Tutoriumsblatt 8

Diskussion: 6. + 7. Juli 2021

Aufgabe 8.1: TCP: Fluss- und Staukontrolle

Erläutern Sie die Gemeinsamkeiten/Unterschiede von Fluss- und Staukontrolle bei TCP.

a) Welches *Problem* versuchen beide zu beheben?

b) An welchen *Stellen* tritt das Problem jeweils auf?

c) Wie *erfährt* der Sender, dass er seine Datenrate durch die *Flusskontrolle* reduzieren muss?

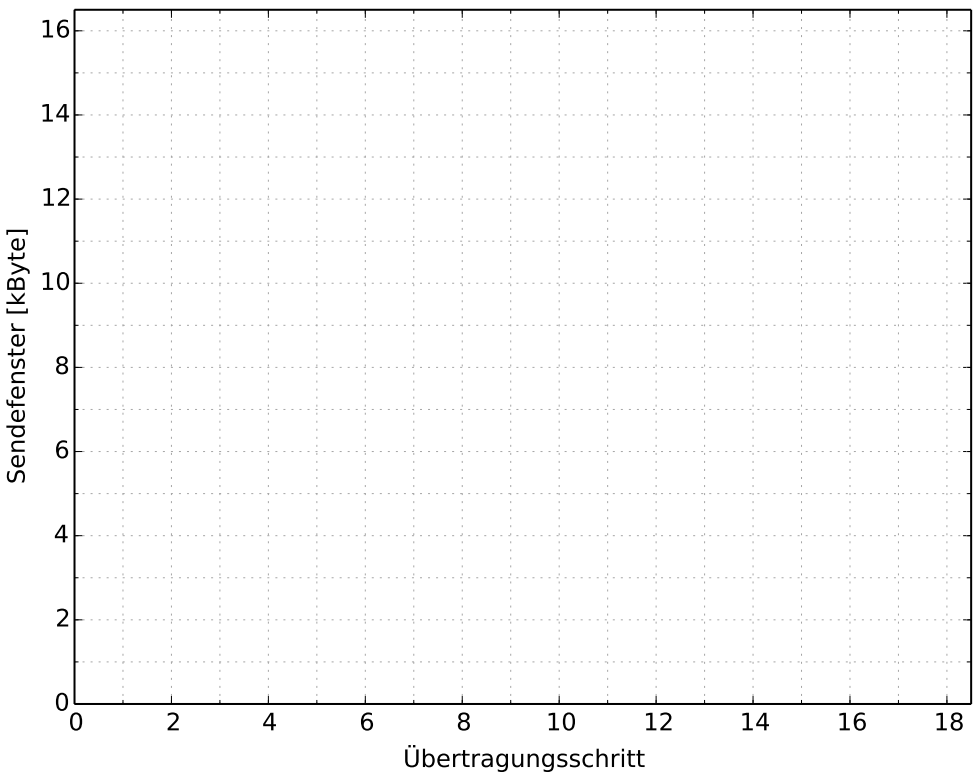
d) Wie verhält es sich im Fall von *Staukontrolle*?

Aufgabe 8.2: TCP Congestion Control

a) Beschreiben Sie knapp den *Slow-Start-Mechanismus* bei TCP. Warum wird ein *Schwellenwert* (Threshold) verwendet?

b) Eine TCP-Verbindung nutze den Slow-Start-Algorithmus mit einem Schwellenwert (Slow-Start Threshold, `ssthresh`) von anfangs 16 kByte. Die MSS sei 1 kByte, die Window Size des Empfängers 24 kByte.

Stellen Sie dar, wie sich die Datenrate in diesem Szenario ändert. *Zeichnen Sie für die Übertragungsschritte 1 bis 18 jeweils die erreichte Übertragungsrate (ausgedrückt über die Größe des Sendefensters `swnd`) sowie den Threshold in das folgende Diagramm ein.*



Als ein Übertragungsschritt werde hier die Versendung der möglichen Datenmenge samt Empfang der zugehörigen Quittungen bezeichnet; wurden alle Quittungen des aktuellen Übertragungsschrittes erhalten, wird im nächsten Übertragungsschritt wieder die gesamte nun mögliche Datenmenge versendet. Bei Übertragungsschritt 5 und 13 findet jeweils ein Timeout statt, der vom Sender als Netzüberlastung interpretiert wird.

c) In der Realität werden Slow-Start und Congestion Avoidance nicht alleine eingesetzt. Gängige Erweiterungen sind *Fast Retransmit* und *Fast Recovery*. *Welchen Zweck haben diese Erweiterungen*?

Aufgabe 8.3: Sicherheitsziele

a) Was ist der Unterschied zwischen *Authentifizierung* und *Autorisierung*?

b) Was sind die Unterschiede zwischen *Vertraulichkeit* und *Integrität*?

c) Ist *Vertraulichkeit auch ohne Integrität* möglich? Ist *Integrität auch ohne Vertraulichkeit* möglich? Begründen Sie Ihre Antwort.

d) Objekte im Internet (Switche, Router, Web-Server, Benutzer-Endsysteme, usw.) müssen häufig in der Lage sein, sicher miteinander zu kommunizieren. Geben Sie *zwei Beispiele* von Objekten an, die eventuell sicher miteinander kommunizieren wollen. Geben Sie auch jeweils an, *welche Sicherheitsmaßnahmen sinnvoll* sind.

Aufgabe 8.4: Shift Cipher

a) Alice sendet folgende verschlüsselte Nachricht an Bob:

$$c = \texttt{GSVSREWGLYXDZIVSVHRYRK}.$$

Sie haben die verschlüsselte Nachricht c mitgehört und möchten diese nun entschlüsseln. Sie wissen, dass Alice eine Shift Cipher verwendet hat und dass nur Großbuchstaben verwendet werden. Sie kennen sogar die Kodierungstabelle:

A	0	E	4	I	8	M	12	Q	16	U	20	Y	24
B	1	F	5	J	9	N	13	R	17	V	21	Z	25
C	2	G	6	K	10	O	14	S	18	W	22		
D	3	H	7	L	11	P	15	T	19	X	23		

Geben Sie den Schlüssel k an, der zur Verschlüsselung verwendet wurde, und entschlüsseln Sie die Nachricht c. Dokumentieren Sie, wie Sie vorgegangen sind, um k zu ermitteln.

Hinweis: Die entschlüsselte Nachricht ist ein deutsches Wort.

b) Gegeben sei nun die folgende Nachricht:

$$c = \texttt{XCYMYL MUNT BUN EYCHY VYMIHXYLY VYXYONOHA.}$$

Geben Sie ein Verfahren an, mit dem Sie, unter der Annahme, einen normalen deutschen Text vorliegen zu haben, bei dem die Satz- und Leerzeichen nicht verschlüsselt worden sind, die Nachricht *ohne Brute-Force-Angriff* entschlüsseln können. Wie lautet der Schlüssel k?