

8. TUTORIUM

DATENKOMMUNIKATION UND SICHERHEIT

TUTORIUMSGRUPPE 18

MATTHIS FRANZGROTE

COMSYS

RWTH AACHEN

07.07.2021

1 Aufgabe 8.1: TCP: Fluss- und Staukontrolle

2 Aufgabe 8.2: TCP Congestion Control

3 Aufgabe 8.3: Sicherheitsziele

4 Aufgabe 8.4: Shift Cipher

AUFGABE 8.1: TCP: FLUSS- UND STAUKONTROLLE

AUFGABE 8.1 A)

Aufgabe

Welche *Problem* versuchen je die Fluss- und Staukontrolle bei TCP zu beheben?

Aufgabe

Welche *Problem* versuchen je die Fluss- und Staukontrolle bei TCP zu beheben?

In beiden Fällen Überlastungen
Aber wovon?

AUFGABE 8.1 B)

Aufgabe

An welchen *Stellen* tritt das Problem jeweils auf?


Aufgabe

An welchen *Stellen* tritt das Problem jeweils auf?

- Flusskontrolle: Überlastung des Empfängers
- Staukontrolle: Überlastung "des Netzes" (also der Router im Netz)

AUFGABE 8.1 c)

Aufgabe

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

Aufgabe

Wie *erfährt* der Sender, dass er seine Datenrate durch die *Flusskontroller* reduzieren muss?

Window-Tag im TCP Header

- Mitsenden der *aktuellen* Fenstergröße in jedem Segment
- Empfänger reduziert den Wert gemäß seinem freien Buffer um einen Überlauf zu vermeiden

Aufgabe

Wie verhält es sich im Fall von *Staukontrolle*?

Aufgabe

Wie verhält es sich im Fall von *Staukontrolle*?

- Keine expliziten Benachrichtigungen, da die Überlastung auf Schicht 3 stattfindet (Trennung der Schichten)
 - Fehlende Bestätigungen suggerieren eine Stausituation
- ⇒ Algorithmen zur Reduktion der Netzlast (Slow Start)
- Aber: Das Fehlen von ACKs kann nicht nur durch Überlast auftreten (auch wenn es meistens der Fall ist)
 - z.B. Übertragungsfehler

Aufgabe

Wie verhält es sich im Fall von *Staukontrolle*?

Weitere Konzepte:

- Random Early Detection:
Router verwerfen im Vorhinein Pakete (wenn Queue Schwellenwert überschreitet), um die Congestion Control zu triggern
- Es gibt aber auch Entwicklungen mit Schichverletzung:
Statt Pakete wie bei RED zu verwerfen doch zustellen, aber Flag im IP Header setzen (Explicit Congestion Notification)
Empfangene IP Instanz gibt dies an die TCP Instanz weiter

AUFGABE 8.2: TCP CONGESTION CONTROL

AUFGABE 8.2 A)

Aufgabe

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

AUFGABE 8.2 A)

Aufgabe

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

Slow-Start:

- Versende erstmal nur ein Segment maximaler Größe (cwnd = 1)
 - Kommt das ACK vorm Timeout an, versende zwei weitere
 - Und so weiter, also versende pro ankommenden ACK zwei Segmente
- ⇒ In jedem Schritt **Verdopplung** der Anzahl der zu übertragenden Segmente



Timeout \rightarrow ssthresh $:=$ cwnd/2
cwnd $:=$ 1

Aufgabe

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

Wofür der Threshold?

- Ginge das ganze munter so weiter, wird irgendwann das Netz überlastet
- Also ab Erreichen des Threshold: Nur noch **linearer** Anstieg der Fenstergröße
- Für jedes empfangene ACK nur **ein** neues Segment versenden
- Sobald einmal eine gesamte Fenstergröße versandt wurde, ein zusätzliches Segment (also bei $cwnd = n$ nach n ACKs)

AIMD

AUFGABE 8.2 B)

Aufgabe

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.

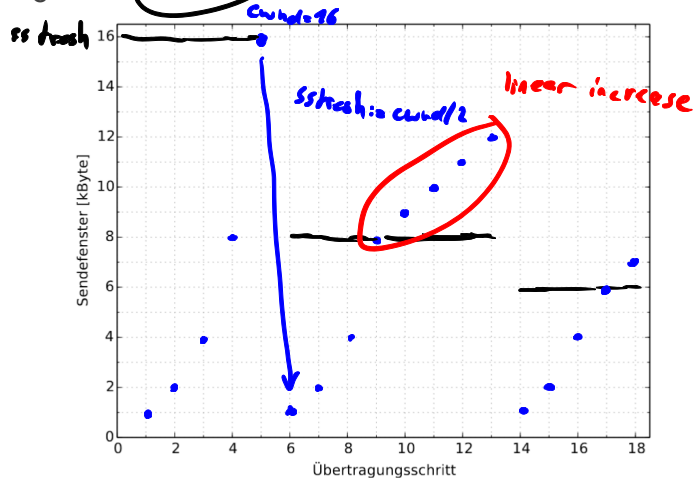
Stellen Sie dar, wie sich die Datenrate in diesem Szenario ändert.

Wichtig: Wir abstrahieren hier in Übertragungsschritte (Versenden der möglichen Datenmenge und Empfang der dazugehörigen ACKs). Wenn alle ACKs da sind, wir die nächste Runde gestartet.

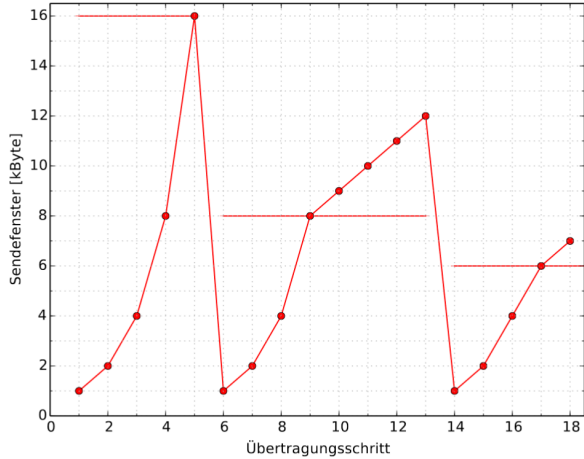
Das ist natürlich realitätsfern, dient hier aber der besseren Darstellung.

AUFGABE 8.2 B)

In Schritt 5 und 13 finden Timeouts statt.



AUFGABE 8.2 B)



AUFGABE 8.2 c)

Aufgabe

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

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?*

Problem:

- Sofortiges Rückfallen auf $cwnd = 1$ ist sehr ineffizient
 - Oft gehen nur vereinzelt Segmente verloren (keine echte Überlast)
- ⇒ TCP-Reno: Zwar auch Reduktion der Datenrate, aber nicht so drastisch

AUFGABE 8.2 c)

Aufgabe

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?

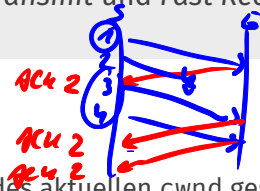
Fast Retransmit:

- Nach dem dritten DUP-ACK:

- ▶ Neuübertragung des fehlenden Segments
 - ▶ ssthresh und cwnd werden auf die Hälfte des aktuellen cwnd gesetzt
- ⇒ kein Rückfall auf cwnd = 1!
- ▶ Rückfall auf cwnd = 1 nur wenn ein Timeout auftritt

- Aber: Bei Reduktion des cwnd sind schon mehr Segmente unterwegs, als dann erlaubt

⇒ Der Sender kann nicht mehr senden bis das ACK des fehlenden Segments eintrifft!



Aufgabe

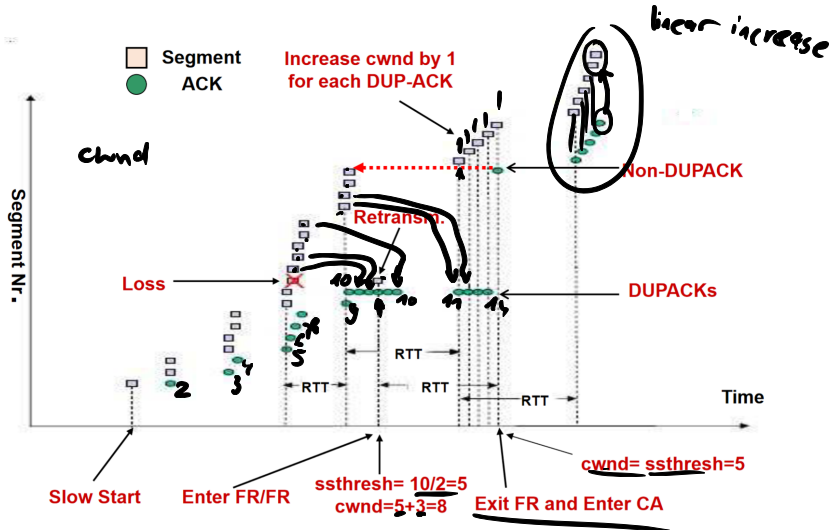
In der Realität werden Slow-Start und Congestion Avoidance nicht alleine eingesetzt. Gängige Erweiterungen sind *Fast Retransmit* und *Fast Recovery*. Welchen Zweck haben diese Erweiterungen?

Deshalb auch noch Fast Recovery:

- Während auf das ACK gewartet wird mit jedem ankommenden DUP-ACK das cwnd um 1 inkrementieren (auch schon für die 3 gerade empfangenen DUP-ACKs)
- Sobald das cwnd groß genug ist, kann für jedes ankommende Segment ein neues geschickt werden

Sobald das erwartete ACK ankommt, $cwnd := ssthresh$ und weiter mit normaler Congestion Avoidance → linear increase

AUFGABE 8.2 C)



AUFGABE 8.3: SICHERHEITSZIELE

AUFGABE 8.3 A)

Aufgabe

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

Aufgabe

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

- **Authentifizierung:** Nachweisen der Identität
- z.B. via Eingabe eines Benutzernames und Password
Dann ist der Benutzer **autorisiert** gewisse Dienste zu nutzen
- Oder ein Server authentifiziert sich beim Client, damit dieser sicher sein kann, das er tatsächlich mit dem gewünschten Server kommuniziert

AUFGABE 8.3 B)

Aufgabe

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

Aufgabe

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

Vertraulichkeit:

- Die Kommunikation ist *geheim*
- Angreifer können also nicht die originale Nachricht aus dem Ciphertext wiederherstellen

Integrität:

- Die übermittelten Daten sind *unverändert*
- Angreifer können die übermittelten also nicht unbemerkt verändern
- Die Kommunikation kann also mitgelesen, aber nicht verändert werden

AUFGABE 8.3 C)

Aufgabe

Ist *Vertraulichkeit* auch ohne *Integrität* möglich? Ist *Integrität* auch ohne *Vertraulichkeit* möglich?

Aufgabe

Ist *Vertraulichkeit* auch ohne *Integrität* möglich? Ist *Integrität* auch ohne *Vertraulichkeit* möglich?

Vertraulichkeit ohne Integrität

- Ja, z.B. wenn verschlüsselte Nachrichten geändert werden, aber nicht ausgelesen werden können
 - z.B. bei AES (ohne CBC, GCM, o.ä.) können einzelne Blöcke sinnvoll ersetzt und getauscht werden (ohne den Inhalt genau zu kennen)
- ⇒ Anständige Verschlüsselungsmethoden verwenden auch immer Integritätsprüfung

Aufgabe

Ist *Vertraulichkeit* auch ohne *Integrität* möglich? Ist *Integrität* auch ohne *Vertraulichkeit* möglich?

Integrität ohne Vertraulichkeit

- Ja, z.B. wenn Nachrichten unverschlüsselt übermittelt werden, aber per MAC (Message Authentication Code) die Integrität sichergestellt wird

Aufgabe

Objekte im Internet (Switches, 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

Objekte im Internet (Switches, 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.

Browser der mit einem Web-Server kommunizieren möchte

- Verschlüsselung, damit niemand die Kommunikation belauschen kann
- Authentifizierung des Servers gegenüber dem Benutzer/Browser, damit sensible Daten nicht an den falschen gehen

Aufgabe

Objekte im Internet (Switches, 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.

Spezieller: Online-Banking

- Zusätzlich auch zwangsläufige Authentifizierung des Benutzer gegenüber dem Server
- Autorisierung beschränkt auf das eigene Konto
- Integritätsprüfung, z.B. damit Überweisungen nicht umgeleitet werden

AUFGABE 8.3 D)

Aufgabe

Objekte im Internet (Switches, 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*.

Zwei Router tauschen Informationen über Nachbarn aus

- Auch andere sollten diese Informationen bekommen → *nicht vertraulich / verschlüsselt*
- Die Routing-Informationen sollten aber korrekt und von vertrauten anderen Routern sein (Authentifizierung, Autorisierung, Integrität)

AUFGABE 8.4: SHIFT CIPHER

AUFGABE 8.4 A)

$k = 7$
FEUR

Alice sendet folgende verschlüsselte Nachricht an Bob:

$c = \text{GSVSREWGLYXDZIVSVHRYRK}$

Sie haben die verschlüsselte Nachricht c mitgehört und möchten diese nun entschlüsseln. Sie wissen, dass Alice einen 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		

Aufgabe

Geben Sie den Schlüssel k an, der zur Verschlüsselung verwendet wurde, und entschlüsseln Sie die Nachricht c .

AUFGABE 8.4 A)

Aufgabe

Geben Sie den Schlüssel k an, der zur Verschlüsselung verwendet wurde, und entschlüsseln Sie die Nachricht c .

Brute-Force:

- Einfach alle möglichen Werte für k durchprobieren
- Das sind nur 25, da $k = 0$ nicht passt
- $k = 1$: FRURQDVFKXWCYHURUGQXQJ
- $k = 2$: EQTQPCUEJWVBXGTQTFPWPI
- $k = 3$: DPSPOBTDIVUAWFSPSEOVH
- $k = 4$: **CORONASCHUTZVERORDNUNG**
- Alle weiteren ergeben nur Murks

AUFGABE 8.4 B)

Aufgabe

Gegeben sei nun die folgende Nachricht:

$c = \text{XC} \underset{\cdot}{\text{Y}} \underset{\cdot}{\text{M}} \text{Y} \text{L} \text{ MUNT BUN } \text{E} \underset{\cdot}{\text{Y}} \underset{\cdot}{\text{C}} \underset{\cdot}{\text{H}} \underset{\cdot}{\text{Y}} \text{ V} \underset{\cdot}{\text{Y}} \underset{\cdot}{\text{M}} \underset{\cdot}{\text{I}} \underset{\cdot}{\text{H}} \underset{\cdot}{\text{X}} \underset{\cdot}{\text{Y}} \underset{\cdot}{\text{L}} \underset{\cdot}{\text{Y}} \text{ V} \underset{\cdot}{\text{Y}} \underset{\cdot}{\text{X}} \underset{\cdot}{\text{Y}} \underset{\cdot}{\text{O}} \underset{\cdot}{\text{N}} \underset{\cdot}{\text{O}} \underset{\cdot}{\text{H}} \underset{\cdot}{\text{.}}$

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* entschlüsseln können. Wie lautet der Schlüssel k ?

AUFGABE 8.4 B)

$c =$ XCMYL MUNT BUN EYCHY VYMIHXYLY VYXYONOH

Einfache Chiffren (wie Ceasar- oder Vigenère-Chiffre) sind sehr anfällig gegen *Dictionary-* oder *Rainbow-Table-Attacks*. Bekannte Wörter (v.a. Passwörter) werden testweise verschlüsselt und verglichen.

AUFGABE 8.4 B)

$c = \text{XC MYL MUNT BUN EYCHY VYMIHXYLY VYXYONOH}$

Alternativ: *Letter frequency analysis*

- Im Deutschen sind die häufigsten Buchstaben etwa:
E: 16.4%, N 9.8%, l: 6.6%, R: 7%, ...
- Y kommt im Cipher am häufigsten vor ($\frac{9}{36} = 25\%$)
- Also könnte Y mit hoher Wahrscheinlichkeit ein E sein
- Schlüssel $k = 25 - 5 = 20$
- Dekodiert: DIESER SATZ HAT KEINE BESONDERE BEDEUTUNG

ÜBUNGSBLATT 8 ABGABEFRIST:
12.07.2021 18:00
LETZTES ÜBUNGSBLATT!

NÄCHSTES TUTORIUM & FRAGESTUNDE:
MITTWOCH 14.07.2021 12:30
(EVENTUELL MIT EINEM 9. TUTORIUMSBLATT)

BITTE FRAGEN ZU ÜBUNGEN UND DER KLAUSUR BIS ZUM 11.07. PER MAIL AN

MATTHIS.FRANZGROTE@RWTH-AACHEN.DE