Università degli Studi di Udine

DIMA — Dipartimento di Scienze Matematiche, Informatiche e Fisiche

Esame di **Reti di Calcolatori**

Soluzione

A.A. 2016-17 — I appello — 23 gennaio 2017

N.B.: il punteggio associato ad ogni domanda è solo una misura della difficoltà, e peso, di ogni domanda. Per calcolare il voto complessivo bisogna normalizzare a 30 (circa).

1. (3pt) Due segnali cosinusoidali a tempo continuo $s_1(t)$ e $s_2(t)$, aventi identica ampiezza A_0 e frequenze f_1 e f_2 distinte, sono emessi simultaneamente da un'unica antenna: $s_1(t) = A_0 \cos(2\pi f_1 t)$ e $s_2(t) = A_0 \cos(2\pi f_2 t)$. In tal modo dall'antenna si genera un segnale risultante $s(t)$ che è uguale alla loro somma algebrica: $s(t) = s_1(t) + s_2(t)$. È noto che questo segnale misurato all'antenna appare come un coseno a frequenza f_r, la cui ampiezza A_r però non è costante bensí oscilla nel tempo in dipendenza dallo sfasamento dei segnali cosinusoidali che formano il coseno risultante: $s(t) = A_r(t) \cos(2\pi f_r t)$. Se $f_1 = 500$ MHz e $f_2 = 450$ MHz, si calcoli il tempo $\tilde{t}$ in corrispondenza del quale l'ampiezza di $s(t)$ misurata all'antenna è nulla: $A_r(\tilde{t}) = 0$.

   R: L'ampiezza A_r è minima quando lo sfasamento è di mezzo periodo: in tal caso il primo e il secondo segnale hanno valore opposto. Poichè ogni 500 periodi del primo segnale il secondo ne completa 450, allora si ha che ogni 5 periodi del primo segnale il secondo ne completa 4.5, e dunque i due segnali si trovano per la prima volta in controfase dopo 5 periodi di $s_1(t)$: $\tilde{t} = 5T_1 = 5/f_1 = 10^{-8}$ s.

2. (4pt) Un cavo per la trasmissione di segnali possiede un fattore di attenuazione $\alpha = 0.5$ e contemporaneamente introduce un rumore medio di potenza $N_0 = 10$ mW, misurata all'uscita del cavo. Nell'ipotesi di dover trasmettere un segnale di potenza $P_0 = 0.3$ W, dopo quante sezioni di cavo il rapporto segnale disturbo varrà 0 dB?

   R: Procedendo per calcoli successivi di potenza e rumore all'uscita di ogni sezione, si trova che la potenza del segnale eguaglia quella del rumore dopo 4 sezioni: $P_4 = P_0/2^4 = 0.018750 = N_0/8 + N_0/4 + N_0/2 + N_0$

3. (3pt) In presenza del rapporto segnale disturbo visto all'esercizio precedente, come converrà settare un codificatore di bit in grado di immettere nel cavo tensioni elettriche nell'intervallo [-5,5] Volt?

   R: L'interpretazione del teorema di Shannon insegna che in presenza di un rapporto segnale disturbo SNR = 1 è possibile inviare non più di due livelli di segnale. Indipendentemente dalla codifica scelta, conviene dunque massimizzare la distanza tra i due livelli ponendone uno a $+5$ Volt e uno a -5 Volt.

4. (3pt) Lo stesso codificatore non possa eseguire più di 10^6 inversioni del valore di tensione al secondo. Qual é in tal caso la capacità del canale in questione nei tre casi in cui si scelga di adottare, rispettivamente, il protocollo di codifica NRZ, Manchester e NRZI?

   R: Il teorema di Shannon permette di calcolare la capacità del canale nell'ipotesi che il codificatore a due livelli possa effettuare 10^6 commutazioni al secondo a causa della limitazione di banda B del canale, il che permette di inviare un uguale numero di bit al secondo utilizzando la codifica NRZ oppure NRZI: $C = B \log_2(1 + \text{SNR}) = 10^6 = 1$ Mbit/s. La codifica Manchester invece a parità di commutazioni permette di inviare solo $10^6/2 = 5 \cdot 10^5 = 500$ kbit/s.

5. (3pt) Una linea di trasmissione di pacchetti di lunghezza $L = 4$ bit ha una probabilità di errore per bit $p = 10^{-6}$. Si assume l'indipendenza dell'errore su ciascun bit. In più si sa che se il primo bit del pacchetto é corretto allora anche il quarto bit del pacchetto é corretto. In quest'ipotesi si calcoli la probabilità che siano presenti tre bit errati su un pacchetto.

   R: Le uniche terne possibili di tre bit scorretti sono (1,2,3), (1,2,4), (1,3,4). Ognuna avviene con probabilità $p^3(1-p)$, da cui $P[\{\text{tre bit errati}\}] = 3p^3(1-p)$.

Una soluzione che faccia uso più ampio delle regole della statistica aiuta a convincersi di questo risultato. Se infatti il primo bit nel pacchetto é corretto allora la probabilità di avere tre errori nel pacchetto è nulla. Viceversa, sapendo che è scorretto allora vi sono tre coppie di due bit scorretti possibili: (2,3), (2,4), (3,4), da cui, per definizione di probabilità condizionata e per il teorema della probabilità totale,

$P[\{\text{tre bit errati}\}] = P[\{\text{tre bit errati}\}|\{\text{primo bit scorretto}\}] \cdot P[\{\text{primo bit scorretto}\}] = 3p^2(1-p) \cdot p.$

6. (3pt) Il polinomio generatore di un codice CRC proprietario a 16 bit sia $C(x) = x^{16}$. Quali bit errati non verrebbero rilevati in pacchetti lunghi 64 bit?

   R: Non vengono rilevati tutti gli errori i cui polinomi divisi per x^{16} hanno resto nullo: x^{16}, x^{32}, x^{48} e tutte le loro possibili combinazioni lineari in aritmetica modulo 2.

7. (2pt) A quale sequenza di bit corrisponde l'indirizzo ethernet 80:cd:2b:e4:b1:f2?

   R: Convertendo da esadecimale in binario si ha immediatamente

   10000000 : 11001101 : 00101011 : 11100100 : 10110001 : 11110010.

8. (3pt) Si dia la formula adoperata nella compressione JPEG per quantizzare i blocchi trasformati.

   R: `QuantizedValue(i,j) = IntegerRound(DCT(i,j)/Quantum(i, j))`, in cui

   `IntegerRound(x) = (round(x+0.5) if x>=0; round(x-0.5) if x<0)`.

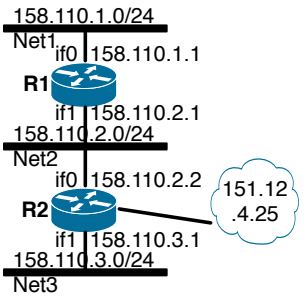
9. (3pt) Due host hanno indirizzi 129.10.20.31 e 129.10.20.35, rispettivamente. Si dia il CIDR della più piccola rete che li contiene entrambi, e si dica quanti host ci possono essere in tale rete.

   R: Si converte 31 e 35 in binario, e si guarda qual è il prefisso comune più lungo; questo sarà parte dell'indirizzo di rete, mentre il resto formerà l'indirizzo di host. 31=00100000, 35=00011111, i primi due bit sono uguali, e quindi il CIDR è 24+2=26. Rimangono 6 bit per gli host, quindi $2^6 - 2 = 62$ host.

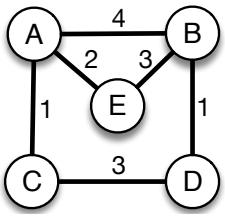
10. (3pt) Si dia la tabella di inoltro del router R2 nella rete a lato.

    R:

Net/CIDR	if	next hop
158.110.1.0/24	if0	158.110.2.1
158.110.2.0/24	if0	-
158.110.3.0/24	if1	-
/	if2	151.12.4.25



11. (3pt) I nodi della rete a lato utilizzano un algoritmo di routing basato sui vettori delle distanze. (a) Si dia la tabella di instradamento del nodo C. (b) Ad un certo punto, il costo del collegamento A-B diventa 1. Si dia il vettore inviato da A a C.



R:

Dest	d	next hop
A	1	A
B	4	D
C	0	-
D	3	D
E	3	A

Dest	d
A	0
B	1
C	1
D	2
E	2

12. (3pt) È possibile stabilire una comunicazione (TCP o UDP) tra una socket con un indirizzo IPv4 e una con un indirizzo IPv6? Perché?

    R: Non direttamente: è necessario passare attraverso un bridge di livello 3, che faccia una traduzione di indirizzi analogo al NAT.

13. (3pt) Tra UDP e TCP, quale protocollo di trasporto può essere usato per le comunicazioni multicast su IPv4? Perché? Questo fatto che conseguenze ha sull'affidabilità della comunicazione?

R: La comunicazione multicast è inerentemente connectionless. Non è possibile stabilire delle connessioni tipo TCP "uno-a-molti", quindi si può usare solo il protocollo UDP. Di conseguenza, le comunicazioni multicast hanno la stessa affidabilità di UDP, ossia di IP: sono best-effort, ma senza garanzia.

14. (3pt) In che stato deve essere la socket di una comunicazione TCP per poter trasmettere dati "nuovi" (ossia, non ritrasmissioni)? E per poter ricevere dati?

    R: Durante la trasmissione di dati nuovi, la socket deve essere in ESTABLISHED o CLOSE-WAIT. Per ricevere dati, deve essere in ESTABLISHED o in FIN-WAIT-1 o FIN-WAIT-2.

15. (3pt) In una certa connessione TCP, è RTT=100ms e MSS=1460 byte. A quale velocità minima (in byte/s) l'applicazione deve scrivere sulla socket, affinché i segmenti trasmessi siano sempre di dimensione massima? In tale situazione, quanto è lo "spreco" percentuale causato dalle intestazioni TCP e IP?

    R: Secondo l'algoritmo di Nagle, è necessario che vengano prodotti dati per almeno 1 MSS ogni RTT, quindi 1460/0,1 = 14600 byte/s. Ricordando che le intestazioni TCP e IP sono di 20 byte l'una, l'overhead è (20+20)(1460+20+20) = 40/1500 = 2,67%.

16. (3pt) Una certa connessione TCP ha MSS=1250, e si trova in fase additiva. All'inizio di un round di trasmissione, è `CongestionWindow`=10000, e nel buffer di uscita ci sono più di 10000 byte da trasmettere. Alla fine del round sono stati ricevuti gli ACK di tutti i segmenti inviati tranne due. Quanto diventa la nuova `CongestionWindow`?

    R: I segmenti invati nel round sono 10000/1250=8. Per ogni ack ricevuto l'incremento è MSS/8 = 156 byte, quindi l'incremento totale è 6*156=936. Alla fine si ha `CongestionWindow`=10936.

17. (3pt) Per ognuno delle seguenti azioni, si dica se è un attacco attivo o passivo e quale aspetto di sicurezza viene attaccato: (a) Cambiare lo sfondo del desktop del PC dell'amico, maldestramente lasciato aperto; (b) Guardare il numero di notifiche di WhatsApp sul cellulare dell'amico; (c) Togliere o spostare il segnalibro in un libro che l'amico sta leggendo.

    R: (a) Attivo; integrità dei dati (immagine di sfondo) (b) Passivo; Confidenzalità dei metadati (c) Attivo; integrità dei metadati.

18. (3pt) Un certo sensore (ad esempio, un termometro) produce pacchetti di dati $M_1, M_2, \ldots$ ognuno lungo 16 byte, che vengono trasmessi su un canale insicuro e inaffidabile (ad esempio, UDP su IP). Si vuole garantire integrità e confidenzialità di questi dati usando crittografia simmetrica (ad esempio AES), supponendo di avere già condiviso una chiave simmetrica. Quale modo di cifratura si può utilizzare?

    R: Si può usare il modo CBC o il modo CTR. In modo CBC, al passo i-esimo si trasmette $E_K(M_{i-1}), E_K(M_i)$, in modo da permettere la decifratura di M_i anche se il pacchetto precedente è andato perduto. In modo CTR, al passo i-esimo si trasmette $i, E_K(M_i)$.

19. (2pt) Il titolare di un certificato X.509 si accorge che la sua chiave privata è stata rubata. A chi si deve rivolgere per far revocare il certificato? Fino a quando tale certificato di revoca rimane in vigore?

    R: Solitamente, alla CA che ha emesso il certificato. Fino alla scadenza naturale del certificato.

20. (3pt) Si consideri il protocollo a lato, dove K_A, K_B sono chiavi simmetrica precondivisa tra A, B e la terza parte fidata C, e K è una chiave di sessione. Il messaggio M è confidenziale? è non ripudiabile? È puntuale (ossia al riparo da attacchi replay)?

    1. $A \to C : E_{K_A}(K, H(M))$
    2. $C \to A : E_{K_B}(K, H(M))$
    3. $A \to B : E_K(M), E_{K_B}(K, H(M))$

    R: È confidenziale, perché cifrato con la chiave di sessione K. È ripudiabile, perché B può creare una falsa K e una falsa "firma" $E_{K_B}(K, H(M))$, e asserire che siano provenute da C. Non è puntuale: un attaccante può reinviare il messaggio al passo 3, senza essere scoperto.

21. (3pt) Nel protocollo a lato PU_B è la chiave pubblica di B, K è una chiave di sessione creata da A e N è una nonce. A è autenticato per B? B è autenticato per A? K è puntuale?

    1. $A \to B : E_{PU_B}(K)$
    2. $B \to A : E_K(N)$
    3. $A \to B : N$

    R: A non è autenticato: non risponde a nessuna sfida che lo identifichi. B è autenticato: riesce a decifrare il messaggio al passo 1. K è puntuale: B riconosce eventuali attacchi replay al passo 3.

22. (3pt) Bob riceve una mail S/MIME firmata da Alice. Nel momento in cui verifica la firma, il certificato X.509 di Alice è stato emesso da una CA nota a Bob ma non è ancora valido: l'inizio del periodo di validità è successivo all'orologio di Bob. Bob può concludere che messaggio è autentico e puntuale?

    R: In teoria sì se il certificato della CA è valido, e se Bob si fida della CA. Questo evento solitamente avviene se l'orologio di Bob è rimasto indietro, ma è possibile (anche se raro) che le CA emettano dei certificati "postdatati". In ogni caso, il client di posta segnala l'anomalia all'utente. La puntualità è affidata al timestamp inserito dal mittente del messaggio, e quindi non completamente verificabile.

23. (3pt) Due applicazioni vogliono comunicare usando SSL o TLS, ed entrambe dispongono di un certificato X.509 valido. Quali meccanismi di definizione della chiave possono essere usati durante la fase di handshake, e quali delle controparti può essere autenticata?

    R: Si possono usare Diffie-Hellman anonimo (che non autentica nessuno), oppure RSA (che autentica il client per il server), oppure Diffie-Hellman effimero (che autentica entrambi).

24. (3pt) Due host comunicano mediante IPsec con AH in modalità trasporto. Cosa succede ad un pacchetto di 1500 byte se deve attraversare una linee la cui MTU è di 572 byte?

    R: Viene frammentato in tre frammenti, come di consueto per IPv4 durante il percorso, e vengono riassemblati dall'host di destinazione prima di essere processati da IPsec. Quindi IPsec non si accorge della frammentazione. Notare che non c'è un header AH in ogni frammento IP: solo il primo lo contiene, gli altri hanno la parte rimanente del payload.