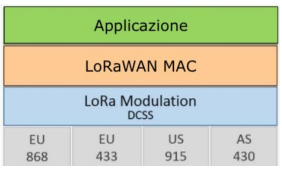
DMIF, Università degli Studi di Udine V appello A.A. 2019-20 — 7 settembre 2020

Esame di **Reti di Calcolatori**

Soluzione

1. La figura a lato mostra lo stack di LoRa (Long Range), molto usato nell'IoT. La comunicazione avviene su varie bande ISM (433 e 868 MHz in Europa, 915 MHz negli USA, ecc), con una modulazione spread spectrum. Lo strato "LoRaWAN MAC" implementa le funzionalità di controllo di accesso al mezzo e di controllo degli errori, ma anche la comunicazione a pacchetti best-effort da nodo a server esterni, passando attraverso dei gateway. (a) A quali strati del modello OSI corrisponde ogni strato di questo stack? (b) In quale strato viene implementato la FEC?



   R: (a) Bande fisiche e LoRa Modulation: stato 1 (fisico); LoRaWAN MAC: strato 2 (datalink) ma anche 3 (rete). Applicazione: dal 4 in su. (b) LoRa Modulation.

2. Un canale analogico di comunicazione opera in una banda di frequenza da 0 a 10kHz. (a) Determinare il rapporto segnale/rumore minimo necessario per una trasmissione con bitrate di 100 kb/s senza errori. (b) Si supponga che per ottenere una trasmissione con errore accettabile, sia necessario una FEC con code rate pari a 0.5. Determinare il numero minimo di bit codificati in un Baud.

   R: (a) Dal teorema SH, $C \leq B\log_2(1+SNR)$ da cui $100kb/s \leq 10kHz\log_2(1+SNR)$ per cui $SNR = 2^10 - 1 = 1023 = 30dB$. (b) Il Baud rate è il doppio della larghezza della banda, quindi 20 kBaud. Se il code rate è 1/2=0.5, allora il bitrate grezzo deve essere 1/0.5 * 100 kb/s = 200 kb/s. Ne segue che il numero di bit per Baud deve essere 200 / 20 = 10.

3. Al fine di riconoscere gli errori, una certa linea di trasmissione aggiunge un bit di parità ogni 4 bit. La probabilità di errore per bit è $p = 10^{-3}$. Qual è la probabilità che un pacchetto di 4 bit con almeno un errore venga accettato come corretto?

   R: Il bit di parità non permette di riconoscere errori su un numero pari di bit. Quindi i casi in cui il pacchetto (di complessivi 5 bit, comprendendo anche quello di parità) è sbagliato ma non riconosciuto come tale sono con 2 o 4 bit errati. La probabilità di 2 errori è $p_2 = \binom{5}{2}p^2(1-p)^3 = 10p^2(1-p)^3$; la probabilità di 4 errori è $p_4 = \binom{5}{4}p^4(1-p) = 5p^4(1-p)$. In totale la probabilità che un pacchetto errato venga accettato è $P = p_2 + p_4$. Per $p = 10^{-3}$, è $9.98 * 10^{-6} \approx 10^{-5}$.

4. Un certo collegamento con un RTT di 10 ms e capacità di 100 Mbps viene utilizzato mediante un protocollo sliding window. Quanto deve essere grande il buffer dell'host trasmittente per riuscire a sfruttare completamente il canale?

   R: Nello sliding window si mantengono i dati già trasmessi finché non abbiamo conferma della ricezione. Per essere sicuri di poter ritrasmettere dati precedentemente inviati ma ancora non riconosciuti entro un RTT, bisogna accumulare la massima quantità di dati trasmissibili in un RTT, ossia $10*10^{-3}*100*10^6 =$ 100000 bit = 12500 byte.

5. Un dispositivo sta trasmettendo un flusso audio ad una cassa Bluetooth. Ricordando che ogni frame BT porta al massimo 483 bit in uno slot e ogni slot dura 625 μs, quanto può essere il bitrate massimo del flusso audio (senza utilizzare trasmissione multislot)?

   R: La capacità totale del canale è $483/(625 * 10^{-6}) = 0.772$ Mbps, ma per avere quella dal dispositivo alle casse bisogna dividere per 2 perché il dispositivo può comunicare solo negli slot pari. Quindi 386 kbps.

6. (a) Qual è un importante vantaggio delle reti a commutazione di circuito rispetto a quelle a commutazione di pacchetto? (b) Quale delle due strategie permette, in linea teorica, un maggior utilizzo dei canali?

R: (a) Che permettono di allocare, a priori, le risorse necessarie per garantire una certa QoS (b) Quella a pacchetti.

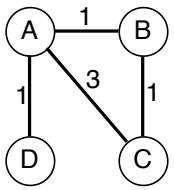
7. Si considerino le seguenti reti: A: 184.85.16.0/22; B: 184.85.16.0/24; C: 184.85.16.0/26. (a) Qual è la rete con il maggior numero di indirizzi disponibile? (b) A quale/i di queste reti appartiene l'indirizzo 184.85.19.15? (c) E l'indirizzo 184.85.16.200?

   R: (a) A, ovviamente. (b) A e basta. (c) a A e B.

8. Un host invia una richiesta ARP per l'indirizzo 185.84.31.5 dalla sua interfaccia 185.84.31.8, nella sotto-rete 185.84.31.0/24. (a) Qual è l'indirizzo IP di destinazione di tale richiesta ARP? (b) Cosa contiene il pacchetto di risposta? (c) Cosa conclude l'host se non riceve alcuna risposta (entro un certo timeout)?

   R: (a) Il broadcast: 185.84.31.255 (b) L'indirizzo MAC (presumibilmente Ethernet) dell'interfaccia che ha l'indirizzo 185.84.31.5 (c) L'host conclude che 185.84.31.5 non è raggiungibile.

9. I router della rete a lato utilizzano un algoritmo di routing basato sul vettore delle distanze, con *split horizon with poison reverse*. Dopo che la rete si è stabilizzata: (a) Si dia la tabella di instradamento di A. (b) Si mostri il vettore delle distanze che A invia a C. (c) Si mostri il vettore delle distanze che B invia ad A.



R: (a)

dest	d	n.h.
A	0	-
B	1	B
C	2	B
D	1	D

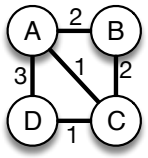
(b)

dest	d
B	1
C	2
D	1

(c)

dest	d
A	∞
C	1
D	∞

10. I router della rete a lato usano DVMRP per instradare il traffico multicast. Sia B il core router di un certo gruppo. (a) Quando viene inviato un pacchetto IP multicast a tale gruppo, quanti pacchetti arrivano in flooding a D? (b) Quale di questi viene inoltrato, e a quale nodo?
    R: (a) 2, da A e da C. (b) Uno (quello che riceve da C), verso A.



11. Un'applicazione C sull'host A invia datagrammi UDP ad un'applicazione S sull'host B. (a) I datagrammi arrivano a B nell'ordine con cui sono stati inviati? (b) In che ordine vengono consegnati a S? (c) È possibile che un datagramma non venga consegnato a S, nonostante sia arrivato a B?

    R: (a) Non necessariamente quello di invio, possono essere scambiati o perduti o duplicati. (b) Quella di arrivo all'host B (c) Sì, se il buffer di arrivo è pieno, i datagrammi vengono scartati.

12. Un host TCP riceve su una certa porta un segmento con SYN=1, SeqNum=1343. (a) In che stato deve trovarsi la socket affinché venga inviato un segmento con SYN=1, in risposta al precedente? (b) Cosa viene inviato in risposta, se la socket associata a quella porta è nello stato CLOSED? (c) E se non c'è nessuna socket associata a quella porta?

    R: (a) LISTEN (apertura passiva). (a) Manda un RST=1. (c) Idem: sempre RST=1.

13. Una socket TCP ha un buffer di uscita di dimensione `MaxSendBuffer`=10000 byte. Ad un dato istante, è `LastByteWritten`=8000, `LastByteAcked`=2000, `LastByteSent`=7000. (a) Quanti (nuovi) byte può ancora spedire alla controparte? (b) Se la `AdvertisedWindow` è 0, quanti byte può ancora produrre l'applicazione che usa quella socket, senza bloccarsi?

    R: (a) `LastByteSent`- `LastByteAcked` = 7000-2000 = 5000.

    (b) Lo spazio occupato nel buffer è quello da `LastByteWritten` a `LastByteAcked`, considerando che è un buffer circolare. Quindi lo spazio ancora disponibile è `MaxSendBuffer` - (`LastByteWritten`-`LastByteAcked`) = 10000 - (8000-2000) = 4000 byte.

14. Un router implementa RED con MinThreshold=20KB e MaxThreshold=60KB per una certa interfaccia. Ad un certo istante la coda di tale interfaccia contiene 18KB. Arrivano al router tre pacchetti in rapida successione, ciascuno di 3KB. Qual è la probabilità che tutti e tre vengano accodati?

    R: Probabilità di scarto nell'intervallo: $Q(l) = (l - 20)/(60 - 20) = (l - 20)/40$. Probabilità di accettazione nell'intervallo: $P(l) = 1 - Q(l) = (60 - l)/40$.

Probabilità di accettazione del primo pacchetto: $P_1 = 1$ (perché è ancora sotto il MinThreshold). Probabilità di accettazione del secondo pacchetto: $P_2 = P(21) = (60 - 21)/40 = 39/40$. Probabilità di accettazione del terzo pacchetto, dopo che il secondo è stato accettato: $P_3 = P(24) = (60 - 24)/40 = 36/40$. Probabilità congiunta: $P = P_1 * P_2 * P_3 = 1 * (39/40) * (36/40) = 0,8775 = 88\%$.

15. Implementando la confidenzialità a livello trasporto: (a) si mette in sicurezza l'intestazione di livello applicativo? (b) E quella di trasporto? (c) È compatibile con le funzioni di instradamento dei router?

    R: (a) sì; (b) no; (c) sì.

16. Un flusso di pacchetti $M_1, M_2, \ldots$ viene cifrato usando AES in questo modo: $C_i = i, E_K(i) \oplus M_i$, dove K è una chiave precondivisa. Se M_i è più lungo di 128 bit, si ripete lo XOR con $E_K(i)$ lungo tutto M_i. (a) Qual è l'operazione che deve fare il ricevitore per decifrare un qualsiasi messaggio C in questo flusso (ossia riottenere il messaggio corrispondente)? (b) È possibile alterare un messaggio cifrato in modo tale che il destinatario non se ne accorga (ossia che decifri il messaggio alterato senza rilevare errori)?

    R: (a) se $C = i, R$, allora $M_i = E_K(i) \oplus R$. (b) Sì, perché posso spostare/togliere/duplicare blocchi di 128 bit all'interno dello stesso messaggio e la decifratura ha successo lo stesso. In pratica è come se usassimo AES in modo ECB.

17. Nel protocollo a lato, K_A, K_B sono le chiavi master precondivise tra A, B e il KDC, e K è una chiave di sessione generata da KDC. (a) La segretezza di K è garantita? (b) E quella di M? (c) K è puntuale per A (ossia non soggetta ad attacchi replay)?

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

    R: (a) Sì, è garantita dalle cifrature al passo 2. (b) No: se E ha una chiave K' da una sessione precedente con B, può spacciarsi per A e ricevere il messaggio destinato ad A: 3. $E \to B : A, E_{K_B}(K')$; 4. $B \to E : E_{K'}(M)$ (c) Sì, per la nonce.

18. Un utente A, titolare di un certificato X.509, si accorge di aver perso la chiave privata corrispondente (ossia, non la trova più). (a) È necessario che richieda l'emissione di un certificato di revoca alla sua CA? (b) E se ha il dubbio che un altro utente possa averla copiata?

    R: (a) No, può aspettare la naturale scadenza. (b) Sì, altrimenti l'altro utente può usarla al posto suo.

19. Si consideri il protocollo a lato, dove: y_A e y_B sono le due chiavi pubbliche D-H; K_A è un segreto precondiviso tra A e la terza parte fidata C, e analogamente per K_B; H è una funzione hash. (a) Questo protocollo è vulnerabile all'attacco MITM? (b) Se un attaccante riesce in qualche modo ad acquisire una vecchia chiave D-H, può forzare A e B a riusarla?

    1. $A \to C : y_A, H(K_A, y_A)$
    2. $C \to B : y_A, H(K_B, y_A)$
    3. $B \to C : y_B, H(K_B, y_B)$
    4. $C \to A : y_B, H(K_A, y_B)$

    R: (a) No, perché C fa da autenticatore dei messaggi. (b) No, perché A e B inventano le mezze chiavi sempre fresche, quindi si accorgerebbero se ci fosse un tentativo di sostituzione con chiavi vecchie.

20. Due host instaurano una comunicazione IPsec con ESP in modalità tunnel. Un pacchetto di 1500 byte deve attraversare un link la cui MTU è di 560 byte. (a) In quanti pacchetti viene frammentato? (b) In quali frammenti è presente l'intestazione IP esterna? (c) E in quali quella interna?

    R: (a) Viene frammentato in tre frammenti. (b) In tutti e tre (altrimenti non possono essere recapitati) (c) Solo il primo; gli altri hanno le rimanenti parti del payload.