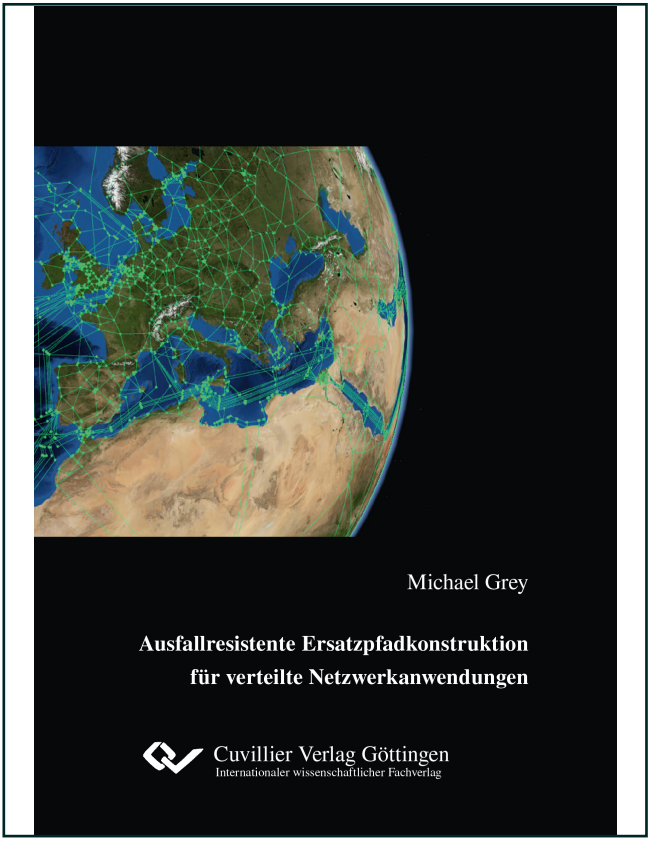
Michael Grey (Autor)

Ausfallresistente Ersatzpfadkonstruktion für verteilte Netzwerkanwendungen



https://cuvillier.de/de/shop/publications/8248

Kapitel 1

Einleitung & Motivation

Die wachsende Nachfrage nach permanentem Zugriff auf Informations- und Kommunikationsangebote führte im Laufe der letzten Jahre und Jahrzehnte zu einem stetig steigenden Bedarf nach weiträumiger und möglichst unterbrechungsfreier Vernetzung. Eine zentrale Rolle nimmt dabei das Internet ein, welches sich heutzutage als globale Plattform für Kommunikationsdienste etabliert hat.

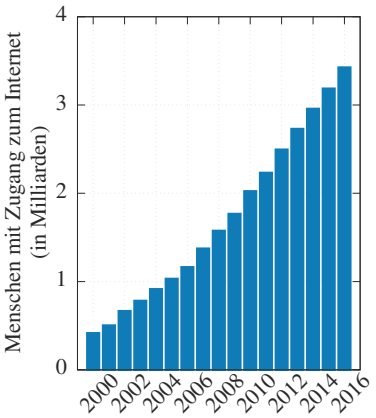


Abbildung 1.1: Statistik zur globalen Anzahl von Menschen mit Zugang zum Internet. Auswertung auf Basis von Daten der *International Telecommunication Union*, der *Weltbank* und der *United Nations Population Division*. [Int17]

Abseits der altbekannten Web-Applikationen werden angesichts der Kosteneffizienz von Internet-basierter Vernetzung dabei bereits seit einigen Jahren Anwendungen über die Internet-Infrastruktur betrieben, welche hohe Ansprüche an deren Zuverlässigkeit stellen. Ein anschauliches Beispiel hierfür sind die verschiedenen Telepräsenz-Anwendungen, welche inzwischen sogar zur aktiven Unterstützung und Durchführung medizinischer Eingriffe verwendet werden. Die zunehmende Abbildung anspruchsvoller Dienste verdeutlicht sich aber auch anhand der Strategien zahlreicher Unternehmen und Behörden, welche ihre privaten und internen Kommunikationsanliegen inzwischen immer häufiger über diese Infrastruktur abwickeln. Aktuelle Trends, wie beispielsweise die flächendeckende Vernetzung von Industrieanlagen im Rahmen von Industrie 4.0 oder das gerne zitierte *Internet-of-Things*, stärken dabei den Eindruck, dass die Bedeutung von Internet-basierter Vernetzung und die hieran geknüpften Anforderungen auch in Zukunft wachsen.

Dass die zugrundeliegende Infrastruktur des heutigen Internets diesen Anforderungen nicht immer gerecht wird, zeigt sich insbesondere im Angesicht korrelierter Ausfälle und wird bereits durch die Auswirkungen verschiedener öffentlichkeitswirksamer Katastrophen der jüngeren Vergangenheit verdeutlicht: Von den großen Erdbeben in Taiwan, Japan oder Nepal [Und07, CPBW11, PH16] über die Hurrikans Harvey und Irma [Bel17] bis hin zu den Anschlägen auf das World Trade Center am 11. September 2001 [OC02] – immer wieder waren

neben den unmittelbaren, verheerenden Auswirkungen auch weiträumige Konnektivitätsverluste in der Netzwerkinfrastruktur zu beobachten.

Verstärkt wird dieser Eindruck durch technische Zwischenfälle, wie den vielfach zitierten, kurzzeitigen Ausfall des Videodienstes *YouTube* durch falsch annoncierte Pfade im Jahr 2008 [Bro08] oder die irrtümliche Annoncierung von rund 37.000 IP-Subnetzen durch einen kleineren chinesischen Provider [Too10] im April 2010. Bis heute treten Beeinträchtigungen durch falsche Annoncierungen in aller Regelmäßigkeit auf, öffentlich bekannt gewordene Störungen aus dem Jahr 2018 betrafen unter anderem die Autonomen Systeme (AS) von *Google* [Nai18], *Amazon* [Goo18] und des Messengers *Telegram* [O'N18]. Genauere Untersuchungen (unter anderem durch *Renesys* [Ren19]) machen dabei deutlich, dass vergleichbare Ereignisse durchaus häufiger zu beobachten sind. Diese Vorfälle sind grundsätzlich auf das Fehlen von Robustheitseigenschaften im Inter-Domain-Bereich zurückzuführen und bestätigen dabei nicht zuletzt die prinzipielle Fehleranfälligkeit und Fragilität des BGP-basierten Routings, insbesondere hinsichtlich des verbreiteten Einsatzes von Routing-Policies. Weitere Brisanz erhält dieser Umstand dabei schließlich durch die Existenz gezielter Angriffe, wie das Umleiten von Netzwerkverkehr durch kompromittierte BGP-Speaker [ND04], welche weitreichende Instabilitäten erzwingen können. Bereits im Jahr 2009 wurde auf einer einschlägigen Sicherheitskonferenz ein praxisrelevantes Angriffsszenario auf das Inter-Domain-Routing demonstriert [PK09].

Ein, insbesondere für kritische Applikationen notwendiges, hohes Verfügbarkeitsniveau kann damit zumindest im öffentlichen Weitverkehrsbereich in der Regel nicht sichergestellt werden.

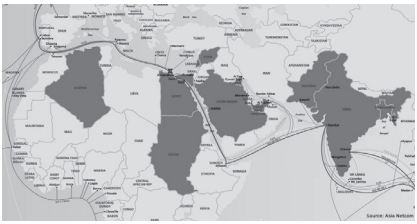


Abbildung 1.2: Charakteristik eines Ausfalls: Nachdem im Jahr 2008 zwei Unterseekabel ausfallen, welche den Mittleren Osten mit Indien verbinden, bricht die Konnektivität unter anderem in weiten Teilen von Ägypten und Indien zusammen (stark betroffene Länder sind dunkel hervorgehoben). Die Ursache des physikalischen Ausfalls ist bis heute nicht geklärt. [Zmi08]

Die grundsätzliche Verlässlichkeit der Internet-basierten Kommunikation durch umfängliche Protokollanpassungen zu steigern, ist darüber hinaus aus heutiger Sicht nicht vorstellbarer. Das Internet im Sinne seiner ursprünglichen Konzeption als *Netzwerk-Middleware*, welche beliebigen Applikationen eine Transportfunktionalität zur Verfügung stellt, gleicht durch zahlreiche Anpassungen heute sprichwörtlich einem Flickenteppich, welcher konzeptionelle Anpassungen nahezu unmöglich macht. Die bis heute schleppende Einführung des erstmals 1990 standardisierten IPv6 ist hierfür nur ein Beispiel. Verschiedenste Projekte, welche im Kontext der Begrifflichkeit *Future Internet* genannt wurden, konnten dementsprechend auch keine praktisch relevanten Ergebnisse vorweisen.

Da eine wesentliche Änderung dieser Ausgangssituation in absehbarer Zeit nicht zu erwarten ist, muss eine realistische Absicherung kritischer Verbindungen mit dem vorhandenen Funktionsumfang auskommen. Die Einrichtung von Transportnetz-Ersatzpfaden für kritische Verbindungen ist hierbei ein vielversprechendes Mittel, um die Ausfallsicherheit auf Ende-zu-Ende-Verbindungen zu erhöhen. Aber auch entsprechende Ersatzpfade, welche durch proaktive Einrichtung effektiv vor Konnektivitätsverlusten schützen können, sind mittels

Transportnetzfunktionalitäten der Zwischensysteme in absehbarer Zeit nicht seriös realisierbar. Konzeptionell verbleibt daher mit Blick auf die Umsetzbarkeit lediglich die Möglichkeit, die Intelligenz der Endsystemen an den Netzrändern zu nutzen, um die Ausfallsicherheit von Verbindungen zu erhöhen.

In Hinblick auf verteilte Anwendungen eröffnet sich an dieser Stelle durch die Einführung von logischen Topologien über dem Transportnetz, welche gezielt überwacht und verwaltet werden können, ein Ausweg. Da Routing-Entscheidungen innerhalb dieser logischen Topologien nicht den Einschränkungen der Transportnetzpfadwahl unterliegen, sind indirekte Alternativen zu den direkten Transportnetzpfaden zwischen zwei Knoten denkbar, welche im Fehlerfall verwendet werden können. Der zusätzliche Aufwand, der mit der Konstruktion und Verwaltung solcher logischen Topologien einhergeht, wird allerdings häufig als nicht zumutbar erachtet.

1.1 Problemstellungen & Beiträge der Arbeit

Um diese Aufwände zu minimieren, und damit einen Einsatz in großen Szenarien sowie eine effiziente Planung von Ersatzpfaden zu ermöglichen, wurde im Verlauf des hier vorgestellten Dissertationsvorhabens ein positionsbasierter Ansatz bereits früh als vielversprechend angesehen. Ausschlaggebend war dabei nicht zuletzt die Erkenntnis, dass kritische Ausfälle in Weitverkehrsnetzen (als Resultat von Naturkatastrophen, terroristischen Aktionen oder gezielten Angriffen auf die Infrastruktur) in der Regel eine geographisch korrelierte Wirkung aufweisen.

Allerdings stellt die heutige Weitverkehrsinfrastruktur grundsätzlich keine Mechanismen zur Erfassung und Verwendung der tatsächlichen Positionen von Infrastrukturkomponenten zur Verfügung. Zum einen ist dies bereits durch technische Limitierungen begründet, da eine solche Auswertung für Endsysteme in den heutigen Protokollimplementierungen nicht direkt vorgesehen ist. Zum anderen behandeln die Internet-Service-Provider aufgrund wirtschaftlicher Interessen und aus Sicherheitsgründen ihre Topologieinformationen in der Regel vertraulich und haben dementsprechend kein Interesse, exakte Positionen der Infrastrukturkomponenten zu veröffentlichen.

Vor diesem Hintergrund wurden im Rahmen dieser Arbeit zunächst die Anforderungen an ein System zur Steigerung der Ausfallresistenz verteilter Applikationen formuliert. Ein systematischer Abgleich mit dem aktuellen Stand der Technik verdeutlichte in der Folge, dass die derzeit bekannten Verfahren weder die gewünschte Ausfallresistenz erzielen können noch Mechanismen für eine effiziente Planung von Ersatzpfaden bereitstellen.

Unter Berücksichtigung dieser Ausgangssituation wurde schließlich ein eigenes Verfahren entwickelt, welches einen skalierbaren Ersatzpfadmechanismus für verteilte Applikationen mit einer Vielzahl von Teilnehmern bereitstellt. Das Verfahren umfasst dabei folgende Teilaspekte, welche auch als wesentliche Beiträge dieser Arbeit angesehen werden können:

- **Positionsschätzung** Da in praktisch relevanten Netzwerkinfrastrukturen üblicherweise keine verlässlichen Positionsinformationen für Transportnetzpfade zur Verfügung stehen, rücken die Positionen von Endsystemen in den Fokus, um das geplante Vorgehen zu ermöglichen. Exakte Positionen sind dabei üblicherweise nur für wenige Endsysteme verfügbar: Aus Gründen der Kosten- und Energieeffizienz werden nur wenige stationäre

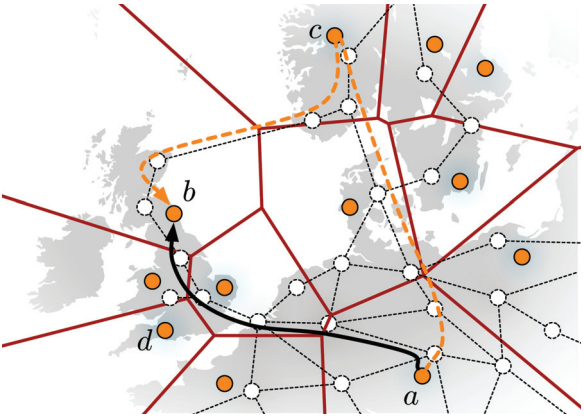


Abbildung 1.3: In praktischen Szenarien können dedizierte Transportnetzverbindungen von einer Vielzahl von logischen Overlay-Verbindungen verwendet werden. In Folge eines Ausfalls der Transportnetzverbindung zwischen *a* und *b* ist ein indirekter Overlay-Pfad über *c* vielversprechend. Ein Pfad über Knoten *d* führt hingegen nicht zu einer Wiederherstellung von Konnektivität. Durch die Voronoi-basierte Strukturierung des Overlays anhand geographischer Positionen wird eine effiziente Suche nach sinnvollen Ersatzverbindungen ermöglicht.

Systeme mit Global Positioning System (GPS)-Empfängern ausgerüstet, wobei die eingeschränkte Signalverfügbarkeit in Gebäuden ohnehin häufig einem Einsatz von satellitengestützter Positionierung entgegensteht. Alternative Ansätze, welche beispielsweise über WLAN Basic Service Set Identifications (BSSIDs) oder eine Auflösung von IP-Adressen Rückschlüsse auf geographische Lokationen erlauben, verwenden im Wesentlichen zentrale Datenbankdienste und erweisen sich im Resultat als vergleichsweise ungenau.

Im Rahmen dieser Arbeit wird daher ein Verfahren vorgestellt, in welchem alle teilnehmenden Endsysteme auf einer Sphärenoberfläche eingebettet werden, wobei die lokalen Positionsfehler mithilfe iterativ ausgeführter Multilateration auf Basis von Paketlaufzeiten minimiert werden. In der Folge wird aufgezeigt, dass mit diesem verteilten Verfahren Endsystem-Positionen für alle Systemteilnehmer effizient geschätzt werden können, sofern ein ausreichendes Maß an Positionsinformationen im gesamten Netzwerkverbund vorhanden ist.

- **Voronoi-basierte Organisation** Um eine effiziente Planung und Kontrolle von Ersatzpfaden zu ermöglichen, ist zunächst eine strukturierte Organisation der Teilnehmer notwendig. Da der Stand der Technik und insbesondere die prominenten Verfahren auf Basis eindimensionaler, verteilter Hashtabellen hierbei keine zufriedenstellende Lösung bieten, wurde im Rahmen dieser Arbeit ein vollständig verteilter, positionsbasierter Ansatz verfolgt, um den Anforderungen der Ersatzpfadplanung gerecht zu werden.

  Wie in Abbildung 1.3 angedeutet, werden Teilnehmer dabei auf Grundlage der ermittelten, aktuellen Positionen in einem Overlay-Netz organisiert. Die entwickelte Technik

basiert dabei auf einer sphärischen Voronoi-Struktur, welche die zusätzlichen Aufwände im Vergleich zu bestehenden Verfahren minimiert.

- **Ersatzpfadplanung** Auf Basis der verteilten Overlay-Struktur wird schließlich eine verteilte Methode zur proaktiven Planung von Ersatzpfaden vorgestellt. Hierbei werden Hilfsmittel der Sphärengeometrie verwendet, um eine hohe Ersatzpfadgüte bei vernachlässigbarer Zusatzbelastung der Teilnehmer durchzusetzen.

Das entstandene Verfahren wurde im Rahmen dieses Dissertationsvorhabens als Erweiterung eines Autokonfigurationsverfahrens für Virtual Private Networks (VPNs) umgesetzt. Diese Erweiterung wird im weiteren Verlauf als Outage Resilient Backup-Path System (ORB) bezeichnet. Neben einer prototypischen Realsystemimplementierung, welche einen Einsatz im globalen Forschungsnetz *PlanetLab* [CCR+03] erlaubt, wurden die wesentlichen Verfahrensbestandteile darüber hinaus auch auf Basis einer Simulationsumgebung umgesetzt. Auf Grundlage von Daten aus einer realen Umgebung kann hierdurch eine detaillierte Evaluierung des Verfahrens erfolgen, insbesondere in Hinblick auf Szenarien mit großen Teilnehmerzahlen.

1.2 Aufbau der Arbeit

Entsprechend der angestrebten Zielsetzung wurde die vorliegende Arbeit in acht Kapitel gegliedert.

Im folgenden Kapitel 2 werden zunächst einige Grundlagen beleuchtet, welche im weiteren Verlauf der Arbeit von Relevanz sind. Dies umfasst eine kurze Charakterisierung der heutigen Internet-Infrastruktur, relevante Problemstellungen der algorithmischen Geometrie, die verwendeten Methoden der Cluster-Analyse, sowie einen kurzen Überblick über sphärische Trigonometrie. Abschließend wird ein kurzer Einblick in verteilte Netzwerkkoordinatensysteme bereitgestellt.

Im darauf folgenden Kapitel 3 werden funktionale und nicht-funktionale Anforderungen an das Gesamtsystem zusammengefasst. Anschließend werden ausgewählte, relevante Arbeiten zum vorliegenden Thema präsentiert und hinsichtlich der formulierten Anforderungen bewertet.

Im Rahmen von Kapitel 4 wird ein Systementwurf zur robusten, verteilten Positionsschätzung von Knoten in globalen Netzen eingeführt. Zunächst wird dabei das Basisverfahren vorgestellt, welches lokale Optimierungen auf Basis von Paketverzögerungen verwendet, um die zunächst unbekannten Positionen zu schätzen. Anschließend wird auf zusätzliche Techniken eingegangen, welche die erreichte Genauigkeit des Verfahrens in globalen Szenarien erhöhen.

Daran anknüpfend, wird schließlich in Kapitel 5 das System zur ausfallresistenten Konstruktion und Verwaltung von Ersatzpfaden präsentiert. Dieses verwendet einen Voronoi-basierten Ansatz zur Organisation von Teilnehmern, welcher zunächst thematisiert wird. Anschließend wird auf die sinnvolle Auswahl geographischer Ersatzpfade sowie deren Einrichtung und Verwaltung eingegangen.

Mit Blick auf die Evaluierung werden in Kapitel 6 ausgewählte Implementierungsdetails zu den, in den vorangegangenen Kapiteln vorgestellten, Verfahrensbestandteilen vorgestellt.

Darüber hinaus werden die Interaktion mit der PlanetLab-Infrastruktur als Plattform für Realsystem-Experimente und wesentliche Modelle für die Durchführung simulativer Experimente adressiert. Hervorzuheben ist dabei ein im Rahmen dieser Arbeit entstandener Topologiegenerator zur synthetischen Erzeugung physikalischer Infrastrukturmodelle.

Eine qualitative und quantitative Evaluierung der vorgestellten Verfahren wird schlussendlich in Kapitel 7 vorgestellt, bevor die Arbeit mit einem kurzen Resümee in Kapitel 8 schließt.

Kapitel 2

Grundlagen

Im Rahmen dieses Kapitels werden die für den weiteren Verlauf dieser Arbeit relevanten Grundlagen vorgestellt. In den folgenden Abschnitten wird dazu zunächst kurz auf das Routing im heutigen Internet eingegangen. Anschließend werden die im Rahmen dieser Arbeit verwendeten Strukturen der algorithmischen Geometrie vorgestellt, bevor ein Überblick über die eingesetzten Methoden der Clusteranalyse gegeben wird. Daran anknüpfend, werden relevante Methoden der sphärischen Geometrie eingeführt. Zum Abschluss wird auf die Grundzüge sogenannter verteilter Netzwerkkoordinatensysteme eingegangen.

Allgemeine Informationen zu IP-Netzwerken und Routing können bei Bedarf unter anderem [KR12] und [TW13] entnommen werden.

2.1 Charakteristika des heutigen Internet-Routings

Ein bekanntes Zitat aus der Literatur beantwortet die Frage nach dem grundsätzlichen Wesen der Internet-Infrastruktur mit einem abstrakten Zusammenhang: *Das Internet ist ein Netzwerk aus Netzwerken [KR12].*

Im Sinne eines globalen Systems besteht das heutige Internet dabei tatsächlich aus unabhängig agierenden *autonomen Systemen (AS)*, welche unter administrativer Kontrolle der jeweiligen Betreiber stehen. Dabei werden Endsysteme und ihre Zufgriffsnetze an den *Rändern* des Internets über verschiedene Hierarchieebenen untereinander verbunden.

Autonome Systeme sind hierbei hierarchisch kategorisierbar. Während die relativ kleine Anzahl der *Tier-1*-Systeme an der Spitze dieser Hierarchie steht und den Kern des Internets bildet, sind die Zugriffsnetze dem Ende der Hierarchie zuzuordnen. In Abbildung 2.1 ist diese Hierarchiestruktur schematisch dargestellt, die kleine Gruppe der darin dargestellten und bereits erwähnten Tier-1-Systeme wird häufig auch als *Backbone* des Internets bezeichnet.

Das Routing innerhalb eines autonomen Systems, im sogenannten *Intra-AS*-Bereich, obliegt der alleinigen Verantwortung des jeweiligen AS-Betreibers. Ein populäres Beispiel für die in diesem Bereich eingesetzten *Interior-Gateway*-Protokolle ist *Open Shortest Path First (OSPF)* [Moy98]. Innerhalb autonomer Systeme kommen dabei in der Praxis auch Architekturen auf Basis von *Multiprotocol Label Switching (MPLS)* [RVC+01] zum Einsatz, beispielsweise um dem Netzbetreiber gezielte Pfadplanung für die, auf der Netzebene eigentlich verbindungslose, Kommunikation zu ermöglichen. Moderne Architekturen in diesem Kontext werden darüber hinaus heutzutage häufig durch Lösungen komplementiert, welche im weitesten Sinne dem Sammelbegriff Software-defined Networking (SDN) zugeordnet werden können. Unter

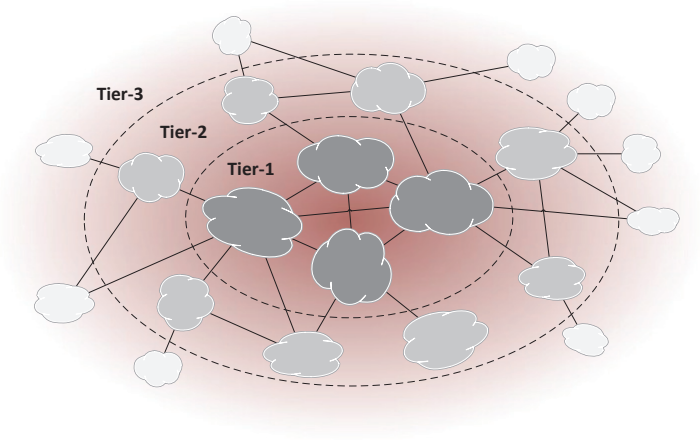


Abbildung 2.1: Hierarchische Struktur der autonomen Systeme.

Zuhilfenahme von Protokollen zur intelligenten Pfadberechnung, wie beispielsweise dem Path Computation Element Communication Protocol (PCEP) [CMMV17], wird die verteilte Kontrollebene des Netzwerks dabei üblicherweise durch zentrale Steuerinstanzen mit einer vollständigen Sicht auf alle relevanten Netzwerkelemente ergänzt, wodurch unter anderem ein effizientes, dynamisches Ressourcenmanagement ermöglicht wird.

Zum Austausch von Routing-Informationen zwischen autonomen Systemen wird in der heutigen Praxis ausschließlich das *Border Gateway Protocol (BGP)* in Version 4 [RLH06] eingesetzt. Entsprechend des Einsatzgebietes im Inter-Domain-Bereich, wird BGP üblicherweise den sogenannten *Exterior-Gateway*-Protokollen zugeordnet.

BGP ermöglicht dabei Inter-Domain-Routing auf Basis von *Policies*, welche die wirtschaftlichen Beziehungen zwischen autonomen Systemen abbilden können. Abgesehen von diesen spezifisch konfigurierten Policies setzt das Protokoll ein Shortest-Path-Routing in Bezug auf die Pfadlänge um. Informationen, die zwischen verschiedenen autonomen Systemen ausgetauscht werden, sind im Allgemeinen gefiltert und aggregiert. Somit trägt auch das Border Gateway Protocol einen Teil zur insgesamt hohen Skalierbarkeit des Internets bei.

2.1.1 Bekannte Schwächen des Inter-Domain-Routings

Allerdings behandelt das auf BGP basierende Inter-Domain-Routing nicht alle Situationen zufriedenstellend. In Bezug auf die Stabilität von Netzwerkpfaden können dabei folgende Problemgruppen unterschieden werden, die mit der Benutzung von BGP einhergehen:

Verzögerte Konvergenz
: BGP benötigt unter Umständen relativ lange, bis es nach einem Pfadausfall zu einem stabilen Zustand zurückfindet. Im schlechtesten Fall können durch das Policy-basierte Routing divergente Zustände im Inter-Domain-Bereich entstehen, wie unter anderem

bereits vor rund zwei Jahrzehnten in [VGE00] gezeigt wurde. Aktuelle Betrachtungen zu möglichen Gegenmaßnahmen [DS17] belegen dabei, dass die verzögerte Konvergenz von BGP-Routen in der heutigen Zeit nach wie vor sehr präsent ist.

Begrenzte Ausdrucksstärke der Policies
Die BGP-Policies beziehen sich immer auf die Inter-Domain-Ebene (AS-Pfade). Somit reicht die Ausdrucksstärke nicht aus, um den Bezug zu einzelnen Kommunikationsflüssen darzustellen. Dadurch wird die Granularität möglicher Ersatzpfade eingeschränkt.

Keine fortgeschrittene Fehlererkennung
Einige kritische Herausforderungen, beispielsweise dauerhafte Überlastung eines Links oder oszillierende Routen, werden durch das BGP-Protokoll nicht erkannt.

Fehlende Sicherheitsmechanismen
Das klassische BGP-Protokoll ist vergleichsweise verwundbar gegenüber einer ganzen Reihe bekannter Angriffe. In vielen Fällen ist dies bereits auf fehlende Authentizität und Integrität von ausgetauschten BGP-Nachrichten zurückzuführen, das größere Problem stellt jedoch das Fehlen von Authentisierungsmechanismen zur Überprüfung der Legitimierung von BGP-Kontrollinformationen dar [KLS02].

Während Letzteres in den vergangenen Jahren durch Protokollerweiterungen wie Border Gateway Protocol Security (BGPsec) [LS17], beziehungsweise den hiermit verbundenen Integritäts- und Authentizitätsvalidierungen auf Basis von Resource Public Key Infrastructure (RPKI) [BA13], zwar grundsätzlich technisch adressiert wurde und insbesondere durch die schleppende Einführung der entsprechenden Erweiterungen [Gol14] weiterhin von Bedeutung ist, wurden die übrigen Themen bisher weitgehend hingenommen – auch weil das Provider-übergreifende, durchgängige Etablieren eines neuen Inter-Domain-Routing-Protokolls aus wirtschaftlichen Gesichtspunkten derzeit kaum vorstellbar ist. Schon aus einem theoretischen Blickwinkel ist daher erkennbar, dass bereits das verwendete BGP-Routing für Instabilitäten im Internet-Routing verantwortlich zeichnen kann. Die eigentlichen Ursachen für die in der Praxis sichtbaren Ausfälle sind dabei gleichwohl deutlich vielfältiger.

2.1.2 Untersuchungen zu Fehlercharakteristika im Inter-Domain-Bereich

Bereits seit mehreren Jahrzehnten befinden sich dabei die verschiedenen Ausfälle und Fehlerzustände, welche im Internet allgegenwärtig auftreten, im Blickpunkt der Forschung. Der private Endnutzer bemerkt auftretende Störungen in aller Regel lediglich anhand kurzzeitig unterbrochener Verbindungen oder Performanzeinbußen im Sinne von Laufzeiten oder erreichten Durchsatzraten.

Grundsätzlich sind Störungen in großen Netzwerkinfrastrukturen wie dem Internet dabei natürlich unvermeidbar. Die Mehrzahl der beobachteten Fehler an den Rändern der Infrastruktur ist dabei auf triviale Ursachen zurückzuführen. Falsch konfigurierte oder defekte Router, physikalische Verbindungsausfälle oder Softwarefehler treten hier vergleichsweise häufig auf und werden in der Regel nicht durch besondere Provider-seitige Schutzmaßnahmen behandelt. Demgegenüber wird die Kerninfrastruktur in der Praxis stärker gegenüber Ausfällen einzelner Komponenten geschützt. Geräteredundanzen und ringbasierte Protection-Pfade für Glasfaserinfrastrukturen entsprechen hier bereits seit vielen Jahren dem Stand der Technik.

Im Folgenden wird allerdings deutlich, dass auch weitaus weniger offensichtliche Fehlverhalten in der Internet-Infrastruktur beobachtet werden können, welche einen signifikanten Einfluss auf die Ende-zu-Ende-Konnektivität in der Infrastruktur nehmen können. Zu allem Überfluss sind Schutzmechanismen gegenüber einigen dieser weniger offensichtlichen Auslöser, wie beispielsweise die bereits angeführte Interaktionsdynamik und das Konvergenzverhalten von BGP, nur schwer zu etablieren.

In Anbetracht der unerwartetermaßen häufig zu beobachtenden, eingeschränkten Pfadverfügbarkeit im Internet wurde den Fehlerursachen nun bereits seit der Entstehung des Internets ein großes Forschungsinteresse zuteil. Aufschlussreiche Betrachtungen ausgewählter Forschungsgruppen werden dabei im Folgenden kurz vorgestellt.

Paxson Der häufig zitierte *Vern Paxson* wird heute als Pionier im Kontext von Fehlerkategorisierung und -analyse angesehen. Unter anderem im Kontext von [Pax97a] führte Paxson, unter Zuhilfenahme des *traceroute*-Werkzeugs, aktive Messungen zwischen verschiedenen Standorten im Weitverkehrsbereich durch, um das Verhalten des Inter-Domain-Routings zu analysieren. Dabei konnten verschiedene Fehlertypen erfasst werden, darunter langanhaltende Routing-Schleifen und eine Vielzahl weiterer Ausfälle. Unter anderem wurde auch festgestellt, dass sich die durchschnittliche Anzahl der Messungen, in deren Kontext ein Fehlerfall bemerkt wurde, im Laufe der frühen Studie stark veränderte. Die Wahrscheinlichkeit einer Fehlersituation im Zuge einer Messung erhöhte sich dementsprechend im Rahmen eines Jahres von 1.5% auf 3.4%. Dadurch wird die Vermutung bestärkt, dass sich das Fehlerverhalten des Internet-Routing im Laufe der Zeit verändert.

Im Rahmen der Arbeit [Pax98] wurden schließlich weitreichende Ergebnisse der durchgeführten Langzeitmessungen präsentiert, welche sich auf verschiedene Effekte auf den Ende-zu-Ende-Pfaden beziehen. An dieser Stelle seien nur einige ausgewählte Erkenntnisse genannt:

- Es wurde gezeigt, dass Paketverluste stark korrelieren und dementsprechend nicht als unabhängige Ereignisse anzusehen sind.
- Verlustraten unterscheiden sich tendenziell auch in Abhängigkeit der jeweiligen geographischen Regionen, welche von Routen traversiert werden.
- Ein guter Indikator für die Fehlerprädiktion eines Pfades wird durch eine Beobachtung des Pfadzustands bezüglich des generellen Auftretens von Paketverlusten ermöglicht. Demgegenüber wird von einer Indikation durch Beobachtung der Paketverlustrate abgeraten.

Labovitz et al. Einen ebenfalls unbestritten großen Einfluss auf die Forschung im Bereich des Inter-Domain-Fehlerverhaltens hat die Forschungsgruppe um *Craig Labovitz*. Bereits im Zuge von [LMJ98] wurden BGP-Informationen von *Internet Service Providern (ISP)* an bestimmten Knotenpunkten verwendet, um die Stabilität des Interdomain-Routings auf fehlerhafte Situationen zu untersuchen und diese zu charakterisieren. Im Rahmen der Studie wurden über neun Monate hinweg definierte Sequenzen von Routing-Updates beobachtet. Beispielsweise konnte gezeigt werden, dass Instabilitäten über alle Präfix-Adressen und autonomen Systeme verteilt auftreten. Außerdem wurde beobachtet, dass ein Großteil der ausgetauschten Routing-Informationen keine Topologieänderung widerspiegelt. Die Motivation der Autoren