



Internet der Zukunft

**Anja Feldmann, Ariane Gintzel, Dan Levin,
Rainer May, Nadi Sarrar, Stefan Schmid, Philipp Schmidt,
Peter Domschitz, Marco Hoffmann,
Phuoc Tran-Gia, Martina Zitterbart**



Das Internet der Zukunft

Inhalt

*Anja Feldmann, Ariane Gintzel, Philipp Schmidt, Dan Levin,
Stefan Schmid, Nadi Sarrar, Rainer May*

Das Internet von Heute und Morgen

Einführung	3
Aktuelle Architektur des Internet	7
Probleme der jetzigen Internet-Architektur	10
Clean-Slate	12
Software Defined Networking	13
Netzwerkvirtualisierung	15
Content Centric Networks	18
Zusammenfassung	20
Literatur	21

*Phuoc Tran-Gia, Martina Zitterbart, Anja Feldmann,
Marco Hoffmann, Peter Domschitz*

Future Internet – Beobachtungen und aktuelle Trends, Chancen und Herausforderungen	23
---	-----------

Impressum

Stiftungsreihe 100

Redaktion
Dr. Erich Zielinski
Petra Bonnet M.A.

Druck der Broschüre
DCC Kästl GmbH & Co. KG

Alle Rechte vorbehalten
© 2012

Die Alcatel-Lucent Stiftung für
Kommunikationsforschung ist
eine nichtrechtsfähige Stiftung
in der treuhänderischen Ver-
waltung des Stifterverbandes
für die Deutsche Wissenschaft.

Angaben nach § 5 TMD/
§ 55 RfStv

Stifterverband für die Deutsche
Wissenschaft e.V.
Barkhovenallee 1
45239 Essen
Telefon: (02 01) 8401-0
Telefax: (02 01) 8401-301
E-Mail: mail@stifterverband.de

Geschäftsführer:
Prof. Dr. Andreas Schlüter
(Generalsekretär)

Das Internet von Heute und Morgen

Anja Feldmann, Ariane Gintzel, Philipp Schmidt, Dan Levin,
Stefan Schmid, Nadi Sarrar, Rainer May

Gut 30 Jahre nach seiner Entstehung ist das Internet ein wichtiger Teil der Gesellschaft geworden. Weltweit wird es von rund einem Drittel aller Menschen genutzt (Dezember 2011, <http://www.internetworldstats.com/stats.htm>), und auch die Mehrzahl der (Noch-)Nichtnutzer wird von ihm beeinflusst, stellt es doch für Firmen wie für Regierungen ein mittlerweile unverzichtbares Medium zur Organisation und vor allem Kommunikation dar. Sein anhaltendes Wachstum verdankt es zum großen Teil seiner Wandlungs- und Anpassungsfähigkeit. Doch während die Anforderungen ungebremst weiter wachsen, ist abzusehen, dass die technischen Möglichkeiten dafür bald erschöpft sein werden. Denn das Internet ist „organisch“ gewachsen, unkontrolliert, ungeplant, nachgerade „anarchisch“, überall wurden Erweiterungen und Veränderungen „angebaut“, um den aktuellen Bedarf zu decken. Technisch gesehen ähnelt es heute daher einem Flickenteppich, bei dem jede weitere Änderung zu unvorhersehbaren Nebenfolgen führen kann. Es befindet sich in einem Zustand zunehmender „Verknöcherung“ („Ossifikation“), der sich nur noch durch eine Neukonzeption beheben lässt. Deshalb arbeiten nationale und internationale Forschungsgruppen bereits seit etwa 10 Jahren daran, das Internet neu zu erfinden – mit dem Anspruch, es modern, innovativ, schnell, energiesparend, effizient, sicher, wirtschaftlich und sozial gerecht nutzbar, erweiterbar - kurz: zukunftssicher zu machen. Wir werden einen kleinen Überblick über das heutige Internet geben, und mögliche Wege für die Zukunft des Internet zeigen.

Einführung

Das Internet ist nicht länger nur ein technisches, sondern auch ein soziales Phänomen. Anders als klassische Medien wie Rundfunk, Zeitungen, selbst Bücher, bei denen Informationen nur von wenigen „Auserwählten“ eingespeist und von den Benutzern lediglich konsumiert werden können, ist im Internet jeder Empfänger auch zugleich ein (potentieller) Sender: Ein Ereignis, das es früher nicht einmal zu einem Fünfzeiler in einer Regionalzeitung gebracht hätte, geht heute über Twitter, Facebook, Blogs, Messenger und Emails um die Welt; es erreicht Millionen von Menschen, die es zur Kenntnis nehmen, kommentieren – und weiterverbreiten. Auf diese Weise wird plötzlich auch politischer Druck aufgebaut, die Menschen wollen an Entschei-

dungen partizipieren, die sie vorher nicht einmal erahnten. Zudem verändert es die Kommunikation der Menschen mit- und untereinander, Arbeitsformen von und in Unternehmen, Reaktion auf Notfälle, die Arbeit des Militärs, die Steuerung von Fertigungsprozessen. Es hat die Erwartungen an zwischenmenschliche Kommunikation, die Interaktion von Computer und Mensch sowie die Kommunikation zwischen Computern verändert und teilweise revolutioniert – und vor allem: beschleunigt.

Nahezu alle Wirtschaftszweige nutzen das Internet – dazu gehören neben Software-Unternehmen wie Microsoft, Google und SAP auch eher traditionelle und produzierende Branchen wie die Automobilindustrie, Dienstleister einschließlich Banken und Versiche-

rungen, und nicht zuletzt Werbung und Presse. Angesichts dieser Auswirkungen und Möglichkeiten stellt sich die Frage, was die Nutzer – Institutionen wie Einzelpersonen – im Internet zu finden erwarten: Was wollen sie erreichen, wofür nutzen sie es?

Für die Milliarden Nutzer des Internet steht eine Vielzahl von Anwendungen zur Verfügung: Das Web birgt Inhalte und Dienste wie Suchmaschinen (z.B. Google, Bing oder nicht-kommerzielle Projekte wie YaCy), Archive und soziale Netze (z.B. Facebook oder Google+), Dienste wie E-Mail, Chat, Dateiaustausch, Internet-Telefonie (VoIP), Fernsehen über das Internet (IP-TV), Video on Demand Streamingdienste wie Netflix oder Videoload, und vieles mehr.

Technische Grundlage all dieser Kommunikation im Internet ist IP, das Internet-Protokoll. Eine gemeinsame Sprache, in der die Milliarden Geräte im Internet miteinander kommunizieren. Es wird über eine Vielzahl darunterliegender Leitungstechnologien hinweg gesprochen und ist die Basis für Transportprotokolle wie TCP, UDP und SCTP, die ihrerseits für die unterschiedlichen Anforderungen der einzelnen Dienste (z.B. Mail, Web, Telefonie, Steuerung) eine geeignete Grundlage bereitstellen. Die Leitungstechnologien – z.B. Ethernet, DSL, Teile der Mobilfunknetze – sind ihrerseits wieder aus unterschiedlichen Hardware-Komponenten zusammengebaut, welche die Informationen aus der IP-Schicht übertragen.

Neben dieser sehr technischen Betrachtungsweise, die in der Anfangszeit des Internet sein vorherrschendes Bild geprägt hatte, gibt es viele andere Aspekte, die zunehmend an Bedeutung gewinnen:

- Die organisatorische Struktur mit diversen Selbstverwaltungsebenen wie der ICANN

(Internet Corporation for Assigned Names and Numbers), der von ihr betriebenen IANA (Internet Assigned Numbers Authority), den diversen regionalen Internet-Registaturen (RIRs) wie dem für Europa zuständigen RIPE (Réseaux IP Européens) und TLD-Verwaltern wie z.B. der für „de“ zuständigen DeNIC.

- Die wirtschaftliche Struktur des Internet, bestehend aus multinationalen Telekommunikationskonzernen, vielen kleineren Internet Service Providern, nationalen und internationalen Wissenschaftsnetzen und vielen Inhaltsanbietern.
- Die sozialen Strukturen, die aus dem Internet erwachsen und sich z.B. in Foren und sozialen Netzwerken kristallisieren, sowie der schon erwähnten „Einflussnahme der Massen“.

Dies alles hatte und hat Einfluss auf den Erfolg und die Struktur des Internet. Alle Teilnehmer haben ihre politischen, wirtschaftlichen, persönlichen, sogar religiösen Interessen, die ihre Einflussnahme und Entscheidungen lenken und begründen. Dieses breite Spektrum von Motiven spiegelt nicht nur den großen Erfolg des Internet wieder, sondern es zeigt ein System in seiner ganzen Komplexität und Vielfalt. Ein System, das konzipiert wurde, um einige wenige Hochleistungsrechner aus dem militärischen und wissenschaftlichen Bereich miteinander zu vernetzen. Dass es diese Vernetzungsaufgabe heute mit Milliarden Teilnehmern immer noch erfüllt, grenzt an ein technisches Wunder.

Trotz der gewaltigen historischen und technischen Dimension sollte es nicht vergessen werden, dass das Internet von Menschen gemacht wurde, tagtäglich verändert und am Leben gehalten wird – oft mit viel persönlichem Engagement, informellen Absprachen

und langjähriger Erfahrung im Beherrschen fast unüberschaubar komplexer Systeme. Und das, ohne dass die überwältigende Mehrzahl der Benutzer auch nur eine Ahnung von der zugrundeliegenden Technik hat, haben will – und haben muss.

Wir Wissenschaftler versuchen, die Fragmente dieses Systems zu verstehen und zukünftige Entwicklungen vorauszusagen, indem wir den Verkehr im Internet und die Aktionen der Benutzer, die für diesen Verkehr verantwortlich sind, beobachten und charakterisieren. Wir versuchen, Herausforderungen und sich ankündigende Probleme rechtzeitig zu identifizieren und mögliche Lösungsansätze zu bewerten.

Denn das Internet ist nicht perfekt. Während sich die öffentliche Diskussion vor allem um Aspekte von Sicherheit, Vertraulichkeit und Datenschutz – teils mit diametral entgegengesetzten Zielen – dreht, sollte nicht vergessen werden, dass sich mit neuen Diensten und deren Einfluss auf unser Leben die Erwartungen und die Anforderungen der Nutzer an das Netz ständig ändern. Und dass der „Goliath Internet“ mittlerweile durch seine eigene Komplexität so mancher notwendigen Änderung selbst im Wege steht. Ein Beispiel dafür ist das in letzter Zeit viel diskutierte „Recht auf Vergessen“, die Möglichkeit, einmal veröffentlichte Daten „zurückzuziehen“ – was technisch und konzeptionell einfach nicht möglich ist. Einige der wichtigsten Herausforderungen sind:

Sicherheit: Sicherheit stellte in der Anfangsphase des Internet keine Anforderung dar – es ging nur um die Verfügbarkeit des Netzes, darum, Daten zugänglich zu machen, und die Teilnehmer vertrauten einander einfach. Die zunehmende Bedeutung des Internet auch für Speicherung und Zurverfügungstellung

privater und selbst geheimer Daten macht Sicherheits- und Datenschutzerfordernungen unverzichtbar, um eben nicht alles für jeden sichtbar zu machen. Die konkrete Ausgestaltung ist ein großes Spannungsfeld zwischen dem technisch Machbaren, der Privatheit, wirtschaftlichen und politischen Interessen, in dem nationale Lösungen auf Dauer keinen Bestand haben werden.

Zuverlässigkeit, Verfügbarkeit: Steigende Relevanz des Internet für den Alltag führt zu steigenden Erwartungen der Nutzer an Zuverlässigkeit und Verfügbarkeit, weit über das hinausreichend, was das Telefonnetz einst geboten hat. Je wichtiger es wird, desto zuverlässiger muss es sein. Mit der Durchdringung durch kritische Infrastrukturen (etwa hoheitliche Kommunikation in Notfällen) wird das Internet selbst zur kritischen Infrastruktur.

Mobilität: Für die Benutzer des Internet ist mit Smartphones und Laptops Mobilität alltäglich geworden. Der damit verbundene Wechsel von Verbindungsort und -technologie (etwa ein Laptop, der eben noch am Netzkabel hing, dann ins WLAN wechselt, und Minuten später per UMTS mit dem Netz verbunden zu sein – ohne, dass der Videostream auch nur ruckeln darf) findet jedoch derzeit wenig Unterstützung vom Netz und den Betriebssystemen, welche die technische Grundlage für diese Mobilität schaffen müssen. Dieser Trend wird sich mit neuen Entwicklungen wie Googles „Project Glass“ noch verstärken.

Problemanalyse: Die Werkzeuge, um Probleme an der Infrastruktur des Internet zu diagnostizieren und Ursachenanalyse zu betreiben, sind sehr limitiert. Vor allem die Analyse von Problemen und Anforderungen, die über Providergrenzen hinweg entstehen, stellen eine große Herausforderung dar. Ohne

die enge, oftmals informelle Zusammenarbeit der Mitarbeiter verschiedener Provider, die sich im Fehlerfall gegenseitig anrufen und gemeinsam die Probleme begutachten, wäre heutzutage kein stabiler Betrieb des Internet möglich. Es müssen bessere Werkzeuge und Methoden für die Analyse von Problemen und die Bestimmung von Anforderungen und Planungen gefunden werden.

Skalierbarkeit: Mit dem Wachstum des Internet auf allen Ebenen (Datenverkehr, Nutzerzahl, ...) bleiben viele Fragen der Skalierbarkeit einiger Teile des aktuellen Internet offen. Nicht überall reicht es, mehr Bandbreite zur Verfügung zu stellen. Besondere Problemfelder stellen dabei die IP-Adressvergabe für das alte Internet-Protokoll IPv4 und die Kapazitäten des Routing System dar.

Dienstgüte: Unterschiedliche Anwendungen stellen unterschiedliche Anforderungen an den Datentransport im Internet – so können zum Beispiel die Latenz (Verzögerung bei der Paketübertragung) und Jitter (Varianz der Verzögerung) für Internet-Telefonie schnell kritische Werte annehmen. Es ist noch unklar, wie und auf welchen Schichten Dienstgütemanagement realisiert werden kann. Zu den technischen Herausforderungen kommt noch die Frage der Netzneutralität: Wo endet technisch nötige Optimierung, und wo fängt wirtschaftliche oder politische Diskriminierung von Datenverkehr an?

Wirtschaftliche Aspekte: Neben diesen eher technischen Fragen stellt sich unter anderem auch die Frage, wie Netzwerk- und Servicebetreiber zukünftig Gewinn erzielen können. Einerseits werden ihre Dienste immer wichtiger für die Allgemeinheit, andererseits sind die Kunden kaum bereit, mehr Geld für die gestiegenen Anforderungen zu zahlen. Die Netzwerk- und Serviceprovider geraten

dabei unter einen immer höheren Gewinn- druck und tun sich schwer, seit über zehn Jahren projektierte Neuerungen wie die Version sechs des Internet-Protokolls (IPv6) einzuführen. Eingedenk dessen ist es vollkommen unklar, wie deutlich teurere Technologieschritte wie Einführung von Glasfasern auf den letzten Kilometern zum Nutzer (FTTH, „Fibre to the Home“) finanziert werden sollen.

Der Klimawandel und die steigenden Energiepreise schaffen zusätzlichen Druck, der aber auch Anreiz für Modernisierung und Innovation ist. Da die Übertragung von Daten über ein weltweites Datennetz im Vergleich zu Speicherung nahe beim Anwender deutlich energiehungriger ist, ist die Optimierung der Verteilung von Daten innerhalb des Netzes ökologisch wie ökonomisch geboten.

Die genannten Herausforderungen sind wohl- bekannt. Schon in den letzten zehn Jahren versuchte man, Lösungen zu finden, konzentrierte sich dafür aber oft auf individuelle Ansätze, die letztlich nur „Kosmetik“ betrieben, da die eigentlichen Problemursachen wo- möglich an einer viel grundlegenden Stelle der Internetarchitektur zu finden waren. Wir wollen zunächst aufzeigen, warum das so ist, und wie die jahrzehntealten Entwurfs-Ziele und daraus resultierenden Designentscheidungen der Internetarchitektur die Lösung aktueller Probleme behindern.

Viele glauben, dass es notwendig und zeitge- mäß sei, die grundlegenden Annahmen und Designentscheidungen zu überdenken und von Grund auf neu zu beginnen: Mittels eines „Clean-Slate-Design-Ansatzes“ sollen Lösun- gen gefunden werden, die gleichzeitig allen genannten Herausforderungen begegnen und zudem Raum lassen für zukünftig not- wendig werdende Änderungen, die heute noch nicht einmal im Ansatz erkennbar sind.

Im Folgenden wollen wir nun Strategien für das Vorgehen auf diesem Weg und mögliche Auswirkungen erläutern.

Aktuelle Architektur des Internet

Bevor erklärt werden kann, warum es so schwierig ist, auf die genannten Herausforderungen mit der aktuellen Internetarchitektur zu reagieren, müssen wir zunächst kurz erläutern, wie das Internet in seiner heutigen Form funktioniert.

Der Architektur des Internet, wie wir es heute kennen, lagen die folgenden **Entwurfsziele** zu Grunde (in der Reihenfolge ihrer Bedeutung zur Entwurfszeit):

1. Bestehende Netzwerke miteinander zu verbinden.
2. Die Überlebensfähigkeit des Netzes zu garantieren.
3. Eine Vielzahl (auch noch unbekannter) Dienste zu unterstützen.
4. Die Verbindung von verschiedenen Netzwerktechnologien zu ermöglichen.
5. Das Netz dezentral zu verwalten.
6. Weitere Rechner mit geringem Aufwand integrieren zu können.
7. Ressourcen eindeutig zuzuordnen zu können.

Um diese Ziele zu erreichen, wurden die folgenden **Design-Prinzipien** gewählt:

- A Schichtenarchitektur
- B Paketvermittlung
- C Ein Netzwerk aus Netzen
- D Intelligente End-Systeme
- E Ende-zu-Ende Kommunikation.

Auf welche Weise haben diese Prinzipien das heutige Internet geprägt, und wie war es mit ihrer Hilfe möglich, die ursprünglichen Ziele zu erreichen?

Schichtenarchitektur

Heutzutage wird die Implementierung von Computernetzen meist als „Netzwerk-Stack“ bezeichnet, weil Netzwerkprotokolle üblicherweise als Schichtenarchitektur entworfen werden. Jede Schicht im Netzwerk-Stack bietet eine bestimmte Funktionalität für die darüber liegenden Schichten an und bedient sich ihrerseits der Funktionalität der darunter liegenden. Diese Struktur ermöglicht die Isolierung der Funktionen und reduziert somit die Komplexität der einzelnen Schichten. Logi-



Abb. 1 :Das Internet-Schichtenmodell

sche Kommunikation findet immer innerhalb einer Schicht statt. Während der jeweiligen Kommunikation durchlaufen die Daten beim Sender den Netzwerk-Stack von oben nach unten und beim Empfänger von unten nach oben.

Das Internet-Schichtenmodell (vgl. Abb. 1) hat die folgenden fünf Schichten (von oben nach unten): Anwendungsschicht, Transportschicht, Netzwerk/IP-Schicht, Medienzugriffsschicht und physikalische Schicht.

Wir betrachten das Modell jetzt von unten nach oben, wie in der Literatur üblich.

Die physikalische Schicht ist verantwortlich für die Codierung der Daten und den Transport über das Medium (z.B. Glasfaser-, Kupferkabel, diverse Funktechnologien).

Die Medienzugriffsschicht ermöglicht direkten Nachbarn, die ein gemeinsames physikalisches Medium verwenden, direkte Kommunikation.

Die Netzwerkschicht, im Internet-Kontext IP-Schicht genannt, ermöglicht Ende-zu-Ende Kommunikation. Dazu erhält jede Gegenstelle eine IP Adresse, die die Gegenstelle weltweit eindeutig identifiziert. Gegenstellen kommunizieren über IP-Pakete, die von den Routern, die die einzelnen Netze des Internet verbinden, anhand der IP-Adresse zum Ziel geleitet werden. So wird letztendlich weltweite Kommunikation möglich. (Entwurfsziel 5 und VII, Design-Prinzip C)

Die Transportschicht ermöglicht Anwendung-zu-Anwendung Kommunikation. Je nach Anforderungen der Anwendung können die Transportprotokolle verschiedene Übertragungsemantiken bereitstellen. Die gebräuchlichsten Transportprotokolle im Internet sind TCP, das einen zuverlässigen Datenstrom mit Fluss- und Staukontrolle bereit-

stellt, und UDP, das unzuverlässigen, aber für die Anwendung transparenten Nachrichtenaustausch ermöglicht. (Entwurfsziel 3)

Die Protokolle auf der Anwendungsschicht (z.B. HTTP für das WWW oder SMTP für Mail) realisieren die eigentliche Kommunikation zwischen Anwendungen über das Internet. Das Socket-API ist das vom Betriebssystem bereitgestellte Bindeglied zwischen im Betriebssystem implementiertem Transportprotokoll und dem in der Anwendung implementierten Anwendungsprotokoll.

Der Gebrauch von Kommunikationsschichten ermöglicht das einfache Verbinden existierender Netzwerke (Design-Prinzip A) und außerdem den Zusammenschluss einer Vielzahl von Netzwerken (Entwurfsziel 1). So lässt sich ein Netzwerk, das einen Dienst zur Verfügung stellt, leicht um höhere Schichten erweitern. Für das Internet bedeutet das, dass jedes Netz, das Pakete an Gegenstellen innerhalb des Netzes weiterleiten kann, (wobei Pakete verloren gehen dürfen), unter der Netzwerkschicht des Internet verwendet werden kann – eine Anforderung, die praktisch jede Netzwerktechnologie erfüllt.

Paketvermittlung

Die Entscheidung, ein paketvermitteltes Netz zu entwerfen, war von dem Willen getragen, es gegen Teil-Ausfälle möglichst unempfindlich zu machen. Wenn etwa ein Bagger eine zentrale Telefonleitung (leitungsvermitteltes Netz) zerstört, sind darüber laufende Telefonate (erst einmal) unterbrochen; bei Internetverbindungen geht hingegen gerade mal ein kleines „Datenpaket“ verloren, bevor sich die anderen Pakete einen neuen Weg zum Ziel suchen (und das verlorene evtl. einfach noch mal übertragen wird). Dies impliziert eine Aufteilung der Daten in kleinere Pakete. Jedes

Paket trägt die Adresse seines Bestimmungsortes und durchquert das Netzwerk unabhängig von anderen Paketen. Die eigentliche Übertragung der Daten erfolgt nach dem „Best-Effort“-Prinzip: Jedes Paket kann die volle Bandbreite der Verbindungen auf dem Weg zum Ziel nutzen, muss aber, falls dieser noch durch andere Pakete belegt ist, ggf. in einer Warteschlange verweilen. Da die Länge der Warteschlangen begrenzt ist, werden Pakete, die auf eine volle Warteschlange treffen, einfach verworfen. Aufgabe höherer Schichten ist es, das zu bemerken und darauf entsprechend (Resending) zu reagieren.

Paketvermittlung hat den Vorteil, dass die Netzwerkebene keine Zustandsinformationen über bestehende Verbindungen halten muss, was das Routing-System massiv vereinfacht und eine gute Skalierbarkeit sicherstellt. Die Kosten für paketvermittelte Netze sind deutlich geringer als die für ein leitungsvermittelltes Netz wie das klassische Telefonnetz (Entwurfsziel 4).

Netzwerk verbundener Netze

Wie Pakete im Internet weitergeleitet werden, wird anhand von IP-Präfixen (einer Gruppe aufeinanderfolgender IP-Adressen) bestimmt, wobei jedem Netz ein oder mehrere IP-Präfixe zugeordnet sind. Die Routing Tabelle auf jedem Router, die für jedes Präfix die nächste Station auf dem Weg zum Zielnetz enthält, wird in einer verteilten Weise berechnet.

Das Internet ist dabei erst einmal eine Sammlung von autonomen Systemen (AS). Jedes AS wird von einem Internet Service Provider (ISP) verwaltet, der ein Backbone-Netzwerk betreibt, das Kunden, andere Dienstleister und ggf. kleinere ISPs verbindet. Innerhalb eines AS wird die Routingtabelle meist mit internen Routingprotokollen (IGPs)

wie OSPF und IS-IS berechnet. Das Routing zwischen Autonomen Systemen wird vom Border-Gateway-Protokoll (BGP) geregelt. Das BGP ist ein Routing-Protokoll, das nicht nur den Austausch von Routinginformationen zwischen Routern verschiedener AS ermöglicht, sondern auch die Implementierung von Routing-Strategien ermöglicht, die die wirtschaftlichen und politischen Bedürfnisse des ISPs widerspiegeln können (z.B. „route nur im Notfall über Provider X, denn dabei fallen hohe Kosten an“). Jeder Router bestimmt die nächste Station auf dem Weg eines Paketes durch Zusammenführen der durch BGP und das IGP gelernten Informationen. Dieses Design des Routing-Systems gewährleistet Überlebensfähigkeit (Entwurfsziel 2) und erlaubt verteiltes Management (Entwurfsziel 5) solange die ISPs zusammenarbeiten.

Intelligente Systeme / Ende-zu-Ende Argument

Dass die Netzwerkschicht oder tiefere Schichten einfach so Pakete verwerfen können, ist eine Folge aus der grundlegenden Entscheidung, das Netzwerk als solches möglichst einfach zu halten. Die Intelligenz, die für manche Anwendungen nötig ist, wird dabei an die beteiligten Endsysteme verlagert. Sollte die Anwendung zuverlässigen Datentransfer oder die Übertragung von mehr Daten als in einem Paket möglich erfordern, dann obliegt es der Verantwortung der Endsysteme diesen Dienst zu bieten. Das populärste Beispiel hierfür ist das Transportprotokoll TCP, das einen kontinuierlichen Datenstrom auf Pakete verteilt und durch Übertragungswiederholung im Fehlerfall zuverlässige Datenübertragung ermöglicht.

Das Ende-zu-Ende Argument ist ein für den Architekten des darunterliegenden Netzes

bequemer Weg, Funktionalität zu verteilen. Es gibt jedoch auch Gründe, Funktionalität innerhalb des Netzwerkes zu realisieren, anstatt sie den Endsystemen zu überlassen: Wenn alle Anwendungen eine gemeinsame Funktionalität benötigen oder eine Verlagerung der Funktionalität in das Netz einer großen Anzahl Anwendungen eine Leistungssteigerung ermöglicht. Obwohl es auf den ersten Blick anders scheinen mag, ist gerade zuverlässige Datenübertragung kein gutes Beispiel für eine solche Funktionalität, denn nicht alle Anwendungen erfordern zuverlässige Datenübertragung. Für VoIP ist die schnelle Übertragung der meisten Pakete wichtiger, als dass alle Pakete ankommen. Andere Anwendungen, wie z.B. das Domain Name System (DNS) haben aus anderen Gründen eigene Mechanismen, die Ende-zu-Ende Zuverlässigkeit zu gewährleisten.

Sowohl Paketvermittlung als auch das Ende-zu-Ende Argument haben sich als positiv für die Überlebensfähigkeit (Entwurfsziel 2) und Wirtschaftlichkeit (Entwurfsziel 4) des Internet erwiesen. Heute lässt sich guten Gewissens sagen, dass das Internet die Entwurfsziele 1 bis 6 sehr gut erfüllt. Das verbliebene Entwurfsziel, die Zuordenbarkeit von Ressourcen, wurde auf eher pragmatischem Wege mittels Hilfskonstruktionen wie DHCP, Ident, Netflow und diversen anderen Anwendungsprotokollen realisiert.

Probleme der jetzigen Internet-Architektur

Warum die heutige Internet-Architektur die zukünftigen Herausforderungen nicht erfüllen kann

Wenn wir die aktuellen Herausforderungen an die Internetarchitektur betrachten, fällt es auf, dass diese sich signifikant von den ursprünglichen Entwurfszielen unterscheiden. Ein gutes Beispiel dafür stellt der Aspekt der Informations- und Datenübertragungssicherheit dar. Obwohl auf verschiedenen Ebenen des Internet mit Protokollen wie IPsec, oder Erweiterungen wie DNSSEC oder SSL Teilaspekte des Internet abgesichert werden konnten, so führt dies noch lange nicht zu einem sicheren Internet. Eine Kombination von zwei sicheren Komponenten ergibt nicht unbedingt ein sicheres System. Jedes System ist nur so sicher wie die schwächste Komponente. Tatsächlich kann das kleinste Versehen zu einem globalen Sicherheitsproblem führen, insbesondere weil erhebliche Funktionalität in anfälligen und schwer austauschbaren Ende-Systemen realisiert wurde. Letztendlich bleibt Sicherheit in einem Internet, das fundamental auf Vertrauen und Zusammenarbeit aufbaut (Design-Prinzip C), eine große Herausforderung und wird vermutlich immer ein Balanceakt zwischen Sicherheit, Leistungsfähigkeit und Benutzbarkeit bleiben.

Ähnlich kompliziert gestaltet es sich, Mobilität innerhalb der derzeitigen Internet-Architektur zu realisieren. Gegenstellen werden durch ihre IP-Adresse identifiziert (Design-Prinzip D), wobei die Hierarchie der Adressvergabe die Hierarchie der Netze widerspiegelt, um Skalierbarkeit zu erreichen (Design-Prinzip B und C), und somit die Position der Gegenstelle im Internet Teil ihrer Adresse wird. Die

meisten Vorschläge, wie man Mobilität realisieren kann, zerstören entweder diese Hierarchie, oder führen zusätzliche IP-Adressen allein zum Zwecke der Mobilität ein. Während der erste Ansatz viele Sicherheitsprobleme mit sich bringt, führt der zweite zu einer Entkopplung von Adressierung und Position im Netz und erfordert somit große Veränderungen in der Art, in der die Adressen genutzt werden.

Eingedenk der dezentralen Verwaltung des Internet (Entwurfsziel 5 / Design-Prinzip C) und des Mangels an Werkzeugen, um die Belegung bestimmter Netzwerkressourcen im Internet bestimmten Nutzern oder Anwendungen zuordnen zu können, kann das Problem des Netzwerkmanagements des Internet getrost als ungelöst bezeichnet werden. Während wir inzwischen sehr genau wissen, wie man extrem schnell Pakete auf der "Forwarding Plane" weiterleitet, ist es größtenteils noch ungelöst, wie man eine "Control Plane" konstruiert, die ein Netz so steuert, dass es zuverlässig und leicht kontrollierbar bleibt, eine leichte Fehlersuche ermöglicht, und trotzdem gut skaliert. Das Netzwerkmanagement betrifft alle Schichten des Netzes, einschließlich der politischen und wirtschaftlichen Rahmenbedingungen. Es ist ein komplexes System, das vor allem von Menschen mit großen Fähigkeiten im Umgang mit Komplexität abhängt und diese Fähigkeit voraussetzt. Die Autoren beängstigt der Gedanke an einen Ausfall von größeren Teilen des Internet, der sich nicht zeitnah beheben lässt, weil die Beteiligten sich dank VoIP und der damit verbundenen Abhängigkeit vom Internet nicht mehr zur Behebung des Ausfalls verständigen können.

Wie Dienstgüte garantiert werden kann ist als Erweiterung des Internet und Entwurfsziel für ATM-Netze (Asynchronous Transfer Mode) im

Detail untersucht worden. Trotzdem gibt es noch eine Reihe von Problemen damit, wie die verschiedenen Schichten (Design-Prinzip A), die zur Erbringung von Dienstgüteggarantien zusammenarbeiten müssen, miteinander interagieren.

Gänzlich ungeklärt ist, wie Dienstgüteggarantien über administrative Grenzen wie z.B. Providergrenzen hinweg erbracht werden können, und wie man dabei Autorisation, Strategien welche Garantien möglich sind und die Abrechnung der Dienste, realisieren kann. (Design-Prinzip B und C)

Die neuen Anforderungen in den Bereichen Sicherheit, Mobilität, der Unterstützung von garantierter Dienstgüte und die Einführung eines kontrollierten Netzwerkmanagements sind extrem schwer innerhalb des bestehenden Netzwerk-Stacks zu implementieren. In Anbetracht dessen scheint es nötig, die Design-Prinzipien zu überdenken: Ist die gewählte Schichtenarchitektur zukunftssicher? Ist Paketvermittlung wirklich für alle Dienste geeignet? Ist die Betrachtung als Netzwerk aus Netzen mit Ende-zu-Ende Kommunikation wirklich die beste Lösung für alle Anwendungen?

Stellt man so grundsätzliche Fragen, so ist es nicht möglich, die Netzwerkstruktur auf nur technischem Level zu betrachten und dabei die wirtschaftlichen und gesellschaftlichen Aspekte außer Acht zu lassen. Für die Anbieter der Netzwerkinfrastruktur, die ISPs, besteht zurzeit die wichtigste Einnahmequelle aus den monatlichen Entgelten, die der Endnutzer für den Internetzugang zahlt. Bei den Tarifen wird nicht unterschieden, ob ein Internetnutzer Daten von einem fernen Kontinent oder einem benachbarten Rechenzentrum bezieht, obwohl dies für den ISP einen gewaltigen Kostenunterschied ausmachen

kann. Besonders ungünstig ist es in dem Fall, wenn die gleichen Daten an einem näherliegenden Ort günstiger zur Verfügung stehen würden, jedoch aus einer entfernten Quelle bezogen werden.

Die Haupteinnahmequellen der Service-Provider (wie Google, Facebook, etc.) kommen aus Werbeeinblendungen und Werbeplatzierungen, sie werden also für die Augenfälligkeit der Inhalte gegenüber ihren Nutzern bezahlt. Sie wählen die Standorte ihrer Rechenzentren in der Regel nach Kosten für Energie und Kühlung aus und nicht unbedingt danach, wo sich die meisten Benutzer aufhalten. Wer die Kosten der Datenverbindung zwischen ISP und Service-Provider bzw. zwischen Nutzer und Service-Provider trägt, hängt vom Einzelfall ab und ist ein fortwährender Machtkampf.

In der Vergangenheit haben sich die als Alternative dazu gehandelten Systeme für Mikro-Zahlungen für die meisten Dienste des Internet als unwirtschaftlich oder impraktikabel herausgestellt oder wurden von den Nutzern nicht angenommen. Die Erfahrung zeigt, dass die Nutzer für die meisten Dienste Flatrates oder Abonnements bevorzugen. An eine neue Architektur wird der Anspruch gestellt, eine einfache Art des finanziellen Ausgleichs zu ermöglichen, der zum Zusammenschluss der Netzwerke passt. Es muss ein sinnvolles ökonomisches Modell für die Evolution des Netzwerks und seiner Dienste gefunden werden, das kontinuierliche Entwicklungsfähigkeit auf lange Sicht ermöglicht.

Clean-Slate

Einen Neuanfang wagen

Die Architektur des Internet, ihrer losen Kopplung der einzelnen Komponenten, hat sich in den letzten 30 Jahren als recht vielseitig erwiesen und ermöglichte einen gewaltigen kontinuierlichen Fortschritt ohne dass sich seine grundlegende Struktur weiterentwickelt hat – getreu dem Motto „*Never change a running system*“. Anforderungen, die nicht direkt in die ursprüngliche Struktur des Internet passen, wurden mit suboptimalen Hilfskonstruktionen gelöst, die der Ossifikation des Internet Vorschub leisten. Das prominenteste Beispiel dafür ist die Adressumsetzung (NAT), die dem Problem der Adressknappheit in IPv4 entgegenwirken soll, aber dabei viele neue Probleme erzeugt und Innovation erschwert. Vielversprechende Forschungsergebnisse, die einen fundamentalen Eingriff in die Struktur des Internet erfordern, wurden zurückgewiesen, da sie nicht direkt umsetzbar waren. Konfrontiert mit der ebenso gewaltigen Komplexität, die im Zuge der inkrementellen Entwicklung entstanden ist, und mit den Herausforderungen, denen das Internet schon in naher Zukunft begegnen soll, wünschen sich viele einen Neuanfang.

Sogenannte Clean-Slate-Ansätze geben die Möglichkeit, einen Neuanfang zu wagen. Fernab von den Zwängen der derzeitigen Architektur und der ihr zu Grunde liegenden, teilweise überholten Annahmen können neue Ideen realisiert, evaluiert und auf ihre Praxis-tauglichkeit überprüft werden. Die Ideen und Ergebnisse, die aus Clean-Slate-Experimenten gewonnen werden, können dann sowohl bei dem Bau neuer Systeme als auch in inkrementellen Weiterentwicklungen bestehender Systeme Verwendung finden.

Warum gerade jetzt? Für einige der aktuellen Herausforderungen, wie Mobilität oder garantierte Dienstgüte, wurden bisher keine überzeugenden Lösungen gefunden, die auf bloßer Weiterentwicklung des Bestehenden basieren. Die Verfügbarkeit optischer Switches für Glasfasernetze, neuer Funktechnologien, riesiger Rechen- und Speicherressourcen und die Erwartungen an das „*Internet der Dinge*“, dass viele Sensoren und Maschinen ins Netz integriert, legen zunehmend ein Überdenken der Entwurfsziele des Internet nahe.

Um Clean-Slate-Ansätze zu evaluieren genügt es nicht, neue Systeme rein theoretisch zu modellieren. Es ist notwendig, sie zu implementieren und in Netzen geeigneter Größe zu testen. Kleine Testbeds sind dazu nicht immer ausreichend, weshalb auf verschiedenen Ebenen größere, über viele Standorte verteilte Testeinrichtungen geschaffen wurden. Zu diesen gehören G-Lab in Deutschland, das FP7 EU-Projekt OFELIA oder das in den USA gestartete GENI-Projekt.

Es wird sich zeigen, welche der derzeit und zukünftig entwickelten Systeme und Protokolle für den Betrieb im Internet oder in größeren privaten Netzen geeignet sind oder sich integrieren lassen. Während die schleppende Einführung von IPv6 eher beängstigend wirkt, zeigt der Einsatz des aus dem Bereich Software-Defined-Networking stammenden Open Flow-Protokolls in ersten, teilweise weltweiten Netzen, wie erfolgreich Clean-Slate-Ansätze sein können.

Um ein besseres Gefühl für den Stand der Forschung und aktuelle Aktivitäten zu vermitteln, wird im Folgenden eine Einführung in die Clean-Slate-Internet-Forschung anhand einiger aktueller Beispiele gegeben.

Software Defined Networking

Das Potential der Abstraktion

Problemformulierung: Die Architektur des Internet ist ein Opfer ihres eigenen Erfolges geworden. Während das Internet wichtige Impulse für Innovation auf der Ebene der Applikationen geliefert hat, resultieren das schnelle Wachstum und die damit einhergehende Komplexität in kritischen Herausforderungen und Problemen auf operationaler Ebene. Das Anwachsen der Komplexität wird als *Internet Ossifikation* bezeichnet – die Unmöglichkeit, mit grundlegenden Protokollen und Mechanismen des Internet zu experimentieren, diese zu verändern, weiterzuentwickeln oder gar gänzlich neu zu gestalten. Sämtliche Versuche, Sicherheits-, Verfügbarkeits- und Skalierungsprobleme des Internet anzugehen, stehen der Notwendigkeit gegenüber, es permanent in Betrieb zu halten. Einige Wissenschaftler verdeutlichen dieses Problem am Beispiel eines Rennwagens, dessen Reifen inmitten eines Wettrenns gewechselt werden müssen, während er bei voller Geschwindigkeit auf der Rennstrecke fährt. In gewisser Hinsicht ist das Problem im Bezug auf das Internet sogar noch komplexer: Wenn das Internet tatsächlich ein Rennwagen wäre, dann wären die Räder nicht nur das Verbindungsstück zwischen Wagen und Straße, sondern wären zusätzlich noch mit fast jeder anderen Komponente des Rennwagens verbunden.

Ein Grund für die Internet Ossifikation ist, dass die Architektur des Internets viele komplexe Zusammenhänge zwischen den einzelnen Komponenten birgt. Durch die Evolution des Internet ist das Ausmaß der Komplexität dieser Abhängigkeiten stetig gewachsen. Dies führt dazu, dass Änderungen an einzelnen Teilen der Netzwerkarchitektur oft zu un-

vorhersehbaren (und ungewollten) Konsequenzen in anderen Teilen führen. Eine Möglichkeit, komplexe Interaktionen zu vereinfachen, ist das Konzept der Abstraktion.

Abstraktion ist ein Prozess, der komplexe Systeme verwaltet, indem die Komplexität hinter vereinfachten, standardisierten Schnittstellen verborgen wird. Beispiele für Abstraktion existieren überall in unserer Welt, nicht nur im Bezug auf Computersysteme – und wir verlassen uns auf sie jederzeit, ohne es überhaupt zu bemerken. Das Gaspedal eines Autos ist ein exzellentes Beispiel, um das Konzept (und das Potential) der Abstraktion durch Verwendung einfacher Schnittstellen zu verdeutlichen. Vergleicht man ein aktuelles Auto mit Autos aus dem frühen letzten Jahrhundert, wird schnell klar, mit wie viel Komplexität ein Fahrer damals konfrontiert war. Heutzutage können Autofahrer die Komplexität des Zusammenspiels von Benzinpumpe, Luft-Treibstoffgemisch und Öldruck getrost ignorieren. Stattdessen können sie sich auf ein einziges Pedal verlassen, um das Auto zu beschleunigen. Die Komplexität all dieser Systeme ist hinter einer einfachen Schnittstelle versteckt, einem einzigen Pedal.

In den letzten Jahren wurden einige unterschiedliche Ansätze vorgestellt, um die Ossi-fikation des Internet zu bekämpfen. Einer dieser Ansätze ist bekannt als *Software-Defined-Networking* (SDN). SDN versucht, vereinfachte und leistungsstarke Abstraktionen in die Netzwerkarchitektur einzubringen. Auf diese Weise versuchen Wissenschaftler die Komplexität der Interaktionen in der Architektur des Internets, mit welcher Netzwerkentwickler und -betreiber heutzutage konfrontiert sind, zu entwirren.

SDNs realisieren diese Abstraktion der Netzwerkkontrolle durch das Definieren einer

standardisierten, programmierbaren Schnittstelle für Netzwerkhardware. Es wurden zahlreiche Implementierungen zur Realisierung von SDNs vorgeschlagen. Allen voran hat die *OpenFlow*-Initiative der Universitäten Stanford und Berkeley aus Kalifornien viel Aufmerksamkeit erhalten und wird bereits in Universitätsnetzwerken in den USA, Europa und Asien verwendet.

Die durch SDNs erreichte Programmierbarkeit stellt einen ansprechenden Mechanismus bereit, welcher sowohl das Experimentieren, die Virtualisierung als auch die Auslegung von neuen Protokollen und Netzwerkarchitekturen im heutigen Internet ermöglicht. Diesem Mechanismus können weitere Informationen über den Datenverkehr und dem daraus resultierenden Zustand des Netzes zur Verfügung gestellt werden, um bessere Kontrollentscheidungen treffen zu können.

Die Programmierbarkeit und Abstraktion von SDNs hat es Wissenschaftlern ermöglicht, neue Ansätze zur Netzwerkkontrolle zu realisieren. Einer der aus der Abstraktion resultierenden Schlüsselfaktoren ist, dass das Netzwerk als einzelne, zentralisierte Einheit betrachtet werden kann, anstatt als eine Menge von verteilten Einheiten (vgl. Abbildung 2 und 3). Dies macht die Aufgabe der Netzwerkverwaltung und -kontrolle konzeptionell einfacher.

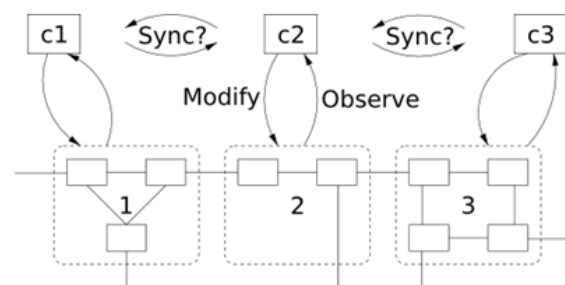


Abb. 2: Verteilte Netzwerkkontrolle

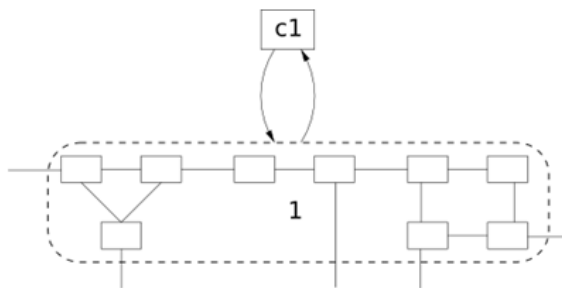


Abb. 3: Logisch zentralisierte Netzwerkkontrolle

Die Möglichkeit, Schlussfolgerungen über ein Netzwerk als einzelnes, zentralisiertes Objekt zu ziehen, ermöglicht neue Ansätze zur Fehlersuche und Fehlerbehebung. Wenn sich ein Netzwerk wie ein einzelnes Objekt verhält, ist es zudem möglich, Vorgänge im Netzwerk aufzunehmen und zu wiederholen, um Fehler zu identifizieren. Wissenschaftler haben bereits begonnen, diese zentralisierte Abstraktion auszuschöpfen, um Netzwerke zuverlässiger zu machen.

Selbstverständlich haben die Vorteile der Abstraktion auch ihren Preis. Sobald Abstraktion zur Reduzierung der Komplexität eingesetzt wird, geht ein Teil der Kontrolle über das System unwiederbringlich verloren. So könnte der Fahrer unseres Rennwagens in manchen Situationen das Bedürfnis haben, mehr Kontrolle über den Motor zu erlangen, als das Gaspedal ihm ermöglicht. Es könnte beispielsweise vorteilhaft sein, das Luft-Treibstoffgemisch – abhängig von den jeweiligen Straßenverhältnissen – manuell zu regulieren, um die maximale Leistung des Rennwagens zu erreichen.

Die gleiche Abwägung gilt auch für SDNs. Entscheidend ist, das richtige Abstraktionsniveau zu finden. Dies bedeutet, die richtige Menge an Komplexität zu exponieren, ohne dabei die Leistungsfähigkeit des Netzwerks einzuschränken. Die Einführung von Programmierbarkeit in die Netzwerkarchitektur birgt ein großes Potential für neue Ansätze

im Netzwerkdesign, wirft aber auch signifikante Fragen bezüglich der Skalierbarkeit und der Limitierungen dieser Ansätze auf.

Mit Software Defined Networking und Open-Flow gewinnen wir eine Programmierschnittstelle für Netzwerke, die uns schnelle Innovationen ermöglicht, in Unabhängigkeit einzelner Hersteller. Existierende Forschungsarbeiten beschäftigen sich hauptsächlich mit SDN-Kontrollsoftware und Anwendungen, wobei aktuell die Architektur von verteilter Kontrollsoftware im Vordergrund der Forschung steht. SDN hat bereits die reine Forschungswelt verlassen und erste produktive Einsätze gefunden, wie etwa bei Google.

Netzwerkvirtualisierung

Für jeden Zweck sein eigenes Netz statt dem Netz für alles?

Virtualisierung ist eines der zentralen Konzepte in der Informatik. Ursprünglich als Maßnahme erdacht teure Ressourcen mehr Nutzern zur Verfügung stellen zu können, kommt der Virtualisierung auch die Aufgabe zu, eine einheitliche Sicht auf verschiedenartige Ressourcen bereitzustellen oder geteilte logisch zu separieren. Beispielsweise wird der Arbeitsspeicher in heutigen Computern derart verwaltet, dass jeder Anwendung ein eigener und unabhängiger, virtueller Adressraum zur Verfügung steht. Der virtuelle Arbeitsspeicher einer Anwendung kann sich dabei auf Bereiche im tatsächlich vorhandenen Arbeitsspeicher sowie auf Bereiche in einem Hintergrundspeicher wie der Festplatte aufteilen.

Virtualisierungstechniken wie *Xen* oder *VMWare* haben maßgeblich zum Erfolg von Cloud-Computing beigetragen. Diese sogenannte Endsystem-Virtualisierung erlaubt es, virtuelle Maschinen mit variabler Speicher-

und Rechenleistung dynamisch und „on demand“ bereitzustellen. Ein sehr flexibles Ressourcenmanagement wird so möglich. Ein Infrastrukturanbieter kann die virtuellen Maschinen flexibel auf die physischen Maschinen verteilen, und somit seine physischen Ressourcen besser ausnutzen.

Aber nicht nur Clouds basieren heutzutage bereits auf Virtualisierungstechniken, sondern immer mehr auch die Verbindungen zwischen den virtuellen Maschinen, physischen Maschinen oder ganzen Standorten von Rechenzentren. Internet Service Provider (ISPs) bieten heute bereits *Virtual Private Network* (VPN) Dienste an, virtuelle Netzwerke, die transparent Standorte weltweit verbinden. Auch Provider nutzen Virtualisierungstechniken um Verkehrsflüsse immer flexibler und effizienter zu steuern. Ein weit verbreitetes Protokoll dafür ist *Multiprotocol Label Switching* (MPLS), welches es ermöglicht, festgelegte Pfade durchs Netz für bestimmte Ziele zu bestimmen. Ein solches „Traffic Engineering“ kann unterschiedlich motiviert sein und zum Beispiel zum Ausgleichen der Verkehrslast innerhalb des Netzes verwendet werden.

Der Trend zur Virtualisierung im Internet ist ungebrochen. Es ist zu erwarten, dass in der Zukunft Internet Service Provider ihre Ressourcen ähnlich flexibel verwalten, wie es heute bei Cloud-Anbietern oder in Rechenzentren üblich ist. Man wird davon ausgehen können, dass es zu einer Vereinheitlichung und Konvergenz von Endsystem- und Linkvirtualisierung kommen wird. Diese Vision wird häufig mit *CloudNets* umschrieben.

Ein CloudNet ist ein virtuelles Netzwerk, welches Ressourcen wie Speicher oder Rechenleistung miteinander verbindet. Erst die explizite Kombination und präzise Abstimmung von Knoten- und Linkspezifikationen erlaubt

es, die vorhandenen Ressourcen optimal zu nutzen. Eine Ressource in der Cloud ist wertlos, wenn der Zugriff auf sie ineffizient ist.

Das CloudNet ist ein sehr allgemeines und mächtiges Konzept. Ein CloudNet kann beliebig spezifiziert sein: Die Knoten des CloudNet können beispielsweise Standortinformation vorgeben („nur Standorte in Europa“), Ressourcen anfordern („mindestens 100 MFLOPs Rechenleistung und 1 Terabyte Speicher“), oder sich auf Technologien beschränken („nur Xen als Virtualisierungstechnik“). Analog können auch Verbindungen zwischen Standorten beschränkt („keine Route über Syrien“) und Anforderungen an sie gestellt werden („mind. 100 Mbit/s Bandbreite“). Das Ziel des CloudNet Anbieters ist es dann, das CloudNet so zu realisieren, dass all diese Spezifikationen erfüllt sind – und andernfalls muss er die Anfrage abweisen.

Die verschiedenen virtuellen Netze können dabei nicht nur gleichzeitig und unabhängig auf der Infrastruktur existieren und die physischen Ressourcen miteinander teilen, sondern auch ganz unterschiedliche Netzwerkprotokolle verwenden. Dementsprechend ist es denkbar, dass es in der Zukunft ein spezielles virtualisiertes Netzwerk für Anwendungen wie Banküberweisungen geben kann, wobei jede Aktion authentifiziert und nachvollziehbar sein muss. Ein anderes virtuelles Netz kann anonyme Kommunikationswege ermöglichen. Da beide Funktionalitäten einander ausschließen, benötigen wir die Ebene der virtuellen Netze. Andere virtuelle Netze können spezialisierte Protokolle für bestimmte Anwendungen bereitstellen, wie z.B. auf Latenz optimierte Netze für Online-Multiplayer-Spiele oder auf Durchsatz optimierte Netze für Datensicherungen. Das bedeutet nicht, dass das Internet so wie wir es kennen nicht weiter existieren wird, sondern es kann

als eines der vielen parallelen virtuellen Netze realisiert sein.

Die Vision des CloudNet motiviert viele noch unbeantwortete algorithmische, technologische und wirtschaftliche Forschungsfragen. Durch die Entkopplung von Diensten von der Infrastruktur ermöglicht es einem ISP, ganz neue Dienste anbieten. Beispielsweise könnte sich eine SAP-Instanz oder ein Spieleserver automatisch näher zum Kunden bewegen. Durch zusätzliche Berücksichtigung von Tageszeiteffekten oder Pendlerbewegungen kann damit das Verhalten von Diensten verbessert werden. Dazu ist es aber notwendig, das dynamische Management der virtuellen Netze grundlegend neu zu betrachten. Das impliziert, dass man virtuelle Netze schnell und unkompliziert erstellen, wachsen und schrumpfen lassen können muss.

Eine Herausforderung besteht darin, eine Ressourcenbeschreibungssprache zu entwickeln, die eine generische Spezifikation virtueller Netze erlaubt. Diese Sprache sollte nicht nur eine einfache Beschreibung von Ressourcen zulassen, sondern auch vage Formulierungen unterstützen, denn alles, was nicht genau spezifiziert ist, steht als Parameterraum für Optimierungen zur Verfügung. Beispielsweise kann die Auswahl der Virtualisierungstechnik der Umgebung überlassen werden. Auch muss es einem Infrastrukturanbieter möglich sein, einem CloudNet-Kunden nur gewisse abstrakte Sichten auf sein Netzwerk zu gewähren, um Geschäftsgeheimnisse wie etwa das genaue Layout seiner physischen Infrastruktur zu schützen.

Eine andere Herausforderung ist die effiziente Realisierung von CloudNet. Die flexible Spezifikation bietet Optimierungsmöglichkeiten, wo und ggf. wann ein CloudNet umgesetzt und aktiviert werden kann. Innerhalb der

Grenzen der Spezifikation soll eine transparente Migration möglich sein. Solche Optimierungen können genutzt werden, um eine größere Anzahl an virtuellen Netzen gleichzeitig zu aktivieren, um Last auf der Infrastruktur zu minimieren oder um Energie zu sparen. Während allgemeine mathematische Ansätze optimale Lösungen ergeben, ist die Berechnung leider häufig so aufwändig, dass es nötig ist, alternative Heuristiken zu erforschen.

Verschiedene Forschungsgruppen haben begonnen, erste CloudNet Prototypen zu entwickeln. Als Technik für die Knotenvirtualisierung wird vorrangig Xen oder VMWare verwendet, für die Verbindungsvirtualisierung wird auf VLANs und OpenFlow zurückgegriffen. Die existierenden Prototypen sind noch in einem frühen Entwicklungsstadium und nur schwierig an spezifische Anwendungen anzupassen. Eine Umsetzung von garantierten Diensten ist derzeit noch problematisch: Während einige Prototypen gute virtuelle Netze in der Theorie berechnen können, bleibt unklar, wie und wie schnell entsprechende Veränderungen aktiviert werden können, insbesondere in globalen Szenarien, die Providergrenzen zu überschreiten.

Trotz der vielversprechenden Vision ist heute deshalb nicht abzusehen, welche Nachteile und Risiken virtuelle Netze mit sich bringen. Falsch platzierte oder adaptive Migration virtuelle Netze können zu Instabilitäten im CloudNet führen. Es ist unbekannt, welche Informationen virtuelle Netze über die darunterliegende Infrastruktur preisgeben. Da diese Infrastruktur eine kritische Ressource des Anbieters ist, wird deren Struktur oft als Betriebsgeheimnis angesehen und soll daher verborgen werden.

Wir sind überzeugt davon, dass sich diese Herausforderungen lösen lassen, aber noch

sehr viel Forschungsarbeit erfordern. Dabei ist internationale Zusammenarbeit unverzichtbar, damit am Ende keine „Insel-Lösungen“ entstehen, die dem Grundkonzept des Internet zuwiderlaufen.

Content Centric Networks

Das Netz der Inhalte

Problemformulierung: Die Architektur des Internet wurde mit dem Ziel entworfen, Daten zwischen Knoten im Netzwerk zu transportieren. Hierbei hat das Netzwerk, vereinfacht gesagt, keinerlei Verständnis der Inhalte und der Bedeutung der Daten, die es transportiert. Insofern kann das Internet als ein Netzwerk charakterisiert werden, welches sich am "Wo?" (den Orten) orientiert und nicht mit am "Was?" (den Inhalten).

Dieses Prinzip kann am besten an einem Beispiel illustriert werden: Nehmen wir an, wir möchten einen Artikel einer Zeitung abrufen (Zugriff auf den Inhalt). Um dies zu tun, starten wir den Browser und tippen den Namen der Webseite "www.nytimes.com" in das Adressfeld ein. Nun beginnt ein komplexer Prozess: Zunächst wird der Name "www.nytimes.com" an das *Domain Name System* (DNS) übergeben, welches den Namen zu einer IP Adresse auflöst. Diese IP Adresse ist global eindeutig und gehört zu einem der zuständigen Server. Sobald der DNS Server mit der zu "www.nytimes.com" zugehörigen autoritativen IP Adresse antwortet, kann unser Betriebssystem eine Verbindung zu dieser IP Adresse aufbauen, und schließlich der Browser die gewünschten Daten herunterladen. Man sieht also: Erst nachdem wir den „Lagerplatz“ der gewünschten Daten ermittelt haben, können wir die Inhalte empfangen.

In der realen Alltagswelt gibt es oft effizientere Möglichkeiten, an eine aktuelle Zeitung zu gelangen. Hierzu müssen wir meistens nicht direkt bis zur Druckerei fahren, um sie dort druckfrisch zu beziehen. Nehmen wir an, unser Mitbewohner lässt seine Zeitung auf dem Küchentisch liegen. Vorausgesetzt, dass er uns gegenüber wohlgesonnen ist, können wir nun einfach die Zeitung aus der Küche nehmen und sie lesen. Wir müssen nicht herausfinden, wo wir die Zeitung eventuell kaufen könnten, geschweige denn das Haus verlassen und zum nächsten Ort fahren, der die gewünschte Zeitung im Angebot hat.

Das Internet ist aus Netzwerken gewachsen, dessen Nutzen pure Ende-zu-Ende Kommunikation war. Heutzutage jedoch sind die Inhalte die treibende Kraft des Internet. Internetnutzer konsumieren immer größere Datenmengen, beispielsweise Video, Dokumente oder Software. Jedoch muss der Benutzer jedes Mal zunächst spezifizieren "Von wo bekomme ich es?" bevor er schließlich auf die Inhalte zugreifen kann.

Im Gegensatz dazu ermöglicht Content Centric Networking, dass das Netzwerk selbst die Nachfrage bzw. das Verlangen nach bestimmten Inhalten ausdrücken kann, unabhängig davon, wo sich die Inhalte im Netzwerk befinden.

So könnte die Kopie vom beliebtesten YouTube-Video direkt von unseren Nachbarn kommen anstatt wiederholt weite Teile des Netzwerkes zu durchlaufen. Es könnten sogar Teile des Videos parallel von unterschiedlichen Orten bezogen werden, was die Downloadzeit weiter reduziert.

Um dieses Ziel zu erreichen, bekommt jeder Inhalt im Netzwerk seinen eigenen eindeutigen Bezeichner. Jede Kopie des jeweiligen Inhalts wird mit dem gleichen Bezeichner

versehen. Wenn wir nun also den Bezeichner für einen gewünschten Inhalt kennen, können wir die Daten von jeder bereits existenten Kopie replizieren, unabhängig davon wo sich die Kopien befinden. Im Gegensatz dazu stellt das heutige Internet keinerlei Mechanismen bereit, Inhalte direkt zu adressieren. Adressen und Namen im Internet beziehen sich nur auf Container von Inhalten – das heißt Orte, an denen gewisse Daten bezogen werden können. Dies führt zu dem Problem, dass Inhalte nur solange verfügbar sind, so lange der jeweilige Container sie bereitstellt. Jeder kennt dieses Problem: Man klickt auf einen Link zu einem älteren Blog-Artikel und muss feststellen, dass dieser nicht mehr existiert. Content Centric Networking kann dieses Problem grundlegend lösen, in dem es die Inhalte adressiert – und nicht die Container. Wenn Inhalte im Netzwerk existieren, kann auf sie über den zugewiesenen Namen zugegriffen werden – für immer.

Jedoch bergen Content Centric Netzwerke signifikante Herausforderungen, das besagte Ziel zu erreichen. Um beliebte Inhalte im Netzwerk effizient zu verwerten, müssen Router Inhalte lokal zwischenspeichern (cachen). Hierbei handelt es sich meistens um große Mengen von Daten. Darüber hinaus können die meisten Inhalte im modernen Internet nicht ohne Probleme zwischengespeichert werden (cacheability): Dynamische Inhalte, welche sich schnell verändern (beispielsweise Statusupdates in sozialen Netzen) oder Inhalte, die direkt von Nutzern erzeugt werden (z.B. Online-Banking) sind gute Beispiele dafür. Des Weiteren werfen Content Centric Netzwerke viele rechtliche und gesellschaftliche Fragen bezüglich des Eigentums und der Kontrolle der Inhalteverteilung auf.

Ob Content Centric Netzwerke angenommen werden und ob sie bis hin zur Größe des Internet wachsen werden, muss sich zeigen. Nichtsdestotrotz liefert die Forschung an diesen Netzwerken bereits wichtige Einblicke, welche in bereits existierende Netzwerkarchitekturen integriert werden können. Offene Fragestellungen im Bezug auf Content Centric Netzwerke können auch wichtige Ergebnisse für bereits existente Computernetzwerke liefern.

Content Centric Networking (CCN) ist ein fundamental neuartiger Ansatz für die Datenvermittlung im Internet. In CCN stehen Inhalte anstelle von Netzwerkadressen im Vordergrund. Es existieren Software-Umsetzungen von CCN welche derzeit in verschiedenen Netzwerkumgebungen ausgewertet werden. Aufgrund des tiefgreifenden Paradigmenwechsels ist ein Einsatz von CCN im Internet in naher Zukunft nicht zu erwarten, jedoch sind viele der Forschungsfragen, wie etwa über die Zwischenspeicherbarkeit von Inhalten, auch für unser derzeitiges Internet relevant.

Zusammenfassung

You can have both: Eat the cake and keep the recipe in mind...

Die Grenzen des technisch Möglichen im Internet sind, wenn auch noch nicht erreicht, so doch in Sichtweite geraten. Um es auf die Anforderungen der Zukunft vorzubereiten, bedarf es Umbauten, die als einfache Änderungen des Bestehenden nicht vorstellbar sind. Daher geht die Forschung von einem Clean-Slate-Ansatz aus, einer Neuentwicklung, die sich nicht mehr in die Limitierungen des „klassischen Internet“ hineinzwängen muss.

Das bedeutet aber gerade nicht „abreißen und neu aufbauen“. Das heutige Netz wird quasi die Infrastruktur des neuen bilden, ohne dabei seine Funktionsfähigkeit zu verlieren. Ein Vergleich:

Das Internet ist wie ein großes, eingeschossiges Gebäude, in dem der Platz für neue Büros langsam knapp wird, in dem es Dutzende verschiedener Wegweiser, Raumbeschriftungen, Installationen gibt. „Clean Slate“ bedeutet nun, auf dieses Gebäude ein neues, beliebig mehrstöckiges zu setzen; in diese oberen Etagen ziehen neue Firmen mit neuen Büros, aber auch alte aus dem „Basement“ werden nach und nach migrieren, bis das Erdgeschoss eines Tages nur noch den Haupteingang und die Fahrstühle in einer komfortablen Halle liefert – und die Technik-Räume, die weder die „Mieter“ noch ihre Kunden jemals betreten müssen.

Clean-Slate gibt uns den nötigen Raum, neue und alternative Denkansätze zu entwickeln, zu erproben und letztlich einzuführen. Im Zuge dessen wird selbstverständlich niemand sein bisheriges Geschäftsfeld verlieren, sondern stattdessen neue dazugewinnen.

Forschung und Industrie sind daher bereits intensiv dabei, in Projekten wie etwa GENI und OFELIA die – teils theoretischen, teils praktischen – Grundlagen der neuen Architektur zu evaluieren. Dabei finden sich auch bereits erste Umsetzungen wie beim Einsatz von OpenFlow durch Google.

Auf den wesentlichen wissenschaftlichen Kongressen und in der Forschungsförderung, z.B. in den USA, Asien und Europa, ist Clean-Slate mehr als nur ein wichtiges Thema. Es ist ein fortwährender Entwicklungsprozess – viele Forschungsfragen sind noch offen, andere werden sich ergeben, wieder andere werden ihren Weg in die nächste Generation von Netzen finden und dann von neuen Clean-Slate-Ansätzen wieder in Frage gestellt werden.

Einige der offenen Themen werden im Whitepaper „Future Internet – Beobachtungen und aktuelle Trends – Chancen und Herausforderungen“ diskutiert. Dabei handelt es sich keineswegs nur um technische Fragen – es besteht die einmalige Chance, diesmal die Technik auch an z.B. soziologischen und ökonomischen Notwendigkeiten und Wünschen auszurichten.

Literatur

D. D. Clark, „The design philosophy of the darpa internet protocols,” in Proc. ACM SIGCOMM, 1988.

C. Huitema, „Routing in the Internet“, Prentice Hall, 1999.

“Building the future internet: From fundamentals to experiments”,

<http://www.cost.esf.org/index.php?id=989>.

L. P. (Ed), “GENI design principles,” Tech. Rep. 06-08, GENI Design Document, 2006.

P. Tran-Gia, A. Feldmann, R. Steinmetz, J. Eberspächer, M. Zitterbart, P. Müller, H. Schotten, „G-Lab Phase 1 – Studien und Experimentalplattform für das Internet der Zukunft“, http://www.german-lab.de/fileadmin/Press/G-Lab_White_Paper_Phase1.pdf

„OFELIA – OpenFlow in Europe Linking Infrastructure and Applications“, <http://www.fp7-ofelia.eu/>

L. Peterson, T. Anderson, D. Blumenthal, D. Casey, D. Clark, D. Estrin, J. Evans, D. Raychaudhuri, M. Reiter, J. Rexford, S. Shenker, and J. Wroclawski, “GENI design principles”, IEEE Computer Magazine, 2006.

N. Mckeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, „OpenFlow: enabling innovation in campus networks“, ACM CCR, 2008.

A. Bavier, N. Feamster, M. Huang, L. Peterson and J. Rexford, „In VINI veritas: realistic and controlled network experimentation“, SIGCOMM Comput. Commun. Rev. 36, 4, August 2006

A. Feldmann, G. Schaffrath and S. Schmid, „CloudNets: Combining Clouds with Networking. ERCIM News, 56–57, 2012.

V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, R. L. Braynard (PARC), „Networking Named Content“, CoN-EXT 2009, Rome, December, 2009

Autorinnen und Autoren

Prof. Anja Feldmann, Ph.D., Studium der Informatik an der Universität Paderborn, danach Wechsel an die Carnegie Mellon University in Pittsburgh, wo sie 1991 den Master und 1995 den Ph.D. erwarb. Nach vier Jahren bei AT&T Labs Research folgte sie Rufen an die Universität des Saarlandes (2000) und die TU München (2002). Seit 2006 ist sie Professorin für Internet Network Architectures bei den Telekom Innovation Laboratories an der TU Berlin. Seit 2010 ist sie Dekanin der Fakultät für Elektrotechnik und Informatik an der TU Berlin. Für ihre international beachtete Arbeit erhielt Anja Feldmann 2011 den Leibnizpreis, den höchstdotierten deutschen Wissenschaftspreis.

Ariane Gintzel, TU Berlin, T-Labs; Studium der Geschichte / Deutsch auf Lehramt sowie von Kultur und Technik / Wissenschafts- und Technikgeschichte an der TU Berlin. Seit 2010 tätig für die Fakultät Elektrotechnik und Informatik der TU Berlin als Gesprächsmoderatorin und in der Planung der Masterprogramme und des Masterstudiengang "Internet Technology" der EIT ICT Labs Master School.

Philipp Schmidt, TU Berlin, T-Labs; Studium der Informatik und Mathematik an der Freien Universität Berlin mit Abschluss als Diplom-Informatiker 2009, danach wissenschaftlicher Mitarbeiter und Lehrassistent im Bereich IT-Sicherheit / Sichere Identität. Seit 2011 Dok-

torand am Lehrstuhl Internet Network Architectures bei den Telekom Innovation Laboratories an der TU Berlin. Er ist seit vielen Jahren im Vorstand eines nichtkommerziellen ISP und verfolgt seit 1996 das Internet von der operativen, wirtschaftlichen und wissenschaftlichen Seite.

Dan Levin, TU Berlin, T-Labs; Studium der Mathematik und Informatik an der University Pennsylvania mit Abschluss als BA 2004. Von 2004 bis 2007 war er als Softwareentwickler bei einem kleinen Unternehmen in Cleveland Ohio tätig. Danach erlangte er 2010 den MA in Informatik an der TU Berlin und war als Gastwissenschaftler bei Deutsche Telekom Inc., R&D Lab Los Altos, USA tätig. Seit 2011 Doktorand am Lehrstuhl Internet Network Architectures bei den Telekom Innovation Laboratories an der TU Berlin

Dr. Stefan Schmid, TU Berlin, T-Labs; Studium der Informatik/Volkswirtschaft und Doktorat im Bereich Peer-to-Peer an der ETH Zürich; Praktikum am CERN, Genf. Danach Postdoc an der TU München (Lehrstuhl Effiziente Algorithmen) und an der Uni Paderborn (Lehrstuhl Theorie verteilter Systeme).

Seit 2009 Senior Research Scientist bei Deutsche Telekom Laboratories und TU Berlin, wo er den CloudNet Prototyp mitentwickelt.

Nadi Sarrar, TU Berlin, T-Labs; seit 2009 wissenschaftlicher Mitarbeiter an der TU Berlin / T-Labs, am Lehrstuhl von Prof. Anja Feldmann. Im Herbst 2009 sowie 2010 besuchte er die T-Labs in Los Altos, Kalifornien, sowie die Universität Stanford um an der Entwicklung von OpenFlow mitzuwirken. Von 2004 bis 2009 studierte er Informatik an der TU Berlin. Während seines Studiums arbeitete er als freiberuflicher Software und Hardwareentwickler für Internet-basierte Telefonesysteme.

Rainer May, TU Berlin, T-Labs arbeitete als Wissenschaftsredakteur für deutsche Zeitschriften, bevor er Mitte der 90er Jahre komplett zur IT wechselte, als Netzwerkdesigner für Internet-Provider tätig war und seit 2000 den technischen Aufbau von Portalen wie „bild.de“ leitete. Derzeit tätig als Systemverwalter am Lehrstuhl von Professorin Anja Feldmann.

Future Internet – Beobachtungen und aktuelle Trends, Chancen und Herausforderungen

Phuoc Tran-Gia, Martina Zitterbart, Anja Feldmann, Marco Hoffmann, Peter Domschitz

Das Internet ist ein großartiges, erfolgreiches, von Menschen geschaffenes Artefakt, welches die Gesellschaft von Grund auf verändert hat. Um diese Auswirkungen zu vergegenwärtigen brauchen wir nur zu betrachten, was ein längerer Ausfall des Internet mit sich bringen würde:

(1) Einige unserer Kinder und Freunde wüssten nicht mehr, wie sie mit ihresgleichen interagieren und wie sie ihre Freizeit verbringen sollten, da sie sich zunehmend auf soziale Netzwerke, Online Spiele, YouTube und andere Onlineunterhaltungsangebote verlassen haben.

(2) industrielle Fertigungsprozesse würden zum Erliegen kommen, da die Kommunikationswege innerhalb und zwischen Firmen sich größtenteils über das Internet abspielen. Folglich würde der „just-in-time“-Bestellmechanismus nicht mehr funktionieren. Man stelle sich vor, wieder zu Fax und Telefon zurückzukehren, statt Emails oder Instant Messages zu senden. Tatsächlich aber würde keiner dieser Mechanismen zur Verfügung stehen, da Fax und Telefon mittlerweile auch über das Internet kommunizieren. Folglich würde man wieder zu Briefsendungen auf dem Postweg mit einer Zustelldauer von mehreren Tagen zurückkehren.

(3) Studenten und Wissenschaftler wüssten nicht, wie sie Publikationen, Informationen und Wissen, welche in den Wissensdatenbanken weltweit im Internet gespeichert sind, abrufen sollen.

(4) Die Steuerung kritischer Infrastrukturen wird problematisch, da sie zunehmend auf Informationen aus dem Internet basieren, um Einflussfaktoren zu gewinnen und um Kontrollinformation zu verbreiten.

Eines ist in der Entwicklung des Internet bisher konstant: der ständige Wandel. Die Nutzung hat sich von Email und FTP in den Anfangsjahren zu Web zwischen 1995 und 2000, über P2P von 2000 bis 2007 und wieder zurück zu Web geändert. Diese Veränderungen sind zum Teil von den Nutzerinteressen getrieben worden, auch von der Art und Weise, wie die Inhalte, inklusive der vom Nutzer selbst erstellten, zugänglich gemacht werden. Zudem ermöglichen Open-APIs und Open-Source-Tools den Nutzern, selbst als Entwickler von Websites und Webapplikationen tätig zu werden. Beispiele hier sind Facebook Apps oder Smartphone Apps, welche eine enorme Menge an Daten und Signalisierungsverkehr verursachen. Die Topologie des Internets unterliegt ebenfalls einer stetigen Veränderung. Anfänglich bestand das Internet aus einem einzigen Backbone, dem NSFNet, und entwickelte sich dann zur bekannten hierarchischen Struktur mit drei Ebenen (Tier-1 auf höchster Stufe bis Tier-3). Heutzutage haben Content Provider wie Google mit YouTube, CDNs, Facebook und iTunes, die Möglichkeit die Verkehrsströme im Internet zu steuern. Zusätzlich fügen die Content Provider eigene Netzressourcen hinzu, wodurch die ursprünglich hierarchische Struktur mehr und mehr eingeebnet wird.

In den Anfangszeiten wurde das Internet nur zur Kommunikation verwendet. Heutzutage wird es neben der Kommunikation auch zur Berechnung und zur Speicherung verwendet. Die normale Kommunikation wird um die Machine-to-Machine Kommunikation erweitert, z.B. in Form von Sensoren zur Erfassung und Weiterverarbeitung von Umweltdaten, wie die Luftverschmutzung. IT-Cloud Provider wie Amazon bieten neue Möglichkeiten an, indem sie Rechenleistung und Speicherkapazität zur Verfügung stellen. Doch damit nicht genug. Durch die Zusammenarbeit mit Equinix, Level 3 und weiteren, wird auch eine „on demand“ Verbindung zwischen dem Endnutzer und einer Cloud ermöglicht. Da dem Endnutzer die Daten in der Cloud ohne eine Anbindung jedoch wenig nützlich sind, sind die ISPs auf den Trend ebenfalls aufgesprungen und bauen Mikro-Datenzentren an den Netz-Aggregationspunkten auf. Die Idee dahinter ist es, dem Nutzer „on demand“ populäre Dienste mit niedriger Latenz und hoher Bandbreite anbieten zu können. Die Mikro-Datenzentren bieten dabei eine gute, skalierbare Möglichkeit, um verschiedene Dienste weltweit anzubieten, ohne Dienst-spezifische Hardware installieren zu müssen. Nichtsdestotrotz nimmt die „Human Computation“ im Zusammenhang mit Crowdsourcing einen immer größeren Stellenwert ein und bildet „menschliche Cloud Computing Plattformen“, die wiederum eine Schnittstelle zu Machine-Clouds benötigen. Aus dem Grunde kann man zwei gegensätzliche Trends beobachten: Auf der einen Seite neigen Firmen dazu sich immer weiter abzuschirmen, um den Einfluss von Mitbewerbern zu minimieren und möglichst viele Kunden an sich zu binden. Auf der anderen Seite bauen ISPs und CDNs Infrastrukturen auf, die zu einem flexiblen System kombiniert werden können. Zusätz-

lich überwachen sie noch netzwerkspezifische Dienste, wie IPTV. Wie die Kommunikation zwischen diesen Systemen ermöglicht werden soll und dabei gleichzeitig exzellente Dienste bereit zu stellen ermöglicht, ist beides – eine große Herausforderung als auch eine große Chance. Tatsächlich werden in der Zukunft Dienste höchstwahrscheinlich innerhalb dienstspezifischer CloudNets verwirklicht werden: Virtuelle Netzwerke, die Human und Machine-Clouds mit Netzwerken kombinieren und alle Typen von Ressourcen anbieten: Speicher, Rechenkapazität und Kommunikation. Durch die Unabhängigkeit vom physikalischen System des zugrundeliegenden Substrate-Netzes können virtuelle Netze und CloudNets, ähnlich zu Cloud Ressourcen, dynamisch vergrößert oder verkleinert und optimal platziert und ggf. migriert werden. Virtualisierung bietet hier vielfältige Möglichkeiten. Obwohl CloudNets die gleichen Substratnetze verwenden und somit die vorhandenen Ressourcen gut auslasten, können CloudNets über andere Netzwerkprotokolle (jenseits von IP) miteinander kommunizieren, die speziell für die Anwendung zugeschnitten sind (z.B. live streaming). Die Möglichkeit des Re-Engineering des Protokollstacks könnte ein Motor für Innovationen sein. Die Chance den Protokollstapel umzuarbeiten, kann ein Antrieb für Innovationen sein. Folglich können Cloud-Netze aktuelle Einschränkungen von IP bewältigen und es ermöglichen, neue Funktionalitäten im Core Netz einzuführen.

Am Anfang war das Internet nur ein drahtgebundenes Kommunikationsmedium. Heutzutage geht es mehr darum überall Internetzugang zu bekommen. Allerdings sind die drahtgebundenen und drahtlosen Netze zu meist physikalisch separiert und werden auch getrennt verwaltet, was den universellen Zu-

gang verhindert. Zusätzlich sind die drahtlosen Ressourcen sehr rar. Das aktuelle Netzdesign berücksichtigt nicht, welche Dienste mit welchen Anforderungen auf dem Netz laufen. Diese von den Anwendungen unabhängige Netzdimensionierung führt unter anderem zu anhaltender Überlast, einem Verkehrsungleichgewicht und Sicherheitsmängeln. Zusätzlich gehen die meisten Applikationen davon aus, dass das Netz allseits verfügbar ist mit allen nötigen Funktionalitäten und Qualitätsansprüchen (QoS/QoE). Zurzeit werden die beiden Aufgaben „Netzwerkdimensionierung und Bereitstellung“ und „Anwendungsentwicklung“ getrennt bearbeitet. Dies führt zu Netzausfall (z.B. NTTs Ausfall in Tokio im Januar 2012), verursacht durch netzwerkunbewusstes Anwendungsdesign. Solche netzwerkunbewussten Anwendungen sind in der Regel egoistisch und führen zu einem hochgradig dynamischen Systemüberlastungsmuster und Verschwendung von Ressourcen (z.B. Skype). Dies ist besonders kritisch für den effizienten Gebrauch der begrenzten drahtlosen Netzwerkkapazität. Eine Möglichkeit wäre der gleichzeitige Gebrauch verschiedener drahtloser und drahtgebundener Technologien (z.B. WiFi, 3G/4G,...). Die flexible Nutzung von vorhandenen Ressourcen oder der gleichzeitige Gebrauch („Resource Pooling“), um höhere Ausfallsicherheit oder Kapazität zu erreichen, erlaubt eine effiziente Nutzung der begrenzten drahtlosen Ressourcen.

Das Internet beruht auf Zusammenarbeit und setzt voraus, dass alle Nutzer sich im Sinne der Gemeinschaft verhalten. Dies hat am Anfang auch wunderbar funktioniert, als das Internet hauptsächlich von Wissenschaftlern genutzt wurde. Leider ist die Annahme der Zusammenarbeit im Allgemeinen nicht länger gegeben. Vielmehr haben die Nutzer ver-

schiedene Bedürfnisse und „Begriffe“ für Sicherheit. Während einige Anwendungen eingebaute Sicherheitsfeatures bereitstellen (z.B. Verschlüsselung innerhalb von Skype), könnte solche Software durch Programmierfehler beeinflusst, durch einen Angreifer gefährdet, oder durch den Endnutzer verändert werden. Solche starren Sicherheitsmuster bringen nicht nur Vorteile, sie verursachen auch zusätzliche Last, verwirren nutzerbasierte Dienste und könnten den Verdacht erregen, dass etwas illegales oder wichtiges versteckt werden soll. Eine Lösung ist „Security-on-demand“, was bedeuten würde, dass es dem Nutzer bzw. der Applikation überlassen wird, ob und in welchem Maße die Daten verschlüsselt werden. Dies kann zu einer flexiblen, anwendungsunabhängigen „on-demand“-Sicherheit führen, in Form eines Provider-basierten VPN-ähnlichem Dienstes. Um Sicherheitsbedenken aus dem Weg zu räumen, könnte die Infrastruktur solcher Dienste dynamisch in einer vertrauenswürdigen Netzwerk-Cloud betrieben werden.

Teil des Erfolges des frühen Internets war, dass es sich auf laufenden Code und grobe Übereinstimmung verlassen hat. Die Tatsache, dass Open Source Software einen integrierten IP Stack beinhaltet, machte das Internet attraktiv und führte zu vielen Vorschlägen, wie man die Basistechnologie verbessern könnte. Unglücklicherweise ist die Situation heute nicht mehr so einfach, da die Performance-Anforderungen bei 100 Gigabit bis 1 Terabit pro Sekunde, speziell im Core Netz, eine kundenspezifische Hardwarelösung erfordern. Vielmehr hat dies zu spezialisierten Hardware- und Softwarelösungen geführt, die als „closed-box“ Lösungen in Form von Routern und Switches im Internet verbaut wurden. Dies ist der Hauptgrund für die Ossifikation des jetzigen Internets. Software-Defined

Networking ist eine Möglichkeit, um dieses Problem anzugehen. Eines der Schlüsselkonzepte des Software-Defined-Networking ist es eine programmierbare Schnittstelle zu den Switches und drahtlosen Zugangspunkten zur Verfügung zu stellen. Software-Defined-Networking ermöglicht das Aufsetzen von virtuellen Netzen, die Realisierung von Overlay-Netzen, die Implementierung neuer Loadbalancing Szenarien, die Überarbeitung der Verkehrsflusssteuerung, etc. Mit OpenFlow ist eine erste Implementierung dieser Idee nun verfügbar. Software-Defined-Networking kann uns erlauben zukünftige Herausforderungen anzugehen, in dem es uns ermöglicht die Internet Kontrollarchitektur – das Network-OS – als Open Source Software neu zu gestalten.

Zusammenfassend lässt sich sagen, dass in den nächsten drei bis fünf Jahren folgende Forschungsherausforderungen adressiert werden müssen, mit den Möglichkeiten, die uns die Virtualisierung, das Software-Defined Networking, als auch das Content-Centric Design bereitstellen:

- Design und Realisierung eines Open Source Netzwerk OS
- Einrichten/ Gründung einer Community, um das Open Source Netzwerk OS aufrecht zu erhalten und weiter zu entwickeln
- Bereitstellung einer integrierten und flexiblen Architektur für einen gemeinsamen drahtgebundenen und drahtlosen Netzzugang
- Ermöglichung netzwerkbewusster Anwendungen, die die begrenzten Ressourcen effizient nutzen und gleichzeitig anwendungsorientierte Netzwerke ermöglichen

- Kontrolle des Zusammenspiels von Anwendungen und Netzwerk im Hinblick auf den Trade-Off zwischen QoE und Kosten (bezogen auf Energieeffizienz, CAPEX, OPEX,...)
- Integration von Kommunikation, Rechenleistung, und Speicher, um die Content-Centric Netzwerke zu unterstützen
- Unterstützung von „on-demand“-Services mit ISP-Hoster Kommunikationsinterfaces, um das Content und Kommunikationssysteme zu verbinden
- Unterstützung virtueller Netzwerke, welche dynamisch wachsen, schrumpfen und den Anforderungen folgen
- Ermöglichung von Security „on-demand“ genauso wie neue Monitoring-Möglichkeiten für QoE Unterstützung

Autorinnen und Autoren

Prof. Dr.-Ing. Phuoc Tran-Gia, Lehrstuhl für Kommunikationssysteme an der Julius-Maximilians-Universität Würzburg

Prof. Dr. Martina Zitterbart, Professorin für Informatik am Karlsruher Institut für Technologie (KIT).

Prof. Anja Feldmann, Ph.D., Professorin für Internet Network Architectures bei den Telekom Innovation Laboratories an der TU Berlin.

Marco Hoffmann, Nokia Siemens Networks GmbH & Co. KG

Peter Domschitz, Alcatel-Lucent Deutschland AG, Bell Labs



Alcatel-Lucent
Stiftung für
Kommunikations-
forschung

Alcatel-Lucent Stiftung

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine gemeinnützige Förderstiftung für Wissenschaft insbesondere auf allen Themengebieten einer „Informationsgesellschaft“, neben allen Aspekten der neuen breitbandigen Medien speziell der Mensch-Technik-Interaktion, des E-Government, dem Medien- und Informationsrecht, dem Datenschutz, der Datensicherheit, der Sicherheitskommunikation sowie der Mobilitätskommunikation. Alle mitwirkenden Disziplinen sind angesprochen, von Naturwissenschaft und Technik über die Ökonomie bis hin zur Technikphilosophie.

Die Stiftung vergibt jährlich den interdisziplinären „Forschungspreis Technische Kommunikation“, Dissertationsauszeichnungen für WirtschaftswissenschaftlerInnen sowie Sonderauszeichnungen für herausragende wissenschaftliche Leistungen.

Die 1979 eingerichtete gemeinnützige Stiftung unterstützt mit Veranstaltungen, Publikationen und Expertisen ein eng mit der Praxis verbundenes pluridisziplinäres wissenschaftliches Netzwerk, in dem wichtige Fragestellungen der Informations- und Wissensgesellschaft frühzeitig aufgenommen und behandelt werden.

www.stiftungaktuell.de

Kontakt

Alcatel-Lucent Stiftung
Lorenzstraße 10, 70435 Stuttgart
Telefon 0711-821-45002
Telefax 0711-821-42253
E-Mail office@stiftungaktuell.de
URL: <http://www.stiftungaktuell.de>