellulari:

1. Voce analogica;
2. Voce digitale;
3. Voce e dati digitali.

2.5.1 Cellulari di I generazione

Il primo esempio di “cellulare” lo si ha nel 1946 quando venne creato il sistema premi e parla, come ad esempio quella dei CB. Negli anni sessanta scompare il tasto per parlare grazie all’IMTS (*Improved Mobile Telephone System*) che utilizzava un trasmettitore ad alta potenza posto in una collina, il quale utilizzava 2 frequenze, una per la ricezione e una per trasmettere. IMTS utilizzava solo 23 canali distribuiti tra 150 e 450 MHz. Il numero limitato di canali faceva sì che alcuni utenti dovevano aspettare molto prima di aver segnale libero.

Sistema telefonico mobile avanzato

Cambiò tutto grazie a AMPS (*Advanced MPS*). Ogni area geografica era divisa in **celle**, in AMPS grandi 10-20 Km. Ogni cella utilizzava un insieme di frequenze diversa da quelle vicine. L’utilizzo di celle piccole richiede meno potenza. L’idea principale sta proprio qui, in celle piccole e grande riutilizzo delle frequenze. Nelle aree in cui il numero di utenti è elevato e il sistema tende a sovraccaricarsi, le celle vengono a loro volta divise in **microcelle** così da aumentare il riuso delle frequenze. Tanto più piccole sono le celle tanto meno potenti devono essere i dispositivi. Da notare il fatto che una frequenza utilizzata da una cella non è più usata nell’area cuscinetto attorno ad essa (area di circa 2 celle). Al centro di ogni cella si trova una stazione la quale è collegata a un dispositivo chiamato MTSO (*Mobile Telephone Switching Office*) o MSC (Mobile Switching Center). In sistemi più grandi sono necessari più MTSO che quindi vengono divisi in livelli. Ogni MTSO colloquia con gli altri. Un telefonino in ogni istante è logicamente posizionato in una certa cella e ogni qualvolta il segnale in tale cella si affievolisce, la stazione base colloquia con le adiacenti per delegare la gestione dell’apparecchio alla cella col segnale più forte. Questo processo è chiamato **handoff** e richiede 30 msec. Esistono 2 tipi di handoff:

- soft handoff: l’acquisizione della nuova stazione avviene prima di interrompere il segnale precedente;
- hard handoff: la vecchia stazione rilascia il telefono prima che la nuova lo acquisisca. La chiamata viene bruscamente interrotta.

Gestione della chiamata

Ogni telefono AMPS ha un numero seriale di 32 bit e un numero di telefono 10 cifre. Ogni volta che viene acceso, il telefono esplora i vari canali e trova il segnale più potente. Il telefono quindi trasmette in broadcast il proprio seriale

e il numero di telefono con un codice di correzione degli errori. La stazione base aggiorna l' MTSO e ogni 15 minuti circa aggiorna la posizione corrente. Per chiamare il telefono acceso invia il numero del chiamato e i propri dati attraverso il canale di accesso e quando riceve la richiesta la stazione base informa l'MTSO. Se il chiamante appartiene a quell'MTSO cerca un canale libero per la chiamata, e trasmette il numero del canale al telefono. Il processo di ricezione è diverso: ogni telefono è in ascolto nel canale di trasferimento e quando l'MTSO riceve il pacchetto che richiede il destinatario lo passa alla stazione base la quale chiede conferma al telefono. In caso affermativo la stazione invia il numero del canale con la chiamata e inizia la conversazione.

2.5.2 Cellulari di II generazione

Nel mondo sono sostanzialmente utilizzati 4 sistemi: D-AMPS, GSM, CDMA e PDC utilizzato solo in Giappone e molto simile al D-AMPS.

D-AMPS (*Digital AMPS*)

Il D-AMPS è totalmente digitale. Progettato per coesistere con AMPS utilizza gli stessi canali a 30 KHz con le stesse frequenze. Si è resa disponibile una nuova banda di frequenza 1850-1910 MHz per sostenere l'aumento del carico. Alcuni cellulari erano in grado di utilizzare entrambe le bande disponibili. Su un telefono D-AMPS il segnale voce preso dal microfono viene digitalizzato e compresso dal **vocoder**, questa compressione permette la condivisione di una coppia di frequenze (upstream/downstream) fino a 3 utenti con multiplexing a divisione di tempo. Ogni coppia di frequenza supporta 25 frame/sec di 40 msec. Ogni frame è diviso in 6 slot temporali. Gruppi di 16 frame costituiscono un superframe, con alcune informazioni di controllo. Concettualmente funziona come AMPS: viene acceso il telefono, viene contattata la stazione e poi rimane in ascolto. Nei tempi in cui il cellulare non riceve né trasmette viene testata la qualità della linea. Questa tecnica è chiamata **MAHO** (*Mobile Assisted HandOff*)

Comunicazioni GSM (*Global System for Mobile communications*)

Molto simile ad D-AMPS però ha i canali più ampi così possono supportare ben 8 utenti in una coppia di frequenze. Un sistema GSM ha 124 coppie di canali simplex ampi 200 KHz e supporta 8 connessioni grazie a multiplexing a divisione di tempo. A ogni stazione attiva è assegnato uno slot temporale su una coppia di frequenze. Quindi teoricamente supporta 992 canali molti di questi però utilizzati come canali di controllo. Trasmissione e ricezione non avvengono nello stesso intervallo di tempo perché il sistema non è in grado di gestirlo. Questo protocollo ha introdotto le schede SIM che contengono al loro interno IMSI (identifica la SIM) e la chiave di crittografi (Ki). L'identificazione avviene così:

1. Il cellulare manda Ki e IMSI in broadcast;
2. L'operatore lo riceve e manda un numero casuale;
3. Il cell lo rimanda firmato con Ki;

4. L'operatore controlla.

Il **canale di controllo broadcast** è un flusso continuo di dati trasmessi dalla stazione base che annuncia identità e stato del canale. Il **canale di controllo dedicato** è utilizzato per aggiornare la posizione, registrare il terminale nella rete e configurare la chiamata. Infine c'è un **canale di controllo comune** che è diviso in 3 sottocanali logici. Il primo è il **canale di paging** utilizzato dalla stazione per annunciare le chiamate in arrivo. Poi c'è il **canale ad accesso casuale** e permette agli utenti di richiedere uno slot sul canale di controllo dedicato. Infine c'è il **canale di assegnazione dell'accesso** che assegna il lo slot del canale di controllo dedicato per ripetere le richieste effettuate dal secondo canale.

CDMA (*Code Division Multiple Access*)

Miglior sistema rispetto a quelli presentati e base per la III generazione a volte chiamato **cdmaOne**. CDMA permette la trasmissione per tutto il tempo attraverso l'intero spettro. Queste trasmissioni multiple simultanee vengono separate tramite tecnica di codifica. L'idea sta nel fatto che i segnali si sommano linearmente. Per cui tutti comunicano ma ogni coppia lo fa in "lingua diversa". Per risalire a ciò che viene detto basta togliere il rumore aggiunto dalle conversazioni di altri. Per riuscire a filtrare tale segnale rumoroso vengono utilizzate le matrici di Hadamard. Tecnicamente il CDMA funziona così:

ogni tempo di bit è diviso in m intervalli chiamati **chip** (generalmente 64-128 chip per bit) e ad ogni stazione viene assegnata una **sequenza di chip** univoca. Per trasmettere un 1 la stazione deve semplicemente inviare tale sequenza se invece invia uno zero deve farne il complemento. Non sono ammessi altri schemi. Per aumentare la quantità di informazione inviabile basta passare da b bit/sec a mb chip/sec aumentando l'ampiezza di banda di un fattore m . CDMA è una forma di comunicazione a spettro distribuito. Ognuna di queste sequenze di chip sono mutualmente ortogonali, ovvero ogni prodotto interno normalizzato di qualunque coppia di sequenze è uguale a 0 (ottenute con i **codici Walsh**).

$$S * T = \frac{1}{m} \sum_{i=1}^m S_i T_i = 0$$

Da cui si deduce che $S * S = 1$ e $S * \bar{S} = -1$. Ora, ogni stazione invia queste sequenze come bit le quali si "mischiano" con le altre, tecnicamente si sommano con gli altri segnali di altre stazioni. Una volta che il segnale arriva alla stazione di destinazione per sapere il bit inviato dalla sorgente basterà moltiplicare il segnale per la sequenza di chip della sorgente e si otterrà il bit inviato. Matematicamente se si deve capire il messaggio C allora sarebbe $S = A + \bar{B} + C$:

$$S * C = (A + \bar{B} + C) * C = A * C + \bar{B} * C + C * C = 0 + 0 + 1 = 1$$

Per la proprietà di ortogonalità tutti i prodotti si sono annullati a parte quello interessato. Questo sistema è in genere utilizzato per reti wireless.

2.5.3 Cellulari di III generazione

La prima proposta di cellulari di III generazione fu fatta dall'ITU con l'intenzione di lanciaarli nell'anno 2000 con ampiezza di banda di 2 MHz e 2Mbps per tutti. Un sogno irrealizzabile che ha visto il tutto slittare qualche anno più avanti e con alcune specifiche smussate come i 2Mbps per chi stava fermo e circa 400 per gli utenti che camminavano e 144 per quelli che si spostano a più alte velocità. I servizi che avrebbe dovuto fornire IMT-2000 (così si chiamava la proposta) erano:

- trasmissione voce ad alta qualità;
- trasmissione messaggi;
- applicazioni multimediali;
- accesso internet.

Per riuscire ad utilizzare questi servizi in tutto il mondo si era pensati di creare un'unica tecnologia per rendere tutto più semplice. Furono fatte diverse proposte.

W-CDMA (*Wideband CDMA*)

Questo protocollo fu proposto da Ericsson. In Europa battezzato col nome **UMTS** (*Universal Mobile Telecommunications System*). Si basa sui fondamenti del CDMA utilizzando però una banda larga a 5 MHz ed è stato progettato per interagire con il sistema GSM anche se non compatibile. Data rate 384 Kbps.

CDMA2000

Proposto da Qualcomm, simile al precedente con la differenza di non interagire con GSM. Altre differenze col precedente sono il tempo di frame, di spettro e una diversa tecnica di sincronizzazione. Data rate 144 Kbps.

EDGE (*Enhanced Data for GSM Evolution*)

Uguale al GSM con un numero maggiore di bit per baud che comportano però più errori per baud. Sistema pensato durante il passaggio da II a III generazione, definito infatti 2.5G.

GPRS *General Packet Radio Service*

Altro schema per 2.5G. Una rete di pacchetti costruita sopra ad D-AMPS e GSM. GPRS permette di inviare e ricevere pacchetti IP in una cella basata su sistema vocale. Quando attivo alcuni slot temporali vengono dedicati al traffico dei pacchetti. Questi slot sono divisi in canali logici. Ogni canale è utilizzato per scaricare i pacchetti nei quali c'è indicato il destinatario. Per inviare un pacchetto la stazione mobile richiede uno o più slot e effettua la richiesta alla base. La base poi invia il pacchetto via internet tramite rete via cavo.

2.5.4 Oltre al 3G

HSDPA (*High Speed Downlink Packet Access*)

HSUPA (*High Speed Uplink Packet Access*)

HSOPA (*High Speed OFDM Packet Access*)

3 Lo strato data link

4 Il sottostrato MAC (*Medium Access Control*)

5 Lo strato network

6 Lo strato trasporto

7 Lo strato applicazione

8 Sicurezza delle reti

A Glossario

B Domande degli appelli

B.1 Capitolo 2

B.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:

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

B.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:

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

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

B.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.

B.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.

B.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.

B.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.

B.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 cellulari 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 agli 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 sopraccitate.

B.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 $S * T = S * (-1 * T) = 0$ se $S \neq T$).

B.1.9 Il GPRS: cos'è, difetti e pregi

Il GPRS è un'evoluzione del GSM 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 sola 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 si autentica.

B.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.

B.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.

B.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 fase.

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.

C Capitolo 3

C.0.13 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 volta un altro escape per non far ignorare le successive. Un difetto di questo metodo è legato all'uso di caratteri a 8 bit. Ad esempio Unicode usa una codifica a 16bit.

C.0.14 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.

C.0.15 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 $2d+1$.

C.0.16 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 più 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 divide 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.

C.0.17 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.

C.0.18 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.

C.0.19 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 uscita 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 approcci: go back n e selective repeat.

C.0.20 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 efficace contro la prevenzione di errori, ma occupa molta banda se la frequenza di errori è alta.

C.0.21 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.

D Capitolo 4

E Capitolo 5

F Capitolo 6

G Capitolo 7

H Capitolo 8