Übungsblatt 6

1. UDP - Prüfsumme

a) Berechnen Sie die UDP-Prüfsumme, welche sich über die folgenden drei 16Bit-Wörter ergibt:

- 1011 1011 0001 0000
- 1001 1001 0101 1001
- 0101 1011 0101 1001

b) Wie kann der Empfänger feststellen, dass im UDP-Paket ein Fehler aufgetreten ist?
c) Wie werden fehlerhafte Pakete auf der Empfängerseite behandelt?

2. TCP Congestion Window

Es wird eine TCP-Reno-Verbindung betrachtet (mit Fast Recovery), die schon seit einer unbekannten Anzahl x von Transmission-Rounds (Übertragungsrunden) besteht. Der folgende Graph gibt die Größe des variablen Congestion Windows in den Transmission-Rounds x bis x+17 an. Zur Erinnerung: In TCP Reno werden Timeouts anders behandelt als mehrfache ACKs.

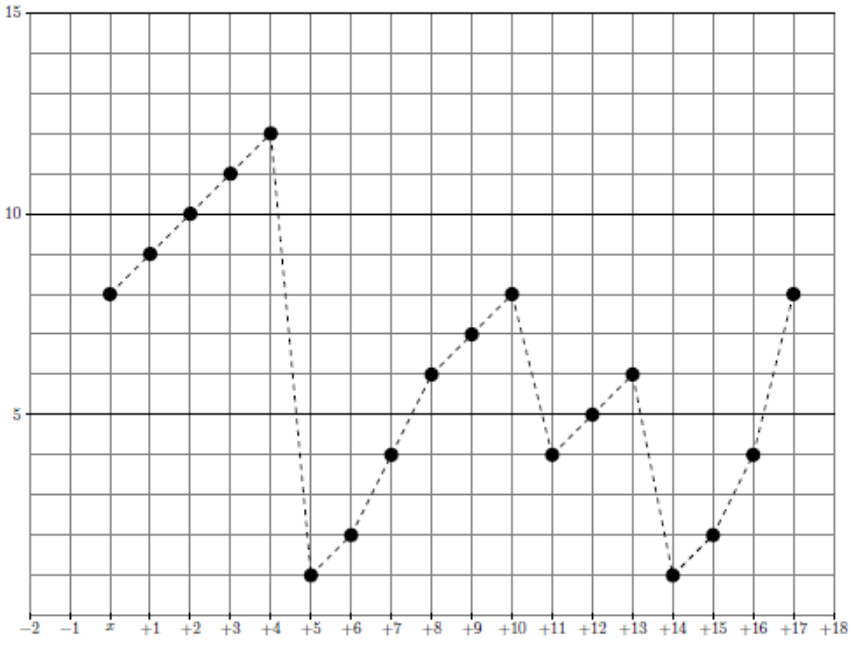

Abbildung 1: TCP-Verlauf

Hinweis: Der Graph enthält einen Fehler (irgendwann nach Übertragungsrunde x+10). Beachten Sie diesen Fehler erst ab Teilaufgabe (e).

Beantworten Sie folgende Fragen:

a) Wurden die Segmentverluste in den Runden x+4, x+10 und x+13 durch Timeouts oder durch mehrfache ACKs erkannt?

b) Welchen Wert hat der Threshold in Runde x+6?
c) Identifizieren Sie alle Zeitintervalle zwischen den Runden x und x+13, in denen TCP Slow-Start aktiv ist.
d) Wie hoch ist der durchschnittliche Datendurchsatz in den Runden x bis einschließlich x+3? Bitte geben Sie auch Ihren Rechenweg an.
e) Der Graph enthält einen Fehler. Lokalisieren und korrigieren Sie diesen direkt in der Grafik bis Runde x+17. Gehen Sie dabei davon aus, dass nach der Runde des Fehlers kein Segmentverlust mehr stattfindet. Sollten Sie den oberen Rand der Grafik erreichen, beenden Sie bitte den Korrekturvorgang.

f) Wie groß ist das Congestion Window in Runde x-1, wenn vor Runde x (seit Beginn der Übertragung) kein Segmentverlust aufgetreten ist, und TCP in Runde x in die Congestion-Avoidance-Phase wechselt?
g) Wie groß ist der Threshold in Runde x-2?
h) Warum ist in Runde x+8 die Größe des cwnd nur 6 und nicht 8?

3. Wireshark

a) Analyse eines Webseiten-Aufrufs mit Wireshark

Rufen Sie eine beliebige Webseite auf, z.B.:

https://www.th-deg.de

Analysieren Sie den Aufruf mit Wireshark und stellen Sie fest, welche Protokolle beteiligt sind. Legen Sie dazu einen Filter fest, der nur Informationen über Ihre eigene IP zulässt. Ihre IP-Adresse finden sie mit dem Befehl ipconfig auf der Komandozeile (cmd).

b) Analyse von Video-Streams

Wir wollen das Verhalten eines typischen Video-Streams analysieren. Rufen Sie eine Internet-Seite mit einem Video als Inhalt (z.B. Youtube) auf und scannen Sie den Verkehr eine Zeit lang.

Zur Trafficanalyse bietet Wireshark eine Übersicht über den aktuellen Netzwerkverkehr. Hilfreich an dieser Stelle ist ein Blick den Wireshark **I/O-Graph** (im Menü Statistiken).

Welches ist die maximale Netzwerkauslastung des Streams?
Wie viele Fehler sind aufgetreten?

Es bestätigt sich die Vermutung wiederkehrender Netzwerkpeaks, die das Netz jeweils nahezu vollständig auslasten. In der Protokollübersicht zeigt sich außerdem, dass dieser Verkehr überwiegend von einer IP-Adresse ausgeht bzw. dahin führt.

Um weiter nach den Ursachen forschen zu können, lässt sich nun ein Filter auf diesen Rechner setzten. Aufschlussreich sind auch die Statistiken, die Wireshark bietet. Unter dem gleichnamigen Menü finden sich unter anderem eine Statistik die mit „**Endpunkte**“,

umschrieben ist.Hier finden sie eine Liste der Kommunikation nach IP-Endgeräten. In dieser Liste ist ersichtlich, dass der Großteil des Datenvolumens von einer IP-Adresse ausgeht bzw. dahin führt. Anhand der IP-Adresse lässt sich nun auch das Gerät ausfindig machen.

c) Auslesen von Zugangsdaten mittels Wireshark

Im Internet gibt es viele Dienste, bei denen der Datenverkehr unverschlüsselt abläuft und somit Benutzerdaten in fremde Hände kommen können. Hier einige Beispiele:

- E-Mail-Abruf über POP3
- Webformulare auf Internet-Seiten
- FTP-Zugang zur Homepage

Deshalb sollten für kritische Daten nur verschlüsselte Protokolle z.B. HTTPS, SFTP usw. verwendet werden.

Zugangsdaten eines FTP-Servers auslesen:
Melden Sie sich an einem FTP-Server an und versuchen Sie die Benutzerdaten auszulesen. Als Beispiel können Sie den Belwue FTP-Server verwenden.

ftp.belwue.de

Geben Sie einen Fantasienamen und Passwort ein. Die Anmeldung wird natürlich fehlschlagen.

Beobachten und analysieren Sie den Netzwerkverkehr der Anmeldung mit Wireshark. Können Sie die Anmeldedaten direkt aus den Datenpaketen ablesen? Verwenden Sie einen Filter für das ftp-Protokoll.

Weitere Informationen zu Wireshark

Wenn Sie sich weiter für Wireshark interessieren, schauen Sie sich die You-Tube-Videos „Introduction to Wireshark (1 bis 3)“ an.

Viel Erfolg !!!