

Messung des Einflusses verschiedener Hintergrundlasten auf die Dienstgüte der Übertragung von Videoströmen mittels TCP

Andrey Kolesnikov und Andreas Gaffron
Arbeitsgruppe Telekommunikation und Rechnernetze
Fachbereich Informatik
Universität Hamburg
Hamburg, Deutschland
kolesnikov@informatik.uni-hamburg.de

Zusammenfassung—Obwohl TCP bekanntlich nicht für die Übertragung von Videoströmen konzipiert wurde und somit diesbezüglich Schwächen besitzt, wird es dennoch häufig zu diesem Zwecke benutzt, weil UDP-Pakete oft zwischen verschiedenen Netzen eingesetzte Adressumsetzer (NAT) oder Firewalls nicht passieren dürfen. Somit wird in dieser Arbeit die Dienstgüte der TCP-Übertragung eines Videostroms bei verschiedenen TCP-Hintergrundlasten untersucht. Unter anderem wurde gemessen, wann es zu Fehlersituationen bei der Videowiedergabe kommt, z.B. aufgrund von zu vielen parallelen Streaming-Sitzungen von verschiedenen Benutzern im WLAN oder nicht ausreichend dimensionierten Puffern im VoD-Client. Die Messumgebung entspricht einem Szenario wie es heutzutage in kleineren Betrieben und vielen privaten Haushalten typischerweise anzutreffen ist.

Schlüsselwörter—TCP, H.264, RTSP, RTP, 802.11g-WLAN, Videostreaming, passive QoS-Messung, Hintergrundlast.

I. EINLEITUNG

Die Übertragungen von Datenströmen aus Sprach- und Videoanwendungen mit Echtzeitanforderungen machen gegenwärtig einen immer größeren Anteil des Netzverkehrs aus. Der Erkenntnis, dass sich TCP für solche Anwendungen wegen seiner Überlastkontrolle und der ggf. dadurch verursachten zu langen Verzögerungen nicht uneingeschränkt eignet, steht die häufige Verwendung dieses Protokolls auch für Echtzeitanwendungen gegenüber. Es wird u.a. in [1] berichtet, dass insgesamt mehr als die Hälfte der Übertragungen des kommerziellen Streaming-Verkehrs über TCP abgewickelt wird.

Ein Grund hierfür dürfte darin liegen, dass Echtzeitanwendungen wie Skype und Windows Media Services TCP verwenden, um restriktive Netzadressumsetzer (Network Address (and Port) Translator, NA(P)T) und Sicherheitseinrichtungen wie Firewalls insbesondere bei Funknetzen [2] zu passieren, welche entsprechenden UDP-Verkehr nicht zulassen. Darüber hinaus ist TCP ein durchgängig verbreitetes und bewährtes Protokoll, das auch anderen TCP-Verbindungen gegenüber wohlwollend (TCP-friendly) ist und dessen Leistungsverhalten relativ genau gesteuert werden kann [1, 3].

Folglich gibt es hier zwei Forschungsrichtungen: Einerseits werden alternative Protokolle entwickelt [4, 5, 6, 7], andererseits wird die Übertragung von Datenströmen mit TCP auch künftig untersucht, um die vorhandenen Vorzüge von TCP auch weiterhin zu nutzen und die Schwächen gewisser Übertragungen mit TCP genau zu lokalisieren, zu quantifizieren und sie soweit wie möglich zu beheben. Diesen letztgenannten Zielen ist auch der vorliegende Beitrag verpflichtet, der sich ein zu untersuchendes Netzszenario ausgewählt hat, wie es heute in vielen privaten Haushalten und kleineren Betrieben zur Übertragung von Videoströmen u.a. von solchen Anwendungen wie Video-on-Demand (VoD), Videokonferenzen oder IPTV genutzt wird.

Im folgenden Abschnitt II wird zunächst die Messumgebung detailliert beschrieben und anschließend in Abschnitt III die Vorgehensweise bei der Durchführung von Messungen erläutert. In Abschnitt IV werden die Messergebnisse vorgestellt und interpretiert. Eine Zusammenfassung der Resultate und ein Ausblick in Abschnitt V schließen den vorliegenden Beitrag ab.

II. MESSUMGEBUNG

Für die durchgeführten Messungen wurde ein Netzszenario im Labor nachgestellt, wie es heutzutage in kleineren Betrieben und vielen privaten Haushalten typischerweise vorzufinden ist (Home Area Network, HAN [8]). Das Fallstudienetz besteht aus einem Vollduplex-Fast-Ethernet-Segment und einem WLAN-Segment, die mit einem Fast-Ethernet-Switch und einer WLAN-Basisstation (WLAN Access-Point, AP) miteinander gekoppelt sind (vgl. Abb. 1). Dabei soll der Rechner VoD-Server in unserem Szenario einen Videoserver des IPTV-Diensteanbieters modellieren und der Rechner Lastgenerator sorgt für die Erzeugung von zusätzlichen TCP-basierten Hintergrundlasten von hypothetischen externen Lastquellen wie z.B. FTP-, HTTP-, POP3- oder auch weiteren VoD- oder IPTV-Servern. Im WLAN-

Segment stellt der Rechner VoD-Client den Empfänger des Videostroms dar, z.B. ein Benutzer-Notebook mit geeigneter Abspielsoftware bzw. eine Streaming-Box, die an das Fernsehgerät angeschlossen ist. Der Rechner Lastsenke wird stellvertretend für weitere Endgeräte im Haushalt bzw. Büro verwendet, die mit dem AP assoziiert sind und Datenströme von hypothetischen externen Servern (modelliert durch den Lastgenerator) erhalten, die aus der Sicht des beobachteten Videostroms eine Hintergrundlast darstellen. Für die Erzeugung der Hintergrundlast wird das Werkzeug UNILOG (Unified Load Generator [9, 10, 11]) verwendet, welches an der Arbeitsgruppe TKRN von einem der Autoren dieses Beitrags hauptverantwortlich entwickelt wurde. Die aus einem oder mehreren TCP-Strömen mit konstanter Datenrate (CBR) bestehende Hintergrundlast wird von dem Rechner Lastgenerator injiziert und zur Lastsenke übertragen.

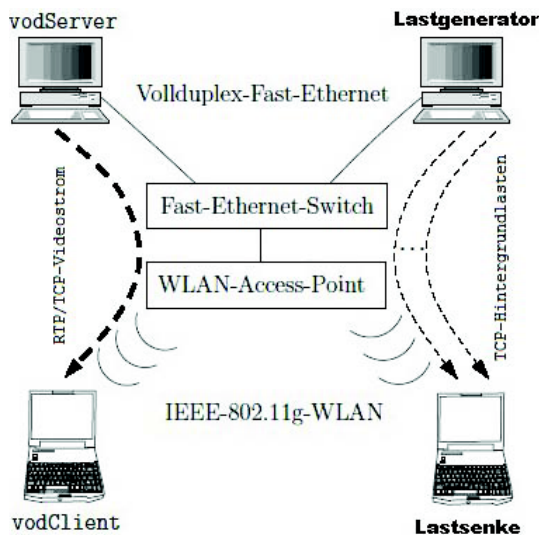


Abbildung 1: Aufbau des Fallstudienetzwerks.

Bei den in der Fallstudie verwendeten PCs handelt es sich um herkömmliche Geräte mit Intel Core 2 Prozessor unter dem Betriebssystem Windows XP Professional. Dabei sind der VoD-Server und der Lastgenerator etwas leistungsschwächer mit 2,13 GHz Prozessortakt und einem Hauptspeicher von 1 GB sowie mit einem Broadcom 57xx Gigabit Ethernet-Controller ausgestattet, während der VoD-Client und die Lastsenke jeweils über 3,25 GB Hauptspeicher und mit 2,83 GHz getaktete Quad Prozessoren sowie einen X-Micro 802.11g-WLAN USB-Stick verfügen. Der VoD-Client empfängt vom VoD-Server den H.264/AVC-codierten Videostrom und den MPEG-4-codierten Audiostrom in einem MPEG-II Transportstrom über den WLAN-Access-Point (DWL-2100AP der Firma D-Link, gemäß IEEE-802.11g mit 54 Mbit/s) und den damit im Voll duplex-Modus verbundenen Fast-Ethernet-Switch (DGS-1008D der Firma D-Link). Der Lastgenerator erzeugt eine künstliche Hintergrundlast in Form von TCP-Paketen, welche parallel zum Videostrom ebenfalls über das Funknetz, jedoch zur Lastsenke übertragen wird. Dadurch entsteht eine Konkurrenzsituation zwischen dem VoD-Client

und der Lastsenke beim Zugriff auf das gemeinsam genutzte WLAN-Funknetz. Die Lastsenke ist insofern nur passiv als sie lediglich TCP-Daten empfängt und Quittungen in Form von TCP-ACKs zurücksendet. Um das Problem nicht wahrnehmbarer Endgeräte (Hidden Station) zu vermeiden, wurden der VoD-Client und die Lastsenke in einem Abstand von vier Metern aufgestellt mit der dazwischen befindlichen WLAN-Basisstation, so dass zwischen allen Stationen im WLAN eine Sichtverbindung besteht. Somit konnte sowohl auf der Basisstation als auch auf den PCs der RTS/CTS-Mechanismus deaktiviert werden.

Auf den einzelnen an den Messexperimenten beteiligten PCs wird folgende Software benutzt. Der den Videostrom erzeugende VoD-Server nutzt den LIVE555 Media Server [12], der Videostrome zum Streaming über RTSP anbietet und für den Transport von RTP-Daten nicht nur UDP, sondern auch TCP verwenden kann. Der VoD-Client verwendet den VLC Media Player [13], der so vorkonfiguriert wurde, dass der Videostrom vom LIVE555 Media Server über TCP angefragt wird. Der Abspielpuffer in VLC wurde so eingestellt, dass der VoD-Client die Videodaten für drei Sekunden speichert, bevor er mit deren Abspielen beginnt. Ferner wurde im VoD-Client die WinDump-Software [14] installiert, welche für die Erfassung und Speicherung des entstehenden Verkehrs in Form von einzelnen PCAP-Dateien pro Messexperiment verwendet wurde.

Die von UNILOG erzeugten TCP-Hintergrundlastströme bestehen aus TCP-Segmenten mit einer TCP-Nutzdatenlänge von 1460 Byte, die in allen Messexperimenten gleich bleibt. Die Zwischenankunftszeiten der Datenversendeaufträge an TCP werden so gewählt, dass jeweils TCP-Datenströme mit einem gewünschten TCP-Datendurchsatz von 0,5 Mbit/s bis hin zu 16 Mbit/s entstehen (s. Tabelle 1).

TABELLE 1: TCP-DATENDURCHSATZ D (IN [MBIT/S]) UND PAKET-ZWISCHENANKUNFTSZEITEN ZAZ (IN [MS]) DER HINTERGRUNDLASTEN

D	0,5	1	2	4	8	10	12	16
ZAZ	23,3	11,7	5,8	2,9	1,46	1,168	0,977	0,73

Für den zu übertragenden Videostrom wurde der frei verfügbare Animationsfilm Big Buck Bunny des Peach-Open-Movie-Projekts [15] in der HD-Version benutzt. Dieser Kurzfilm dauert 9 Minuten und 56 Sekunden, besitzt eine Bildwiederholfrequenz von 24 Hz und besteht aus 14314 Einzelbildern zu je 1280x720 Pixeln. Dies ergibt nach der Codierung gemäß H.264/AVC bzw. MPEG-4 für den Audioteil eine Datei mit einer Dateigröße von 421 MB. Zwischen dem Originalfilm und der komprimierten Version sind beim Abspielen nahezu keine Unterschiede zu erkennen. Bei der Übertragung des Videofilms im Fallstudienetz ohne Hintergrundlast wurden beim VoD-Server ca. 310.668 RTP-Pakete erfasst.

III. DURCHFÜHRUNG DER MESSUNGEN

Die Qualität der Videübertragung wird in dieser Fallstudie mithilfe von passiven Messungen ermittelt, wofür

der im VoD-Client eintreffende RTP/TCP-Verkehrsstrom mithilfe von WinDump im PCAP-Format aufgezeichnet und anschließend mithilfe des kommandozeilenorientierten Protokollanalytators TShark [16] untersucht wird. Somit sind keine Änderungen an der in dem VoD-Client und VoD-Server installierten Software erforderlich und man erhält objektive, quantitative Qualitätsmaße aus der RTP-Schicht (bzw. bei Bedarf aus der TCP- sowie IP-Schicht), welche die vom Betrachter wahrgenommene Filmqualität beeinflussen. Die Fallstudie verwendet folgende Maße zur Bestimmung der Qualität der Videoübertragung:

IP-Durchsatz: der Durchsatz auf IP-Ebene gibt an, welche Datenmenge (inklusive des IP-Headers) der VoD-Client während einer Streamingsitzung vom Server (in Form von TCP-Segmenten) empfangen und zu ihm (z.B. in Form von Quittungen als TCP-ACKs) gesendet hat.

Sequenzfehleranzahl: ein Sequenzfehler in der RTP-Schicht liegt vor, wenn ein RTP-Paket beim VoD-Client ankommt und seine Sequenznummer nicht dem Inkrement der Sequenznummer des zuletzt empfangenen RTP-Pakets entspricht.

Paketverlust: der VoD-Client meldet in den Receiver-Reports (RR) in regelmäßigen Abständen die Anzahl der RTP-Pakete, die er erwartet, jedoch nicht erhalten hat (RFC 3550).

Jitter: ist ein Maß für die Schwankung der Zwischenankunftszeiten der Pakete beim Empfänger und wird als mittlere Abweichung der Differenz zwischen den Paketabständen bei dem Empfänger und dem Sender gemäß RFC 3550 fortlaufend berechnet. Der VoD-Client fügt den jeweils aktuellen Jitterwert in seine Receiver Reports ein. Für diese Fallstudie soll der Median aller Jitterwerte aus den Receiver Reports den mittleren Jitter einer Streamingsitzung angeben.

Duplikatenanzahl: hierbei handelt es sich um TCP-Segmente, die der VoD-Client mehrfach erhalten hat. Dies kann passieren, wenn z.B. der VoD-Client einen WLAN-Rahmen mit einem TCP-Segment erhält und die entsprechende WLAN-Bestätigung vom VoD-Client den AP nicht erreicht. Der AP würde folglich denselben WLAN-Rahmen nach Ablauf eines Timers erneut aussenden, so dass beim VoD-Client ein TCP-Duplikat entsteht, welches von TCP verworfen wird. In der RTP-Schicht des VoD-Clients entstehen somit keine RTP-Duplikate. Die Anzahl der TCP-Duplikate liefert ebenfalls ein Maß für die Auslastung des WLANs und damit ein indirektes Maß für die wahrgenommene Qualität des Videofilms.

In einem Messerperiment besteht die Hintergrundlast aus einer festen Anzahl an TCP-Strömen, wobei für jeden TCP-Strom derselbe angestrebte TCP-Datendurchsatz vorgegeben wird. In einer Serie von Experimenten wird die Anzahl der TCP-Ströme konstant gehalten, während ihr vorgegebener Datendurchsatz von Experiment zu Experiment verändert wird. Um sicherzustellen, dass die Rahmenbedingungen im

WLAN für alle Experimente annähernd gleich sind, wird vor dem Start jedes Experiments der Durchsatz einer TCP-Übertragung vom VoD-Client zum Lastgenerator mithilfe des Iperf-Werkzeugs [17] 5 Sekunden lang gemessen und das Experiment nur dann weiter ausgeführt, wenn der gemessene TCP-Durchsatz über dem Schwellenwert von 20 Mbit/s liegt. Um statistisch signifikante, aussagekräftige Resultate zu bekommen, wird jedes Experiment fünfmal wiederholt und Mittelwerte sowie die Standardabweichung für die Werte der Qualitätsmaße ermittelt. Wegen der hohen Anzahl der Experimente (ca. 400 Stück) wurde die Durchführung der gesamten Fallstudie einschließlich der Fernsteuerung des UNILOG-Lastgenerators und des VLC-Players, der Paketaufzeichnung mit WinDump, der Protokollanalyse mit TShark und schließlich der Ermittlung von Werten der Qualitätsmaße mithilfe von selbstentwickelten Python-Skripts komplett automatisiert.

IV. MESSERGEBNISSE

Bei der Interpretation der Messergebnisse muss die für TCP-Übertragungen nutzbare Übertragungskapazität im WLAN berücksichtigt werden. Für das verwendete IEEE 802.11g WLAN mit OFDM-Modulationsverfahren und 54 Mbit/s (Brutto-)Datenrate ergibt sich eine nutzbare Übertragungskapazität von ca. 24,4 Mbit/s (errechnet als maximal erzielbare Nettodatenrate einer TCP-Übertragung bei TCP-Nutzdatenlänge von 1460 Byte, wobei die Übertragungszeiten für TCP- und MAC-Bestätigungen berücksichtigt und der zusätzliche Overhead durch die Beacon-Rahmen und Backoff-Wartezeiten beim Medienzugriff nicht einkalkuliert wird, vgl. [18], Abschnitt 8.6). Die tatsächlich erzielte Nettodatenrate kann weit unter diesem Wert liegen, da es z.B. zu Kollisionen zwischen den einzelnen WLAN-Stationen beim Medienzugriff kommen kann.

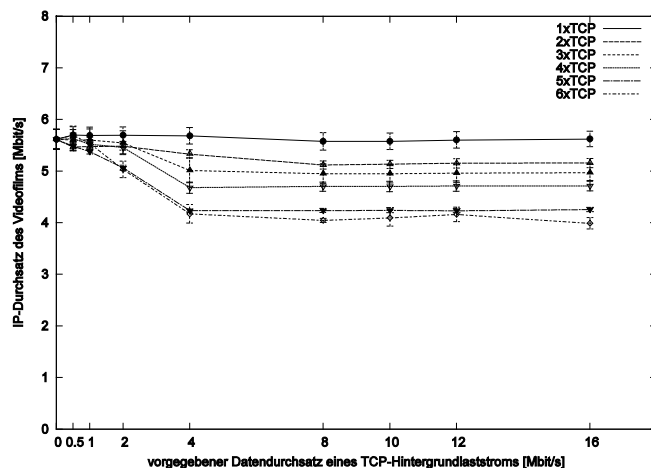


Abbildung 2: IP-Durchsatz des Videofilms unter mehreren verschiedenen TCP-Hintergrundlasten mit 95%-Konfidenzintervallen.

Beim Streaming des Videofilms im Fallstudienetz ohne Hintergrundlast liegt der mittlere IP-Durchsatz des Videofilms auf der Seite des VoD-Clients (ermittelt mit einem Messinter-

vall von 1 Sekunde) nicht über 5,7 Mbit/s (vgl. Abb. 2), wobei Filmstellen mit starken Bewegungen existieren, die in den einzelnen Messintervallen einen Durchsatz von bis zu ca. 18,7 Mbit/s erzeugten. Wenn die Hintergrundlast aus einem einzigen TCP-Strom besteht, ist die Übertragungskapazität des Funkkanals ausreichend und die Durchsatzwerte des Videostroms sind alle nahezu identisch und betragen ca. 5,7 Mbit/s. Bei zwei TCP-Hintergrundlastströmen mit einem angestrebten Datendurchsatz von jeweils 8 Mbit/s sinkt der Durchsatz des Films auf ca. 5,1 Mbit/s. Bei drei TCP-Hintergrundlasten wird die Übertragungskapazität der Funkstrecke bereits bei Vorgabe eines angestrebten Durchsatzes von jeweils 4 Mbit/s erreicht und der Durchsatz des Films reduziert sich auf ca. 5 Mbit/s. Eine weitere Erhöhung des angestrebten Durchsatzes der Hintergrundlasten bringt keine Verminderung des Filmdurchsatzes mit sich, da die Übertragungskapazität der Funkstrecke zwischen den drei Hintergrundlastströmen und dem Videostrom geteilt wird. Bei fünf Hintergrundlasten mit jeweils 2 Mbit/s ist der Videodurchsatz von 5,06 Mbit/s subjektiv noch akzeptabel. Bei Vorgabe eines Durchsatzes von 4 Mbit/s für die Hintergrundlasten sinkt der Filmdurchsatz auf ca. 4,2 Mbit/s und die Bildqualität ist für den Betrachter nicht mehr akzeptabel.

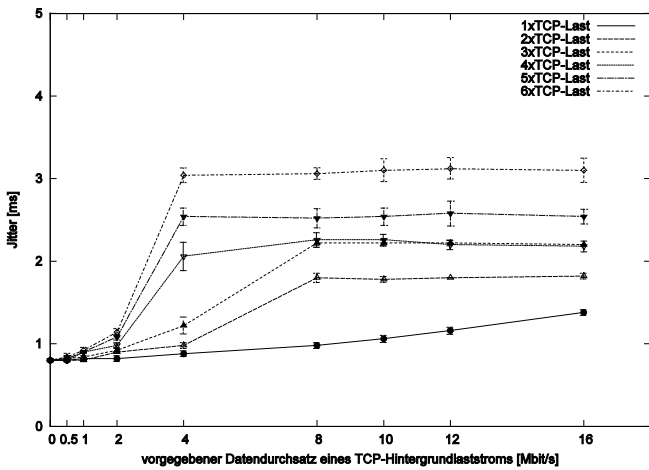


Abbildung 3: Mittlerer Jitter des Videostroms unter mehreren verschiedenen TCP-Hintergrundlasten mit 95%-Konfidenzintervallen.

Ohne Hintergrundlast wird ein Jitterwert von 0,8 ms gemessen (vgl. Abb. 3). Bei einer einzigen Hintergrundlast steigen die Jitterwerte auf maximal 1,3 ms an. Anhand der Jitterwerte lässt es sich gut beurteilen, ab welcher Hintergrundlast die Bildqualität nicht mehr akzeptabel ist. Sobald der Jitterwert über 2 ms liegt, sind die Verzögerungsschwankungen so stark, dass die Abspielqualität des Videofilms inakzeptabel wird. Dieser Wert wird bei drei Hintergrundlasten mit vorgegebenem Durchsatz von 8 Mbit/s erreicht und bei vier Hintergrundlasten bereits bei einem Durchsatz von 4 Mbit/s. Bei Vorliegen von mehr als einer Hintergrundlast kann in der Abb. 3 abgelesen werden, dass ab einem bestimmten vorgegebenen Durchsatz der Hintergrundlasten (z.B. ab 8 Mbit/s bei drei Hintergrundlasten) die Jitterwerte des Videostroms nicht mehr ansteigen.

Bei der Untersuchung der als PCAP-Dateien aufgezeichneten RTP-Sitzungen zwecks Ermittlung der RTP-Sequenzfehleranzahl ist aufgefallen, dass vereinzelt (für weniger als 0,01% der RTP-Pakete) Verluste von TCP-Segmenten noch vor der Übertragung im WLAN (also vermutlich aufgrund eines Überlaufs im Eingangspuffer des APs) aufgetreten sind. In diesen Fällen musste das verlorene TCP-Segment vom VoD-Server erneut angefordert werden. Dies verhinderte zwar einen Sequenzfehler in der RTP-Schicht, führte aber dazu, dass beim Eintreffen des wiederholten TCP-Segments im VoD-Client die Deadline des enthaltenen RTP-Pakets sowie der RTP-Pakete aus den im TCP-Puffer zwischengespeicherten TCP-Segmenten überschritten wurde und deutlich merkbare Bildfehler entstanden.

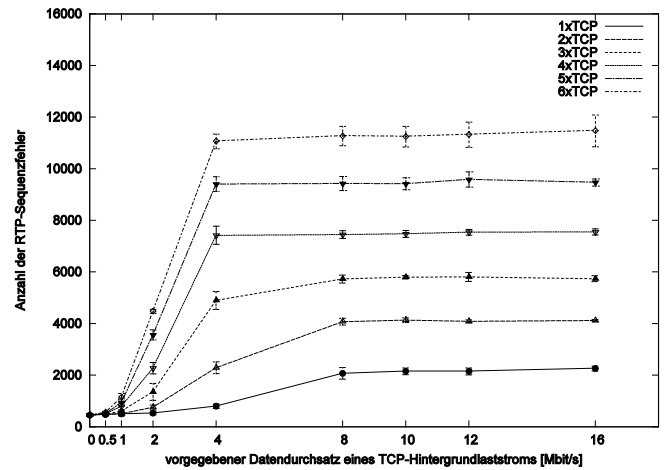


Abbildung 4: Anzahl der RTP-Sequenzfehler unter mehreren verschiedenen TCP-Hintergrundlasten mit 95%-Konfidenzintervallen.

Bei der Erhöhung des vorgegebenen Durchsatzes bzw. der Anzahl von Hintergrundlasten ließ sich ein deutlicher Anstieg der RTP-Sequenzfehler beobachten (vgl. Abb. 4). Dies war auf den ersten Blick etwas überraschend, da die Ende-zu-Ende-Fehlerkontrolle von TCP Paketverluste beheben sollte und somit keine RTP-Sequenzfehler zu erwarten waren. Allerdings erhält der VoD-Server in den Receiver Reports des VoD-Clients regelmäßig (i.d.R. alle 5 Sekunden) die aktuellen Jitter- und Verlustwerte sowie Zeitstempel für die RTT-Abschätzung und hat somit die Möglichkeit, seine Datenrate den Netzbedingungen dynamisch anzupassen. In unserem Streamingszenario wurde das Filmmaterial im Voraus als MPEG-II Transportstrom verpackt und der VoD-Server (LIVE555 Media Server) ließ bei steigender RTT einige RTP-Rahmen offensichtlich einfach aus, so dass in der RTP-Schicht beim VoD-Client RTP-Sequenzfehler registriert wurden. Das Auslassen der RTP-Rahmen durch den VoD-Server lässt sich auch an der Größe der entstehenden PCAP-Datei während der Aufzeichnung der RTP-Sitzung mit WinDump erkennen. Beim Streaming des Films ohne Hintergrundlast entstand ca. 450 MB große PCAP-Datei, während z.B. bei drei Hintergrundlasten mit 4 Mbit/s ca. 387 MB und bei vier Hintergrundlasten mit 4 Mbit/s nur noch ca. 360 MB aufgezeichnet wurden.

Aus der Abbildung 5 ist ersichtlich, dass auch bei der Übertragung des Videofilms ohne Hintergrundlast ca. 11.000 RTP-Pakete in dem letzten Receiver Report (RR) des Videostroms als verloren gemeldet werden. Diese RTP-Pakete überschreiten ihre Abspieffrist und werden demnach von dem Demuxer in der RTP-Schicht des VoD-Clients verworfen. Andererseits werden durch die H.264-Videocodierung Bildfehler reduziert, so dass beim Betrachten des Films ohne Hintergrundlast keine oder wenige Fehler zu sehen sind.

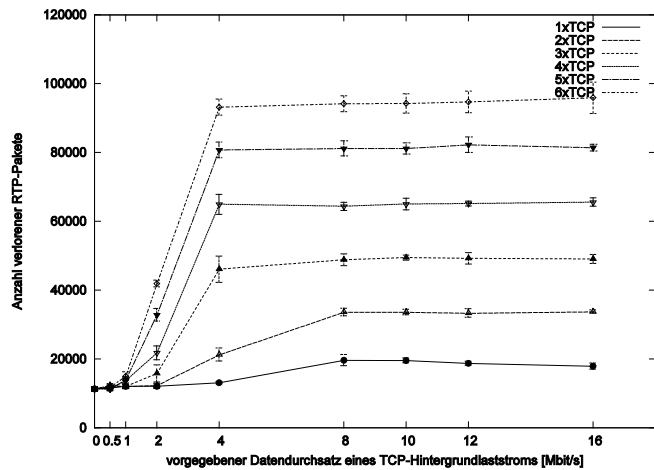


Abbildung 5: Anzahl verllorener RTP-Pakete unter mehreren verschiedenen TCP-Hintergrundlasten mit 95%-Konfidenzintervallen.

Die Anzahl der RTP-Paketverluste steigt rapide an, wenn mehr als drei Hintergrundlasten anliegen. So werden bei fünf Hintergrundlasten mit einem vorgegebenen Durchsatz von 2 Mbit/s ca. 30.000 RTP-Pakete als verloren gemeldet. Analog zu den bisherigen Beobachtungen kann angemerkt werden, dass ab einem bestimmten vorgegebenen Durchsatz der Hintergrundlasten sich die Anzahl der verlorenen Pakete in der Versuchsreihe nicht mehr weiter erhöht. Das Maximum der RTP-Paketverluste in einer Versuchsreihe wird bei einer Hintergrundlast mit 8 Mbit/s und bei drei Hintergrundlasten bereits mit 4 Mbit/s erreicht (vgl. Abb. 5).

Abschließend soll noch der Verlauf der Anzahl der TCP-Segmentduplikate diskutiert werden, der in Abb. 6 exemplarisch für eine TCP-Hintergrundlast dargestellt ist. TCP-Duplikate konnten in den Paketmitschnitten der RTP-Sitzungen beobachtet werden, da die Paketerfassung mit WinDump direkt auf Ethernet-Ebene, also noch vor der Verarbeitung durch IP und TCP erfolgt.

TCP-Duplikate entstanden hauptsächlich im WLAN-Segment des Fallstudienetzes, wenn ein WLAN-Rahmen mit einem TCP-Segment im VoD-Client empfangen wurde und die entsprechende WLAN-Bestätigung vom VoD-Client an den AP auf der Funkstrecke verloren ging, so dass der AP nach Ablauf eines Timers denselben WLAN-Rahmen erneut aus-senden musste. In der RTP-Schicht des VoD-Clients entstanden dadurch keine RTP-Duplikate, da die doppelten TCP-Segmente bereits von TCP verworfen wurden. Anzumerken ist

eine relativ geringe Anzahl und eine sehr starke Streuung der Paketduplikate (man beachte die Größe der 95%-Konfidenzintervalle in Abb. 6, wobei sich ein Anstieg der Paketduplikate mit steigender Hintergrundlast trotzdem beobachten lässt). Die starke Streuung der Paketduplikate kann u.a. auf den sporadischen Einfluss anderer Funknetze in der Umgebung des Fallstudienetzes zurückgeführt werden, welche ggf. denselben bzw. einen benachbarten Kanal benutzen.

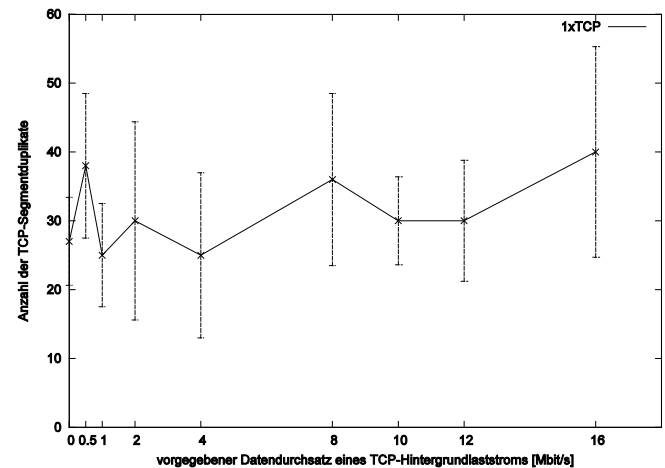


Abbildung 6: Anzahl der TCP-Segmentduplikate unter mehreren verschiedenen TCP-Hintergrundlasten mit 95%-Konfidenzintervallen.

V. ZUSAMMENFASSUNG UND AUSBLICK

In diesem Beitrag wurden Auswirkungen verschiedener TCP-Hintergrundlasten auf die Übertragungsqualität eines H.264-codierten Videofilms quantitativ anhand von QoS-Parametern wie IP-Durchsatz, Jitter, Anzahl der Sequenzfehler, Paketverluste und Paketduplikate untersucht. Die Auswertung der Messergebnisse hat gezeigt, dass auch bei Streaming des ausgewählten Animationsfilms ohne Hintergrundlast Bildfehler entstehen, da manche RTP-Pakete nicht rechtzeitig ankommen und vom VoD-Client verworfen werden. Ein Großteil der Bildfehler wird allerdings durch die H.264-Videocodierung ausgeglichen, sodass bei der Wiedergabe des Videofilms die einzelnen Bildfehler kaum auffallen.

Bei Vorliegen von Hintergrundlast wird die Übertragungskapazität im WLAN von den einzelnen TCP-Hintergrundlastströmen und dem beobachteten RTP/TCP-Videostrom geteilt. Spätestens bei vier Hintergrundlastströmen mit jeweils 4 Mbit/s ist die nutzbare Übertragungskapazität der Funkstrecke ausgeschöpft und die Werte der betrachteten QoS-Parameter des RTP/TCP-Videostroms (IP-Durchsatz, Jitter, Sequenzfehler, Paketverluste sowie Paketduplikate) verändern sich bei weiterer Erhöhung der Datenraten der Hintergrundlastströme kaum mehr. Infolge der steigenden Hintergrundlast im WLAN erhöhen sich die Anzahl der RTP-Paketverluste und die geschätzten Werte der RTT im gesamten Fallstudienetz. Der VoD-Server wird darüber mithilfe von Receiver Reports des VoD-Clients informiert und kann seine Datenrate den

Netzbedingungen dynamisch anpassen. Der in dieser Fallstudie verwendete VoD-Server LIVE555 Media Server ließ in solchen Fällen eine bestimmte Anzahl an RTP-Rahmen aus. Dies führte zu Sequenzfehlern in dem beobachteten RTP-Strom und bei erhöhter Anzahl ausgelassener RTP-Rahmen zu irreparablen Bildfehlern bei der Videowiedergabe.

Insgesamt lässt sich festhalten, dass obwohl Video-streaming an sich eine ziemlich robuste Anwendung darstellt, es trotzdem aber sehr schnell zu Fehlersituationen bei der Videowiedergabe kommen kann, z.B. bei nicht ausreichend dimensionierten Puffern in dem VoD-Client, zu vielen parallelen RTSP-Sitzungen von verschiedenen Benutzern im WLAN oder Belastung der Upload-Leitung zum ISP durch das Hochladen einer großen Datei, wodurch die Übertragung von TCP-Bestätigungen zum VoD-Server ggf. verlangsamt wird.

Bei der Wahl eines Protokolls für den Transport von VoD-Strömen aus der Sicht des Content-Providers ist zu berücksichtigen, dass viele ISPs den UDP-Verkehr anderer Provider insbesondere bei Multicast ins eigene Netz nicht hereinlassen dürfen, um den dortigen TCP-Verkehr nicht zu beeinträchtigen. Solange sich also der avisierte Empfänger des Videostroms im Netz desselben ISPs befindet, kann der Videostrom über UDP als Unicast bzw. als Multicast bereitgestellt werden, wie dies i.d.R. von IPTV-Diensteanbietern auch vorgenommen wird. Soll der Videostrom auch den Empfängern außerhalb des eigenen Netzes angeboten werden, ist also ggf. TCP das Transportprotokoll der Wahl, welches auch den Vorteil der einfachen Firewall-Konfiguration bei dem Empfänger mit sich bringt. In beiden Fällen könnten noch zusätzliche Maßnahmen auf der Providerseite ergriffen werden, um die Abspielqualität der angebotenen Ströme zu verbessern, wie z.B. die Transkodierung des Films zur Begrenzung der für die Videoübertragung erforderlichen Datenrate (und damit verbundener Vermeidung kurzfristiger Lastspitzen) sowie die Reservierung einer festen Übertragungskapazität für die Videoübertragung, wie dies von den Anbietern der IPTV-Dienste aktuell gelöst wird.

Bei dem vorliegenden Beitrag handelt es sich um einen Bericht aus einem laufenden Projekt. In weiteren Experimenten werden wir parallel zu den Verkehrsmessungen auch die Bildqualität des übertragenen und dabei ggf. gestörten Videos mithilfe von Metriken wie PSNR (engl. Peak Signal-to-Noise Ratio) oder SSIM (engl. Structural Similarity) vergleichen und nach Zusammenhängen zwischen den resultierenden Werten für Bildqualität und gemessenen Paketdaten suchen. Hier wäre es interessant, unsere Messungen in Zusammenhang mit analytischen Modellen für Multimedia-Streaming über TCP (vgl. z.B. [19]) zu setzen. Ferner sind Experimentserien mit anderen Typen von Hintergrundlast wie z.B. VBR-Strömen oder burstartigem Verkehr geplant, wozu UNILOG entsprechend vielfältige Möglichkeiten bereitstellt.

Ein sehr interessantes Szenario für eine anschließende Fallstudie wäre die Untersuchung der Übertragungsqualität

sowie die Analyse der Blockierungswahrscheinlichkeit [20] von IPTV-Datenströmen, wobei der Lastgenerator UNILOG in Verbindung mit einem entsprechenden noch zu entwickelnden IPTV-Modell für die Generierung von zusätzlichen IPTV-Kanälen als Hintergrundlast zum Einsatz kommen kann.

LITERATUR

- [1] G. Eason, E. Brosh, S.A. Baste, V. Misra, D. Rubenstein, H. Schulzrinne, The Delay-Friendliness of TCP for Real-Time Traffic, *IEEE / ACM Transactions on Networking*, Vol. 18, No. 5, pp. 1478-1491, 2010.
- [2] L. Mäkinen, J.K. Nurminen, Measurement on the Feasibility of TCP NAT Traversal in Cellular Networks, in *Proc. of the Next Generation Internet Networks*, Krakow, April 7, 2008, pp. 261-267.
- [3] H. Luo, S. Ci, D. Wu, H. Tang, End-to-end optimized TCP-friendly rate control for real-time video streaming over wireless multi-hop networks, *Journal on Visual Communication and Image Representation*, Vol. 21, No. 2, pp. 98-106, 2010.
- [4] New Streaming Protocol for IPTV Enables High-Quality Live Transmissions, <http://www.pr.com/press-release/301895> (31.05.11).
- [5] E. Kohler, M. Handley, S. Floyd, Designing DCCP: Congestion control without reliability, in *Proc. of the ACM SIGCOMM'06*, Pisa, Italy, pp. 27-38, 2006.
- [6] T. Dreibholz, E.P. Rathgeb, I. Rüngeler, R. Seggelmann, M. Tüxen, R.R. Stewart, Stream Control Transmission Protocol: Past, Current, and Future Standardization Activities, *IEEE Communications Magazine*, Vol. 49, No. 4, pp. 82-88, 2011.
- [7] A. Fey, Optimierung von TPC für Videokommunikation, VDM Verlag Dr. Müller, 2007 (als Buch veröffentlichte Diplomarbeit, Untersuchung selbst abgeleiteter TCP-Varianten zur Videokommunikation, Fachbereich Informatik, Universität Hamburg, 2006).
- [8] R. Gaudino, D. Cardenas, M. Bellec, B. Charbonnier, N. Evanno, P. Guignard, S. Meyer, A. Pizzina, I. Mollers, D. Jager, Perspective in next-generation home networks: Toward optical solutions?, *IEEE Communications Magazine*, Vol. 48, No. 2, pp. 39-47, 2010.
- [9] A. Kolesnikov, Konzeption und Entwicklung eines echtzeitfähigen Lastgenerators für Multimedia-Verkehrsströme in IP-basierten Rechnernetzen, *Echtzeit 2008*, Boppard, 27. - 28. November, pp. 91-100, 2008.
- [10] A. Kolesnikov, M. Kulas, Lastgenerierung an IP-Schnittstellen mit dem UniLoG.IP-Adapter, *Zeitschrift Praxis der Informationsverarbeitung und Kommunikation (PIK)*, Vol. 33, Heft 2, pp. 130-139, 2010 (s. auch *MMBnet'09*, Wolfinger B.E., Heidtmann K. (Hrsg.), Hamburg, 2009).
- [11] A. Kolesnikov, M. Kulas, Load Modeling and Generation for IP-based Networks: A Unified Approach and Tool Support, 15th Intern. GI/ITG Conf. on "Measurement, Modelling and Evaluation of Computing Systems" and "Dependability and Fault Tolerance", *MMB & DFT*, Essen, pp. 91-106, 2010.
- [12] LIVE555MediaServer, <http://www.live555.com/mediaServer> (31.05.11)
- [13] VLC media player, <http://www.videolan.org> (31.05.11)
- [14] WinDump, <http://www.winpcap.org/windump/default.htm> (31.05.11)
- [15] Big Buck Bunny - Kurzfilm, <http://www.bigbuckbunny.org> (31.05.11)
- [16] TShark: Terminal-based Wireshark, http://www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.html (31.05.11)
- [17] Iperf, <http://www.nwlab.net/art/iperf/> (31.05.11)
- [18] J. Rech, *Wireless LANs, 802.11-WLAN-Technologie und praktische Umsetzung im Detail*, Heise, 3. Auflage, 2008.
- [19] B. Wang, J. Kurose, P. Shenoy, D. Towsley, Multimedia Streaming via TCP: An Analytic Performance Study, *ACM Trans. on Transactions on Multimedia Computing, Communications, and Applications*, Vol. 4, No. 2, 2008, pp. 16.2-16.22.
- [20] J. Lai, B.E. Wolfinger, S. Heckmüller, Decreasing Call Blocking Probability of Broadband Services in Networks with Tree Topology, in *Proc. of SPECTS 2011*, June 27 - 30, 2011, Den Haag, Netherlands.