Escola Politécnica da Universidade de São Paulo
Departamento de Engenharia de Telecomunicações e Controle

PTC2550 - Redes de Comunicação de Dados e Transporte Multimídia
1o semestre 2017

Lista de Exercícios Suplementares 3

1) [Kurose and Ross, 2017, p. 612] Considere uma conexão TCP rodando sobre *Mobile IP*. Verdadeiro ou falso: A fase de conexão TCP entre o correspondente e o *host* móvel passa através da rede nativa do móvel, mas a fase de transferência de dados ocorre diretamente entre o correspondente e o *host* móvel, sem passar pela rede nativa.

2) [Kurose and Ross, 2017, p. 612] Quais são as providências que podem ser tomadas para evitar que um único enlace sem fio degrade o desempenho de uma conexão que usa TCP na camada de transporte fim-a-fim?

3) [Kurose and Ross, 2013] Considere a Figura 1. Similarmente à nossa discussão em aula, suponha que o vídeo seja codificado a uma taxa de bit constante e, assim, cada bloco de vídeo contenha quadros que devem ser reproduzidos a cada quantidade de tempo fixa, Δ. O servidor transmite o primeiro bloco de vídeo em t_0, o segundo bloco em $t_0 + \Delta$, o terceiro bloco em $t_0 + 2\Delta$ e assim por diante. Uma vez que o cliente inicie a reprodução, cada bloco deve ser reproduzido Δ unidades de tempo depois do bloco anterior.

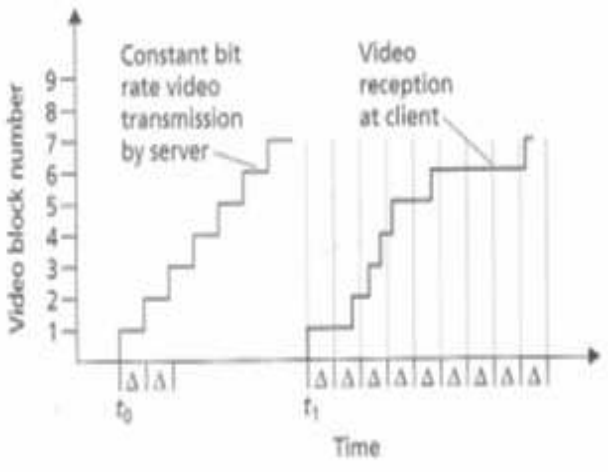

Figura 1: [Kurose and Ross, 2013]

a) Suponha que o cliente inicie a reprodução logo depois que o primeiro bloco chega em t_1. Na Figura 1, quantos blocos de vídeo (incluindo o primeiro bloco) terão chegado no cliente a tempo para sua reprodução? Explique como você chegou a essa resposta.

b) Suponha agora que o cliente inicie a reprodução em $t_1 + \Delta$. Quantos blocos de vídeo (incluindo o primeiro bloco) terão chegado ao cliente em tempo para sua reprodução? Explique como você chegou a essa resposta.

c) No mesmo cenário do item (b), qual é o maior número de blocos que serão armazenados em algum momento no buffer do cliente, esperando pela reprodução? Explique como você chegou na sua resposta.

d) Qual o menor atraso de reprodução no cliente de forma que todo bloco de vídeo tenha chegado a tempo para reprodução? Explique como você chegou na sua resposta.

4) [Kurose and Ross, 2013] Considere o modelo simples para *streaming* HTTP estudado em aula. Lembre-se que B denota o tamanho do buffer do aplicativo cliente e seja Q o número de bits armazenados no *buffer* antes que o aplicativo cliente inicie a reprodução. Lembre-se também que r denota a taxa de consumo de vídeo. Assuma que o servidor envia bits a uma taxa constante x sempre que o *buffer* do cliente não está cheio.

a) Suponha que $x < r$. Como discutido em aula, nesse caso a reprodução alterna entre períodos de reprodução contínua e períodos de congelamento. Determine o comprimento de cada reprodução contínua e cada período de congelamento em função de Q, r e x.

b) Agora suponha que $x > r$. Em que instante $t = t_f$ o buffer do aplicativo cliente fica cheio?

5) [Kurose and Ross, 2017, p. 760] Considere a figura a seguir. Um transmissor começa a mandar áudio em pacotes periodicamente em $t = 1$. O primeiro pacote chega ao receptor em $t = 8$.

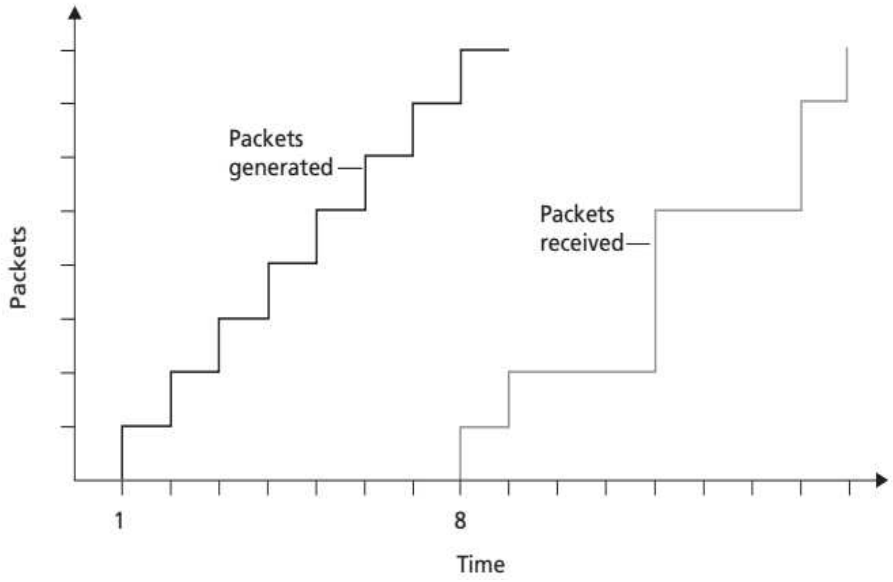

Figura 2:

(a) Quais são os atrasos (do transmissor para o receptor, ignorando os atrasos de reprodução) dos pacotes 1 ao 8? Note que cada segmento horizontal ou vertical da figura tem 1, 2 ou 3 unidades de tempo.

(b) Se a reprodução do áudio começa em $t = 9$, quais dos primeiros oito pacotes enviados não chegarão a tempo para reprodução?

(c) Qual o mínimo atraso de reprodução no receptor que tem como resultado todos os primeiros oito pacotes chegando em tempo para sua reprodução?

6) [Kurose and Ross, 2017, p. 760] Considere novamente a Figura 2, mostrando os instantes de transmissão e recepção de pacotes de áudio.

(a) Compute o atraso estimado para os pacotes 2 a 8 usando a fórmula para d_i vista na Aula 16. Use $\alpha = 0{,}1$.

(b) Compute o desvio estimado do atraso em relação à média para os pacotes 2 a 8 usando a fórmula para v_i vista na Aula 16. Use $\beta = 0{,}1$.

7) [Kurose and Ross, 2017, p. 760] David está em seu PC e que chamar Beatriz, que também está trabalhando em seu PC. Os PCs de David e Beatriz estão equipados com *software* baseado em SIP para fazer e receber chamadas telefônicas. Assuma que David conhece o endereço IP do PC de Beatriz. Ilustre o processo de estabelecimento de chamada SIP.

8) [Kurose and Ross, 2017, p. 761]

(a) Considere uma chamada em conferência de áudio no Skype com $N > 2$ participantes. Suponha que cada participante gere um fluxo constante de r bps. Quantos bits por segundo o iniciador da chamada precisa enviar? Quantos bits por segundo cada um dos $N - 1$ participantes precisa enviar?Qual a taxa total de envio, agregada sobre todos os participantes?

(b) Repita o item (8a) para uma chamada de videoconferência usando um servidor central.

(c) Repita o item (8b) mas agora supondo que cada *peer* envia uma cópia do seu fluxo de vídeo para cada um dos $N - 1$ *peers*.

9) Considere o policiamento "balde de fichas" da Figura 3 que foi discutido em aula.

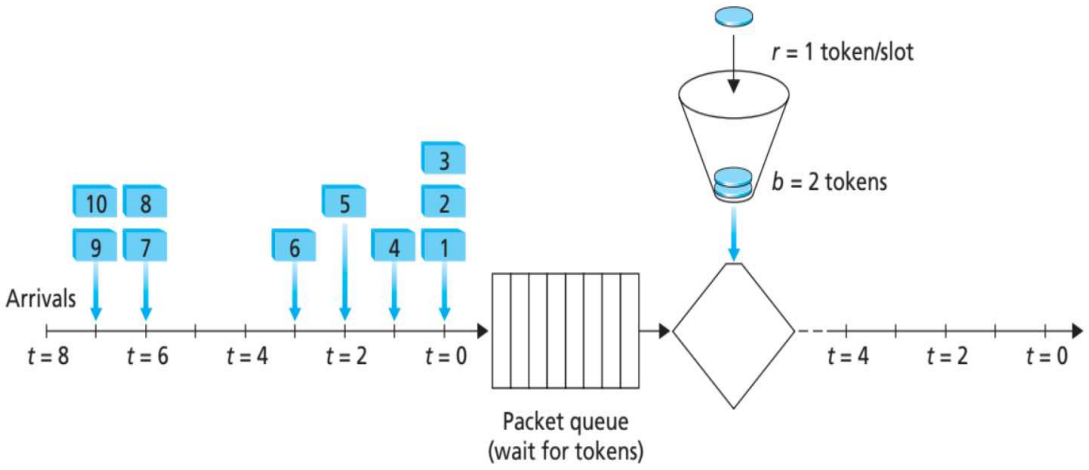

Figura 3:

O balde inicialmente está cheio em $t = 0$. Considere dessa vez que $\boldsymbol{r = 2}$ fichas/*slot*.

(a) Seguindo o que foi feito em aula, para cada *slot* de tempo, identifique os pacotes que estão na fila e o número de fichas no balde, imediatamente após as chegadas terem sido processadas mas antes dos pacotes terem passado a fila e retirado uma ficha.

Assim, por exemplo, em $t = 0$, os pacotes 1, 2 e 3 estão na fila e existem 2 fichas no balde.

(b) Para cada *slot* de tempo indique quais pacotes são transmitidos após terem retirado uma ficha. Assim, por exemplo, em $t = 0$, os pacotes 1 e 2 são transmitidos.

10) [Kurose and Ross, 2017, p. 763] Considere novamente o sistema da Figura 3 e suponha agora que $r = 3$ e que $b = 2$. Mudam as respostas do Exercício 9?

11) [Kurose and Ross, 2017, p. 694] Usando a cifra monoalfabética do Slide 13 da Aula 19, codifique a mensagem "Esta e uma mensagem secreta". Decodifique a mensagem "fsgg ash".

12) a) Usando RSA, escolha $p = 5$ e $q = 7$ e codifique os números 12, 19 e 27 separadamente. Aplique o algoritmo de decriptação à versão encriptada dos números para obter a mensagem em texto aberto.

b) Escolha p e q por conta própria e encripte 1834 como uma única mensagem m.

13) [Kurose and Ross, 2017, p. 695] Considere o RSA com $p = 7$ e $q = 13$.

a) Quais são os valores de n e z?

b) Seja $e = 17$. Essa é uma escolha aceitável para e?

c) Encontre d tal que $ed \mod z = 1$

d) Encripte a mensagem $m = 9$ usando a chave (n,e). Seja c o texto cifrado correspondente. Mostre todo o trabalho.

e) Mostre que decriptando-se c do item anterior obtém-se $m = 9$ novamente.

14) [Kurose and Ross, 2017, p. 697] A figura no Slide 20 da Aula 22 mostra as operações que a Alice deve realizar com PGP para obter confidencialidade, autenticação e integridade. Faça o diagrama de operações correspondente que Bob deve realizar sobre o pacote recebido por Alice.

15) Suponha que Alice queira enviar um e-mail para Bob. Bob tem uma par de chaves público-privada $\left(K_B^+, K_B^-\right)$ e Alice tem o certificado de Bob. Mas Alice não tem um par chave pública-chave privada. Alice e Bob (e o mundo inteiro) compartilham a mesma função de *hash* $H(\cdot)$.

a) Nessa situação, é possível projetar um esquema de modo que Bob possa verificar se Alice criou a mensagem? Se sim, mostre como com um diagrama de blocos para Alice e Bob.

b) É possível projetar um esquema que forneça confidencialidade para o envio de mensagens de Alice para Bob? Se sim, mostre um diagrama de blocos para Alice e Bob.

Referências

Kurose, J. and Ross, K. (2013). *Redes de Computadores e a Internet: Uma Abordagem Top Down*. Pearson.

Kurose, J. and Ross, K. (2017). *Computer Networking: A Top-Down Approach*. PEARSON EDUC.