Contents

1 Serie di Fourier

Un segnale che ha una durata finita può essere immaginato semplicemente come la ripetizione infinita dell'intero schema, ossia come una rappresentazione dove l'intervallo da T a $2T$ è uguale all'intervallo da 0 a T. La serie di Fourier è infatti, in matematica, la rappresentazione di una funzione periodica tramite la combinazione lineare di funzioni sinusoidali (seno e coseno).
È possibile quindi rappresentare un segnale tramite delle funzioni di questo tipo, le quali permettono una analisi e modellazione molto efficacie.
Su questo principio si basano tutte le reti, ed in generale il passaggio di dati tramite mezzi di trasmissione > purtroppo, nella pratica, questi ultimi attenuano in modo non uniforme i componenti della serie di Fourier, generando così una distorsione del segnale.
Per ovviare a questa distorsione, le ampiezze fino ad una certa frequenza vengono trasmesse senza modifiche, da quella frequenza in poi vengono attenuate > l'intervallo di frequenze trasmesse senza una forte attenuazione è chiamato banda passante (generalmente viene indicata come banda passante quella compresa tra 0 e la frequenza dove la potenza è attenuata del 50%).

Pregi scomporre un segnale in più componenti permette uno studio più preciso del segnale.

Difetti none

Ambiti d'uso viene ampiamente usata nelle comunicazioni in generale, per la trasmissione dei dati > la scomposizione del segnale in più sinusoidi migliora la comprensione delle onde. Si passerà poi alle varie modulazioni per ovviare ai problemi dovuti alle attenuazioni o alle distorsioni.

2 Bit rate o baud rate

Il *bitrate* è una quantità di informazioni digitali che viene trasferita o registrata in una certa unità di tempo. Si tratta quindi della velocità di trasmissione, espressa in *bit/s*.
La velocità di trasmissione è anche detta banda e dipende dal tipo di mezzo trasmissivo utilizzato e dalle sue condizioni fisiche al momento dell'uso.
Il baudrate invece rappresenta il numero di "simboli" che viene trasmesso in un secondo, ossia un determinato e fisso numero di bit (che differisce in base alle techiche di modulazione utilizzate). Non va confusa con il sopracitato bitrate, in qunato misurano unità differenti ($bitrate = baudrate \cdot n$ dove n è la cardinalità dell'alfebo utilizzato).

Pregi grazie a queste unità di misura è possibile dare una rappresentazione quantitativa della velocità di trasmissione del mezzo.

Difetti none

Ambiti d'uso queste metriche vengono utilizzate nelle reti wireless e cablate.

3 Satelliti

Esistono 3 tipi principali di satelliti: i LEO, i MEO, i GEO, rispettivamente *lwo earth orbit*, *medium earth orbit* e *geostationary earth orbit*.
In generale, i satelliti comunicano tra loro ad alte frequenze, questo per diminuire la dispersione ed aumentare la banda, possono infatti essere pensati come dei grandi ripetitori di microonde posti nel cielo. Ciò può essere fonte di complicanze nel caso vi siano condizioni meteorologiche avverse, che potrebbero creare interferenze.

- **LEO** sono posti inferiormente alla fascia di Van Allen inferiore, di conseguenza sono i più bassi dei 3 tipi. Vengono usati principalmente per le telecomunicazioni, hanno una bassa latenza e necessitano di meno potenza per trasmettere rispetto agli altri tipi (ciò vale da entrambi i lati della comunicazione, cioè anche per gli apparecchi terrestri che trasmettono al satellite). Il costo per mandarli in orbita, inoltre, è più basso rispetto ai MEO e GEO. Alcuni satelliti LEO sono Iridium (gruppo di 66 satelliti

che ruotano attorno al globo e forniscono servizi di fax, telefonia vocale exx ovunque nel mondo mare e in volo compresi, creando in questo modo una rete di telecomunicazioni nello spazio e trasmettono il segnale ricevuto), Globalstar (formato da molti meno satelliti rispetto a Iridium, i quali non creano propriamente una rete nello spazio, in quanto fungono solo da ripetitori del segnale che viene trasmesso in realtà dalla rete terrestre) ma anche la più recente Starlink (progetto fondato dalla agenzia spaziale SpaceX con lo scopo di portare la connessione internet satellitare a bassa latenza ovunque nel mondo e con costi contenuti rispetto alle alternative già esistenti).
In generale, i satelliti LEO sono molto utilizzati in ambito militare, per le telecomunicazioni ma anche per i sistemi di telerilevamento di sensori.

- **MEO** compresi tra la fascia di Van Allen inferiore e la fascia di Van Allen superiore troviamo i satelliti *medium earth orbit*. Si tratta infatti di satelliti in orbita media, ciò comporta che il costo per lanciarli in orbita si ainferiore rispetto ai satelliti geostazionari, ma allo stesso tempo non ne siano necessari così tanti come i satelliti LEO.
  Necessitano tuttavia di più potenza di questi ultimi per trasmettere, siccome sono più distanti, olter ad avere potenzialmente più rischi di interferenze. Inoltre, rispetto ai satelliti GEO, si perde la comodità del punto fisso) rispetto all'equatore terrestre). In questa fascia troviamo Sputnik, il primo satellite lanciato in orbita della storia e soprattutto i satelliti che si occupano del sistema GPS. Quest'ultimo era all'inizio una esclusiva militare, tuttavia si è poi deciso di aprirne l'utilizzo al pubblico)in principio con una precisione di 100 metri, poi ridotta a 20 metri). In generale, a causa del fatto che prima di triangolare la posizione sarebbe necessario per i dispositivi sulla terra attendere il passaggio e la trasmissione del segnale da parte di 3 o 4 satelliti, il "tempo di fix" per ottenere la posizione dovrebbe essere molto lungo, anche di qualche minuto. Questo problema è tuttavia stato risolto dal sistema A-GPS > si tratta di un potente computer centrale che viene utilizzato dagli ISP / operatori di servizi mobile, il quale ha la funzione di calcolare costantemente la posizione dei satelliti del GPS, per poi fornirla direttamente ai telefoni cellulari che richiedono una calibrazione della posizione.

- **GEO** i satelliti *geostationary earth orbit* sono collocati al di sopra della fasci di Van Allen Superiore, si tratta di satelliti definiti come "geostazionari", in quanto la loro posizione risulta fissa rispetto alla linea equatoriale terrestre. Vengono collocati infatti a distanza di 2 gradi nel pinao equatoriale fra loro, ne deriva che c'è spazio solo per 180 satelliti di questo tipo > ciò comporta che il loro lancio sia spesso fonte di collisioni e dispute fra i diversi paesi.
  In generale, si tratta di satelliti di grossa dimensione, la cui funzione principale è la trasmissione satellitare di contenuti televisivi, oltre che essere molto utilizzati in ambito meteorologico. I lanci dei satelliti GEO sono molto costosi, tuttavia il loro vantaggio principale è la stabilità (utile per questioni sia di osservazione ma anche di orientamento delle antenne). Possiamo contare sui satelliti geostazionari della seconda metà del XX secolo, il primo esemplare "commerciale" è stato Intelsat I, un satellite realizzato da Comsat.

Pregi rispetto alla fibra, i satelliti danno una maggiore garanzia di copertura e permettono di connettere/raggiungere con la stessa velocità l'intera superficie del globo. Per questo motivo i satelliti vengono infatti molto utilizzati in luoghi inospitali o difficilmente raggiungibili da connessioni cablate.

Difetti costi maggiori per l'installazione di un sistema satellitare rispettoa all'installazione della fibra ottica, economa di mantenimento molto esosa, soprattutto per quanto riguarda i satelliti in orbita più alta (attualmente infatti per le telecomunicazioni si è orientati ad utilizzare la fibra piuttosto che la connessione satellitare).

Ambiti d'uso sono utilizzati nell'ambito delle telecomunicazioni (vocali e via fax), i MEO per la gestione del sistema GPS, i GEO in ambito meteorologico ed in generale tutti i sateliti in ambito militare.

4 Modem e modulazione

Per inviare segnali digitali attraverso una linea telefonica il computer deve convertire i dati in forma analogica per poterle trasmetterere attraverso l'ultimo miglio. Questa conversione avveien attraverso un dispositivo

chimato modem.
I problmei pincipali delle linee di trasmissione però:

1. la perdita di energia per via della propagazione del segnale verso l'esterno, dipendente dalla frequenza del segnale. Questa perdita è anche detta **attenuazione**;

2. distorsione, causata dal fatto che ogni componente di Fourier si propaga a velocità diverse rispetto al cavo;

3. rumore, ovvero l'energia indesiderata generate da sorgenti esterne al trasmittore. Per minimizzare questi problemi viene utilizzata la trasmissione AC che introduce un tono continuo, chiamato portale d'onda sinusoidale, la cui ampiezza, frequenza o fase possono essere modulate per trasmettere informazioni. Un apparecchio che accetta un flusso seriale di bit in ingresso e produce una portata modulata è appunto il modem.

Modulazione FSK si modula la frequenza in maniera proporzionale all'ampiezza che si vuole trasmettere, ovvero cambia la frequenza in base al simbolo che si vuole trasmettere.

Modulazione AM modulazione in ampiezza in proporzione all'ampiezza da trasmettere, viene usata principalmente nelle trasmissioni radio.

Modulazione PSK modulazione di fase, cambio fase del segnale a seconda del simbolo da trasmettere.

5 FDM, TDM, CDM (algoritmi di multiplexing e selezione banda)

Ne esistono 3 tipi diversi:

- FDM (frequency division multiplexing), divide lo spettro in varie bande di frequenza e ad ogni utente viene assegnata una porzione della banda con uso esclusivo. Vengono usati 12 canali voce uniti in multiplexing nella banda tra 60 e 108 MHz. Viene usato dal GSM.

- TDM (time division multiplexing), l'intera banda viene assegnata a tutti gli utenti a turno per un tempo limitato secondo Round Robin. Usato da Bluetooth, GPRS, GSM.

- CDM (code division multiplexing), anche conosciuto come CDMA, è il protocollo di accesso multiplo a canale condiviso. È realizzato moltiplicando in trasmissione l'informazione generate per un'opportuna parola detta "chip", questa sequenza in uscita sarà successivamente modulata e trasmessa sul canale. In ricezione il segnale sarà costituito dalla somma vettoriale di tutti i segnali trasmessi dalle singole stazioni.

6 Modulazione di frequenza

Durante l'invio di informazioni, il segnale può subilre attenuazione, distorsione o vnire in generale disturbato dal rumore > per questo motivo si tende ad evitare l'uso di un largo intervallo di frequenze. Questi effetti rendono la trasmissione in banda base (DC) una soluzione adatta solo a velocità basse e distanze brevi. Piuttosto, per risolvere questi problemi viene utilizzata la trasmissione AC, ossia un tono continuo (portata d'onda sinusoidale) nell'intervallo compreso tra 100hZ e 200hZ, lavorando sulla modulazione della sua ampiezza (modulazione AM), frequenza (modulazione FM) o fase.
La modulazione di frequenza (FM) non è altro quindi che una tecnica di trasmissione utilizzata per trasmettere informazioni usando la variazione di frequenza dell'onda portante. Rispetto all modulazione in ampiezza (AM) ha il vantaggio di essere molto meno sensibile ai disturbi e permette una trasmissione di miglior qualità. Ha inoltre un'efficienza energetica molto maggiore dato che la potenza del segnale modulato FM è esclusivamente quello della portante.

pregi permette di ridurre i problemi di attenuazione e distorsione della linea.

difetti necessita di circuiti complessi sia per la generazione del segnale sia per la sua ricezione. Questi problemi sono stati, per la maggior parte, superati dalle attuali tecnologie.

ambiti d'uso la modulazione FM viene utilizzata soprattuto in ambito di broadcasting commerciale ed è in generale molto più comune della modulazione in ampiezza.

7 Modulazione Delta

La modulazione delta è un tipo di compressione e digitalizzazione dei dati di un segnale analogico. Si tratta di una variazione del differntial pulse coe modulation (DPCM) ed è stato introdotto con la generazione 2G dei telefoni mobili. A differenza del segnale analogico, il senglae digitale ricavato dalla modulazione delta utilizza molta meno banda, ma perde una discreta quantità di informazioni essendo un tipo di compressione lossy.
A differenza di altre tecniche, piuttosto che quantizzare il valore della forma d'onda analogica in ingresso, la modulazione delta quantizza la differenza tra la fase corrente e quella precedente. Nella sua forma più semplice, la variazione dell'onda per ogni unità di tempo può essere descritta da un singolo bit 1 od un singolo bit 0, rispettivamente se il segnale in ingresso è positivo (aumento nel grafico che descrive l'onda) o negativo (diminuizione nel grafico che descrive l'onda).
Grazie a questa tecnica, è possibile comprimere e digitalizzare il segnale analogico, con il risultato di gravare meno sulle linee e permettere comunicazioni più veloci, a discapito della precisione. Per questo motivo si possono presentare problemi in ambiti nei quali il segnale cambia troppo velocemente (è infatti l'utilizzo della modulazione delta per comprimere e digitalizzare la musica), in quanto si perderebbero molti dati. Se il cambiamento del segnale analogico è troppo ampio, si ha quindi una perdita di dati, ma in ambito telefonico (più precisamente nelle chiamate), questo non è un problema.

ambiti d'uso comunicazioni satellitari o nelle comunicazioni voce/mobile.

8 QAM, QAM16, QAM64 e QPSK

QAM è una modalità di modulazione in fase ed in ampiezza (sia digitale che analogica) per questo motivo si può rappresentare in "costellazioni". Le portanti sono sinusoidi. Ogni pallina equivale ad uno spostamento sull'asse temporale dell'onda che sta trasmettendo > questo consente di aumentare il bitrate, tuttavia, quendo questi spostamenti sono troppo piccoli è possbile che a causa di interferenze vengano scambiati i simboli che si stanno trasmettendo. Proprio per questo motivo, QPSK è il tipo di modulazione più robusta (pur essendo solo di fase) > più si aumentano i puntini, più aumenta il data rate, ma anche la fragilità della connesione.
QAM è quindi un sistema di modulazione numerica di ampiezza in quadratura, sia digitale che analogica. Il termine quadratura indica che differiscono di 90 gradi.
Il segnale in ingresso viene suddiviso e modulato per l'ampiezza. Nel caso di segnali digitali, si sommano i segnali modulati e si ottiene una forma d'onda che risulta una combinazione della modulazione di fase e qualla di ampiezza. Ciascun tipo di modulazione QAM è caratterizzato da un diagramma (costellazione) su vui sono rappresentati tutti gli stati della portante.
La QAM, rispetto alla PSK (phase shift keying), migliora l'immunità di rumore.
QAM16, QAM64, ecc invece non sono latro che un tipo di costellazione QAM che utilizza rispettivamente 4 ampiezza e 4 fasi (QAM16) oppure 16 ampiezza e 16 fasi (QAM64), per un totale di 16 o 61 punti diversi nella costellazione.
In realtà, il miglior spostamento sarebbe quello di tipo circolare, tuttavia i circular QAM, pur essendo ottimali dal punto di vista della robustezza, non vengono utilizzati a causa della difficoltà nella generazione e decodifica dei messaggi.
In generale, nelle modulazioni QAM non viene utilizzata la modulazione in frequenza in quanto è così più facile generare il segnale e facilita la sincronizzazione dello stesso.

pregi permette di aumentare il data rate.

difetti ogni modem ha un suo schema di costellazione e può comunicare solo con altri modem che possiedono lo stesso, anche se la maggior parte dei modem più recenti è comunque in grado di emulare costellazioni più lente della propria.

ambiti d'uso fa parte dello stato fisico, questo tipo di modulazione è utilizzato come standard nei modem telefonici.

9 Codifica Manchester

Si tratta di una tecnica per trasmettere codici binari e determinare gli 1 e gli 0, è utilizzata nel protocollo Ethernet a causa della sua capacità di auto-sincronizzazione (la codifica ethernet non necessita di un segnale esterno di sicronia).
Inizialmente la codifica Manchester era stata giudicata da molti una scelta sbagliata e veniva reputata carente rispetto ad altre tecniche di trasmissione di dati binari, questo a causa del fatto che per utilizzarla era richiesto il doppio della banda rispetto alla pura conversione binaria 0-5 volt. Tuttavia, grazie anche all'avanzamento tecnologico ed all'aumentare della velocità media di trasmissione dei dati, si è rivelata nel corso degli anni una scelta corretta, essendo la codifica Manchester una tecnica molto precisa, oltre che ad essere vantaggiosa dal punto di vista economico (l'hw non è molto costoso).
Nella codifica Manchester, i bit vengono indentificati da 2 picchi invece che 1 (ed è questo il motivo per cui 50% della banda va persa), infatti in questo tipo di codifica è la direzione del cambio di energia che identifica gli 1 e gli 0, e non il picco in sè.

10 Tecniche di stuffing

Lo scopo dello strato fisico è quello di prendere un flusso di bit e cercare di portarlo il più integralmente possibile agli strati superiori > di norma, tuttavia, non esiste alcuna garanzia riguardo la correttezza dei dati. Il modo migliore per farlo è quello di suddividere il flusso di bit in dei frame, per poterli così controllare in maniera migliore.
Uno dei metodi più utilizzati è il byte stuffing, che consiste nell'utilizzare un particolare byte conosciuto come flag byte (FLAG) che delimiterà l'inizio e la fine di un frame > in questo modo, se il destinatario dovesse perdere la sincronizzazione, può semplicemente ricercare il flag byte per capire dov'è l'inizio e la fine del frame corrente.
C'è tuttavia un problema: nel caso si volesse trasmettere informazioni/bit che coincidono con i bit scelti come flag byte, il destinatario potrebbe cadere in confusione. Nel byte stuffing, la soluzione che è stata addottata è quella di utilizzare un ulteriore byte conosciuto come escape byte (ESC), da aggiungere ad ogni occorrenza reale dei bit corrispondenti al FLAG (intesi quindi come bit da trasmettere e non come fine/inizio di un frame). Questa procedura di aggiunta di byte aggiuntivi per determinare le caratteristiche dei frame, in generale, è conosciuta come stuffing.

pregi risolve il problema della sincronizzazione dei frame, permettendo una suddivisione dei bit in frame.

difetti [legato all-uso di caratteri da 8 bit (1 frame), che non è supportata da tutte le codifiche. Inoltre, il numero di bit superflui (ESC byte, FLAG byte, ecc) è notevole.
La soluzione che è stata adottata per questi difetti è l'utilizzo di una procedura di stuffing diversa, conosciuta come bit stuffing > si tratta di una tecnica che permette di creare data frame con un numero arbitrario di frame, oltre che permettere l'utilizzo di un numero arbitrario di bit negli stessi (e quindi non solo 8 come nel byte stuffing).
Il bit stuffing è molto più efficace: inserisce infatti solo un bit ogni volta che trova una sequenza dei primi n-1 bit uguale al FLAG di n bit. Siccome questo bit viene inserito sempre a parte nei FLAG, ricostruire il messaggio originale risulta molto semplice, basterà infatti togliere il bit superfluo ogni volta che si incontra la seguenza di n-1 bit.

ambiti d'uso il bit stuffing viene utilizzato nel protocollo HDLC, il byte stuffing nel protocollo Ethernet (per migliorare la sincronizzazione ad elevatissime velocità).

11 ALOHA

In telecomunicazioni ALOHA è un protocollo di rete atto a garantire le funzionalità di accesso multiplo al mezzo di trasmissione dati condiviso tra più utenti > si tratat quindi di un protocollo multiaccesso, ciò significa che indipendentemente dal numero di utenti connessi alla rete, la banda sfruttata rimane stabile e non si avvicina allo 0 all'aumentare di essi.
ALOHA puro > nella sua variante base, in ALOHA ogni utente spedisce i propri pacchetti senza sapere se il canale trasmissivo è occupato (manca il carrier sense) e quindi senza sincronizzazione con gli altri utenti della rete. Se il pacchetto dovesse collidere con altri, viene semplicemente fatto attendere un tempo casuale (opportunamente limitato) per poi riprovare l'invio. Con ALOHA puro, la banda massima sfruttata del canale trasmissivo è intorno al 18%.

pregi permette l'accesso multiplo di più utenti allo stesso mezzo trasmissivo e favorisce le comunicazioni broadcast.

svantaggi è molto poco efficiente in telecomunicazioni con tante stazioni.

ambiti d'uso protocollo utilizzato a livello di indirizzi MAC, viene usato dalle varie stazioni nelle comunicazioni broeadcast per condividere lo stesso mezzo trasmissivo tra più utenti.

11.1 ALOHA slotted

Aggiungendo la temporizzazione si ottiene ALOHA slotted, in questo protocollo, che è un miglioramento ed aggiornamento dell'ALOHA base. Esistono degli slot di tempo che determinano l'accesso al mezzo trasmissivo, infatti, gli utenti non possono trasmettere a cavallo di questi. Con ALOHA slotted, la banda massima sfruttata dael canale trasmissivo raddoppia (circa 36%).

pregi miglioramento di ALOHA puro, raddoppia il grado di successo.

svantaggi è richiesto un segnale di sicronia esterno che gestisce gli slot di tempo ed indichi alle stazioni quando trasmettere.

12 CSMA

Il CSMA è una tecnica di trasmissione dati per la quale ogni dispositivo perima di avviare la trasmissione dei dati deve verificare se latri nodi stanno trasmettendo sullo stesso canale, rilevando quindi la presenza di portanti. Solo se il canale risulta livero, il dispositivo inizia la trasmissione, altrimenti è tenuto ad attendere un tempo arbitrario e diverso in base allo standard CSMA utilizzato prima di riprovare.

CSMA 1-persistente primo tra i protocolli CSMA, ha la particolarità di inviare con probabilità 1 sul canale in caso di nessun rilevamento. La possibilità di inviare non appena il canale risulta libero non lo rende immune da collisioni, le quali comunque potrebbero accadere nel caso di stazioni che controllano nello stesso momento un canale vuoto ed inviano contemporaneamente.

CSMA non-persistente prima di trasmettere, ogni stazione controlla il canale. Se lo trova libero, inizia ad inviare dati, altrimenti se risulata occupato, la stazione non esegue un controllo continuo per tasmettere subito il proprio frame, ma attende un intervallo di tempo casuale prima di ripetere l'algoritmo (allunga quindi il delay).

CSMA p-persistente variante che si applica su canali divisi in intervalli temporali. Quando è pronta a trasmettere ogni stazione controlla il canale. Se lo trova libero, trasmette subtio con probabilità p, e rimanda fino all'intervallo successivo con probabilità 1=1-p. Nel caso in cui anche quell'intervallo risultasse libero, la stazione trasmette oppure rimanda un'altra volta. Il processo si ripete finchè il frame non è stato trasmesso.

pregi migliora di molto le prestazioni di ALOHA ed ALOHA slotted, oltre che ad avere il vantaggio di annullare la propria trasmissione in caso di collisione (così da risparmiare tempo e banda).

difetti none

ambiti d'uso utilizzato prevalentemente in connesioni dove il rilevamento delle collisioni non è realizzabile (es. connessioni wireless). Utilizzato nello standard IEEE 802.3 (Ethernet), oltre che nelle reti LAN Ethernet (nella variante migliorata CSMA/CD).

13 Protocolli a contesa limitata / Adapdive Tree Walk

CSMA/CD non è sufficiente se le stazioni trasmittenti sono tante, siccome aumenta in tal caso il content period, onoltre non è adatto ad un carico di rete basso. CSMA invce ha caratterisctiche inverse. Cercando infatti di trovare un metodo che combini le caratteristich emigliori di uno e dell'altro si è capito che l'unico modo per ridurre le collisioni (anche dei piccoli pacchetti appositi) è ridurre i contendenti > su questa constatazione si basano i protocolli a contesa limitata.
In questi ultimi, le stazioni vengono divise in gruppi (non necessariamente disgiunti) ed ongi gruppo si contende uno slot. La suddivisione in gruppi, inoltre, cambia in base al diverso carico di rete, dato che con un carico alto c'è più probabilità di collisioni (gruppi piccoli), viceversa con un carico basso c'è meno probabilità di collisioni.
Il protocollo Adaptive Tree Walk segue queste modalità: idelamente partendo 1 singolo gruppo che contende per ogni slot, ed in caso di collisione viene diviso in due (contenimento x 2 slot diversi). Queto avviene ricorsivamente sui sottogruppi. Chiaramente (organizzando la suddivisione in gruppi come in grafo ad albero), in una situazione reale non si parte dal livello 1 ma dal livello $log(2q)$, dove q è il nmero di stazioni previste che vogliono trasmettere (in base al traffico dati precedente) in modo tale da distribuirle una per gruppo (si spera) ed evitare le collisioni (se si partisse più in alto, la possibilità di collisioni sarebbe molto alta, rendendo di fatto inutile partire da così in alto).

pregi garantisce un ritardo limitato in caso di basso carico ed una buona efficienza in caso di carico più elevato.

ambiti d'uso viene utilizzato nelle connessioni con più stazioni che vogliono trasmettere nello stesso mezzo di trasmissione.

14 Stazione nascosta

Quello della stazione nascosta è un problema che si verifica nelle comunicazioni wireless ed è dovuto al fatto che i dispositivi non conoscono l'intera topologia della rete di cui fanno parte. Questo porta inevitabilmente al crearsi di zone di interferenza nelle quali si verificano delle collisioni. La stazione nascosta quindi non è altro che una stazione che vuole inviare un segnale ma non riesce a ricevere i segnali dei concorrenti a causa della distanza.
Supponiamo per esempio di avere tre dispositivi A, B e C: A vuole inviare a B, prima di farlo, ascolta se ci sono altre connessioni, altrimenti procede all'invio. C però è troppo distante da A e quest'ultimo non riesce a sentirlo, ma è abbastanza vicino a B per inviargli dati > lo fa e va in conflitto con l'invio di A.
Il problema della stazione nascosta è stato risolto dal MACA, ossia il protocollo Multiple Access with Collosion Avoidance ed all'utilizzo di pacchetti RTS (request to send) e CTS (clear to sent). Questi ultimi, tra l'altro risolvono anche il problema della stazione esposta.

15 stazione esposta

Il problema della stazione esposta invece è l'inverso di quello della stazione nascosta. Supponiamo di avere 4 dispositivi A, B, C e D: B trasmette ad A, C vuole inviare un pacchetto a D e controlla la presenza di portante sul mezzo di trasmissione, rilevando che B non intralcerebbe la trasmissione di C, ma questo non lo può sapere, e di conseguenza si genera uno stallo inutile.

16 Descrivere i vari tipi di cavo e confronto

I principali tipi di cavo utilizzato nelle telecomunicazioni sono: il doppino (o cavo annodato / UTP), il cavo coassiale e la fibra ottica:

- Cavo annodato (UTP), cavo formato da una coppia di fili annodati da qui la dicitura "twisted" il quale serve a limitare l'interferenza reciproca (crosstalk). I due fili sono detti anche "doppini" e sono spessi circa 1mm ciscuno. Possono estendersi per diversi km senza chiedere amplificazione del segnale e vengono usati per trasmettere dati analogici e digitali. UTP3 Bandwidth250MHz, UTP5 Bandwidth600MHz;
- Cavo coasiale, essendo pi schermato del cavo annodato si pu; estendere per distanze maggiori e a velocit' pi' elevate. Viene utilizzato maggiormente per la tv via cavo e le MAN e la sua Bandwidth è di circa 1GHz;
- Cavi in fibra ottica, un sistema ottico è formato da tre componenti fondamentali: la sorgente luminosa, il mezzo di trasmissione e il ricevitore. Un impulso di luce indica il valore 1 e l'assenza indica il valore 0. Il mezzo di trasmissione è una fibra di vetro sottilissima in silicio. Quando viene colpito dalla luce, il rilevatore genera un impulso elettrico. Collegando ad un estremo una sorgente di luce e un rilevatore dall'altro si crea un sistema di trasmissione unidirezionale che accetta un segnale elettrico, lo converte e lo trasmette sotto forma di impulso luminoso; all'altra estremità della fibra converte nuovamente output in segnale elettrico. I cavi in fibra sono molto simili a quelli coassiali solamente che appunto non sono avvolti da una calzatura conduttrice ma da un rivestimento in silicio. Nei cavi in fibra al centro si trova il nucleo di vetro attraverso il quale si propaga la luce, diametro di 50 micron per quelle multimodali, mentre dagli 8 ai 10 micron per quelle monolocali (monomodali). Il nucleo è circondato da un rivestimento di vetro chiamato cladding che ha un indice di rifrazione più basso. Le fibre si possono collegare in tre modi diversi: connettori > perdono circa il 10-20% del segnale, ma semplificano la riconfigurazione dei sistemi; meccanicamente, le estremità sono appoggiate tra loro; a fusione, formando una connessione solida.

16.1 Confronto

Le fibre ottiche rispetto ai cavi in rame sono notevolmente più costose e sono meno pieghevoli, inoltre più laboriose da unire. D'altro canto però la fibra ha più bandwidth e tiene meglio il segnale, inoltre è più piccola e leggera. La fibra è dielettrica e dunque nelle situazioni di maletempo non vi si presentano problemi di alte interferenze elettriche e inoltre sono più difficili da intercettare, infatti richiede un intervento fisico sul cavo (derivazioni).

17 AMPS

L'AMPS tratta dei telefoni di prima generazione. In AMPS le aree geografiche sono celle ampie 10-20km, ognuna delle quali utilizza frequenze non utilizzate dalle celle vicine. Vengono utilizzate celle relativamente piccole e il riutilizzo delle frequenze di trasmissione delle celle vicine ma non adiacenti. Nei casi in cui vi sono delle celle il numero di persone [auntato fino a sovraccaricare il sistema, viene ridotta la potenza e le celle sovraccaricate vengono divise in celle più piccole chiamate microcelle.
Al centro di ogni celle è presente una stazione di base, la quale comunica con tutti i telefoni presenti nella cella, questa base è costituita da un computer e un trasmettitore, ricevitore collegato ad un'antenna. Il sistema AMPS utilizza 832 canali full duplex ognuno costituito da una coppia di canali simplex, ampi ciascuno 30kHz.

18 GSM

Il GSM tratta dei telefoni di seconda generazione, quelli a voce digitale. La sua struttura è formata da 4 tipi di celle: macro, micro, pico e umbrella.

- macro, sono le più grandi, sopraelevate rispetto agli edifici e hanno un raggio massimo di 35 km;
- micro, come si può intuire sono più piccole delle macro e coprono un'ampiezza pari agli edifici;

- pico, sono molto piccole, usate nelle aree molto dense, tipicamente indoor;
- umbrella, è una piccola estensione usata per coprire i buchi tra quelle appena citate.

Il GSM sfrutta multiplexing a divisione di frequenza, con ogni apparecchio che trasmette su una frequenza e riceve su una più alta, una singola coppia di frequenza è divisa in slot temporali e condivisa tra più utenti. Un sistema GSM ha 124 coppie di canali simplex e supporta otto connessioni separate mediante multiplexing a divisione di tempo.
A ogni stazione attava è assegnato uno slot su una coppai di canali. Trasmissione e ricezione non avvengono nello stesso intervallo temporale perché GSM non è in grado di fare entrambe le azioni contemporaneamente. Introducendo pure l'utilizzo della SIM card, in cui vengono salvati i dati descrittivi dell'abbonato e ha la funzione di autenticazione e autorizzazione all'utilizzo della rete.

pregi interoperabilità tra reti diverse che fanno capo ad un unico standard internazionale. Introduzione della comunicazione di tipo digitale.

difetti none

ambiti d'uso viene utilizzato appunto nella seconda generazione di telefoni cellulari, ed è il sistema più diffuso al mondo.

19 CDMA

Il CDMA è un sistema di comunicazione mobile introdotto dalla seconda generazione di telefoni cellulari. Si tratta di un protocollo completamente diverso da AMPS e GSM, in quanto questi ultimi utilizzano TDM ed FDM, che suddividono in spazi dedicati ad un singolo utente rispettivamente il tempo e lo spettro di frequenze disponibili.
Nel caso di CDMa, ogni utente trasmette utilizzando l'intero spettro, contemporaneamente agli altri utenti > cià è possibile perchè ad ogni stazione viene assegnata una sequenza di bit che codifica l'1 ed una speciale che codifica lo 0, ed essendo le sequenze delle varie stazioni ortogonali tra loro, i vari segnali sis sommano linearmente (al posto di collidere ed oscurarsi completamente) durante la trasmissione. Per estrarre un segnale dagli altri è sufficiente fare il prodotto scalare della somma dei dsegnali per la sequenza assegnata alla stazione.
Questo procedimento aumente anche la sicurzza in quanto per distinguere il segnale è necessario conoscere la sequenza di bit assegnata alla stazione che si vuole ascoltare.
CDMA rispetto a GSM e D-AMPS opera in una banda di 1,25 MHz, permettendo agli utenti di avere un'ampiezza di banda considerevole.

pregi Grazie all maggiore efficienza spettrale, il CDMA garantisce uan maggior velocità di trasmissione dati. Provvede inoltre a garantire una maggior sicurezza rispetto ai predecessori, in quanto il demux è fattibile solo grazie all conoscenza delle parole di codice. Migliora l'efficienza di uso della banda: se dei dispositivi non trasmettono ci saranno minori interferenze. Migliora l'handoff, in quanto non è necessario cambiare frequenza. Celle vicine percepiranno il medesimo segnale.

difetti none

ambiti d'uso viene utilizzato nei telefoni di seconda generazione, come alternativa a D-AMPS e GSM.

20 Handoff

Nell'ambito della telefonia mobile, con handoff si intende la procedura tramite la quale un terminale cambia canale (frequenza e slot di tempo) durante una comunicazione.
Ogni area geografica è divis in celle, al centro di ogni cella si trava una stazione base, che comunica con tutti i telefoni che si trovano all'interno della cella stessa. Quando un telefono mobile inizia ad abandonare

fisicamente l'area descritta da una cella, la stazione base di quest'ultima si accorge del movimento del terminale e controlla il livello potenza del segnale ricevuto dalle stazioni adiacenti. Una volta decretato quella più forte, trasferisce il terminale a quella cella. Il telefono viene informato della nuova centrale di cambiamento e forzato al cambiamento. Questa procedura è conosciuta come handoff.

soft handoff Il telefono è acquisito dalla nuova stazione base prima che venga interrotto il segnale dalla stazione precedente (non vi è nessuna perdita di continuità, ma il dispositivo deve essere in grado di gestire più frequenze contemporaneamente).

hard handoff la vecchia stazione di base rilascia il telefono prima che la nuova riesca ad acquisirlo.

21 UDP

L'UDP è un protocollo a livello trasporto che aggiunge al protoccolo IP (livello network) il concetto di porte, ovvero consente di usare socket, cioè associazioni IP-porta. Si tratta di un protocollo che nasce dall'esigenza di distinguere i processi e servizi operanti all'interno di una macchina, siccole di questi ultimi ne possono esistere molti e con compiti anche tanto diversi fra loro all'intero di un singolo computer conneso in rete > la necessità di distinguerli nasce proprio per questo motivo.
È importante ricordare che all'interno del protocollo UDP non sono previsti controlli di flusso/gestione (questi sono invece forniti dal protocollo TCP), e per questo motivo UDP predilige la velocità di trasmissione a discapito della correttezza del messaggio.
Infatti, UDP vieen spesso utilizzato nell'anbito delle videochat o servizi simili dove la correttezza/integrità del messaggio non è essenziale, ma avere la velocità di trasmissione più alta possibile e la latenza più bassa possibile sì.
UDP è inoltre utilizzato dal protocollo DNS, che si occupa di associare URL facilmente memorizzabili ad indirizzi IP > questo è, tra l'altro, proprio il motivo per il quale il protocollo DNS è esposto ad attacchi di tipo DNS spoofing.

pregi è un protocollo rapido ed efficace e soprattutto molto utile per applicazioni leggere e/o che necesitano di avere una bassa latenza.

difetti non fornisce alcuna affidabilità sull'integrità del messaggio in quanto non c'è alcun controllo sul riordinamento dei pacchetti o sulla ritrasmissione di quelli persi.

ambiti d'uso vedi sopra (comunicazioni broadcast, comunicazioni multitask, applicazioni di rete che sono elastiche per quanto riguarda la perdita di dati).

22 ARP

ARP è un protocollo che permette di "tradurre" indirizzi IP in indirizzi MAC, e per questo motivo risulta fondamentale per le connesioni in entrata all'interno della LAN (local area Network).
Siccome gli indirizzi MAC sono pre-assegnati ed unici per ogni host, avere una gestione centralizzata non sarebbe efficiente perchè per ogni cambiamento della rete il gestore centralizzato dovrebbe riaggiornare tutte le corrsipondenze IP-MAC > la cosa viene infatti gestita in maniera distribuita: quando uno switch riceve un frame che nella sua ARP-table non è associato a nessun MAC address, manda in broadcast una ARP request nella quale viene richiesto qual'è l'host (assieme al suo relativo MAC address) che possiede tale indirizzo IP. L'host in questione risponde poi con un ACK ed in piggy'backing manda il suo MAC address. Siccome anche l'ACK stesso si trova in broadcast, anche gli altri host all'interno della LAN riceveranno l'informazione e la salveranno.
Nel caso in cui un nuovo host dovesse connettersi all rete, anche quest'ultimo manderà una ARP request richiedendo se qualcun altro possiede il suo stesso indirizzo IP, così che eventuali errori (IP duplicato) possano essere rilevati ed evitati fin da subito. Inoltre, questa procedura è utile anche per comunicare agli altri dspositivi in rete di creare l'associazione IP-MAC.

23 NAT

Si trata di un protocollo che è stato introdotto a causa della carenza degli indirizzi IP, la NAT box associa una porta (L4) ad un indirizzo IP locale e rende in questo modo possibile la connessione di più dispositivi (all'interno della stessa LAN) ad un unico indirizzo IP "globale". Infatti, NAT utilizza determinati indirizzi IP riservati, quali 10.0.0.0/8, 17.18.0.0/10 e 192.168.0.0/16 per creare le reti colali > si tratta di classi equivalenti dad IP classful, ma ciò non è un problema in quanto sono solo locali (ed è pertanto possibile utilizzare sempre gli stessi indirizzi, purché ciò venga fatto in LAN diverse).
Il protocollo NAT è molto utile perché riduce il fabbisogno di indirizzi IP, ma non rende la connessione connection oriented, introducendo una falla nel sistema super robusto (ad attacchi esterni) per cui è stato creato il protocollo IP. Infatti, nel caso in cui la NAT box non sia raggiungibile, la macchina rimane solo una LAN.
Per le comunicazioni verso l'esterno, il corrispondente dell'ACK è il DHCP, il quale tuttavia viene gestito questa volta "centralmente", essendo gli IP in questo caso assegnati allo stesso modo (centralmente).

pregi permette di raggruppare sotto un unico indirizzo IP assegnanto dall'ISP molteplici macchine presenti in una sottorete locale.

difetti viola il modello architetturale del protocollo IP, non essendo questi più univoci (possibili conflitti, per esempio con connessioni FTP).

ambiti d'uso utilizzato all'interno del router.

24 Flooding

Il flooding è un modo per instradare i pacchetti IP (pur essendo utilizzato anche in altri contesti) in cui viene prima copiato il pacchetto e successivamente inviato a tutti router connessi alla rete (a parte quello da cui proviene il pacchetto stesso).
Si tratta di una startegia che possiede delle caratteristiche peculiari, infatti utilizzando il flooding si ha la certezza che se un pacchetto può arrivare a destinazione, ci arriverà sempre per la strada più breve. Questo succede perché tutte le strade in questione vengono tentate allo stesso momento. Ne deriva che, se usato male, il flooding può portare facilmente a sovraccarichi di rete.
A causa della necessità di dover tenere sotto controllo il flooding (cioè evitare che sommerga la rete) esiste il campo TTL, ossia time to leave > normalmente nei pacchetti IP è settata a 255, ogni volta che un pacchetto raggiunge un router il valore decresce di 1, qundo arriva ad essere 0 il pacchetto viene in automatico eliminato. Inoltre, nel caso in cui un router riceva un pacchetto uguale a quello che ha inviato, quest'ultimo verrà eliminato > per fare ciò, è logico pensare che sarebbe necessaria una grande quantità di memoria dove immagazzinare i pacchetti ricevuti e poterli controllare, ma la soluzione che è stata adottata è quella di utilizzare solo un unico numero n che traccia la sequenza di pacchetti inoltrati: se n=5, pacchetti da 0 a 5 vengono scartati.

pregi è semplice da attuare ed assicura la ricezione del pacchetto alla stazione desiderata.

difetti spreco di banda, pacchetti duplicati (che sono difficili da gestire) e rischio di cicli infiniti.

ambiti d'uso utilizzato nello strato network. È molto utile come metrica di confronto per altri algoritmi di routing (a causa della sua caratteristica di riuscire a scegliere sempre il percorso più breve). Viene utilizzato molto anche a livello militare (in situazioni del genere, a causa di bombardamenti exx che potrebbero colpire un data center, l'avere pacchetti duplicati all'interno della rete è paradossalmente una cosa positiva).

25 Choke packet

Il choke è un pacchetto che viene inviato ad un router che sta immettendo troppi pacchetti in rete saturando quindi parte della infrastruttura. La funzione dello choke packet è quella di risolvere il problema dimezzando i pacchetti che il router che riceve il choke potrà immettere nella rete per un certo periodo di tempo > nel

caso in cui più router contemporaneamente inviino choke packet nello stesso momento allo stesso router, vi possono ovviamente essere problemi, in quanto tale router potrebbe finire ad essere bloccato totalmente (nel caso in cui 1 solo choke packet sarebbe stato sufficiente a risolvere il problema di saturazione). Infatti, la soluzione che viene adottata è quella di permettere ad ogni router di ricevere un solo choke alla volta, ignorando quindi "piogge di choke" in arrivo. Un'altra problematica da considerare è che la rete venga saturata completamente dai pacchetti inviati ad un router prima che il choke packet giunga a destinazione > soluzione: choke hop by hop: agiscono come un normale choke, ma "strozzano" anche i router per i quali passano lungo il percorso per arrivare al router "pericoloso".

pregi choke permette di risolvere la congestione della linea.

difetti choke lento a reagire, in quanto l'host produttore di pacchetti congestionanti ci mette un po' a ricevere il choke > con choke hop by hop si ha un miglioramente.

pregi choke hop by hop rispetto al choke normale, è molto più veloce nella decongestione della rete.

difetti choke hop by hop richiede un utilizzo più intensivo del buffer di trasmissione fra mittente e destinatario.

ambiti d'uso strato network, si tratta di un algoritmo di controllo della congestione di rete.

26 Token bucket

Per evitare che la rete si saturi a causa di una "pioggia" momentanea di pacchetti (che causerebbe un fisiologico crollo di prestazioni) possono essere utilizzati i token bucket > per ogni intervallo di tempo viene generato un token: qunndo arriverà un pacchetto, questo verr immagazzinato in un buffer, e potrà proseguire solo se vie è un token disponibile.
Nel caso in vui non vi fossero molti pacchetti in arrivo, i token verrano accumulati fino ad un tetto prestabilito > in questo modo, nei momenti di maggior congestione della rete, più pacchetti potranno passare contemporaneamente.
L'algoritmo token bucket infatti riprende l'idea del leaky bucket, ma aggiunge il concetto di token. La differenza sta nel fatto che token bucket non scarta i pacchetti quando il "secchio" è pieno. Per implementare il token bucket è sufficiente l'utilizzo di una variabile che tenga conto del numero dei token, e li diminuisca quando un paccehtto viene inviato.

pregi rispetto al bucket di tipo leaky, questo algoritmo non scarta alcun pacchetto e gestisce meglio eventuali burst improvvisi di pacchetti.

difetti consentendo di trasmetter raffiche di dati insieme, potrebbero crearsi problemi di sicurezza se la rete venissa compromessa e finisse in mani sbagliate.

ambiti d'uso strato network, viene utilizzato per gestire il traffico in una rete dati. È finalizzato a regolare l'output di trasmissione.

27 Distance vector routing

Si tratta del primo algoritmo di routing usato in ARPANET e funziona nel seguento modo: ogni router, quando si collega alla rete, chiede ai router vicini le loro tabelle di routing ed enendovi insieme l'informazione riguardo il tempo che attende per riceverle crea in questo modo la propria tabella di routing > quest'ultima è costruita da un entry per router, il tempo necessario per cui gli arrivi un pacchetto e quele sia la via migliore tra i router vicini. Per avere un routing dinamico, che tiene conto del carico della rete e le modifiche alla topologia, le tabelle di routing si aggiornano continuamente e dinamicamente: se un collegamento migliora o peggiora di velocità le tabelle di routing vengono subito aggiornate.
Tuttavia, nel caso in vui un nodo venga scollegato, nasce un problema noto con il nome di count to infinity

> siccome i router si baseranno su tutte le altre tabelle che ancora non sono state aggiornate, il percorso (per i router) diventerà sempre più lungo, tendendo ad infinito un aggiornamento per volta. D'altra parte, si tratta di un buon algoritmo per i suoi tempi, in quanto è molto scalabile (aggiungere un router è un processo molto veloce).

pregi ogni router è in grado di conoscere il percorso migliore per arrivare a tutti i nodi adiacenti.

difetti non tiene conto della banda della linea quantdo sceglie i percorsi. Esiste la possibilità che si creino cicli infiniti. Impiega troppo tempo a raggiungere la convergenza.

ambiti d'uso strato network, ha la funzione di instradare i pacchetti ai vari router della rete. si tratta di un algoritmo adattivo e quindi dinamico.

28 Link state routing

Si tratta dell'algoritmo di routing che ha di fatto sostituito il distance vector routing. Nel link state routing, ogni router possiede un identificativo univoco, inoltre quando si collega alla rete manda ai router a lui collegati un pacchetto HELLO, ed esi risponderanno con il proprio identificativo, oltre ad altre informazioni. Dopo di ciò, tramite un apposito ECHO a cui i router rispondono subito, il nuovo router acquisisce le informazioni riguardo la velocità di ogni collegamento. Appena queste informazioni vengono raccolte viene generato un paccehtto che le contiene, che viene inoltrato tramite flooding a tutti i nodi della rete. Questo pacchetto ha una durata di vita oltre la quale verrà considerato obsoleto e scartato.
Il fatto che questo pacchetto contentente tutte le informazioni venga trasmesso tramite flooding rappresenta la principale differenza rispetto la distance vector routing, e ne previene il problema del count to infinity. Infatti, ogni volta che passa un certo intervallo di tempo oppure in presenza di eventi speciali quali modifica, disconnessione o connessione del router viene rieseguito l'intero processo. Un router scarterà uno di questi pacchetti se: ne ha già ricevuto uno più recente; ha già inoltarto in precedenza il suddetto file; è già scaduto il suo tempo di vita.
Una volta che un router riceve l'intera serie completa di pacchetti identificativi di ogni router della rete, potra costruire il grado della rete stessa > sarà in grado di applicare l'algoritmo di Dijkstra e trovare i percorsi più brevi per raggiungere ogni altro router.

pregi si tratta di un lagoritmo molto scalabile e che molto raramente genera cicli, è veloce a trovare il cammino più veloce ed è in grado di gestire reti molto caotiche.

difetti i router hanno bisogno di molta memoria e capacità di calcolo.

ambiti d'uso strato network, sostituito al distance vector routing. Molto utilizzato al giorno d'oggi.

29 QoS

Con QoS si intende Quality of Service, ossia il livello di qualità raggiunto da un determinato servizio di rete. I principali indicatori della qualità raggiunta da un servizio di rete sono 4, anche se nella pratica ogno singola applicazione/software valuterà quali consederare più importanti nel contesto dove opear. Gli indicatori sono:

- affidabilità: una applicazione è affidabile quando nessun bit può venire trasmesso in maniera incorretta (CRC);
- banda: ogni protocollo ed applicazione differisce dalle altre per l'esigenza di banda, ossia la velocità di trasmissione dei dati;
- delay: che risulta per ovvi motivi importantissimo per applicazioni del tipo videoconferenza, live, trascurabile per altre come la messaggiistica;

- jitter: ossia il grado di variabilità del ritardo di trasmissione. Una applicazione con velocità di trasmissione mediamente costante ha un jitter basso, viceversa, una applicazione dove la velocità di trasmissione è variabile a causa di qualche condizione ha un jitter alot. Questo può portare ad una ricezione dei dati ad intervalli molto irregolari. Alcuni applicazioni, quali lo streaming video, oppure lo screen sharing, risultano inutilizzabili nel caso di jitter alto. Altre invece, come quelle di trasferimento file o quelle di posta elettronica, non sono molto soggette a problemi anche in caso di jitter alto.

30 Numero di bit necessari per il riconoscimento degli errori di trasmissione

Per la gestione degli errori sono state sviluppate due strategie di base: la prima si basa su una codifica a correzione d'errore; mentre la seconda è una codifica a rivelazione d'errore. L aprima introduce una ridondanza tale da riuscire a ricostruire il messaggio in caso di anomalie. La seconda introduce ridondanza sufficiente a capire che quando si verifica un errore, dando la possibilità di richiedere una ritrasmissione.
Un frame consiste in m bit di dati e r bit ridondanti per i controlli, $n = m + r$ è la lunghezza totale del frame. Per trovare d errori è necessaria una codifica con distanza $d + 1$. Per correggere d errori è necessaria una codifica con distanza $2d + 1$.

pregi rilevare semplicemente l'errore permette di diminuire la quantità di bit dati. Tuttavia rilevazione e correzione permette un minor numero di invii, e permette la ricostruzione autonoma del frame.

difetti la semplice rilevazione non permette la ricostruizione del dato, la rilevazione ecorrezione però necessita del doppio dei bit per poter essere attuata.

ambiti d'uso starto data-link. Nelle reti wireless conviene utilizzare una codifica a correzione dell'errore, così da ricostruire il messaggio in casi d'errore (se doveses solo rilevare e richiedere un altro invio, il rischio della presenza di nuovi errori sarebbbe alta, quindi conviene usare questa).

31 Go back N

Si tratta di un protocollo con cui può essere utilizzata una sliding window in cui il mittente ha duna finestra di $n > 1$ ed il ricevente uan finestra di 1 (così che) se un pacchetto viene perso, l'intera finestra a partire dall'errore deve essere rispedita. Nel caso si prospetti di trovare pochi errori, può essere considerato un buon protocollo, altrimenti risulta inefficiente in quanto potrebbe far perdere troppa banda.
In generale, è un processo dove il mittente continua a mandare un numero di frame specificato nella windows size, anche senza aver ricevuto alcun ack. Per utilizzare Go back N sono quindi necessari un buffer grande n per ricevere, ed n timer.

pregi se gli errori non sono tanti, grazie all'invio a raffica di pacchetti senza attenere l'ack corrispondente, risulta essere un protocollo molto efficace.

ambiti d'uso viene utilizzato in generale in tutti quei sistemi dove la finestra di invio è più grande di quella ricevente (che è invece particolarmente scarsa).

32 DES

DES è uno standard di criptaggio internazionale, creato da IBM su commissione del governo americano, originariamente avrebbe dovuto avere una chiave di 128 bit e blocchi da 64 bit, ciò però non consentiva ai servizi di intelligence americana di decriptare (abbastanza velocemente) i messaggi, e per questo motivo si è deciso alla fine di ridurre la chiave a 56 bit.
Nello specifico, si tratta di un product cipher, cioè un cifrario che combina 2 o più trasformazioni, il quale sfrutta infatti 19 passaggi fra una P-box (production box) ed una S-box (substitution box).
P-box: esegue permutazioni dei messaggi in stile cifrario a sostituzione.
S-box: sostituisce n bit con m bit: le associazioni fra le varie permutazioni di n bit e gli m bit di uscita

possono essere rappresentate semplicemente da una tabella.
Entrambe le box sono molto efficienti ed è possibile reallizzarle facilmente in $hw >$ grazie a 19 passaggi fra le due si ottiene un algoritmo sufficientemente sicuro.

33 Triple DES

A due anni dalla nascita dell'algoritmo DES, a causa dell'avanzamento esponenziale nelle capacità di calcolo dei computer, diventa anche per gli utnetni comuni (e quindi non solo per i servizi di intelligence) troppo facile decriptarlo > viene per questo motivo creato un nuovo standard, che, tuttavia, per ragioni sia pratiche che economiche doveva essere retrocompatibile. Si tratta del Triple DES, che è basato direttamente sul DES originale. Infatti, si aggiunge semplicemente una ulteriore chiave a 56 bit e viene eseuita poi la codifica analogamente a quanto avviene nel DES, ma questa volta tutti i passaggi vengono, di fatto, ripetuti 3 volte. Per rimanere retrocompatibile, il Triple DES sfrutta le proprietà del DEs che garantiscono a quest'ultimo di essere un metodo di cifratura a chiave simmetrica > ciò rende l'algoritmo di codifica interscambiabile, infatti il Triple DES codifica in 3 fasi e decodifica specularmente.
Nello specifico, la retrocompatibilità è data da:
$CK1 > DK2 > CK1$ (decodifica)
$DK2 > CK1 > DK2$ (codifica)
Ponendoi $K1 = K2$, i primi due passaggi si annullano e di conseguenza ritorna ad essere un semplice DES.

pregi permettono una cifratura a blocchi.

difetti a causa della dimensione ridotta della chiave DES non è molto sicuro, inoltre, sia con Triple DES che con DES lo stesso testo in chiaro produrrà sempre il medesimo testo cifrato.

ambiti d'uso non è più utilizzato: è stato sostituito da AES.

34 One Time Pad

Si tratta di una modalità di criptaggio che, nel caso la chiave utilizzata si asempre nuova, risulta al 100% sicura. Consiste nel fare lo XOR fra una chiave casuale lunga quanto il messaggio da criptare ed il messaggio stesso. La parte più difficile del processo OTP è riuscire a trovare chiavi sempre diverse, in quanto gli algoritmi al momento esistenti sono in grado di creare solamente output pseudo-casuali. Questo è molto importante in quanto il OTP può essere considerato veramente sicuro solamente se la chiave non viene mai ripetuta, altrimenti facendo lo XOR fra due messaggi con la stessa chiave si otterrevve proprio il messaggio in chiaro (dove poi tra l'altro si potrebbe applicare anche la frequency analysis).
Per questi motivi, ai giorni nostri OTP viene raramente utilizzato nella sua variante originale, viene spesso scelto di approssimarlo tramite la tecnica dello stream cypher.

pregi in generale OTP se eseguito a dovere, ovvero con chiavi sempre nuove, non può mai venire compomesso matematicamente > decifrare il messaggio senza conoscere la chiave è impossibile.

difetti la chiave non può essere memorizzata digitalmente (si perderebbe la sicurezza), quindi mittente e destinatario devono entrambi avere in principio una copia scritta della stessa. Ovviamente, una altro difetto è che la quantità di dati che possono essere trasmessi equivale al numero di chiavi che si posseggono.

ambiti d'uso utilizzato poco, seppur esattamente sicuro, a causa della sua scarsa praticabilità. In generale il suo utilizzo più comune è nell'ambito dello spionaggio.

35 Stream Cypher

Lo stream cypher è un cossiddetto cifrario di flusso, ovvero una variante del cifrario a blocchi. Si tratta di una tecnica crittografica che sfrutta un vettore di iniziazione (IV, initialation vector) ed una chiave, le

quali cifrate insieme generano un keystream completamente indipendente dal resto in chiaro > in seguito è possibile cifrare nuovametne il keystream con la chiave un numero arbitrario di volte al fine di ottenere keystream sempre differenti, da mettere infine a XOR con il testo.
In generale, lo stream cypher quindi simula il OTP, mettendo in fila gli IV criptandoli più volte. Anceh in questo caso, quindi, l'IV non deve essere riutilizzato più volte. Inoltre, se l'IV dovesse essere troppo corto, diventerebbe possibile effettuare attachi ad analisi di frequenza per decifrare il testo (per esempio WEP), rendendo la crittografia non troppo sicura.

pregi garantisce una alta elasticità agli errori ed inoltre la keystream è indipendente dai dati.

difetti bisogna stare attenti a non riutilizzare né l'IV né i keystream che ne derivano, altrimenti lo stream cypher è vulnerabile.

ambiti d'uso semplificare il protocollo OTP.

36 CIDR

Inizialmente si era pensato di distribuire gli indirizzi IP in pacchetti di 3 dimensioni differenti:

- 16 milioni di IP (classe C);
- 65 mila IP (classe B);
- 256 IP (classe A).

Questo, teoricamente, sarebbe stata una scelta efficacie, tuttavia l apratica e la società ne hanno, nel corso degli anni, dimostrato gli evidenti difetti. Infatti, 256 IP sembrano pochi e quando una società o azienda doveva scegliere quale pacchetto comprare, spesso e volentieri era propensa acomprare il secondo pacchetto (classe B), usandone in media solo 50 ¿ a causa di un mero fattore psicologico, un grandissimo spreco di indirizzi IP: presto questi ultimi vennero a mandcare, e si fu constretti a correre ai rapari, grazie proprio al CIDR (classless inter-domain routing).
Grazie ad esso gli indirizzi IP non vengono più forniti per classi fisse, ma in blocchi di dimensioni variabili (purché sempre potenze di 2), utilizzando una maschera sub-net mask, che permette di distinguere la parte dell'indirizzo di rete dell'IP da quella per gli host > questa maschera tuttavia complica il compito dei router, i quali non possono più raggruppare gli indirizzi IP in base alla classe, ma devono tenere conto di tutti i bit dell'indice (con conseguenti tabelle degli indirizzi che diventano enormi, assieme alle ricerche sulle stesse).
Questo problema è stato risoltao grazie alle aggregate entries > i router creano delle regole di routing che uniscono i vari indirizzi con i bit più significativi. Per consentire un indirizzamento corretto ha la priorità la regola più lunga.

37 ICPM

Si tratta di un sotto-protocollo del protocollo IP che ha il compito di gestire eventi inaspettati, per esempio:

- può mandare un echo;
- senala al mittente se in un pacchetto il tiem to leave è arrivato a 0;
- manda choke packets (funzione deprecata, gestita a livello trasporto);
- segnala una destinazione non raggiungibile.

Si tratta di un sotto-protocollo he viene in generale utilizzato per testare la connessione di rete, più nello specifico, la sua velocità e i suoi percorsi.

pregi protocollo molto utilizzato per tesstare le performance di una connessione.

difetti alcuni dei pacchetti sono ormai obsoleti perchè la risoluzione del problema viene gestita meglio in altri livelli.

casi d'uso strato network.

38 IPV6

Nonostante NAT e CIDR, gli indirizzi IPV4 restano pochi, perciò è stata creata la versione 6 del protocollo IP ed è cominciata la sua diffusione.
IPV6 ha indirizzi di 128 bit, non è retrocompatibile con IPV4, ma lo è con i suoi sotto-protocolli (UDP, TCP, DNS, ...).
IPV6 semplifica l'intestazione, infatti prevede solo 8 campi rispetto ai 13 della versione precedente. Ciò consente ai router di elaborare molto più velocemente i pacchetti in arrivo.
Migliora il supporto per le opzioni, rendnedo campi che prima erano obbligatori, opzionali. Un altro grande passo in avanti riguarda la sicurezza, oltre ad un miglioramento generale del QoS.
Ormai, il grosso della rete è basato sul protocollo IPV4, ed essendo IPV6 non direttamente retrocompatibile, il pasaggio ad esso sis ta rivelando lento ed impegnativo. C'è sicuramente la necessità di mantenere il supporto ad IPV4 almeno un altro paio di decenni.

39 IPSEC

IPSEC è un insieme di regole e protocolli di telecomunicazioni per la creazione di connessioni sicure su una rete. IPSEC aggiunge al protocollo IP la crittografia e l'autenticazione allo scopo di renderlo più sicure e trasparente. IPSEC è diviso in due parti principali:

- descrive 2 nuovi header che possono essere aggiungi ai pacchetti, che portano la security identifier, controllo di integrità ed altre informazioni;
- chiamata ISAKMP (Internet Security Association and Key Management Protocol), che è un protocollo per la negoziazione delle chiavi.

Transport mode e tunnel mode sono due modalità di funzionamento di IPSEC.
Nel primo caso, il pacchetto IP originale viene inserito dopo l'header. Nel secondo caso, invece, il pacchetto IP originale viene incapsulato nel corpo di un nuovo pacchetto IP con un nuovo header (che diventa un Authentication Header).

pregi il framework può vivere anche se altri protocolli diventano obsoleti o ne vengono aggiungi di nuovi.

difetti nel caso della modalità tunnel, il pacchetto IP avrà un header in più, aumentando quindi la dimensione del pacchetto nell'insieme.

casi d'uso strato network.

40 HMAC

Facente parte dell'Authentication Header dell'IPSEC, si tratta di un campo di lunghezza variabile che contiene la firma digitale del payload. Quando la security association è stabilita, viene anche stabilito quale algoritmo di firma verrà utilizzato.
Normalmente la crittografia achiave pubblica non viene utilizzata in quanto i pacchetti devono essere spediti rapidamente. Siccome la connessione security association è basata sullo scambio di una chiave per la criptazione simmetrica, la stessa viene utilizzata nella computazione della firma digitale.
Un semplice modo per farlo è quello di calcolare l'hash del pacchetto più la chiave simmetrica. Uno schema di questo tipo è chiamato HMAC. Garantisce sia l'integrità che l'autenticità del messaggio. È possibile utilizzare HMAC con qualsiasi funzione di hash. Questo per rendere possibile una sostituzione della funzione nel caso non fosse sufficientemente sicura.