Appunti di Reti di Telecomunicazioni

Giulio Ermanno Pibiri

luglio 2012

Data Communications Quando comunichiamo non facciamo altro che condividere informazione. Questa condivisione può essere locale oppure remota. La comunicazione locale è quella che avviene, per esempio, tra individui che parlano tra di loro, mentre la comunicazione remota ha luogo a distanza. Lo stesso termine *telecomunicazione*, include telefonia, telegrafia e televisione e significa *comunicazione a distanza*. *Tele* è una parola greca che significa *lontano*. Per il termine *data* si intende qualsiasi rappresentazione condivisa dell'informazione, tra coloro che comunicano. Una *data communication* è uno scambio di informazioni tra due o più dispositivi, attraverso qualche mezzo di comunicazione (ad esempio un cavo). Affinché la comunicazione abbia esito, i dispositivi devono essere adeguatamente equipaggiati: essi sono costituiti da una parte hardware e una software. La qualità di una data communication dipende da 4 caratteristiche principali:

1. Delivery: il sistema deve poter trasmettere correttamente l'informazione ai destinatari.
2. Accuracy: il sistema deve poter trasmettere i dati in maniera accurata. I dati corrotti o alterati dalla comunicazione sono di fatto inutilizzabili.
3. Timeliness: il sistema deve trasmetter i propri dati in tempo ragionevole. Spesso i dati trasmessi in ritardo sono inutili. Quando i dati vengono ricevuti praticamente nello stesso istante nel quale sono stati inviati, si parla di *real-time* communication.
4. Jitter: il termine si riferisce alla variazione del tempo di arrivo del pacchetto di informazione. Si riferisce spesso al ritardo di arrivo dei pacchetti informativi che trattano audio o video.

Architettura e componenti Le reti sono organizzati secondo un modello gerarchico a strati (layers). Ogni livello comprende un insieme di funzioni e servizi tra loro omogenei. La motivazione di pensare ad una rete di TLC come ad una struttura a livelli risiede nella grande flessibilità che permette. Dopo aver definito le regole di tra i livelli adiacenti, un dato livello può essere aggiornato con un impatto minimo sull'intera architettura.

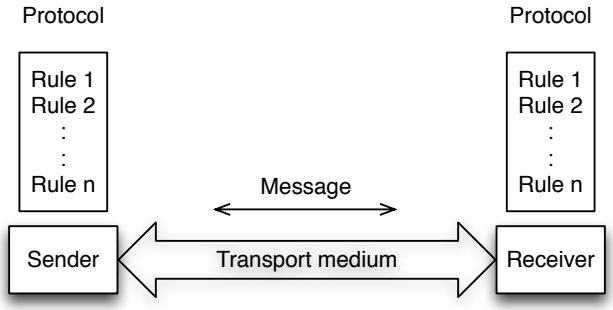
Un sistema di comunicazione ha 5 componenti essenziali:

1. Message: è il messaggio informativo che deve essere comunicato. Le attuali forme dei messaggi includono testo, audio, video e immagini.
2. Sender: è il dispositivo che invia il Message.
3. Receiver: è il dispositivo che riceve il Message.
4. Transmission Medium: è il mezzo fisico attraverso il quale il Message giunge al destinatario.
5. Protocol: un protocollo è una insieme di regole che definiscono la comunicazione di informazioni. Rappresenta un accordo comune ai mezzi che devono comunicare: è ciò che rende possibile la comunicazione. Senza di esso, i diversi dispositivi potrebbero essere tra loro connessi, ma senza scambio informativo (similitudine con persone che parlano lingue diverse). Consente il trasferimento dell'informazione tra livelli di pari importanza (peer) delle due pile protocollari sorgente e destinazione. Sono il motore di attivazione per i servizi.

La comunicazione tra due diversi dispositivi può essere di diversi tipi: *simplex*; *half-duplex* o *full-duplex*. La modalità simplex si riferisce ad una comunicazione unidirezionale: è come una strada a senso unico. Soltanto un dispositivo può trasmettere e l'altro può soltanto ricevere (esempio monitor e tastiera di un pc). L'intera capacità del canale viene sfruttata per l'invio dei dati in una direzione. La modalità half-duplex abilita alla trasmissione e alla ricezione entrambi i dispositivi, ma non allo stesso tempo (esempio walkie-talkies). L'intera capacità del mezzo comunicativo può quindi essere usata per entrambe le direzioni. La modalità full-duplex invece garantisce che i due dispositivi possano ricevere e inviare dati contemporaneamente (esempio comune di telefonata tra due persone). La capacità del mezzo viene chiaramente divisa tra le due direzioni.

Un qualsiasi servizio è implementato in un livello attraverso operazioni specifiche che lo caratterizzano. Queste operazioni specifiche prendono il nome di primitive. Si possono distinguere 4 tipologie fondamentali per le primitive.

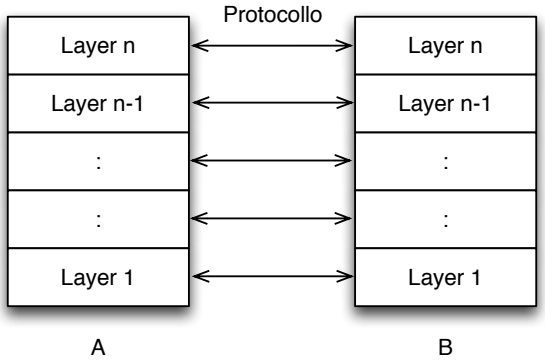
Figura 1: Sistema di comunicazione



- Request: viene attivata per richiedere un servizio specifico;
- Indication: evidenzia la necessità di attivare un servizio;
- Response: indica la risposta ad una richiesta;
- Confirm: chiude la sequenza confermando il servizio.

Mettendo tutto assieme, possiamo riassumere dicendo che un *servizio* è un insieme di primitive che un livello offre ai livelli adiacenti. Il servizio definisce quali operazioni il livello è in grado di fornire in relazione alle modalità di interfaccia. Tipicamente non vengono specificate le modalità con le quali un servizio viene implementato.

Figura 2: Struttura a layers



Networks Una *rete di telecomunicazione* è un insieme di dispositivi, i *nodi*, connessi tra loro attraverso mezzi di comunicazione (*communication links*). Molte reti si suddividono il carico da processare tra i nodi: invece di avere un'unica unità operativa per il processo, il carico viene distribuito su computers separati. Chiaramente una rete di telecomunicazione (nel seguito, RTLC) deve possedere alcune caratteristiche fondamentali. Le più importanti sono: *performance*, *reliability* e *security*.

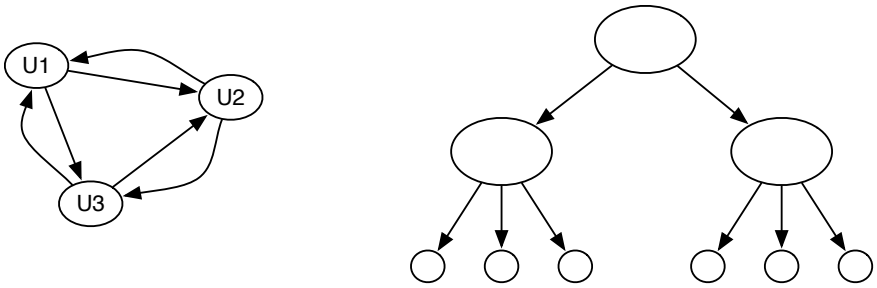
La *performance* può essere valutata in molti modi. Un modo è fare riferimento alle metriche di *throughput* e *delay*. Chiaramente, vorremmo un elevato throughput e un basso delay, ma sfortunatamente i due parametri sono direttamente proporzionali: più carico è presente sulla rete e maggiori sono i ritardi comunicativi, come insegna l'esperienza di ogni giorno.

La *reliability* di una RTLC è misurata come la frequenza di fallimento, il tempo che intercorre tra un guasto e il suo ripristino e la robustezza della rete in caso di catastrofe.

La *security* misura il grado di protezione cui i dati sono affetti durante la loro trasmissione sulla rete.

I vantaggi di una RTLC sono evidenti: uso condiviso delle risorse e collaborazione tra i processi. Uno dei maggiori svantaggi è invece da considerarsi l'elevata complessità di gestione nel caso, specialmente, in cui un elevato numero di dispositivi forma la rete. Intuitivamente, per realizzare una rete in modalità base tra tutti gli utenti, supponiamo essi siano in numero N, è creare tante coppie di collegamenti. L'immediato vantaggio è che tutti gli utenti sono in tal modo connessi, ma la soluzione diventa ben presto impraticabile quando il numero N diventa molto grande. Il numero dei collegamenti è infatti $\frac{N(N-1)}{2}$. La soluzione è infatti quella di prevedere i nodi, dispositivi di aggregazione. L'utilizzo dei nodi di aggregazione dà vita ad una struttura gerarchica delle RTLC.

Figura 3: Connessione base e struttura gerarchica



Commutazione In telecomunicazioni il termine commutazione indica l'insieme delle funzionalità e relative tecniche su cui è basato il funzionamento logico dei nodi di una rete di telecomunicazione, ovvero un'operazione all'interno di un nodo che tratta l'informazione da trasmettere sotto forma di segnale, affinché sia indirizzata verso la destinazione desiderata. In altre parole essa associa un ramo d'ingresso ad uno d'uscita al segnale in transito ed è attuata per mezzo delle funzioni d'indirizzamento e di instradamento. In altri termini, l'operazione di commutazione nel suo insieme permette di costruire dei percorsi di informazioni tra diversi utenti all'interno della stessa rete di telecomunicazione. La più importante e funzionalità base di una RTLC è proprio tale operazione di commutazione.

Tipi di connessione I nodi della rete sono tra loro connessi tramite dei *links*, assumibili come i sentieri di comunicazione attraverso i quali i dati sono trasferiti da un dispositivo ad un altro e visualizzabili come delle linee che connettono diversi punti su un foglio. Affinché la comunicazione avvenga, i dispositivi devono essere connessi tra loro nello stesso modo, allo stesso tempo. Esistono due tipi possibili di connessione:

1. la connessione *punto-punto* rappresenta un link dedicato di comunicazione tra due dispositivi e quindi la modalità di comunicazione prevede lo scambio di informazione tra le sole due entità collegate;
2. la connessione *multi-punto* sfrutta un singolo link per mettere in comunicazione diversi dispositivi. Tale connessione suddivide quindi il carico spaziale e temporale tra i diversi dispositivi. Se i dispositivi possono usare il link contemporaneamente, allora si parla di un connessione con condivisione spaziale; se i dispositivi sono regolati da turni, allora si parla di connessione timeshared. Lo scambio di comunicazione avviene tra un'entità e un sottoinsieme delle altre entità della rete.

La modalità di comunicazione *broadcast* prevede lo scambio di informazione da un'entità della rete a tutte le altre.

Classificazione Le RTLC si possono classificare in base ai seguenti criteri: *servizio offerto*; *topologia*; *area di copertura geografica*.

Topologia Il termine *topologia* fisica, si riferisce al modo col quale una rete viene realizzata fisicamente. Due o più dispositivi sono connessi tramite un link e due o più links costituiscono una topologia. La topologia di una rete è una *rappresentazione geometrica* delle relazioni esistenti tra i links e i dispositivi loro connessi. Esistono 5 topologie di base: *mesh*; *star*; *bus*, *ring* e *tree*.

1. Mesh: in una topologia mesh ogni dispositivo ha una connessione dedicata punto-punto. Il termine *dedicato* significa che il link ospita solo il traffico di informazione presente tra i due nodi. In una rete di n nodi, il numero dei links fisici può essere così calcolato: ogni nodo è connesso ai restanti $n-1$ nodi, perciò abbiamo un numero di links fisici pari a $n(n-1)$. Se la tipologia del link è quella duplex, allora possiamo dividere il numero ottenuto per 2, ottenendo quindi:

$$\frac{n(n-1)}{2}$$

duplex-mode links. Per poter essere connesso a $n-1$ nodi, un singolo dispositivo deve essere equipaggiato con esattamente $n-1$ porte di I/O. Gli ovvi vantaggi che offre questa topologia di architettura sono diversi: anzi tutto l'uso dei links dedicati si riflette in una eliminazione del traffico sull'intera rete; l'architettura è robusta dato che un guasto ad un link non compromette gli altri; l'uso dei links dedicati ha come conseguenza anche la sicurezza delle informazioni che vi viaggiano, dato che soltanto quel mezzo di comunicazione può ospitare quei dati. Tra gli svantaggi ricordiamo la complessità quadratica della rete: se aumenta il numero dei nodi, la complessità dei collegamenti aumenta in modo quadratico. Inoltre è presente un elevato numero di porte, $n-1$, per ciascun dispositivo, le cui installazioni e manutenzioni sono assai costose.

2. Star: in questo tipo di topologia, i diversi dispositivi hanno un link dedicato ad un controllore centrale, chiamato spesso *hub*. I nodi quindi non sono direttamente connessi gli uni agli altri. Se due diversi dispositivi vogliono comunicare tra loro, devono necessariamente passare prima dal controller: il dispositivo invia i dati al controller e questi li ritrasmette all'altro dispositivo. Rispetto ad un'architettura mesh, quella star prevede un numero di cablaggi molto minore e questo si riflette anche sul numero di porte I/O presenti su ciascun dispositivo. È sufficiente una sola porta per un dispositivo: minore costo di installazione e riconfigurazione. Una configurazione star è ugualmente robusta rispetto ad una mesh, dato che la rottura di un collegamento non ha conseguenze su tutti gli altri. Il grosso svantaggio di una rete di questo tipo si ha nel caso di rottura dell'hub. Se esso muore, l'intero sistema muore con lui.

3. Bus: le due topologie descritte erano entrambe punto-punto. Al contrario, una topologia bus è multi-punto. L'architettura a bus è costituita da un cavo connettore centrale, chiamato backbone (spina dorsale), al quale tutti i dispositivi della rete sono connessi mediante *drop lines* e *taps*. Le drop lines sono semplici connessioni che corrono tra un dispositivo e il backbone, mentre i taps sono i connettori, attraverso i quali il cablaggio è possibile. Parte dell'energia che attraversa il backbone viene dispersa dai taps: in questo modo capiamo che esiste un limite costruttivo del numero di taps che un bus è in grado di supportare e sulla distanza tra questi taps. I vantaggi di questa topologia sono nell'uso ridotto dei links utilizzati e nella facile implementazione. Non è invece garantita la robustezza della rete in questo caso. È ugualmente difficile l'isolamento del guasto. Se il backbone si rompe, tutta la rete non funziona più. Potrebbe pure essere difficile e costoso aggiungere nuovi dispositivi alla rete, dato la dispersione e il deterioramento del segnale informativo a causa dei taps.

4. Ring: in questo caso di topologia ogni dispositivo della rete possiede due connessioni punto-punto ai propri dispositivi adiacenti. Ogni dispositivo è pure dotato di un ripetitore. Quando due dispositivi intendono comunicare, i bits informativi sono rigenerati dal ripetitore che provvede a trasmetterli al dispositivo adiacente e così via, fino al dispositivo ricevitore dell'informazione. I rings sono abbastanza semplici da installare e riconfigurare: aggiungere o eliminare un dispositivo richiede la modifica di soli due collegamenti. Il limite è ancora una volta rappresentato dal numero dei dispositivi connessi e la lunghezza dell'anello. L'individuazione del fallimento è circostanziata però: dato che in generale, un segnale è sempre in circolo sull'anello, se uno dei dispositivi non rigenera il segnale mediante il proprio ripetitore, allora può segnalare un guasto. Tuttavia, il traffico unidirezionale di questa topologia può rappresentare uno svantaggio: una rottura dell'anello rende inutilizzabile l'intera rete. Spesso allora si prevede la costruzione di un doppio anello.

5. Tree: l'inoltro dell'informazione è vincolata a seconda di come sono disposti gli utenti della rete.

Infine è bene ricordare che le varie topologie possono essere fuse tra loro, dando origine a delle architetture ibride.

Geografia delle reti Le reti di *computers* sono costruite per differenti entità. Questo è il motivo per cui sono necessari degli standards per permettere la comunicazione di queste reti eterogenee tra di loro. I due standards più famosi sono il modello OSI (Open System Interconnection) e il modello Internet. Oggigiorno, quando parliamo di reti, ci riferiamo principalmente a due categorie: LAN (local area network) e WAN (wide area network). L'estensione geografica della loro area di copertura è la caratteristica principale di queste reti. Inoltre offrono un buon buon tasso di controllo degli errori.

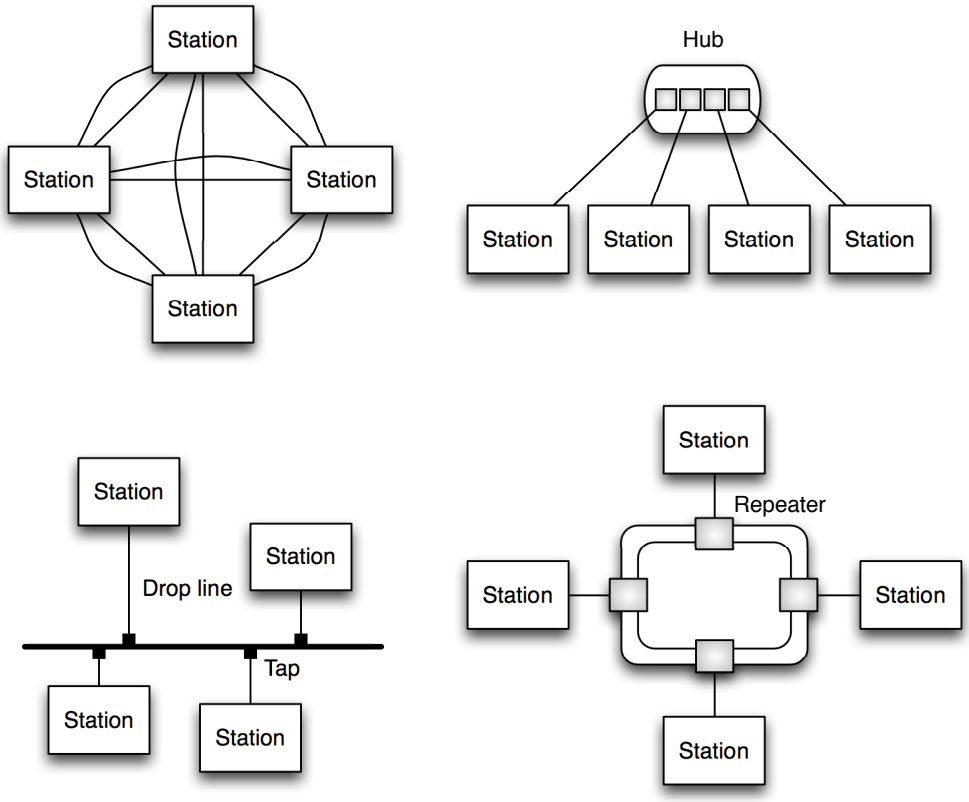
Le reti LAN sono le classiche reti private che, famiglie, uffici o strutture commerciali possono ospitare. Attualmente le dimensioni di una rete LAN si estendono per pochi chilometri. Solitamente queste reti fanno uso di un unico mezzo di comunicazione e sono costruite per mezzo di architetture a bus, ring o star. Le LANs attuali hanno una velocità di flusso informativo pari a 100 o 1000 Mbps (megabits per second). La LAN Wireless è l'evoluzione della tecnologia LAN. Le reti WAN provvedono a coprire distanze molto estese, come regioni, continenti o addirittura tutto il mondo. Le WANs possono essere costruite in modo complesso come lo è Internet, oppure anche in maniera semplice. Ricordiamo pure un'altra tipologia di reti, che è la MAN (metropolitan area network). Le MANs sono da considerarsi una via di mezzo per dimensione tra una LAN e una WAN. Solitamente sono le reti che troviamo nel territorio di una città. Sono costruite per poter offrire connessioni ad alta velocità: un buon esempio di loro utilizzo è quello fatto dalle compagnie telefoniche, che vendono ai clienti linee DSL molto veloci.

Lo standard di riferimento per queste reti è lo standard IEEE 802 (*Institute of Electrical and Electronics Engineering*).

L'architettura di queste reti si compone di 4 livelli.

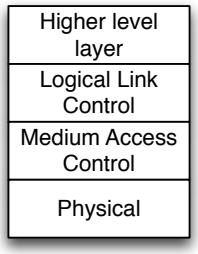
1. Higher level layers.

Figura 4: Topologie di rete



2. LLC (Logical Link Control): ha il compito di gestire l'integrità dell'informazione scambiata tra nodi della rete. Deve definire la connessione e controllarne l'integrità. Questo livello serve essenzialmente a trasmettere al livello più alto le funzionalità offerte dallo strato MAC.
3. MAC (Medium Access Control): è di fatto la parte caratterizzante l'architettura specifica. Prevede la definizione di una tecnica per la condivisione dell'accesso ad un mezzo fisico condiviso. Le tecniche MAC si suddividono in due grandi categorie: *ordinate* e *casuali*.
4. Physical.

Figura 5: Struttura LAN



Tecniche MAC L'accesso al messo condiviso può avvenire in due modalità: *geted*, quando l'accesso è limitato per un tempo massimo definito; *esaustivo*, quando non vengono introdotte nessun tipo di limitazioni.

Tra le tecniche MAC usate per la definizione di una tecnica di accesso ad uno stesso mezzo fisico condiviso, ricordiamo:

- ordinate: tra queste tecniche la più usata è quella *polling* ad interrogazione, assieme a *token-ring* e TDMA, FDMA. Prevedono regole fisse per distribuire equamente l'uso del mezzo in modo equo. L'utilizzo è esclusivo e così non vi sono problemi di conflitto sull'accesso (collisioni). Solitamente prevede una tipologia di rete organizzata a bus. Il polling prevede l'invio di un messaggio di autorizzazione all'accesso al canale ad ogni nodo connesso alla rete e un successivo messaggio di rilascio. Esistono due modalità: *hub-polling* e *roll-call*.

  - hub-polling: esiste un nodo centrale, chiamato hub che ha il compito di gestire i messaggi di accesso e rilascio ai vari nodi della rete. L'hub serializza le diverse richieste di invio dati dei nodi. In questo modo possono pesare assai i tempi di commutazione delle rete.
  - roll-call: prevede una fase cooperativa dei nodi per gestire l'accesso/rilascio dell'uso del canale. In questo modo vengono ridotti i tempi di latenza dell'hub polling. Viene sempre abilitata la stazione più lontana. Le altre stazioni sono in ascolto del suo messaggio di terminazione.

  La modalità *token-ring* utilizza chiaramente una tipologia di rete ad anello. Non esiste una stazione master come l'hub, ma i diversi nodi sono messi in connessione tramite la presa di un *token* (testimone). Dopo il rilascio del token, esso viene rimesso nella rete.

- non ordinate: si annoverano l'*aloha* (assieme alla sua variante *aloha-slotted*) e il CSMA. La modalità casuale aloha prevede l'accesso condiviso da più utenti verso un unico punto di accesso, chiamato spesso nodo satellite. Il nodo che riceve il messaggio informativo invia in broadcast a tutti gli altri nodi, una notifica di avvenuta ricezione (riscontro diretto). Per il rilevamento di una collisione si sfrutta il fatto che il tempo della trasmissione è noto. Per la risoluzione di una collisione si vincola a trasmissione ad effettuarne un'altra in un intervallo di tempo statisticamente indipendente per evitare un'altra collisione. La sua variate aloha-slotted regola l'accesso al canale mediante un ordinamento temporale prefissato, organizzato tramite degli slots. Questa versione consente quindi un miglior utilizzo della risorsa trasmissiva, ossia del canale. Non esiste quindi nessun tipo di regolazione all'acceso: appena un nodo ne ha la possibilità tenta di connettersi. Questo può comportare una certa competizione nell'accesso con conseguente collisione. Se si verifica una collisione può avvenire la mutua distruzione delle informazioni. Le differenti tecniche di accesso casuale prevedono modalità specifiche per evitare le collisioni (caso CSMA) e regolare le collisioni nel caso in cui avvengano.

  Il CSMA (*Carrier Sensing Multiple Access*) è una tecnica che prevede l'ascolto del canale da parte dei nodi, prima di effettuarne l'accesso (è il principio di buona maniera *ascolta-prima-di-parlare*). Se il canale rileva la presenza di segnale di un altro utente connesso, allora non si procede alla fase di accesso e si interpreta questo evento come una *collisione virtuale*. Viene quindi ridotta la possibilità di collisione, ma non eliminata.

Esempio di uso CSMA Consideriamo due nodi A e B. Supponiamo che la trasmissione dei dati avvenga a pacchetti, la cui durata temporale è τ. Il tempo di propagazione tra i due nodi è noto e uguale a σ. Il tempo di propagazione σ sarà molto minore di τ: $\tau >> \sigma$. Immaginiamo di osservare la rete dal punto di vista del nodo A. Il nodo A, immediatamente dopo il termine della fase di accesso, ascolta il canale e se rileva segnale significa che pure il nodo B è connesso e quindi è avvenuta una collisione. L'intervallo di tempo σ rappresenta quindi il tempo di vulnerabilità della rete. Si assume come valore di riferimento il massimo valore di σ, che di solito viene indicato con a. Affinchè si abbia un buon comportamento nella rete, deve essere soddisfatta la condizione:

$$a << \tau.$$

Rilevamento di una collisione Una collisione viene rilevata non appena due nodi fanno richiesta di connessione ad un mezzo trasmissivo condiviso. Il riconoscimento è esplicito e prevede l'invio di un messaggio di riscontro su un canale separato in modalità broadcast. Se la collisione si verifica, si entra in una modalità chiamata di *risoluzione*.

Esiste la modalità a riscontro diretto utilizzato in aloha; oppure la rilevazione di segnale che avviene in CSMA. In questo caso, una volta trasmessa l'informazione, il nodo rimane in ascolto sul canale per un tempo prefissato α. Se avviene una collisione viene percepito ancora il segnale e così i diversi nodi possono accorgersene.

Tecniche per prevenire una collisione

- 1-Persistent: la stazione si mantiene in ascolto nel canale fintantochè non lo trova libero. Allora accede. Rappresenta un buon approccio laddove si intende ridurre i tempi di latenza e la probabilità che due stazioni diventino attive contemporaneamente è bassa. Se è alta, potrebbe verificarsi il monopolio del canale da parte di una delle due stazioni.

- Non-Persistent: ogni volta che una stazione rileva il canale occupato, riprogramma un nuovo tentativo di accesso con modalità casuale (collisione virtuale). Ha un buon funzionamento quando vi sono diverse e frequenti richieste d'accesso.

- P-Persistent: è simile alla modalità precedente, ma viene introdotta una probabilità legata agli accessi. Se il canale viene rilevato come libero, allora un nodo vi accede con probabilità P (fissata), oppure con probabilità 1-P si ritiene verificata una collisione virtuale.

- CSMA/CD (Collision Detection): viene mantenuta la stazione in ascolto per tutta la durata della trasmissione. Così facendo, si riduce la perdita dei dati in seguito ad una collisione, se viene rilevata.

Internet working È un insieme di metodologie volte a migliorare o estendere le reti di TLC. Vi sono in gioco 3 apparecchi principali.

- *Repeater*: è un dispositivo in grado di estendere il segnale di una rete LAN. Ha il vantaggio di poter estendere l'area di utilizzo della rete, ma d'altro lato posso anche aumentare eccessivamente il numero degli utenti. Chiaramente le reti LAN devono essere omogenee dal livello MAC in poi e compatibili a livello fisico.

- *Bridge*: sono dei dispositivi in grado di disaccoppiare i domini di collisione . Ogni frame informativo è vincolato a nascere e morire nella propria rete; diventa condiviso quando reti diverse vogliono comunicare. In questo caso il bridge cerca di mantenere le prestazioni nonostante l'aumento di utenti.

- *Router*: ha la capacità di interpretare le richieste di connessione a livello di rete. Seleziona cosa ripetere leggendo la testata dei pacchetti, evitando così traffico inutile che crea congestione. È una forma più semplice e aggiornata degli auto-commutatori.

Rete telefonica La rete telefonica usa circuiti di commutazione. Essa trae le sue origini nel lontano 1800. Agli inizi, era un sistema che faceva uso dei segnali analogici per trasmettere la voce degli utenti. Con l'avvento dell'era del computer, negli anni '80 del Ventesimo Secolo, cominciò a trasportare dati in aggiunta alla voce. A partire da quegli anni in poi, la rete telefonica ha introdotto molti cambiamenti tecnici e adesso risulta tanto digitale quanto analogica. La rete telefonica è regolata dagli standard emanati da CCITT (*Comité consultatif international téléphonique et télégraphique*). Il risultato del processo di standardizzazione è che la banda lorda di un canale per il trasporto del segnale telefonico è di 4 kHz. In realtà, la banda utile è considerata 300-3400 Hz.

Nelle telecomunicazioni, il *multiplexing*, è il meccanismo o la tecnica per cui la capacità disponibile di un collegamento in uscita viene condivisa tra diversi canali trasmissivi in ingresso, combinando più segnali analogici o flussi di dati digitali, detti segnali tributari, in un solo segnale trasmesso su un singolo collegamento fisico. In tutti i casi in una comunicazione dati il multiplexing permette di risparmiare sul cablaggio riducendo il numero di linee di segnale e sul numero di componenti. In un sistema multiplexed, n linee condividono la banda di un unico link (many-to-one).

L'operazione di multiplexing applicata a segnali individuali, consente un migliore utilizzo dei mezzi trasmissivi e di individuare nuove topologie di rete più efficienti.

Una tecnica molto usata nella telefonia è la FDM (Frequency Division Multiplexing). Consiste nel dividere la banda del canale a disposizione in sottobande di uguale ampiezza, tipicamente dette *canali*, assegnandole in maniera biunivoca agli utenti. Ogni sorgente S_i genera un segnale ad una data frequenza f_i. Allora si ripartisce la banda disponibile del canale tra le diverse sorgenti, evitando sovrapposizioni: il segnale multiplex viene costruito traslando lo spettro delle S_i in n intervalli di frequenza disgiunti e contigui. Vi sono particolari specifiche redatte dal CCITT per quanto riguarda il valore di n e la disposizione del segnale risultante sull'asse delle frequenze. Se risultano 12 canali si parla di gruppo base; con 60 canali si super-gruppo e con 300 canali di master-gruppo.

Applicando il teorema del campionamento a segnali analogici limitati in banda, ottengo che la trasmissione del segnale da continua diventa intermittente. Applicando allora la quantizzazione e la conseguente codifica binaria, associo ad ogni campione del segnale una sua rappresentazione numerica-digitale, ovvero una sequenza di simboli binari. Nel caso specifico della telefonia, il numero dei simboli binari, ovvero di bits, è 8. Il passo di campionamento del segnale si ottiene dalla condizione di campionamento: $T_c = \frac{1}{2f_m}$, nel nostro caso $f_m = 4$ kHz. Ottengo così un intervallo di campionamento pari a 125 μ secondi. Dividendo tale valore per il numero dei bits utilizzati per rappresentare un campione numerico, riesco a sapere il tempo di trasmissione di un singolo bit: $\tau = \frac{125\mu s}{8}$. La banda di frequenza necessaria sarà allora: $B = \frac{1}{\tau} = 64$ kHz.

La tecnica che permette di condividere uno stesso mezzo fisico tra più utenti è detta: TDM (Time Division Multiplexing). Se intendo aggregare N utenti tra loro, la banda di cui devo disporre è NB, con $B = 64$ kHz. Il tempo viene suddiviso in frame, i canali, di durata prefissata. Lo standard attuale prevede l'utilizzo di 32 canali a 8 bits ciascuno. In questo modo, in uno stesso intervallo di tempo si hanno $32 \cdot 8 = 256$ bits e quindi la banda risultante sarà: $B = \frac{1}{\frac{125\mu s}{256} bit} = 2048 \frac{Mbit}{s}$.

Attualmente, la rete telefonica possiede una struttura gerarchica: ogni nodo ha un ruolo differente. Non è automatico supporre che la comunicazione tra nodi di pari livello è concessa. I piani nei quali la rete è suddivisa sono:

1. Centro nazionale (CN);

2. Centro di compartimento (CC);

3. Centro di distretto (CD);

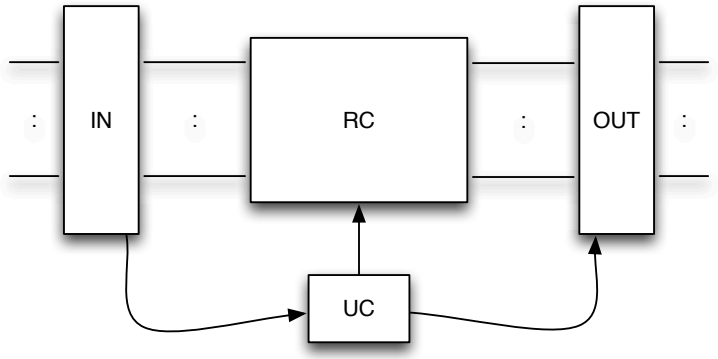
4. Centro di settore (CS);

5. Centro di rete urbana (CRU).

I centri indicati sono i cosiddetti switching-office, ovvero dei centri di commutazione ciascuno dei quali contenente diversi commutatori. I commutatori mettono in comunicazione tra loro i diversi piani gerarchici. Prima di passare al piano successivo, si cerca di completare la comunicazione al livello più basso, impegnando il minor numero di nodi possibili.

Commutatore È di fatto, l'elemento che sta alla base di una rete di telecomunicazione, perché implementa l'operazione di commutazione.

Figura 6: Struttura di un auto-commutatore



La struttura di un auto commutatore è formata da una *rete di connessione* centrale (RC); due *blocchi di terminazione* per le linee di ingresso (IN) e di uscita (OUT) e da un'*unità di controllo* (UC). Il blocco iniziale per le linee di ingresso serve ad estrarre e segnalare all'unità di controllo le diverse richieste di connessione. L'unità di controllo è l'elaboratore software principale che interpreta la richiesta di connessione che le arriva dal blocco di ingresso e la trasferisce alla rete di connessione centrale; successivamente ricostruisce la segnalazione e la invia al blocco di uscita. Da ultimo comunica alla rete di connessione quando terminare la connessione (comunicazione).

Se il numero delle linee del blocco IN, sia esso n_{IN}, è maggiore del numero delle linee di uscita del blocco OUT, $n_{IN} > n_{OUT}$, allora ho un *concentratore*. Viceversa, se $n_{IN} < n_{OUT}$, allora ottengo un *distributore*.

Tra i compiti principali di un auto commutatore abbiamo quindi menzionato: mettere in collegamento, instradare il collegamento, tra le linee di ingresso e le linee di uscita (mettere in comunicazione il chiamato con il chiamante) all'avvio della comunicazione; supervisionare il collegamento; resettare da ultimo lo stato della rete di comunicazione.

Essenzialmente due sono i modi per realizzare fisicamente la rete di connessione centrale: la divisione di tempo (strutture T) e la divisione di spazio (strutture S).

Strutture S Le strutture S a divisione si spazio realizzano la connessione fisica tra una linea di ingresso e la linea di uscita desiderata.

I collegamenti sono disposti a matrice: si deve stabilire la connessione elettrica (un tempo avveniva tramite relè) tra l'utente sorgente e l'utente destinazione. Per tutto il tempo della comunicazione, il collegamento deve rimanere chiuso, dopodichè lo riapro per ripristinare lo stato iniziale.

Il *relè* è un dispositivo elettrico comandato dalle variazioni di corrente per influenzare le condizioni di un altro circuito. In sostanza il relè è un interruttore che non viene azionato a mano ma da un elettromagnete.

Detto N il numero di linee di ingresso e linee di uscita, poiché devo garantire la possibilità di comunicazione tra qualsiasi coppia di linea ingresso e linea uscita, ottengo un numero di punti di connessione pari a $N \cdot N = N^2$.

La tecnologia realizzativa è stata inizialmente costituita dall'uso dell'elettromeccanica, fondata sull'utilizzo dei relè. L'impiego dei BJT in sostituzione all'uso dei relè per la comunicazione, ha permesso a questa struttura di avere tempi di aggiornamento molto più rapidi (chiamati *tempi di riconfigurazione*), adattandosi per la telefonia sia analogica che digitale. Nella telefonia analogica avviene un flusso continuo di corrente elettrica tra la sorgente e la destinazione e così gli utenti rimangono tra loro in connessione per tutta la durata della comunicazione. Nella telefonia numerica la comunicazione viene percepita come continua dagli utenti, anche se

in realtà è limitata dal tempo del canale, mediante l'operazione di campionamento. Dopo aver trasferito gli 8 bits per un campione, il commutatore fa in modo che la linea di ingresso non sia più collegata con la linea di uscita. Quindo di fatto oggigiorno le strutture S sono di tipo elettronico. Le strutture a divisione di spazio S sono non bloccanti.

Una struttura vine definita come *non bloccante* quando è sempre possibile ammettere una linea di ingresso ad una qualsiasi linea in uscita libera.

Il costo realizzativo di una struttura S è legato al numero di connessioni complessivamente possibili. Riprendendo l'esempio sulla matrice quadrata $N \times N$ e generalizzandolo, se possiedo m linee di ingresso e n linee di uscita, il costo C della struttura sarà dato da:

$$C = m \cdot n.$$

Nel caso della telefonia numerica, la struttura S realizza solo il cambio di linea, lasciando inalterato il numero del canale nell'ambito della trama di arrivo. Ad esempio, potrei avere: canale 7 e linea 1 in ingresso $\longmapsto$ canale 7 e linea 4 in uscita; ma non canale 3 e linea 2 in ingresso $\longmapsto$ canale 8 e linea 4 in uscita.

Strutture T In forma semplificata, le strutture T possono essere di buon grado assimilate a delle memorie R/W, equipaggiate con un'adeguata logica di controllo. Una struttura T consente di permutare i canali nell'ambito di una stessa trama. A differenza della struttura S essa opera su una stessa linea e quindi ha un funzionamento del tutto diverso. In questo modo, posso chiedere la comunicazione tra canali diversi. Vi sono dei vincoli realizzativi: ad esempio il tempo di trama è di 125 μS indipendentemente dal numero dei canali. Ogni cella ha la capacità di 8 bits e il numero di celle è uguale al numero maggiore dei canali a disposizione. Per semplicità supponiamo di avere un numero di canali N di ingresso pari a quello di uscita.

Vediamo le diverse modalità operative di una struttura T.

- Scrittura sequenziale-lettura casuale: in questa modalità i canali vengono scritti in memoria seguendo l'ordinamento della trama di arrivo e ripetuti sull'uscita in accordo alla regola di permutazione richiesta. Questo significa che i gruppi di 8 bits vengono scritti all'interno delle celle di memoria in modo da conservare la loro posizione relativa: canale 3 $\longmapsto$ posizione 3 nella memoria. In accordo con la regola di permutazione voluta, i gruppo di 8 bits vengono letti e trasferiti in uscita in corrispondenza degli slots richiesti.

- scrittura casuale-lettura sequenziale: in questa modalità (simmetrica rispetto alla precedente), i canali vengono letti dalla memoria seguendo l'ordinamento della trama e scritti in memoria secondo la regola di permutazione richiesta. La permutazione è quindi in ingresso.

Il costo di una struttura T viene solitamente assimilato al costo della "memoria", valutato in termini di tempo di accesso richiesto, definito così:

$$t_a \leq \frac{125\mu S}{2N},$$

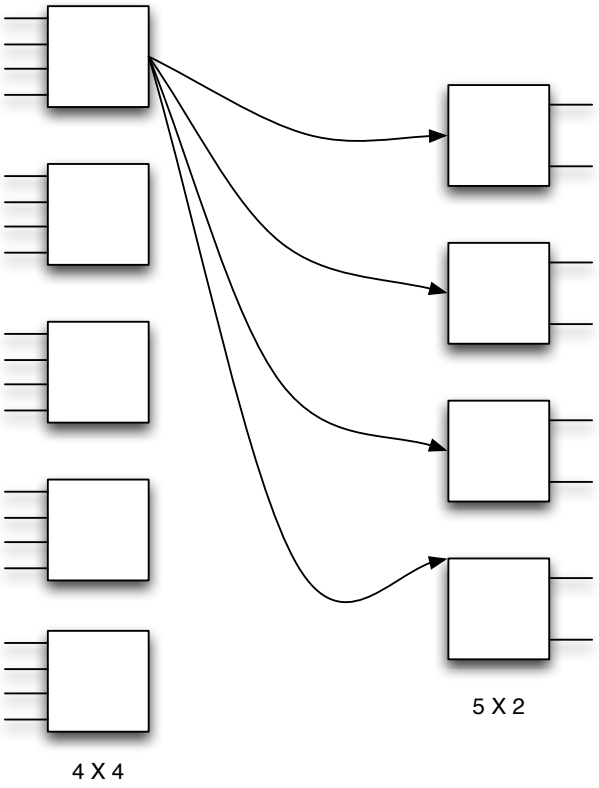
dato che devo garantire in un unico tempo, 2 accessi completi alla memoria, uno in scrittura e uno in lettura. Come per le strutture di tipo S, anche le T sono di tipo non bloccante.

Strutture multi-stadio Lo scopo di una struttura multistadio è quella di aumentati i gradi di libertà delle operazioni di commutazione: cambio di canale e di linea. Inoltre si intende ridurre il costo totale, mantenendo inalterati i requisiti funzionali.

Possiamo distinguere tra strutture multi-stadio omogenee e non omogenee.

- strutture omogenee solitamente con tecnologia S:
  - S-S (2 stadi);
  - S-S-S (3 stadi).
- strutture non omogenee:
  - T-S (2 stadi);
  - S-T (2 stadi);
  - T-S-T (3 stadi);
  - S-T-S (3 stadi).

Figura 7: Dettaglio di struttura a due stadi



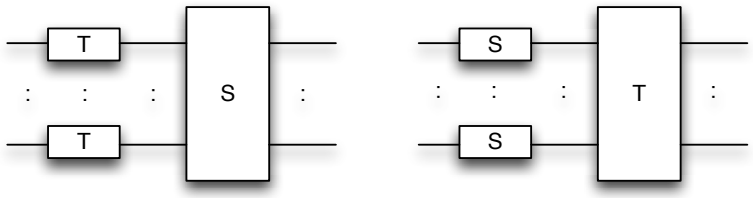
Strutture di commutazione a due stadi non omogenee Tali strutture consentono di sfruttare i vantaggi delle due strutture S e T, permettendo in tal modo di poter effettuare sia n cambio di linea sia una permutazione di canale. Esse di suddividono in due grandi categorie: strutture T-S e strutture S-T.

- T-S: un caso d'uso potrebbe essere canale 3 - linea 1 $\longmapsto$ canale 8 - linea 3. Esso avviene nel seguente modo: prima mediante la struttura T, canale 3 - linea 1 $\longmapsto$ canale 8 - linea 1; poi mediante la struttura S, canale 8 - linea 1 $\longmapsto$ canale 8 - linea 3. La struttura realizzata è quindi *bloccante*: se per esempio voglio che due canali di una stessa trama in ingresso debbano essere ripetuti in canali con lo stesso numero d'ordine ma su linee diverse, non posso farlo.

  Supponiamo che la linea 1 e 3 siano disponibili nel canale 1. Allora vorrei poter espletare la seguente richiesta: canale 3 - linea 2 $\longmapsto$ canale 1 - linea 1 e canale 7 - linea 2 $\longmapsto$ canale 1 - linea 3. Ma dato che la struttura di tipo S consente il cambio di linea mentre lascia inalterato il canale, completare le due richieste non è proprio possibile.

- S-T: aumenta la flessibilità della commutazione. È simmetrica rispetto alla struttura T-S. Anch'essa è di tipo bloccante però: ogni volta che ho due richieste da commutare in canali con lo stesso numero d'ordine in linee di ingresso diverse su canali diversi della stessa linea di uscita, non posso farlo.

Figura 8: Strutture T-S e S-T



Strutture a 2 stadi S Vediamo le strutture S-S tramite un esempio. Supponiamo di voler connettere 20 linee in ingresso con 8 linee di uscita. Utilizzando una struttura monostadio S, avrei un costo di $C = 20 \cdot 8 = 160$. Supponiamo di poter fare di meglio attraverso una struttura in due stadi. Facciamo le seguenti assunzioni:

- suddividiamo gli ingressi in 5 gruppi da 4 linee;
- suddividiamo le uscite in 4 gruppi di 2 linee.

Ciascuno dei 5 blocchi da 4 linee è realizzato internamente mediante la struttura matriciale 4×4. I 4 gruppi da 2 linee invece saranno delle matrici 5×2 per poter avere in ingresso una linea di uscita dei blocchi precedenti e asserire in uscita le due linee. Allora il costo totale dell'architettura sarà:

$$C = C_{stadio1} + C_{stadio2} = 5 \cdot (4 \cdot 4) + 4 \cdot (5 \cdot 2) = 120 < 160.$$

Quindi abbiamo ottenuto una notevole riduzione rispetto al caso monoblocco. La struttura S-S è però bloccante: due richieste in ingresso ad uno stesso blocco dello stadio 1 che vogliono andare in uscita ad uno stesso blocco dello stadio 2, non lo possono fare. Per poterlo fare chiaramente dovrei prevedere un numero di connessione molto maggiore, esattamente per ciascuno dei blocchi dello stadio 1 prevedere un numero di uscite verso ciascuno dei blocchi del secondo stadio pari al numero di uscite presenti sui blocchi del secondo stadio. Nel nostro esempio vorrebbe dire che i blocchi del primo stadio diventano matrici 4×8 e quelli del secondo diventano matrici 10×2. Il costo raddoppia in questo caso anche se viene risolto il problema del blocco di comunicazione: rimane comunque un approccio improponibile.

Strutture a 3 stadi La motivazione che spiega il loro utilizzo è da ricercarsi nel fatto che si riesca ridurre il costo della struttura rispetto al singolo stadio e a mantenerne le stesse qualità funzionali. Si verifica che sono strutture non bloccanti. Come già detto, possono essere omogenee nel caso in cui siano composte da blocchi dello stesso tipo; oppure non omogenee quando i blocchi possono essere di tipo diverso.

Strutture S-S-S Supponiamo di avere un numero di linee di ingresso pari a quello di uscita, sia esso N. Chiaramente il costo della struttura singola S corrispondente è N^2.

Per vedere l'architettura della struttura S-S-S si ricorre all'esempio di suddivisione visto per le strutture a 2 stadi. Suddividiamo quindi il numero delle linee in ingresso N in gruppi di n linee di ingresso ciascuno: otteniamo un numero di gruppi pari $\frac{N}{n}$. Quindi il numero di blocchi S sia al primo che al secondo stadio sarà pari a $\frac{N}{n}$. Il costo della struttura complessiva chiaramente sarà dato dalla somme dei costi dei singoli stadi:

$$C = C_{stadio1} + C_{stadio2} + C_{stadio3} = \frac{N}{n}(n \times k) + k(\frac{N}{n} \times \frac{N}{n}) + \frac{N}{n}(k \times n) = 2Nk + k\frac{N^2}{n^2},$$

dove abbiamo lasciato variabile e pari a k il numero delle linee di uscita dai blocchi del primo stadio, in modo da porci il problema di trovare il k minimo che garantisca la condizione di non blocco e origini il costo minore.

Seguendo il metodo di Clos, si deriverà k in funzione di n considerando la garanzia del non blocco per il caso peggiore. Per poter operare nel seguente modo sono utili le seguenti supposizioni:

- l'unica linea libera in ingresso al primo blocco del primo stadio richiede di essere connessa con l'unica linea libera in uscita all'ultimo blocco del terzo stadio;
- ipotesi di Clos:
  - gli insiemi costituiti dalle linee di ingresso del primo blocco $(n-1)$ del primo stadio e dalle linee di uscita dell'ultimo blocco del terzo stadio sono disgiunti;
  - i blocchi del secondo stadio che hanno un ingresso occupato dalle richieste in ingresso al primo blocco del primo stadio sono distinti da quelli che hanno un'uscita occupata dalle richieste in uscita all'ultimo blocco del terzo stadio.

Sotto queste ipotesi, il k di Clos diventa $2n-1$. Otteniamo allora un costo approssimato di

$$C \simeq 4nN + 2\frac{N^2}{n},$$

supponendo senza perdita di generalità che n e N siano entrambi $>> 1$.

Derivando il costo rispetto ad n otteniamo:

$$\frac{dC(n)}{dn} = 4N - 2\frac{N^2}{n^2} = 0,$$

da cui segue $n_{opt} = \sqrt{N/2} \Rightarrow C_{opt} = 4\sqrt{2}N^{3/2}$. Vi sono però dei vincoli che l'n ottimo deve rispettare: esso deve essere intero e sottomultiplo di N. Se questa condizione non viene verificata, allora la soluzione rimane pur sempre accettabile ma sarà non ottima (sub-ottima). Vogliamo allora individuare un intervallo di valori che rendono soddisfatto il nostro vincolo. Individuiamo i due estremi e chiamiamoli n_1 e n_2 rispettivamente: $n_1 \leq n_{opt} \leq n_2$. Per i due valori si dovrà calcolare il costo della struttura a 3 stadi e poi verificare quale da origine a costo minore.

Strutture T-S-T Si intendono risolvere le situazioni di blocco delle strutture T-S e S-T, mantenendone i gradi di libertà (cambio linea + cambio canale). Avendo N linee in ingresso e N linee in uscita, il costo della matrice S è fissato al solito N^2, quindi devo ottimizzare il costo per le strutture T. Chiaramente il costo complessivo dipenderà dal costo dei singoli stadi. Il costo del primo e del terzo stadio dipenderà dalla scelta del parametro k, avendo assunto n fisso come parametro progettuale. Ottimizzare il costo significa, in modo analogo per le strutture S-S-S, ricavare il più piccolo k per il quale la condizione di non blocco rimane valida.

Secondo la relazione di Clos, ho $n-1$ canali occupati sulle trame ingresso/uscita. L'insieme degli $n-1$ canali in ingresso è disgiunto dall'insieme degli $n-1$ canali in uscita. Le posizioni occupate dai due blocchi di canali nella trama con k posizioni, sono distinte. Quindi se intendo realizzare un collegamento, dovrò avere un numero di canali k tale che $k = 2n-1$.

Cenni sulle strutture a 5 stadi Anche per esse, il motivo realizzativo sta nel cercare di ridurre il costo della struttura a tre stadi, da cui vengono originate, senza perdita di funzionalità. Si ottengono dalle strutture a 3 stadi sostituendo a ciascuno dei blocchi del secondo stadio, una equivalente struttura a tre stadi.

Formula di Lee La formula di Lee introduce il concetto di evento statistico. Si applica in particolar modo alle strutture multi-stadio a tre o più livelli, con l'obiettivo di ridurre il costo realizzativo. Supponiamo nel seguito, di lavorare con una struttura S-S-S. Sia a la probabilità associata al verificarsi dell'evento: "Una linea in ingresso al primo blocco del primo stadio è occupata. ", con $0 \leq a \leq 1$. Si presuppone che la possibilità di ripetere in uscita al primo blocco una richiesta in ingresso sia uniforme per tutte le linee: $1/k$. La probabilità di avere una linea in uscita al primo blocco-primo stadio sarà allora data da:

$$P = \frac{na}{k}.$$

Questa è pure la probabilità di avere una linea occupata in uscita dai blocchi del secondo stadio. Dobbiamo adesso stabilire qual'è la probabilità di riuscire a connettere una linea libera in ingresso con una linea libera in uscita. Fissato un cammino, il cammino stesso non sarà disponibile con probabilità $1-(1-P)^2$. Allora, avendo k alternative indipendenti, posso definire la probabilità di blocco, così: $P_B = [1-(1-P)^2]^k$, che è appunto la formula di Lee.

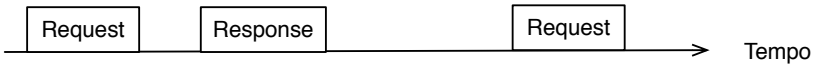
Il vantaggio della formula di Lee è di comportare una riduzione di costo rispetto a Clos: fissato a posso trovare k, dato n, in modo che il valore di P_B sia accettabile.

Lo svantaggio è costituito dal fatto che è una formula probabilistica, dunque non esatta. Inoltre, essa non soddisfa la condizione di Clos.

Reti per trasmissioni di dati Le caratteristiche base del traffico di dati sono:

- intermittenza: il flusso dei dati non è continuo nel tempo, bensì segue una logica del tipo: richiesta - risposta - richiesta - risposta - ...eccetera;
- asimmetria: nell'uso di una connessione il traffico nella linea di trasmissione è minore del traffico nella linea di ricezione (basti pensare al download di un file);
- affidabilità: le trasmissioni dei dati sono sensibili all'integrità (assenza di errori) dell'informazione ricevuta. Si possono infatti verificare degli errori di comunicazione.

Figura 9: Traffico dei dati



Classificazione del traffico

- Traffico asincrono: caratterizzato da un flusso intermittente, senza una periodicità precisa.
- Traffico Isocrono: flusso con caratteristiche stringenti di periodicità, ovvero con cadenze temporali fisse (voce, video).
- Traffico sincrono: non isocrono ma con caratteristiche di continuità su intervalli di tempo.

Architettura ISO/OSI L'acronimo OSI sta per *Open System Interconnection*, mentre ISO per *International Standard Organization*.

L'architettura ISO/OSI è composta di 7 livelli, che sono in ordine dal basso verso l'alto: Phisical, Data link, Network, Transport, Session, Presentation, Application.

1. Physical: il livello più basso è quello fisico e permette il collegamento al mezzo fisico, come ad esempio cavi coassiali, fibra ottica, radio...eccetera. Gestirà la trasmissione in forma numerica dell'informazione nel canale.

2. Data link: il livello di collegamento serve per potre accedere in maniera multipla al mezzo fisico e gestire l'integrità dell'informazione scambiata.

3. Network: il livello rete espleta una funzione fondamentale che è l'instradamento (*routing*). Si occupa di individuare il percorso migliore per raggiungere l'utente destinatario.

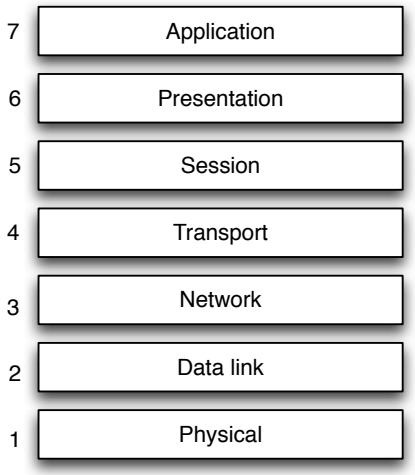
4. Transport: ha il compito di sovraintendere al corretto trasferimento dell'informazione attraverso la rete. Si preoccupa di controllare il rispetto dell'ordinamento temporale di generazione del flusso informativo quando richiesto (connection oriented).

5. Session: questo livello gestisce l'apertura e la chiusura di un collegamento eventualmente verificando l'abilitazione all'accesso (autenticazione).

6. Presentation: si occupa di interpretare correttamente i dati attraverso una data semantica e quindi generare informazione. Rende compatibili sintassi e semantica dell'informazione scambiata tra sorgente e destinatario.

7. Application: è il livello che si occupa di rendere disponibili per l'utente alcuni servizi della rete, come posta elettronica, il controllo di dispositivi remoti, ...eccetera.

Figura 10: Protocollo ISO/OSI



Architetture proprietarie Prima dello standard ISO/OSI erano in vigore diverse architetture proprietarie, tra le quali l'SNA (System Network Architecture) dell'IBM e il DNA (Digital Network Architecture) della Digital. Di fatto, la nascita dell'ISO/OSI ha decretato la morte di queste architetture proprietarie.

Chiaramente, essendo costruite specificatamente per poter operare con dispositivi di uno stesso costruttore presentano una struttura semplificata rispetto al modello ISO/OSI. Questa semplificazione si evidenzia maggiormente ai livelli superiori: ad esempio il livello di presentazione diventa inutile.

Tipologia dei servizi I servizi che può offrire una rete di TLC si distinguono i due categorie principali: quelli orientati alla connessione (*connection oriented*) e quelli non orientati alla connessione (*connection less*). I primi richiedono al nodo destinazione di ripristinare l'ordinamento temporale di generazione del flusso informativo. I secondi non lo richiedono. Un'altra suddivisione può essere basata sul fatto o meno che l'utente ricevente riscontri la corretta ricezione dell'informazione. Si dicono *affidabili* e *non affidabili*.

Modalità di commutazione di una rete Dato che non è possibile connettere tutti i computer su un'unica rete, essere sono tra loro interconnesse tramite i commutatori (*switchs*). Il loro ruolo è quello di gestire la comunicazione tra diversi nodi terminali, inviando e ricevendo dati.

Esistono 3 modalità di commutazione in una rete.

1. Commutazione di circuito: viene individuato un percorso fisico che collega sorgente e destinazione. Tale percorso rimane fisso ed è ad uso esclusivo della coppia sorgente-destinazione. Si compone di tre fasi: creazione del collegamento e ricerca del percorso migliore (*setup*); mantenimento del percorso e controllo (*usage*); abbattimento del collegamento (*reset*). La commutazione di circuito è vantaggiosa laddove si richiede sempre la stessa connessione tra quei due nodi sorgente-destinazione; quando il tempo di utilizzo è molto maggiore del tempo impiegato per le fasi di setup e reset. Lo svantaggio è che non è prevista nessuna forma di *storage* nei nodi di trasferimento.

2. Commutazione di messaggio: è una prima risposta alla soluzione delle criticità della modalità commutazione di circuito. L'entità protagonista di questa modalità è il messaggio (l'informazione che viaggia), ma il suo trasferimento può essere fatto in diversi *steps*. L'inoltro del messaggio avviene quindi link-to-link e non end-to-end come per la commutazione di circuito. Non necessita della fase di reset, dato che il setup è suddiviso tra di diversi nodi intermedi. Il vantaggio avviene quando la connessione è discontinua e la quantità di informazione è limitata. Lo svantaggio principale è il fare troppo affidamento sui nodi links, aumentando in tal modo la probabilità d'errore sui bits informativi. Inoltre, sempre a causa di questi passaggi intermedi del messaggio, potrebbero avvenire ritardi di trasferimento.

3. Commutazione di pacchetto: nasce per poter risolvere le criticità della modalità precedente in commutazione di messaggio, ottenendo un migliore utilizzo della rete. Qui l'informazione viene divisa in pacchetti, assieme di pochi bits, e questo implica la riduzione della possibilità di errori.

Vi sono altre due modalità da ricordare oltre alle 3 principali. Esse sono: modalità di *circuito virtuale*; modalità a *datagramma*.

Nel circuito virtuale viene prevista una fase di setup per calcolare il cammino migliore end-to-end. I vantaggi principali sono nella non necessità di dover effettuare operazioni alla destinazione per rispettare l'ordinamento. Il cammino è appunto virtuale: l'intero collegamento e i rami sono condivisi con altri flussi informativi.

Nella modalità datagramma non è previsto un collegamento statico end-to-end come nel circuito virtuale, ma link-to-link. In questa modalità si parallelizzano le fasi di ricezione e trasmissione dell'informazione: mentre un nodo sta ricevendo un pacchetto, può intanto trasmettere il precedente. Si ha quindi una riduzione dei ritardi dovuti al trasferimento dei dati. Non avviene prenotazione effettiva né virtuale delle risorse.

Reti TCP/IP Sono state introdotte da un progetto di ricerca negli USA, chiamato ARPANET. Riprende la classica filosofia a livelli, individuandone 4. A livello internazionale, l'ente che si occupa della standardizzazione è l'*Internet Achitecture Board*.

1. Application: è il livello già visto per l'architettura ISO/OSI.

2. Transport: possiede le stesse caratteristiche e masioni del livello ISO/OSI. Include a sua volta i seguenti punti:

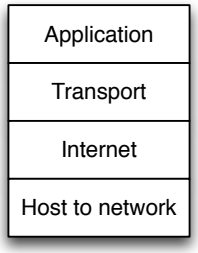
   - il TCP (Transmission Control Protocol) si occupa di rendere compatibili i diversi servizi connection ordiented con il livello IP.
   - UDP (User Datagram Protocol) si interfaccia direttamente con i livello IP (Internet Protocol) in quanto è specifico di servizi connection less. Tipicamente viene preferito al precedente quando il parametro di latenza è molto importante.

3. Internet: ha la funzione di consentire lo scambio di pacchetti dati tra nodi di rete connessi attraverso diverse tipologie di rete. Si basa su una modalità connection less. Anche qui le sue funzionalità base sono quelle del livello Network di ISO/OSI.

4. Host-to-network: è il livello più basso e per questo uno dei più fondamentali; si occupa infatti di rendere compatibili le esigenze dei livelli superiori con differenti tipologie di reti.

Protocollo DQDB (Distributed Queue Dual Bus) Questo protocollo si compone di due caratteristiche principali, che sono la *coda distribuita* e il *doppio bus*. Il doppio bus è dovuto al fatto che in tal modo è costruita la rete. La coda distribuita consente di rispettare l'ordinamento temporale delle richieste nell'accedere al mezzo condiviso: viene seguita una politica FIFO. Si tratta quindi di un protocollo di accesso ordinato.

Figura 11: Struttura TCP/IP



In ogni bus è presente una struttura a trama temporale: 2 bits hanno il ruolo di gestire l'utilizzo/accesso e i restanti bits sono d'informazione. Il bit A gestisce l'accesso: 0 se non è stato prenotato l'accesso, 1 se è stato prenotato. Il bit U gestisce l'utilizzo: 0 se libero, 1 se è usato.

Ogni nodo dovrà possedere un'architettura duale per la gestione dell'accesso al doppio bus. L'accesso al mezzo fisico avviene secondo la divisione di tempo. Le trame conterranno le "prenotazioni"dei nodi per l'accesso.

Consideriamo il caso in cui la trasmissione debba avvenire sul bus superiore. In questo caso, la trama del bus inferiore, viene utilizzata per contenere le prenotazioni di accesso dei nodi alla rete.

Ogni stazione possiede un orologio e tutti gli ordini di tutte le stazioni sono sincroni, così da sapere quando si presentano gli istanti di accesso. La trasmissione è vincolata dal senso di percorrenza del bus e dalla posizione relativa da raggiungere.

Ogni stazione è strutturata nel seguente modo:

- contatore add/drop: incrementa di 1 il suo contenuto tutte le volte che osserva nel bus interiore uno slot con il corpo prenotazione settato a 1. Decrementa di uno il suo contatore ogni volta che osserva nel bus superiore uno slot con il campo utilizzo settato a 0.
- contatore drop: viene decrementato ogni volta che nel bus di trasmissione passa uno slot utilizzabile, serve per capire quando è il turno per l'accesso (valore = 0).
- buffer di dati memorizzati in attesa della trasmissione.

Se x è il valore del contatore in un istante di temo t, questo x è il numero di stazioni che hanno notificato la necessità di accesso per trasmettere un pacchetto nel bus di interesse.

Se il nodo ha necessità di accesso:

1. si mette a 1 il corpo prenotazione del primo pacchetto utile osservato nel bus inferiore;
2. si trasferisce il valore del contatore add/drop al contatore drop.

Il valore trasferito questa volta rappresenta quante stazioni a monte nel bus prenotazione hanno notificato la necessità d'accesso. La stazione attende per la trasmissione che il valore sia 0. Durante la fase di attesa, il contatore add/drop rimane attivo per tenere traccia delle richieste prima di averne una nuova. In linea generale, vengono privilegiate per acquisizione del diritto di accesso i nodi più vicini al punto di generazione della trama di prenotazione.

Si possono presentare due casi di utilizzo. Il primo è quando il nodo A utilizza la rete in maniera continua e esclusiva ma ad un certo punto il nodo B diventa attivo. Allora si evidenzia il trattamento privilegiato per il nodo A avendo a disposizione, supponiamo più slots del nodo B. Viceversa, nel caso 2 è il nodo A che non riesce mai a trasmettere perchè si verifica il caso esclusivo del nodo B.

Una soluzione a questo problema può essere quella di assegnare un massimo numero di slots che lo stesso nodo può usare consecutivamente. Si introduce un numero massimo di slots prenotati.

Protocollo FDDI (Fiber Distributed Data Interface) Questo protocollo trova applicazione nelle dorsali per l'interconnessione di reti LAN; per dispositivi ad alta velocità con grandi necessità di accesso.

Il mezzo fisico utilizzato per la comunicazione è la fibra ottica; il numero massimo dei nodi che si possono connettere alla rete è 500. L'estensione massima è di 100 km. Ha la classica topologia a doppio anello, nel quale soltanto quello esterno è attivo e quello più interno subentra a quello esterno nel caso di rotture e malfunzionamenti di quest'ultimo.

Il livello MAC della rete consente un arbitraggio temporale basato sul metodo token ring.

La rete consente la gestione di due diverse tipologie di traffico mediante due modalità specifiche: il caso di traffico sincrono (grosse quantità di dati) che è sempre privilegiata; il caso di traffico asincrono (sporadico) viene gestito in modalità best effort (attraverso 8 livelli di priorità).

Sono previste per la rete due diverse tipologie di trame:

- *data frame*: sono relative al trasporto dell'informazione. Ogni nodo che riceve un data frame lo copia nel suo buffer e lo ripete in uscita. Il destinatario prima di rimandarlo in rete lo marca come letto. Può essere rimosso solo dal mittente, quando è stato correttamente ricevuto.

- *token frame*: hanno una struttura predefinita e nota a tutti i nodi della rete. Vengono utilizzate per la condivisione dell'accesso.

Il protocollo prevede un controllo di integrità dell'informazione trasmessa su base E2E.

Durante la fase di set-up della rete, si definisce il valore di un parametro di riferimento, detto *token target rotation time* (TTRT):

$$TTRT \geq \sum_{i=1}^{N_d} \alpha_i + \sum_{i=1}^{N_d} d_i,$$

dove con N_d si indica il numero di nodi nella rete; α_i la necessità di accesso in un'unità di tempo, dichiarata dal nodo i-esimo per la trasmissione del traffico sincrono; d_i è il tempo di passaggio del token dal nodo i al nodo successivo.

Ogni nodo ha un proprio orologio attraverso il quale valuta il parametro TRT (*token rotation time*). Il tempo misurato va dall'istante di arrivo del token all'istante di arrivo successivo. Oltre a quest'orologio, ogni nodo possiede un ulteriore contatore a decremento che ogni volta che il nodo acquisisce il diritto all'accesso alla rete, viene settato al valore THT (*token holding time*), così definito:

$$THT = \{ \begin{array}{cc} \alpha_i & TTRT - TRT \leq \alpha_i \\ TTRT - TRT & altrimenti \end{array}$$

Se B è il valore della banda nominale della rete, al nodo i-esimo viene garantito un accesso di questa entità:

$$\frac{\alpha_i B}{TTRT}.$$

Per una rete FDDI, si definisce come efficienza il parametro $\eta = \frac{TTRT - RL}{TTRT} \leq 1$, con $RL = \sum_{i=1}^{N_d} d_i$ (ritardo di latenza). Chiaramente i valori più alti di η si riferiscono ai valori minori di RL. La condizione ideale si ha quando $RL = 0$.

Reti wireless Tra i migliori vantaggi di una rete wireless ricordiamo la possibilità di accesso ubiquo e in mobilità. Fanno uso di una topologia di rete estesa. Vi è sempre una più elevata richiesta dei servizi wireless, legata soprattutto alla sua grande comodità. Quando le LAN sono wireless si possono indicare col nome di WLAN.

Le reti wireless sono reti infrastrutturate: è presente un nodo con funzionalità specifiche, detto access point che deve solitamente gestire la connessione verso i terminali utente (client) e verso una rete cablata tradizionale.

Spesso possono anche essere costruite ad hoc. Nel qual caso non è previsto un access point, ma i terminali di accesso comunicano tra di loro spesso con finalità cooperative.

Le maggiori difficoltà di una rete wirless risiedono nella natura del canale di comunicazione:

- maggiore sensibilità ai disturbi;

- sicurezza non molto forte.

Volendo fare un'analisi SWOT (Strenghts-Weakness-Opportunities-Threats):

- vantaggi: connettività ubiqua; riduzione costi di cablaggio; facilità dispiegamento; tecnologia matura.

- svantaggi: banda di accesso inferiore rispetto a reti cablate; la banda tipicamente è condivisa; sensibilità ai disturbi; si possono avere dei problemi nel caso dei servizi real-time. In questi casi, per far fronte agli effetti dannosi del canale si ricorre alla frammentazione dell'informazione trasmessa: essa si riorganizza in blocchi di lunghezza max fissata.

- opportunità: sviluppo di applicazioni specifiche; sviluppo di nuove tipologie di servizio; riduzione dei costi di apparati; convergenza.

- minacce: sicurezza e riservatezza.

La Wi-Fi Alliance si occupa di definire gli standards e certificare gli apparati. È un'associazione internazionale no-profit formata da industrie del settore e centri di ricerca per la standardizzazione delle architetture. Lo standard ha già conosciuto diverse evoluzioni. Attualmente di ha un accesso al mezzo fisico di tipo OFDM (*Ortogonal Division Multiplexing*): viene suddivisa la banda utile in bande elementari ortogonali tra loro. Sono previste più portanti tra loro ortogonali.

La wireless lavora nella banda dei 5 GHz e consente una banda nominale di accesso di 54 Mb/s. Una seguente evoluzione è stata redatta nello standard IEEE 802.11g, che lavora nella banda 2.4 GHz. L'ultima versione è la IEEE 802.11n.

Per quanto riguarda il livello MAC di una rete wireless, esso si basa sulla tecnica a rivelazione di portante con l'aggiunta di una funzionalità finalizzata a prevenire la collisione, anzichè rivelarla semplicemente. Si parla infatti di CSMA/CA (*Collision Avoidance*).

Spesso è prevista una fase di accesso senza contesa nelle reti wireless con AP. Questa modalità è detta PCF (*Point Coordination Function*).

Può verificarsi il problema di monopolizzazione dell'accesso. Allora si assegna un valore massimo detto TXOP (Transmint Opportunity) a tutti i terminali. Questo parametro può essere definito e implementato anche nel caso di uno specifico servizio.

Problema del terminale nascosto Questo problema si manifesta nel caso delle reti wireless nel caso in cui un nodo rimane visibile soltanto dall'AP (Access Point), ma non dagli altri nodi che sono comunque in connessione con l'AP. Questo provoca difficoltà nel controllo di accesso al mezzo. La distanza tra due nodi, ad esempio tra A e B, impedisce la rilevazione della portante e quindi possono verificarsi collisioni. Si verifica una collisione quando entrambi fanno richiesta di accesso al canale, non potendo vedersi l'un l'altro. La questione viene risolta con CSMA/CA: essa prevede infatti lo scambio di messaggi di ACK (*handshake*) tra mittente e destinatario. Vi è pure il problema opposto, chiamato del terminale esposto. Questo avviene quando un terminale, ad esempio C, rimane esposto al traffico informativo tra altri nodi, ad esempio tra A e B. Egli è inabilitato alla trasmissione, dato il traffico che gli è presente attorno.

Standard IEEE 802.16-WiMAX Nasce con l'obiettivo di allargare l'area di servizio e aumentare il datarate offerto. È utilizzato per risolvere il problema del digital divide, ed è stato pensato per un uso tipicamente residenziale. Viene pure aumentata la sicurezza della rete. La maggiore criticità è legata alla scarsa mobilità offerta.

Ha un'architettura in 5 livelli, in ordine dal basso verso l'alto:

1. QPSK; 16-QAM; 64-QAM (in ordine di *bitrate* consentito) sono le modulazioni numeriche alla base del livello fisico: è pensato per lavorare nella banda di frequenze a 5 GHz. La vulnerabilità agli errori del canale è proporzionale al bitrate consentito. In base alla posizione che l'utente ha rispetto alla base station (BS), verrà adottata la modulazione che consente lui una migliore qualità di connessione. Una misura della qualità è il livello del segnale percepito.

2. sottostrato di convergenza;

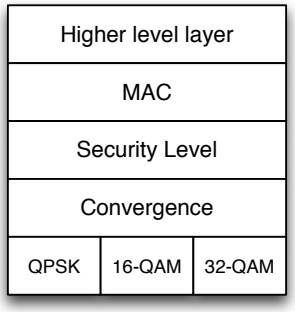
3. sottostrato di protezione;

4. livello MAC;

5. sottostrato di convergenza di servizio.

6. a seguire i vari higher levels.

Figura 12: Architettura



Vediamo che è possibile scegliere la modulazione numerica da utilizzare (maggiore libertà) ed esiste pure la possibilità di modificare la forma di protezione (codifica) da utilizzare per garantire l'integrità dell'informazione trasmessa. Questa tecnica è detta: AMC (*Adaptive Modulation and Coding*).

Per quanto riguarda il livello MAC, la tecnica di utilizzo nel canale è di tipo ordinato. Sono possibili due modalità:

- FDD (*Frequency Division Duplexing*): vengono individuate bande distinte per la trasmissione della BS verso i propri clients (downlink) e per la trasmissione in senso opposto (uplink);
- TDD (*Time Division Duplexing*): la banda di accesso viene suddivisa tra comunicazione uplinks e downlinks, con modalità half-duplex (separazione temporale delle due fasi).

L'accesso viene realizzato assegnando risorse nei domini tempo-frequenza. Ho la possibilità di trasmettere contemporaneamente per un tempo prefissato (slot) su N bande distinte di frequenza. Se ΔB è la sottobanda elementare, allora $N \cdot \Delta B$ è la banda totale.

Questo protocollo individua 4 classi di servizio (Quality of Service).

- Servizio a bit rate costante: rappresenta ad esempio il caso di trasmissioni di collegamenti telefonici (voce). Riserva le risorse di accesso ad intervalli di tempo regolari.
- Servizio a bit rate variabile in tempo reale: è il caso di trasmissioni multimediali con bit rate variabile. La stazione base interroga i clients chiedendo loro la necessit di banda per l'accesso.
- Servizio a bit rate variabile non in tempo reale: la stazione base dispone di una lista per l'interrogazione diretta degli utenti. Gli utenti che non rispondono a interrogazioni successive vengono tolti dalla lista. Essi poi vengono messi in un gruppo cui viene rivolta un'interrogazione collettiva. L'inserimento avviene con modalità di accesso casuale in risposta ad una interrogazione broadcast di tutti i potenziali utenti non attivi.
- Best effort: per tutto il traffico rimanente non viene fatta alcuna interrogazione. L'accesso viene conquistato dai terminali superando una fase di contesa casuale. Vengono comunicate trama per trama le risorse banda-tempo disponibili che vengono messe a contesa, appunto.

Bluetooth Viene ideato da un progetto Ericsson nel 1994. Nel 1998 fu istituito il SIG (*Special Industry Group*). Il bluetooth è ormai diventato uno standard con l'IEEE 802.15.1.

I più importanti caratteristiche del bluetooth sono:

- raggio limitato a pochi metri, solitamente non più di 10 con banda tipica di lavoro a 2.5 GHz a 79 canali (ciascuno a banda 1 MHz);
- accesso funzionante dovunque;
- dimensioni contenute e con costi conseguenti ridotti;
- connessioni voce/dati;
- supporta la tecnologia peer-to-peer.

È di fatto la tecnologia che permette di dar luogo a quelle che prendono il nome di WPAN (*Wireless Personal Area Network*).

Anche il bluetooth possiede un'architettura protocollare, assieme ad un accesso piuttosto semplice.

Solitamente un dispositivo, detto *primary*, mette in connessione più dispositivi che prendono il nome di dispositivi *secondary* (modalità *piconet*) A sua volta uno di questi dispositivi può diventare fonte di connessione per altri, divenendo un dispositivo *primary/secondary* (modalità *scatternet*).

Tecnologia RFID (Radio Frequency Identification) È una tecnologia per l'identificazione automatica. I dispositivi usati sono i *tag passivi*. Essi sono costituiti da un microchip e da un'antenna e non hanno alimentazione. La loro dimensioni sono dovute principalmente all'antenna. Possono essere di sola lettura oppure anche lettura/scrittura. Il sistema RFID si basa sulla lettura a distanza di informazioni: quando interrogato da un lettore il tag risponde con le informazioni in esso contenute.

- tecnologia a basso costo;
- facile da utilizzare;
- di lunga durata;
- data rate di 2 Kbps;
- raggio di copertura piccolo e dipendente dall'antenna.

Reti ISDN (Integrated Services Digital Networks) Si tratta di reti integrate nelle tecniche e nei servizi. Lo scopo di queste reti è stato quello di far convivere tecnologie diverse all'interno di un'unica gestione dell'informazione. In particolare, una rete di questo tipo deve gestire in maniera trasparente per l'utente la modalità di commutazione di pacchetto (CP) e di circuito (CC).

Si è avvertita la necessità di integrare in una rete i due servizi tipici voce/dati, ovvero la necessità di far coesistere la modalità a commutazione di circuito con quella a commutazione di pacchetto. È una rete interamente numerica.

Sono previste due tipologie di canali: quelli informativi e quelli trasmissivi di dati (detti anche di segnalazione). La tipologia di accesso avviene attraverso 4 tipi di canali: i canali B, D, E e H. I canali B (bearer) sono di tipo informativo e servono al trasporto della voce a pacchetti, fax e dati. Hanno una velocità di accesso di 64 Kb/s. I canali di tipo D (demand) trasportano la segnalazione commutata a pacchetto e hanno una velocità di accesso che può assumere il valore 16 Kb/s o 64 Kb/s in relazione al loro utilizzo. Sono utilizzati per il trasporto della segnalazione o dati a basso rate con modalità commutazione di pacchetto (CP). I canali di tipo E sono utilizzati principalmente per la trasmissione di segnalazione di rete per servizi a commutazione di circuito. I canali di tipo H sono canali dedicati invece al trasporto dell'informazione ad alto bitrate.

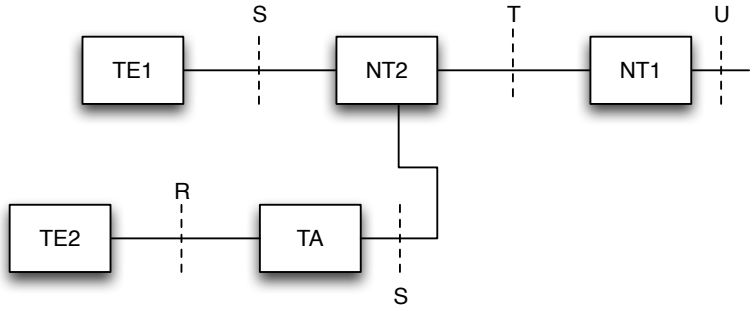
Accesso base: $2B + D =\simeq 144Kb/s$.

Accesso primario: $30B + D =\simeq 2Mb$.

Interfaccia utente-rete Consideriamo una rete composta di 5 blocchi principali:

- TE1: terminale in standard ISDN;
- TE2: terminale non standard ISDN;
- TA: terminal adapter;
- NT2: dispositivo che opera ai primi 3 livelli OSI (PABX);
- NT1 dispositivo che opera solo a livello fisico (multiplexing per canali utente).

Figura 13: Interfaccia rete-utente



Allora S è l'interfaccia a standard ISDN; R è l'interfaccia non a standard ISDN; T è l'interfaccia apparati utente terminazione di rete; U è l'interfaccia tra terminazione ISDN e nodo ISDN.

Raccomandazione X.25 Specifica le modalità di interfacciamento tra un terminale di utente (DTE: *Digital Terminal Equipment*) e la terminazione (DCE: *Digital Circuit Equipment*) della rete verso l'utente. È stato il primo protocollo a consentire la trasmissione dei dati a pacchetto su una linea pubblica commutata. Ci si riferisce spesso all'analogia dell'ufficio postale dove ci sono convenzioni per la consegna del pacco, ma non ci si preoccupa del trasferimento vero e proprio.

L'architettura protocollare dei primi tre livelli è composta da:

- livello fisico: prevede la trasmissione in canale di qualità non elevata. Data rate 64 kB/s.
- livello data link (LAP-B: Link Access Protocol-Balanced): garantisce l'integrità dell'informazione scambiata tra DCE e DTE. La modalità bilanciata non assegna in maniera esclusiva il ruolo di master.
- livello rete (PLP).

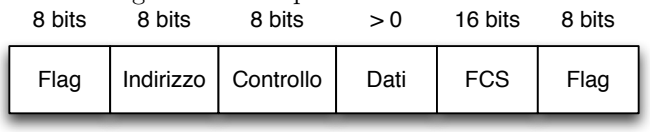
Il mezzo trasmissivo era previsto non di elevata qualità. Come conseguenza di questo, il livello data link dovrà implementare adeguati meccanismi per garantire l'integrità dell'informazione.

Qui, il protocollo previsto è noto come LAP-B. Esso prevede due modalità di servizio e pacchetto:

- circuito virtuale. Si tratta di una connessione logica tra qualsiasi coppia DTE che prevede tre fsi: setup, scambio dai e rilascio (le tre fasi classiche).
- circuito virtuale permanente. Consente la comunicazione tra due qualsiasi DTE su base connessione predefinita. Connessione sempre disponibile ed utilizzata esclusivamente per lo scambio di informazioni.

Al livello LAP-B la trama è formata a blocchi di bits, nel seguente modo: 8 bits di flag, 8 bits di indirizzo, 8 bits di controllo, un numero ¿ 0 di bits di dati, 16 bits di FCS e 8 bits di flag per concludere. Un flag è una sequenza fissata di 6 zeri con un 1 rispettivamente in testa e in coda. In questo contensto serve per delineare l'inizio e la fine di un frame, infatti i flag lavorano a coppie per un unico frame.

Figura 14: Composizione della trama



I bits di indirizzo servono per identificare DCE/DTE; i bits di controllo servono per identificare il frame (informativo, di segnalazione,...eccetera); i bits di FCS servono per proteggere il frame dai possibili errori nel canale.

Vi è però un problema: la sequenza 10000001 potrebbe verificarsi nei bits dedicati ai dati, con conseguente perdita di informazione (trama troncata). Allora lo posso risolvere con la tecnica del *bit stuffin*: introduco sistematicamente un bit a 1 dopo il riscontro di 5 bits a 0 successivi ad un bit a 1. Ovviamente in ricezione scarterò il bit a 1 dopo 5 0 consecutivi.

Nel livello rete PLP ogni flusso informativo viene identificato da un'etichetta, un colore (LCI: *Logical Channel Identifier*): questo principio è chiamato condivisione dinamica della banda. I flussi generati da uno stesso terminale condividono l'accesso al mezzo fisico. A livello fisico i pacchetti sono trattati indistintamente dalla loro colorazione; mentre a livello di rete il principio LCI è utilizzato per suddividere i flussi informativi ed eseguire operazioni di commutazione nei nodi di transito.

Tempo fa, ogni flusso dati veniva identificato nei nodi in transito mediante la propria etichetta e linea di arrivo. La commutazione avveniva in due fasi:

- fisica. Viene commutata la linea.
- logica. Definisco la nuova etichetta del flusso sulla linea di uscita. Il campo di definizione dell'etichetta ha soltanto valore locale.

Per la commutazione, si impone che la richiesta di banda di tutti i servizi attivi su uno stesso mezzo fisico non debba superare la capacità massima del mezzo stesso.

Segnalazione di rete La segnalazione di una qualsiasi rete di telecomunicazioni è fondamentale per garantire lo scambio di informazioni fra gli utenti della stessa rete.

Questa segnalazione di rete può avvenire attraverso due modalità principali:

- segnalazione in banda. In questo caso l'informazione relativa alla segnalazione di rete viene inviata nella banda del segnale informativo.
- segnalazione fuori banda. In questo caso, invece, la segnalazione avviene su una banda diversa da quella del segnale informativo.

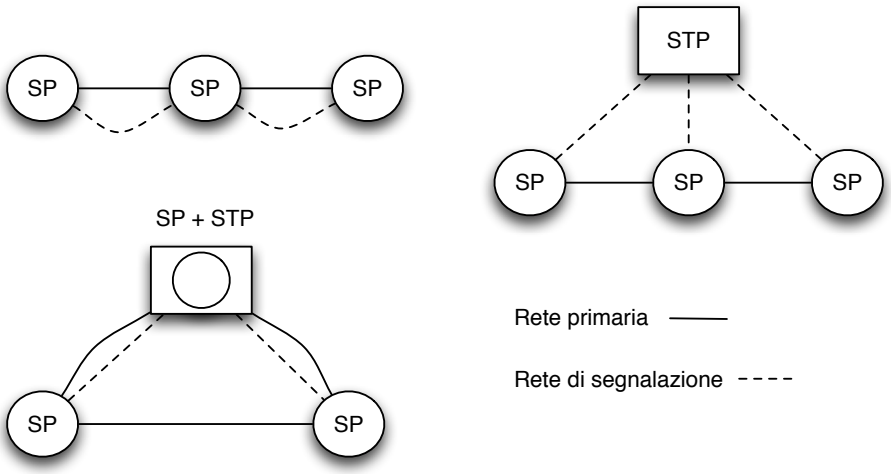
La tendenza è quella di condividere la risorsa dedicata alla segnalazione per il controllo di più flussi informativi: viene quindi posto un canale comune.

Oggigiorno il sistema moderno di segnalazione di rete è il sistema SSN7 (Sistema Segnalazione N.7). Esso viene impiegato, ad esempio, nelle reti ISDN.

Sistema Segnalazione SSN7 Viene previsto l'impiego di reti CP. Gli elementi principali di questa rete sono essenzialmente due.

- Signal Point (SP): è un collettore per l'informazione di segnalazione. Tipicamente viene associato fisicamente ad una struttura di commutazione.
- Signal Transfer Point (STP): ha la possibilità di commutare i flussi di segnalazione. Svolge la funzione di auto-commutatore limitatamente alla rete di segnalazione.

Figura 15: Reti SP/STP



Vengono utilizzate 3 topologie di rete: in modalità *associata*; in modalità *quasi associata*; in modalità *non associata*.

- Nella modalità associata vengono utilizzati soltanto SP (costo contenuto). Viene duplicata la topologia della rete primaria per creare una rete di segnalazione.
- Nella modalità non associata vengono usati sia SP che STP. La rete primaria ha una struttura associata, mentre esistono lei collegamenti a ciascun SP all'STP che compongono la rete di segnalazione. Viene così implementato un controllo globale e non per linea di giunzione.
- Nella modalità quasi associata vengono impiegati sia SP che STP. In particolare viene fuso un SP con un STP e possiede una modalità di controllo integrata.

Vediamo la sua architettura protocollare. Possiede forti analogie con il protocollo ISO/OSI. Essa prevede due parti principali.

- User Part (UP): è specifica del servizio offerto dalla rete; ad esempio voce, video, ...eccetera.
- Message Trasfert Part (MTP): opera come servizio per la UP e si compone a sua volta di altri 3 livelli. Livello fisico, di collegamento e di rete.

Frame Relay Abbiamo visto che la raccomandazione X25 presenta un collegamento molto pesante, pensato per mezzi trasmissivi di buona qualità e non consente di gestire picchi di traffico informativo. Per questo è stato introdotto un nuovo protocollo che rispetto a X25 offre un servizio minimale. Questo protocollo è appunto il Frame Relay e le sue caratteristiche principali sono: essere connection oriented; non affidabile (sposta la sua affidabilità, il proprio successo, sul mezzo trasmissivo) e la segnalazione avviene fuori banda. Sono reti basate sulla modalità circuito virtuale. I vantaggi che consente sono: data rate elevati; architettura protocollare semplificata; gestione dinamica delle richieste di banda; costo contenibile; funzioni limitate nel livello di collegamento (semplicità). Un'analogia con l'X25 è l'impiego delle etichette logiche DLCI (*Datalink Logical Connection Identifier*: viene previsto nei frames un campo dedicato alle etichette.

La loro possibilità di impiego di reti frame relay è legata alla interconnessione su lunghe distanze di reti TCP/IP.

Rete ATM (Asynchronous Transfer Mode) Questa rete nasce per rispondere alle esigenze di alta velocità di accesso necessaria per servizi video interattivi e ad una flessibilità di impiego nel caso dei servizi disomogenei per la velocità di accesso. La rete prevede un mezzo fisico di elevata qualità, ossia la fibra ottica. È essenzialmente uno standard di livello fisico. La trasmissione dell'informazione è basata su blocchi elementari detti *celle*. Conseguenza di questo, è la possibilità di garantire velocità di accesso elevate e considerare raro l'evento di ricezione con errori i un flusso informativo, almeno su base link-to-link.

La rete ATM fa uso della filosofia *Core-Edge*, ossia localizza su base end-to-end tutte le funzionalità superiori al livello fisico.

La rete ATM ha una struttura protocollare organizzata in livelli. Si distinguono 3 piani protocollari.

- User Plane: si compone di più livelli ed è dedicato alla gestione delle applicazioni degli utenti nella rete (gestione lato utente dei servizi).

- Control Plane: si compone anch'esso di più livelli ed è dedicato alla gestione delle segnalazioni.
- Management Plane: serve a consentire l'interazione tra i due livelli appena visti.

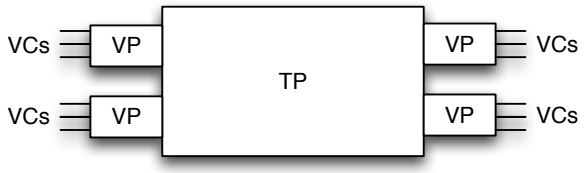
Il livello ATM è quello che da il nome alla rete stessa, dato che è colui che fornisce i servizi fondamentali per il funzionamento: gestisce le operazioni di mux/demux dele celle; genera i campi VPI/VCI (*Virtual Path/Circuit Identifier*) e genera la testata delle celle.

ATM prevede la condivisione logica di uno stesso mezzo fisico (fibra ottica) a due livelli (sottostrati):

- VC (Virtual Circuit): la banda viene suddivisa in diversi VC. Un VC solitamente è riferito ad uno specifico servizio utente.
- VP (Virtual Path): è riferito all'aggregazione di più VC. Rappresenta un'allocazione di capacità a taglio grasso. Fornisce anche una connessione virtuale tra due switch.

Infine il Transmission Path aggrega diversi VP.
Una connessione virtuale è univocamente identificata dalla coppia (VPI, VCI).

Figura 16: Fibra ATM



Architettura ATM Il livello AAL (*ATM Adaptation Layer*): prevede la suddivisione in 4 sottostrati specifici dei servizi che si vogliono attivare (AAL1/AAL2/AAL3-4/ALL5). La funzione base di questo livello è quella di rendere compatibile il flusso informativo con il formato delle celle accettate dallo strato ATM. Esso prevede due sottostrati: il CS (Convergence Sublayer) e il SAR (Segmentation and Reassembly). Il primo serve per garantire l'integrità dei dati trasferiti allo strato ATM. Il secondo è responsabile durante la fase di trasmissione, delle operazioni di frammentazione dei frames in celle. In ricezione, esegue l'operazione di ripristino della struttura originaria.

AAL1 si occupa della gestione di servizi isocroni con tasso costante: voce e video.

AAL2 inizialmente si doveva preoccupare di servizi con rate variabile isocroni. Attualmente viene impiegato per trasmettere traffico aggregato a basso bit rate, ad esempio nelle reti cellulari.

AAL 3-4 è stato pensato per servizi orientati alla connessione e non tipo asincrono.

AAL5 è un sottolivello semplificato pensato per il trasporto del traffico con politica best-effort.

SDH (Synchronous Digital Hierarchy) L'SDH è un protocollo di livello fisico usto per la trasmissione telefonica e di dati i reti geografiche (WAN), cioè di trasporto. Il suo compito è di aggregare flussi di dati a bit-rate diversi e ritrasmetterli tutti insieme a grandi distanze. Consente di raggiungere elevati livelli di qualità e notevoli strumenti per il controllo. Nelle reti SDH si ha una topologia ad anello, simile a quella giù vista per le reti FDDI.

Dispositivi principali del protocollo.

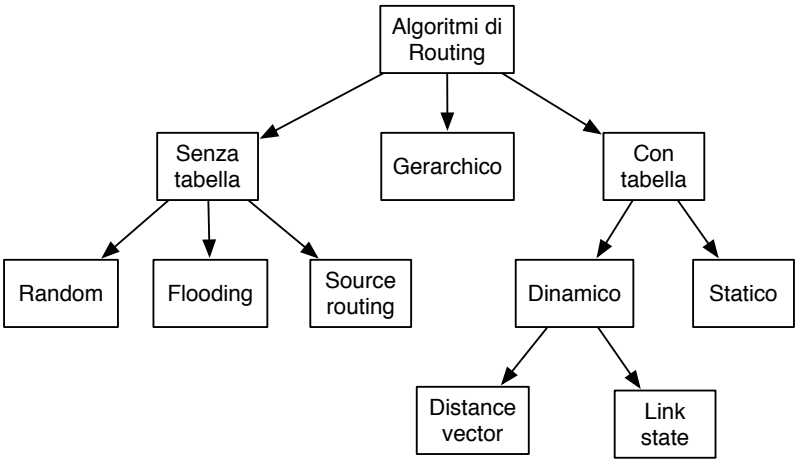
- Mux/Demux: servono ad aggregare/disaggregare flussi di dati singoli. Tipicamente sono presenti all'inizio e alla fine di una via di collegamento.
- Repeater: operano direttamente sul segnale (in genere ottico) per rigenerarlo in potenza e coprire collegamenti più lunghi.
- Add/Drop multiplexer: sono presenti nei nodi di transito di una rete SDH. Consentono di inserire o estrarre flussi dati da un collegamento.

Trama base di SDH: viene indicata con la sigla STM-1. L'elemento base è il gruppo di 8 bits. 9 righe $\times$ 270 colonne $\times$ 8 bits. Il periodo di ripetizione della trama STM-1 è di 125 μS. Velocità di accesso R:

$$R = \frac{270 \cdot 9 \cdot 8bits}{125 \cdot 10^{-6}} = 155.32Mbps,$$

con rate informativo pari a 150 Mbps.

Figura 17: Classificazione degli algoritmi di routing



Classificazione delle tecniche di Routing Con tabella significa che un nodo registra in una propria memoria, per ogni richiesta di instradamento in ingresso, quale linea di uscita deve essere interessata.

Senza tabella, i nodi non prevedono abbinamenti ingresso/uscita predefiniti. Sono di tipo reattivo cioè attivati soltanto su richiesta.

Un algoritmo di routing è centralizzato quando sono previste essenzialmente le tabelle e un'unità di elaborazione dell'algoritmo centralizzata.

Un algoritmo si dice distribuita quando viene prevista un'esecuzione dell'algoritmo in forma distribuita, detta anche cooperativa. Anche in questo caso sono previste delle tabelle per la memoria.

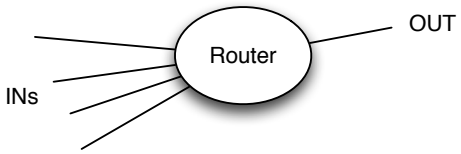
Un algoritmo è isolato quando vengono tipicamente fa riferimento a realizzazioni senza uso di tabelle. Prevede l'esecuzione in locale (stand-alone).

Algoritmi senza tabella

- Random: è una tecnica semplice e robusta. A fronte di una richiesta in ingresso seleziono in maniera random una delle possibili uscite. Non è una tecnica ottima, in generale.

- Flooding: viene semplificato l'algoritmo di routing, decidendo che ogni richiesta di inoltro presente sugli ingressi, venga ripetuta su tutte le uscite. Sicuramente è robusta e va ad interessare il percorso migliore. La caratteristica di robustezza spiccata della tecnica, rende possibile il suo utilizzo in applicazioni specifiche (militari o safe-critical).

Figura 18: Algoritmo random senza tabella



È possibile che si verifichi uno svantaggio operativo, laddove la facilità di gestione della rete comporta la continua ripetizione di informazione non più attuale.

Una possibile soluzione consiste nell'inserimento di un campo che riporta il valore massimo delle volte che un pacchetto può essere ripetuto in uscita. Un nodo che riceve un pacchetto che presenta quanto valore a 0, significa che non lo può più ripetere e lo scarta. Chiaramente se non è 0 il valore del campo, ogni volta che il pacchetto viene ripetuto, si decrementa il valore del contatore di 1.

- Source routing: in questa categoria, come dice il nome stesso, il percorso che devono seguire i pacchetti è già noto e specificato.

  Il *path-server* è il percorso per i flussi dati che è inviato ai nodi dal server centrale.

  Se il percorso non è già stato specificato, si può operare nella modalità *path-discovery*. Questa procedura di scoperta del percorso migliore da usare è gestita dal nodo e tiene conto dell'effettivo stato della rete in quanto prevede una fase di scoperta gestita con modalità flooding.

Algoritmi con tabella Essi possono essere sia di tipo centralizzato che di tipo distribuito.

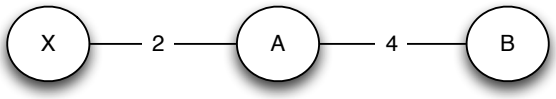
- Distance vector: ogni nodo dispone di una tabella che associa ad ogni possibile destinazione un percorso mediante la specifica del nodo vicino, chiamato next-hop. Nella stessa tabella è specificato il costo del percorso. Nella fase di inizializzazione ogni nodo conosce il costo dei collegamenti solo con i propri vicini. Laddove non si conosce il costo, la tabella ospiterà il simbolo ∞. Il risultato finale dell'algoritmo sarà aver riempito la tabella relativa ad ogni nodo con i costi dei cammini ottimi da nodo a nodo.

  L'implementazione dell'algoritmo avviene in maniera collaborativa: ogni nodo definisce in modo autonomo la propria tabella di routing. Ogni nodo, poi la pubblica successivamente. Poi i nodi si scambiano le proprie tabelle e in base a confronti, aggiornano i propri costi verso i gli altri nodi. Il processo continua finchè non vine individuato il cammino di costo minore (ottimo) per ciascun nodo.

  In alcun casi, l'aggiornamento delle tabelle può avvenire su richiesta in seguito al verificarsi di situazioni anomale.

  Può verificarsi un caso di instabilità, quando un collegamento di interrompe. Consideriamo il caso di una collegamento A $\longmapsto$ X interrotto. Solitamente, a seguito di interruzione di collegamento, il costo risultante viene settato a ∞. Può verificarsi un caso di instabilità tra due nodi però. Supponiamo che vi sia un collegamento B $\longmapsto$ A $\longmapsto$ X. Supponiamo che ad un certo punto si interrompa il collegamento A $\longmapsto$ X. Allora A setterà sulla propria tabella, aggiornandola, il costo per andare in X pari a ∞. Se il nodo B riceve l'aggiornamento di A, quindi egli saprà che non potrà può raggiungere il nodo X. Fin qui, tutto bene. Se però B pubblica la propria tabella prima di ricevere l'aggiornamento da A, allora egli vedrà che è sempre possibile raggiungere il nodo X anche quando è in realtà isolato.

  Figura 19: Caso di instabilità

  Allora possono essere intraprese diverse strade per far fronte a questo problema. Tecnica infinto-finito: si prevede di assegnare un valore max al costo di un collegamento. La tecnica split-horizon prevede invece l'invio di aggiornamenti solo per i cammini che non interessano il nodo destinazione. La tecnica split-horizon e poison reverse consente di non aggiornare il costo dei cammini che coinvolgono il nodo destinazione garantendo comunque un tempo di vita adeguato: con questo metodo B pubblicizza ad A il costo del collegamento verso X, assegnandogli un valore convenzionale grande, in quanto non interessa ad A (perchè vede direttamente X).

- Link state: con il link state un nodo deve avere la visibilità estesa a tutta la rete. Con questo algoritmo ci si limita alla misura del costo dei collegamenti con i nodi direttamente connessi (adiacenti). La tabella di routing per ogni nodo, in fase iniziale, comprende solo il costo per i vicini. Anche in questo algoritmo è prevista una fase collaborativa. I risultati dei due algoritmi sono ovviamente gli stessi. Si arriva quindi a definire una stessa rete ad albero, per ogni nodo della rete, che comprende i percorsi a costo minimo in grado di connettere quel nodo a tutti gli altri.

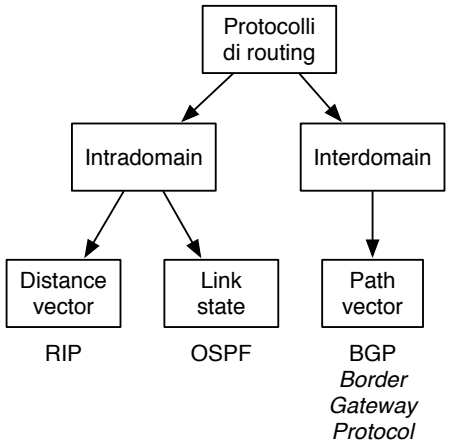
Questi due algoritmi trovano applicazione, per esempio, nell'algoritmo di Belmann e Ford.
h: passo d'iterazione
D_j^j: distanza del nodo considerato dal nodo j al passo h
d_{ij}: distanza del nodo i dal nodo j

1. $h = 0$, $D_j^h = \infty \forall j \neq s$
2. $h = h + 1$; $D_j^h = min_i(D_i^{h-1} + d_{ij}, D_j^{h-1})$
3. if $h = h_{max}$ stop else go to 2

Algoritmi gerarchici Nascono con lo scopo di rispondere al problem di un numero di routers potenzialmente ingestibile.

Autonomous System è un raggruppamento di più routers, visto dall'esterno come un unico dominio.

Figura 20: Classificazione dei protocolli di routing

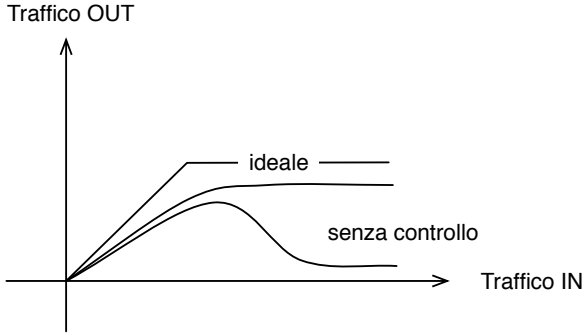


Protocolli di routing

1. AS terminale: è un sistema autonomo con una sola connessione verso un altro AS.
2. AS di transito: ha più connessioni verso AS, così da consentire il transito di messaggi.
3. AS con più connessioni: è simile al precedente ma non consente il transito.
   Tipologie di routing multi-casi.
   - Unicast: la comunicazione avviene tra sorgente ed utilizzatore;
   - Multicast: da uno a molti;
   - Broadcast: da uno a tutti.

Controllo della congestione La *congestione* di un collegamento avviene quando i parametri di riferimento sono fuori limite, si sono pertanto verificati dei ritardi.

Figura 21: Congestione dei dati



Per effettuare il controllo della congestione, si può ricorrere a due metodologie di analisi:

- metodi reattivi: si attivano dopo che la congestione è stata rilevata;
- metodi preventivi: si utilizzano per riuscire a prevenire (evitare) che la congestione abbia luogo.

Il metodo reattivo *Sliding Window* è basato sul credito che possiedono i nodi (metodo credit based). La trasmissione dei pacchetti da parte di un nodo è regolata da permessi che possono essere revocati se una congestione viene rivelata.

Il funzionamento di questo metodo è il seguente. Sia W il numero iniziale di pacchetti (credito) dato al nodo sorgente. I W pacchetti saranno trasmessi entro un intervallo temporale, finestra, di ampiezza Wτ, con τ = tempo di trasmissione di un pacchetto. Questa tecnica prevede un riscontro diretto da parte del nodo destinazione.

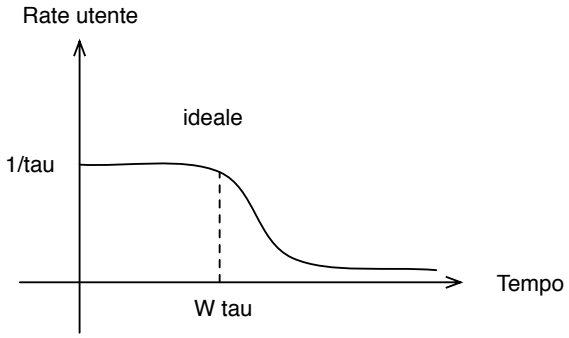
Se il riscontro arriva alla sorgente entro il tempo di finestra, allora la finestra viene fatta scorrere di una posizione e quindi si procede alla trasmissione di un nuovo pacchetto.

Se, viceversa, il riscontro arriva con un ritardo superiore al tempo di finestra, allora la trasmissione di un nuovo pacchetto viene ritardata. Se il riscontro avviene ad un tempo T>Wτ, allora il rate effettivo sarà:

$$\frac{W}{T} < \frac{1}{\tau}.$$

Il vero inconveniente è che non viene garantito all'utente almeno un rate minimo.

Figura 22: Rate utente minimo



Alcuni metodi preventivi sono l'*Admission Control* usato, ad esempio, in ATM. Altri esempi sono i metodi rate-based.

Il metodo *Leaky Bucket* significa letteralmente "secchio forato".

Assieme al metodo *token bucket* (cestino dei permessi), esso permette di trasmettere in sequenza tutti i pacchetti fino ad esaurire il numero di abilitazioni possedute (buffer).

Vengono riversati sulla rete i pacchetti con un fissato data rate. Vengono mantenuti nel buffer quelli per la trasmissione. Se vengono generati più pacchetti di quelli che è possibile mantenere nel buffer, essi vengono persi. In questo modo si controlla il rate max.

l vantaggio è che riesco a gestire meglio i picchi inaspettati del traffico e a controllare il rate medio.

Il token bucket ottiene un certo credito trasmissivo. Poi, quando c'è da trasmettere, lo fa utilizzando il credito a disposizione alla max velocità consentita dalla linea. Se ci sono k token e ci sono $h > k$ pacchetti da inviare, i primi k pacchetti sono immediatamente spediti, gli altri lo saranno in futuro quando si sarà acquisito altro credito trasmissivo.

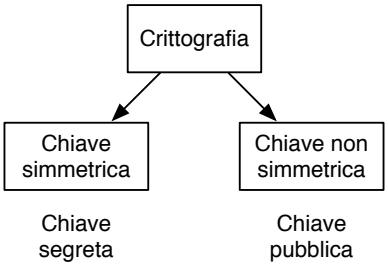
Sicurezza di rete Ottenere una buona sicurezza per le RTLC è oggigiorno un obiettivo sempre più importante, che tanto più si fa imminente tanto più si affinano le tecnologie e metodologie di aggressione informatica sui dati.

Ciò che preme di più mantenere, per una buona rete, è:

- riservatezza in quanto si vorrebbe che l'informazione scambiata rimanesse segreta;
- integrità di messaggio nel caso in cui si utilizzino tecniche di cifrazione per quest'ultimo;
- autenticazione dei dispositivi con i quali viene effettuata una connessione;
- protezione nei riguardi di intrusioni non autorizzate.

La crittografia è un ambito di studio che cerca metodi sempre più raffinati per cifrare (crittare) i dati informativi sulla rete.

Figura 23: Classificazione della crittografia



Tecnica a chiave simmetrica Il codice di Cesare prevedeva di numerare le lettere dell'alfabeto con i primi 21 numeri naturali: A $\longmapsto$ 0; B $\longmapsto$ 1; ... ; Z $\longmapsto$ 20. Prevedeva di scegliere un numero intero a piacere e di utilizzarlo come chiave. Dopo la scelta, veniva sommata la chiave ad ogni rappresentazione numerica di ciascuna parola del messaggio e successivamente riconvertita. In questo modo, ad esempio, la parola CIAO, corrispondente al codice 2/8/0/12, diventa HPET, corrispondente al codice 2+5/8+5/0+5/12+5 = 7/13/5/17.

Algoritmi a chiave pubblica Tra gli algoritmi più famosi e più utilizzati al mondo, ricordiamo l'RSA (Rivest-Shamir-Adelmann). A grandi linee, l'algoritmo consta dei seguenti passi:

- si scelgono due numeri primi e primi tra loro p e q (problema della ricerca dei numeri primi grandi);
- $n = pq$ e $z = (p-1)(q-1)$;
- scelgo un $e < n$ e diverso da 1 che sia primo rispetto a z;
- trovo un d tale che $ed - 1$ sia divisibile per z, ovvero: $(ed-1)modz = 0$;
- allora pongo che la chiave pubblica è (n, e), mentre la chiave privata è (n, d).

Le funzioni per la codifica e per la decodifica sono rispettivamente: $c = m^e modn$ e $m = c^d modn$, dove m rappresenta il numero corrispondente alla lettera e c rappresenta la codifica della lettera.

Un esempio di attacco del livello 3 (livello Network) per una rete potrebbe essere: un nodo malevolo risponde in modo errato alla richiesta di aggiornamento del costo di un collegamento. Si risolve il problema con l'autenticazione di ogni nodo.

Reti di sensori L'obiettivo primario di una rete ad hoc è quello di creare una rete non strutturata, impiegando soltanto la cooperazione dei partecipanti. Solitamente una rete ad hoc viene creata on demand a per no specifico scopo, senza richiedere una infrastruttura preesistente. In questa modalità i nodi devono essere doppiamente equipaggiati, per poter operare contemporaneamente sia da end-points che da routers. Essi devono essere auto-organizzati per poter stabilire una rete. Lo scopo più importante di queste reti è la mobilità spaziale e temporale. Si adattano bene a qualsiasi tipo di topologia di rete, dato che si possono auto-riorganizzare.

All'inizio del 21-esimo secolo un nuovo argomento di ricerca è emerso: la costruzione dei sensori e delle reti da loro originate. Una rete di sensori wireless (Wireless Sensor Network - WSN) serve a collezionare risultati di misurazioni e inviare questi ultimi ad una base centrale, chiamata sink station. Una rete di sensori, e quindi i sensori stessi, deve implmentare due operazioni fondamentali:

- sensing (percepire);
- communicating (comunicare).

Le maggiori caratteristiche di una rete di sensori sono le seguenti:

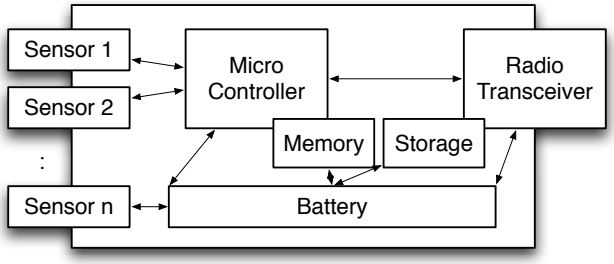
- grande numero di nodi;
- i nodi devono essere abbastanza vicini tra loro;
- flusso asimmetrico di informazioni;
- la comunicazione è formata dallo scatenarsi (triggering) di eventi o users-query;
- energia limitata;
- topologia statica;
- basso prezzo, dimensioni e peso per nodo;
- sensibilità ai fallimenti;
- i nodi non possiedono un IP (ID univoco) come nelle reti usuali;
- sicurezza dei dati limitata.

Le principali differenze di una rete di sensori rispetto ad una rete ad hoc sono la possibilità di contenere diversi ordini di grandezza superiore nel numero di nodi; ospitare una grande densità di nodi, inclini potenzialmente al fallimento; possibilità di cambiare la topologia di rete a seguito del fallimento dei nodi; potere computazionale limitato ed energia limitata; assenza di IP univoco; stretta collaborazione nell'operazione di sensing.

L'architettura di un nodo-sensore si compone dei seguenti pezzi hardware:

- un numero variabile di sensori, da 1 a n;
- un micro-controllore;
- radio-trasmittente;
- memoria e storage;
- batteria.

Figura 24: Struttura di un sensor node



Le applicazioni dei sensori sono svariate attualmente e coprono moltissimi ambiti tecnologici, come: quello militare, ambientale, del benessere, domestico, esplorazione di ambienti marini e non, monitoraggio ambientale, eccetera.

I diversi tipi di sensori si differenziano in base allo scopo per il quale sono stati costruiti e al loro uso. Così si possono distinguere sensori per la magnitudo sismica; per il monitoraggio termale, visuale, acustico, radar, eccetera.

La modalità operativa del sistema operativo a bordo nei nodi-sensori è legata al concetto di evento: al verificarsi di un evento, esso deve essere immediatamente processato dalla rete di sensori. Questo paradigma costruttivo viene chiamato in letteratura: event-driven.

Il messaggio informativo viene creato mediante due metodi essenziali:

- Push. Fa affidamento a misurazioni periodiche e vi è una comunicazione diretta del dato verso la base station (sink).
- Pull. È una strategia reattiva, che ha bisogno di una rchiesta attiva prima di cominciare una trasmissione.

Sensor Network Design I fattori più importanti di design per una rete di sensori sono:

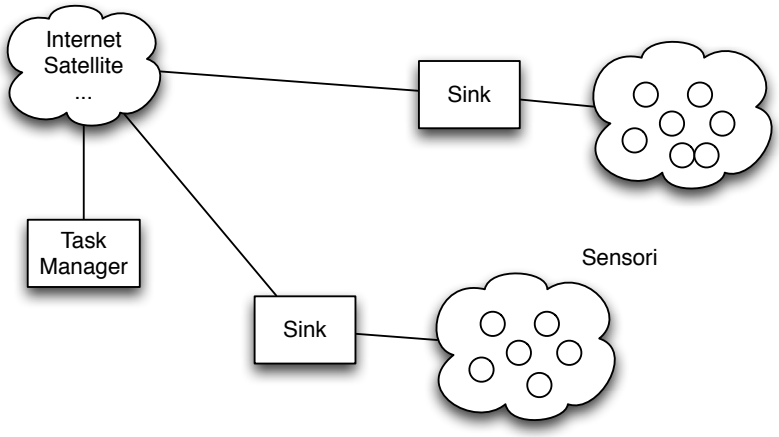
- scalabilità. Spesso il numero dei sensori può raggiungere ul milione in alcune applicazioni. La densità dei sensori in una regione (cluster) può andare dalle poche unità, fino alle centinaia.
- costi di produzione. Devono esser necessariamente contenuti e questo si ripercuote su tutta la WSN.
- vincoli hardware di produzione.
- topologia di rete. Bisogna che sia modificabile. I nodi devono potersi muovere ed essere sottoposti a forze esterne piuttosto dure (vento, pioggia). La modifica della topologia di rete potrebbe essere dovuta alla posizione dei sensori; alla scarsa raggiungibilità; all'energia mancante o al malfunzionamento.
- applicazioni sull'ambiente operativo. I sensori devono poter accedere all'ambiente operativo in maniera libera.
- trasmissione. Le modalità di trasmissione sono importantissime: possono essere radio, infrarosso o supporti ottici.
- consumo di energia (lifetime). I nodi di sensori hanno una forza limitata. La vita di un nodo-sensore dipende dalla durata della batteria a bordo. Solitamente vengono montate due batterie: una primaria ed una secondaria. La prima non ricaricabile e la seconda ricaricabile.

  Il problema del risparmio energetico è quello centrale per le WSN.

  Un sensore può essere un data originator o un data router. Sono necessari efficienti protocolli di networking.

  La consumazione della batteria è principalmente dovuta alle operazioni di:

Figura 25: Rete di sensori wireless (WSN)



– comunicazione (trasmissione e ricezione). Il power consumption per una comunicazione (P_c) è pari a

$$P_c = P_{te} + P_{re} + P_o,$$

con $P_{te/re}$ è il potere di consumazione per la radio-ricetrasmittente, mentre P_o è il potere trasmissivo per l'output.

– data processing (computazione) e sensing. È principalmente dovuta al tipo di applicazione; la modalità di percezione (sporadica o costante); la complessità di rilevamento dei dati; la rumorosità dell'ambiente.

Architettura delle reti di sensori Oltre ai classici layers di applicazione, trasporto, rete, collegamento e fisico, troviamo anche dei piani (planes) organizzativi (management) che sono richiesti per coordinare i layers al fine di svolgere le funzionalità critiche e caratteristiche delle WSN, come il consumo energetico, l'operazione di sensing sull'ambiente.

- Power management plane: controlla come un sensor-node utilizza il proprio potere di batteria;
- Mobility management plane: controlla e registra il movimento dei nodi-sensore;
- Task management plane: bilancia e schedula i compiti di sensing dei diversi sensori presenti in una precisa regione.

Il livello fisico è responsabile della selezione delle frequenze, trasporto delle frequenze, generazione, modulazione e scoperta del segnale e della crittazione dei dati, quando è richiesta.

Il livello di collegamento è responsabile del multiplexing dei dati di stream e dell'integrità dei dati. È essenzialmente il livello MAC. L'obiettivo primario del livello MAC è gestire l'accesso al wireless radio link e lo scambio ai pacchetti tra i nodi connessi. Vi sono due approcci base: quello con contesa e senza contesa.

Il livello di network deve assolvere essenzialmente a due compiti principali: routing (instradamento dei pacchetti) e data forwarding (passaggio di informazioni).

Il livello di trasporto garantisce di mantenere il flusso di dati se l'Application layer lo richiede.

Il livello Application implementa specifiche operazioni, organizza e coordina i processi per renderli effettivi. Questo livello espleta due funzioni principali:

- Query processing. La query dell'utente viene disseminata, diffusa ai nodi sensori e poi ricollezionati i risultati per l'utente. Vi si possono distinguere 3 approcci principali: push-based; pull-based; push-pull. Nella prima modalità (push) sono i sensori che cominciano il processodi information delivery, nella seconda è il sink che lo comincia. Nella terza, entrambi possono iniziarlo, dando vita ad una cooperazione.

  Le query possono a loro volta essere classificate in: continue, snapshot e storiche. Possono essere data-centric quando cercano informazioni da una collezione di sensori invece che da uno individualmente; geografiche quando la loro ricerca è estesa su un'intera area geografica.

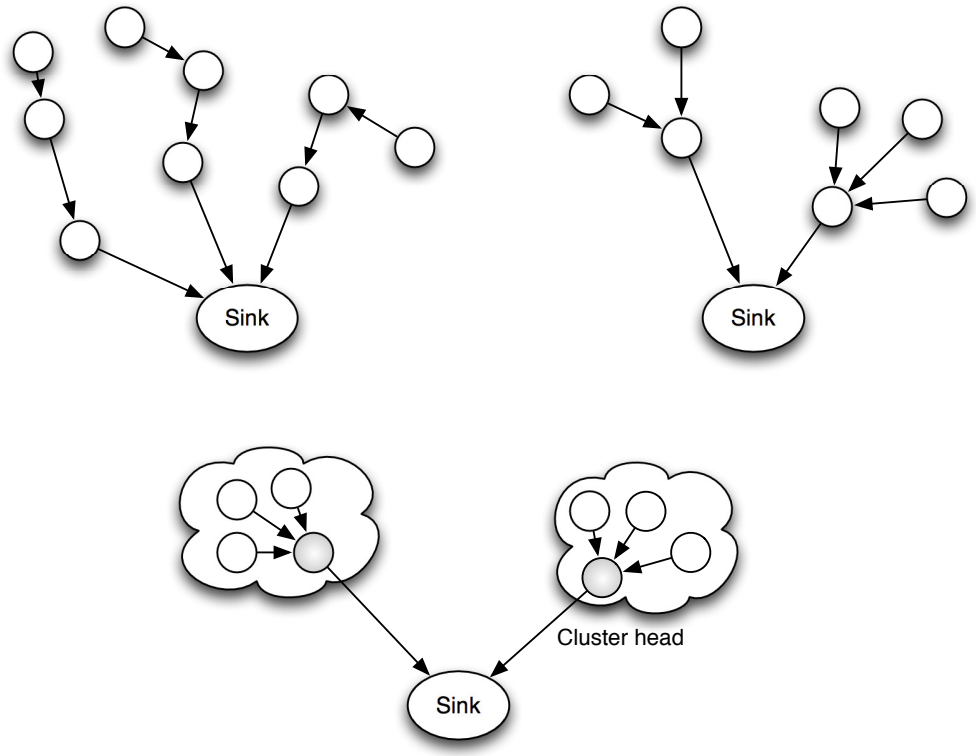
  I dati restituiti dalla query spesso subiscono una fare di aggregazione/fusione. I motivi principali di questa procedura sono i vincoli energetici della rete e nella ridondanza e correlazione presente tra i dati restituiti stessi. È una procedura che viene usata per poter anche predire degli eventi. L'aggregazione di più dati consiste nel combinarli tra loro mediante operazioni come media statistica, mediana, eccetera, in modo

da rappresentare l'informazione originaria. L'operazione di fusione, comporta l'aggiunta di informazioni (timestamp e locazione) sotto forma di metadati.

L'aggregazione e la fusione non sono prive di problematiche. Basti pensare alla distribuzione dell'errore che può essere presente nelle misurazioni dei sensori (chiaramente sconosciuta). Il problema dell'aggregazione dei dati in modo ottimale è un problema difficile NP. Esistono comunque sofisticati algoritmi che offrono buoni risultati.

Tra le topologie di aggregazione/fusione più ricorrenti ricordiamo: aggregazione a catena; ad albero; a grid.

Figura 26: Topologie



- Sensor Network Management. I casi reali di reti di sensori richiedono evidentemente dei administration tools. I punti chiave di questi tools sono i seguenti:
  - data overload: a quantità dei dati cresce drammaticamente con il numero dei sensori;
  - health monitoring: le condizioni ambientali e i vincoli di hardware rendono difficile il monitoraggio da parte dei sensori;
  - information visualization: vi sono molte sfide nel presentare un grande carico di informazioni.

  Gli amministratori della rete interagiscono con essa tramite il Network management tool. I suoi compiti devono essere: accendere/spegnere i sensori; muovere i nodi-sensori; interrogare i nodi-sensore; sincronizzare i nodi-sensore; scambiare i dati mediante algoritmi; dettare le regole dell'aggregazione dei dati collezionati.

  Essi devono possedere le seguenti caratteristiche: basso consumo energetico; non devono interferire con altri sistemi; devono essere tolleranti agli errori; adattarsi alle diverse topologie di reti; essere scalabili e adattabili alle dimensioni della rete.

  Possono essere di 3 tipi:

  - Passivi. Il sistema colleziona informazioni sulla rete e pre-processa le informazioni (off-line analysis).
  - Reattivi. Sono sistemi event-triggered. Il monitoraggio della rete è cominciato se un evento viene registrato. È possibile una riconfigurazione della rete a seguito di un evento. I dati vengono processati real-time (on-line analysis).
  - Proactive. Attivamente colleziona le informazioni sulla rete e le processa in modo real-time (on-line analysis).

  Spesso si tratta di architetture distribuite.

Protocollo MAC per WSN Gli obiettivi del protocollo MAC di una rete di sensori sono quelli già visti per le reti generiche, ma in più hanno quelli specifici per i sensori, in particolare:

- evitare le collisioni;
- scalabilità;
- efficienza energetica;
- latenza;
- equità;
- throughput;
- utilizzazione della banda.

I maggiori sprechi energetici che possono avvenire in una rete di sensori sono essenzialmente dovuti alle fasi di idle-listening dei processi; trasmissione e ricezione di informazioni (questi comuni a tutte le wirless network). L'obiettivo primario è ridurre al minimo il consumo energetico.

I maggiori problemi sono dovuti alle collisioni, laddove due nodi-sensore trasmettono i propri dati simultaneamente. I dati sono persi ed è richiesta una ri-trasmissione. Si può verificare il fenomeno dell'overhearing, quando un nodo riceve un pacchetto che non era a lui destinato. L'idle-listening è dannoso perchè spreca batteria del nodo-sensore.

Vi sono dei problemi con i quali deve scontrarsi il livello MAC delle WSN e che sono principalmente dovuti alle caratteristiche costruttive delle WSN. Vi sono problemi architetturali, come ad esempio: alta densità dei nodi; alta probabilità di collisione; problemi energetici già citati; problemi dovuti alla scarsa memoria e capacità computazionale dei nodi-sensore (complessi algoritmi non posso essere implementati; la convenzionale architettura a grandi livelli non si adatta bene); si devono possedere dei pacchetti di quantità limitata; encoders/decoders di basso costo.

Contention-based protocols Ogni volta che un pacchetto può essere trasmesso, il nodo si contende la trasmissione con i suoi vicini per l'accesso al canale. Il problema sta nella possibile presenza di una collisione, laddove due o più nodi fanno richiesta al canale contemporaneamente. C'è sempre il problema del terminale nascosto.

Multiple Acces with Collision Avoidance (MACA) È uno schema MAC basato sulla contesa. Se più nodi devono parlare con uno stesso nodo allo stesso tempo, cercano di inviare lui un messaggio quando egli inizia ad ascoltare.

Se un nodo fallisce nel proprio tentativo di conquistare il mezzo, egli va a dormire e si risveglia quando il destinatario è libero di ascoltare ancora.

Il campo *durata* in ogni pacchetto trasmesso indica per quanto tempo la trasmissione rimanente dovrà esistere se un nodo riceve un pacchetto destinato ad un altro. Egli sa quanto tempo dovrà rimanere silent. Il nodo setta questo valore in un vettore (NAV) è decide per lui un timer. La risoluzione delle collisioni è allora possibile: quando un nodo ha dei dati da trasmettere, per prima cosa controlla il contenuto di NAV, se non è 0, allora significa che il mezzo è occupato (virtual carrier sense).

MACAW È la versione di MACA per le reti wireless e introduce delle caratteristiche specifiche per queste reti al fine di ottenere una performance migliore.

Il problema è il seguente: in una configurazione a singola cella, i due nodi clients inviano i loro dati contemporaneamente al nodo master.

Algoritmo MACAW backoff (MILD-Multiplicative Increase and Linear Decrease): quando si verifica una collisione l'intervallo di backoff viene incrementato di un fattore moltiplicativo pari a 1.5 e se si verifica un successo, decrementato di 1.

Può avvenire anche il seguente problema: in una configurazione a doppia cella, entrambi i nodi clients inviano i propri dati ai rispettivi masters ma sono nello stesso range tra di loro. I clients inviano i dati alla loro stazione base e ogni streams è generato con lo stesso data-rate.

Oppure il problema opposto: i masters inviano i dati ai rispettivi clients, ma sono nello stesso range.

Oppure i due problemi mischiati tra loro: un clients invia dati al proprio master e l'altro master invia dati al proprio client. I masters sono nello stesso range. È un problema irrisolto.

S-MAC Il problema S-MAC (Sensor-MAC) è semplice: la fase di idle del nodo-sensore consuma troppa energia vitale. La soluzione proposta è rendere periodici i tempi di ascolto e dormita (listen e sleep). Ogni nodo va in un periodico sleep-mode durante il quale spegne la propria radio e setta un timer per il proprio risveglio. Quando si risveglia è pronto all'ascolto e rileva se qualche nodo vuole parlare con lui.

Chiaramente per poter funzionare correttamente è richiesta una fase di sincronizzazione. Per mantenere la sincronizzazione di schedule, sono scambiati periodicamente dei pacchetti SYNC. Il periodo di sincronizzazione è il periodo durante il quale, un nodo invia un pacchetto SYNC. I ricevitori del pacchetto SYNC aggiornano i loro timer counters immediatamente dopo averlo ricevuto.

fare più approfondito?? 18 parte II

Power-Control MAC protocol Il protocollo MAC Power-Control prevede una soluzione per localizzare il controllo dell'energia variando il potere di trasmissione per ridurre il costo energetico complessivo. Il protocollo migliora pure l'utilizzo dei canali wireless.

$$P_{desired} = (P_{max}/P_r)R_{xthresh} \cdot C,$$

dove $P_{desired}$ = è il potere trasmissivo usato; P_{max} = massimo potere trasmissivo disponibile; P_r = livello di potere ricevuto; $R_{xthresh}$ = è il livello della soglia di rumore; C = costante che dipende dalle condizioni ambientali.

Algoritmi di routing per WSN Gli algoritmi di routing per le reti WSN sono completamente distribuiti; cercano di minimizzare la coordinazione e il numero di messaggi in broadcast (costosi). Perchè non possiamo utilizzare i classici algoritmi di routing per le reti WSN? Perchè i sensor-nodes non possiedono un IP come i nodi delle normali reti; i sensori collaborano per riuscire in un unico goal; i nodi intermedi nel percorso di trasmissione possono effettuare aggregazioni di dati.

Le sfide più importanti sono le seguenti (sempre le solite):

- nodi limitati in potenza (calcolo e batteria);
- computazione: aggregazioni di dati; soppressione delle inormazioni ridondanti;
- comunicazione: limitazione della banda.

L'obiettivo primario è ancora una volta quello di minimizzare la dissipazione di energia. La cosa migliore sarebbe quella di avere: router che calcolano il percorso più breve; evitare i cicli di informazione; minimizzare i consumi; avere delle informazioni sulla topologia di rete.

L'algoritmo address-based di routing funziona identificando un percorso in base all'indirizzo di destinazione che possiedono i messaggi di dati. Ha bisogno tuttavia che i nodi possiedano un indirizzo univoco. Purtroppo si verificano dei ritardi nelle fasi di connessione e disseminazione.

Ad esempio, un pacchetto che ha l'indirizzo *TO:2* è passato di nodo in nodo fino a raggiungere la sua destinazione finale, ossia il nodo 2.

Il protocollo proactive routing, invece, fa affidamento sulla collezione periodica di dati e sullo scambio di informazioni topologiche sulla rete. Provvedono in questo modo, informazioni sempre nuove sulla rete (up-to-date).

Vi sono anche dei protocolli reactive on demand. Rispetto ai precedenti, non collezionano periodicamente informazioni e così riducono notevolmente il costo energetico. Essi cercano il percorso per un pacchetto se e solo se egli dev'essere trasmesso. Il ritardo di delay è maggiore però.

L'algoritmo DSDV (Destination Sequenced Distance Vector) periodicamente invia aggiornamenti a tutti i nodi vicini. Per ridurre il costo di aggiornamento, un approccio incrementale è qui utilizzato. Il vantaggio di questo algoritmo è la disponibilità di conoscenza dei percorsi ad ogni momento e di tutti i nodi. Chiaramente questo vantaggio diventa uno svantaggio per la banda, che viene ridotta. Il bisogno di aggiornamento comporta limitazioni alla sua efficienza.

L'algoritmo DSR (Dynamic Source Routing) non mantiene delle tabellee di routing per ogni nodo della rete. DSR utilizza pacchetti separati per scoprire il percorso migliore dalla sorgente alla destinazione, che sono: Route Request e Route Reply. Il vantaggio è che DSR non ha bisogno di inoltrare su tutta la rete messaggi per aggiornare le tabelle. Vi è sempre lo svantaggio di una lenta fase di set-up.

L'algoritmo AODV (Ad Hoc on Demand Distance Vector) è di tipi reattivo e cerca i percorsi tra la sorgente e la destinazione per un particolare messagio, su richiesta. Lo stesso procedimento di scoperta del percorso (route) usato in DSR è qui adottato. Possiede gli stessi vantaggi del DSR. Lo svantaggio è che la scoperta del percorso deve essere istanziata per ogni richiesta.

Possiamo dare una tassonomia dei diversi algoritmi di routing per le WSN, nel seguente modo:

- Data Centric Protocol: determinano la destinazione di un messaggio secondo la semantica del pacchetto. Hanno bisogno di tipi di messaggio predefiniti. Non sono presenti informazioni su indirizzi o quant'altro: uso semplificato. Viene adottata una modalità flooding probabilistica.
  - Flooding;
  - Gossiping;
  - SPIN;
  - Directed Diffusion;
- Hierarchical Protocols:
  - LEACH;
  - HEEND.
- Location based (geografici) protocols.

Flooding È una modalità di comunicazione molto semplice. Prevede di inviare un massaggio dati in broadcast a tutti i nodi vicini. Un messaggio è originato dal nodo più in alto a sinistra della rete e poi ripetuto a tutti i rimanenti, finchè i nodi non decidono di scartare il messaggio. Le principali modifiche a questo schema generale sono: Flooding geografico; Time to Live (TTL) Flooding. La strategia TTL è ugualmente semplice: appena viene ricevuto un nuovo pacchetto, viene incrementato il TTL di 1. Allora si controlla se il TTL attuale è minore di quello massimo (MAXTTL). Se è così, si prevede all'invio del pacchetto in broadcast, altrimenti non si fa niente. C'è il rischio di una broadcast storm, di una implosione dei messaggi. Accade quando il pacchetto vine ripetuto eccessivamente in broadcast a tutta la rete.

Gossiping Il concetto primario è trarre vantaggio dai risultati del flooding, ma risolvendo il problema della ridondanza dei messaggi. Il messaggio viene inoltrato ad un solo nodo vicino, scelto in maniera random. Tutti i messaggi si assumono come di pari importanza. Ogni trasmissione è effettuata con probabilità p. L'algoritmo è identico a quello precedente, soltanto che la condizione dell'if ha in AND anche quella che tiene conto della probabilità ($p_h < p$). Il problema è proprio quello di individuare una probabilità p ottimale. Chiaramente sono richieste delle informazioni topologiche sulla rete.

È possibile ottimizzare il gossiping utilizzando per i primi k nodi un flooding puro e per i restanti uno schema a gossiping con probabilità. Osservazioni sui nodi vicini sono utilizzate per stimare una probabilità di gossiping ottimale. Ogni volta che un pacchetto si avvicina alla destinazione, la sua probabilità di essere re-broadcastato aumenta.

Anche se queste tecniche sono semplici e reattive, hanno alcuni svantaggi, come: problema dell'implosione dei messaggi; potere di batteria ridotto; dati in overlap; resource blindness (nessuna conoscenza su potere informativo libero).

Lo SPIN (Sensor Protocol for Information via Negotiation) utilizza tre tipi di messaggi: ADV, REQ, DATA. Non appena un sensore ha qualcosa di nuovo, manda un messaggio di ADV (advertisement) in broadcast che contiene i nuovi dati, i metadati. I nodi interessati usano un pacchetto di richiesta del pacchetto. Allora i dati sono inviati con i pacchetti DATA. Questa operazione viene ripetuta finchè tutti i nodi non ne ottengono una copia. SPIN-PP e un protocollo di handshake articolato in 3 fasi. I vantaggi sono la sua semplicità; evita le collisioni e ha un costo minimale di start-up. Non è in grado, però, di isolare i nodi che vogliono ricevere informazione ma utilizza messaggi broadcast: spreca potere non necessario.

Lo SPIN-EC aggiunge un'euristica per la conservazione dell'energia. Fintantochè l'energia è piena, SPIN-EC si comporta come SPIN-PP. Quando l'energia comincia a scarseggiare, allora SPIN-EC riduce la partecipazione dei nodi (DORMANT). Così vengono introdotti diversi punti di forza: nessun ritardo e risparmio energetico fino al 70%.

Tecniche Agent-based L'idea principale è propagare delle query a seconda degli eventi della rete. Un numero fissato di eventi è presente sulla rete. Essi portano informazione circa gli eventi precedenti e distribuiscono questa informazione sulla rete (in modo random). Questo porta alla definizione di percorsi a particolari eventi.

Ogni nodo deve mantenere delle informazioni sui nodi adiacenti e una tabella per tenere informazioni sugli eventi. La tabella viene aggiornata non appena arriva un agente. Un agente viene creato tutte le volte che un nodo è testimone in un nuovo evento. Un certo grado di probabilità è presente in questa operazione. Gli agenti possono essere visti come pacchetti dotati di lunga vita. Un agente può collezionare informazioni su nuovi eventi e diffonderli su tutta la rete.

Algoritmi Direct-diffusion Questa tipologia di algoritmi sono stati costruiti per venire incontro alla tipiche caratteristiche di una rete WSN. Lo scopo principale è quello di identificare la locazione dei sink nodes.

In questo scenario, viene utilizzato un sistema di nomi: i dati sono nominati usando attributi in coppia (ATTRIBUTE-VALUE). L'interesse dei nodi così può essere espresso direttamente. I nodi sink rinforzano particolari vicini per disegnare dei percorsi di più alta qualità (elevato data rate).

Un nodo arbitrario (solitamente il sink) usa le coppie attributo/valore per costruire query on-demand.

I sinks periodicamente inviano messaggi broadcast ai sensori di interesse per estrarre le informazioni di interesse per le query in una particolare area. Come l'interesse si propaga, i dati possono essere localmente trasformati in ogni nodo o memorizzati temporaneamente (cached).

Quando un sensore individua un obiettivo, egli cerca nelle memorie cache per un riscontro dell'informazione cercata. Se la trova, frutta il percorso di alto rate costruito per trasmettere l'informazione.

I nodi sensori mandano le risposte GRADIENT SETUP indietro ai nodi sinks. Ogni sensore sul percorso compara gli interessi con i gradienti e aggiorna i propri campi gradiente. Ogni sensore poi trasmette i propri campi gradiente ai nodi vicini.

Possiamo identificare diversi criteri in base ai quali un gradiente dovrebbe essere rinforzato: l'ammontare dei dati ricevuti da un vicino; basso rate; variazione dei ritardi.

I dati sono inviati dalla sorgente alla destinazione, fino al sink, seguendo il percorso stabilito. Ogni nodo intermedio propaga il proprio pacchetto al vicino, fino al sink. Diverse modalità di propagazione dell'informazione possono essere definite: trasferimento su singolo percorso; trasferimento su più linee di percorso, ciascuno con un traffico proporzionale al proprio gradiente; trasferimento da singola sorgente a più sinks; trasferimento da sorgenti multiple a multipli sinks.

I maggiori vantaggi dell'algoritmo Direct Diffusion sono: essere un meccanismo data-centric, quindi non c'è nessun bisogno di un meccanismo di addressing. Ogni nodo può aggregare, percepire e memorizzare informazione. Il Direct Diffusion è efficiente dal punto di vista dell'energia, perchè è un modalità on demand. Non è necessaria mantenere un'informazione topologica sulla rete.

Gli svantaggi consistono nel fatto che non è generalmente applicabile in quanto è un sistema query driven. Per una applicazione dinamica, esso richiede un continuo flusso di dati, quindi non rappresenta una buona scelta. Gli schemi di nomi che utilizza l'algoritmo devono essere sempre definiti a priori ogni volta.

Protocolli gerarchici I protocolli gerarchici di routing sono stati proposti per far fronte ai problemi di scalabilità e riduzione del consumo energetico delle WSNs.

L'idea è raggruppare i nodi in cluster ragion con un nodo che funge da cluster head, con la responsabilità di aggregare, fondere e trasmettere i dati, secondo un qualche criterio.

I nodi cluster heads possono poi formare un livello ulteriore prima di poter raggiungere il nodo sink.

L'obiettivo del clustering è di massimizzare la similarità tra i diversi cluster e minimizzarne la differenza.

Una tecnica clustering deve essere scalabile e far fronte a diversi tipi di attributi.

Si possono distinguere diversi tipi di clustering:

- Distance-based Clustering;
- Conceptual Clustering;
- Centralized;
- Distributed or self-organized.

Vi sono due approcci principali, già menzionati: LEACH (Low Energy Adaptive Clustering Hierarchy) e HEED (Hybrid Energy-efficient Distributed Clustering Approach). L'obiettivo comune è ridurre il consumo energetico al fine di ampliare la vita della rete.

L'idea alla base del LEACH è di selezionare un nodo in maniera random e di eleggerlo a cluster head, così che l'energia viene dissipata tra tutti i nodi della rete. La formazione dei cluster è basata sulla potenza del segnale ricevuto.

Il cluster funziona attraverso due fasi. La fase di set-up, durante la quale i sensori si auto-eleggono per essere cluster heads locali con una certa probabilità (bilanciare la dissipazione di energia) e la Steady phase.

Un sensore sceglie un numero random compreso tra 0 e 1. Se tale numero è meno della soglia $T(n)$, allora il sensore diviene un cluster head. Se n è un elemento di G, allora$T(n) = P/1–P[rmod(1/P)]$, dove P è la percentuale per diventare un cluster-head, r è il round corrente e G è un set di nodi che non sono diventati mai ancora cluster heads negli ultimi $1/P$ rounds.

Dopo che i cluster-heads sono stati selezionati, essi avvisano tutti i sensori della rete che lo sono diventati. Ogni nodo ha accesso alla rete tramite i nodi heads, mediante un minimo di energia per essere raggiunti. Dopo che i nodi hanno ricevuto tale avviso dai cluster heads, essi decidono a quale cluster appartenere in base alla potenza del segnale di AD che i heads hanno loro mandato. Poi i nodi informano la testa del proprio cluster che

adesso fanno parte del suo cluster. Infine, le cluster heads stabiliscono i tempo in cui i sensori possono inviare loro i dati.

Ma qual è il numero ottimale di cluster?? Se sono troppo pochi, allora i nodi sono lontani dalle cluster heads, se sono molti, tanti nodi inviano i dati ai sinks.

Le conclusioni del LEACH sono le seguenti: riescono a ottenere un fattore 7 di riduzione sull'energia dissipata in confronto con la Direct Communication. I nodi muoiono in modo random e questo aumenta la vita della rete. È un metodo completamente distribuito e non richiede la conoscenza completa della rete. Rimane un metodo non applicabile in regioni larghe.

HEED rappresenta l'evoluzione diretta di LEACH. Il problema può essere formulato nel seguente modo: N nodi sono dispersi in un'area. L'obiettivo è identificare un set di cluster che coprono l'intero settore. I vincoli presenti sono che ogni nodo dev'essere mappato in un solo cluster; ogni nodo deve essere in grado di comunicare con il proprio cluster, mediante una singola connessione.

Protocolli di routing geografici Le tabelle di routing contengono informazioni su quale sarà il prossimo nodo cui dovrà essere trasmesso il pacchetto informativo. Esse vengono costruite esplicitamente. Un'alternativa consiste nel costruirle implicitamente, ricavando l'informazione dal posizionamento fisico dei nodi. Questo da vita ad algoritmi di routing geografico.

Data una destinazione, il nodo che possiede il messaggio seleziona il nodo successivo, secondo:

- la sua posizione;
- la posizione della destinazione;
- la posizione dei suoi vicini.

Maggiore è il raggio di scoperta del nodo che tiene il messaggio, e maggiore è il consumo energetico che ne deriva.

Due diverse nozioni di costo sono definite:

- costo di informazione: l'energia che è richiesta per acquisire informazioni topologiche;
- costo di comunicazione: l'energia richiesta per trasferire i dati dalla sorgente alla destinazione su un dato percorso della rete.

Ogni nodo può calcolarsi il costo ottimale del percorso da seguire. Così, il costo per la comunicazione è minimo, ma il costo della topologia è massimo. Vi è un chiaro tradeoff tra i due costi (per il calcolo del percorso ottimo e per la topologia della rete): il costo dell'informazione topologica aumenta all'aumentare del range; il costo della comunicazione solitamente diminuisce quando il range aumenta.

La domanda cui vorremo rispondere è allora la seguente: quanto esteso dovrà essere il range di ogni nodo della rete, affinchè sia garantito un routing geografico efficiente?

Applicazioni

- Militari;
- Ambientali;
- Rilevamento di incendi;
- Health care applications;
- monitoraggio dei prodotti agricoli;
- pulizia delle strade;
- sensori di allarme: edifici, strade, ecc.
- monitorare gli sports: calcio, baseball, atletica, ecc.
- monitoraggio dei fondali marini.