FORMULARIO RETI

TRASMISSIONE

throughput

throughput medio = L / RTT (quindi RTT / 1000 se dato in ms, ottengo così un risultato in KB/s)

- L = dimensione di 1 pacchetto (KB)
- RTT = Round Trip Time (s)

massimo throughput = (capacità canale) / (dispositivi connessi)

buffering

buffering medio = $\frac{RTT * C}{\sqrt{N}}$ (ma questo non sappiamo cosa sia)

- RTT = Round Trip Time (s)
- C = Capacità (Gbps)
- N = numero di flussi (numero puro)

utilizzo canale

utilizzo = (bit trasmessi) / (capacità canale)

per congestionare router di una certe rete R

(L * a) / R = 1

- L = dimensione di 1 pacchetto
- a = frequenza di arrivo dei pacchetti
- R = dimensione (capacità) del canale di uscita

se invece (L * a) / R = 0, la rete NON è congestionata

WIRELESS

conversione da sommare dB a moltiplicare in mW

-3 dB	½ power in mW (/ 2)
+3 dB	2x power in mW (* 2)
-10 dB	1/10 power in mW (/ 10)
+10 dB	10x power in mW (* 10)

lunghezza d'onda λ = (e / f)

- e = velocità (della luce) = 300.000.000 m/s
- f = frequenza (Hz) (1/s)
- in questo modo il risultato è in metri

fresnel zone

R60% = $43.3 * \sqrt{(d/4f)}$

R100% = $72.2 * \sqrt{(d/4f)}$

- R% = raggio della zona di fresnel, 60% o 100% (feet)
- d = distanza (miglia)
- f = frequenza (GHz)

free space loss (in dB) = $-(A + 20Log_{10}(f) + 20Log_{10}(d))$

- A = 36.6dB se c'è nebbia (o disturbi vari) altrimenti 32.4dB
- f = frequenza (MHz)
- d = distanza (miglia)

potenza necessaria

potenza necessaria = potenza ricevuta - Receiver sensitivity (- fade operating margin)

- $potenza\ ricevuta = potenza\ trasmessa + guadagni + free\ space\ loss$
- Receiver sensitivity = sensibilità del ricevente (ha segno negativo)
- fade operating margin = margine per assicurarsi una buona connessione
    - è un valore compreso tra 10 e 20 in base a quanto si vuole "essere prudenti"

power difference tra Tx e Rx signal (in dB)

power difference = $10Log((Power\ Rx) / (Power\ Tx))$

- power Tx = potenza della rete sorgente (Watt)
- power Rx = potenza della rete destinazione (Watt)
    - esempio:
      un segnale trasmesso da [Tx] a 100 mW è ricevuto da [RX] a 0.000005 mW
    - Power Difference (dB) = 10 * log([RX] /[TX]) = 10 * log(0.000005mW/100mW) = -73 dB

CONVERSIONE

dBm = 10 * Log(mW)

mW = 10^(dBm/10)

CYBERSECURITY (da 05-introduzione-alla-network-security.pdf)

Siano A e B le due entità comunicanti

- **chiave simmetrica Ks (per privacy dei messaggi, anche quelli grandi)**
  - usata per avere privacy
  - Si cripta il messaggio e insieme al messaggio criptato si invia la chiave criptata con la chiave pubblica del ricevente.
  - si può criptare anche un messaggio grande

  A e B hanno la stessa chiave Ks tale **m = Ks(Ks(m))**
  esempio:
  A = [Ks(m),KB+(Ks)]
  B = Ks = KB-(KB+(Ks)) ; m = Ks(Ks(m)),
- **hashing (per integrità del messaggio)**
  - per fare in modo che il messaggio ricevuto sia integro (necessario ma non sufficiente per la non ripudiabilità)
  - si invia una coppia composta da:
    - messaggio in chiaro m
    - messaggio hashato H(m)
- **non ripudiabilità (integrità + certezza del mittente)**
  - si invia una coppia composta da:
    - messaggio in chiaro m
    - messaggio hashato H(m) criptato con chiave privata del mittente KA-[H(M1)] (ovvero firma digitale del solo hash)
- **non replay (per ricevere il messaggio una e una sola volta)**
  - viene aggiunto un nonce R (che può essere generato random dal mittente o inviato in precedenza dal ricevente)
  - *esempio:*
    - *[m, R]*

- **RSA (per privacy dei messaggi piccoli)**
  - utilizzo chiavi pubblico-privata

COSE A CASO

- **commutazione di pacchetto:** è una tecnica di accesso multiplo a divisione di tempo, specificamente concepita per il trasporto di dati, utilizzata per condividere un canale di comunicazione tra più nodi in modo non deterministico, suddividendo l'informazione da trasferire in pacchetti trasmessi individualmente e in sequenza, seguendo un meccanismo di instradamento dettato da relative tabelle di instradamento. La commutazione di pacchetto trova applicazione nelle reti di calcolatori e più in generale nelle reti di telecomunicazione. Esempi di reti basate sulla commutazione di pacchetto sono le reti locali di calcolatori e Internet.
- **commutazione di circuito:** A differenza della commutazione di pacchetto, la commutazione di circuito è una tecnica che prevede un canale dedicato ed univoco.
- **differenza utilizzo IPv4 e MAC address:** L'indirizzo IP viene usato per trasportare dati da una a un'altra rete usando il protocollo TCP/IP. Il MAC address viene usato per portare i dati al dispositivo corretto presente su una rete.

Un esempio pratico: supponiamo che il vostro nome sia "Mario Rossi", che non è sufficientemente univoco come identificatore. E se ci aggiungessimo informazioni genealogiche (cioè, il vostro "produttore")? Sareste "Mario Rossi, figlio di Giorgio, figlio di...", tornando abbastanza indietro nel tempo diventerebbe sufficientemente univoco. Questo rappresenterebbe il vostro MAC address.
Se vi volessi mandare un pacco, non potrei di certo dire all'ufficio postale "Mandatelo a Mario Rossi, figlio di Giorgio, figlio di...", perchè ci vorrebbe comunque anche l'indirizzo di casa. Ma nemmeno quello è sufficiente: mi serve l'indirizzo di casa e il tuo nome, altrimenti riceverai il pacco ma non saprai se era destinato a te o a tua moglie. L'indirizzo IP dice DOVE stai, il MAC address invece CHI sei.
In altri termini: il vostro modem/router ha un indirizzo IP univoco ("indirizzo di casa") assegnato dal vostro ISP ("ufficio postale"). I dispositivi collegati al modem o router ("quelli che abitano a casa") hanno indirizzi MAC univoci ("nomi personali").
L'indirizzo IP porta i dati verso il router/modem ("casella postale") e poi il modem/router li inoltra al dispositivo corretto ("il destinatario").

- **ARP** (Address Resolution Protocol) è un protocollo ausiliario di livello rete il cui scopo è ottenere l'indirizzo MAC di una stazione di cui è noto l'indirizzo IP. Un pacchetto IP infatti può arrivare a destinazione solo se è noto l'indirizzo MAC della stazione destinataria. (Ricordiamoci che il pacchetto deve essere inoltrato al livello data-link prima essere trasmesso sulla rete). Per assolvere il suo compito ARP si serve di una una tabella (ARP cache) in cui sono memorizzate le corrispondenze fra IP e MAC.

  La procedura per ottenere l'indirizzo MAC di destinazione, nel caso di due stazioni A e B sulla stessa rete è la seguente:
  1. La stazione A cerca nella cache l'indirizzo IP di B
  2. Se lo trova, acquisisce l'indirizzo MAC di B e avvia la trasmissione del pacchetto
  3. Se non lo trova, invia una un pacchetto broadcast, contenente i propri indirizzi MAC , IP e l'indirizzo IP di B, in cui richiede l'indirizzo MAC di B
  4. La stazione B invia un pacchetto di risposta con il proprio indirizzo MAC
  5. la stazione A memorizza nella cache l'IP e il MAC di B e inizia la trasmissione

  Se la stazione B è oltre il router, cioè sta in un'altra rete, la procedura è analoga, ma l' eventuale richiesta ARP riguarderà l'indirizzo MAC del router di default.
  La cache ARP può contenere sia voci dinamiche che statiche.
  Le voci dinamiche vengono aggiunte e rimosse automaticamente. Quelle statiche restano nella cache fino a quando il sistema non viene riavviato.
  Ciascuna voce dinamica della cache ARP ha una durata potenziale di 10 minuti. Se una voce non viene riutilizzata entro 2 minuti dall'aggiunta, scadrà e sarà rimossa dalla cache ARP. Se invece la voce viene utilizzata, riceverà altri due minuti di durata. Se una voce continua ad essere utilizzata, riceverà ancora due minuti di durata fino a un massimo di 10 minuti.
- **ICMP.** L'Internet Control Message Protocol (ICMP) è come ARP protocollo ausiliario che opera al livello Rete . La sua funzione è permettere agli host e ai router di rilevare alcuni errori e riportare informazioni sullo stato del collegamento di due stazioni o router. ICMP rileva automaticamente l'errore quando:
  - Un pacchetto IP non è in grado di raggiungere la propria destinazione.

    - Un router non riesce a inviare pacchetti alla velocità corrente di trasmissione.
    - Un router reindirizza l'host di invio per utilizzare una route migliore per la destinazione
- I messaggi ICMP vengono incapsulati e inviati nei pacchetti IP.

Richiesta echo	Determina se un nodo IP (un host o un router) è raggiungibile sulla rete
Risposta echo	Risponde a una richiesta echo ICMP
Destinazione non raggiungibile	Informa l'host che un pacchetto IP non può essere inviato
Quench sorgente	Comunica all'host di ridurre la velocità di invio dei pacchetti IP a causa di una congestione
Reindirizzamento	Comunica all'host una route preferita
Tempo scaduto	Indica che il Time-to-Live (TTL) di un pacchetto IP è scaduto

- In telecomunicazioni, il **controllo del flusso** è un meccanismo utilizzato nelle reti di computer per controllare il flusso di dati tra un mittente e un destinatario, in modo tale che un ricevitore lento non sarà superato da un mittente veloce. Il controllo del flusso fornisce metodi al ricevitore per controllare la velocità di trasmissione in modo tale che il ricevitore possa gestire i dati trasmessi dal mittente. Il **controllo di congestione** invece è un meccanismo che controlla il flusso di dati quando si verifica effettivamente la congestione. Controlla i dati che entrano in una rete in modo tale che la rete possa gestire il traffico all'interno della rete.
    - Il controllo del flusso (in inglese Flow Control) è un meccanismo che controlla il flusso di dati tra un mittente e un destinatario in modo tale che un ricevitore più lento non venga sopraffatto dalla quantità di dati trasmessi da un mittente veloce. Questa situazione può verificarsi a causa di diversi motivi, come la mancanza di potenza di elaborazione del destinatario rispetto al mittente o al destinatario che ha un carico di traffico pesante rispetto al mittente. I meccanismi utilizzati nel controllo del flusso possono essere classificati in base al fatto che il destinatario invii feedback al mittente. Nel meccanismo di controllo del flusso ad anello aperto, il ricevitore non invia alcun feedback al mittente ed è il metodo di controllo del flusso più utilizzato. Nel controllo del flusso a ciclo chiuso, le informazioni sulla congestione vengono ritrasmesse al mittente. I tipi di controllo del flusso comunemente usati sono la congestione della rete, il controllo del flusso a finestre e il buffer dei dati.
    - Il controllo di congestione (in inglese Congestion Control) fornisce metodi per regolare il traffico in ingresso a una rete in modo che possa essere gestito dalla rete stessa. Il controllo di congestione impedisce a una rete di raggiungere un collasso congestizio in cui si verificano poche o nessuna comunicazione utile a causa della congestione. Il controllo di congestione viene applicato principalmente alle reti a commutazione di pacchetto. L'obiettivo del controllo di congestione è mantenere il numero di pacchetti all'interno della rete al di sotto di un livello che ridurrebbe notevolmente le prestazioni. Il controllo di congestione è implementato nei protocolli del livello di trasporto TCP (Transmission Control Protocol) e UDP (User Datagram Protocol). In TCP vengono utilizzati algoritmi di avvio lento e backoff esponenziale. Gli algoritmi di controllo di congestione sono classificati in base alla quantità di feedback ricevuto dalla rete e all'aspetto delle prestazioni che mira a migliorare. Oppure, sono classificati in base a criteri come le modifiche

che devono essere apportate sulla rete corrente e il criterio di equità utilizzato dall'algoritmo.

- In telecomunicazioni e informatica, nell'ambito delle reti informatiche, un **protocollo di rete connection-less**, ossia senza connessione, si distingue per il fatto che lo scambio di dati a pacchetto tra mittente e destinatario (o destinatari) non richiede l'operazione preliminare di creazione di un circuito, fisico o virtuale, su cui instradare l'intero flusso dati in modo predeterminato e ordinato nel tempo (sequenziale).
  I protocolli connection-less (di cui due esempi tipici sono Ethernet e UDP) suddividono il flusso di dati in entità (frame, segmenti) che vengono instradate singolarmente in modo indipendente l'una dall'altra, senza interazioni di ritorno tra sorgente e destinatari/o (per esempio per verificare se il destinatario è raggiungibile) e senza controllo sulla corretta sequenza temporale di inoltro.
  A differenza dei protocolli connection-oriented (ossia i protocolli che richiedono di creare un circuito predeterminato tra sorgente e destinatari prima di iniziare lo scambio di dati vero e proprio, come ad esempio il TCP), i protocolli connection-less non garantiscono quindi né l'effettiva consegna del singolo pacchetto né che i pacchetti vengano consegnati nella loro sequenza temporale corretta.
  I protocolli connection-less sono utilizzati nei casi in cui si richiede di minimizzare i ritardi o latenze di trasmissione dei pacchetti ed è tollerata o tollerabile la perdita di qualche pacchetto, come ad esempio per la trasmissione di informazioni audio-video real-time (streaming).
- La **rilevazione e correzione dell'errore**, in matematica, informatica, telecomunicazioni, e teoria dell'informazione, ha grande importanza pratica nel mantenimento dell'integrità dell'informazione nei sistemi con un canale rumoroso, o nei dispositivi per l'immagazzinamento dei dati caratterizzati da una scarsa affidabilità.
  - La rilevazione d'errore consiste nella capacità di scoprire la presenza di errori causati dal rumore o da altri fenomeni deterioranti durante una trasmissione di dati (ad es. tramite il bit di parità).
  - La correzione d'errore consiste invece nell'ulteriore abilità di ricostruire i dati originali, eliminando gli errori occorsi durante la trasmissione.

  Vi sono due differenti schemi di base per la progettazione della codifica di canale e del protocollo per un sistema che corregge gli errori:

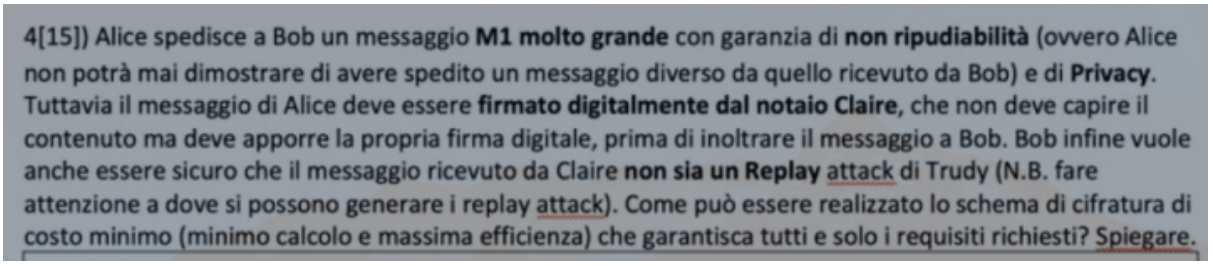
  - Automatic repeat-request (ARQ): Il mittente invia i dati ed anche un codice a rilevazione d'errore, che sarà utilizzato in ricezione per individuare gli eventuali errori, ed in tal caso chiedere la ritrasmissione dei dati corrotti. In molti casi la richiesta è implicita; il destinatario invia un acknowledgement (ACK) di corretta ricezione dei dati, ed il mittente re-invia solo quei dati per i quali non ha ricevuto, entro un prefissato tempo limite (timeout), il corrispondente ACK.
  - Forward Error Correction (FEC): Il mittente codifica i dati con un codice a correzione d'errore (error correction code, ECC) ed invia il messaggio codificato. Il destinatario non invia mai alcun messaggio verso il mittente; esso decodifica ciò che riceve nella maniera più simile possibile a quella di un certo insieme prefissato di parole accettabili. Tali codici sono realizzati in modo tale che dovrebbe occorrere una quantità "irragionevole" di errori nei

dati, affinché il destinatario decodifichi erroneamente, ottenendo finalmente dei dati diversi da quelli effettivamente inviatigli.

Entrambi gli schemi implicano l'introduzione di ridondanza (overhead) nel flusso di dati tra mittente e destinatario diminuendo così la portata utile (throughtput) informativa ovvero diminuendo l'efficienza di trasmissione e aumentando così la banda necessaria. Essi possono essere anche combinati tra loro, in modo tale che gli errori più lievi siano corretti senza necessità di ritrasmissione, e quelli più pesanti siano invece solamente individuati per poi richiedere la ritrasmissione.

-

Esercizio 4 dello scritto-2021-02-18



4[15]) Alice spedisce a Bob un messaggio **M1 molto grande** con garanzia di **non ripudiabilità** (ovvero Alice non potrà mai dimostrare di avere spedito un messaggio diverso da quello ricevuto da Bob) e di **Privacy**. Tuttavia il messaggio di Alice deve essere **firmato digitalmente dal notaio Claire**, che non deve capire il contenuto ma deve apporre la propria firma digitale, prima di inoltrare il messaggio a Bob. Bob infine vuole anche essere sicuro che il messaggio ricevuto da Claire **non sia un Replay** attack di Trudy (N.B. fare attenzione a dove si possono generare i replay attack). Come può essere realizzato lo schema di cifratura di costo minimo (minimo calcolo e massima efficienza) che garantisca tutti e solo i requisiti richiesti? Spiegare.

M1 molto grande quindi no RSA, ma dato che serve privacy usiamo Ks. Per la non ripudiabilità usiamo inviamo una coppia data da m e la il messaggio hash H(M1) criptato con chiave privata di A.
Aggiungiamo un nonce R1 perché Bob vuole essere sicuro del non-replay
Quindi Alice spedisce (KA-(Ks[H(M1)],R1],m),KB+(Ks))

Il notaio deve apporre la firma digitale quindi cripta con la sua chiave privata ciò che ha ricevuto da Alice. Aggiungiamo un nonce R2 perché Bob vuole essere sicuro del non-replay
KC-((Ks(KA-[H(M1),R1],m),KB+(Ks)),R)

soluzione:
Kc+(Ka-(H(m)), KS(m), Kb+(KS), R1) M2 = Ka-(H(m)), KS(m), Kb+(KS)

Kc-(H(M2), R2), M2