Contents

la congestione di un collegamento porta a parametri di riferimento fuori limite

1 Tecniche di controllo del flusso

ci sono metodi reattivi, che si attivano una volta che la congestione è stata rilevata, e metodi preventivi, che utilizzano metodologie che tendono a evitare che la congestione accada

1.1 Metodi reattivi

1.1.1 Sliding window

metodo credit based[1] la trasmissione dei pacchetti da parte di un nodo è regolata da dei "permessi" che possono essere "revocati" se la congestione è stata rilevata

funziona che inizi con W pacchetti di credito iniziale verso un nodo

questi saranno inviati entro un intervallo di tempo, (per tenere traccia et al è richesto il riscontro) se il riscontro arriva alla sorgente entro il tempo di finestra la finestra scorre di una posizione e si procede alla trasmissione di un nuovo pacchetto, se invece il riscontro arriva con ritardo superiore al tempo di finestra allora la trasmissione di un nuovo paccchetto viene ritardata.

non ci ho capito UNA SEGA

[1] yo bing chiling

1.2 Metodi preventivi

admission control noto ad esempio in ATM

altri metodi rate based

i metodi leaky bucket e token bucket permettono di trasmettere in sequenza tutti i pacchetti fino ad esaurire il numero di abilitazioni possedute

1.2.1 Algoritmo leaky bucket

vengono riversati sulla rete pacchetti con un data rate fissato, vengono mantenuti nel buffer quelli per la trasmissione. se vengono generati più pacchetti di quanti ne stanno nel buffer questi pacchetti extra vengono perduti, in questo modo non si controlla il data rate medio, ma si controlla quello massimo

1.2.2 Algoritmo token bucket

si ottiene un certo credito trasmissivo, quando poi c'è da trasmettere lo si fa utilizzando il credito a disposizione, alla velocità massima consentita dalla linea, se ci sono k token e devo mandare $h > k$ pacchetti allora i primi k vengono trasmessi con il credito di k, e gli altri dovranno aspettare che arrivi altro credito

2 Sicurezza di rete

riservatezza ci piacerebbe se l'informazione che mando restassero cazzi mia

integrità del messaggio se si usano tecniche per privacy sarebbe gradito che queste non avessero un impatto negativo sull'integrità della comunicazione

autenticazione si vuole sapere l'identità di chi parla

sicurezza operativa protezione nei riguardi di intrusioni non autorizzate, OPSEC BOIIIII

crittografia metodo per rendere minimo il trasferimento dell'informazione (?)

2.1 Tecniche a chiave simmetrica

prevede una chiave che consiste nel concordare uno spostamento del simbolo associato alla lettera un esempio è il codice di cesare il codice di cesare fa cagare il cazzo tipo alla seconda guerra mondiale in cui finivano tutte le frasi con "heil hitler" e gli hanno fatto il known plaintext attack di cristo grazie alan

2.2 Tecniche a chiave asimmetrica (public key)

RSA RSA è figo