Sichere und qualitativ hochwertige

Voice over IP Anwendung

Es ist der klare Trend zu erkennen, dass Voice over IP (VoIP) immer stärker auch über das Internet genutzt wird. Dabei ist die Vertraulichkeit ein wichtiger Aspekt für den Erfolg dieses neuen Angebots. Die Frage in diesem Kontext lautet: „Wie kann verschlüsselt werden und was hat die Verschlüsselung für einen Einfluss auf die Sprachqualität?"

Quality of Service (QoS) und Sprachqualität

Bei VoIP sind zweierlei Qualitäten von Bedeutung: Zum einen die Qualität der Übertragungsstrecke (QoS) und zum anderen die Qualität der Sprache (Sprachqualität). Dabei nehmen die Eigenschaften der Übertragungsstrecke Einfluss auf die Qualität der übertragenen Sprache.
Der Unterschied besteht darin, dass die Qualitätseigenschaften der Übertragungsstrecke objektiv bestimmt, die Sprachqualität jedoch nur subjektiv bewertet werden kann. Um die Übertragungstrecke zu bewerten, gilt es die QoS-Parameter Bandbreite, Delay, Jitter und Packet Loss zu messen und auszuwerten. Bei der Sprachqualität hingegen spielen subjektive Faktoren eine große Rolle. Diese wird auf einer Skala zwischen 1 und 5 bestimmt und Mean Opinion Score (MOS) genannt. Ein MOS von 5 bedeutet ausgezeichnete Sprachqualität, ein MOS von 1 bezeichnet eine unverständliche Sprachverbindung.

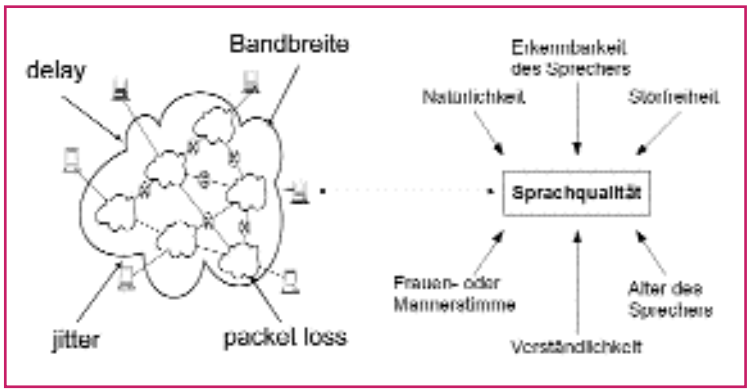

Abbildung 1: Einflüsse auf die Qualität von VoIP

Werden die QoS-Parameter kontrolliert und gesteuert, kann prinzipiell auch eine Sprachqualität zugesichert werden. Diese Zusicherung der QoS-Parameter wird in einem Service-Level-Agreement (SLA) mit den jeweiligen Providern ausgehandelt und festgelegt.
Um die Sprachqualität innerhalb eines Netzwerkes pragmatisch messen und vorhersagen zu können, wurden verschiedene Verfahren entwickelt. Diese Verfahren ermöglichen es, durch gemessene Werte der QoS-Parameter einen subjektiven Hörtest zu simulieren. Durch diese Simulationen ist es möglich, die Sprachqualität zu berechnen und dadurch den MOS auszudrücken [Rett07].

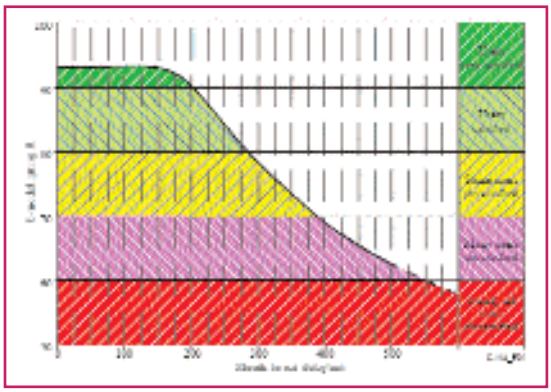

Abbildung 2: Determination of the effects of absolute delay by the E-model

Der ITU-T Standard G.114 legt durch QoS-Richtwerte fest, dass ein Delay kleiner 150 ms Voraussetzung für eine sehr gute Sprachqualität ist, ein Delay von 200 ms nicht überschritten werden sollte und ein Delay größer als 300 ms eine nicht akzeptable Sprachqualität verursacht. Auch ein Packet Loss von 5% darf nicht überschritten werden. Wie sich der Delay auf die Sprachqualität auswirkt, ist in Abbildung 2 dargestellt, welche aus dem ITU-T Dokument G.114 entnommen wurde.

Im Rahmen eines Forschungsprojektes am Institut für Internet-Sicherheit – if(is), wurde der Einfluss von verschiedenen Sicherungsmaßnahmen (IPSec und SSL (OpenVPN)) auf die Qualität von VoIP-Verbindungen analysiert.

Bei allen getesteten Sicherheitsmaßnahmen entsteht Overhead, der bei verschlüsselten Sprachdaten mit übertragen werden muss. In Anbetracht der Tatsache, dass Sprachpakete sehr klein und der Verschlüsselungs-Overhead konstant pro Paket ist, entsteht ein Mehr an Daten von deutlich über 25 Prozent, abhängig von Verschlüsselungsmodus und Sprach-Codec [BaPo07].
Die Untersuchungen, die im Institut für Internet-Sicherheit - if(is) durchgeführt wurden sind zuerst in einer optimalen LAN-Umgebung und anschließend in einer simulierten realen Umgebung umgesetzt worden.

IPSec

Eine der untersuchten Sicherheitsmaßnahmen ist IPSec, die mit OpenSWAN umgesetzt wurde. Wie in der Abb. 4 zu sehen ist, wird die Datenmenge durch die Einführung von IPSec erhöht.

Der Overhead für jedes Paket durch IPSec beträgt 22 bis 38 Byte je nach Konfiguration [Back07].
Die in der Abb. 4 dargestellten Ergebnisse setzen sich aus der Anzahl übertragener Bytes zweier Telefonate mit der Dauer von neun Sekunden zusammen, die über eine ungesicherte Verbindung (Referenz) und über IPSec gesicherte Verbindungen übertragen wurden. Da der bei dieser Messung eingesetzte Codec G.711 Sprachdaten ohne jegliche Kompression digitalisiert und überträgt, können hier durch Kompression Einsparungen von bis zu 20% pro Anruf erreicht werden.

Andere Codecs, wie z.B. der G.726 komprimieren die zu übertragenen Daten selber so stark, dass hier keine oder nur eine sehr geringe Kompression durch OpenSWAN und somit Einsparung der Datenmenge erzielt werden kann. Anhand der in Abb. 5 dargestellten Messwerte ist zu erkennen, dass Verschlüsselung mit und ohne transparen-

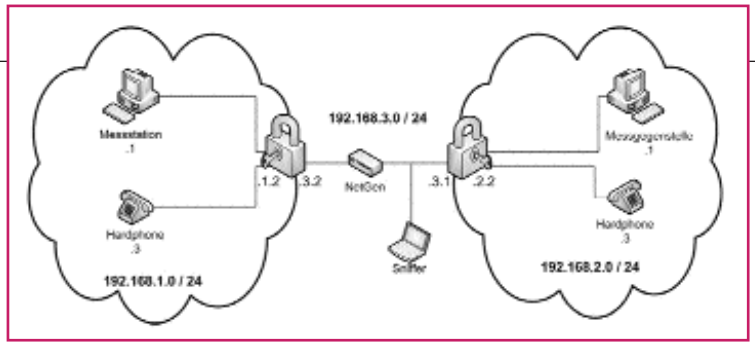

Abbildung 3: Messaufbau

te Kompression den Delay nur im unkritischen Maße erhöht (max. 0.5 ms).

TLS/SSL (OpenVPN)

Eine weitere Implementierung zur Absicherung von übertragenen Daten ist TLS/SSL (OpenVPN). Es unterscheidet sich von IPSec

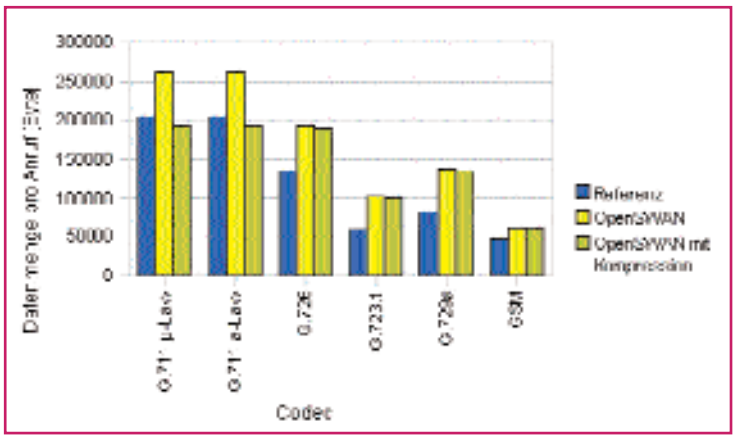

Abbildung 4: Zusätzlicher Overhead durchOpenSWAN

in der Art der Verschlüsselung und der Paketierung der getunnelten Daten. OpenVPN implementiert das Keymanagement ähnlich wie SSL/TLS und setzt zur Verschlüsselung

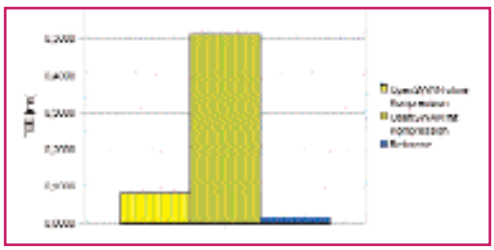

Abbildung 5: Zusätzlicher Delay durch OpenSWAN

OpenSSL EVP ein. Den durch OpenVPN entstehenden Overhead veranschaulicht Abb. 6.

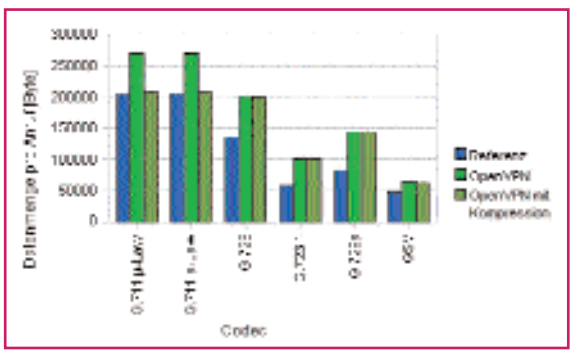

Abbildung 6: ZusätzlicherOverhead durchOpenVPN

Der Overhead für jedes Paket durch OpenVPN beträgt 28 bis 44 Byte je nach Konfiguration [Back07]. OpenVPN erzielt bezüglich der Kompression etwas schlechtere Ergebnisse als OpenSWAN.

Abb. 7 veranschaulicht, dass auch bei OpenVPN kein zeitkritischer Einfluss durch Verschlüsselung entsteht. Aus der Sicht der Qualitätsbewertung sind hier keine gravierenden Auswirkungen zu verzeichnen.

Zusammenfassend kann festgestellt werden, dass sich IPSec (OpenSWAN) und TLS/SSL (OpenVPN) nicht negativ auf die Qualität eines VoIP-Gesprächs in einem LAN auswirken. Diese Laborumgebung repräsentiert allerdings ein ideales Netz.

Ergebnisse in einer realen Netzumgebung, wie z.B. das Internet

Mit der Hilfe der Software NetGen wurde ein reales Netz entsprechend simuliert. NetGen ist eine Layer 2 Bridge, die die Netzwerkparameter Delay, Packet Loss und Jitter künstlich verschlechtert. Dazu werden ankommende Daten in einem Ringbuffer zwischengespeichert (Delay) oder verworfen (Packet Loss). NetGen ist eine Entwicklung des Fachbereichs für Kommunikationstechnik der FH-Köln und wurde entwickelt, um ein reales Netz reproduzierbar nachzubilden.

Bei dieser Messreihe wurde der Delay auf der Leitung von ca. einer Millisekunde auf bis zu 400ms End-to-End-Delay erhöht. In Abb. 8 werden die Ergebnisse dieser Messreihe dargestellt, die das Verhalten der Sprachqualität wie erwartet darstellt d.h. es gibt eine deutliche Verschlechterung der Sprachqualität mit steigendem Delay.

Ein weiteres Szenario war die schrittweise Erhöhung der benutzten Bandbreite durch ein kontrolliertes Einspielen von Datenpaketen in das Testnetzwerk. Da Daten innerhalb eines Netzes unterschiedliche Größen aufweisen können und sich somit das Verhalten des Netzes ändern kann, wurde dieses Szenario auf zwei Arten simuliert: Mit einem Hintergrundrauschen zunächst durch große und anschließend durch kleine Paketgrößen. Abb. 9 veranschaulicht deutlich den Unterschied zwischen einer Belastung durch große und kleine Datenpakete. Es ist zu erkennen, dass es schneller zu einem hohen Delay bei kleinen Datenpaketen kommt. Innerhalb der Testumgebung ist das darauf zurückzuführen, dass deutlich mehr Rechenleistung erforderlich ist, um kleine Datenpakete zu verarbeiten. Sowohl die Referenz-Messung als auch alle eingesetzten Sicherheitsmechanismen waren mit einer großen Anzahl kleiner Datenpakete überfordert und hatten somit auch einen hohen Delay zu Folge. Die Grenze der Messreihe war somit der Prozessor des Sicherheitsgateways (IPSec oder TLS (OpenVPN)) und nicht das Übertragungsmedium.

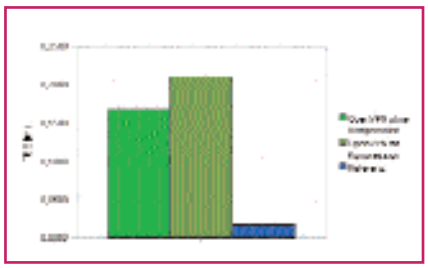

Abbildung 7: Zusätzlicher Delay durch OpenVPN

Die Messungen wurden aufgrund dessen mit einem Delay von 30ms durchgeführt, der bis zu 6 ms schwankt (Jitter). Anhand dieser Messung konnte bestätigt werden, dass sich ein größerer Jitter bei der Kommunikation nicht negativ auswirkt, solange ein genügend großer Jitter-Buffer vorhanden ist, der diese Schwankungen kompensiert.

Das Fazit dieser Messreihe ist, dass bei einem Jitter bis zu 6ms die Integration der getesteten Sicherheitsimplementierung keine Probleme bezüglich der Sprachqualität mit sich bringt. Es kam zu keinem Packet Loss oder erhöhtem Delay, was darauf schließen lässt, dass die getesteten Sicherheitsme-

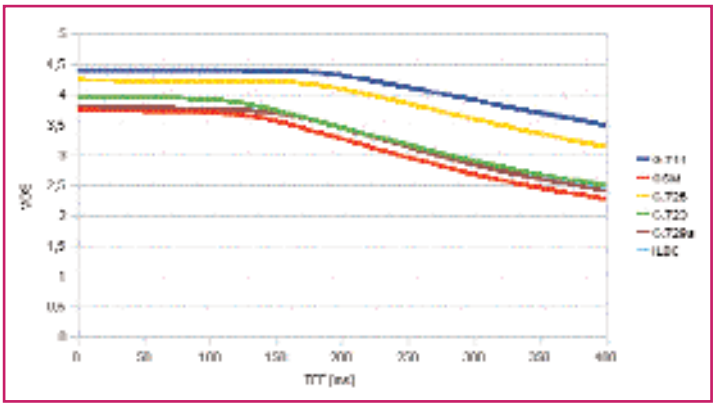

Abbildung 8: Verschlechterung des MOS mit zunehmendem Delay (T_{EE})

chanismen keinen Einfluss auf den Jitter haben. Da sich mit steigender Auslastung der Bandbreite auch das Delay erhöht, bleibt es nicht aus, dass sich auch der Jitter erhöht. Trotz erhöhtem Jitter befindet sich die

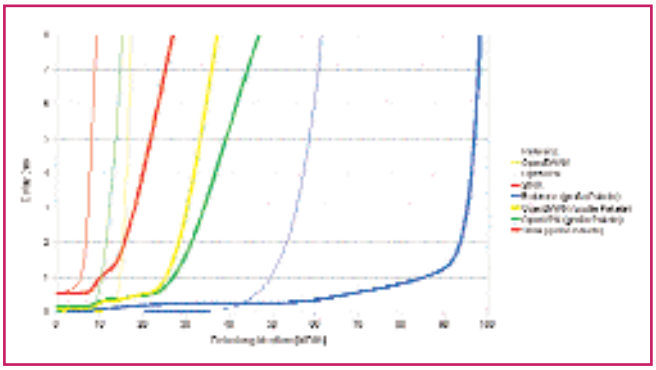

Abbildung 9: Verschlechterung des Delay (T_{EE}) mit zunehmender Auslastung des Übertragungsmediums

Sprachqualität zu keinem Zeitpunkt in einem kritischen Bereich, da der Jitter-Buffer diesen Jitter ausgleichen kann.

Packet Loss wirkt sich unterschiedlich auf die Qualität eines VoIP-Gesprächs aus. Je nach Codec können bis zu 5% Paketverlust ausgeglichen werden. In der Regel ist pro Paket 20ms bis 30ms Sprache enthalten , was ca. einer Silbe entspricht. Der Verlust eines Paketes entspricht daher etwa dem Wegfall einer Silbe im Sprachstrom. In Testreihen, bei denen ein Gespräch subjektiv

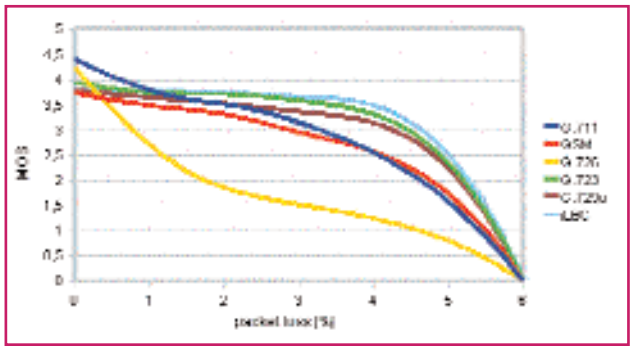

Abbildung 10: Verhalten des MOS pro Codec mit steigendem packet loss

bewertet wurde, war – abhängig vom eingesetzten Codec - ein Paketverlust bis 20% noch akzeptabel. Mit 20% Paketverlust kann der Gesprächspartner nicht mehr anhand seiner Stimme erkannt werden, da die synthetisierte Stimme zunehmend blechern klingt. Ab 30% Paketverlust war der Kommunikationspartner nicht mehr zu erkennen und unverständlich. Die objektive Bewertung hingegen geht strenger mit der Bewertung der Sprachqualität um, da ein simulierter Gehörgang nicht die Fähigkeit besitzt, aus dem Kontext eines Gesprächs die fehlenden Silben zu rekonstruieren.

Abb. 10 zeigt die objektive Bewertung des MOS mit steigendem Packet Loss in einem Netz ohne hohen Delay oder Jitter. Hier ist deutlich zu erkennen, dass jeder Codec anders auf Packet Loss reagiert. Die Grenze für eine gute Bewertung liegt zwischen 4% und 5%. Der Verlauf des berechneten MOS mit integrierten Sicherheitsmechanismen gleicht dem Verlauf des MOS aus der Referenz-Messung.

Dies bedeutet, dass sich zu keinem Zeitpunkt das Netz durch eine zusätzliche Sicherheitsmaßnahme stark beeinflussen lässt. Daraus lässt sich schlussfolgern, dass eine zusätzliche Sicherheitsimplementierung keine positiven oder negativen Einflüsse auf die Sprachqualität hat. Die Sicherheitsimplementierungen verhal- ten sich bei steigendem Packet Loss transparent und können somit auch in schlechten Netzen eingesetzt werden.

Schlussbetrachtung

Aufgrund der erhobenen Ergebnisse können Empfehlungen ausgesprochen werden, die je nach Zustand des Netzes (QoS) dafür sorgen, dass ein Telefonat eine gute Sprachqualität (MOS) erreicht. Innerhalb dieses Forschungsprojektes wurde gezeigt, dass mehrere Faktoren Einfluss auf die subjektive Wahrnehmung einer Sprachübertragung haben.

Die benötigte Bandbreite für den verwendeten Codierer muss während eines Gesprächs permanent zur Verfügung stehen. Zeitliche Vorgaben wie Jitter und Delay müssen kontinuierlich gewährleistet sein. Paketverluste müssen verhindert oder mit Hilfe eines passenden Codierers ausgeglichen werden.

Hierbei gilt zu beachten, dass sowohl die Infrastruktur als auch jeder einzelne Teilnehmer die Sprachqualität beeinflussen kann. Zu den Faktoren zählen somit: Die Anbindung an das Transportnetz, die Endgeräte, der Netzzustand, die verwendeten Codecs, der VoIP-Server und die verwendete Hardware für eine Verschlüsselung.

In Zukunft werden viele IP-basierte Dienste mit unterschiedlichen Sicherheits- und Qualitätsansprüchen über die Netzwerke laufen. Sowohl Firmen als auch Privatpersonen werden sich mit den Themen Sicherheit und Qualität näher befassen müssen, um den beiden immer wichtigeren und unterschiedlichen Aspekten gerecht zu werden.

Literatur

[BaPo07] P. Backs, N. Pohlmann: „Voice over IP aber sicher", IT-SICHERHEIT – Management und Praxis, DATAKONTEXT, 5/2007

[Back07] P. Backs: „Analyse von Sicherheitsmaßnahmen für Voice over IP", Diplomarbeit, Institut für Internet-Sicherheit if(is), FH-Gelsenkirchen 2007

[Rett07] C. Rettinghausen: „Quality of Service bei Voice over IP in Bezug auf Sicher-heitsimplementierungen", Diplomarbeit, Institut für Internet-Sicherheit if(is), FH-Gelsenkirchen 2007

Prof. Dr. Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssi-cherheit sowie Leiter des Instituts für Internet-Sicherheit - if(is) an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de).

Dipl.-Inform. (FH) Claas Rettinghausen forschte im Rahmen seiner Diplomarbeit im Bereich „Sicherheit von Voice over IP" im Institut für Internet-Sicherheit und ist jetzt VoIP-System-Architekt bei der CARPO GmbH. http://www.qossip.de/ http://dnserver.nt.fh-koeln.de/grebe/