Technische Universität München
Lehrstuhl für Kommunikationsnetze

Beiträge zu einem teilautomatisierten Netzmanagement für breitbandige Transportnetze

Dipl.-Ing. Univ. Christian Alfons Bernd Merkle

Vollständiger Abdruck der von der Fakultät Elektrotechnik und Informationstechnik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr.-Ing. Rolf Witzmann

Prüfer der Dissertation:

1. Univ.-Prof. Dr.-Ing. Jörg Eberspächer
2. Priv.-Doz. Dr. rer. nat. Helmut Reiser, Ludwig-Maximilians-Universität München

Die Dissertation wurde am 19.04.2012 bei der Technischen Universität München eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am 20.07.2012 angenommen.

Vorwort

Diese Arbeit ist während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Kommunikationsnetze an der Technischen Universität München entstanden.

Mein besonderer Dank gilt Herrn Prof. Eberspächer, der mir nach meiner Diplomarbeit am Lehrstuhl für Kommunikationsnetze die Chance gegeben hat, wissenschaftlich zu arbeiten und die Promotion durchzuführen. Als mein Betreuer gab er mir den Freiraum für die eigenständige Forschung am Lehrstuhl. Durch die gemeinsamen Gespräche und Diskussionen erhielt ich wertvolle Anregungen, die meine wissenschaftliche Arbeit bereichert haben und zum stetigen Vorankommen der Dissertation beitrugen. Sehr hilfreich für die Arbeit war auch das Netzwerk von Prof. Eberspächer zu ehemaligen Doktoranden und Kollegen.

Mein Dank gilt ebenfalls Herrn Priv.-Doz. Dr. Helmut Reiser für seine freundliche Bereitschaft, das Zweitgutachten in meinem Promotionsverfahren zu übernehmen.

Die Grundlagen meiner Forschung basieren zum großen Teil auf den zwei Projekten Robust Operation and Planning of cost efficent Networks und 100 *Gbit/s Carrier Ethernet Transport* (100GET). Für die erfolgreiche Zusammenarbeit möchte ich besonders meinen Projektpartnern Claus Gruber, Andreas Kirstädter, Thomas Michaelis und Dominik Schupke bedanken.

Bedanken möchte ich mich ebenso bei meinen ehemaligen Kollegen am Lehrstuhl für die angenehme und freundschaftliche Arbeitsatmosphäre und den stetigen wissenschaftlichen Austausch. Mein besonderer Dank gilt meinem ehemaligen Bürokollegen Stephan Eichler, der meine Diplomarbeit betreute und mir den Lehrstuhl näher brachte. Ebenfalls möchte ich mich bei Robert Nagel für die Anregungen und Kommentare zu meiner Dissertation bedanken.

An dieser Stelle möchte ich mich auch bei Herrn Dr. Martin Maier für die administrative Unterstützung und die angenehme Zusammenarbeit bedanken. Herr Maier half nicht nur aufgetretene Probleme schnell und unkompliziert zu lösen, sondern wusste auch immer durch einen hilfreichen Kommentar die Mitarbeiter zu motivieren.

Ein ganz besonderer Dank gilt meinen Eltern und meiner Freundin Julia. Sie brachten mir viel Verständnis und Geduld entgegen und motivierten mich immer wieder bei der Fertigstellung der Dissertation.

München, im April 2012 Christian Merkle

Kurzfassung

In der Arbeit werden Beiträge zum Management optischer Weitverkehrsnetze geliefert. Im Fokus stehen die Verkehrsmodellierung, die Analyse von Fehlermechanismen und die Entwicklung eines neuartigen teilautomatisierten Netzmanagementsystems. Das entwickelte dienstorientierte Verkehrsmodell dient als Eingabeparameter für das Netzmanagementsystem und berücksichtigt das spezielle Routing der untersuchten Dienste. Um die Ausfallsicherheit von Weitverkehrsnetzen zu erhöhen, wird sowohl ein Bewertungssystem für Konfigurationsfehler als auch ein Degradationsmodell für optische Komponenten zur proaktiven Fehlersuche erarbeitet. Ein eigens entwickelter Planungsprozess des Netzmanagementsystems bewertet die aktuelle Netzsituation und berechnet optimale Ersatzkonfigurationen. Im Fehlerfall stellt dieser entweder sofort eine vorberechnete optimale Ersatzkonfiguration zur Verfügung oder ermittelt mithilfe einer Heuristik eine (sub-)optimale Lösung.

Abstract

This dissertation contains contributions to the management of optical transport networks. The focus is on traffic modeling, analysis of failure mechanism, and the development of a novel semi-automatic network management system. The developed service oriented traffic models serve as input parameters for the network management system and include the special routing of the analyzed services. An evaluation system for configuration failures and a degradation model for optical network components to find failures proactively are considered to increase the resilience of transport networks. The specially developed planning process of the network management system uses the results of the analysis and the current network situation to pre-calculate optimal backup configurations. In the failure case the process provides either a pre-calculated optimal backup configuration or calculates with a heuristic a (sub-)optimal solution.

Inhaltsverzeichnis

1 Einführung

1.1 Motivation der Arbeit

In den letzten Jahren konnte man weiterhin riesige Wachstumsraten von $40\,\%$ bis $60\,\%$ des Datenverkehrs in Weitverkehrsnetzen beobachten [Cis08] und [LIJOJ10]. Dieses Wachstum hat sich unter anderem durch neue Dienste wie Content Delivery Networks (CDNs) und durch die Verfügbarkeit von breitbandigen Zugangstechnologien wie Digital Subscriber Line (DSL) oder Fiber To The Home (FTTH) weiter beschleunigt. Gleichzeitig steigt die Erwartungshaltung nach hohen Bandbreiten zu immer geringeren Preisen, ohne jedoch Abstriche bei der Dienstgüte in Kauf nehmen zu wollen. Diese beiden Entwicklungen erfordern den Aufbau von sehr leistungsfähigen, flexiblen und kostengünstigen Netzen, die dynamisch zur Laufzeit an die aktuelle Situation angepasst werden können.

Die Überwachung und Anpassung eines Weitverkehrsnetzes erfolgt anhand einer Steuerungs- beziehungsweise Managementebene. Mittels der beiden Ebenen werden Informationen und Fehlerereignisse in heutigen Netzen detektiert und an den Netzbetreiber gesendet. Dazu verfügen die Steuerungs- und Managementebene über eine Vielzahl an unterschiedlichen Überwachungsprotokollen, welche die benötigten Informationen über das Weitverkehrsnetz an den Netzbetreiber senden. Die Planung und Anpassung des Netzes erfolgt heute weitestgehend manuell durch den Netzbetreiber. Die manuelle Konfiguration ist aber zeitaufwendig und fehleranfällig wie verschiedene Studien zeigen [MWA02], [OGP03], [Woo04] und [FB05].

Eine Herausforderung ist die Automatisierung des Netzmanagements insbesondere die Planung und die Konfiguration eines Weitverkehrsnetzes. Das Netzmanagement benötigt hierfür zusätzliches Wissen über die Netzkomponenten, um Fehler automatisch zu erkennen und selbständig zu lösen. In einem ersten Schritt müssen die erhaltenen Informationen vom Netzmanagement kategorisiert und bewertet werden, um Rückschlüsse auf das Verhalten des Netzes zu ziehen. Die Schwierigkeit für ein automatisiertes Netzmanagement liegt anschließend darin, anhand der gewonnen Erkenntnisse eine optimale Planung des Routings für die aktuelle und zukünftige Netzsituation durchzuführen. Um eine flexible und kostengünstige Anpassung des Netzes durch ein Netzmanagementsystem zu gewährleisten, besteht die Möglichkeit, optimale Ersatzkonfigurationen für zukünftige Änderungen bereits im Voraus automatisiert zu planen und bei Bedarf anzuwenden. Eine entscheidende Frage in diesem Zusammenhang ist, welche zukünftigen Fehlerszenarien und wie lange im Voraus diese geplant werden.

Daraus leitet sich die Fragestellung ab, welche Maßnahmen ein Netzmanagementsystem ergreift, wenn ein unvorhergesehener Fehler eintrifft, für den keine geeignete Ersatzkonfiguration existiert. Auch in diesem Fall soll das automatisierte Netzmanagement ohne das Eingreifen des Netzbetreibers eine schnelle und kostengünstige Lösung finden. Die vorliegende Arbeit widmet sich genau diesen Fragestellungen, entwickelt dafür Lösungsmöglichkeiten und liefert ausführliche Untersuchungen.

1.2 Einordnung der Arbeit

In der Arbeit wird von der in Abbildung 1.1 dargestellten Inter-Domänen-Sichtweise auf ein Weitverkehrsnetz ausgegangen.

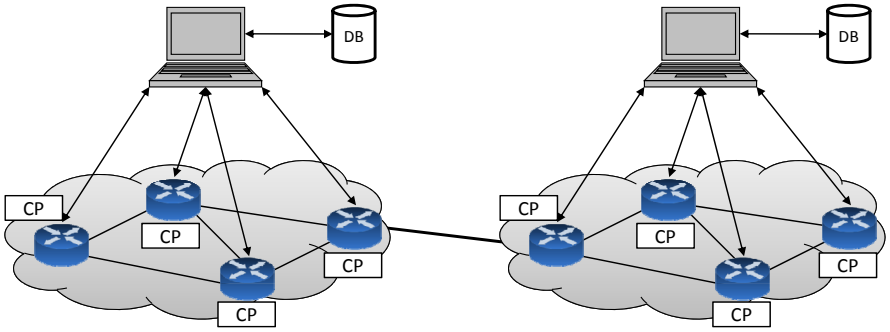


Abbildung 1.1: Netzmanagement innerhalb einer Domäne

Die Betrachtung einer Domäne hat den Vorteil, dass nur ein zuständiges Netzmanagement existiert und sich somit alle Informationen über das Netz in einer Hand befinden. Damit kann das gesammelte Wissen benutzt werden, um automatisiert eine Planung des Netzes durchzuführen, damit das Netz beispielsweise auf Verkehrsveränderungen vorbereitet ist.

Diese Arbeit geht von einem zentralen Netzmanagementsystem aus, das zur Überwachung und Anpassung des Netzes verwendet wird. Der Austausch von Managementinformationen zwischen zwei unterschiedlichen Weitverkehrsnetzen verschiedener Netzbetreiber ist aus Gründen der Geheimhaltung der Netzinformationen nicht gewünscht und wird deshalb in dieser Arbeit nicht betrachtet. Zusätzlich zur Managementebene ist die Verwendung einer Steuerungsebene möglich, die wie die Transportebene vom Netzmanagement überwacht wird und dem Netzmanagement Informationen zur Verfügung stellt.

Ein Fokus der Arbeit liegt auf der Bereitstellung von zusätzlichem Wissen für das Netzmanagement, um proaktiv Fehler zu finden. Das umfasst zum einen die Verwendung von zusätzlichen physikalischen Informationen über die Netzkomponenten, die in die Vorausplanung des Netzmanagements aufgenommen werden, und zum anderen die Bewertung der gesammelten Informationen. Ein weiterer Schwerpunk beschäftigt sich mit der Realisierung eines teilautomatisierten Netzmanagementsystems

und den darin enthaltenen Planungsprozessen, die automatisiert auf Netzveränderungen reagieren. Um ein allgemeingültiges Netzmanagementsystem zu entwerfen, werden keine spezifischen Eigenschaften der einzelnen Kommunikationsschichten betrachtet. In den jeweiligen Kapiteln werden die Grundannahmen über die Netzkomponenten und die verwendeten Kommunikationsschichten formuliert.

Abhängig von den vorhandenen Informationen plant das Netzmanagement zukünftige Fehlerszenarien voraus. Durch einen geeigneten Planungsprozess werden in dieser Arbeit so viele zukünftige Fehlerszenarien wie möglich vorausberechnet, wobei die Reihenfolge der Berechnung von der Auftrittswahrscheinlichkeit der Fehler bestimmt wird. Zusätzlich wird ein Kostenmodell für die Umkonfiguration eines Weitverkehrsnetzes realisiert, das die Anzahl der Konfigurationen auf ein notwendiges Maß reduziert, um hohe Ausfallzeiten durch Neukonfigurationen zu vermeiden.

1.3 Beitrag der Arbeit

Das Ziel dieser Arbeit ist, ein flexibles teilautomatisiertes Netzmanagement zu entwickeln, das im fehlerfreien Fall proaktiv optimale Ersatzkonfiguration vorausberechnet um im Fehlerfall schnell eine Ersatzkonfiguration zur Verfügung zu stellen. Eine wichtige Voraussetzung, um eine schnelle Reaktion des Netzmanagements zu gewährleisten, ist eine kontinuierliche Bewertung und Einordnung der aktuellen Netzsituation. Basierend auf der Bewertung entscheidet das Netzmanagement, welche Ersatzkonfigurationen als nächstes vorab geplant werden und wann eine Neukonfiguration des Netzes stattfindet.

Deswegen werden im ersten Teil der Arbeit die Rahmenbedingungen für das teilautomatisierte Netzmanagementsystem geschaffen. Zuerst werden dienstorientierte Verkehrsmodelle entwickelt, die als Eingabeparameter für die Planung in dem Netzmanagementsystem dienen. Die Verkehrsmodelle berücksichtigen sowohl das spezielle Routing der untersuchten Dienste als auch den Standort von Unternehmen und das Vorhandensein von Internet-Austauschknoten. Internet-Austauschknoten beeinflussen das Routing aller Dienste, wenn diese über verschiedene Netzbetreiber geroutet werden. Die entwickelten Verkehrsmodelle werden abschließend mit Hilfe einer Fallstudie parametrisiert, um für jeden betrachteten Dienst eine Verkehrsmatrix und das entsprechende Routing in einem Referenznetz zu erhalten.

Anschließend werden Fehlermechanismen von Konfigurationsfehlern und deren Auswirkung auf ein Weitverkehrsnetz untersucht und bewertet. Die Herausforderung bei Konfigurationsfehlern besteht darin, dass sie häufig nur indirekt zu detektieren sind, da sie keine Alarmnachrichten auslösen, die an das Netzmanagement gesendet werden. Deshalb werden in dieser Arbeit die Auswirkungen der Konfigurationsfehler beschrieben und anhand eines entwickelten Bewertungsschemas evaluiert. Dieses wird in das Netzmanagementsystem integriert, um eine proaktive Suche nach Konfigurationsfehlern zu ermöglichen und gefundene Konfigurationsfehler für die anschließende Fehlerbehebung zu priorisieren.

Um die Ausfallsicherheit von Weitverkehrsnetzen zu erhöhen und physikalische Ausfälle zu minimieren, wird in der Arbeit ein Degradationsmodell von optischen Komponenten zur proaktiven Fehlersuche entwickelt. Das Degradationsmodell ordnet den optischen Komponenten einen Degradationsverlauf zu, welcher die Alterung der jeweiligen physikalischen Komponente beschreibt. Das Netzmanagement überprüft regelmäßig die Degradationswerte und erhält damit Informationen über den aktuellen Zustand jeder optischen Netzkomponente. Anhand der Informationen berechnet das Netzmanagement optimale Ersatzkonfigurationen für einen bevorstehenden Ausfall und plant zusätzlich die Wartungsphase des Netzes.

Im letzten Teil der Arbeit wird das teilautomatisierte Netzmanagementsystem realisiert. Das Zusammenspiel und der Informationsaustausch der einzelnen Managementmodule werden eingehend dargestellt. Ein Schwerpunkt ist dabei die Entwicklung des Planungsprozesses, welcher aus zwei Optimierungsprozessen besteht. Der erste Optimierungsprozess ist eine ganzzahlige lineare Optimierung zur Vorausberechnung zukünftiger Fehlersituationen, die aus der Analyse der Konfigurationsfehler und dem Degradationsmodell hervorgehen. Der zweite Optimierungsprozess verwendet einen evolutionären Algorithmus zum schnellen Bereitstellen einer Lösung, falls keine geeignete Ersatzkonfiguration vorausberechnet wurde. Zuletzt wird der Planungsprozess erweitert, indem *Reconfigurable Optical Add-Drop Multiplexer* (ROADM)s zur flexiblen Umkonfiguration eines Weitverkehrsnetzes betrachtet werden, um nachträglich ohne zusätzliche Kosten Schutzpfade zu installieren.

1.4 Struktur der Arbeit

Die weiteren Untersuchungen in dieser Arbeit unterteilen sich in sieben Kapitel. Die Struktur der Arbeit ist in Abbildung 1.2 gezeigt.

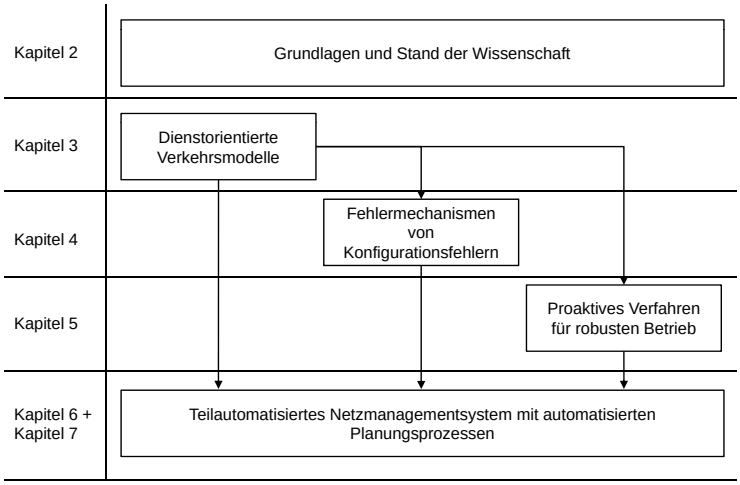


Abbildung 1.2: Übersicht über den Aufbau der Dissertation

Kapitel 2 beschreibt die Grundlagen für die darauf folgenden Untersuchungen und

erläutert den Stand der Wissenschaft.

Kapitel 3 befasst sich mit der Modellierung dienstorientierter Verkehrsmodelle die zur Berechnung des Verkehrsaufkommens und des Routings verwendet werden. Anhand der Verkehrsmodelle werden die Optimierungen in dem Netzmanagementsystem durchgeführt.

In Kapitel 4 werden die Auswirkungen von Konfigurationsfehlern auf ein Weitverkehrsnetz beschrieben und ein Bewertungsschema entworfen, anhand dessen die Konfigurationsfehler kategorisiert und priorisiert werden. Das Bewertungsschema ist unter anderem ein Bestandteil des Netzmanagementsystems und dient zur Bestimmung der Optimierungsreihenfolge der Fehlerszenarien.

Um eine proaktive Suche nach Fehlern zu ermöglichen, wird in Kapitel 5 ein Degradationsmodell für optische Komponenten entwickelt und untersucht. Die Basis bildet die Degradation von Lasern, deren Degradationswerte ermittelt und an das Netzmanagement gesendet werden. Anhand dieser Werte ist eine Planung des Reparaturprozesses der degradierten Komponenten möglich, was zu einer Verringerung der Ausfallzeit des untersuchten Netzes führt.

In Kapitel 6 und Kapitel 7 erfolgt die Realisierung des teilautomatisierten Netzmanagementsystems. Dabei wird zunächst in Kapitel 6 der Aufbau des Managementsystems und die Interaktion der einzelnen Module beschrieben. Anschließend werden die entwickelten Planungsprozesse betrachtet. In Kapitel 7 werden die Planungsprozesse anhand von verschiedenen Fehlerszenarien untersucht und die Ergebnisse eingehend dargestellt.

Abschließend werden die wesentlichen Bestandteile und Ergebnisse der Dissertation in Kapitel 8 zusammengefasst.

2 Grundlagen und Stand der Wissenschaft

In diesem Kapitel werden die technischen Grundlagen beschrieben, die zum Verständnis der Arbeit notwendig sind. Ebenso wird auf den relevanten Stand der Wissenschaft eingegangen. Abschnitt 2.1 beschäftigt sich mit den unterschiedlichen Transportnetzarchitekturen heutiger und zukünftiger Netze. Dabei liegt der Fokus auf der Beschreibung von IP über Carrier Grade Ethernet, welches eine mögliche Alternative für eine zukünftige Netzarchitektur darstellt.

Anschließend werden in Abschnitt 2.2 Verkehrsmodelle vorgestellt, die zur Berechnung des Verkehrsaufkommens in Weitverkehrsnetzen verwendet werden. Die meisten dieser Modelle basieren auf einem populationsbasierten Ansatz, welcher die Grundlage für das in der Arbeit entwickelte dienstorientierte Verkehrsmodell bildet.

Im Anschluss werden in Abschnitt 2.3 die Detektion von Konfigurationsfehlern beschrieben. Dabei werden Verfahren gezeigt, die es ohne vorhandene Alarmnachrichten ermöglichen, potentielle Konfigurationsfehler zu identifizieren. Die Detektion von Konfigurationsfehlern ist die Voraussetzung, dass das in dieser Arbeit entwickelte teilautomatisierte Netzmanagementsystem diese durch eine Umkonfiguration des Netzes beheben kann. Neben dem Auffinden von Konfigurationsfehlern ist auch die proaktive Suche nach weiteren Fehlern eine wichtige Voraussetzung für eine höhere Ausfallsicherheit. Deshalb werden in Abschnitt 2.4 proaktive Verfahren vorgestellt, die potentielle Fehler detektieren, bevor sie sich auf das Weitverkehrsnetz auswirken.

In Abschnitt 2.6 werden unterschiedliche teilautonome beziehungsweise autonome Netzmanagementarchitekturen vorgestellt. Dabei werden die Vorteile eines autonomen Netzmanagements und die verschiedenen Ansätze zur Erreichung der Teilautomatisierung beschrieben. Die Grundlagen für die ganzzahlige lineare Optimierung sowie für Heuristiken werden im letzten Abschnitt 2.7 dargestellt. Dabei wird auf die Vor- und Nachteile der jeweiligen Verfahren eingegangen.

2.1 Heutige und zukünftige Netzarchitekturen

Zur Darstellung heutiger Transportnetze bedient man sich der Methode der logischen Schichtendarstellung. Häufig wird ein Transportnetz, wie in Abbildung 2.1 gezeigt, in drei abstrakte Schichten aufgeteilt, die als Transport-, Steuerungs- und Managementebene bezeichnet werden.

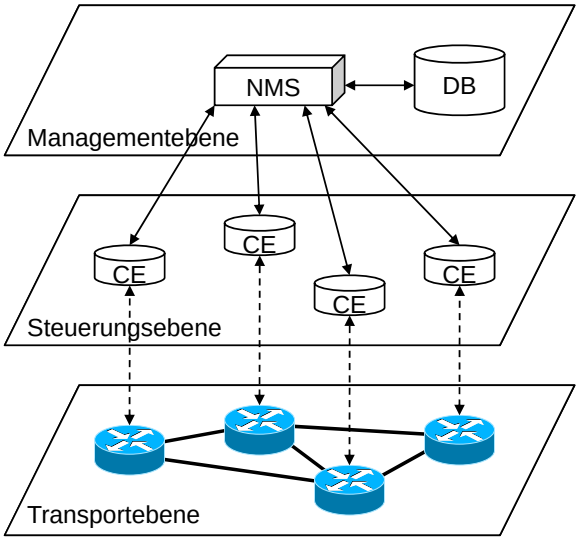


Abbildung 2.1: Transport-, Steuerungs- und Managementebene eines Transportnetzes

Während die Transportebene für den Datenaustausch der Nutzer zuständig ist, gewährleisten die Steuerungs- und Managementebene den Betrieb des Netzes und die gewünschte Dienstgüte der angebotenen Dienste. Die Signalisierungsnachrichten werden entweder über das gleiche Weitverkehrsnetz oder über ein getrenntes Netz geroutet. Im ersten Fall spricht man von einem virtuellen Signalisierungsnetz, da es auf der physikalischen Schicht die gleichen Ressourcen wie die Daten verwendet. Im zweiten Fall existieren real zwei getrennte Netze, um die Signalisierungsnachrichten und die Daten zu routen. Durch die Verfügbarkeit verschiedener neuer Technologien verbunden mit höherer Rechenleistung der Netzknoten, ist es bei Pfadausfällen im Netz möglich, automatisch auf Ersatzwege umzuschalten beziehungsweise neue Dienste automatisch einzurichten. Dies wird üblicherweise mit Hilfe von Protokollen der Steuerungsebene wie *Intermediate System to Intermediate System* (IS-IS) und *Open Shortest Path First* (OSPF) gewährleistet, die anhand der Daten in der Verkehrsmanagementdatenbank die kürzesten Pfade in einem Netz und die Ersatzwege berechnen. Die weiteren Aufgaben einer Steuerungsebene sind neben der Verbindungssteuerung auch die Topologieerkennung und das Bandbreitenmanagement.

Damit ein Netzbetreiber sein Transportnetz betreiben und managen kann, benötigt er eine Managementebene zur Verwaltung der Informationen über das Netz. Die Managementebene setzt sich aus verschiedenen *Netzmanagementsystemen* (NMS) zusammen und erlaubt dem Netzbetreiber das Netz zu überwachen und innerhalb einer Netzdomäne zu konfigurieren. Netzmanagement bezieht sich auf die Fähigkeit eines NMS, *Betrieb, Administration und Wartung* (OAM) eines Netzes zu gewährleisten. Dies wird durch die *Fehler, Konfiguration, Abrechnung, Leistungsmerkmale und Sicherheit* (FCAPS)-Funktionalitäten sichergestellt, die jede Managementebene bereitstellt.

In den heutigen Netzen gibt es verschiedene NMS, die sich in der Managementarchitektur, dem Informationsmodell oder den Managementprotokollen unterscheiden. Eine Architektur und Framework für *Telekommunikationstechnik Managementnetz*

(TMN) wurde von der *International Telecommunication Union* (ITU) in [Int85] definiert. Ein Ende-zu-Ende Kommunikationsdienst wird heute über viele Technologien und unterschiedliche Kommunikationsnetze angeboten. Verschiedenste Dienste wie *Digital Subscriber Line* (DSL), Ethernet und Funkübertragung mit einem immer höheren Verlangen nach Bandbreite und Mobilität stehen heute zur Verfügung. Die verschiedenartigen Dienstangebote resultieren in Kommunikationsnetzen, die aus einer Vielzahl unterschiedlicher Netzkomponenten bestehen. Deshalb ist es notwendig, standardisierte Managementinterfaces zu definieren, auf die ein Netz- oder Dienstanbieter zurückgreifen kann. Dies wird mit dem Framework für TMN umgesetzt, das Interface-Definitionen in die TMN Standardisierung einbringt.

Ein weiterer Aspekt des heutigen Netzmanagements besteht in der Zusammenarbeit von Steuerungsebene und Netzmanagementebene. Im Wesentlichen existieren zwei Möglichkeiten ein Kommunikationsnetz zu betreiben. Eine Möglichkeit ist die ausschließliche Verwendung einer Netzmanagementebene, die für die Überwachung des Netzes zuständig ist. Da keine Steuerungsebene vorhanden ist, müssen deren Aufgaben ebenfalls von der Netzmanagementebene übernommen werden. Die zweite Realisierung beinhaltet Steuerungs- und Managementebene zum Betrieb eines Netzes. Werden beide Ebenen verwendet, kann die Netzmanagementebene auf die gesammelten Daten der Steuerungsebene zurückgreifen. Ein Beispiel hierfür ist die *Traffic Engineering Database* (TED), die jeder Netzknoten pflegt und in der die aktuellen Topologie- und Verkehrsinformation gespeichert werden. Des Weiteren wird die Steuerungsebene von der Netzmanagementebene konfiguriert und überwacht, was einen zusätzlichen Aufwand für die Netzmanagementebene darstellt. In dieser Arbeit wird ein Netzmanagementsystem entwickelt, das sowohl mit als auch ohne Steuerungsebene arbeiten kann. Zusätzlich wird noch die Erweiterung der Steuerungsebene um ein *Path Computation Element* (PCE) betrachtet. Ein PCE wird durch die *Internet Engineering Task Force* (IETF) als Element definiert, welches Netzpfade und Routen basierend auf einem Netzgraphen berechnet.

2.1.1 Heutige Weitverkehrsnetzarchitektur

In diesem Abschnitt wird die in der Arbeit verwendete Netzarchitektur vorgestellt. Ein Beispiel für eine heutige Netzarchitektur ist die *Internet Protocol* (IP)/*Multi-Protocol Label Switching* (MPLS)/*Synchronous Digital Hierarchy* (SDH)/*Dense Wavelength Division Multiplexing* (DWDM)-Architektur. Auf der untersten Schicht befindet sich ein optisches DWDM-Transportnetz, welches sehr hohe Bandbreiten ermöglicht. Heutzutage können bis zu 80 Kanäle mit 80 Gbit/s auf einer Übertragungsstrecke gemultiplext werden. Die nächsthöhere Schicht in der Architektur ist die SDH-Schicht. SDH arbeitet in der elektrischen Domäne und bietet ein sehr flexibles Multiplexingschema, bei dem Datenströme von 155 Mbit/s auf höhere Datenströme gemultiplext werden können, ohne die eingehenden Datenströme völlig zu demultiplexen. Zusätzlich bietet SDH erweiterte Schutz- und Vermittlungsmechanismen im Vergleich zu DWDM, die im Falle eines Ausfalls des Arbeitspfads ein schnelles

Umschalten auf einen Ersatzpfad erlauben. Die IP/MPLS-Schicht ist für das Routing der Pakete verantwortlich. MPLS bringt dabei den verbindungsorientierten Ansatz in die IP-Domäne. Dies hat den Vorteil, dass eine Verkehrsplanung möglich ist, da durch die Labels der Pfad in dem MPLS-Netz bestimmt ist. Durch das Hinzufügen eines Labels an ein IP-Paket, müssen die Router innerhalb des Transportnetzes nicht die gesamte IP-Routingtabelle durchsuchen, um den nächsten Hop zu bestimmen. Die Weiterleitung der Pakete anhand des Labels ist damit wesentlich einfacher und schneller als im Vergleich zum IP-Routing.

2.1.2 Ethernet als Weitverkehrsnetztechnologie

Trotz der genannten Vorteile bei IP/MPLS und SDH gibt es Bestrebungen auf eine alternative Transportnetzarchitektur zu migrieren. Dies hat mit dem Erfolg von Ethernet im *Local Area Network* (LAN)-Bereich zu tun. Allgemein akzeptierte Schätzungen gehen davon aus, dass heutzutage 90 % des gesamten Internetverkehrs auf Ethernet-Protokollen beruht. Ethernet-Interfaces sind kostengünstig und die Technologie einfach zu betreiben und zu warten. Um das Paradigma einer Ende-zu-Ende Übertragung in einer Technologie zu erreichen, wurde Ethernet als geeigneter Kandidat identifiziert, um damit Datenverkehr über Zugangs-, Metro- und Weitverkehrsnetze zu übertragen. Die Netzbetreiber betrachten Ethernet als Technologie, mit der sie ihre traditionellen *Frame Relay* (FR), *Asynchronous Transfer Mode* (ATM), oder SDH/*Synchronous Optical Network* (SONET) Infrastruktur ersetzen können. Deshalb gab es in den Jahren 2005 und 2006 zahlreiche Untersuchungen zu dem Thema Carrier Grade Ethernet und dessen Vorteile. Im Folgenden werden einiger dieser Studien kurz beschrieben.

Meddeb vergleicht in [Med05] die heutigen Transportnetzprotokolle mit Ethernet und stellt die Vor- und Nachteile von Ethernet als Transportnetztechnologie dar. Als Hauptargumente für Carrier Ethernet führt der Autor die weite Verbreitung von Ethernet in lokalen Netzen, die kontinuierlich steigende Übertragungsrate sowie die einfache Handhabung von Ethernet auf. Als weitere Vorteile von Ethernet als Transportnetztechnologie werden die granularen Zugangsgeschwindigkeiten zwischen einigen 1 Mbit/s bis hin zu mehreren 10 Gbit/s, die einheitliche Technologie in Zugangs-, Metro- und Kernnetz und die geringen Einrichtungskosten von Ethernet genannt. Die fehlenden OAM-Fähigkeit sowie die Skalierbarkeit von Ethernet werden als Nachteile aufgeführt. Zusätzliche Herausforderungen bei der Verwendung von Ethernet im Kernnetzbereich sind der Wettbewerb mit bereits existierenden Technologien und der Kompromiss zwischen Carrier Grade und Dienstgütetauglichkeit, Einfachheit und Flexibilität von Ethernet. Auch in [ABMR06] werden die Vor- und Nachteile sowie die Herausforderung an Ethernet analysiert. Die Autoren gehen vor allem auf den Ethernet Standard 802.1ah ein.

Eine weitere ausführliche Diskussion über verschiedene Carrier Grade Ethernet-Technologien findet sich in [Iwa06]. Neben der Beschreibung des 802.1ah Standards erfolgt eine Zusammenfassung der Verfügbarkeits-, OAM- und Dienstgüte-

Kontrolltechnologien für Carrier Ethernet Transport. Daneben führt der Autor eine neue Ethernet Kernnetztechnologie ein, die als Global Open Ethernet (GOE) bezeichnet wird. Die größte Veränderung ist dabei das neue Tag-Stacking-Schema, welches dem Ethernet-Standard zusätzlich Skalierbarkeit, Verfügbarkeit und Betriebsfunktionalitäten hinzufügt. Eine ausführliche Beschreibung von GOE findet sich in [IHU+04]. Ein aktuellere Studie, die ebenfalls einen Überblick über Carrier Ethernet liefert und die neuesten Erweiterungen des 802.1Qay Standards umfasst, findet sich in [FA08].

Eine Kostenstudie und ein Kostenvergleich verschiedener Transportnetztechnologien sind in [SEK05], [KGRB06] und [DKL06] aufgeführt. Die Autoren betrachten dazu die Preisentwicklung der *Gigabit-Ethernet* (GbE)-Bandbreite in der Vergangenheit und extrapolieren diese Kurve für die Zukunft. Ebenso werden die Preisentwicklungen der alternativen Technologien extrapoliert und mit der von GbE verglichen. Die Autoren kommen zu dem Schluss, dass GbE einen Kostenvorteil im Vergleich zu den anderen Technologien besitzt.

Damit Ethernet in Weitverkehrsnetzen eingesetzt werden kann, muss der Ethernet-Standard Eigenschaften wie Skalierbarkeit und schnelle Ersatzschaltung erfüllen. Die notwendigen Erweiterungen werden in [IEEe] und [IEEb] eingehend dargestellt. Im Folgenden werden zwei dieser Architekturen vorgestellt, die in dieser Arbeit bei der Fehlerbetrachtung und dem Netzmanagementsystem berücksichtigt werden.

2.1.3 IP/MPLS/Ethernet/DWDM

Die IP/MPLS/Ethernet/DWDM-Architektur in Abbildung 2.2 ist durch eine Ethernet- und *Wavelength Division Multiplexing* (WDM)-basierte Transportebene charakterisiert, bei der die Knoten im Netz, welche die Pakete auf IP-Ebene weiterleiten, nur am Rand des Netzes verwendet werden oder wenn ein IP-Dienst angeboten werden muss.

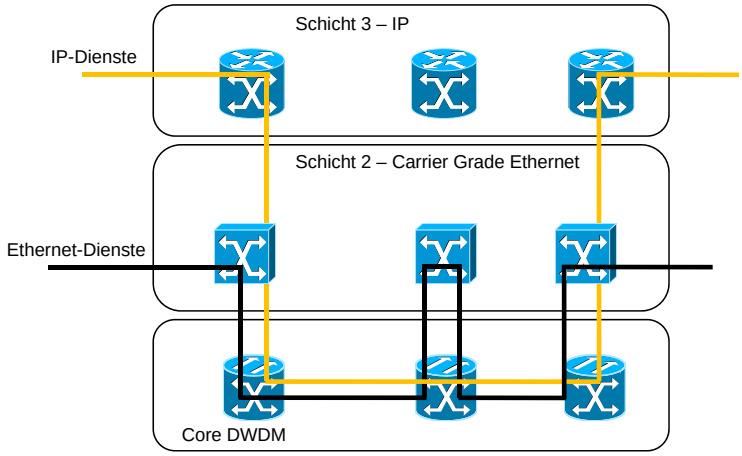


Abbildung 2.2: IP/MPLS/Ethernet/DWDM-Architektur

Um Ethernet-Dienste anzubieten, werden die Header der Datenpakete von anderen Diensten nicht betrachtet, sondern die Weiterleitung erfolgt anhand eines Ethernet

Headers, der an die Pakete hinzugefügt wird. Auch IP- und SDH-Dienste werden mittels passender Tunnelansätze auf Ethernet-Dienste abgebildet. Bei der Verwendung von Ethernet als Transportnetztechnologie findet das IP-Routing nur an den Eingangs- beziehungsweise Ausgangsknoten statt. Auf dem Pfad innerhalb eines Ethernet-Transportnetzes wird eine Ethernet- oder WDM-Vermittlung durchgeführt.

Durch die Abbildung der Dienste auf Ethernet-Tunnels verringert sich die Anzahl der Knoten in einem Netz, die IP-Routing-Kapazitäten benötigen. Dadurch sollen eine schnellere und einfachere Weiterleitung ermöglicht und die Betriebskosten eines Kommunikationsnetzes gesenkt werden. Dagegen erhöht sich jedoch die Anzahl der Ethernet-/WDM-Knoten innerhalb des Netzes. Ein auf Ethernet basierendes Transportnetz kommt allerdings nicht ganz ohne IP-Funktionalität aus, da heute bereits viele IP-Dienste wie *Voice-over-IP* (VoIP) existieren, die auch in Zukunft angeboten werden. Deshalb müssen die Netzbetreiber prüfen, welche IP-Funktionalität auf welchen Netzknoten in einem ethernetbasierten Weitverkehrsnetz benötigt wird.

2.1.4 IP/MPLS/Ethernet/SDH/DWDM

Eine weitere Carrier Ethernet Transportnetzarchitektur ist die Verwendung einer Ethernet-, SDH- und DWDM-basierten Transportebene, wie in Abbildung 2.3 dargestellt.

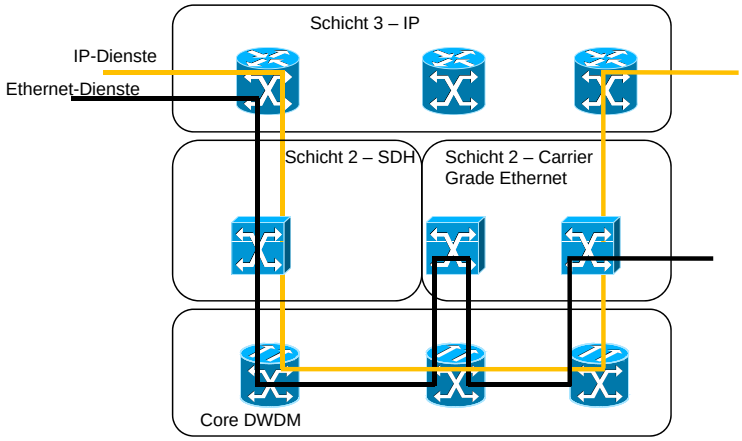


Abbildung 2.3: IP/MPLS/Ethernet/SDH/DWDM-Architektur

Wie bei der vorher beschriebenen Ethernetarchitektur, findet das IP-Routing nur an Eingangs- beziehungsweise Ausgangsroutern statt. Innerhalb des Netzes wird wiederum eine Ethernet- oder WDM-Vermittlung durchgeführt. Der Unterschied zur vorherigen Architektur besteht im Transport der SDH-Dienste. Diese Dienste werden bei der IP/MPLS/Ethernet/SDH/DWDM-Architektur wie in den heutigen Netzarchitekturen auf der SDH-Schicht vermittelt und nicht auf Ethernet-Tunnels abgebildet. Alle Dienste werden somit auf der niedrigsten möglichen Schicht vermittelt, was die Vermittlung an den Netzknoten vereinfacht, da sich die Protokollumsetzungen zwischen zwei Technologien verringern. Allerdings existieren mit Ethernet und SDH

zwei Schicht-2-Technologien, die ähnliche Aufgaben umfassen und diese Architektur kostenintensiver machen. Beide Technologien vereinen zum Beispiel dieselben Schutzmechanismen und OAM-Funktionalitäten für die jeweiligen Dienste. Auch die Wartung eines derartigen Transportnetzes ist aufwendiger, da die Netzknoten eine größere Funktionalität besitzen, die überwacht und konfiguriert werden muss.

Das in dieser Arbeit realisierte Netzmanagementsystem geht von einer IP/MPLS/-X/DWDM-Architektur aus. Wobei X für eine beliebige Schicht-2-Technologie steht. Die Planungsprozesse berücksichtigen die Verzögerungszeiten der Pfade auf den höheren Schichten und die Wellenlängenzuweisung der DWDM-Schicht. Ob die Verzögerungszeiten durch eine Schicht-2-Vermittlung oder ein Schicht-3-Routing entstehen, ist für die Planung unerheblich. Daher wird für das Netzmanagement keine bestimmte Schicht-2-Technologie definiert.

2.2 Modellierung von Verkehrsmodellen

Eine wichtige Größe bei der Netzplanung stellen die Verkehrsanforderungen der Nutzer in einem Transportnetz dar. Da es keine realistischen Verkehrsmessungen aufgrund der Vertraulichkeit dieser Informationen gibt, existieren einige wissenschaftliche Aktivitäten zur Modellierung und Vorhersage des Datenverkehrs. In [DW00] beschreiben die Autoren ein populationsbasiertes Verkehrsmodell für Sprach-, Daten- und Internetverkehr. Die Verkehrsanforderungen des Sprach- und Datenverkehrs basieren in diesem Ansatz zusätzlich noch auf der Distanz zwischen den Städten. Der Internetverkehr basiert dagegen auf der Anzahl der Internet-Hosts von jeder Stadt. Die Autoren berechnen des Weiteren eine Wachstumsrate für die drei Dienste, die sie anhand von Verkehrsdaten aus der Vergangenheit ableiten. Das vorgestellte Modell eignet sich für eine allgemeine Betrachtung der genannten Dienste, allerdings fehlen netzübergreifende Einflussfaktoren wie Internet-Austauschknoten, an denen man eine hohe Konzentration des Verkehrs vorfindet.

Weitere Verkehrsmodelle für drei verschiedene Referenznetze werden in [HBB+04] diskutiert. Die Autoren unterteilen den Verkehr in Sprache, Daten und IP ähnlich wie in [DW00]. Der Sprach- und Datenverkehr hängt wiederum von der Population und der Distanz zwischen zwei Städten ab. Zusätzlich werden noch Konstanten eingeführt, die durch den Vergleich von gemessenem Verkehr und Gesamtverkehr bestimmt werden. Die Autoren führen verschiedene Verkehrsgranularitäten und Aufteilungsverhältnisse des Verkehrs ein, die für eine Studie über statische und dynamische Verkehrsbedingungen verwendet werden.

In [Rou05] wird zur Verkehrsmodellierung ein Ansatz basierend auf dem Gravitationsmodell vorgestellt. Das Gravitationsmodell nimmt an, dass der Verkehr, der zwischen den Orten geroutet wird, proportional zu dem Volumen ist, das aus dem Produkt an eingehendem und ausgehendem Verkehr an diesen Orten ist. Der Vorteil des Modells besteht in dessen Einfachheit und der schnellen Erstellung von Verkehrsmatrizen, da es nur einen Parameter benötigt, um das Verkehrsaufkommen zu bestim-

men. Allerdings zeigt das Modell eine geringe Genauigkeit für die zukünftige Schätzung von Verkehrsmatrizen. Die zukünftige Schätzung des Verkehrsaufkommens ist aber ein entscheidender Punkt für die in dieser Arbeit entworfene teilautomatisierte Netzmanagementarchitektur, um optimale Ersatzkonfigurationen für ein zukünftiges Szenarien zu berechnen. Deshalb ist die Abschätzung des zukünftigen Verkehrsaufkommens ist auch ein Teil des in dieser Arbeit entworfenen Verkehrsmodells.

Die Autoren in [NST05] beschreiben zwei grundsätzliche Probleme, die bei der Betrachtung von synthetisch generierten IP-Verkehrsmatrizen entstehen. Das erste Problem besteht beim Generieren von Verkehrsmatrizen, die bestimmte räumliche und temporäre Muster enthalten, welche in realen Transportnetzen beobachtet werden. Das zweite Problem ist die Zuweisung von bestimmten Verkehrsvolumina an Knotenpaare in einer gegebenen Topologie. Um die genannten Probleme zu überwinden, werden in dem Paper statistische Charakteristiken aus realen Weitverkehrsnetzen extrahiert und mit den generierten Verkehrsmatrizen verglichen. Basierend auf Hypothesentests werden diejenigen Verteilungen identifiziert, die eine gute Übereinstimmung mit den realen Verkehrsmessungen liefern. Für die Lösung des zweiten Problems, schlagen die Autoren die Verwendung einer ganzzahligen linearen Optimierung oder Heuristik vor. Die Hypothesentests werden auch in dieser Arbeit angewendet, um die entwickelten dienstorientierten Verkehrsmodelle zu überprüfen.

Die Autoren in [CVFC09] stellen zwei effiziente Methoden zur Schätzung von Online-Verkehrsmatrizen vor und vergleichen diese miteinander. Der erste Ansatz betrachtet ein räumliches Modell für Quell-Ziel-(OD)-Verkehrsflüsse, welches basierend auf *Simple Network Management Protocol* (SNMP)-Messungen das Volumen der OD-Verkehrsflüsse schätzt. Die zweite Methode besteht aus einer rekursiven Schätzung der zuvor erstellten Verkehrsmatrix, indem ein Kalman-Filter-Ansatz gewählt wird. Beide Ansätze werden anhand von drei Referenznetzen überprüft. Die Kalman-Filter-Methode liefert dabei bessere Ergebnisse, da sie auf den Daten des ersten Ansatzes beruht. Dem ersten Ansatz stehen dagegen nur die SNMP-Messungen zur Verfügung, was zu einer höheren Fehlerrate führt. Die Autoren stellen abschließend fest, dass beide Ansätze im Vergleich zum Gravitationsmodell eine bessere Abschätzung der Verkehrsmatrizen liefert.

Die in Kapitel 3 entwickelten Verkehrsmodelle basieren auf den Modellen in [DW00] und [HBB+04], betrachten aber neue Dienste wie *Internet Protocol Television* (IPTV), *Video On Demand* (VoD) und *Content Delivery Networks* (CDN)s. Die genannten Dienste unterscheiden sich von den in der Literatur genannten derart, dass man abhängig von den Standorten der Server und der Platzierung der Internet-Austauschknoten eine stark unsymmetrische Verkehrsmatrix erhält. Dies bedeutet, dass das Verkehrsaufkommen beispielsweise von Knoten a nach Knoten b sehr gering ist, weil nur Signalisierungsnachrichten versendet werden. In entgegengesetzter Richtung ist das Verkehrsaufkommen jedoch um ein Vielfaches höher, da in diese Richtung der Datenverkehr fließt. Die entwickelten Verkehrsmodelle erweitern die bestehenden Modelle, indem Internet-Austauschknoten in die Betrachtungen mit einfließen. Die untersuchten Verkehrsmodelle werden anhand der Ergebnisse von Hypothesentests

wie in [NST05] überprüft.

2.3 Detektion von Konfigurationsfehlern

Im diesem Abschnitt werden einige spezielle Verfahren zur Detektion von Konfigurationsfehlern vorgestellt. Neben Hardware- und Linkfehlern, die häufig die Kommunikation in einem Transportnetz beeinflussen, tragen auch Konfigurationsfehler zu Netzausfällen bei. Die Schwierigkeit liegt darin, einen Netzausfall auf einen Konfigurationsfehler zurückzuführen, da im Gegensatz zu einem Ausfall eines Links oder einer Hardwarekomponente keine Alarmmeldung im Netz erzeugt wird. Aufgrund einer Netzanomalie oder eines Ausfalls einer Netzkomponente müssen Rückschlüsse gezogen werden, ob diese durch eine Fehlkonfiguration ausgelöst wurden. Konfigurationsfehler können zu Netzausfällen, Leistungseinbußen und Sicherheitslücken führen. Eine Studie aus dem Jahr 2002 [MWA02] schätzt, dass die Hälfte der Netzausfälle von manuellen Konfigurationsfehlern stammen. Ähnliche Resultate wurden in einer Studie über Internetdienste [OGP03] gefunden. Daneben gibt es noch zahlreiche Studien über BGP-Konfigurationsfehler [FR01], [MWA02], [FB05] und [LTWG05], die aufzeigen, dass diese ebenfalls für eine Vielzahl von Netzanomalien verantwortlich sind.

Die Fehleranfälligkeit der manuellen Konfiguration liegt in der Komplexität der Aufgabe. Routerhersteller bieten eine Vielzahl an Konfigurationsbefehlen und Konfigurationsoptionen an, um das Netz für den Datentransport und die Netzüberwachung optimal einzustellen. Die Betriebssysteme von Juniper [Jun] oder Cisco [Cis] besitzen über 600 verschiedene Konfigurationsbefehle. Des Weiteren laufen auf den Netzknoten mehrere Protokolle gleichzeitig, die gegebenenfalls voneinander abhängen und nacheinander konfiguriert werden müssen. Da die Netze immer dynamischer werden, müssen Konfigurationseinstellungen häufiger und schneller angepasst werden. Ein weiterer Punkt für die Fehleranfälligkeit ist die manuelle Interaktion mit einem Befehlsinterface vom Hersteller. Tools zur Vereinfachung der Konfiguration von Routern sind bereits vorhanden, jedoch stellen diese häufig nur Templates für die Einrichtung eines neuen Dienstes oder Kunden zur Verfügung.

Daneben führt die manuelle Konfiguration von Transportnetzen zu teuren Fehlern und Verzögerungen bei der Einrichtung von Diensten für neue Nutzer [CGG+04]. Netzadministratoren müssen eventuell Upgrades begrenzen oder Upgrades und die Einführung von neuen Merkmalen, Protokollen und Diensten verzögern. Zusätzlich werden für die manuelle Konfiguration von Netzen Fachkräfte benötigt, welche für die spezielle Konfigurationssoftware ausgebildet werden müssen. Da jeder Hersteller sein eigenes Betriebssystem mitliefert, müssen die Techniker speziell für jedes Produkt geschult werden.

In der Literatur werden einige Verfahren vorgestellt, welche die Detektion von Konfigurationsfehlern ermöglichen. Das grundlegende Problem bei der Suche nach Konfigurationsfehlern besteht darin, dass häufig keine Fehlermeldung vorhanden

ist und der Netzbetreiber nicht genau weiß, was er genau überwachen muss, um den Fehler zu finden. Die Autoren in [KW04] beschreiben ein System, das aufgrund einer Analyse der Konfigurationsstruktur eines Betriebssystems automatisch vier Korrektheitsbedingungen basierend auf dieser Struktur ableitet. Durch die Analyse werden Konfigurationsklassen generiert, von denen anschließend die Bedingungen für eine korrekte Konfiguration entwickelt werden. Das von den Autoren entwickelte System erkennt bei der Evaluierung eines realen Datenbanksystems erfolgreich 33 % der Fehler. Weitere spezielle Methoden für die Routerkonfiguration werden in [EAK05], [FB05] und [LTWG05] beschrieben. In der erstgenannten Studie verwenden die Autoren ein Bayessches Framework anstelle eines vordefinierten Modells, um Fehlkonfigurationen von Routern zu finden. Der vorgestellte Algorithmus besteht dazu aus einer Trainings- und Detektionsphase. Die Konfigurationszeilen werden vereinfachend als unabhängig voneinander angenommen und über die Anzahl der gleichen Konfigurationsbefehle plus Konfigurationsparameter wird eine Wahrscheinlichkeit für das Auftreten dieser Konfigurationszeilen berechnet. Anschließend erfolgt ein Vergleich der realen Konfiguration mit den berechneten Wahrscheinlichkeiten für deren Auftreten.

In [FB05] und [LTWG05] werden Konfigurationsfehler in *Border Gateway Protocol* (BGP) untersucht. Die Studie in [FB05] verwendet ein Tool, welches eine statische Analyse anwendet, um Fehler in BGP zu finden. Dazu definieren die Autoren zwei abstrakte Aspekte für die Korrektheit der BGP-Konfiguration, welche von jedem Router eingehalten werden müssen. Anschließend werden Bedingungen auf diesen Korrektheitsspezifikationen abgebildet, anhand derer die Router getestet werden. Die Detektion von BGP-Fehlkonfigurationen erfolgt in [LTWG05] anhand der BGP-Präfixe der benachbarten autonomen Systeme und der Beziehung der autonomen Systeme untereinander. Dies erfolgt anhand eines vordefinierten Algorithmus der die eingehenden und ausgehenden Routen mit den Routing-Regeln vergleicht und Verletzungen dieser Regeln überprüft.

Eine weitere Methode, um Router-Fehlkonfigurationen zu entdecken, wird in [LLW+06] beschrieben. Die Autoren verwenden dazu Data Mining und definieren Assoziationsregeln, um die Konfigurationsdateien zu überprüfen. Treten Abweichungen von den Regeln auf, deutet dies auf eine mögliche Fehlkonfiguration hin. Der Algorithmus wird abschließend anhand von drei Beispielnetzen evaluiert.

2.4 Proaktive Verfahren zur Vermeidung von Netzfehlern

In diesem Abschnitt werden einige Verfahren für die proaktive Suche nach Netzfehlern vorgestellt. Wird dem Netzmanagement der Ausfall eines Links oder eines Netzknotens durch eine Alarmnachricht mitgeteilt, existiert bereits ein Fehler im Netz und Pakete gehen verloren, falls keine Ersatzschaltung aktiviert wurde. Um den Verlust von Daten in einem Netz zu vermeiden, werden in der Literatur einige

Verfahren beschrieben, die potentielle Fehlerquellen bereits vor ihrem Auftreten detektieren. Durch das vorzeitige Auffinden von Fehlern soll der Verlust von Daten vermieden werden. Neben Hardware-Fehlern, die meistens eine Alarmnachricht an das Netzmanagementsystem senden, gibt es auch noch weitere Fehler wie Konfigurationsfehler, die Anomalien im Netz erzeugen, aber keine Alarmnachricht generieren. Auch diese Fehler sollen mit proaktiven Verfahren detektiert werden, bevor es zu einer Verringerung der Netzperformanz kommt.

Eine Studie aus dem Jahr 1997 [HJ97] zeigt, dass das Thema proaktive Detektion von Netzfehlern nicht neu ist. In dieser Studie werden die gemessenen Daten eines Transportnetzes mit Bayeeschen-Netzen kombiniert, um unbekannte Fehler zu entdecken. Dazu wird das normale Verhalten eines Netzes durch Wahrscheinlichkeitsverteilungen beschrieben und Netzfehler entsprechend den Abweichungen von der Wahrscheinlichkeitsverteilung detektiert. Die Netzdaten werden mit Hilfe des SNMPs alle 15 Sekunden gesammelt und überprüft. Die Autoren zeigen mittels einer Simulation, dass ein ungewöhnliches Verhalten eines Fileservers 12 Minuten bevor dessen Zusammenbruch detektiert werden kann. Diese Methode eignet sich, um Konfigurationsfehler, wie sie in dieser Arbeit betrachtet werden, zu detektieren. Da Konfigurationsfehler häufig eine Netzanomalie hervorrufen, kann durch die Abweichung der Wahrscheinlichkeitsverteilung die Konfigurationsfehler entdeckt werden.

Eine weitere Studie basierend auf ATM-Netzen wird in [HS99] beschrieben. Die Autoren schlagen vor, das Netzfehlermanagement als teilweise beobachtbaren Markoff-Entscheidungsprozess (POMDP) zu formulieren. Markoff-Entscheidungsprozesse modellieren dabei ein System als Markoffkette mit Zustandsübergängen. Mit teilweise beobachtbar meinen die Autoren, dass einige Zustände der Markoffkette gegebenenfalls geschätzt werden müssen. Dazu verwenden sie intelligente Agenten, die im Fehlerfall eine optimale Managementaktion durchführen, um einen Fehler zu beheben. Um den POMDP-Ansatz für ein intelligentes System verwenden zu können, muss das POMDP-Problem ohne Kenntnis des exakten realen Systems gelöst werden. Deshalb kommt ein Simulator zum Einsatz, welcher der realen Situation ähnelt und mit dessen Hilfe die optimale Regel für einen Fehlerfall gelernt wird. Die Agenten bringen die gelernten Regeln in das reale System ein und lernen weiterhin dazu, um eventuelle Inkonsistenzen zwischen Simulator und realem System aufzulösen.

Ein Ansatz, der statistische Modelle und auf neuronalen Netzen basierende Klassifikatoren verwendet, wird in [LM02] beschrieben. Der Klassifikator wird mit Hilfe von funktionierenden Testkonfigurationen und Fehlermodellen in einem Testnetz trainiert und anschließend auf ein reales Netz übertragen. Anhand von Simulationen wird die Fehlklassifizierungsrate des Algorithmus überprüft. Die Ergebnisse in [LM02] zeigen, dass die Methode mit dem zusätzlichen Trainieren von Fehlermodellen im Vergleich zu der Methode, bei der nur funktionierende Konfigurationen trainiert werden, als effektive Startpunkte für die Fehlersuche in realen Netzen verwendet werden können, wenn in dem realen Netz eine ähnliche Fehlersituation existiert.

Die vorgestellten Detektionsansätze eignen sich gut für das Auffinden von Konfigurationsfehlern, die oftmals nur durch bestimmte Anomalien wie ein höheres

Verkehrsaufkommen oder eine größere Verzögerung der Pakete auffallen. Allerdings zeigen die Studien, dass das Training der Algorithmen entscheidend für eine hohe korrekte Fehlerdetektion ist. Daher werden in Kapitel 4 die Auswirkungen von Konfigurationsfehlern betrachtet und bewertet. Die Untersuchungen können zum Training von statistischen Modellen benutzt werden, um die Detektion von Konfigurationsfehlern zu verbessern. Die vorgestellten Algorithmen verwenden allerdings keine Informationen über den aktuellen Zustand der Netzelemente, die anschließend zur Vorausplanung von Ersatzkonfigurationen für Fehlerfälle sowie zur Vorausplanung der Wartungsphase verwendet werden können. In Kapitel 5 wird deshalb ein Degradationsmodell entworfen und untersucht, das bevorstehende Ausfälle von Netzkomponenten erkennt und die Information an das Netzmanagement sendet.

2.5 Netzmanagement

Die Komplexität heutiger Kommunikationsnetze nimmt aufgrund des steigenden Datenverkehrs, der Einführung neuer Dienste und der steigenden Größe der Kommunikationsnetze immer weiter zu. Für Netzbetreiber wird es daher immer wichtiger mittels geeigneter Managementsysteme die Netzressourcen effizient zu verwalten, um die Betriebskosten des Netzes zu minimieren. Die *Internationale Organisation für Standardisierung* (ISO) hat das *Open Systems Interconnection* (OSI) Netzmanagementmodell definiert, welches die allgemeinen Funktionen eines Netzmanagement beschreibt [Yem93] und [JP98]. Das Netzmanagementmodell beschreibt ein Framework und Richtlinien zur Überwachung, Wartung und Konfiguration großer Kommunikationsnetze. Das Framework definiert die fünf Funktionen Fehler, Konfiguration, Abrechnung, Performanz und Sicherheit des heutigen Netzmanagements. Jede dieser Funktionen steht für einen bestimmten Bereich des Netzmanagements, die im Folgenden erläutert werden.

2.5.1 Fehlermanagement

Beim Fehlermanagement handelt es sich um eine Reihe von Funktionen, die für Detektion, Isolierung und die Korrektur von aufgetretenen Fehlern in einem Kommunikationsnetz zuständig sind. Für die Fehlerdetektion wird das Netz überwacht und die gesammelten Daten in einer Managementdatenbank gespeichert. Netzkomponenten wie Switches und Router besitzen eine *Management Information Base* (MIB), in dem die Daten einer Netzkomponente gespeichert werden. Die Informationen werden über Netzmanagementprotokolle wie SNMP regelmäßig abgefragt und können vom Konfigurationsmanagement modifiziert werden. Mittels SNMP werden auch Alarmnachrichten von Netzkomponenten an das Netzmanagement gesendet. Eine Alarmnachricht wird von einer Komponente gesendet, sobald sie den Ausfall eines Interfaces, eines Links, oder eines benachbarten Knotens feststellt. Es handelt sich hierbei vor allem um physikalische Ausfälle, die von einer Komponente eindeutig

bestimmt werden können. Allerdings werden physikalische Fehler häufig auf mehreren Schichten von mehreren Komponenten detektiert, was zu einer Vielzahl an gesendeten Alarmmeldungen führt. Das Fehlermanagement besitzt deshalb meistens ein Filterungssystem, um einerseits die Vielzahl der Alarmnachrichten auf die entscheidenden Alarmnachrichten zu reduzieren und andererseits den Alarmnachrichten Prioritäten zuzuordnen. Anhand der Priorität einer Alarmnachricht wird anschließend die Fehlerbehebung durchgeführt. Neben der Detektion von Fehlern umfasst das Fehlermanagement ebenso die Protokollierung, Analyse und Behebung der aufgetretenen Fehler. Die Behebung der Fehler erfolgt anhand von vordefinierten Korrekturmechanismen, wie zum Beispiel dem automatischen Umschalten auf einen Ersatzweg.

2.5.2 Konfigurationsmanagement

Das Konfigurationsmanagement ist ein weiterer Funktionsbereich des OSI Netzmanagementmodells, das für das Sammeln und Speichern der Konfigurationsdaten von Netzkomponenten zuständig ist. Dazu nutzt es ein Netzmanagementprotokoll wie SNMP, um die Konfigurationsdaten aller Netzkomponenten zu erhalten und zu überwachen. Durch die Überwachung kann das Konfigurationsmanagement Änderungen an der Konfiguration einer Netzkomponente feststellen und überprüfen. Außerdem ist das Konfigurationsmanagement für die Erstellung neuer Konfigurationen zuständig, welche auf die jeweiligen Netzkomponenten übertragen werden. Eine weitere Aufgabe ist die Planung der Wartungsphase des Netzes. Dabei muss berücksichtigt werden, wie viele Netzkomponenten gleichzeitig konfiguriert werden und zu welcher Uhrzeit die Konfiguration stattfinden soll. Die Dokumentation und der Zeitpunkt der Konfigurationsänderungen sind ebenso ein Teil des Funktionsbereichs. Damit lassen sich Fehler, die durch eine falsche Konfiguration entstehen leichter Auffinden.

2.5.3 Abrechnungsmanagement

Das Abrechnungsmanagement umfasst das Sammeln und Verwalten von Informationen über die Benutzung eines Netzes. Dabei werden sowohl der Benutzungszeitraum als auch die benutzten Ressourcen eines Netzes durch den Nutzer erfasst und gespeichert. Die Informationen dienen zur Abrechnung der Kosten zwischen Netzbetreiber und Kunden. Für die Abrechnung werden unter anderem die Protokolle Remote Authentication Dial-In User Service (Radius), Terminal Access Controller Access Control System (Tacacs) und Diameter eingesetzt. Eine weitere Aufgabe besteht in der Administration der Benutzer, der Passwörter und der Zugangsberechtigungen.

2.5.4 Leistungsmanagement

Das Leistungsmanagement umfasst die Auswertung der Benutzungsstatistiken eines Kommunikationsnetzes. Dazu werden Daten über die Auslastung der Ressourcen, der Fehlerraten und der Antwortzeiten von Netzkomponenten überwacht und ausgewertet. Anhand der Daten wird der aktuelle Zustand eines Kommunikationsnetzes bestimmt und zukünftige Trends abgeleitet. Zustand meint in diesem Zusammenhang, die Leistungsdaten eines Netzes wie beispielsweise die Auslastung der einzelnen Links und Knoten sowie die Überwachung von Verzögerungen und Paketverlusten. Mit Hilfe der Trendanalyse werden zukünftige Anforderungen an das Netz identifiziert und es wird überprüft, ob ein Ausbau der Netzkapazitäten notwendig ist. Das Leistungsmanagement ist für die Optimierung eines Netzes zuständig und arbeitet mit dem Fehlermanagement zusammen, dessen Daten ebenfalls verarbeitet werden.

2.5.5 Sicherheitsmanagement

Das Sicherheitsmanagement dient zur Überprüfung der Zugangsberechtigungen der verschiedenen Nutzer zu einem Kommunikationsnetz. Es enthält Funktionen zur Erstellung, Löschung und Überwachung von Sicherheitsdiensten und Sicherheitsmechanismen innerhalb eines Netzes. Des Weiteren überwacht es mittels der Sicherheitsdienste, dass die Daten der Netzkomponenten nicht unerlaubt verändert werden. Die Verbreitung und Überwachung von Schlüsseln für die Verschlüsselung von Daten gehört ebenfalls zum Sicherheitsmanagement.

Eine Sicherheitsarchitektur für ein Managementsystem auf der Basis von Mobilen Agenten findet sich in [Rei01]. In dieser Arbeit werden sowohl Sicherheitsanforderungen als auch Sicherheitsmechanismen abgeleitet, die an Mobile Agenten gestellt werden. Ein weiteren entwickeltes Prinzip ist der Grundsatz des Vertrauens durch Einbettungsbeziehungen. Das bedeutet, dass ein Mobiler Agent dem Agentensystem vertraut, auf dem er eingesetzt wird. Die vorgestellten Lösungen eignen sich für den Einsatz in domänenübergreifenden Managementsystemen. Ein Framework für Sicherheitsmanagement für Kooperationen zwischen verschiedenen Unternehmen wird in [Rei08] entwickelt. Als Technologie werden Grids verwendet, welche eine optimale Kooperations- und Koordinationsplattform darstellen. Das Framework umfasst Kriterien zur Bewertung von Sicherheitsmechanismen und eine Schwachstellenanalyse, aus der eine Algorithmus zur dynamischen Berechnung von Trust Levels entwickelt wird. Die Arbeit umfasst des Weiteren ein zweistufiges Vorgehensmodell aus Analyse- und Synthesephase, mit dessen Hilfe ein Sicherheitsverantwortlicher das Framework auf sein konkretes Anwendungsszenario anwenden kann.

2.5.6 Managementinformationsdatenbank

Wie bereits erwähnt, werden die Informationen eines Netzes über ein Netzmanagementprotokoll ausgetauscht. Die Informationen die dem Netzmanagement zur Verfügung stehen, werden in der MIB gespeichert. Die Informationen selbst werden als Managed-Objekte (MO) bezeichnet. Zur Beschreibung der MO dient eine Regelsammlung des Netzmanagements. Ein MO stellt keinen Datenwert dar, sondern beschreibt, wo dieser Datenwert zu finden ist. Die MIB besteht aus verschiedenen MIB-Modulen, die hierarchisch aufgebaut sind. Die MIB eines Netzmanagements und der Netzkomponenten werden regelmäßig mit den Informationen aus dem Konfigurationsmanagement erneuert.

In dieser Arbeit, insbesondere in Kapitel 6 und Kapitel 7, wird das Fehlermanagement von Weitverkehrsnetzen betrachtet. Dabei wird sowohl auf die proaktive Detektion von Fehlern eingegangen als auch auf die Verarbeitung der Informationen im Planungsprozess zur Vorausplanung von Fehlerfällen. Ein weiterer Schwerpunkt bei der Betrachtung des Fehlermanagements ist die Bestimmung und Vorabberechnung von zukünftigen Fehlerszenarien sowie die schnelle Reaktion des Netzmanagement auf einen tatsächlich aufgetretenen Netzfehler. Die übrigen beschriebenen Funktionsbereiche des Netzmanagements sind nicht Teil dieser Arbeit.

2.6 Automatisierte Netzmanagementsysteme

Kommunikationsnetze haben sich in den letzten Jahren durch die Einführung neuer Technologien rapide verändert und haben sich von einfach verbundenen Netzknoten zu einer komplexen Infrastruktur entwickelt. Heutige Infrastrukturen verbinden verschiedene Technologien wie Festnetz und Funkübertragung, mobile und feste Knoten und diverse Dienste, wie Ende-zu-Ende, Realzeit und Dienstgüte miteinander. Die Netzknoten unterscheiden sich zusätzlich noch im Bezug auf Größe, Kapazität und Leistung. Diese heterogene Infrastruktur führt zu vielen unterschiedlichen Element-Managementsystemen, die in ein übergeordnetes netzweites Netzmanagementsystem eingegliedert werden müssen. Das Netzmanagement also die Überwachung, Fehlersuche und Konfiguration von Kommunikationsnetzen findet heutzutage meistens noch manuell statt. Um die Flexibilität und Robustheit der Netze gegen Veränderungen zu erhöhen, werden sowohl in der Industrie wie auch in der Wissenschaft automatische beziehungsweise autonome Netzmanagementsysteme untersucht. Das Ziel von automatischen Netzmanagementsystemen ist es, die Überwachung und Steuerung von Netzen zu vereinfachen, indem Prozesse automatisiert und der Netzbetrieb optimiert wird, ohne oder nur mit geringfügiger Interaktion des Netzbetreibers. Dabei liegt ein Fokus der Forschung auf der Entwicklung von verteilten Algorithmen, die verschiedene Selbstverwaltungsfunktionalitäten aufweisen und diese automatisch durchführen.

Der Unterschied zwischen autonomen und automatischen Systemen liegt darin, dass

autonome Systeme nicht nur Aufgaben automatisch ausführen, sondern auch auf Veränderungen selbständig reagieren. Autonomic Networking [ABB+06], [SSH06], [MK06] ist ein Konzept, das in den letzten Jahren eine größere Beachtung gefunden hat. Dabei folgt Autonomic Networking dem Konzept von Autonomic Computing [KC03], eine Initiative, die im Jahr 2001 von IBM gestartet wurde. Das Ziel von Autonomic Networking ist, selbstverwaltende Netze zu erstellen, die auf Veränderungen ohne Einschreiten des Netzbetreibers reagieren. Der Netzbetreiber übernimmt in solch einem System die passive Rolle, bleibt aber der endgültige Entscheidungsträger, da er für das Transportnetz verantwortlich ist und den Vertrag mit den Kunden schließt. Folgende vier Eigenschaften werden als Kerneigenschaften von autonomen Systemen bezeichnet [SSH06]:

- Selbstheilung: Aufgrund der Bewertung des aktuellen Netzzustands führt das System eine Korrektur durch, um Fehler im Netz zu beheben. Die Korrekturaktionen sollen möglichst keine Störung des Netzbetriebs hervorrufen.
- Selbstschutz: Das System detektiert selbständig Anomalien wie unautorisierter Zugang oder generelle Angriffe und führt autonom Veränderungen durch, um das Netz robuster gegen Veränderungen zu machen.
- Selbstkonfiguration: Die Netzkomponenten können sich dynamisch an die Veränderung der Netztopologie, beispielsweise dem Hinzufügen neuer Netzkomponenten, anpassen ohne oder mit minimalem Eingriff des Netzbetreibers.
- Selbstoptimierung: Anhand der gesammelten Informationen führt das Netzmanagement eine Optimierung der Netzressourcen durch, so dass die Dienstgütekriterien der Kunden erfüllt werden.

Zukünftige autonome Netzmanagementsysteme sollen die genannten Eigenschaften besitzen, um auf Veränderungen wie Netzfehler und neue oder veränderte Verkehrsanforderungen dynamisch zu reagieren. Im Vergleich zu heutigen Systemen sollen zukünftige Managementsysteme in weiten Teilen unabhängig von einem Netzbetreiber die Überwachung, Planung und Konfiguration eines Netzes durchführen. Immer wieder kommt es in Transportnetzen zu Netzausfällen aufgrund von Konfigurationsfehlern bei der Wartung der Netze [Bac09], [Hei09] und [Hei10]. Autonome Systeme gehen dabei noch einen Schritt weiter als automatische Systeme. Automatische Systeme führen selbständig anhand von vordefinierten Regeln Algorithmen aus. Dies bedeutet aber, dass ein Netzbetreiber die Regeln manuell ändern muss, wenn er das Verhalten des Managementsystems verändern möchte. Bei autonomen Systemen werden zu Beginn ebenfalls Regeln definiert, aber im Gegensatz zum automatischen System lernt das Netz selbstständig über sein Verhalten und passt die Regeln und sein Verhalten an die neuen Situationen an. Allerdings ist zu bedenken, dass der Netzbetreiber für das Verhalten in seinem Transportnetz verantwortlich ist und gegebenenfalls bei Nicht-Erfüllung eines Vertrags Strafzahlungen leisten muss. Daher stellt sich die Frage, inwieweit die Netzmanagementsysteme selbständig und unabhängig von dem Netzbetreiber arbeiten sollen. In dieser Arbeit wird deshalb in Kapitel 6 ein teilautomatisiertes Netzmanagementsystem vorgestellt, das einen

automatisierten Planungsprozess besitzt, allerdings die Ergebnisse der Planung nicht automatisch zur Konfiguration des Netzes verwendet, sondern auf eine Bestätigung durch den Netzbetreiber wartet.

In der Literatur werden verschiedene Architekturen für autonomes Netzmanagement vorgeschlagen [MK06], [ABB+06], [JvdMB+07], [EGDH08] und [TLG08]. Alle Architekturen haben gemeinsam, dass eine Kontrollschleife existiert, die kontinuierlich durchlaufen wird. Diese Kontrollschleife umfasst die Funktionen Überwachung, Analyse und Konfiguration eines Netzes. Die Architektur in [EGDH08] unterscheidet sich von den anderen darin, dass sie kein zentrales Managementsystem besitzt, sondern die Intelligenz auf die Netzknoten verteilt wird. Die Autoren argumentieren mit der höheren Komplexität eines zentralen Systems und führen an, dass ein zentrales System einen einzelnen Ausfallpunkt (Single Point of failure) besitzt. Allerdings ist der entscheidende Nachteil eines verteilten Systems, dass keine globale Sicht auf das Transportnetz existiert und die Aktualität der Daten an jedem Knoten geringfügig abweicht. Deshalb ist die Sichtweise jedes Knotens auf das Netz unterschiedlich und keine globale Optimierung des Routings möglich.

Die hier aufgeführten autonomen Netzmanagementsysteme haben gemeinsam, dass sie die Netzdaten, welche sie durch die Überwachung erhalten, in einer geeigneten Form beschreiben müssen, damit das Managementsystem eine automatische Analyse der Daten durchführen kann. Drei Informationsmodelle, die in der Forschung häufig verwendet werden und für Kommunikationsnetze geeignet sind werden kurz vorgestellt. Das allgemeine Informationsmodell (CIM) [Fora], welches von der Distributed Management Task Force (DMTF) entwickelt und standardisiert wurde, bietet eine allgemeine Definition von Managementinformationen für Systeme, Netze, Anwendungen und Dienste. Dieses besteht aus einer Spezifikation, welche die Integration mit anderen Managementmodellen definiert, und ein Schema, welches das aktuelle Modell beschreibt.

Eine weiteres Informationsmodell ist DEN-ng [Str02], welches den Nachteil von CIM behebt, das Geschäftsdienste mit Gerätekonfigurationen nicht verbinden und die Ergebnisse überwachen kann. DEN steht dabei für Directory Enabled Networks und stellt eine Spezifikation eines objektorientierten Informationsmodells zur Beschreibung von Objekten und die Beziehung zwischen den Objekten dar. Zusätzlich spezifiziert es eine Modellabbildung auf ein Format, welches in einem Verzeichnis gespeichert werden kann, das LDAP als Zugangsprotokoll benutzt. DEN-ng ist die Erweiterung von DEN, das die Übersetzung von Geschäftsregeln auf die Konfiguration von Geräten ermöglicht. Zusätzlich präsentiert es Regeln als Zusammenhang von ähnlichen Unterregeln und erweitert die Benutzung von Regeln, wann eine Einheit verändert wird. Das DEN-ng Informationsmodell bietet somit einen Ansatz, um die Bedürfnisse der Anwendungen und Dienste, die durch ein Netz angeboten werden, als allgemeinen Satz von Abstraktionen zu modellieren.

Ein von verschiedenen Telekommunikationsunternehmen entwickeltes Informationsmodell ist das sogenannte Shared Information and Data Model (SID) [Rei07]. Das Modell definiert Objekte und Beziehungen zwischen den Objekten, welche

die Beschreibung von Managementinformationen ermöglichen. Das SID-Modell ist objektorientiert in UML abgebildet und zum Teil aus dem DEN-ng-Modell abgeleitet. Das in dieser Arbeit entwickelte teilautomatisierte Netzmanagementsystem besitzt ebenfalls eine Datenbank, in der alle relevanten Informationen des Transportnetzes gespeichert werden. Der Fokus der Arbeit liegt nicht auf der Entwicklung eines neuen Informationsmodells, so dass eines der beschriebenen Modelle eingesetzt wird.

Wie bereits erwähnt existieren in der Literatur sowohl zentrale als auch dezentrale Ansätze für die Realisierung eines Netzmanagementsystems. Daher werden kurz die jeweiligen Vor- und Nachteile der beiden Ansätze diskutiert. Die am häufigsten genannten Vorteile eines dezentralen Managementsystems sind die geringere Komplexität, die schnellere lokale Reaktion eines Teilsystems und das nicht Vorhandensein einer einzigen Ausfallstelle. Durch die verteilte Intelligenz müssen nur die lokalen Informationen gespeichert und analysiert werden, was weniger Speicherbedarf und Rechenleistung erfordert. Des Weiteren ist bei einem Ausfall eines der Netzmanagementsysteme nur ein begrenzter Bereich des Transportnetzes betroffen, während die restlichen Systeme noch funktionstüchtig sind. Ein weiterer wichtiger Punkt ist die Skalierbarkeit von Managementsystemen. Abhängig von der Netzgröße und der Anzahl der überwachten Netzelemente kann zum einen das verwendete Datenbanksystem aber auch die CPU-Leistung überlastet werden. Dies kann bei sehr großen Netzen, die eventuell über mehrere Länder betrieben werden, vermieden werden.

Allerdings haben verteilte Systeme auch einige Nachteile, die im Folgenden kurz erläutert werden. Jedes der Teilsysteme besitzt eine abweichende Sichtweise auf das Transportnetz, die durch die abweichenden Informationen zustande kommen. Daher weiß kein Teilsystem, wie sich eine Konfigurationsänderung auf die übrigen Netzbereiche auswirkt. Die Berechnung einer globalen optimalen Konfiguration ist aufgrund der verteilten Informationen ebenfalls nicht möglich. Speziell in Fehlerfällen kann deshalb nicht garantiert werden, dass ein Umrouten des Verkehrs eventuell über andere Netzbereiche möglich wäre. Hierzu ist eine Kommunikation zwischen den Teilmanagementsystemen notwendig, um beispielsweise Informationen über die Linkauslastungen zu erhalten. Die zusätzliche Kommunikation erhöht allerdings wieder die Komplexität der Teilsysteme. Dagegen sind zentrale Netzmanagementsysteme der klassische Ansatz wie sie schon länger für Weitverkehrsnetze verwendet werden. Ein wesentlicher Vorteil ist die zentrale Datenhaltung, die eine globale einheitliche Sicht auf das Transportnetz und dadurch auch eine globale Optimierung ermöglicht. Vor allem im Fehlerfall ist eine globale Sicht hilfreich, um eine Lösung zu finden, mit der alle Verkehrsanforderungen trotz der reduzierten Netzkapazität geroutet werden können. Die Nachteile eines zentralen Managementsystems wurden bereits durch die Vorteile des dezentralen Ansatzes erwähnt. Diese sind die Skalierbarkeit und Ausfallsicherheit des Netzmanagements bei sehr großen Transportnetzen. Allerdings kann durch redundante Server und Rechner der Ausfall eines zentralen Netzmanagementsystems minimiert werden. Ein weiterer Nachteil ist die steigende Komplexität bei steigender Anzahl an überwachten Netzkomponenten.

In dieser Arbeit wird ein zentrales Netzmanagementsystem realisiert, das mittels des

in Kapitel 7 entwickelten Planungsprozesses eine globale Optimierung durchführt, um für zukünftige Fehlerfälle optimale Ersatzkonfigurationen vorauszuberechnen. Die vorliegende Arbeit verwendet ein zentrales Netzmanagementsystem, um die gespeicherten Informationen zentral zu verwalten, damit ein globales optimales Routing und Fehlermanagement erreicht wird. Allerdings werden bei dem in Kapitel 5 vorgestellten proaktiven Verfahren, die Degradationswerte dezentral auf den Knoten ausgewertet und an das Netzmanagementsystem übermittelt.

2.7 Planung von Transportnetzen

Wie bereits im Abschnitt 2.5 erwähnt, wird in dieser Arbeit ein teilautomatisiertes Fehlermanagement und insbesondere der Planungsprozess des Netzmanagements betrachtet. Damit das Fehlermanagement automatisch und schnell auf Netzfehler reagieren kann, muss der Planungsprozess in kurzer Zeit eine Lösung zur Verfügung stellen. Die zur Behebung des Fehlers zur Verfügung stehende Zeit hängt vor allem von den betroffenen Netzressourcen und Diensten ab. Allerdings darf der Planungsprozess des Fehlermanagements nicht mehrere Wochen für eine Lösung benötigen, sondern die Planung sollte wesentlich kürzer als die tatsächliche Reparaturzeit dauern, um eine positive Auswirkung auf das Netz zu haben. Die Reparaturzeit von Netzkomponenten liegt im Bereich von Stunden und setzt sich aus der Anfahrtszeit der Techniker, der Austauschzeit und der Testzeit der Komponenten zusammen. Der Planungsprozess muss daher in wenigen Stunden oder sogar Minuten eine geeignete Lösung bereitstellen.

Im Folgenden werden die Grundlagen zur Optimierung von Transportnetzen beschrieben, die im Kapitel 6 und Kapitel 7 angewandt werden. In dieser Arbeit wird ein teilautomatisiertes Netzmanagement realisiert, das zur Fehlerbehebung zwei verschiedene Planungsalgorithmen verwendet. Im fehlerfreien Netzzustand werden mittels einer ganzzahligen linearen Optimierung vorab definierte Ersatzkonfigurationen berechnet, die im Fehlerfall zum Einsatz kommen. Existiert im Fehlerfall keine geeignete Ersatzkonfiguration, schaltet das Netzmanagement auf den zweiten Planungsprozess um, der zur schnellen Fehlerbehebung einen heuristischen Ansatz benutzt.

2.7.1 Lineare Optimierung

Eine *Lineare Optimierung* (LP) ist ein Optimierungsproblem, bei dem sowohl das Optimierungsziel als auch die Nebenbedingungen aus linearen Gleichungen bestehen. Dabei wird die folgende Darstellung der Gleichungen als Standardform für LP bezeichnet.

$$\min c^T x = z \tag{2.1}$$
$$Ax = b \tag{2.2}$$
$$x \geq 0 \tag{2.3}$$

Das Optimierungsziel ist die Minimierung oder Maximierung der Gleichung $min\, c^T x = z$ unter der Bedingung das $Ax = b$ gilt. Zur Lösung solch eines Optimierungsproblems wird häufig der Simplex-Algorithmus [Dan63] verwendet.

2.7.2 Ganzzahlige lineare Optimierung

Während bei der linearen Optimierung alle Variablen kontinuierlich sind, werden bei einer *Ganzzahligen linearen Optimierung* (ILP) auch Variablen verwendet, die nur ganzzahlige Werte annehmen können. Bei der Optimierung von Transportnetzen finden ILPs ihre Anwendung, wenn zusätzlich Wellenlängen betrachtet werden, die entweder vorhanden sein können oder nicht. Optimierungen mit diskreten Variablen stellen eine mathematische Herausforderung dar und sind häufig NP vollständig. Das einfache Runden einer Variablen auf den nächsten ganzzahligen Wert führt dabei nicht zwangsweise zu einer optimalen beziehungsweise zu einer zulässigen Lösung. Das Optimierungsproblem lässt sich ähnlich wie für LPs beschreiben, allerdings dürfen die Variablen x_i nur diskrete Werte annehmen.

$$\min c^T x = z \tag{2.4}$$
$$Ax = b \tag{2.5}$$
$$x \geq 0 \tag{2.6}$$
$$x \in \mathbb{N}^m \tag{2.7}$$

Führt man eine Relaxierung der Variable x_i durch so erhält man Gemischte Ganzzahlige lineare Programme (MIPs). Ein Teil der Variablen kann kontinuierliche Werte annehmen, während die restlichen Variablen nur diskrete Werte annehmen können. Diese Mischform kann ebenfalls verwendet werden, um ein LP zu lösen, indem zunächst kontinuierliche Werte erlaubt sind. Die Ergebnisse für die diskreten Werten sind dann in den Lösungen enthalten.

2.7.3 Optimierung von Weitverkehrsnetzen

Im Folgenden werden die grundlegenden Formulierungen, die später in Kapitel 7 verwendet werden, vorgestellt, um ein Netzplanungsproblem als LP oder ILP zu formulieren. Um die Komplexität der Optimierung zu reduzieren, werden im ersten

Schritt die k-kürzesten Pfade zwischen Quell- und Zielknoten berechnet. Eine gleichzeitige Optimierung der Transportnetzpfade könnte den Kapazitätsbedarf im Transportnetz weiter senken, wäre aber aufgrund ihrer Komplexität mit der verfügbaren Rechenleistung nicht in akzeptabler Zeit lösbar. Zur Berechnung der k-kürzesten Pfade wird der Dijkstra-Algorithmus [Dij59] verwendet. Dazu werden einem gegebenen Graphen $G(\mathbb{V}, \mathbb{E})$ Kantengewichte w(e) zugeordnet und der kürzeste Pfad von einem Quellknoten zu einem Zielknoten abhängig von den Kantengewichten gesucht.

Eine weitere Aufgabe bei der Berechnung von kürzesten Pfaden, welche in der Netzplanung betrachtet wird, ist die Suche nach kürzesten knoten- und kantendisjunkten Pfaden zwischen Quell- und Zielknoten. Die unterschiedlichen kürzesten Pfade dürfen keine Knoten oder Kanten gemeinsam haben. Knoten- und kantendisjunkte Pfade sind vor allem bei der Planung von Ersatzpfaden für Arbeitspfade relevant. Zur Lösung des Problems wird in Kapitel 7 der Algorithmus von Bhandaris [Bha97] verwendet.

Um das Ziel, eine bestimmte Anzahl an Verkehrsanforderungen $d \in \mathbb{D}$ innerhalb eines Transportnetzes zu senden, existieren zwei grundlegende Formulierungen für eine geeigente beschreibung des LPs. Diese sind die flussbasierte und die pfadbasierte Methode, auf die in den nächsten Abschnitten kurz eingegangen wird.

Flussbasierte Methode

Die flussbasierte Methode (flow based approach) basiert auf dem Prinzip der Flusserhaltung der Kirchoffschen Regeln. Bei diesem Ansatz werden Verkehrsanforderungen von Quellknoten q zu Zielknoten z anhand von Flussvariablen $f_{q,z,k}$ für jede Kante k in dem Transportnetz definiert. Dabei wird ein Fluss am Quellknoten in das Netz eingefügt und am Zielknoten wieder entfernt. Für die dazwischenliegenden Knoten gilt die Regel der Flusserhaltung, das heißt, die Zwischenknoten dürfen keine Flüsse hinzufügen oder entfernen.

Pfadbasierte Methode

Die pfadbasierte Methode modelliert die Verteilung des Verkehrs auf einer bestimmten Anzahl von vorausberechneten Pfaden. Anstatt die Flüsse auf einer Knotenbasis zu betrachten, werden Flussvariablen für alle möglichen Pfade, auf denen der Verkehr geroutet werden kann, definiert. Die Flussvariablen beschreiben den Anteil des Gesamtverkehrs auf den vorausberechneten Pfaden von q nach z.

Beide Methoden haben ihre Vor- und Nachteile und ihre Anwendung hängt von den gewünschten Zielen ab. Aufgrund der Ähnlichkeit zum zielbasierten Routing ist die Formulierung des flussbasierten Ansatzes einfacher, allerdings wird eine Flussgleichung für jeden Knoten und jede Anforderung benötigt. Deshalb muss in Weitverkehrsnetzen eine große Anzahl an Gleichungen behandelt werden. Die Berechnung mit dem Simplex-Algorithmus für große Netze ist komplex, da gewöhnlich

die Anzahl der Iterationen der Simplex-Methode proportional zu der Anzahl der generierten Nebenbedingungen ist. Der pfadbasierte Ansatz benötigt dagegen die Vorausberechnung von Pfaden. Daher ist eine Variable für einen Pfad und eine Variable für eine Anforderungsbeziehung ausreichend. Allerdings kann das Optimum nicht mehr garantiert werden, wenn nur eine Untermenge an Pfaden verwendet wird. Dafür lassen sich gute Ergebnisse in annehmbarer Zeit berechnen. In Kapitel 6 wird ein pfadbasierter Ansatz verwendet, da aufgrund der Vorausberechnung von Pfaden die Anzahl der Nebenbedingungen bei der Optimierung kleiner als beim flussbasierten Ansatz ist.

2.7.4 Heuristiken

Neben der ganzzahligen linearen Optimierung verwendet das in dieser Arbeit realisierte Netzmanagement heuristische Lösungen, wenn im Fehlerfall keine geeignete Ersatzkonfiguration vorhanden ist. Heuristiken eignen sich aufgrund der schnellen Berechnung einer Lösung, was in einem Fehlerfall notwendig ist. Allerdings hängen die Qualität der Lösung und die Geschwindigkeit von den Startwerten der Heuristik ab. Ein heuristischer Ansatz für eine WDM-Topologie findet sich in [MBRM96]. Die Autoren beschreiben einen iterativen Ansatz der Simulated Annealing mit Flow Deviation kombiniert. Simulated Annealing verwenden die Autoren für die Suche nach einer guten Topologie und Flow Deviation dient dazu, den Verkehr optimal zu routen. Allerdings existiert keine Begrenzung der Anzahl der Wellenlängen beim kombinierten Ansatz, was die Suche nach einer Lösung vereinfacht. Ein erster Vergleich zwischen Heuristiken und optimalen Algorithmen findet sich in [RS96]. Verschiedene heuristische Ansätze, welche die Lösungszeit des WDM-Grooming-Szenarios weiter reduzieren, werden in [DG06] diskutiert.

Die genetischen Algorithmen stellen eine Klasse von Heuristiken dar. Ein genetischer Algorithmus ist ein Suchalgorithmus, der vom Prozess der natürlichen Evolution abgeleitet ist. Er basiert auf der natürlichen Selektion und Rekombination von Genomen in der Natur und unterscheidet sich von traditionellen Suchalgorithmen in folgenden Punkten [Gol89]:

- Arbeitet mit der Kodierung der Parameter und nicht mit den Parametern selbst
- Nutzt eine Population an Punkten für die Suche und nicht nur einen einzigen Punkt
- Nutzt Informationen der Zielfunktion, nicht Derivate oder andere Hilfsinformationen

Der genetische Algorithmus startet mit einer bestimmten Anzahl an Genomen in einer Generation, die miteinander kombiniert werden, um eine neue Generation zu bilden. Selektion stellt sicher, dass Genome mit einer schlechten Fitness aussortiert werden. Bleibt die Fitness einer Generation oder des besten Genoms über eine bestimmte Anzahl an Generationen konstant, wird der Algorithmus abgebrochen. Eine genauere

Beschreibung des genetischen Algorithmus folgt in Kapitel 7.

Eine weitere populäre Heuristik ist Simulated Annealing. Diese Methode ist von dem Abkühlungsprozess in Metallen abgeleitet, der verwendet wird, um Metalle zu erwärmen und kontrolliert abzukühlen, so dass diese ihre Eigenschaften durch die Neuanordnung der Atome verbessern. Die Temperatur entspricht bei der Optimierung einer Wahrscheinlichkeit, mit der sich ein Zwischenwert der Optimierung verschlechtern darf. Dadurch kann der Algorithmus ein lokales Optimum wieder verlassen und das globale Optimum finden. Allerdings kann wie bei allen Heuristiken nicht garantiert werden, dass der Algorithmus das globale Optimum findet. Einen Vergleich des genetischen Algorithmus mit Simulated Annealing findet man in [MC96], bei dem die beiden Algorithmen in ATM-Netzen verwendet werden, und in [TB00], in dem beide Methoden für das Design von Leitungspartitionierungsproblemen angewendet werden. Beide Ansätze zeigen, dass Simulated Annealing zwar schneller zu einer Lösung kommt als der genetische Algorithmus, allerdings der genetische Algorithmus bezogen auf die Fitnessfunktion bessere Ergebnisse erzielt. Der Grund für die bessere Fitness der besten Lösung beim genetischen Algorithmus liegt an dem vorhanden Pool an Lösungen, den jede Generation besitzt. Da beim genetischen Algorithmus mit einer bestimmten Wahrscheinlichkeit auch schlechte Lösungen überleben, findet der Algorithmus besser aus einem lokalen Optimum heraus. Das Vorhandensein von mehreren Lösungen stellt auch einen Vorteil für einen Netzbetreiber dar, der damit auf mehrere unterschiedliche Lösungen zurückgreifen kann.

3 Entwicklung und Analyse dienstorientierter Verkehrsmodelle

In diesem Kapitel werden dienstorientierte Verkehrsmodelle vorgestellt, bei denen nicht die momentane Änderung des Verkehrs, sondern die statischen Verkehrsmuster von Diensten wie *Internet Protocol Television* (IPTV), *Video On Demand* (VoD), *Content Delivery Networks* (CDN)s und *Peer to Peer* (P2P) betrachtet werden. Die vorgestellten Verkehrsmodelle berücksichtigen die räumliche Verteilung des Verkehrsaufkommens zwischen zwei oder mehreren Knotenpaaren in einem Weitverkehrsnetz. Es werden nur diejenigen Dienste untersucht, die in heutigen und zukünftigen Weitverkehrsnetzen den größten Anteil am Verkehrsaufkommen ausmachen. Für jeden dieser Dienste wird zunächst ein analytisches Modell entwickelt, mit dem sich das Verkehrsaufkommen zwischen den Netzknoten abhängig von bestimmten Eingangsparametern bestimmen lässt.

Abschließend erfolgt die Parametrisierung und Analyse des Verkehrsmodells anhand eines Beispielnetzes. Anhand des Fallbeispiels wird mit Hilfe eines Hypothesentests ein Vergleich mit Verkehrsmodellen aus der Literatur durchgeführt, um die entwickelten Verkehrsmatrizen mit real gemessenen Verkehrsmatrizen zu vergleichen. Die Ergebnisse in diesem Kapitel wurden in [PMKS07] und [PMS+11] veröffentlicht.

3.1 Verwendete Dienste und entwickeltes Verkehrsmodell

Die vorgestellten Verkehrsmodelle basieren auf dem Ansatz aus [DW00], bei dem die Anzahl der Internet-Hosts für die Beschreibung der Verkehrsströme verwendet wird. Dieser Ansatz wird um zwei Maßnahmen erweitert, die den heutigen Datenaustausch im Internet stärker berücksichtigen. Der Internetverkehr wird nicht nur nach Daten- und Sprachverkehr unterschieden, sondern nach den einzelnen Dienste differenziert. Zusätzlich werden noch die Internetknoten, an denen Netzbetreiber den Verkehr untereinander austauschen, in dem Modell berücksichtigt. An den Internet-Austauschknoten, wie den deutschen Internetknoten in Frankfurt (DE-CIX), entsteht ein hohes Verkehrsaufkommen, da an diesen Netzknoten der Verkehr von einem Netzbetreiber zu einem anderen übergeben wird. So kann es vorkommen, dass die Daten von zwei Nutzern, die sich zwar an dem selben Ort aber bei zwei unterschiedlichen Netzbetreibern befinden, erst den Weg über einen Internet-Austauschknoten

nehmen, anstelle des direkten kürzesten Pfads. Abbildung 3.1 zeigt den schematischen Aufbau des Netzmodells, welches für die Verkehrsanalyse verwendet wird.

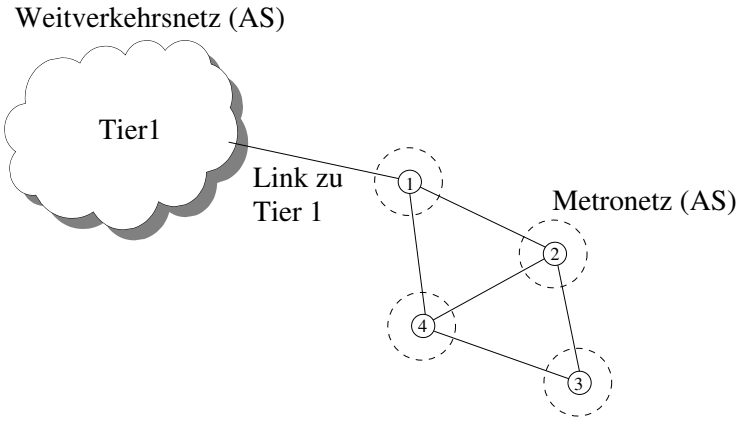


Abbildung 3.1: Verwendetes Netzmodell für die Verkehrsmodelle

Die Knoten 1 bis 4 in dem Modell entsprechen Metronetzen die über ein Weitverkehrsnetz mit weiteren Metronetzen verbunden sind. Ein Metronetz stellt also einen Netzknoten in einem Weitverkehrsnetz dar. Als Metronetze werden üblicherweise Transportnetze innerhalb von Städten sowie ihrer näheren Umgebung bezeichnet. Weitverkehrsnetze bezeichnen die Netzinfrastruktur eines Landes oder die Netzinfrastruktur über Ländergrenzen hinweg. In Abbildung 3.1 ist ein Weitverkehrsnetz bestehend aus vier Metronetzen gezeigt, das über einen Tier-1 Netzbetreiber mit weiteren Weitverkehrsnetzen verbunden ist. Ein Tier-1-Anbieter ist für die Weiterleitung der Daten aus einem Weitverkehrsnetz innerhalb eines Landes über Ländergrenzen hinweg verantwortlich. Beispielsweise wird ein europäisches Weitverkehrsnetz über einen Tier 1-Netzbetreiber mit einem Weitverkehrsnetz in den USA verbunden.

Die vorgestellte Verkehrsanalyse konzentriert sich auf den internen Verkehr eines *Autonomes System* (AS), der durch die oben beschriebenen Dienste generiert wird. Ein AS bezeichnet in dieser Arbeit eine Netzinfrastruktur, die einem Netzbetreiber gehört und von diesem überwacht wird. Ein AS ist daher entweder ein Metronetz oder ein Weitverkehrsnetz. Allgemein können drei Kategorien von Verkehrsströmen unterschieden werden:

- Transitverkehr durch ein autonomes System
- Interner Verkehr innerhalb eines autonomen Systems
- Transitverkehr, der in einem autonomen System terminiert wird oder entsteht

Transitverkehr sind Verkehrsströme, die durch ein AS durchgeleitet und von einem dedizierten Eingangs- zu einem Ausgangsknoten transportiert werden. Die Last die durch diese Transitverkehrsflüsse hervorgerufen wird, hängt von den vertraglichen Regeln zwischen dem Netzbetreiber und den Transitpartnern ab und wird in dem Modell als additive Konstante behandelt. Interner Verkehr bezeichnet diejenigen Verkehrsflüsse, die innerhalb eines AS entstehen und innerhalb dessen wieder terminiert werden. Die internen Verkehrsströme verlassen ein AS nicht. Bei der letzten Kategorie

handelt es sich um Transitverkehrsströme, die in einem AS entstehen und zu einem anderen AS geroutet und dort terminiert werden.

Der Peering-Verkehr zwischen verschiedenen Providern wird in dem dienstorientierten Verkehrsmodell ebenfalls abgebildet. Peering bezeichnet in dieser Arbeit Netzknoten, an denen Netzbetreiber den internen Verkehr an einen anderen Netzbetreiber übergeben, um den Verkehr zum Zielknoten zu routen, der sich in einem anderen AS befindet. In jedem AS existiert mindestens ein Peering-Knoten. Peering-Knoten routen besonders viele Verkehrsflüsse, da sich mehrere Netzbetreiber an einem Peering-Knoten gegenseitig die Daten übergeben.

Eine weitere Einflussgröße auf das Routing der Verkehrsströme stellen Server dar, auf denen Inhalte bestimmter Dienste gespeichert werden. Beispielsweise speichern Dienste wie CDNs den Inhalt auf weltweit verteilten Servern, entsprechend der Nachfrage der Kunden. Das Verkehrsmodell berücksichtigt dies, indem ein Ortsfaktor verwendet wird, der angibt, welcher Anteil des Verkehrsaufkommens eines Dienstes in dem Netz eines Betreibers bleibt und welcher Verkehrsanteil an einem Peering-Knoten an ein anderes Netz übergeben wird. In Abbildung 3.2 ist die Datenverteilung der einzelnen Dienste dargestellt.

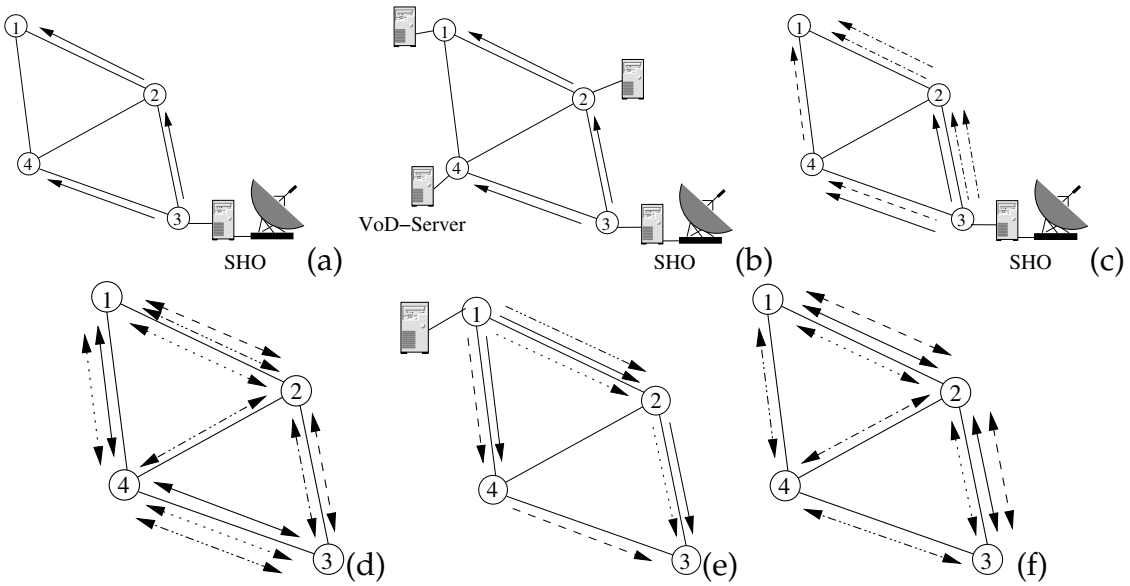


Abbildung 3.2: Datenverteilung der einzelnen Dienste (a) IPTV, (b) lokales VoD, (c) zentrales VoD, (d) P2P, (e) CDN, (f) VPN

Die Anzahl der Pfeile auf den Kanten gibt abstrakt das Verkehrsaufkommen auf den jeweiligen Kanten an. Die verschiedenen Pfeilarten stehen dabei für einen Verkehrsfluss von Ziel- zu Quellknoten. Bei den Diensten IPTV, VoD und CDN hängt die Datenverteilung entscheidend von der Verteilung der Server ab, auf dem die Inhalte gespeichert sind. Für den VoD-Dienst werden in diesem Kapitel zwei Szenarien unterschieden, die in Abbildung 3.2 (b) und (c) dargestellt sind.

In Abbildung 3.2 (b) werden die Inhalte sowohl an der Einspeisestelle der Inhalte (Knoten 3) als auch auf lokalen Servern an den Netzknoten gespeichert. Ein Netzknoten entspricht wiederum einem Metronetz. In Abbildung 3.2 (c) werden die Inhalte dagegen ausschließlich am Einspeiseknoten gespeichert und von dort verteilt.

Die in Tabelle 3.1 gezeigten Parameter dienen als Grundlage zur Berechnung der Verkehrsmatrizen für die einzelnen Dienste. Die Parameter dienen zur Unterscheidung der Routingprofile der Dienste und schließen unterschiedliche Faktoren wie Bevölkerungsdichte und Unternehmensdichte an einem Standort mit ein, die unterschiedlich starke Auswirkungen auf das berechnete Verkehrsaufkommen pro Dienst haben.

Parameter	Beschreibung
$p_n \in [0,1]$	Peering-Knotenfaktor, der die Größe des Peering-Knotens an Knoten n angibt.
$t_n^i \in \{0,1\}$	Indikator, ob Knoten n als Speicherort für Verkehrstyp i dient.
$m_{sd}^i \in \{0,1\}$	Faktor, der angibt, ob ein Link, der Knoten s und d verbindet, existiert und ein Teil des Multicast-Baums i ist.
$b_n^i \in [0,1]$	Anteil der Bevölkerung am Knoten n zur Hauptverkehrsstunde, die Verkehr vom Typ i erzeugt. Definiert als Produkt der Penetration des Diensttyps i und dem Anteil maximal gleichzeitiger Nutzer.
$l \in [0,1]$	Ortsfaktor, der angibt, welcher Anteil des Verkehrs innerhalb eines Netzes bleibt.
$P_n \in \mathbb{Z}^+$	Anzahl Nutzer bei Knoten n.
$T_{sd}^i \in \mathbb{R}$	Verkehrsaufkommen des Dienstes i von Knoten s zu Knoten d.
$C_u^i \in \mathbb{R}$	Durchschnittliche Datenrate des Verkehrstyps i pro Nutzer.
$C_n^i \in \mathbb{R}$	Durchschnittliche Datenrate des Verkehrstyps i pro Knoten.
$c_n \in \mathbb{R}$	Faktor, der die Konzentration der Unternehmenszentren an Knoten n angibt.

Tabelle 3.1: Parameter des dienstorientierten Verkehrsmodells

Das Verkehrsaufkommen zwischen zwei Knotenpaaren berechnet sich aus der Bevölkerungsdichte P_n und der Anzahl der Unternehmen c_n an einem Standort. Für die Unternehmensdichte pro Knoten wurde die Studie in [Hut05] verwendet, welche die Aufteilung der Unternehmen in Deutschland analysiert. Der Peering-Knotenfaktor p_n umfasst den Wertebereich $[0,1]$ und beschreibt, ob es am Knoten n einen Peering-Punkt gibt und wenn ja, welche Größe dieser besitzt. Auf diese Weise wird berücksichtigt, dass ein Transportnetz mehr als einen Peering-Knoten besitzen kann. In dem Modell kann auch ein Ersatz-Peering-Knoten verwendet werden, der als Entlastung bei sehr hohem Verkehrsaufkommen oder im Fehlerfall des primären Peering-Knotens dient. Im allgemeinen bestimmen die Netzbetreiber, welche Knoten als Peering-Knoten verwendet werden. Peering-Knoten besitzen besonders hohe Anforderungen bezüglich der Prozessorgeschwindigkeit, der Routing-Kapazität und

des Pufferspeichers.

3.1.1 IPTV

Der IPTV-Verkehr wird im Kernnetz zwischen Quellknoten und Zielknoten über einen Multicast-Baum verteilt. An der Quelle befindet sich das *Super Hub Office* (SHO), von dem aus die verschiedenen Sender in das Netz eingespeist werden. Die Übertragung des IPTV-Verkehrs findet von den SHO zu lokalen *Video Hub Office* (VHO)s statt, die den Verkehr wiederum zu den Nutzern weiterleiten. Die Verwendung von mehreren SHOs, so wie unterschiedliche Multicast-Bäume, sollen eine hohe Verfügbarkeit garantieren. Das Verkehrsaufkommen von IPTV hängt von der Anzahl der Anbieter, der angebotenen Kanäle und der angebotenen Auflösung und Datenrate ab. Die heutige Datenrate für *Standard Definition Television* (SDTV) beträgt zwischen $3{,}5$ Mbit/s und $5{,}0$ Mbit/s, während für hochauflösendes Fernsehen *High Definition Television* (HDTV) die Datenrate zwischen $8{,}0$ Mbit/s und $12{,}0$ Mbit/s liegt. Die Verkehrslast T_{sd}^{IPTV} zwischen Knoten s und d, die IPTV generiert, hängt sowohl von der benötigten Bitrate C_n^{IPTV} als auch von den benutzen Links m_{sd}^{IPTV} zwischen s und d ab.

$$T_{sd}^{\mathrm{IPTV}} = \sum_{i \in \mathbb{Z}^+} C_n^{\mathrm{IPTV}} \cdot m_{sd}^{\mathrm{i}} \tag{3.1}$$

3.1.2 Video on Demand

VoD dient zur Verteilung von Videodiensten zu individuellen Kunden gemäß ihrer Anfrage. Dabei wird zu jedem Kunden, der einen bestimmten Film anfordert, ein Videostream gesendet. Da die Speicherung aller Filme auf einer Datenbank mit zunehmender Anzahl an Nutzern und zunehmender Popularität von Filmen nicht skaliert, werden aktuelle populäre Filme auf lokalen VHOs gespeichert, um den Verkehr im Kernnetz zu minimieren. Dazu werden die Inhalte auf den VHOs regelmäßig erneuert, indem aktuellere Filme während Nebenverkehrszeiten, beispielsweise in der Nacht, von den SHOs zu den VHOs übertragen werden [CCY+06]. Der Datentransfer der Filme auf die VHOs erfordert keine bestimmte Bandbreite oder zeitliche Begrenzungen und kann daher mittels Protokollen wie dem *File Transfer Protocol* (FTP) übertragen werden.

Auch wenn Internetdienstanbieter eine große Vielfalt an VoD-Inhalten anbieten möchten, ist es nicht kosteneffizient, alle Filme auf jeder vorhanden VHO zu speichern, da diese dann mit schnellerer Hardware und größerem Speicher aufgerüstet werden müssen. Stattdessen bietet sich die Verwendung eines Cache-Management-Algorithmus an, der basierend auf der Anzahl der Filmanfragen von Nutzern, die populären Inhalte von der SHO zu den entsprechenden VHOs verschiebt. Die restlichen Filme sind nur auf der SHO gespeichert und werden auf Anfrage mittels

einer Unicast-Übertragung zu den Nutzern geroutet. Damit nur die beliebtesten Filme auf einem VHO gespeichert werden, sorgt eine Zeitüberwachung dafür, dass nach einer vorgegebenen Zeit weniger angeforderte Filme wieder auf dem VHOs gelöscht werden, wenn deren Nachfrage unter einen gewissen Schwellenwert gefallen ist. Der Unicast-Verkehr von der SHO zu den Nutzern wird durch die Verwendung des Cache-Management-Algorithmus, den benutzen Codecs und der Anzahl der Benutzer zur Hauptverkehrsstunde beeinflusst. Dagegen hängt der Verkehr zum Erneuern der auf dem VHO gespeicherten Filme von der Anzahl der monatlich erneuerten VoD-Titel und der Anzahl der Titel ab, die auf einem VHO gespeichert sind. Wie bereits erwähnt werden zwei verschiedene VoD-Szenarien untersucht: VoD-Inhalte, die exklusiv auf den SHO gespeichert werden und VoD-Inhalte die sowohl auf dem SHO als auch auf den VHOs gespeichert werden.

Speicherung der VoD-Inhalte exklusiv auf dem SHO

Zunächst werden die VoD-Inhalte exklusiv auf dem SHO gespeichert und zu den individuellen Nutzern auf deren Anfrage gesendet. Die Verkehrsverteilung für diese Verbreitung der VoD-Inhalte ist in Abbildung 3.3 (c) dargestellt. Die Verkehrslast im Weitverkehrsnetz steigt mit der Anzahl der Nutzer an, da identische Inhalte mittels eines Verkehrsflusses pro Nutzer übertragen werden. Die Größe C_u^{cVoD} gibt die durchschnittliche Datenrate pro Nutzer für einen On-Demand-Inhalt an und der Parameter t_s^{cVoD} indiziert, ob der Knoten s als Speicherort für VoD-Inhalte dient.

$$T_{sd}^{\mathrm{cVoD}} = t_s^{\mathrm{cVoD}} \cdot (1 - t_d^{\mathrm{cVoD}}) \cdot b_d^{\mathrm{cVoD}} \cdot P_d \cdot C_u^{\mathrm{cVoD}} \tag{3.2}$$

Des Weiteren ist für die Berechnung des Verkehrsaufkommens wiederum die maximale Anzahl der aktiven Nutzer zur Hauptverkehrsstunde entscheidend. Dies wird mithilfe des Parameters b_d^{cVoD} modelliert, der den prozentualen Anteil der aktiven Nutzer angibt, die VoD-Inhalte nutzen.

Speicherung der VoD-Inhalte auf dem SHO und den VHOs

In diesem Abschnitt wird die Speicherung der VoD-Inhalte sowohl auf dem SHO als auch auf den VHOs betrachtet. Lokal auf den VHO zu speichernde Inhalte können während Nebenverkehrszeiten mit geringer Datenrate von dem SHO zu den VHOs übertragen werden, um keine zusätzliche Bandbreite während Hauptverkehrszeiten zu verwenden. Abbildung 3.3 (d) zeigt die Verteilung der zentral und lokal gespeicherten VoD-Inhalte. Das SHO, welches sich bei Knoten 13 (Munich) befindet, überträgt die VoD-Inhalte über ein Multicast-Schema zu den VHOs. Die entsprechende Formel wird in ähnlicher Weise abgeleitet, wie für den Fall der broadcast IPTV-Inhalte. Der Indikator m_{sd}^{lVoD} gibt dabei an, ob der VoD-Verkehr C_n^{lVoD} den Link sd benutzt.

$$T_{sd}^{\mathrm{lVoD}} = C_{n}^{\mathrm{lVoD}} \cdot m_{sd}^{\mathrm{lVoD}} \tag{3.3}$$

Der gesamte lokale VoD-Verkehr C_n^{lVoD} berechnet sich aus der Anzahl der On-Demand-Filme, der durchschnittlichen Speichergröße jedes Films und der Erneuerungsrate der Inhalte.

3.1.3 Content Delivery Networks

Video Streaming hat in den letzten Jahren einen steigenden Anteil am Internetverkehr erfahren und trägt mittlerweile zu 13 % am gesamten Internetaufkommen bei [Cis08]. Um die Verkehrsstruktur von Video-Sharing-Webseiten zu analysieren, wurde eine Fallstudie anhand der Website Youtube durchgeführt. Eine entscheidende Eigenschaft des Internetverkehrs von Youtube ist, dass der Verkehr über ein Unicast-Schema verbreitet wird. Jede Nutzeranfrage wird unabhängig von den anderen bedient, so dass dieselben Inhalte zu denselben Orten mehrfach parallel übertragen werden und einen wesentlichen höheren Verkehr auf den entsprechenden Links verursachen. Aus diesem Grund werden CDN verwendet, um durch effizientes Verteilen der Inhalte, den Verkehr im Kernnetz erheblich zu reduzieren und die Netzkosten zu verringern. CDNs sind ein Netz lokal verteilter Server, die miteinander verbunden sind und Inhalte effizient an die Nutzer übermitteln.

Als Grundlage für die Untersuchungen von CDNs wird das Verkehrsmodell von Akamai [Aka11] verwendet. Es wird ein Verteilungsort bei Knoten s angenommen, an dem der Speicherortindikator t_s^{CDN} den Wert eins annimmt. Die Größe C_u^{CDN} repräsentiert die durchschnittliche Datenrate pro Nutzer für einen CDN-Inhalt.

$$T_{sd}^{\mathrm{CDN}} = t_s^{\mathrm{CDN}} \cdot (1 - t_d^{\mathrm{CDN}}) \cdot b_d^{\mathrm{CDN}} \cdot P_d \cdot C_u^{\mathrm{CDN}} \tag{3.4}$$

Abbildung 3.2 (e) zeigt die Verteilung des CDN-Inhalts von dem CDN-Server an Knoten 1 zu den restlichen Weitverkehrsnetzknoten. Aufgrund des angenommen Unicast-Verteilungsschemas sind mehrere Verkehrsflüsse pro Kante möglich.

3.1.4 Peer-to-Peer

Bei der Berechnung des P2P-Verkehrs haben die Peering-Knoten (Internet-Austauschknoten) eines Weitverkehrsnetzes einen entscheidenden Einfluss auf das Routing. Da die Daten innerhalb eines P2P-Netzes abhängig vom Inhalt weltweit gespeichert sind, erfolgt der Austausch der Daten über mehrere Netze von unterschiedlichen Netzbetreibern. Wie oben bereits erläutert, wird der Verkehr zwischen zwei Netzbetreibern an den Peering-Knoten übergeben, was dazu führt, dass an diesen Knoten ein besonders hohes Verkehrsaufkommen entsteht. Um das Muster der Verkehrsflüsse von P2P zu beschreiben, werden zwei zusätzliche Parameter verwendet. D_i bezeichnet

den gesamten durch die Nutzer erzeugten abgehenden Verkehr bei Knoten i und D_{ij} beschreibt die Menge des Verkehrs von Knoten i der für Knoten j bestimmt ist.

$$D_i = b_i^{\mathrm{P2P}} \cdot P_i \cdot C_u^{\mathrm{P2P}} \tag{3.5}$$

Beim P2P-Verkehr kommt der Ortsfaktor l aus Tabelle 3.1 zum tragen, der angibt, mit welcher Wahrscheinlichkeit der gesuchte Inhalt in dem selben Netz des Nutzers ist, der diesen Inhalt sucht. Aufgrund der Eigenschaft von heutigen P2P-Netzen, dass die Daten von mehreren Nutzern gleichzeitig heruntergeladen werden, unterteilt sich der gesamte ausgehende Verkehr an einem Knoten in den internen Verkehrsanteil D_i^{I} und den externen Verkehrsanteil D_i^{E}. Der interne Verkehrsanteil beschreibt das Verkehrsaufkommen, das innerhalb des Netzes eines Netzbetreibers bleibt. Der externe Verkehrsanteil beschreibt dagegen denjenigen Verkehrsanteil, der über einen Peering-Knoten zu einem anderen Netzbetreiber geroutet wird. Schaut sich beispielsweise ein Kunde am Knoten „München“ einen Film auf einem Server in den USA an, so wird der Verkehr aus Sicht des deutschen Netzbetreibers in diesem Modell als externer Verkehr bezeichnet.

$$D_i^{\mathrm{I}} = l \cdot D_i \tag{3.6}$$

$$D_i^{\mathrm{E}} = (1 - l) \cdot D_i \tag{3.7}$$

Das Verkehrsaufkommen D_{ij}^{I}, das den gesamten internen Verkehr zwischen Knoten i und Knoten j repräsentiert, wird berechnet, indem das gesamte Verkehrsaufkommen von Knoten i zu allen anderen Netzknoten entsprechend den aktiven Nutzer skaliert wird. Die Skalierung erfolgt anhand der Wahrscheinlichkeit mit der Knoten i eine Verbindung zu einem Peer in einem Knoten j aufnimmt. Diese Wahrscheinlichkeit ist proportional zum Anteil der aktiven Nutzer an diesem Knoten.

$$D_{ij}^{\mathrm{I}} = \frac{b_j^{\mathrm{P2P}} \cdot P_j}{\sum_{\forall k} b_k^{\mathrm{P2P}} \cdot P_k} \cdot D_i^{\mathrm{I}} \tag{3.8}$$

Für die Berechnung des externen P2P-Verkehrs wird angenommen, dass dieser über die Peering-Knoten geroutet wird. Die Größe des eingehenden Verkehrs entspricht dabei der des ausgehenden Verkehrs.

$$\begin{aligned} D_{ij}^{\mathrm{E}} = & \lfloor \frac{1}{1+p_i} \rfloor \cdot p_j \cdot D_i^{\mathrm{E}} + \\ & + \lfloor \frac{1}{1+p_j} \rfloor \cdot p_i \cdot D_j^{\mathrm{E}} + \\ & + \lceil p_i \cdot p_j \rceil \cdot p_j \cdot D_i^{\mathrm{E}} \end{aligned} \tag{3.9}$$

Daher existieren vier unterschiedliche Fälle, abhängig davon, ob der Quell- oder der

Zielknoten einen Peering-Knoten darstellt. Für den Fall, dass beide Knoten keine Peering-Knoten sind, erfolgt kein Austausch des Verkehrs über diese Knoten und D_{ij}^{E} ist Null. Die drei verbleibenden Fälle sind:

- Die Quelle ist kein Peering-Knoten und das Ziel ist ein Peering-Knoten (1)
- Die Quelle ist ein Peering-Knoten und das Ziel ist kein Peering-Knoten (2)
- Beide Knoten, Quelle und Ziel, sind Peering-Knoten (3)

Alle drei Fälle werden durch die Summanden in der Formel für das externe Verkehrsaufkommen D_{ij}^{E} abgebildet. Aufgrund der Begrenzung der Peering-Knotenfaktoren p_n auf eins, erfolgt eine automatische Skalierung des Routings.

Für Fall (1) ist der erste Term in Formel 3.9 ungleich Null und der erzeugte Verkehr an Knoten i, der für externe Netze bestimmt ist, wird entsprechend der Größe des Peering-Knotens i zu Knoten j gesendet. Dasselbe gilt für Fall (2), bei dem die Quelle ein Peering-Knoten ist. In diesem Fall ist der zweite Term der Formel 3.9 ungleich Null. Zusätzlich wird angenommen, dass eingehender und abgehender Verkehr an einem Knoten sich ungefähr die Waage halten. Im Fall (3) ist D_{ij}^{E} gleich $p_j \cdot D_i^{\mathrm{E}}$ und damit korrespondiert der Anteil des externen P2P-Verkehr mit der Größe des Peering-Knotens j. Das gesamte Verkehrsaufkommen T_{sd}^{P2P} zwischen den Knoten s und d berechnet sich nach Formel 3.10 aus der Summe des internen (D_{sd}^{I}) und externen (D_{sd}^{E}) P2P-Verkehrsaufkommens.

$$T_{sd}^{\mathrm{P2P}} = D_{sd}^{\mathrm{I}} + D_{sd}^{\mathrm{E}} \tag{3.10}$$

Die Verteilung des P2P-Verkehrs ist in Abbildung 3.2 (d) vereinfacht dargestellt. Dabei ist zu beachten, dass das eingehende und ausgehende Verkehrsaufkommen eines Peering-Knotens, abhängig von den gesuchten Inhalten, in der Regel höher liegt als das Verkehrsaufkommen der restlichen Knoten eines Weitverkehrsnetzes. Dies ist vor allem bei internationalen Inhalten der Fall.

3.1.5 Virtual Private Networks

Virtual Private Networks (VPN)s werden unter anderem in Site-to-Site VPNs und Remote Access VPNs untergliedert. Site-to-Site VPNs verbinden mehrere räumlich verteilte Geschäftsstellen eines Unternehmens über mehrere Weitverkehrsnetze hinweg miteinander. Dagegen dienen Remote Access VPNs dazu, mobile Nutzer oder Nutzer von zu Hause aus mit dem Netz eines Unternehmens zu verbinden. Frühere Studien haben gezeigt, dass die durchschnittlich jährlich erwartete Wachstumsrate für Geschäftsverkehr im Bereich von 15 % bis 45 % liegt [GD11] und einen immer größeren Anteil am gesamten Netzverkehr ausmacht.

Zur Berechnung des VPN-Verkehrs wird wiederum der populationsbasierte Ansatz in Kombination mit einem Gewichtungsfaktor zur Beschreibung der Anzahl der Unternehmen an einem Standort verwendet [Hut05]. Der ausgehende Verkehr an

einem Knoten ist somit proportional zur Anzahl der Bevölkerung an einem Knoten, gewichtet mit dem Faktor c_s, der die Konzentration von Unternehmenszentren an einem Standort angibt.

$$T_{sd}^{\mathrm{VPN}} = \frac{c_d \cdot b_d^{\mathrm{VPN}} \cdot P_d}{\sum_{\forall k} c_k \cdot b_k^{\mathrm{VPN}} \cdot P_k} \cdot c_s \cdot b_s^{\mathrm{VPN}} \cdot P_s \cdot C_u^{\mathrm{VPN}} \tag{3.11}$$

Wie bei der Berechnung des P2P-Verkehrs beschrieben, wird das gesamte ausgehende Verkehrsaufkommen auf die Zielknoten entsprechend ihrer Wichtigkeit verteilt. Die Verteilung des VPN-Verkehrs zwischen Kernnetzknoten ist in Abbildung 3.2 (f) exemplarisch dargestellt. Die Knoten 1 und 3 stellen Knoten mit einer höheren Konzentration von Unternehmenszentren dar, was zu einem erhöhten Verkehrsaufkommen führt.

3.2 Fallstudie anhand eines Referenznetzes

In diesem Abschnitt wird eine Fallstudie für die oben beschriebenen Verkehrsmodelle durchgeführt, die als Eingangsparameter für die Netzplanung in Kapitel 7 dient. Als Netztopologie wird das Deutschland-17-Knotennetz verwendet [HBB+04]. Das Verkehrsaufkommen zwischen den Weitverkehrsnetzknoten wird für das Jahr 2010 berechnet und eine Prognose für eine dreijährige Zeitspanne erstellt. Die resultierenden Verkehrsflüsse sind in Abbildung 3.3 dargestellt. Die Pfeile geben dabei die Richtung des Verkehrsflusses an und die Anzahl der Pfeile symbolisiert die Größe des Verkehrsaufkommens auf der jeweiligen Kante.

3.2.1 Parametrisierung des Verkehrsmodells

Im Folgenden wird beschrieben, welche Werte für die Eingabeparameter des Verkehrsmodells verwendet werden, um das Verkehrsaufkommen zwischen den Kernnetzknoten mit den vorher hergeleiteten Formeln zu berechnen. Um die fehlenden Parameter aus Tabelle 3.1, wie zum Beispiel die Verkehrslast zur Hauptverkehrszeit an Knoten n, für das Verkehrsmodell zu bestimmen, werden entsprechend die Parameter aus der Untersuchung in [BGH+03] gewählt und auf das Jahr 2010 skaliert. Aus den skalierten Verkehrsmatrizen können anschließend die fehlenden Parameter für die in dieser Arbeit neu entwickelten Verkehrsmodelle verwendet werden. Für die Skalierung des Verkehrsaufkommens im Jahr 2010 werden die Daten aus [SM09] für die Zeitspanne von 2004 bis 2008 und die Daten aus [FT00] für die Zeitspanne 2008 bis 2010 betrachtet. Die Verkehrsmatrizen aus dem Jahr 2004 werden zunächst für das untersuchte Referenznetz mit den jährlichen Wachstumsraten aus [BGH+03] auf das Jahr 2008 hochgerechnet. Im nächsten Schritt werden die Verkehrsmatrizen entsprechend den Daten aus [SM09] und [FT00] für das Jahr 2010 extrapoliert.

Aufgrund der erhaltenen Verkehrsmatrizen, können die fehlenden Parameter für

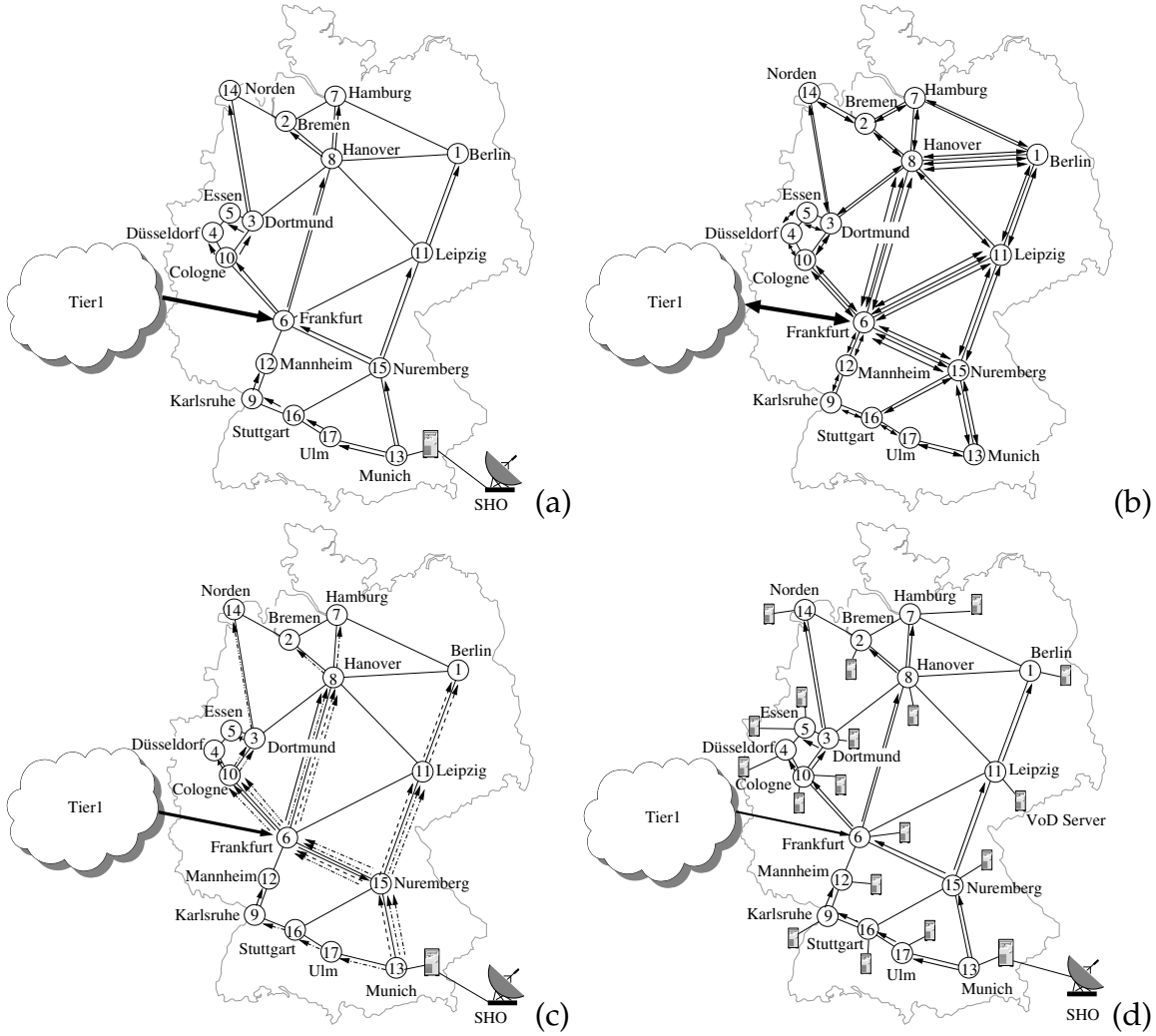


Abbildung 3.3: Verkehrsmuster von (a) IPTV, (b) P2P, (c) zentrales VoD, (d) lokales VoD

die P2P-, CDN- und VPN-Dienste abgeleitet werden. Diese sind der Spitzenanteil zur Hauptverkehrsstunde an Knoten n, der den Verkehr vom Typ i (b_n^i) erzeugt und die durchschnittliche Datenrate C_u^i des Verkehrstyps i pro Nutzer. Zusätzlich wird eine Gleichverteilung für b_n^i für alle Knoten n vom Dienst i angenommen. Daher muss nur das Produkt aus b_n^i und C_u^i abgeschätzt werden. Im ersten Schritt wird der Verkehr des Modells als Funktion dieser beiden Variablen berechnet. Die vorherige Skalierung der Verkehrsmatrizen aus der Literatur und der Vergleich mit den Modellen in [BGH+03] erlaubt die Abschätzung der fehlenden Variablen, die zur Berechnung des Verkehrsaufkommens mit Hilfe der entwickelten Verkehrsmodelle benötigt werden.

Für die Betrachtung von IPTV wird angenommen, dass sich innerhalb des Referenz-

netzes in München die SHO befindet. Um das Datenvolumen zu berechnen, werden drei verschiedene IPTV-Dienstanbieter angenommen, von denen jeder 100 Kanäle anbietet, die aus SDTV und HDTV Kanälen bestehen. Des Weiteren ist immer nur eine der SHOs zur gleichen Zeit aktiv, während die übrigen Weitverkehrsnetzknoten als VHOs agieren. Alle Systemparameter zur Berechnung der Verkehrslast pro Dienst für das Jahr 2013 sind in Tabelle 3.2 zusammengefasst.

Parameter	Wert
Anzahl Provider	3
Kanäle pro Provider	100
Datenrate SDTV	7 Mbit/s
Datenrate HDTV	12 Mbit/s
Anzahl on-demand Titel	$2000 - 6000$
Speichergröße pro Film	4.5 Gbit/s - 20 Gbit/s
Anteil der VoD-Nutzer	10 %

Tabelle 3.2: Systemparameter für die Berechnungen

Bei der Berechnung der Verkehrslast für IPTV spielt die Anteil der HDTV-Kanäle eine entscheidende Rolle. Für die Berechnungen wurden zwei unterschiedliche Verteilungen angenommen, die von dem prognostizierten Jahr abhängen. Für das Jahr 2010 werden mehr SDTV als HDTV-Kanäle angenommen, um die Markteinführung von IPTV zu berücksichtigen. Für Verkehrsprognosen zu einem späteren Zeitpunkt werden entsprechend die Anzahl der HDTV-Kanäle erhöht. Die gleiche Vorgehensweise wird für den VoD-Dienst angewandt. Zunächst werden eine geringere Anzahl an gespeicherten Filmtitel pro SHO und VHO angenommen, die auch eine geringere Speichergröße besitzen. Diese Annahme spiegelt Filmtitel mit einer geringeren Auflösung wieder, wie sie zumeist heute angeboten werden. Für Prognosen über das Jahr 2010 hinaus, werden entsprechend sowohl die Anzahl der gespeicherten Filmtitel als auch die Speichergröße der Filmtitel erhöht.

Eine weitere Einflussgröße bei einem VoD-Dienst ist die Erneuerungsrate, mit der Filme auf der VHOs aktualisiert werden. Um eine Obergrenze für das Datenvolumen angeben zu können, wird ein Worst-Case-Szenario gewählt, in dem angenommen wird, dass alle auf der VHO gespeicherten Filme, einmal im Monat erneuert werden. In der Realität hängt die Erneuerungsrate von der Beliebtheit der einzelnen Filmtitel ab und sollte unter der angenommenen Obergrenze liegen. Um die benötigte Bandbreite der Filme zu bestimmen, die nicht auf der VHO, sondern nur auf der SHO gespeichert sind, wird angenommen, dass zehn Prozent der IPTV-Nutzer auch den VoD-Dienst benutzen [Net06]. Nach [Gmb09] werden für 2013 fünf Millionen IPTV-Nutzer erwartet und es wird angenommen, dass 15 % der IPTV-Nutzer den VoD-Dienst zur Hauptverkehrsstunde verwenden.

Eine weitere Einflussgröße für den VoD-Verkehr in einem Kernnetz stellt die Anzahl

der erfolgreich abgerufenen Filmtitel von der VHO dar. Für die Untersuchungen variiert die Trefferquote für das Vorhandensein von Filmen zwischen 60 % und 95 %. Je niedriger die Trefferquote gewählt wird, umso mehr Nutzeranfragen müssen von einer VHO zu der SHO weitergeleitet werden und verursachen so eine höhere Verkehrslast im Weitverkehrsnetz. Die Trefferquote beeinflusst nicht nur die Höhe des Verkehrsaufkommens, sondern auch die Dienstgüte, die für den Verkehr benötigt wird. Für den Fall, dass der angeforderte Filmtitel sich nicht auf der VHO befindet, wird der Filmtitel von der SHO zum Kunden übertragen. Daher muss die Dienstgüte über die gesamte Strecke erfüllt werden.

Der größte deutsche Internet-Austauschknoten in Frankfurt (DE-CIX) [Exc] dient als Haupt-Peering-Knoten für die Untersuchungen der Verkehrslast von CDN, P2P und VPN für das Deutschland-17-Knotennetz. Das bedeutet, dass alle Verkehrsströme in andere Länder, beziehungsweise aus anderen Ländern, über diesen Knoten geroutet werden. Damit hat der Internet-Austauschknoten ein besonders hohes Verkehrsaufkommen zu bewältigen, da hier alle Verkehrsströme aller Netzknoten aggregiert werden, die das Referenznetz verlassen. Als Ersatz-Peering-Knoten dient der Knoten „Norden“, der allerdings in den beschriebenen Untersuchungen nicht verwendet wird. Als Quellknoten für CDN-Dienste dient ebenfalls Frankfurt, da hier die Verkehrsflüsse aus anderen Netzen von und nach Deutschland zusammenlaufen.

Wie bereits erwähnt, richten sich die Wachstumsprognosen der betrachteten Dienste für 2008 bis 2010 nach den Untersuchungen in [Gmb06], [SM09] und [LIJM+09]. Diese sind - abhängig vom jeweiligen Dienst - unterschiedlich hoch und betragen zwischen 31 % für P2P-Verkehr in Deutschland und 158 % für CDN innerhalb eines Jahres. Der eingeführte Gewichtungsfaktor c_n für Unternehmenszentren für das VPN-Modell orientiert sich an der Studie in [Hut05]. Diese Studie belegt die Verteilung der 100 größten Unternehmen in Deutschland. Somit erhalten Städte wie München, Hamburg und Stuttgart, in denen viele Unternehmen angesiedelt sind, einen höhere Gewichtung als andere Städte.

3.2.2 Diskussion der Ergebnisse

In Abbildung 3.4 sind die Verkehrsvolumina aller betrachteten Dienste im Jahr 2010 dargestellt. Die Diagramme zeigen das Verkehrsaufkommen zwischen Quell- und Zielknoten, wobei der Quellknoten derjenige Knoten ist, an dem der Verkehr generiert wird. Für IPTV und VoD wird der Verkehr am Knoten 13 (München) generiert und mit Hilfe eines Multicast-Schemas zu allen anderen Knoten verteilt. Der Verkehrsaufkommen ist unabhängig vom Routing dargestellt und gibt das Gesamtvolumen pro Knoten an. In Abbildung 3.4 (b) wird der schlechteste Fall für VoD-Unicast-Verkehr betrachtet, bei dem der gesamte Inhalt nur auf einem VHO (Knoten 13) gespeichert ist. Der P2P-Verkehr ist innerhalb des Referenznetzes gleichmäßig verteilt und hängt vor allem von der Bevölkerungszahl und dem gewählten Peering-Knoten bei Knoten 1 (Berlin) und Knoten 6 (Frankfurt) ab. Dies gilt ebenfalls für VPN-Verkehr, wobei sich hier die Anzahl der Unternehmenszentren an den Knoten noch zusätzlich auswirken.

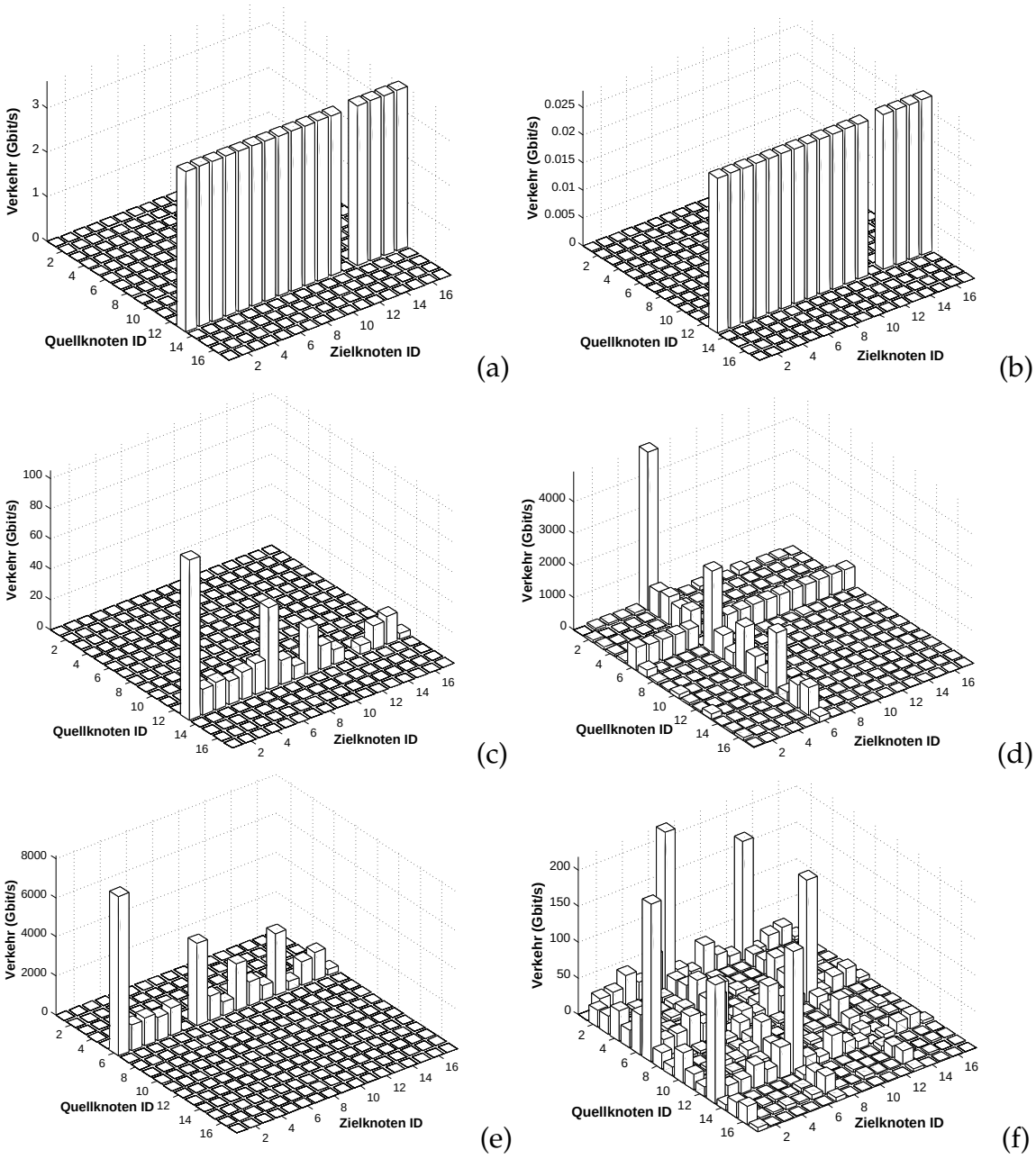


Abbildung 3.4: Verkehrsvolumen pro Dienst. (a) IPTV, (b) zentrales VoD, (c) lokales VoD, (d) P2P, (e) CDN, (f) VPN

In Abbildung 3.5 ist die aggregierte Verkehrsmatrix aller Dienste gezeigt. Das Verkehrsaufkommen ist an Knoten 6, dem Internet-Austauschknoten am höchsten, da hier das Peering mit anderen Netzbetreibern stattfindet. Es zeigt sich, dass P2P immer noch erheblich zum Gesamtverkehrsaufkommen in dem Referenznetz beiträgt, auch wenn der prozentuale Anteil des P2P-Verkehrs in den letzten Jahren abgenommen hat.

Beim Vergleich der Ergebnisse der verschiedenen Dienste zeigt sich, dass das Verkehrsaufkommen zwischen den Knoten nicht symmetrisch ist. Obwohl die mittlere relative Differenz eines Anforderungspaares (m,n) und (n,m) unter zehn Prozent beträgt, erreichen einige Anforderungspaare Unterschiede bis zu 420 %. Die Dienste mit dem höchsten Verkehrsaufkommen sind P2P und nutzergenerierte Inhalte, welche in dem CDN-Graph abgebildet sind. Bei den Multicast-Diensten ist die benötigte Übertragungsbandbreite im Vergleich zu Unicast-Diensten vernachlässigbar.

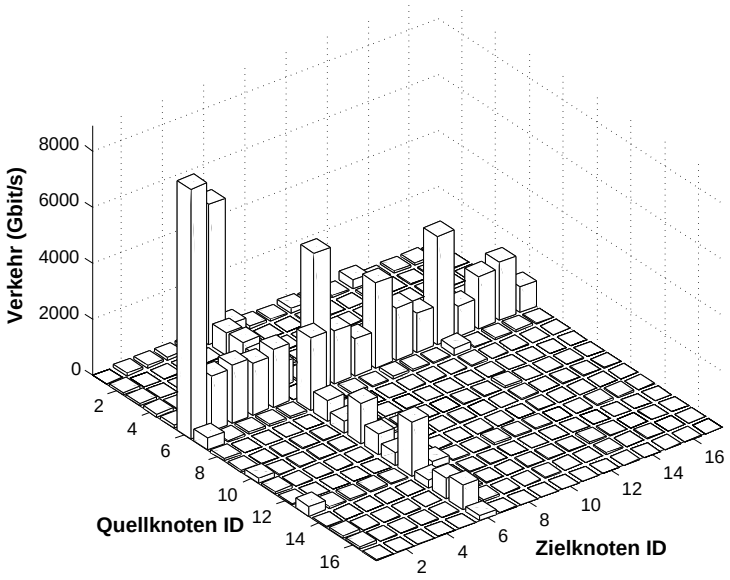


Abbildung 3.5: Aggregiertes Verkehrsvolumen aller Dienste

Die Autoren in [NST05], [CFV08] und [CVFC09] stellen Methoden vor, um synthetisch generierte mit real gemessenen Verkehrsmatrizen zu vergleichen. In [NST05] finden sich Schlüsseleigenschaften aktueller Verkehrsmatrizen von großen Weitverkehrsnetzen, wie Sprints europäisches Weitverkehrsnetz und das Abilene-Netz. Als Schlüsseleigenschaft beschreiben die Autoren die großen Unterschiede des Verkehrsaufkommens zwischen den Verkehrsflüssen, die bis zu sieben Größenunterschiede umfassen. Eine weitere Schlüsseleigenschaft ist die logarithmische Normalverteilung der untersuchten Verkehrsmatrizen. Die Untersuchungen zeigen, dass eine Gleichverteilung zum zufälligen Generieren von Verkehrsmatrizen weniger geeignet ist.

Die Autoren in [CFV08] und [CVFC09] untersuchen zusätzlich Methoden, um realistische Matrizen für kurze und lange Zeitspannen zu erstellen. Eine kurze Zeitspanne entspricht beispielsweise einem Tag, während eine lange Zeitspanne über mehrere

Tage bis Wochen reicht. Die in dieser Kapitel entwickelten Verkehrsmodelle werden im Folgenden mit den Methoden aus den aufgeführten Papern verglichen, um festzustellen, ob sie ähnliche Eigenschaften aufweisen.

Wie in [NST05] werden in Abbildung 3.6 die Verkehrsanforderungen zwischen den Knotenpaaren in aufsteigender Reihenfolge des mittleren Verkehrsaufkommens sortiert. Wie beim Sprint- und Abilene-Netz beobachtet, ist das Verkehrsaufkommen für das verwendete Referenznetz nicht gleichmäßig verteilt, sondern erstreckt sich über vier Zehnerpotenzen. Damit haben die entwickelten Verkehrsmatrizen einen ähnlichen Größenunterschied wie in [NST05]. Das unterschiedlich hohe Verkehrsaufkommen entsteht zum einen durch den Peering-Knoten und zum anderen durch die Server, an denen die Fernsehsender und Filme eingespeist sowie die Inhalte der CDN-Dienste für lokale Anfragen gespeichert werden.

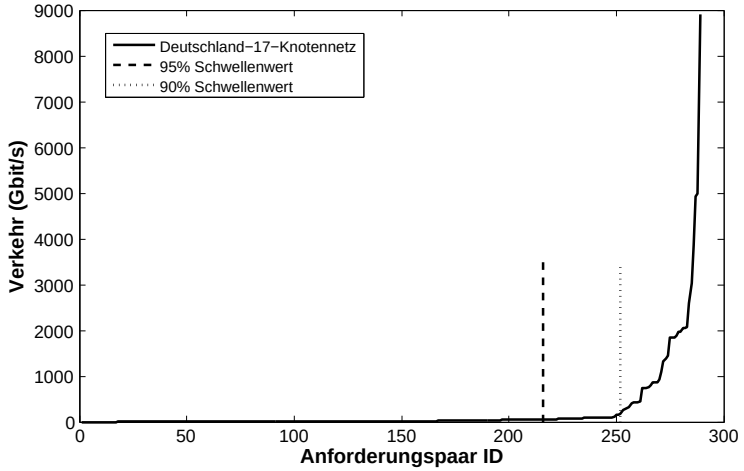


Abbildung 3.6: Verkehrsanforderungen zwischen den Knotenpaaren sortiert nach der mittleren Verkehrsrate

Die aufsteigende Sortierung der Verkehrsanforderungen wird dazu verwendet, um eine statistische Verteilung zu finden, die der Verteilung der Verkehrsanforderungen der berechneten Verkehrsmatrizen entspricht. Ziel ist es, eine ähnliche statistische Verteilung der Verkehrsmatrizen zu finden wie in den genannten Literaturquellen. Dazu wird ein Hypothesentest durchgeführt, der eine Nullhypothese H_0 besitzt, die beispielsweise lautet: „Die Verteilung der Verkehrsmatrizen entspricht einer logarithmischen Normalverteilung“. Als Güte für den Hypothesentest wird der Chi-Quadrat-Test verwendet.

In [NST05], [CFV08] und [CVFC09] haben die Untersuchungen gezeigt, dass für Verkehrsanforderungen mit Größenunterschieden bis zu vier Zehnerpotenzen, wie in Abbildung 3.6, keine angemessene Verteilung gefunden werden kann. Alle Verteilungen verfehlen den Hypothesentest. Die Erklärung der Autoren ist der große Unterschied in den Verkehrsaufkommen zwischen den einzelnen Verkehrsanforderungen. Deshalb werden die Anforderungen, wie in Abbildung 3.6 dargestellt, mittels eines Schwellenwerts in zwei Gruppen aufgeteilt. Die in diesem Kapitel verwendeten

Schwellenwerte liegen bei 90 % beziehungsweise 95 % und stellen in Abbildung 3.6 die Anforderungspaare rechts von den zwei vertikalen des gesamten berechneten Verkehrsaufkommens dar. In [NST05] wird gezeigt, dass die logarithmische Normalverteilung eine gute Übereinstimmung mit real gemessenen Verkehrsvolumina zwischen Knotenpaaren besitzt. Deshalb wird im Folgenden anhand des Chi-Quadrat-Tests untersucht, ob die gezeigte Verteilung der Verkehrsanforderungen ebenfalls einer logarithmischen Normalverteilung entspricht. Die Ergebnisse sind in Abbildung 3.7 dargestellt.

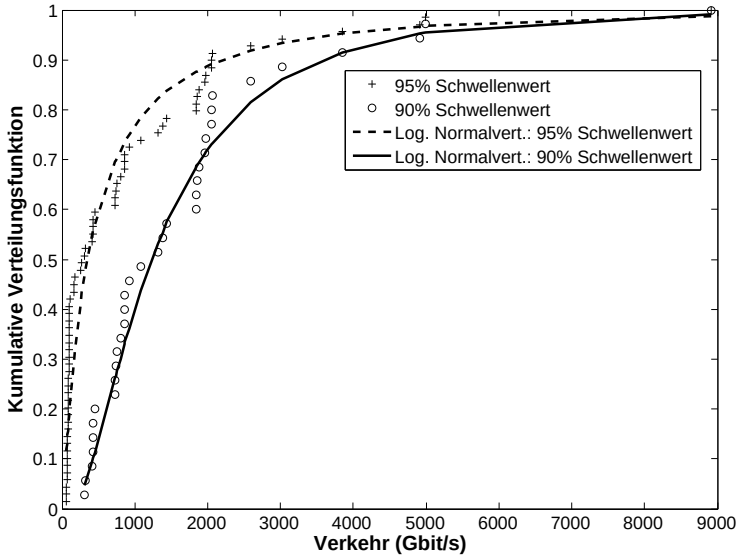


Abbildung 3.7: Kumulative Verteilungsfunktion der Fallstudie

Der Verteilungstest wurde mit den Parametern der Verteilung durchgeführt, die mit Hilfe einer Maximum-Likelihood-Schätzung bestimmt wurden. Die Ergebnisse für den 90 % und 95 % Schwellenwert sind die kumulativen Verteilungen in Abbildung 3.7. Die Kreise beziehungsweise die Kreuze stellen die berechneten Werte für die Schwellenwerte 90 % beziehungsweise 95 % dar. Die durchgezogenen Linien entsprechen der logarithmischen Normalverteilung für beide Schwellenwerte. Die Entscheidung, ob die Hypothese, dass die Verteilung der logarithmischen Normalverteilung entspricht, akzeptiert wird, basiert auf der Teststatistik in [NST05]. Als Güte des Fitnesstests wird der Chi-Quadrat-Test gewählt, der den p-Wert als Metrik für die Abschätzung verwendet. Der Test wird für ein Signifikanzlevel von fünf Prozent durchgeführt. Dies entspricht einem Konfidenzinterval von 95 %. Der Mittelwert für alle Verkehrsanforderungen beträgt $\mu = 1{,}43$ Gbit/s und die Standardabweichung beträgt $\sigma = 0{,}8$ Gbit/s. Für jeden der beiden Abschnitte wurden acht Unterteilungen verwendet. Folglich ergeben sich sieben Freiheitsgrade. Der kritische Wert beträgt somit 14,07 für ein Signifikanzniveau von $\alpha = 0{,}05$.

Der Testwert liegt bei 11,6 beziehungsweise 12,9, daher wird die Hypothese für beide Grenzwerte akzeptiert. Allerdings zeigen die Testwerte, dass mit dem 90 % Schwellenwert eine bessere Übereinstimmung mit der logarithmischen Normalverteilung

erreicht wird.

Mit den Ergebnissen aus dem Hypothesentest zeigt sich, dass das beschriebene Modell Verkehrsmatrizen erzeugt, die real gemessenen Matrizen entsprechen. Wie in der Literatur gezeigt, stellt die logarithmische Normalverteilung eine geeignete Beschreibung der Verkehrsmatrizen dar. Die Verkehrsmatrizen weisen Verkehrsanforderungen auf, die sich um mehrere Größenordnungen unterscheiden. Ein Drittel der Verkehrsanforderungen transportieren 90 % des gesamten Verkehrsaufkommens innerhalb des Netzes. Die statistischen Untersuchungen bestätigen damit die Gültigkeit der in diesem Kapitel entwickelten Verkehrsmodelle.

3.3 Zusammenfassung

In diesem Kapitel wurden dienstorientierte Verkehrsmodelle entwickelt, die den in der Literatur häufig verwendeten populationsbasierten Ansatz um Internet-Austauschknoten und Unternehmensstandorte erweitern. Für das Routing der Verkehrsanforderungen wird zwischen internen und externen Verkehrsströmen unterschieden. Es wurde gezeigt, dass die externen Verkehrsströme zu einem hohen Verkehrsaufkommen an den Internet-Austauschknoten und zu asymmetrischen Verkehrsmatrizen führen. Zusätzlich wurde untersucht, wie sich der Standort der Server und die Erfolgsquote bei der Suche nach Filmtiteln auf das Routing der entsprechenden Dienste auswirkt. Mittels der entwickelten Modelle wurden anhand eines Beispielnetzes die Verkehrsmatrizen der betrachteten Dienste berechnet. Dazu wurden verschiedene Studien in der Literatur über künftige Verkehrszuwächse in Weitverkehrsnetzen herangezogen.

Am Ende des Kapitels erfolgte mittels eines Hypothesentests eine statistische Überprüfung der berechneten Verkehrsmatrizen. Die statistischen Analysen haben die Asymmetrie des Verkehrsaufkommens der einzelnen Verkehrsanforderungen bestätigt, im Gegensatz zu den in der Planung häufig verwendeten symmetrischen Verkehrsmatrizen. Durch einen Hypothesentest wurde gezeigt, dass die Verkehrsmatrizen einer logarithmischen Normalverteilung entsprechen, was in der Literatur als geeignete Verteilung beschrieben wird.

4 Fehlermechanismen in heutigen Weitverkehrsnetzen

Neben den Verkehrsanforderungen, wie in Kapitel 3 beschrieben, beeinflussen auch Netzfehler das Routing innerhalb eines Netzes. Typische Fehler, die in einem Weitverkehrsnetz auftreten, sind Linkausfälle, Stromausfälle und Wartungsfehler. Neben den Hardwareausfällen kommt es auch zur Beeinträchtigung der Performanz eines Netzes, die durch falsche Konfiguration einer oder mehrere Netzelemente ausgelöst werden. Der Ausfall eines Links oder eines Knotens beruht nicht immer auf einem physikalischen Fehler, sondern kann auch durch einen Konfigurationsfehler verursacht werden. In diesem Kapitel werden zunächst die Konfigurationsaufgaben beschrieben, die an einem Router beziehungsweise Switch anfallen. Dabei wird davon ausgegangen, dass die Netzelemente mittels eines *Command Line Interface* (CLI) konfiguriert werden. Die Konfiguration eines Weitverkehrsnetzes verlangt fundierte Kenntnisse über autonome Systeme und Domänenwissen, sowie spezielle Kenntnisse im Bereich der verwendeten Protokolle wie beispielsweise *Multi-Protocol Label Switching* (MPLS) und *Open Shortest Path First* (OSPF). Die Herausforderung besteht darin, das Netz kontinuierlich an die Veränderungen in der Netztopologie sowie an Verkehrsveränderungen anzupassen, welche in einem großen Transportnetz häufig auftreten und eine Anpassung der Konfigurationsparameter verlangen. Die manuelle Konfiguration ist allerdings fehleranfällig, wie verschiedene Studien [FR01], [MWA02], [CGG+04] und [LTWG05] zeigen, und kann zu Netzfehlern und Netzanomalien mit unvorhersehbaren Folgen auf die geroutete Verkehrsanforderungen führen.

Diverse veröffentlichte Pressemitteilungen aus den letzten Jahren [Bac09], [Hei09], [Wil09] und [Hei10] zeigen, dass Konfigurationsfehler in heutigen Netzen immer wieder auftreten. Da es sich bei Netzfehlern, die durch Konfigurationsfehler ausgelöst werden, um sensible Daten der Netzbetreiber handelt, werden solche Mitteilungen nur selten veröffentlicht. Im Allgemeinen dürften die durch Konfigurationsfehler hervorgerufene Netzstörungen deutlich höher liegen.

In der Literatur finden sich viele Beispiele für Ausfallsicherheitsmechanismen, die verwendet werden, um im Fehlerfall einen Arbeitspfad durch einen vorher berechneten Ersatzpfad zu schützen. Diese Mechanismen lassen sich sehr gut auf Fehler wie Linkausfälle oder Routerausfälle anwenden, bei denen man eine Alarmmeldung von der entsprechenden Netzkomponente erhält und daher auf den Ersatzpfad umschalten kann. Bei Konfigurationsfehlern besteht die Schwierigkeit darin, diese Art von Fehlern zu erkennen und den exakten Ort zu identifizieren. In Abschnitt 4.2

werden die unterschiedlichen Auswirkungen von Konfigurationsfehlern beschrieben, die teilweise nur indirekt aufgrund von Anomalien im Netz entdeckt werden.

Nach der Diskussion der Konfigurationsfehler und deren Auswirkung in Abschnitt 4.2, erfolgt in Abschnitt 4.3 die Evaluierung dieser Fehler. Dieses Bewertungsschema dient dazu, die Konfigurationsfehler basierend auf verschiedenen Faktoren kategorisieren zu können und zu bestimmen, in welcher Reihenfolge diese bearbeitet werden. Außerdem bildet das Bewertungsschema die Auswirkungen der Konfigurationsfehler ab, die sich unter anderem anhand der Störungen und der Zeitdauer berechnen lassen.

Das Auffinden von Konfigurationsfehlern ist nicht Teil dieser Arbeit. In diesem Kapitel werden durch Konfigurationsfehler ausgelöste Fehlermuster beschrieben, die als Eingangsparameter für statistische Methoden verwendet werden können, um Konfigurationsfehler in einem Weitverkehrsnetz zu lokalisieren.

4.1 Konfigurationsparameter der Netzkomponenten

In diesem Abschnitt wird die Konfiguration mittels CLI eingehender dargestellt. Dazu werden die Konfigurationsschritte und die potentiellen Fehlerauswirkungen analysiert. Es existieren verschiedene Möglichkeiten eine Netzkomponente zu konfigurieren. Zum einen gibt es die Betriebssoftware, die von den Herstellern mitgeliefert wird, ein Managementsystem, welches eine Auswahl an Tools und Anwendungen bereitstellt, um die Konfiguration zu unterstützen, oder das CLI. Das CLI hat den Vorteil, dass die vollständige Konfigurationsparameteranzahl zur Verfügung steht und dadurch eine individuelle Konfiguration der Netzelemente möglich ist. Ebenso bietet das CLI Vorteile bei der Fehlerfindung, da ein direkter Zugang zum Gerät besteht. Aus den genannten Gründen wird in diesem Kapitel die Konfiguration der Netzkomponenten über das CLI betrachtet. Die in diesem Kapitel vorgestellten Analysen wurden bereits in [Mer08a] und [Mer08b] veröffentlicht.

Routerhersteller bieten eine Vielzahl an Konfigurationsbefehlen und -optionen an, um das Verhalten des Routers an das entsprechende Transportnetz anzupassen. Ein Router-Betriebssystem, beispielsweise von Juniper oder Cisco, beinhaltet über 600 verschiedene Konfigurationsparameter. Die Konfiguration eines Routers kann in mehrere Kategorien unterteilt werden. In dieser Arbeit werden im Wesentlichen drei unterschieden: Interface-, Protokoll- und Sicherheitskonfigurationen. Die Interface-Konfiguration enthält Parameter wie das Setzen der IP-Adresse, der erlaubten Paketgröße oder verschiedener Überwachungsparameter. Eine weitere Kategorie stellen die zu konfigurierenden Protokolle dar. Welche Protokolle auf einem Router aktiviert werden, hängt sowohl vom Einsatz eines Routers innerhalb des Weitverkehrsnetzes als auch von den notwendigen Protokollen für den Betrieb des Transportnetzes ab. Die am häufigsten verwendeten Protokolle sind *Intermediate System to Intermediate System* (IS-IS), OSPF, *Border Gateway Protocol* (BGP) und MPLS. Eine Beispielkonfiguration des IS-IS ist in Abbildung 4.1 gezeigt.

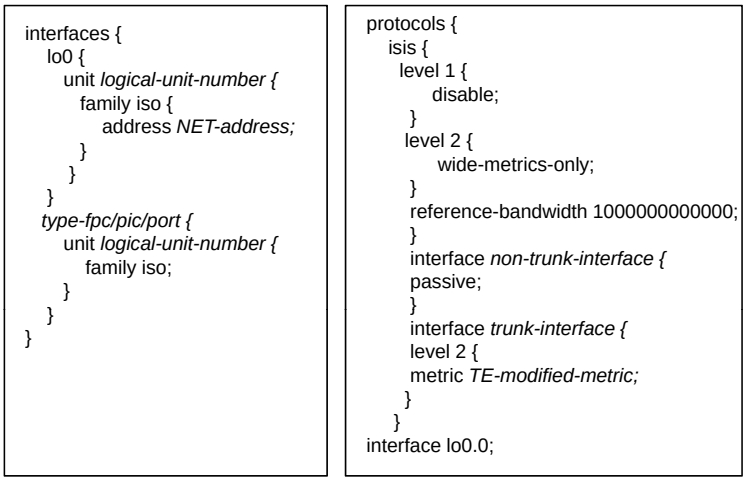


Abbildung 4.1: Beispielkonfiguration eines Routers mit dem CLI von Cisco

Auf der linken Seite ist die Konfiguration des Interfaces dargestellt, auf dem das Protokoll verwendet wird. Hierzu muss dem Interface eine Netzadresse zugewiesen werden. Die rechte Seite zeigt die anschließende Konfiguration des IS-IS-Protokolls. Das Protokoll muss aktiviert und dem entsprechenden Interface zugeordnet werden. In der Abbildung wird das IS-IS Protokoll auf Interface 0 aktiviert. Daneben lassen sich noch eine Reihe zusätzlicher Parameter konfigurieren, wie beispielsweise die verwendete Bandbreite auf dem Interface.

Ein Auswahl an Konfigurationsmöglichkeiten der Interfaces und der auf Schicht-3 am häufigsten eingesetzten Protokolle ist in Tabelle 4.1 gegeben. Die Übersicht beschränkt sich auf die am häufigsten verwendeten Konfigurationsschritte die gleichzeitig am ehesten zu einem Konfigurationsfehler führen. Die fettgedruckten Parameter stellen die minimale Konfiguration dar, um das jeweilige Interface beziehungsweise Protokoll in einem Netz zu verwenden.

Um die Protokolle zu aktivieren ist nur eine minimale Anzahl an Konfigurationsschritten notwendig. Häufig reicht es bereits aus, das Protokoll auf einem Interface des Routers zu aktivieren. Das Protokoll verwendet in diesem Fall die Standardeinstellungen des Herstellers. Allerdings sind weitere Konfigurationsschritte vorzunehmen, um das Protokoll und dessen Verhalten an das entsprechende Transportnetz anzupassen. Die entscheidenden Konfigurationsparameter zur Beeinflussung des Routings sind unter anderem die Filterregeln, die Authentifizierungseinstellungen sowie die Export- und Import-Regeln. Diese Konfigurationen können direkt auf dem Interface und innerhalb des Protokolls gesetzt werden. Mit Hilfe der Filterregeln wird das Verhalten des Interfaces für verschiedene Situationen konfiguriert. Beispielsweise wird eine Überlast auf einem Link oder Ende-zu-Ende Pfad verhindert, indem Pakete eines bestimmten Pakettyps am Interface blockiert werden oder generell nur bestimmte Pakete über das Interface weitergeleitet werden.

Zusätzlich ist eine Vielzahl an Sicherheitseinstellungen möglich, zum Beispiel die Aufteilung eines Weitverkehrsnetzes in mehrere virtuelle Netze. Die Authentifizie-

Interface	Konfigurationsparameter (Datentyp)
IP-Adresse	**IP-Adresse setzen (int)**; Mehrere IP-Adressen setzen **(int)**; IP-Adressüberwachung **(int)**; IP-Routing **(int)**
IP-Dienst	MTU-Größe **(int)**; IP-Abrechnung **(double)**; Performanzparameter **(double)**; Überwachung und Wartung IP-Netz **(int, string)**
Routing-Regeln	Übereinstimmungsbedingungen **(int, string)**
Protokolle	
IS-IS	**Aktivierung (int)**; Netzadresse **(int)**; Export-Regeln **(string)**; Authentifizierung **(string)**; Filterregeln **(int, string)**
OSPF	**Aktivierung (int)**; Netzadresse **(int)**; Gebiets-ID **(int)**; Import/Export-Regeln **(int, string)**; Authentifizierung **(int, string)**; Filterregeln **(int, string)**; Kostenmetrik **(int)**; Timer **(int)**
BGP	**Aktivierung (int)**; AS-Nummer **(int)**; Peer-Gruppe **(int)**; Nachrichtenaktualisierung **(int)**; Filterregeln **(int, string)**; Import-/Exportregeln **(int, string)**; Authentifizierung **(int, string)**; Route-Reflektor **(int)**
MPLS	**Aktivierung (int)**; Manuelle/automatische Regeln **(int, string)**; Filterregeln **(int, string)**; Verkehrsklassen**(int)**; Schnelles Rerouting; Bandbreitenzuweisung **(int)**; Hop-Limit **(int)**; Kanten- oder Knotenschutz **(int)**
RSVP	**Aktivierung (int)**; Bandbreitenzuweisung **(int)**; Authentifizierung **(int, string)**; Kanten- oder Knotenschutz **(int)**; Nachbarschafts-Ausfall-Benachrichtigung **(int)**
LDP	**Aktivierung (int)**; Import/Export-Regeln **(int, string)**; LDP-“Hallo“-Intervall **(int)**; LDP-Haltetimer **(int)**; LDP-Keep-Alive-Nachrichten **(int)**
GMPLS	**Aktivierung (int)**; LMP; Netz-Peers **(int)**

Tabelle 4.1: Minimal notwendige (fettgedruckt) und zusätzliche Konfigurationsparameter

rung zwischen zwei Routern, die über den selben Link verbunden sind, erlaubt es, sicherzustellen, ob Pakete zwischen den Interfaces der beiden Routern gesendet werden dürfen. Dadurch ist es möglich, ein Netz so zu konfigurieren, dass nur vertrauenswürdige Router innerhalb einer Domäne kommunizieren können. Die Export- und Import-Regeln werden von einem Router genutzt, um gelernte Routen an andere Router zu exportieren oder diese von anderen Routern zu importieren. Im nächsten Abschnitt wird anhand der Konfigurationsmöglichkeiten eines Routers analysiert, welche Auswirkungen eine Fehlkonfiguration auf das Netz und die gerouteten Anwendungen hat.

4.2 Konfigurationsfehlerszenarien

Zur Bestimmung der Konfigurationsfehler wurden die Konfigurationshandbücher von Juniper [Jun] und Cisco [Cis] als Referenz verwendet. Ein Zusammenstellung der häufigsten Konfigurationsfehler in einem Weitverkehrsnetz sind in den Tabellen 4.2 und 4.4 dargestellt. Zwei Auftrittsmöglichkeiten müssen bei der Betrachtung von Konfigurationsfehler in Weitverkehrsnetzen unterschieden werden. Zum einen existieren Konfigurationsfehler, die durch das Setzen eines falschen Parameters oder Parameterwerts entstehen und dadurch die Funktionsweise des Protokolls verändern oder beeinträchtigen. Die zweite Entstehungsart von Konfigurationsfehlern beruht auf der Wechselwirkung zwischen mehreren Protokollen. Das bedeutet, dass die Protokolle zwar unabhängig voneinander funktionstüchtig sind, aber zur Laufzeit eventuell Ergebnisse des anderen Protokolls benötigen, welche aufgrund einer falschen Einstellung nicht zur Verfügung stehen.

Im Folgenden werden potentielle Konfigurationsfehler und deren Auswirkung auf das Transportnetz beschrieben. Dazu werden für die Analyse neben IP-, Ethernet- und WDM-Schicht die drei Kategorien Interface, Protokolle, Dienstgüte und Sicherheit unterschieden. Danach erfolgt die Analyse von Konfigurationsfehlern auf der optischen Schicht und von Softwarefehlern.

4.2.1 IP- und Ethernet-Schicht

In der Tabelle 4.2 sind die häufigsten Konfigurationsfehler auf der IP- und Ethernet-Schicht zusammengefasst. Bei der Beschreibung der Konfigurationsfehler wird dabei nicht auf einzelne Befehle eingegangen, sondern die Konfiguration wird thematisch nach bestimmten Bereichen sortiert. Das Ziel der Analyse ist es, die Fehlermuster zu beschreiben, die aufgrund von Konfigurationsfehlern entstehen. Jeder der 600 möglichen Konfigurationsparameter kann zu einer Anomalie führen. Allerdings wird eine Vielzahl dieser Befehle nur selten oder überhaupt nicht verwendet. Nachfolgend werden zunächst Interface- und IP-Protokollfehler analysiert.

Interface und Protokolle	Konfigurationsfehler (Datentyp)
IP Adresse	Falsche IP Adresse **(int)**, gleiche IP Adresse auf zwei verschiedenen Routern **(int)**
Dienstgüte	Falscher Wartepuffer für Kontroll- oder Datenpakete **(int)**
Routing-Regeln	Falsche Richtlinien **(int, string)**, falsche Filterregeln **(int, string)**, falsche Bandbreitengrenze (**(int)**)
Konfigurationshierarchie	Protokoll auf den verschiedenen Hierarchiestufen nicht aktiviert **(int)**
IS-IS	Falsche Authentifizierungsmethode **(int, string)**, falsche Filterregeln **(int, string)**, nicht konfigurierte Parameter, die bei anderen Protokollen verwendet werden **(int, string)**, falsche MTU-Größe **(int)**
OSPF	Falscher Gebiets ID **(int)**, falsches „Hallo“ Zeitintervall **(int)**, nicht konfigurierte Parameter, die bei anderen Protokollen verwendet werden **(int, string)**
BGP	Fehlkonfiguration der AS **(int)**, fehlerhafte Nachbarschaftsadressen und Gruppenart **(int, string)**, falsche IP Adresse in Präfixliste **(int)**, falsche Filterregeln **(int, string)**, falsche Einstellung der BGP-Gewichte **(int)**
MPLS	Falscher Bandbreitenparameter **(int)**, falsche Richtlinien **(int, string)**, Fehlkonfiguration der LDP-Tunnelungsanweisung **(int, string)**
RSVP	Fehlkonfiguration der Authentifizierungsmethode **(int, string)**, nicht konfigurierte Nachbarschafts-Ausfall-Benachrichtigungen **(int)**
LDP	Fehlkonfiguration des „Hallo‘“-Timers **(int)** und Haltezeit **(int)**, falsche Authentifizierungsmethode **(int)**
VPN	Fehlkonfiguration Router Distinguisher **(int)**, falsche Authentifizierungsmethode **(int, string)**, falsche Filterregeln **(int, string)**

Tabelle 4.2: Zusammenfassung potentieller Konfigurationsfehler eines Routers

Konfigurationsfehler eines Router-Interfaces

Um einen Router verwenden zu können, müssen zunächst die benötigten Interfaces aktiviert werden. Jedem Interface ist dabei eine IP-Adresse zugeordnet, wobei die selbe Adresse an jedem Router nur einmal vergeben werden kann, da dies vom Betriebssystem überprüft wird. Allerdings erfolgt keine Überprüfung der IP-Adresse innerhalb des Weitverkehrsnetzes, so dass die Möglichkeit besteht, die gleiche IP-Adresse an zwei Interfaces auf verschiedenen Routern zu vergeben. Dies hat zur Folge, dass das Ziel nicht mehr eindeutig bestimmbar ist und, abhängig von den gelernten Routen im Netz, ein Router das Paket zu dem einen oder dem anderen Router mit der selben IP-Adresse sendet. Damit entsteht beim Routen der Pakete ein unvorhersehbares Verhalten im Netz. Alternativ können Schleifen im Weitverkehrsnetz entstehen, wenn die Router unterschiedliche Ziele unter der selben IP-Adresse in ihrer Routingtabelle gespeichert haben. Die Pakete werden abhängig vom jeweiligen Router zu einem anderen Ziel-Router gesendet. Falls die Router entlang eines Routing-Pfades unterschiedliche Ziele in den Routingtabellen haben, senden sich die Router die Pakete ständig hin und her, bis der Hop-Zähler des Pakets ausläuft.

Eine weitere Konfigurationsmöglichkeit an den Interfaces eines Routers ist der Wartepuffer für Pakete. In einem Router werden verschiedene Wartepuffer zur Priorisierung der Datenpakete und Wartepuffer für Signalisierungs- und Datenpakete verwendet. Eine Fehlkonfiguration der Wartepuffer kann dazu führen, dass Signalisierungspakete in die Wartepuffer für Datenpakete einsortiert werden und aus diesem Grund eine größere Verzögerung erfahren. Da Steuerungsnachrichten periodisch zwischen Routern ausgetauscht werden, um eine Verbindung aufrecht zu erhalten, kann ein ausbleibendes Steuerungspaket zum Abbau der Verbindung zwischen zwei Routern führen. Dies kommt zum Beispiel bei der Verwendung von MPLS vor, welches periodisch „Hallo“-Nachrichten an seine Nachbarn sendet. Empfängt ein Router innerhalb eines bestimmten Antwortintervalls keine Antwortpakete, wird der ursprüngliche Pfad abgebaut und auf einen Ersatzpfad umgeschaltet. Alle Pakete die über die ursprüngliche Verbindung geroutet wurden, müssen dann auf Ersatzwege umgeleitet werden. Im schlechtesten Fall werden die Pakete an einem Interface verworfen, bis eine Ersatzverbindung aufgebaut wurde.

Ein weiterer Fehler besteht darin, dass Datenpakete in die falsche Warteschlange einsortiert werden. Beispielsweise wenn hochpriore Datenpakete in eine Warteschlange mit niedriger Priorität einsortiert werden. Wie bei den Signalisierungspaketen kann dies zu einer größeren Verzögerung der hochprioren Datenpakete führen, wenn diese in eine Warteschlange mit hohem Paketaufkommen einsortiert werden. Handelt es sich dabei um Datenverkehr einer bestimmten Dienstgüte, kann dies zur Verletzung der Dienstgüte führen. Dienste wie zum Beispiel IPTV, welche in Kapitel 3 behandelt wurden, benötigen eine bestimmte Bandbreite und eine maximale Verzögerung, um den zu übertragenden Inhalt fehlerfrei darzustellen. Aufgrund der Verzögerung einzelner Datenpakete kann dies gegebenenfalls nicht mehr gewährleistet werden. Besteht zwischen Netzbetreiber und Kunde eine vertraglich festgelegte Dienstgüte, kommt es bei einer Nichteinhaltung seitens des Netzbetreibers zu einer vereinbarten

Strafzahlung an den Kunden.

Die aufwendigsten Konfigurationseinstellungen eines Routers sind die Routing-Regeln, die angeben, wie ein Router auf verschiedene Signalisierungs- und Datenpakete reagiert. Die Komplexität liegt zum einen an der Anzahl der auszuführenden Befehle und zum anderen an dem notwendigen Wissen, welche Einstellungen zu welchem Routingverhalten führen. Innerhalb der Routing-Regeln sind die Filterregeln ein wichtiges Instrument zur Regelung des Datenverkehrs. Mithilfe der Filterregeln wird definiert, welche Pakete weitergeleitet und welche am Interface blockiert werden. Die Routing-Regeln an einem Router werden durch verschiedene Parameter wie die IP-Adresse, Quell- und Ziel-MAC-Adresse und Portnummer beeinflusst. Die fehlerhafte Konfiguration mindestens einer dieser Parameter führt dazu, dass die „falschen“ Pakete an einem Interface eines Routers gefiltert beziehungsweise weitergeleitet werden. Abhängig davon kommt es eventuell zum Ausfall eines Dienstes beziehungsweise zu einer Überlast innerhalb des Netzes. Weitere Auswirkungen von falsch konfigurierten Filterregeln sind zum Beispiel Sicherheitslücken, die einen Angriff auf ein Netz ermöglichen, nicht verbundene Netzknoten oder höhere Blockierungen und größere Verzögerungen, die auf einem oder mehreren Links auftreten.

Neben den Filter- und Routing-Regeln, kann auf jedem Interface auch die zur Verfügung stehende Bandbreite konfiguriert werden. Dadurch besteht die Möglichkeit, verschiedenen Verkehrsklassen eine bestimmte maximal verfügbare Bandbreite zuzuordnen. Eine Fehlkonfiguration der maximalen Bandbreite kann zu Performanzeinbußen des höher priorisierten Verkehrs führen, wenn nicht ausreichend Bandbreite auf den Links, über die der Verkehr geroutet wird, zur Verfügung steht. Zur Erhöhung der Netzsicherheit können neben der Filterung von Paketen auch Zugangslisten konfiguriert werden. Daneben existieren verschiedene unterschiedliche Zugangslisten, um Schicht-2 oder Schicht-3 Verkehr zu filtern. Konfigurationsfehler bei den Zugangslisten führen zu Paketverlusten, höherem Verkehr und zu Sicherheitsrisiken auf den betroffenen Links und Pfaden.

Um ein Protokoll verwenden zu können, muss es zuerst auf dem entsprechenden Interface aktiviert werden. Danach erfolgt die Konfiguration der protokollspezifischen Einstellungen. Wenn das Protokoll auf dem Interface nicht aktiviert wird, kann keine Verbindung zum Interface aufgebaut werden. Somit werden auch keine Pakete über das entsprechende Interface geroutet. Zusätzlich muss ein Protokoll auf den verschiedenen Interface-Hierarchien aktiviert werden, ansonsten funktioniert das Protokoll nicht im vollen Umfang. Die fehlende Aktivierung eines Protokolls auf dem Interface kann unterschiedliche Auswirkungen auf den Netzbetrieb haben. Im besten Fall verringert sich durch die Fehlkonfiguration nur die Performanz auf dem betroffenen Interface. Die Fehlkonfiguration kann aber auch zu Paketverlusten oder zum Abbau einer bestehenden Verbindung führen, wenn zwei miteinander verbundene Interfaces nicht kommunizieren können.

Ein weiterer Konfigurationsfehler entsteht, wenn die Abhängigkeiten von Protokollen nicht berücksichtigt werden. Einige Protokolle benötigen die Daten von anderen Protokollen, um fehlerfrei zu funktionieren. Beispielsweise benötigt MPLS bestimmte

Daten vom *Interior Gateway Protocol* (IGP). MPLS beruht auf der Verbreitung von Labels, die angeben, welches Interface an einem Router zur Weiterleitung des Datenpakets verwendet wird. Vor der Verteilung der Labels, benötigt das *Label Distribution Protocol* (LDP) die Informationen über die Linklängen und die kürzesten Wege im Netz, um die Labels entsprechend zwischen den Routern zu verteilen.

Konfigurationsfehler auf IP-Schicht

In diesem Abschnitt werden Konfigurationsfehler der wichtigsten heute verwendeten Protokolle beschrieben. Eine Übersicht über die Konfigurationsfehler ist ebenfalls in Tabelle 4.2 enthalten. Die Konfigurationsfehler der genannten Protokolle stehen stellvertretend für die anderen existierenden Kommunikationsprotokolle, die mit ähnlichen Parametern konfiguriert werden. Die minimale Konfigurationsaufgabe ist das Aktivieren des Protokolls. Die Protokolle laufen dann mit einer Standardeinstellung, die den Betrieb des Netzes gewährleisten. Allerdings verwendet jeder Netzbetreiber seine eigenen Einstellungen, um ein Protokoll an das Transportnetz anzupassen.

Eine gemeinsame Eigenschaft der meisten Protokolle sind die Konfigurationseinstellungen für „Hallo“-Timer und „Dead“-Timer. Der „Hallo“-Timer bestimmt, in welchen periodischen Zeitintervallen eine Netzkomponente „Hallo“-Pakete an alle direkten Nachbarn sendet, um deren Verfügbarkeit zu überprüfen. Die Zeitintervalle der „Hallo“-Timer müssen dabei auf allen direkt verbundenen Routern, die selben Zeitintervalle besitzen, da es ansonsten zum Abbau der Verbindung kommen kann oder eine Verbindung zwischen zwei Netzkomponenten erst gar nicht zustande kommt. Das gleiche gilt für die Konfiguration des „Dead“-Intervall-Timers. Der „Dead“-Timer gibt an, in welchem Zeitintervall eine „Hallo“-Nachricht von einem Nachbarknoten erwartet wird. Besitzen die direkt verbundenen Netzknoten ein unterschiedliches Zeitintervall, kann dies zum Abbau der Verbindung führen. Auch die Kombination der Zeitintervalle von „Hallo“- und „Dead“-Timer muss bei der Konfiguration der Protokolle beachtet werden. Die beiden Zeitintervalle müssen ebenfalls aufeinander abgestimmt sein, damit die „Hallo“-Nachrichten rechtzeitig vor dem Ablaufen des „Dead“-Timers eintreffen. Wenn beispielsweise ein sehr großes „Hallo“-Intervall auf dem einen Router und ein sehr kurzes Dead-Intervall auf dem Nachbar-Router gewählt wird, baut der Router mit dem kurzen Zeitintervall des „Dead“-Timers die Verbindung zum anderen Router nach einer gewissen Zeit ab, da er innerhalb des Dead-Timer-Zeitintervall keine „Hallo“-Nachricht empfängt und die Verbindung zu seinem Nachbar als nicht verfügbar erklärt. Die Fehlkonfiguration der Timer führt zu Paketverlusten, solange die Pakete nicht auf einem Ersatzweg umgeleitet werden. Ist kein Ersatzweg vorhanden, kommt es zum Ausfall von Diensten, die über die betroffenen Pfade geroutet werden. Andererseits kann das Umrouten der Datenpakete auf Ersatzwegen zur Überlast in anderen Bereichen des Transportnetzes führen, wenn eine Vielzahl an Verbindungen und damit ein hohes Verkehrsaufkommen betroffen ist.

Ähnlich der Konfiguration eines Interfaces gibt es bei Protokollen ebenfalls die

Möglichkeit, eine Authentifizierungsmethode zu konfigurieren. Damit Nachbarknoten eine Verbindung über ein bestimmtes Protokoll aufbauen können, muss die selbe Authentifizierungsmethode konfiguriert sein. Die Authentifizierung dient dazu, Verbindungen nur zwischen Netzkomponenten aufzubauen, die sich gegenseitig vertrauen. So wird gewährleistet, dass keine Verbindungen zu nicht vertrauenswürdigen Netzkomponenten aufgebaut werden. Verwenden zwei direkt verbundene Netzknoten nicht dieselbe Authentifizierungsmethode, werden die ankommenden Signalisierungs- und Datenpakete verworfen. Die versehentliche Verwendung unterschiedlicher Authentifizierungen verhindert den Aufbau einer Verbindung zwischen verschiedenen Routern oder führt zum Abbau einer oder mehrerer existierender Verbindungen, wenn der Konfigurationsfehler im laufenden Netzbetrieb auftritt. Wiederum kommt es zu Verlusten von Paketen, bis die betroffenen Datenpakete auf einen Ersatzweg umgeroutet werden. Ebenfalls kann es wie bei der Fehlkonfiguration der Timer zum Ausfall von Diensten über die betroffenen Verbindungen kommen.

Die Konfiguration der Linkgewichte auf einem Interface erlaubt es dem Netzbetreiber, das Routing in seinem Netz zu beeinflussen. Durch das Zuweisen von höheren Linkgewichten und somit höheren Kosten für die Benutzung eines Links wird der Verkehr auf den entsprechenden Links reduziert. Der Netzbetreiber hat dadurch die Möglichkeit, Verkehr in seinem Netz zu verlagern, was beispielsweise bei einer bevorstehenden Netzwartung hilfreich ist. Der Verkehr kann vor der Wartung auf Alternativwege umgeroutet und der Einfluss der Wartung auf den Verkehr reduziert werden. Ein zu hohes Link- oder Pfadgewicht an einem Interface führt allerdings dazu, dass der angeschlossene Link nur geringfügig oder überhaupt nicht benutzt wird, da bei der Berechnung der kürzesten Pfade ein Weg über diesen Link zu teuer ist und damit für das Routing ausgeschlossen wird. Werden beispielsweise die Linkgewichte von mehreren Links zu hoch eingestellt, so entsteht eine ungünstige Lastverteilung in einem Weitverkehrsnetz. Der Verkehr wird dann über eine geringe Anzahl an Pfaden geroutet, was zu einem höheren Verkehrsaufkommen auf den entsprechenden Links führt. Vor allem beim BGP, das für das Routing zwischen autonomen Systemen verwendet wird, kann eine Fehlkonfiguration zu einem hohen Verkehrsaufkommen oder Stau auf bestimmten Links führen, da der gesamte Transitverkehr zwischen den autonomen Systemen betroffen ist.

Eine weitere Fehlkonfigurationsmöglichkeit bei Protokollen wie IS-IS, OSPF und BGP ist die Einstellung der Import- und Export-Regeln für die Routingtabellen der Netzknoten. Das Importieren beziehungsweise Exportieren der Routingtabellen erlaubt den Netzknoten, gelernte Routen von anderen Netzknoten zu übernehmen. Der Netzbetreiber erhält dadurch eine weitere Möglichkeit die Verkehrslenkung in seinem Netz zu beeinflussen. Zum Beispiel können mehrere Netzknoten als Eingangsknoten für Transitverkehr konfiguriert werden, um eine Lastteilung durchzuführen. Fehlerhafte Import- beziehungsweise Export-Regeln verursachen, dass Netzknoten die gelernten Routen nicht weiterleiten oder dass gelernte Routen fälschlicherweise an andere Router weitergeleitet werden. Ein Netzbetreiber hat zum Beispiel kein Interesse daran den Transitverkehr zwischen zwei anderen autonomen Systemen unentgeltlich durch sein Netz routen zu lassen. Ebenso stellen falsch gelernte Routen

eine Sicherheitslücke dar, wenn die Routen zu einem falschen autonomen System exportiert werden. Ein Netzknoten außerhalb einer Domäne hat in diesem Fall Zugriff auf die Routen einer fremden Domäne. Die Verkehrsdaten könnten somit protokolliert und Unbefugten zugänglich gemacht werden. Die Fehlkonfiguration kann aber auch zum Abbruch der Kommunikation zwischen autonomen Systemen führen, wenn die Routen nicht mehr exportiert oder importiert werden. Gegebenenfalls sind dann einzelne Kunden nicht mehr miteinander verbunden. Wie bereits bei den vorangegangenen Konfigurationsfehlern erwähnt, ist das schlechteste Szenario der Ausfall von Verbindungen und daraus entstehende Strafzahlungen an den Kunden, falls bestimmte Dienstgütekriterien vertraglich festgehalten wurden.

Eine weitere Maßnahme zur Beeinflussung der Verkehrslenkung in einem Weitverkehrsnetz, stellt die Konfiguration eines Interfaces einer Netzkomponente dar, damit dieses als überlastet erscheint. Mit dieser Einstellung verhindert ein Netzbetreiber, dass Transitverkehr und Verkehr innerhalb des eigenen Transportnetzes über bestimmte Links geroutet werden. Damit werden Kapazitäten freigehalten, damit sie für Ersatzpfade zur Verfügung stehen. Eine fehlerhafte Konfiguration führt zu suboptimalen Verkehrsverteilungen innerhalb des Weitverkehrsnetzes und belastet die restlichen Links stärker. Die Auswirkungen reichen von größeren Verzögerungen und Paketverlusten bis hin zu Ausfällen von Diensten.

Neben der Verkehrslenkung besteht auch die Möglichkeit, die maximal verfügbare Bandbreite pro Link zu begrenzen, um Verkehrslenkung durchzuführen. Hierfür kann Verkehrs-Policing oder -Shaping aktiviert und eine maximale Bandbreite pro Link konfiguriert werden. Der Unterschied der beiden Verfahren liegt darin, dass beim Policing die Pakete verworfen werden, wenn die maximal definierte Bandbreite erreicht wird. Beim Shaping werden die Pakete in einem Puffer gespeichert und später weitergeleitet. Wird allerdings bei beiden Verfahren eine zu niedrige Maximalbandbreite für einen Link definiert, kann eine größere Blockierung von Paketen entstehen, welche die Performanz der entsprechenden Anwendung reduziert. Durch eine zu niedrige eingestellte Bandbreite können Dienste wie IPTV oder CDNs eventuell nur noch eingeschränkt angeboten werden, da die erforderliche Bandbreite nicht vorhanden ist. Insbesondere beim Policing-Verfahren wirkt sich eine zu geringe Bandbreite negativ aus, da bei zu hoher Datenrate der Anwendung die Pakete verworfen werden. Aber auch beim Shaping-Verfahren können bei einer zu niedrig eingestellten Bandbreite, die entsprechenden Wartepuffer am Netzknoten überlaufen, was ebenfalls einerseits zu einer Blockierung von Datenpaketen führt und andererseits die Wartezeit der Pakete erhöht.

Damit die Netzknoten innerhalb eines autonomen Systems untereinander kommunizieren können, müssen sie dieselbe Gebietskennung besitzen um Nachbarschaftsbeziehungen aufzubauen. Wenn eine andere Gebietskennung verwendet wird, kann die entsprechende Netzkomponente keine Kommunikationsbeziehung mit den anderen Netzkomponenten aufbauen und ist innerhalb des autonomen Systems nicht verfügbar. Die Auswirkungen einer falschen Gebietskennung auf einem oder mehreren Netzknoten umfasst alle bereits vorher beschriebenen Auswirkungen. Zusätzlich

besitzen diejenigen Kunden, die über den Router mit der falschen Gebietskennung verbunden sind, keinen Zugang zum Weitverkehrsnetz.

Ein Netzbetreiber hat die Möglichkeit, innerhalb seines Transportnetzes mehrere VPNs zu konfigurieren. Damit kann der Provider garantieren, dass die Netze verschiedener Kunden virtuell voneinander getrennt sind. Um ein VPN zu konfigurieren muss zunächst der Router-Kennzeichner konfiguriert werden, der angibt zu welchem VPN oder VPN-Dienst ein Paket gehört. Ebenso können, wie bei den Protokollen, Regeln für VPNs definiert werden, die die Filterung von Paketen erlauben oder das Importieren beziehungsweise Exportieren von gelernten Routen ermöglichen. Werden die Router-Kennzeichner falsch konfiguriert, sind eventuell zwei verschiedene VPNs fälschlicherweise miteinander verbunden. Für den Kunden bedeutet dies ein Sicherheitsrisiko, da andere Kunden Zugriff auf die Daten haben. An allen Routern müssen die gleichen Regeln verwendet werden, da ansonsten die Router untereinander teilweise nicht kommunizieren können. Ebenso kann es zu einer eingeschränkten Kommunikation kommen, wenn die Import- und Exportregeln fehlerhaft konfiguriert sind. Gelernte Routen werden im Transportnetz nicht weitergeleitet oder importiert und daher können Teile des VPNs nicht erreichbar sein. Auch besteht wiederum die Gefahr eines Sicherheitsrisikos, wenn durch das Importieren beziehungsweise Exportieren der Routing-Tabellen eine Verbindung zwischen zwei verschiedenen VPNs besteht.

Eine weitere Fehlerquelle besteht bei der Aktualisierung einer Konfiguration auf einem Router. Damit ein Router die neue Konfiguration übernimmt, muss diese durch einen Befehl aktiviert werden. Ansonsten behält die alte Konfiguration ihre Gültigkeit und alle vorgenommen Änderungen gehen verloren. Dadurch entsteht ein unvorhersehbares Verhalten innerhalb des Netzes, wenn einige Netzkomponenten die neue Konfiguration besitzen. Abhängig von den vorgenommen Konfigurationsänderungen an anderen Routern kann es zum Abbau von Verbindungen, zu höherem Verkehr auf einzelnen Links, oder zu Blockierungen von Paketen kommen. Das Problem bei einer nicht aktivierten Konfiguration besteht darin, dass auf den verschiedenen Netzkomponenten unterschiedliche Konfigurationseinstellungen existieren und gegebenenfalls die Protokolle keine Daten austauschen, da die Interface- und Protokolleinstellungen auf den Netzkomponenten nicht mehr zusammenpassen. Alle bereits beschriebenen und in Tabelle 4.2 zusammengefassten Konfigurationsfehler können auftreten.

Konfigurationsfehler auf der Ethernet-Schicht

Wie im vorherigen Abschnitt werden zunächst die Interface-Konfiguration von Ethernet betrachtet. Dabei wird im Detail nur auf die Konfigurationsschritte und Konfigurationsfehler eingegangen, die in den vorherigen Abschnitten noch nicht analysiert wurden.

Auf Ethernet-Interfaces kann die Größe der *Maximum-Transmission-Unit* (MTU) konfiguriert werden. Dies erlaubt dem Netzbetreiber die Größe der Pakete dem Netz-

betrieb anzupassen und gegebenenfalls die maximale Paketgröße pro Interface zu erhöhen, um den Datendurchsatz zu steigern. Die Standard MTU-Größe beträgt 1548 Bytes und kann bis zu einer Paketgröße von 9216 Bytes vergrößert werden, welche dann als Jumbo-Frames bezeichnet werden. Allerdings müssen die Pakete auf allen Ethernet-Interfaces dieselbe MTU-Größe haben, ansonsten können die Pakete auf dem entsprechenden Interface nicht verarbeitet werden. Derartige Schwierigkeiten treten auf, wenn ein jumbo-fähiges Gigababit-Ethernet-Interface mit einem nicht jumbo-fähigem Ethernet-Interface verbunden wird. Es muss dann beachtet werden, dass auf dem jumbo-fähigen Interface die Paketgröße nicht die maximale Paketgröße des anderen Interfaces überschreitet. Der Fehler kann ebenfalls auftreten, wenn ein Ethernet-Switch verwendet wird, der Jumbo-Frames nicht unterstützt. Eine falsche MTU-Größe kann auch dazu führen, dass die Kommunikation nur noch unidirektional zwischen zwei Switches stattfindet. Das ist beispielsweise der Fall, wenn das Quell-Interface keine Jumbo-Frames erlaubt, das Ziel-Interface und alle dazwischen liegenden Interfaces diese aber erlauben. Wird am Ziel-Interface die maximale MTU-Größe konfiguriert, ist zwar eine Kommunikation von der Quelle zum Ziel möglich, allerdings umgekehrt nicht. Die Jumbo-Frames werden am Quell-Interface nicht verarbeitet und deshalb verworfen. Bleiben Bestätigungen für die gesendeten Datenpakete aus, wiederholt TCP daraufhin die nicht beantworteten Pakete, was zu zusätzlichen Datenpaketen auf einer Verbindung führt. Die unidirektionale Kommunikation kann auch zu einem Abbau der Verbindung führen, wenn bei einem Protokoll der höheren Schichten wie OSPF die „Hallo“-Nachrichten ausbleiben.

Wie auf der IP-Schicht verfügen die Protokolle auf der Ethernet-Schicht ebenfalls über „Hallo“- und „Dead“-Timer. Eine Fehlkonfiguration der Timer hat dieselben Auswirkungen, wie sie bereits für die IP-Schicht diskutiert wurden. Falsch gesetzte Timer führen zum Abbau bestehender Verbindungen oder verhindern den Aufbau einer neuen Verbindung. Auch auf Ethernet-Schicht besteht die Möglichkeit VPNs zu konfigurieren. Die Auswirkungen entsprechen wiederum denen auf der IP-Schicht.

Auf der Ethernet-Schicht gibt es bereits einige Fehler- und Managementfunktionen, um den Netzbetrieb auf dieser Schicht zu überwachen. Diese werden allgemein als *Betrieb, Administration und Wartung* (OAM) bezeichnet. Neben dem Aktivieren dieser Funktionalität müssen auch die Haltezeit und der Parameter für die Kontinuitätsüberwachung konfiguriert werden. Dazu gibt es verschiedene Domänenlevel innerhalb einer Wartungsdomäne, mit deren Hilfe bestimmt wird, bis zu welchen Netzknoten eine Überwachungsnachricht gesendet und anschließend an diesem Punkt terminiert werden soll. Protokolle wie Tracerout und Loopback können unter Verwendung der Domänenlevels für die Überwachung des Netzes angewendet werden. Die fehlerhafte Konfiguration der Domänenlevel oder der Wartungsdomänen führt zur Blockierung der Überwachungsnachrichten an dem entsprechenden Endknoten einer Domäne und ruft Fehlermeldungen an den entsprechend zugeordneten Überwachungsknoten hervor. Eine korrekte Netzüberwachung, Fehlerüberprüfung und Fehlerfindung sind gegebenenfalls nicht mehr möglich.

Weitere Ethernet-Überwachungsprotokolle zum Betreiben, zum Administrieren und

zum Überwachen eines Ethernet-Netze sind im IEEE Standard 802.ah [IEEe] definiert und können ebenfalls aktiviert werden. Recovery, Link-Überwachung, Remote-Fehlerdetektion und Remote-Loopback sind Überwachungsprotokolle, die auf jedem Interface aktiviert werden müssen. Des Weiteren müssen die Interface ID, die maximale Rate, die minimale Rate und die Zeitüberschreitungsparameter konfiguriert werden. Das falsche Setzen eines der Parameter führt zu einer nicht korrekt funktionierenden Ethernet-Überwachung und kann zu fehlerhaften Alarmen und Fehlerreaktionen im Transportnetz führen. Eine Zusammenfassung der beschriebenen Fehler findet sich in Tabelle 4.3.

Ethernet-Schicht	Konfigurationsfehler (Datentyp)
MAC-Adresse	Falsche MAC-Adresse **(int)**
QoS-Parameter	Fehlerhafte Konfiguration der Bandbreite **(int)**; falsche Klassifizierungsmethode **(string)**, falscher Priorisierungsparameter **(int)**
Paketgrößer	Falsche MTU-Paketgröße **(int)**
Timer	Fehlkonfiguration des „Hallo‘“-Timers **(int)**, „Dead“-Timers **(int)** und der Haltezeit **(int)**
OAM	Falsche Interface-ID **(int)**; Funktion nicht aktiviert **(int)**; flasche Timer **(int)**
Authentifizierung	Falsche Authentifizierungsmethode **(int, string)**

Tabelle 4.3: Zusammenfassung möglicher Konfigurationsfehler auf der Ethernet-Schicht

4.2.2 Konfigurationsfehler auf der WDM-Schicht

In diesem Abschnitt wird die Konfiguration der WDM-Schicht betrachtet. Die Konfigurationsaufgaben der WDM-Komponenten beinhaltet nicht das Konfigurieren von Protokollen wie bei der Ethernet- und IP-Schicht, sondern das Einstellen von physikalischen Größen wie Wellenlängen und Stromgrenzwerten, um das Verhalten der Komponente zu beeinflussen.

Für die Übertragung der Daten auf der optischen Schicht werden Laser verwendet, bei denen sich die Übertragungsleistung einstellen lässt, um den notwendigen Signal-zu-Rausch Abstand für eine erfolgreiche Übertragung zu erreichen. Ist die Leistung zu gering, verkürzt sich der Übertragungsweg und die Bitfehlerrate nimmt bei der Übertragung zu. Jeder Laser besitzt ein oberes Leistungslimit bis zu dem er betrieben werden darf. Wird das Leistungslimit überschritten, erfolgt nach einer gewissen Zeit eine automatische Abschaltung des Lasers, um eine Beschädigung zu verhindern [MTB99].

Um eine höhere Übertragungskapazität zu erreichen, werden in heutigen Weitver-

kehrsnetzen bis zu 80 Wellenlängen pro Link übertragen. Dazu werden Laserarrays verwendet, wobei jeder Laser eines Arrays auf eine bestimmte Wellenlänge eingestellt wird. Verwenden zwei Laser aufgrund eines Konfigurationsfehlers die gleiche Wellenlänge auf einen Link, kommt es zu Interferenzen und die Daten können am Empfänger nicht korrekt detektiert werden. Bei einer Übertragungsrate von 80 Gbit/s pro Wellenlänge entsteht dadurch ein hoher Datenverlust, der eine Vielzahl von Nutzern und Anwendungen betrifft.

Die Frequenz eines Lasers kann durch Modulation des Laserpumpstroms oder durch die Betriebstemperatur verändert werden. Ein falsch eingestellter Laserpumpstrom beziehungsweise eine falsche Betriebstemperatur bewirkt, dass der Laser Licht mit einer falschen Frequenz in die Glasfaser emittiert. Dadurch kommt es zu Interferenzen auf dem Link, wie bereits oben beschrieben. Neben Interferenzen kann es aber auch zur Blockierung der Wellenlänge an einem Add/Drop-Multiplexer kommen, wenn dieser die fälschlicherweise verwendete Wellenlänge terminiert. Eine höhere Temperatur ist nicht nur für die Verschiebung der Frequenz des ausgesandten Lichts verantwortlich, sondern führt auch zu einer schnelleren Alterung des Lasers. Jeder Laser hat eine spezifische Betriebstemperatur, die für einen fehlerfreien Betrieb eingehalten werden muss. Wird die maximale Betriebstemperatur durch eine fehlerhafte Einstellung überschritten, kann dies zu einem sofortigen Ausfall des Lasers führen. Ein weiterer Effekt ist das schnellere Absinken der Signalstärke eines Lasers, was gleichzeitig den SNR am Empfänger reduziert und zu einer fehlerhaften Detektion des Signals führt.

Laser können auch durch direkte und externe Signale moduliert werden [RS02]. Ein externer Modulator ist beispielsweise das *Mach-Zehnder-Interferometer* (MZI) [JCS+03]. Um einen Laser mit einem MZI zu modellieren, wird eine bestimmte Spannung an dem MZI angelegt, um die zwei Arme des MZI konstruktiv und destruktiv zu überlagern. Bei der konstruktiven Überlagerung ergibt sich eine Ausgangsleistung am Ausgang des MZI und bei der destruktiven Überlagerung ergibt sich keine Ausgangsleistung. Wird die Eingangsspannung des MZI fehlerhaft konfiguriert, erfolgt eine falsche Modellierung des Ausgangssignals. Das bedeutet, dass die konstruktive und destruktive Überlagerung der zwei Arme zur falschen Zeit erfolgt und somit der Laser eine andere Modulation erfährt.

Das gleiche gilt für einstellbare Empfänger, die Wellenlängen in einem bestimmten Frequenzbereich in elektrische Signale umwandeln [RS02]. Wie bei einem Laser führt eine Fehlkonfiguration am Empfänger dazu, dass dieser die empfangenen Wellenlängen blockiert, wenn diese aus einem anderen als dem eingestellten Frequenzbereich ist. Die Blockierung einer Wellenlänge kann auf einer höheren Schicht, das Rerouting des Datenverkehrs auf Ersatzwege auslösen, wenn dies das verwendete Protokoll vorsieht.

Zur optischen Verstärkung der Wellenlängen, werden in Weitverkehrsnetzen sogenannte *Erbium dopted Fiber Amplifier* (EDFA)s eingesetzt. Mittels EDFAs werden alle Wellenlängen innerhalb eines Glasfaserkabels verstärkt. Zur Verstärkung des optischen Signals besitzt ein EDFA einen Pumplaser, der die Ionen im aktiven Material

des Verstärkers auf ein höheres Energieniveau hebt. Dabei hängt die benötigte Pumpleistung für eine konstante Ausgangsleistung von der übertragenen Wellenlänge ab. Wird die Pumpleistung des optischen Verstärkers zu niedrig eingestellt, ist die Verstärkung des Eingangssignals und folglich der SNR am Empfänger zu gering. Wie oben beschrieben erhöht dies die Wahrscheinlichkeit für eine fehlerhafte Detektion des Signals am Empfänger. Wenn die Pumpleistung des EDFAs zu hoch eingestellt ist, erhöht sich die spontane Emission der angeregten Ionen und es verbleiben weniger angeregte Ionen für die stimulierte Emission. Dadurch sinkt der Verstärkungsfaktor des EDFAs und das Eingangssignal wird nicht ausreichend verstärkt. Auch die Betriebstemperatur des Verstärkers hat einen Einfluss auf die Verstärkung. Mit zunehmender Temperatur nimmt der Verstärkungsfaktor ab, was wiederum den SNR am Empfänger negativ beeinflusst [KDL97].

Die oben beschriebenen Konfigurationsfehler eines EDFAs können für den Verlust von Informationen auf einem Link oder Pfad verantwortlich sein, da das Eingangssignal nicht korrekt verstärkt wird. Ein geringerer SNR am Ausgang des EDFAs reduziert die Übertragungsreichweite des Sendesignals, so dass das Signal am Empfänger eventuell nicht mehr richtig detektiert wird. Da ein EDFA alle Wellenlängen auf einer Glasfaser zur selben Zeit verstärkt, sind von diesem Fehler alle Wellenlängen des Links betroffen. Protokolle, die auf höheren Schichten verwendet werden, wie zum Beispiel OSPF, versuchen automatisch Ersatzwege zu berechnen, falls der Arbeitspfad nicht mehr vorhanden ist. Somit wird der Verkehr des gesamten Links neu geroutet und kann zu Blockierungen der Datenpakete auf anderen Links führen, wenn die restliche Kapazität im Weitverkehrsnetz nicht ausreichend dimensioniert ist.

Wie bereits erwähnt, werden in heutigen Transportnetzen mehrere verschiedene Wellenlängen gleichzeitig auf einem Netzlink übertragen, um die nutzbare Bandbreite zu erhöhen. Die Verwendung mehrerer Wellenlängen wird als DWDM bezeichnet. Für das Multiplexing der Wellenlängen auf einen Link wird ein DWDM-Kontroller verwendet. Die Konfiguration eines DWDM-Kontrollers umfasst das Einstellen des Empfangsleistungsschwellwerts des Transponders, die Kanalnummer der Wellenlänge und die Übertragungsleistung. Wie bereits bei den Lasern beschrieben, ist die Übertragungsleistung entscheidend für das SNR am Empfänger und damit für die Signalqualität. Um eine fehlerfreie Übertragung der Daten zu gewährleisten muss eine ausreichend hohe Übertragungsleistung konfiguriert werden. Liegt ein empfangenes Signal unter diesem Schwellenwert, wird der *Loss of Signal* (LoS)-Alarm ausgelöst, der angibt, ob die Signalqualität am Empfänger für eine fehlerfreie Detektion zu gering ist. Ein zu hoher Schwellenwert für die Empfangsleistung führt dazu, dass das Signal vom Empfänger fehlerfrei empfangen wird, aber trotzdem ein Alarm ausgelöst wird und die Protokolle auf den höheren Transportschichten den Verkehr auf die Ersatzwege umrouten. Ein zu niedrig eingestellter Schwellenwert bewirkt das Gegenteil, so dass auch bei einem schwachen Empfangssignal kein Alarm ausgelöst wird. Die fehlerhafte Übertragung wird somit nicht auf der optischen Schicht detektiert, sondern erst durch die Protokolle auf den höheren Schichten, wenn der Inhalt der Pakete analysiert wird. Da der Fehler erst auf einer höheren Kommunikationsschicht detektiert wird, dauert die Fehlerfindung ebenfalls länger,

als wenn auf der optischen Schicht ein Alarm ausgelöst wird.

Ein weiteres optisches Element, welches in Transportnetzen eingesetzt wird, ist der *Reconfigurable Optical Add-Drop Multiplexer* (ROADM). Dieser erlaubt es während der optischen Übertragung Wellenlängen zu entfernen und hinzuzufügen. Diese Eigenschaft erleichtert die Planung von Kommunikationsnetzen, da an jeder Stelle im Netz, an der ein ROADM verwendet wird, die verwendeten Wellenlängen flexibel verändert werden können. Im Vergleich zu Knoten, an denen Wellenlängen fest eingestellt werden, erhöht sich bei ROADMs die Flexibilität, da der Netzbetreiber irgendeine freie Wellenlänge für das Routing verwenden kann und nicht die fest eingestellte Wellenlänge verwenden muss. Die Möglichkeit Wellenlängen flexibel hinzuzufügen erhöht jedoch auch die Fehlerwahrscheinlichkeit beim Konfigurieren der ROADMs. Eine Fehlkonfiguration des ROADMs kann zum Blockieren oder zum Hinzufügen einer falschen Wellenlänge führen. Ebenso kann im Fehlerfall die Ersatzschaltung bei falsch hinzugefügten Wellenlängen fehlschlagen.

WDM-Schicht	Konfigurationsfehler (Datentyp)
Verstellbarer Laser	Zu geringe Signalverstärkung **(int)**, Wellenlängenverschiebung **(int)**; schnelle Alterung der Komponenten **(int)**
Optischer Empfänger	Detektion einer falschen Wellenlänge **(int)**
Optischer Verstärker	Zu geringe Signalverstärkung **(int)**
Patchfeld	Erzeugung von Schleifen; nicht verbundene Kunden; Sicherheitsrisiken
Wellenlängenzuweisung	Wellenlängen am Empfänger terminiert **(int)**; Interferenz auf einem Link **(int)**
Wellenlängenkontroller	Zu geringe Signalverstärkung **(int)**
ROADM	Hinzufügen und Terminierung falscher Wellenlängen **(int)**, Interferenzen auf einem Link **(int)**

Tabelle 4.4: Zusammenfassung möglicher Konfigurationsfehler auf der optischen Schicht

Eine weitere Fehlkonfigurationsmöglichkeit betrifft das Patchfeld an der Rückseite der Netzkomponenten. Wenn beispielsweise eine Interface-Karte ausgetauscht wird, müssen die Kabelverbindungen getrennt und neu gesteckt werden. Ein fehlerhaftes Verbinden der Glasfaserverbindungen führt zu einer Vielzahl von Störungen im Netz. Im Netz können Schleifen entstehen, die dazu führen, dass Pakete mehrfach gesendet werden, ohne das Ziel zu erreichen. Bestimmte Interfaces im Netz sind durch eine fehlerhafte Steckverbindung nicht mehr erreichbar oder Kunden, die über die fehlerhafte Verbindung an das Transportnetz angeschlossen sind, haben keine Verbindung mehr zum Netz.

4.2.3 Diskussion

In den vorherigen Abschnitten wurden die am häufigsten verwendeten Konfigurationsschritte und die daraus resultierenden Fehler und Auswirkungen diskutiert. Die Analysen haben gezeigt, dass Konfigurationsfehler ein ähnliches Fehlermuster wie physikalische Fehler besitzen. Konfigurationsfehler beeinflussen dabei nicht nur einen Link beziehungsweise Knoten in einem Weitverkehrsnetz, sondern reduzieren die Performanz in großen Bereichen des Netzes. Die Auswirkung eines Fehlers hängt dabei immer von der Anzahl der Netzknoten ab, die fehlerhaft konfiguriert wurden.

Aber bereits eine Fehlkonfiguration auf einem Netzknoten kann sich auf weite Teile des Netzes auswirken. Zum Beispiel die falsche Eingabe einer IP-Adresse auf einem Interface führt dazu, dass im schlechtesten Fall ein gesamtes *Autonomes System* (AS) nicht mehr erreichbar ist, wenn der Fehler auf einem Netzeingangsrouter auftritt. Die Fehlermuster der beschriebenen Konfigurationsfehler aller betrachteten Schichten sind in Tabelle 4.5 zusammengefasst.

Konfigurationsfehler	Potentielle Fehlermuster
Adressenfehler	Ausfall einzelner Interfaces oder gesamter Knoten; Schleife im Netz;
Fehlerhafte Filterregeln	Linkausfall; Paketverluste; Umrouten des Verkehrs auf Ersatzlink oder -pfad; Erhöhtes Verkehrsaufkommens auf anderen Links; Größere Verzögerung der Pakete
Fehlerhafte Authentifizierung	Linkausfall oder Pfadausfall; Umrouten des Verkehrs auf Ersatzlink oder -pfad
Fehlerhafte Timer	Linkausfall oder Pfadausfall; Umrouten des Verkehrs auf Ersatzlink oder -pfad; erhöhtes Verkehrsaufkommen auf anderen Links
Falsche Verkabelung	Schleifen im Netz; Linkausfall
Flascher Pumpstrom	Linkausfall; fehlerhafte Übertragung
Falsche Wellenlängenzuweisung	Interferenzen auf einem Link; Paketverluste

Tabelle 4.5: Fehlermuster der analysierten Konfigurationsfehler

Die genannten Konfigurationsfehler führen zu Fehlermustern, die physikalischen Fehlern ähneln, da sie ebenfalls Linkausfälle oder Hardwareausfälle hervorrufen können. Die Fehlkonfiguration eines Patchpanels auf einem Knoten führt beispielsweise zum Ausfall des entsprechenden Links. Eine Steuerungsebene oder Managementebene routet anschließend den Datenverkehr auf Ersatzwege um. Für einen Netzbetreiber erscheint der betroffene Link als physikalisch ausgefallen und auf den anderen Links, auf denen der betroffene Verkehr umgeroutet wird, beobachtet er eventuell ein erhöhtes Verkehrsaufkommen und eine höhere Verzögerung. Das Beispiel zeigt,

dass ein Konfigurationsfehler eine Reihe unterschiedlicher Fehlermuster in einem Weitverkehrsnetz hervorruft. Die falsche Konfiguration der Laser oder Empfänger kann ebenfalls zu einem physikalischen Ausfall führen. Für einen Netzbetreiber besteht die Schwierigkeit darin, die genannten Auswirkungen eindeutig einem Konfigurationsfehler zuzuordnen.

Da eine allgemeine Angabe über die Auswirkung eines Konfigurationsfehlers nur schwer möglich ist, wird im nächsten Abschnitt eine Bewertungsmetrik für Konfigurationsfehler und deren Auswirkungen entwickelt. Die Metrik dient dem Netzmanagementsystem in Kapitel 6 dazu, aufgetretene Konfigurationsfehler zu bewerten und die Lösung der Fehler zu priorisieren.

4.3 Bewertung und Gewichtung der Konfigurationsfehler

Die im vorherigen Abschnitt beschriebenen Konfigurationsfehler wirken sich unterschiedlich auf ein Weitverkehrsnetz aus. Deshalb erfolgt in diesem Abschnitt eine Bewertung der Fehler anhand verschiedener Parameter. Die Gewichtung eines Fehlers bestimmt, mit welcher Priorität nach einer Lösung für den Fehler gesucht wird. Da häufig mehrere Fehler gleichzeitig und an verschiedenen Orten in einem Weitverkehrsnetz auftreten, ist eine Abstufung der Fehler notwendig.

In Tabelle 4.6 sind diejenigen Kriterien aufgeführt, die zur Bewertung der Konfigurationsfehler beitragen.

Betroffene Anzahl	Fehlerauswirkung	Zeitdauer (min)	SLA Verletzung
Kanten	Anstieg Verzögerung	$t < 1$	Nein
Knoten	Erhöhtes Verkehrsaufkommen	$1 < t < 5$	Ja
Verkehrsanforderungen	Anstieg Blockierung	$5 < t < 60$	-
-	Nicht verbunden	$60 < t < 1440$	-
-	-	$1440 < t$	-

Tabelle 4.6: Systemparameter für die Bewertung der Konfigurationsfehler

Mittels der Bewertungskriterien bestimmt das Netzmanagementsystem in Kapitel 6, in welcher Reihenfolge die aufgetretenen Konfigurationsfehler gelöst werden. Ein Konfigurationsfehler wird dazu nach verschiedenen Gesichtspunkten bewertet. Wie stark sich ein Fehler auf ein Weitverkehrsnetz auswirkt, hängt vor allem von der Anzahl der betroffenen Kanten, Knoten und Verkehrsanforderungen ab. Daher erfolgt mit steigender Anzahl an betroffenen Netzelementen eine höhere Gewichtung der

Fehler. Daneben werden die Auswirkungen der Konfigurationsfehler gewichtet. Relevant sind vor allem die Verzögerungen und Blockierungen die aufgrund eines Konfigurationsfehlers auf den Links entstehen. Je höher die Verzögerung oder Blockierung ist, umso höher ist auch die entsprechende Gewichtung. Wie im vorherigen Abschnitt dargestellt, rufen bestimmte Konfigurationsfehler mehrere Störungen gleichzeitig hervor, weshalb in solch einem Fall alle auftretenden Symptome zur Gewichtung des Fehlers beitragen.

Ein weiterer Bewertungsparameter ist die Zeitspanne, während der ein Konfigurationsfehler besteht und die Performanz des Netzes beeinträchtigt. In Tabelle 4.6 sind verschiedene Zeitintervalle dargestellt, innerhalb derer sich die Gewichtung des Konfigurationsfehlers erhöht. Als letzter Parameter fließt die Verletzung der Dienstgüte, die sogenannten *Service Level Agreement* (SLA), in die Bewertung der Konfigurationsfehler ein. Da die Nichteinhaltung der Dienstgüte zu Strafzahlungen führt, werden die entsprechenden Parameter besonders hoch gewichtet, um eine schnelle Behebung des Fehlers zu erreichen. Der Parameter für die Verletzung der Dienstgüte ist null, solange keine Verletzungen der Dienstgüte erfolgen.

Um eine Gewichtung der verschiedenen Konfigurationsfehler zu erhalten, werden die beschriebenen Parameter mit Gewichtungsfunktionen beschrieben und tragen entsprechend der Formel 4.1 zur Gesamtgewichtung eines Fehler bei.

$$G_j(g_a,g_f,g_z,g_{SLA}) = \frac{1}{\sum_{j=1}^{N_G} g_j} \cdot \sum_{j=1}^{N_G} g_j \cdot F_j(g_a,g_f,g_z,g_{SLA}) \tag{4.1}$$

Die Gewichtung G_j eines Fehlers berechnet sich aus der Summe der einzelnen Gewichtungsfunktionen, die durch den Gewichtungsfaktor w_j geteilt wird, um die Gewichtung G_j auf den Bereich $[0,1]$ zu normieren. Die einzelnen Gewichtungsfunktionen g_a, g_f, g_z und g_{SLA} sind folgendermaßen definiert.

$$g_a = \mu \cdot x \quad \forall x \in [0,x_{max}], \quad x_{max} > 0, \mu > 0 \tag{4.2}$$

$$g_f = \mu \cdot e^{\mu \cdot x} \quad \forall x \in [0,x_{max}], \quad x_{max} > 0, \mu > 0 \tag{4.3}$$

$$g_z = \mu \cdot t \quad \forall t \in [0,\mathbb{R}^+], \mu > 0 \tag{4.4}$$

$$g_{SLA} = \begin{cases} 1000 & : B > B_S \vee D > D_S \vee C < C_{min} \\ 0 & : sonst \end{cases} \tag{4.5}$$

Alle Gewichtungsfunktionen außer g_{SLA} stellen streng monoton steigende Kurven dar, welche mit steigendem Einfluss der Fehler auf das Weitverkehrsnetz zunehmen. Der Parameter μ wird vom Netzbetreiber festgelegt und dient zur Skalierung der einzelnen Funktionen, um bestimmten Auswirkungen eines Fehlers eine höhere Gewich-

tung zu geben. Die Funktionen g_a und g_z besitzen einen linearen Verlauf und beschreiben die Anzahl der betroffene Knoten und Kanten sowie die Zeitdauer des Fehlers. Es wird angenommen, dass die Kosten für die Verletzung der Dienstgüteparameter linear mit der Zeitdauer ansteigen und deshalb auch die Gewichtungsfunktion g_z linear zunimmt. Die Gewichtungsfunktion g_a erhöht sich mit zunehmender Anzahl an Netzknoten und Kanten. Die Gewichtungsfunktion g_f hängt mit der Blockierung und Verzögerung auf den Links zusammen, die aufgrund eines Konfigurationsfehlers entstehen. Das bedeutet, dass mit zunehmenden auftretenden Verzögerungen und Blockierungen die Gewichtungsfunktion g_f ansteigt. Dabei orientiert sich der Verlauf der Kurve an der Verkehrstheorie und steigt exponentiell an. Für den Verlauf wird ein Wartesystem zugrunde gelegt, bei dem die Warteschlange exponentiell mit dem steigenden Angebot zunimmt. Die Funktion g_{SLA} gibt an, ob bei bestimmten Diensten die Dienstgüte verletzt wird. Überschreiten Dienstgüteparameter wie die Blockierung B und die Verzögerung D einen vertraglich festgelegten Schwellwert, kommt es zu einer Verletzung der Dienstgüte. Dasselbe gilt, falls die Kapazität C unter den zugesicherten Wert C_{min} fällt. Eine Verletzung der Dienstgüte wird in Formel 4.1 höher gewichtet als die restlichen Parameter.

Die beschriebenen Gewichtungsfunktionen ermöglichen es, einen aufgetretenen Konfigurationsfehler einzustufen und zu gewichten. Allerdings ist es nicht möglich, jedem Konfigurationsfehler eine feste Gewichtung zuzuteilen. Die Gewichtung hängt wie dargestellt von verschiedenen Faktoren wie Netzgröße und betroffenen Diensten ab und daher ergeben sich eventuell für zwei gleiche Konfigurationsfehler in unterschiedlichen Weitverkehrsnetzen unterschiedliche Gewichtungen. Auch eine generelle Aussage, dass beispielsweise die Fehlkonfiguration der Filterregeln eine höhere Gewichtung besitzt als eine Fehlkonfiguration der IP-Adresse, kann nicht getroffen werden. Aufgrund der diskutierten Auswirkungen stellen Konfigurationsfehler wie Filterregeln meistens einen schwerwiegenderen Fehler dar, aber eine genauere Aussage kann nur anhand der aktuellen Netzsituation erfolgen. Deshalb werden die beschriebenen Gewichtungsfunktionen in dem teilautomatisierten Netzmanagementsystem in Kapitel 6 verwendet, um anhand der aktuellen Auswirkung eines Fehlers dessen Gewichtung und Priorität zu ermitteln.

4.4 Zusammenfassung

In diesem Kapitel wurden potentielle Konfigurationsfehler auf den verschiedenen Schichten und deren Auswirkung auf ein Weitverkehrsnetz diskutiert. Dazu wurden die Konfigurationsfehler nach Schichten aufgeteilt beschrieben. Ein wichtiger Aspekt ist dabei die Häufigkeit und die Komplexität der Konfigurationsaufgaben. Dazu wurde anhand der Anzahl an Konfigurationsbefehlen von heutigen Router die Gesamtanzahl der Konfigurationen in einem Weitverkehrsnetz bestimmt. Die Untersuchungen haben gezeigt, dass vor allem die Filterregeln und die Abhängigkeiten zwischen den Protokollen die größten Auswirkungen auf ein Netz haben.

Die Herausforderungen beim Auffinden von Konfigurationsfehlern beruhen darauf, dass häufig keine Alarmnachrichten gesendet werden, die einen Hinweis auf den Fehler liefern. Die Beschreibung der Konfigurationsfehler und die potentiellen Auswirkungen dienen dazu, Anomalien im Netz, die keine Alarmnachrichten hervorrufen, auf Konfigurationsfehler zurückzuführen. Die Analyse der Konfigurationsfehler hat gezeigt, dass diese unter anderem für Verbindungsabbrüche, höhere Verzögerungen und höhere Paketverluste verantwortlich sind. Oftmals bewirkt ein Konfigurationsfehler auch mehrere dieser Fehler zur gleichen Zeit. Das Auffinden von Konfigurationsfehlern war nicht Teil dieses Kapitels. In der Literatur existiert eine Reihe von statistischen Methoden, um von Fehlermustern auf Konfigurationsfehler zu schließen. Die in diesem Kapitel beschriebenen Fehlermuster dienen als Eingangsparameter für statistische Methoden zur Detektion von Konfigurationsfehlern.

Da nicht alle Konfigurationsfehler dieselbe Auswirkung auf ein Weitverkehrsnetz haben, wurde ein Bewertungssystem entwickelt, das die Konfigurationsfehler anhand von verschiedenen Kriterien klassifiziert. Für jedes Kriterium wurde eine Gewichtungsfunktion verwendet, die abhängig von der Auswirkung eines Kriteriums unterschiedlich stark zur Gewichtung des Konfigurationsfehlers beiträgt.

5 Proaktives Verfahren für robusten Betrieb eines Weitverkehrsnetzes

In diesem Kapitel wird ein proaktives Verfahren zur Detektion von Degradationen von *Erbium dopted Fiber Amplifier* (EDFA) und Lasern sowie verschiedene Austauschstrategien für die degradierten Komponenten entwickelt. Das Ziel ist es, durch eine geeignete Beschreibung des Degradationsverlaufs der optischen Komponenten rechtzeitig einen bevorstehenden Ausfall zu erkennen und diesem dem Netzmanagement mitzuteilen. Das rechtzeitige Erkennen eines bevorstehenden Ausfalls soll die Ausfallzeit eines Links reduzieren und die Gesamtverfügbarkeit des Netzes erhöhen. Dazu wird das in dieser Arbeit entwickelte Degradationskonzept mit einem Fehler-pro-Zeit (FIT) Modell verglichen, welches die Fehlerrate einer Komponente pro 10^9 Stunden angibt.

Anschließend an die Beschreibung des Degradationskonzepts werden verschiedene Austauschstrategien für EDFAs anhand eines beispielhaften Links vorgestellt. Dabei wird untersucht, wie sich der gleichzeitige Austausch von einem oder mehreren EDFAs auf die Verfügbarkeit eines Links oder des gesamten Netzes auswirkt. Danach erfolgt anhand eines Beispielnetzes eine Analyse der Betriebskosten der verschiedenen Austauschstrategien.

Im letzten Abschnitt des Kapitels wird das Degradationskonzept auf Laser und Empfänger erweitert. Ebenso wird die Auswirkung der Anzahl der Netzbetriebszentren auf den Reparaturprozess und die Verfügbarkeit des Netzes untersucht. Die höhere Anzahl an Betriebszentren ermöglicht es, mehrere Netzkomponenten innerhalb einer Arbeitsschicht zu reparieren sowie Fahrzeit und Betriebskosten einzusparen.

5.1 Schicht-1 Überwachung von optischen Komponenten

Bei hochbitratigen Übertragungssystemen sind kohärente Empfänger für eine wesentliche Bandbreitenerhöhung geeignet. Kohärente Empfänger verwenden einen *lokalen Oszillatorlaser* (LO), um das optische Signal unter Verwendung eines optischen 90°-Hybrid [TZI+07] abwärts zu konvertieren. Für die Rückgewinnung der Inphase und Quadraturkomponente des optischen Signals werden zwei Single-Ended-Fotodioden oder zwei symmetrische Detektoren pro orthogonaler Polarisation verwendet. Dadurch wird das optische Signal in ein elektrisches Signal gewandelt. Die digitale

Signalverarbeitung ermöglicht einen flexiblen Gebrauch von höherwertigen Modulationsverfahren mit höherer spektraler Effizienz wie *Quadratur Phase Shift Keying* (QPSK) [WE06]. Ein optischer Empfänger mit digitaler Signalverarbeitung ist nicht nur imstande, alle linearen Verzerrungen der Glasfaser auszugleichen, sondern kann auch Überwachungsinformationen ohne zusätzlichen Aufwand liefern. Während des Entzerrens erlauben die verschiedenen Entzerrungszustände in der digitalen Signalverarbeitung einen Rückschluss auf die physikalischen Eigenschaften des optischen Kanals. Abbildung 5.1 zeigt einen optischen kohärenten Empfänger, der Überwachungsfähigkeiten mit einschließt.

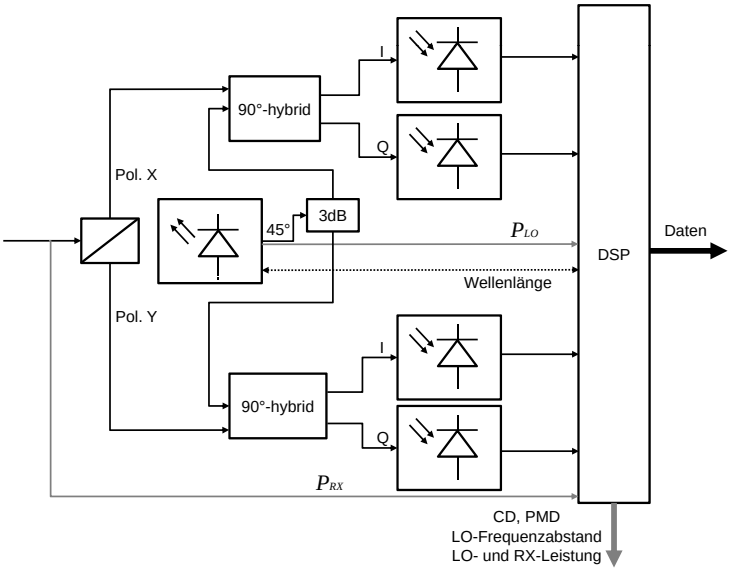


Abbildung 5.1: Optischer kohärenter Empfänger

Wie in konventionellen Empfängern üblich, wird die Leistung des Eingangssignals überwacht. Das LO-Lasermodul überwacht auch die eigene Leistung. Die aktuell verwendete Wellenlänge ist dem LO-Lasermodul ebenfalls bekannt, da es die Transmitterlaserwellenlänge für die richtige Abwärtskonvertierung zu entzerren hat. Die digitale Signalverarbeitung liefert Informationen über die *Chromatische Dispersion* (CD), *Polarisationsmodendispersion* (PMD) [HKP+08] und den Frequenzabstand zwischen Sender und Empfänger [TZI+07].

Der Ausfall eines optischen Kanals wird durch unterschiedliche Komponenten in einem optischen Transportnetz erzeugt. Abhängig davon, welche Komponente den Ausfall verursacht, sind eine oder mehrere Wellenlängen beziehungsweise der gesamte Link betroffen. Einzelne Wellenlängenfehler sind weniger kritisch, da nur ein Teil des Verkehrs auf einem Link umgeroutet werden muss. Für einen einzelnen Wellenlängenfehler können sowohl ein Laser als auch ein Empfänger am gleichen Link verantwortlich sein. Die Leistungsüberwachung des empfangenen Signals und die LO-Laser bieten Hinweise auf eine sich verschlechternde Signalqualität. So hängt beispielsweise der Signal-Rausch-Abstand am Empfänger von der LO-Laserleistung ab. Eine abnehmende Leistung an irgendeinem Laser kann ein Anzeichen für einen

bevorstehenden Fehler sein, welcher zu einem Netzmanagementsystem gesendet werden kann. Der Frequenzabstand zwischen LO-Laser und dem *Transmitter* (TX)-Laser wir kompensiert, indem die Information der digitalen Signalverarbeitung verwendet wird. Der LO-Laser wird auf die Wellenlänge des TX-Lasers eingestellt und der verbleibende Frequenzabstand, der in Intradyne-Empfang resultiert, wird durch eine digitale Trägerrückgewinnung (Carrier Recovery) kompensiert. Die Abweichung des TX-Lasers führt jedoch zu einem Ausfall, wenn der Einstellbereich des LO-Lasers überschritten wird. Dies tritt auf, wenn ein DFB-Laser einen signifikant kleineren Einstellbereich besitzt als ein ECL, der als LO verwendet wird. Des Weiteren kann die TX-Laser-Abweichung zu Interferenzen mit benachbarten Kanälen führen. Aus den genannten Gründen kann eine Frequenzabweichung von zwei Lasern als Hinweis auf einen bevorstehenden Fehler dienen.

Der Ausfall eines gesamten Links beeinträchtigt alle Wellenlängenkanäle auf diesem Link und stellt daher für den Netzbetrieb einen äußerst kritischen Fehlerfall dar. Den Ausfall eines Links rufen verschiedene Komponenten hervor. Optische Verstärker sind eine mögliche Fehlerquelle. Wenn die Netztopologie bekannt ist, kann die Empfangsleistung von allen Kanälen, die durch denselben EDFA oder Raman-Verstärker erhöht werden, überwacht und Leistungsabweichungen durch das Managementsystem festgestellt werden. Dieselbe Methode kann bei der Detektion von Abweichungen bei optischen Filtern angewandt werden. Optische Filter terminieren die voreingestellte Wellenlänge auf einem Link. Ist die falsche Wellenlänge eingestellt, führt dies ebenfalls zu Linkausfällen. Auch Glasfaserausfälle können mittels der Leistungsüberwachung lokalisiert werden. Die Glasfaserdispersion verändert sich mit den Umgebungsbedingungen und kann als Maß für einen bevorstehenden Fehler herangezogen werden [VL03]. Chromatische Dispersion kann mit einem kohärenten optischen Empfänger innerhalb eines gewissen Bereichs kompensiert werden. Allerdings kann es auch ein Problem für Legacy-Kanäle auf demselben Link darstellen. Deshalb ist es sinnvoll, aus den CD-Werten, die bei der digitalen Signalverarbeitung gemessen werden, eine Warnnachricht für die Legacy-Kanäle zu generieren und diese an ein Managementsystem zu senden. Darüber hinaus ist es sogar möglich, steigende Temperaturen zu erkennen. Diese sind ein Anzeichen für einen Ausfall des Temperaturkontrollsystems an einem physikalischen Knotenpunkt, an dem die dispersionskompensierende Glasfaser installiert ist.

Im Folgenden werden kurz drei Störeinflüsse eines optischen Übertragungssystems vorgestellt, die an einem Empfänger detektiert und als Warnnachricht an das Managementsystem gesendet werden können. Zunächst werden zwei Dispersionseigenschaften des sich in einer Faser ausbreitenden Lichts beschrieben. Als Dispersion bezeichnet man im Allgemeinen, dass die Phasengeschwindigkeit einer Lichtwelle oder die Gruppengeschwindigkeit mehrerer Lichtwellen von der Frequenz abhängt.

5.1.1 Chromatische Dispersion

Die CD tritt bei der Ausbreitung von Licht in einer Glasfaser auf und führt zur Verbreiterung des Pulses am Empfänger. Die Verbreiterung ist umso größer, je länger die Übertragungsstrecke ist. Durch die Verbreiterung des Pulses kann es am Empfänger zu Interferenzen mit den vorausgegangenen oder nachfolgenden Impulsen kommen. Die CD besteht aus zwei Effekten: der Material- und Wellenleiterdispersion [EWAD88]. Dabei wird oftmals unter der CD nur die Materialdispersion in einer Standard-Monomode-Faser verstanden. Da sich die CD messen lässt und dispersionskompensierende Glasfasern existieren, kann die Dispersion kompensiert werden. Die Kompensation der Dispersion erfolgt ebenfalls wie die Verstärkung in konstanten Abschnitten, um eine Interferenz mit weiteren Lichtimpulsen zu vermeiden. Verändert sich die chromatische Dispersion in einer Faser, beispielsweise durch eine veränderte Temperatur oder Druck auf die Faser, wird diese durch die dispersionskompensierende Glasfaser nicht vollständig kompensiert und am Empfänger kann diese Abweichung detektiert werden. Die abweichenden Werte werden beispielsweise mittels *Simple Network Management Protocol* (SNMP) an das Netzmanagementsystem gesendet, um die Veränderung und einen potentiellen Ausfall der Faser zu melden.

5.1.2 Polarisationsmodendispersion

Eine weitere Einflussgröße auf das ausbreitende Licht, stellt die PMD dar. Bei der PMD breiten sich die unterschiedlichen Polarisationen des Lichts unterschiedlich schnell aus. Die Laufzeitunterschiede zwischen den Polarisationen hängen ebenfalls von der Länge der Strecke ab. Der Einfluss der PMD ist bei Übertragungssystemen mit $10\,\mathrm{Gbit/s}$ im Vergleich zur CD vernachlässigbar. Allerdings ändert sich dies, wenn höhere Übertragungsraten von $40\,\mathrm{Gbit/s}$ oder mehr verwendet werden. Da die PMD nicht kompensiert werden kann, muss vor Inbetriebnahme der Glasfaser, diese auf PMD untersucht werden. Des Weiteren hängt die PMD auch von der Temperatur, dem Zug und dem Druck auf die Faser ab. Das bedeutet, dass sich die PMD im Betrieb ändern kann und es somit zu Interferenzen zwischen den einzelnen Lichtimpulsen kommt. Diese sich verändernden Eigenschaften sind ein Grund, diese am Empfänger zu detektieren und an das Netzmanagementsystem zu senden, um Veränderungen der PMD schnellstmöglich zu erkennen und reagieren zu können, bevor Daten verloren gehen.

5.1.3 (Pump-)Laser Degradation

Optische Komponenten sind ebenfalls einem Alterungsprozess unterworfen. Dabei stellen Laser eine wichtige Rolle in heutigen Transportnetzen dar, da sie mit am häufigsten eingesetzt werden. Sie werden nicht nur als Sender, sondern auch als Pumplaser in optischen Verstärkern wie EDFAs eingesetzt. Ein Laser kann spontan ausfallen oder, wie später für EDFAs beschrieben, schrittweise degradieren [Wat91].

Die Degradationsrate hängt dabei von verschiedenen Faktoren wie Temperatur, Belastung und Kristallwachstumsparameter ab. Durch die Degradation nimmt die aktive Region, die stimuliert werden kann, ab und es stehen weniger aktive Ionen zur Verfügung. Die graduelle Degradation kann durch Algorithmen, wie in [Rap05] vorgestellt, überwacht und ebenfalls an den Netzbetreiber beziehungsweise das Netzmanagementsystem gesendet werden. Anhand der aktuellen und vergangenen physikalischen Werte eines Lasers können Rückschlüsse auf die zukünftige Degradation geschlossen werden. Eine detailliertere Beschreibung weiterer Degradationseffekte von Lasern findet man in [Wat91].

5.2 Überwachung von Degradationsparametern

Für die proaktive Fehlerfindung in Weitverkehrsnetzen müssen zusätzliche Informationen berücksichtigt werden, die einen Rückschluss auf zukünftige Entwicklungen erlauben. In Kapitel 4 wurden deshalb auf Protokollebene Konfigurationsfehler und deren Auswirkungen untersucht, um zu bewerten, ob es sich bei einer vorhandenen Netzanomalie um einen Konfigurationsfehler handelt. Mithilfe des Bewertungsschemas für Konfigurationsfehler, lässt sich die Priorität bei der Suche nach einer Lösung definieren.

Um den Ausfall von optischen Netzkomponenten frühzeitig zu erkennen, müssen zusätzliche Informationen von den physikalischen Parametern erfasst werden und an ein Netzmanagement gesendet werden. Mittels der Werte der optischen Netzkomponenten ist es möglich, diejenigen Abschnitte in einem Weitverkehrsnetz zu bestimmen, die mit hoher Wahrscheinlichkeit als nächstes ausfallen werden. Das Netzmanagementsystem, das in Kapitel 6 entwickelt wird, kann durch dieses Wissen die Vorausplanung von Ersatzkonfigurationen steuern und muss nicht sämtliche Fehlerszenarien vorausplanen. Teile der Ergebnisse aus diesem Kapitel wurden bereits in [Mer10] veröffentlicht.

5.2.1 Überwachungsprotokoll zur Parameterabfrage

Die im vorherigen Abschnitt beschriebenen detektierten Werte werden regelmäßig an das Netzmanagementsystem übermittelt, um den aktuellen Status der Netzkomponenten zu übermitteln und einen bevorstehenden Ausfall zu verhindern. Dazu eignet sich SNMP, welches auch zur Konfiguration und zur Abfrage von Konfigurationsparametern der Komponenten eingesetzt wird. Die Management Information Base jeder Komponente muss dazu um die jeweiligen Degradationswerte erweitert werden, damit die Werte in der Datenbank der Komponente gespeichert werden. Mittels der „Get“-, „Response“-Funktionen erfolgt eine Abfrage der entsprechenden Werte. Alternativ werden mittels der „Trap“-Funktion die Werte periodisch an das Netzmanagement übermittelt.

5.2.2 Häufigkeit der Abfrage der Degradationswerte

Um einen möglichst genauen Degradationsverlauf aller Netzkomponenten zu erhalten, ist eine regelmäßige Abfrage der Degradationswerte entscheidend. Die Häufigkeit der Abfrage orientiert sich an dem aktuellen Zustand der jeweiligen Netzkomponente. Wie später in Abschnitt 5.3 diskutiert, werden die optischen Netzkomponenten in einem bestimmten Arbeitsbereich betrieben. Dieser Arbeitsbereich wird durch einen Anfangswert und einen maximal zulässigen Grenzwert definiert. Bei den betrachteten EDFAs ist dies zum Beispiel der aktuelle Pumpstrom, der für die Verstärkung des Eingangssignals benötigt wird.

Für die Abfrage der Degradationswerte sind zwei verschiedene Strategien denkbar. Die einfachere Methode definiert ein konstantes Zeitintervall, innerhalb dessen die Werte zum Netzmanagement gesendet werden. Der Vorteil dieses Verfahrens besteht darin, dass man einen genauen Verlauf der Degradation abbilden kann und durch Interpolation der Werte den weiteren Verlauf der Degradation abschätzen kann. Allerdings ist der Signalisierungsverkehr höher, da die Werte regelmäßig an das Netzmanagement gesendet werden, auch wenn die Netzkomponente noch keine Anzeichen einer Degradation aufweist. Somit wird zusätzlicher Signalisierungsverkehr in einem Weitverkehrsnetz generiert. Allerdings hängt die Höhe des Signalisierungsverkehrs von der Anzahl der abgefragten optischen Komponenten ab.

Die zweite Methode hängt von dem aktuellen Degradationszustand der optischen Komponenten ab. Zu Beginn der Lebensdauer eine Komponente werden die Degradationswerte seltener abgefragt als gegen Ende der Lebensdauer. Mit dieser Strategie wird berücksichtigt, dass gegen Ende der Lebensdauer der Austausch der optischen Komponente wahrscheinlicher und ein häufigeres Senden notwendig wird.

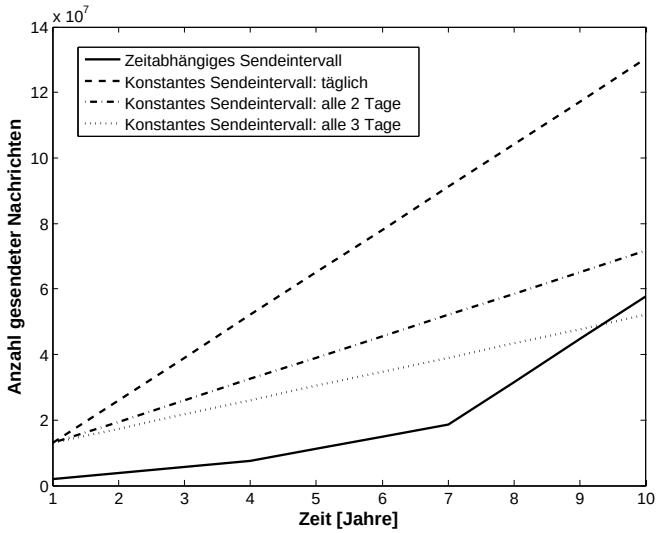


Abbildung 5.2: Anzahl der gesendeten Degradationsnachrichten

In Abbildung 5.2 sind die Anzahl der gesendeten Degradationsnachrichten für die zwei unterschiedlichen Methoden dargestellt. Als Grundlage wurde das Deutschland-

50-Knoten-Referenznetz verwendet, welches aus 88 Kanten besteht. Zur Berechnung der Anzahl der gesendeten Degradationsnachrichten werden Laser, optische Empfänger und optische Verstärker betrachtet. Es werden zwei Laser und zwei Empfänger pro Kante und Wellenlänge angenommen. Auf jeder Kante können 100 Wellenlängen gleichzeitig gesendet werden. Hinzu kommen noch 481 optische Verstärker. Die gestrichelten beziehungsweise gepunkteten Linien zeigen die Anzahl der Nachrichten für ein konstantes Sendeintervall. Der Vorteil des degradationsabhängigen Sendens von Nachrichten macht sich besonders in den ersten Jahren bemerkbar. Im Vergleich zu einem konstanten Sendeintervall werden innerhalb der ersten fünf Jahre zwischen 63,30 % und 82,86 % weniger Degradationsnachrichten gesendet. Auch über einen Lebenszyklus von 10 Jahren werden bei dem degradationsabhängigen Senden 19,48 % beziehungsweise 55,71 % weniger Nachrichten gesendet. Vergrößert man das Sendeintervall beim konstanten Senden allerdings auf drei Tage, werden nach 10 Jahren weniger Nachrichten gesendet. Das degradationsabhängige Senden entspricht eher dem Degradationsverhalten der optischen Komponenten. Wenn sich eine Komponente ihrem Degradationsschwellenwert nähert, sendet diese häufiger Degradationsnachrichten an das Netzmanagement, das damit einen genaueren Verlauf der Degradation erhält.

Zusätzlich zu den regelmäßig gesendeten Degradationswerten, um beispielsweise einen Degradationsverlauf analysieren zu können, wird noch eine Alarmnachricht gesendet, sobald eine Komponente ihren Degradationsschwellenwert erreicht hat. Der Degradationsschwellenwert wird von einem Netzbetreiber festgelegt und definiert die obere Grenze bei deren Erreichen die Netzkomponente auf den Status „Austauschen“ gesetzt wird. Dieses Ereignis wird unabhängig von den anderen Degradationsnachrichten gesendet. Die Limitierung der Degradationsnachrichten auf die Alarmnachricht beim Erreichen des Schwellenwerts ist ebenfalls eine Möglichkeit, allerdings fehlen dem Netzbetreiber dann Informationen über den aktuellen Degradationszustand der restlichen optischen Komponenten. Dies wird genauer in Abschnitt 5.3 diskutiert, in dem verschiedene Austauschstrategien analysiert werden.

5.2.3 Planung der Wartungsphase

Der Grundgedanke bei der Erfassung der Degradationswerte in einem Netzmanagementsystem besteht darin, die Komponenten auszutauschen, bevor sie ausfallen. Dadurch ergeben sich zwei entscheidende Vorteile für einen Netzbetreiber. Zum einen können Verkehrsanforderungen neu geroutet werden, bevor der Link deaktiviert wird. Damit werden Ausfälle von Diensten vermieden. Der zweite Vorteil besteht darin, dass die Wartungsphase eines Weitverkehrsnetzes besser planbar ist. Der Netzbetreiber kann somit Konfigurationen am Weitverkehrsnetz beziehungsweise den Austausch von Hardwarekomponenten im Voraus besser planen, wenn die Degradation von Komponenten berücksichtigt wird. Auf diese Weise kann der Netzbetreiber den Austausch von Netzkomponenten und eine Neukonfiguration von Protokollen in einem Schritt vornehmen. Wie später in Abschnitt 5.3 gezeigt, ist es

möglich, mehrere degradierte Komponenten in einer Arbeitsschicht auszutauschen. Dadurch ergibt sich eine Zeitersparnis beim Reparaturprozess, die sich wiederum auf die Betriebskosten eines Netzes auswirkt. Ebenso kann der Netzbetreiber die Ersatzteile in den Lagern reduzieren, da die Anzahl der spontanen Ausfälle reduziert wird und der Netzbetreiber, sobald eine Komponente degradiert ist, noch genügend Zeit hat, eine Ersatzkomponente zu ordern.

5.3 Austauschstrategien anhand optischer Verstärker

Dieser Abschnitt beschreibt die Degradation des Pumplasers eines EDFAs und die Dimensionierung des Pumpstromschwellenwerts, ab dem eine Warnnachricht an das Managementsystem gesendet wird. Wie bereits beschrieben, muss der Pumpstrom eines EDFAs abhängig von den Alterungseffekten der Komponenten erhöht werden, um die gleiche Verstärkung zu erzielen. Dabei folgt die Anhebung des Pumpstroms keinem linearen Verlauf sondern einem exponentiellen Verlauf wie in Abbildung 5.3 gezeigt.

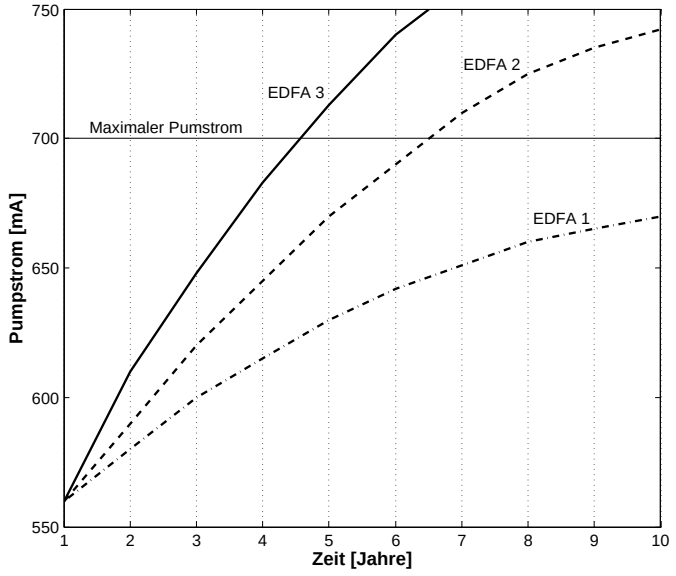


Abbildung 5.3: Verschiedene Degradationskurven für EDFAs

In der Abbildung sind mehrere Kurven dargestellt, da verschiedene EDFAs unterschiedliche Degradationsverläufe besitzen, die unterschiedlich schnell verlaufen. Das bedeutet, dass bestimmte EDFAs früher den vorgegebenen Schwellenwert erreichen und eine Warnnachricht an das Managementsystem senden. Zu Beginn der Lebensdauer ist der Kurvenverlauf steiler, was einer stärkeren Erhöhung des Pumpstroms entspricht, als gegen Ende der Lebenszeit, an der der Pumpstrom in kleineren Stufen erhöht werden muss. Der Anfangswert des Pumpstroms wurde aus einem Datenblatt eines Herstellers entnommen und gibt den benötigten Pumpstrom für den optischen

Verstärker an. Dieser liegt bei $550\,mA$ und wird für alle Betrachtungen in diesem Kapitel verwendet. In Abbildung 5.3 ist ebenfalls der maximale Pumpstrom eingezeichnet, der bei $700\,mA$ liegt. Oberhalb des maximalen Pumpstroms nimmt die Verstärkung eines EDFAs ab, da der Pumpstrom auf den genannten Bereich ausgelegt wurde und nicht weiter erhöht werden kann. Erreicht ein EDFA den oberen Schwellwert, schickt er eine Warnnachricht an das Netzmanagementsystem.

Mit der Methode in [Rap05] ist es möglich den aktuell benötigen Pumpstrom zu bestimmen, der für die richtige Verstärkung des Signals erforderlich ist. Die Bestimmung des Pumpstroms erfolgt direkt am Verstärker, so dass dieser mittels geeigneter Protokolle die aktuellen Werte an ein Netzmanagementsystem senden kann. Mithilfe des aktuell bestimmten Messwerts überprüft das Netzmanagement, ob der EDFA noch in einem gültigen Arbeitsbereich des Pumpstroms arbeitet. Um einen Verstärker auszutauschen bevor er ausfällt, definiert der Hersteller oder der Netzbetreiber einen Schwellenwert, ab dem ein Verstärker eine Warnnachricht an das Netzmanagement sendet. Die Wahl des Schwellenwerts hängt davon ab, wie lange die Restlaufzeit eines Verstärkers sein soll. Die Restlaufzeit errechnet sich aus der Differenz zwischen dem maximalen Pumpstrom und dem aktuellen Pumpstromwert und gibt an, wie lange der EDFA noch fehlerfrei funktioniert. Die Restlaufzeit eines EDFAs definiert auch, wie lange ein Netzbetreiber auf weitere degradierte EDFAs warten kann, bis diese ebenfalls ihren Degradationsschwellenwert erreicht haben und eine Warnnachricht senden. Der Vorteil eines niedrigeren Schwellenwerts besteht in der größeren Restlaufzeit eines EDFAs. Eine längere Restlaufzeit ermöglicht die effizientere Planung der Wartungsphase. Der Verkehr kann bereits im Voraus von dem betroffenen Link umgeroutet werden, wodurch der Ausfall von Diensten verhindert wird.

Die Planung des Reparaturprozesses erhöht die Verfügbarkeit des Netzes, da der Verkehr vor dem Ausfall einer Komponente oder eines Links umgeroutet wird. Ein weiterer wichtiger Punkt für einen Netzbetreiber sind die Betriebskosten des Netzes. Melden die Netzkomponenten ihren aktuellen Status an ein Netzmanagementsystem, muss ein Netzbetreiber die Ersatzkomponenten nicht mehr lagern, sondern kann diese nach dem Empfang einer Warnnachricht bestellen. Auch der Reparaturprozess der Netzkomponenten kann optimiert werden, wenn vorher bekannt ist, welche Komponenten ausgetauscht werden. In den folgenden Untersuchungen werden die beschriebenen Vorteile analysiert. Zunächst wird ein einzelner Link mit optischen Verstärkern betrachtet. Anschließend wird das Degradationsmodell anhand eines Referenznetzes analysiert.

Für die Simulationen wird ein EDFA-Abstand von 80 km angenommen. Für die Degradation der EDFAs werden die Kurven aus Abbildung 5.3 verwendet. Jedem EDFA wird zu Beginn der Simulation zufällig eine dieser Kurven zugeordnet. Wenn ein EDFA ausgetauscht wird, erfolgt eine zufällige Neuzuweisung einer Degradationskurve.

5.3.1 Betrachtung eines beispielhaften Links

Zunächst wird ein Link mit einer Länge von 1000 km betrachtet, wie er in einem europäischen oder amerikanischen Weitverkehrsnetz häufig vorkommt. Auf dem Link befinden sich 12 EDFAs. Die Glasfaser hat ebenfalls eine Ausfallwahrscheinlichkeit von $380\,FIT/km$. Ein FIT bedeutet dabei ein Fehler pro $10^9\,h$. Die mittlere Zeit zwischen zwei Fehlern beträgt somit für die Glasfaser $380/10^9\,h$. Für den Austausch der EDFAs werden zwei Reparaturteams angenommen, die beide dem *Netzbetriebszentrum* (NOC) in der Mitte des Links zugeordnet sind. Jedes Reparaturteam ist für eine Hälfte des Links zuständig. Das NOC ist in der Mitte des Links platziert, da ansonsten die Fahrzeit zwischen NOC und einem ausgefallenen EDFA die Arbeitszeit der Techniker pro Schicht überschreitet. Für das Reparaturteam wird eine Arbeitszeit von acht Stunden angenommen, innerhalb derer sowohl die Fahrzeiten als auch die Reparaturzeiten der EDFAs liegen müssen. Der Austausch eines EDFAs dauert inklusive der Aktivierung des Links zwei Stunden. Die Ersatzteile befinden sich ebenfalls an dem NOC und werden als vorrätig angenommen.

Die Betriebskosten werden bei der Untersuchung des Links noch nicht betrachtet. Dies erfolgt erst im nächsten Abschnitt, in dem das Degradationskonzepts anhand eines Referenznetzes untersucht wird. Die Betriebskosten sind ein wichtiger Faktor für einen Netzbetreiber und setzen sich aus den Kosten der EDFAs, der Reparatur und den Strafzahlungen des Netzbetreibers an einen Kunden zusammen. Strafzahlungen treten auf, wenn die Dienstgüte eines Dienstes von Seiten des Netzbetreibers nicht eingehalten wird. Im Folgenden werden zunächst zwei unterschiedliche Austauschstrategien der EDFAs auf dem beispielhaften Link analysiert.

Austausch der degradierten EDFAs

Im ersten Szenario werden nur die EDFAs auf dem Link ausgetauscht, die den Degradationsschwellenwert erreicht haben. Der Austausch erfolgt nicht sofort, wenn die Warnnachricht am NOC empfangen wird, sondern jeweils am Ende eines Jahres oder falls eine Glasfaser ausfällt. Abhängig von der Wahl des Schwellenwerts berechnet sich die theoretische Restlaufzeit des EDFAs, die in diesem Beispiel größer als ein Jahr gewählt wurde. Für die Simulationen wird ein Zeitraum von 30 Jahren betrachtet, wobei die ersten zwei Jahre nicht in der Statistik berücksichtigt werden, um eventuelle Einschwingeffekte zu vermeiden. In Abbildung 5.4 ist die Anzahl der EDFA-Ausfälle innerhalb von 30 Jahren für drei verschiedene Schwellenwerte aufgetragen.

Bei einem Pumpstromschwellenwert von 600 mA müssen im Mittel 67 EDFAs ausgetauscht werden. Wie zu erwarten, nimmt die Anzahl der ausgewechselten EDFAs mit steigendem Schwellenwert ab. Der Austausch der 67 EDFAs führt zu 25 Linkausfällen. Allerdings stellen die Linkausfälle keine unvorhergesehenen Ausfälle dar, sondern werden von dem Netzbetreiber bewusst durchgeführt, um die degradierten EDFAs auszutauschen. Der Verkehr auf dem Link wird vor dem Austausch umgeroutet und verhindert damit den Ausfall der gerouteten Dienste.

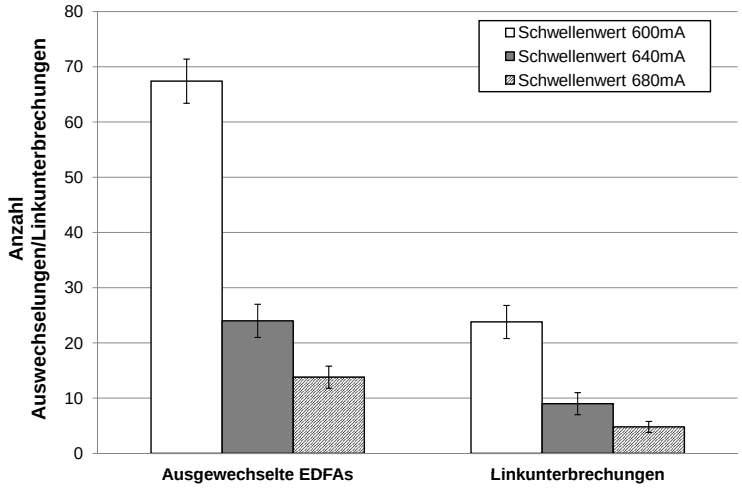


Abbildung 5.4: Szenario 1: Anzahl der ausgewechselten EDFAs und Anzahl der Linkausfälle

Austausch aller EDFAs

Im zweiten Szenario werden am Ende des Jahres alle EDFAs auf dem Link ausgetauscht, sobald mindestens ein EDFA eine Warnnachricht sendet. Diese Strategie berücksichtigt, dass unabhängig von der Anzahl der auszuwechselnden EDFAs, der Link deaktiviert werden muss. In Abbildung 5.5 sind wiederum die Anzahl der ausgetauschten EDFAs in 30 Jahren für drei verschiedene Schwellenwerte aufgetragen.

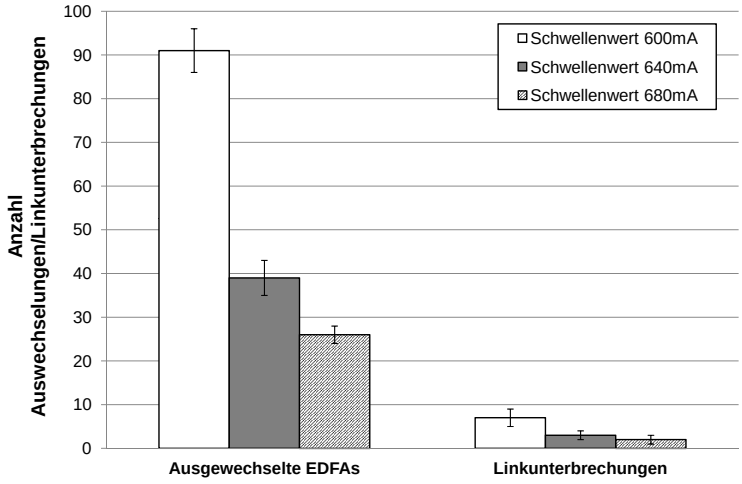


Abbildung 5.5: Szenario 2: Anzahl der ausgewechselten EDFAs und Anzahl der Linkausfälle

Im Vergleich zum ersten Simulationsszenario steigt die Anzahl der ausgetauschten EDFAs für alle drei Schwellenwerte an. Für einen Schwellenwert von 600 mA steigt

die Anzahl der ausgewechselten EDFAs um 25 %. Bei einem Schwellenwert von 680 mA werden im Vergleich zum vorherigen Szenario beinahe doppelt so viele EDFAs getauscht. Der Vorteil des zweiten Szenarios zeigt sich bei der Betrachtung der Anzahl der Linkunterbrechungen. Die 92 ausgewechselten EDFAs führen zu sieben Linkunterbrechungen und damit zu einer Reduktion der Unterbrechungen um 70,83 %. Die Anzahl der Linkunterbrechungen für beide Szenarien ist in Abbildung 5.6 dargestellt.

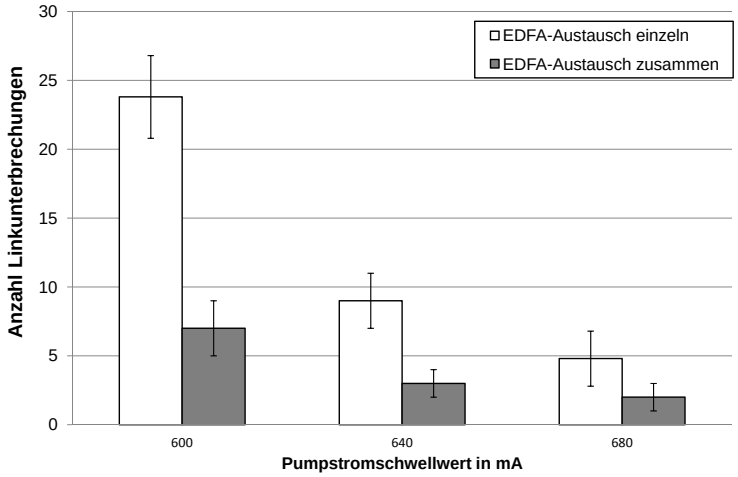


Abbildung 5.6: Anzahl der Linkunterbrechungen für beide Szenarien

Für die beiden anderen Schwellenwerte ergeben sich ähnliche Ergebnisse. Die maximale Reduktion für die simulierten Szenarien beträgt 72 %. Die geringere Anzahl an Linkunterbrechungen erhöht die Verfügbarkeit des Links, wenn ein Weitverkehrsnetz über ausreichend Netzkapazität verfügt und der Netzbetreiber vor der Deaktivierung des Links die Verkehrsanforderungen auf Alternativwege umleiten kann. In diesem Fall lohnt sich die zweite Strategie nicht, da die Anzahl der Linkunterbrechungen keine Auswirkung auf die Dienste hat und nur zu höheren Kosten führt. Ein anderes Szenario ergibt sich, wenn nicht genügend Restkapazität im Netz vorhanden ist und der Netzbetreiber nicht den gesamten Verkehr umrouten kann. Die Anzahl der Linkunterbrechungen wirken sich in diesem Fall negativ auf die Verfügbarkeit des Netzes aus, weshalb eine Reduzierung der Linkunterbrechungen notwendig ist.

Allerdings sind die Anzahl der Linkunterbrechungen nicht das einzige Kriterium für die Dienstgüte eines Weitverkehrsnetzes. Eine weitere Vergleichsgröße stellt die Reparaturzeit des Links dar, die angibt, wie lange der Link deaktiviert ist. Da im zweiten Szenario alle EDFAs auf dem Link getauscht werden, erhöht sich auch die Austauschzeit und somit die Ausfallzeit des Links. Deshalb wird im Folgenden die Reparaturzeit für die zwei unterschiedlichen Szenarien berechnet.

$$t_{reparatur} = max(t_{reparaturTeam1}, t_{reparaturTeam2}) + t_{EDFA_X - EDFA_Y} \tag{5.1}$$

Die Reparaturzeit entspricht der Austauschzeit der EDFAs plus der Fahrzeit zwischen den EDFAs. Die Fahrzeit zum ersten EDFA kann vernachlässigt werden, da der Link erst deaktiviert wird, wenn das Reparaturteam diesen erreicht. Der Austausch eines EDFAs dauert wie bereits erwähnt zwei Stunden. Die Fahrzeit zwischen zwei EDFAs $t_{EDFA_X - EDFA_Y}$ berechnet sich abhängig von der Entfernung zwischen den EDFAs.

Im ersten Simulationsszenario, bei dem nur die degradierten EDFAs ausgetauscht werden, beträgt die mittlere Entfernung 200 km. Die mittlere Entfernung berechnet sich aus der Summe der Abstände zwischen den jährlich auszutauschenden EDFAs, geteilt durch die Anzahl der Wegstrecken. Somit ergibt sich in 30 Jahren eine gesamte Reparaturzeit von 171,42 h. Im zweiten Simulationsszenario, bei dem alle EDFAs getauscht wurden, ist die Entfernung konstant und beträgt 420 km pro Reparaturteam. Die Entfernung ergibt sich aus den Abständen zwischen den EDFAs auf einer Hälfte des Links. In diesem Fall ergibt sich eine Reparaturzeit von 126 h. Ein Vergleich der Reparaturzeiten zeigt, dass diese ihm zweiten Szenario um 26,5 % niedriger sind. Das gleiche gilt für die Ausfallzeit des Links, die der Reparaturzeit entspricht.

Die Ergebnisse zeigen, dass der gleichzeitige Austausch aller EDFAs die Ausfallzeit des Links verringert und damit die Verfügbarkeit erhöht. Um eine Aussage treffen zu können, welche der beiden Austauschstrategien zu einer höheren Verfügbarkeit des Weitverkehrsnetzes führt, muss ein Referenznetz mit einer größeren Anzahl an Links betrachtet werden. Wie bereits beschrieben hängt es allerdings auch von der gesamten Netzkapazität ab, ob die höhere Verfügbarkeit eines einzelnen Links eine positive Auswirkung auf das gesamte Netz hat.

Neben den Reparaturzeiten spielen auch die Betriebskosten des Netzes eine entscheidende Rolle. Die höhere Anzahl an ausgewechselten EDFAs führt zu höheren Kosten bei der Beschaffung der EDFAs. Allerdings reduziert sich die Reparaturzeit und damit die Reparaturkosten. Daneben existieren noch die zeitabhängigen Strafzahlungen an den Kunden für einen Dienstausfall. Eine ausführliche Analyse der Betriebskosten erfolgt in Abschnitt 5.3.2 anhand eines Referenznetzes.

Vergleich des Degradationsmodells mit einem FIT-Ratenmodell

Um die Ergebnisse aus dem vorherigen Abschnitt zu vergleichen, wird das Degradationsmodell mit einem FIT-Ratenmodell verglichen. Beim FIT-Ratenmodell erfolgen die EDFA-Ausfälle unvorhergesehen. Obwohl beim Degradationsmodell die aktuellen Degradationswerte der EDFAs abgefragt werden, kann ein unvorhergesehener Ausfall nicht ausgeschlossen werden. Deshalb werden bei der Verwendung des Degradationsmodells auch spontane Ausfälle der EDFAs zugelassen, um deren Einfluss auf die Verfügbarkeit des Links zu ermitteln.

Wie bereits erwähnt beruht das FIT-Ratenmodell auf der Annahme, dass die optischen Verstärker eine bestimmte Fehlerrate besitzen. Für die folgenden Simulationen wird eine FIT-Rate von 4000 verwendet. In Abbildung 5.7 sind das FIT-Ratenmodell, das Degradationsmodell ohne spontane Ausfälle und das Degradationsmodell mit

spontanen Ausfällen der EDFAs dargestellt. Die spontane Ausfallwahrscheinlichkeit eines EDFAs beträgt ein Prozent.

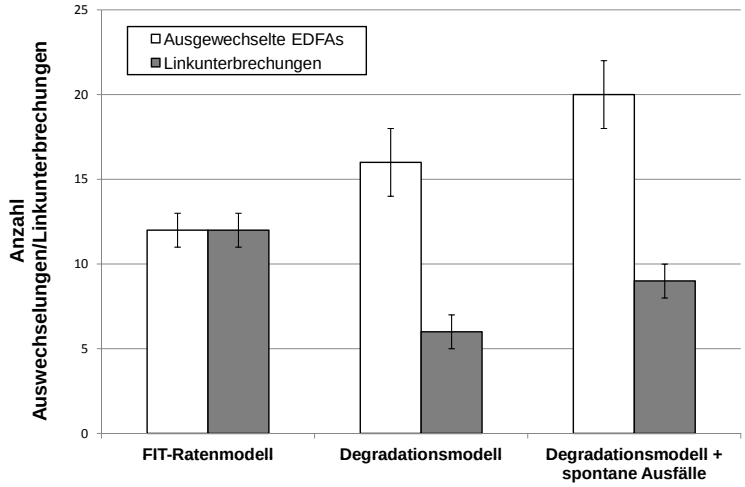


Abbildung 5.7: Anzahl der EDFA-Ausfälle und Linkunterbrechungen

Das Diagramm zeigt, dass die Anzahl der ausgewechselten EDFAs bei beiden Degradationsmodellen höher ist als für das FIT-Ratenmodell. Dies ist auf den vorzeitigen Austausch der EDFAs zurückzuführen, der im Mittel zu einer geringeren Lebensdauer der EDFAs im Vergleich zum FIT-Ratenmodell führt. Erweitert man das Degradationsmodell auch um unvorhergesehene EDFA-Ausfälle, steigt die Anzahl der ausgewechselten EDFAs gegenüber dem normalen Degradationsmodell um durchschnittlich drei EDFAs an.

Der entscheidende Vorteil des Degradationsmodells zeigt sich beim Vergleich der Linkunterbrechungen. Beim FIT-Ratenmodell entspricht jeder Ausfall eines EDFAs einer Linkunterbrechung. Beim Degradationsmodell ermöglicht die Restlaufzeit eines EDFAs allerdings, dass der Austausch nicht sofort durchgeführt werden muss, sondern der Netzbetreiber auf weitere degradierte EDFAs warten kann. Die Anzahl der Linkunterbrechungen ist daher beim Degradationsmodell ohne spontane Ausfälle um 41,67 % geringer als bei dem FIT-Ratenmodell. Auch bei der Betrachtung von spontanen Ausfällen ist Anzahl der Linkunterbrechungen beim Degradationsmodell um 25 % geringer.

Der Austausch aller EDFAs auf einem Link, sobald mindestens ein EDFA degradiert ist, führt auch beim Vorhandensein von spontanen Ausfällen, zu weniger Linkunterbrechungen als das FIT-Ratenmodell. Die Anzahl der Linkunterbrechungen entspricht ungefähr der Anzahl beim Degradationsmodell, bei dem nur die degradierten EDFAs ausgetauscht werden. Allerdings steigt wiederum die Anzahl der ausgetauschten EDFAs an.

Wie anhand der Ergebnisse gezeigt, steigt die Anzahl der ausgewechselten EDFAs im Vergleich zum FIT-Ratenmodell an. Deshalb erfolgt im nächsten Abschnitt bei

der Betrachtung eines Referenznetzes auch die Untersuchung der Betriebskosten des Degradationsmodells.

5.3.2 Deutschland-50-Knotennetz

In diesem Abschnitt erfolgt die Untersuchung des Degradationsmodells anhand eines Referenznetzes. Die Analysen sollen einen Aufschluss darüber geben, ob die Überwachung der Degradationsparameter aller optischer Netzkomponenten die Verfügbarkeit des Netzes erhöht und die Reparaturzeit reduziert. Die Ergebnisse des FIT-Ratenmodells dienen dabei als Referenz für die Ergebnisse des Degradationsmodells.

Als Beispielnetz wird das Deutschland-50-Knotenmodell [SND11] verwendet, welches aus 50 Knoten und 88 Kanten besteht und eine mittlere Linklänge von 131 km besitzt. Die gesamte Linklänge umfasst 8874,13 km und es werden 241 EDFAs verwendet. Entscheidend für die Reparaturdauer in einem Weitverkehrsnetz ist die Anzahl der NOCs, an denen sich sowohl die Techniker als auch die Ersatzkomponenten befinden. Zunächst wird die minimale Anzahl von zwei NOCs verwendet, die sich an den Knoten Hannover und Würzburg befinden. Jeder Standort deckt somit eine Hälfte des Beispielnetzes ab, für die eines der Reparaturteams verantwortlich ist. Damit in dem Beispielnetz mehr als zwei EDFAs gleichzeitig in einer Arbeitsschicht repariert werden können, müssen mindestens zwei NOCs vorhanden sein. Der limitierende Faktor für die Reparatur von mehreren EDFAs in einer Arbeitsschicht stellt die Fahrzeit zwischen NOC und EDFA dar. Mit steigender Anzahl von NOCs verringert sich sowohl die Entfernung als auch die Fahrzeit des Reparaturteams.

In dem FIT-Ratenmodell wird für die EDFAs wiederum eine FIT-Rate von 4000 verwendet [MSSW05]. Für beide Modelle wird für einen EDFA eine Reparaturzeit von 2 h angenommen [VCP+06] und zur Reparatur eines EDFAs wird ein Techniker benötigt.

FIT-Ratenmodell

Die Fehlerwahrscheinlichkeit eines EDFAs im Zeitintervall t wird mit Formel 5.2 berechnet.

$$P(T_{out} \leq t) = 1 - \exp(-\lambda_{FIT} \times t) \tag{5.2}$$

Die Wahrscheinlichkeit, dass genau ein EDFA innerhalb eines Jahres ausfällt, beträgt 2,47 % und die Wahrscheinlichkeit, dass mindestens ein EDFA innerhalb eines Jahres ausfällt, liegt bei 99,76 %. Die angenommenen Fehlerwahrscheinlichkeiten führen im Mittel zu 5,77 ausgewechselten EDFAs pro Jahr. Die Reparaturzeit für die ausgefallenen optischen Verstärkern berechnet sich mit Formel 5.3 und beträgt 6,69 h pro EDFA.

$$\bar{t}_{Repair} = \frac{\sum_{k=1}^{N}(t_{NOC-EDFA_k} + t_{repair})}{N} \tag{5.3}$$

N bezeichnet die Anzahl der ausgefallenen EDFAs, $t_{NOC-EDFA_k}$ ist die einfache Fahrzeit zwischen NOC und $EDFA_k$ und t_{repair} ist die Reparatur- und Testzeit pro EDFA. Für das FIT-Ratenmodell muss zusätzlich die Fahrzeit von einem NOC zu dem ausgefallen EDFA berücksichtigt werden, da das Routing über den Link ab dem Ausfall unterbrochen ist. Bei dem Degradationsmodell wird der Link erst deaktiviert, wenn das Team beim entsprechenden EDFA angekommen ist. Die gesamte Reparaturzeit beim FIT-Ratenmodell über eine Simulationszeit von 100 Jahren beträgt 3857,97 h.

Degradationsmodell

Zum Vergleich wird in diesem Abschnitt das Degradationsmodell untersucht. Der Vorteil des Modells besteht in der Planbarkeit der Wartungsphasen. Durch das Signalisieren der Degradationswerte weiß der Netzbetreiber, dass ein EDFA auswechselt werden muss. Aufgrund der Restlaufzeit eines degradierten EDFAs kann der Netzbetreiber mit dem Austausch noch eine bestimmte Zeit warten, um auf weitere Warnnachrichten von anderen degradierten EDFAs zu warten. Der Netzbetreiber hat dadurch den Vorteil, dass er durch die Planung des Reparaturprozesses mehrere EDFAs während der Arbeitsschicht eines Technikers reparieren lassen kann. Damit reduziert sich die Fahrzeit des Technikers. Ein Beispiel für den eben beschriebenen Vorteil zeigt Abbildung 5.8, in der zwei unterschiedliche Reparaturszenarien dargestellt sind.

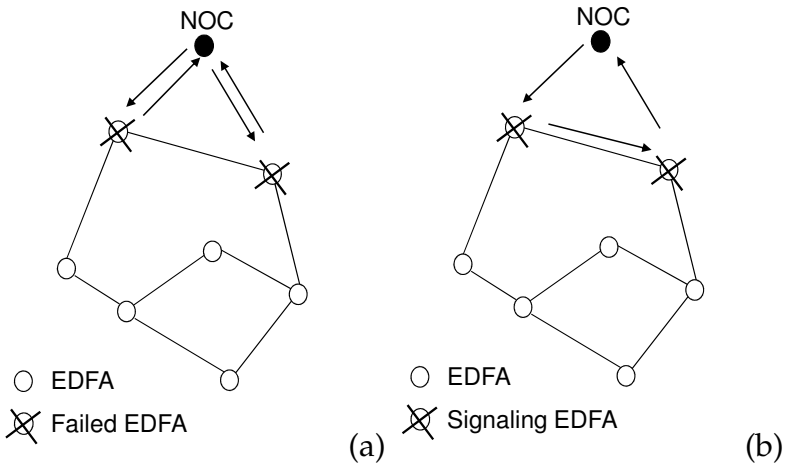


Abbildung 5.8: (a) EDFAs unabhängig repariert (b) EDFAs zusammen ausgewechselt

In Abbildung 5.8 (a) werden zwei EDFAs unabhängig voneinander repariert, wie es zum Beispiel beim FIT-Ratenmodell der Fall ist. Das Reparaturteam muss deshalb

bei jeder Reparatur von dem NOC zu dem betroffenen EDFA und wieder zurück fahren. In Abbildung 5.8 (b) wurde der Reparaturprozess im Voraus geplant und die zwei degradierten EDFAs können in einer Arbeitsschicht ausgetauscht werden. Mit der Reparatur in einer Arbeitsschicht ist gemeint, dass die Techniker von dem ersten auszutauschenden EDFA nicht zurück zum NOC fahren, sondern zu dem nächsten degradierten EDFA, um diesen ebenfalls zu wechseln. Das Ziel ist es, Fahrzeiten zu reduzieren, indem in einer Arbeitsschicht mehrere EDFAs ausgewechselt werden, ohne zum NOC zu fahren. Damit sich die Reparatur von mehreren EDFAs in einer Arbeitsschicht rentiert, muss die Fahrzeit kleiner sein, als die einzelnen Fahrten zwischen EDFAs und NOC. Die Reparaturzeit der EDFAs ist in beiden Szenarien gleich und kann daher vernachlässigt werden. Die Fahrzeit des Reparaturprozesses berechnet sich mit Formel 5.4.

$$t_{travel} = t_{NOC-EDFA_x} + x \times t_{EDFA_x-EDFA_y} + t_{EDFA_y-NOC} \tag{5.4}$$

Die gesamte Fahrzeit setzt sich aus der Fahrzeit zwischen NOC und den ersten angefahrenen EDFA, der Fahrzeit zwischen den EDFAs sowie der Fahrzeit zwischen dem letzten EDFA und NOC zusammen.

Mit den Degradationskurven aus Abbildung 5.3 ergeben sich für das Deutschland-50-Knotennetz im Mittel 7,2 ausgewechselte EDFAs pro Jahr. In 42 % der Fälle werden zwei EDFAs gleichzeitig in einer Arbeitsschicht repariert. In den übrigen Fällen wird nur ein EDFA pro Arbeitsschicht repariert, da die Distanz zwischen den EDFAs zu groß ist. Aufgrund der Verwendung von zwei NOCs beträgt die Entfernung zwischen NOC und EDFAs bis zu 400 km. Daher wird durch die Fahrzeit zwischen NOC und EDFA bereits die Hälfte der Arbeitszeit einer Arbeitsschicht verbraucht, weshalb nur ein EDFA ausgetauscht werden kann. Die Ergebnisse der Untersuchungen für das FIT-Ratenmodell und das Degradationsmodell sind in Tabelle 5.1 zusammengefasst.

Parameter	FIT-Ratenmodell	Degradationsmodell	Unterschied
Verwendete NOCs	2	2	-
Ausfallwahrscheinlichkeit	4000	Degradationskurven	-
Ausgewechselte EDFAs pro Jahr	5,77	7,2	+24,78 %
Mittlere Arbeitszeit pro EDFA	6,69 h	6,85 h	+2,39 %
Gesamte Fahrzeit	2703,97 h	3036,43 h	+12,30 %
Gesamte Reparaturzeit	3857.97 h	1440 h	-62,67 %
Gesamtkosten pro Jahr	70956 $	86425 $	+21,80 %

Tabelle 5.1: Zusammenfassung der Ergebnisse für das Deutschland-50-Knotennetz

Aus der Tabelle wird ersichtlich, dass bei dem Degradationsmodell die Anzahl der

durchschnittlich getauschten EDFAs höher ist, als für das FIT-Ratenmodell. Wie bereits bei der Betrachtung eines Links, ergibt sich die Differenz aus dem vorzeitigen Austausch der EDFAs. Der vorzeitige Austausch führt zu einer kürzeren Lebensdauer der optischen Verstärker. Die theoretische Restlaufzeit bei einem Schwellenwert von 680 mA liegt im Mittel zwischen ein und zwei Jahren, um genügend Zeit für die Planung der Wartungsphase zu haben.

Der Vorteil des Degradationsmodells wird beim Vergleich der Reparaturzeiten deutlich. Das Degradationsmodell besitzt eine um 62 % geringere Reparaturzeit als das FIT-Ratenmodell, wofür zwei Gründe verantwortlich sind. Die größte Einsparung der Reparaturzeit beruht darauf, dass bei dem Degradationsmodell die Fahrzeit zu einem EDFA nicht als Ausfallzeit gilt, da der EDFA noch funktionstüchtig ist. Der zweite Beitrag ergibt sich aufgrund des Austauschs von mehreren EDFAs in derselben Arbeitsschicht, was wiederum Fahrzeit im Vergleich zum FIT-Ratenmodell einspart. Die Reparaturzeit stellt beim Degradationsmodell gleichzeitig die Ausfallzeit eines Links dar und wird somit ebenfalls um 62 % reduziert. Durch den vermehrten Austausch der EDFAs steigt allerdings auch die Anzahl der Fahrten und damit die Fahrzeiten der Techniker. Allerdings tragen diese Fahrten, wie bereits erwähnt, nicht zu den Ausfallzeiten bei. Die Fahrzeiten lagen bedingt durch die Reparatur von mehreren EDFAs in einer Arbeitsschicht um 11 % niedriger als wenn die EDFAs unabhängig getauscht werden.

Analyse der Betriebskosten beider Simulationsszenarien

Neben der Reparaturdauer sind allerdings auch die Kosten des Reparaturprozesses eine relevante Größe für den Netzbetreiber. Die Kostenunterschiede in den untersuchten Szenarien beruhen hauptsächlich auf der Dauer der Reparaturzeit, der Anzahl der ausgewechselten EDFAs und der Anzahl der EDFAs, die in einem Lager vorrätig sind.

$$c_{Repair} = (c_{Salary} \times t_{repair}) + c_{EDFA} + c_{stock} \tag{5.5}$$

$$C_{Stock} = 0.05 \times P_{EDFA} \times N_{EDFA} \tag{5.6}$$

Die Kosten für den Reparaturprozess werden durch die Kosten der Techniker, die Kosten der EDFA und die Kosten für das Lager beschrieben. Weitere Kosten wie Benzin und Wartung der Fahrzeuge werden hier nicht berücksichtigt. Das Gehalt für einen Techniker wird mit 36,19 $ pro Stunde angenommen [Pay11]. Die Kosten für eine EDFA betragen 11850 $ [VCP+06]. Für die Kosten des Lagers werden 5 % der Equipmentkosten veranschlagt und diese berechnen sich aus der Anzahl der EDFAs und ihrer Ausfallwahrscheinlichkeit pro Jahr. Für das FIT-Ratenmodell ergibt sich bei einer Anzahl von 557 ausgetauschten EDFAs und Gesamtkosten für den Reparaturprozess von 70956 $ pro Jahr.

Um die Kosten für das Degradationsmodell zu berechnen werden dieselben Formeln verwendet. Es wird angenommen, dass sich nur ein EDFA im Lager befindet, da der

Netzbetreiber nach dem Empfang einer Warnnachricht ausreichend Zeit hat, einen neuen EDFA zu bestellen. Ein EDFA wird lediglich für einen spontanen Ausfall vorgehalten. Somit ergeben sich für das Degradationsmodell Gesamtkosten von 86425 $ pro Jahr.

Wie die Ergebnisse zeigen, fallen die Kosten für das Degradationsmodell höher aus. Dies liegt hauptsächlich an der höheren Anzahl an ausgewechselten EDFAs, die ebenfalls zu einer längeren Fahrzeit führt. Demgegenüber stehen aber eine Verringerung der Ausfallzeit der einzelnen Links und eine um 62 % höhere Gesamtverfügbarkeit des Netzes. Für eine genauere Aussage über die Kosten beider Modelle müssen auch die Strafzahlungen aufgrund der Verletzung der Dienstgüte betrachtet werden. Entscheidend für die Höhe der Strafzahlungen ist die Ausfalldauer eines Dienstes. Da die Reparaturzeit beim FIT-Ratenmodell wesentlich höher als beim Degradationsmodell ist, werden auch die Strafzahlungen höher liegen. Eine Betrachtung der Strafzahlungen erfolgt im nächsten Abschnitt, in dem das Degradationskonzept um zusätzliche optische Komponenten erweitert wird und zusätzlich der Einfluss von mehr als zwei NOCs auf die Reparatur- und Ausfallzeiten betrachtet wird.

5.4 Allgemeines Fehlermodell für optische Netzkomponenten

Die Analysen in Abschnitt 5.3 haben gezeigt, dass ein proaktives Fehlermodell die Verfügbarkeit des Weitverkehrsnetzes erhöht. In diesem Abschnitt wird das Modell auf weitere optische Netzkomponenten ausgeweitet, die sich ebenfalls zur Beschreibung mittels eines Degradationsmodells eignen. Ähnlich wie der Pumplaser eines EDFAs verhalten sich auch die Sendelaser und Empfangsdioden in den Knoten eines Weitverkehrsnetzes. Es wird angenommen, dass die Anzahl der Transponder sowie die Anzahl der Empfänger an einem Knoten der Anzahl der Links pro Knoten entspricht. Dementsprechend werden an einem Knoten ein Laser und ein Empfänger pro Link benötigt. Für das bereits verwendete Beispielnetz ergeben sich insgesamt 352 Laser und Empfänger, welche dieselben Degradationskurven wie in Abbildung 5.3 besitzen. Es wird wiederum ein Schwellenwert von 680 mA angenommen. Die Ergebnisse sind in Tabelle 5.2 dargestellt.

Ähnlich wie für die EDFAs ergibt sich für die Betrachtung aller optischen Komponenten eine höhere Anzahl an getauschten Komponenten aufgrund des vorzeitigen Austauschs. Bei dem Degradationsmodell werden insgesamt 27,03 % mehr Komponenten ausgetauscht als beim FIT-Ratenmodell, was zu einer höheren Fahrzeit von 19,13 % führt. Allerdings ist die Ausfallzeit beim Degradationsmodell um 73,85 % geringer. Wie zu erwarten, sinkt die Ausfallzeit bei einer größeren Anzahl an betrachteten Netzkomponenten weiter ab. Die Ergebnisse bestätigen die Resultate aus Abschnitt 5.3.2, dass sich die Ausfallzeiten mit Hilfe des Degradationsmodells erheblich verringern. Da die Laser und Empfänger eine geringere Reparaturzeit als die EDFAs benötigen, erhöht sich auch der Anteil der Netzkomponenten, die in einer

Parameter	FIT-Ratenmodell	Degradationsmodell	Unterschied
Verwendete NOCs	2	2	-
Ausfallwahrscheinlichkeit	2850	Degradationskurven	-
Ausgewechselte EDFAs pro Jahr	5,85	7,72	+31,97 %
Ausgewechselte Laser/Empfänger pro Jahr	8,74	12,35	+41,30 %
Mittlere Arbeitszeit pro EDFA	6,58 h	6,69 h	+1,68 %
Mittlere Arbeitszeit pro Laser	5,56 h	5,63 h	+1,26 %
Mittlere Arbeitszeit pro Komponente	5,97 h	6,04 h	+1,17 %
Gesamte Fahrzeit	6672,18 h	7948,58 h	+19,13 %
Gesamte Reparaturzeit	8716,18 h	2779 h	-73,85 %
Gesamtkosten pro Jahr	151136,89 $	206514,10 $	+36,64 %

Tabelle 5.2: Zusammenfassung der Ergebnisse für das Deutschland-50-Knotennetz für alle optischen Komponenten (2 NOCs)

Arbeitsschicht ausgetauscht werden können. Während bei den vorherigen Simulationen 11 % der Fahrzeiten durch Mehrfachreparaturen pro Arbeitsschicht eingespart wurden, ergibt sich für das Degradationsmodell mit allen Netzkomponenten eine Fahrzeitreduzierung um 16,07 %. Die Einsparung fällt nur geringfügig höher aus, da bei der Verwendung von zwei NOCs die Entfernungen zwischen NOC und optischer Komponente im Mittel sehr hoch sind und sich daher nur in seltenen Fällen mehrere Netzelemente in einer Arbeitsschicht reparieren lassen.

Bisher wurde davon ausgegangen, dass die Reparaturteams und die Ersatzteile auf zwei NOCs verteilt sind und jedes Team für eine Hälfte des Netzes zuständig ist. Die Untersuchungen haben gezeigt, dass dadurch nur in sehr seltenen Fällen mehrere Komponenten in einer Arbeitsschicht getauscht werden. Bei der Untersuchung der Reparaturzeit der EDFAs war dies nicht weiter von Bedeutung, da aufgrund der Reparaturzeit von 2 h eines EDFAs, nur maximal drei EDFAs in einer Arbeitsschicht repariert werden können. Anders sieht es bei der Betrachtung der Laser und Empfänger aus. Nach [VCP+06] dauert die Reparatur von Transpondern und Empfängern jeweils nur 1 h. Deshalb ergibt sich für die kombinierte Betrachtungen von EDFA, Lasern und Empfängern einer größere Fahrzeitreduzierung im Vergleich zu den EDFAs. Um dies genauer zu untersuchen, wird im Folgenden der Einfluss von mehreren NOCs auf den Reparaturprozess untersucht.

Verwendung von mehreren NOCs

In den folgenden Untersuchungen werden fünf NOCs an den Standorten Hamburg, Leipzig, Köln, Würzburg und München angenommen. Die Ergebnisse sind in Tabelle 5.3 zusammengefasst.

Parameter	FIT-Ratenmodell	Degradationsmodell	Unterschied
Verwendete NOCs	5	5	-
Ausfallwahrscheinlichkeit	2850	Degradationskurven	-
Ausgewechselte EDFAs pro Jahr	5,85	7,72	+31,97 %
Ausgewechselte Laser/Empfänger pro Jahr	8,74	12,35	+41,30 %
Mittlere Arbeitszeit pro EDFA	5,04 h	5,06 h	+0,40 %
Mittlere Arbeitszeit pro Laser	4,00 h	3,95 h	-1,25 %
Mittlere Arbeitszeit pro Komponente	4,42 h	4,38 h	-0,09 %
Gesamte Fahrzeit	4485,16 h	4535,71 h	+1,13 %
Gesamte Reparaturzeit	6529,16 h	2779 h	-65,10 %
Gesamtkosten pro Jahr	150345,40 $	205279,19 $	+36,54 %

Tabelle 5.3: Zusammenfassung der Ergebnisse für das Deutschland-50-Knotennetz für alle optischen Komponenten (5 NOCs)

In dem FIT-Ratenmodell werden durchschnittlich 5,85 EDFAs und 8,74 Laser und Empfänger getauscht. Insgesamt erfolgt ein Austausch von 1459 optischen Komponenten. Die Reparaturzeit beträgt pro EDFA 5,04 h und 4,00 h pro Laser/Empfänger. Zusammen ergibt sich damit eine mittlere Reparaturzeit von 4,42 h pro Netzkomponente. Die gesamte Fahrzeit für den Austausch der Netzkomponenten beträgt 4485,16 h. Die Fahrzeit ist damit im Vergleich zum FIT-Ratenmodell mit zwei NOCs um 32,78% geringer. Die Ergebnisse zeigen bereits bei dem FIT-Ratenmodell, dass durch eine höhere Anzahl an NOCs die Fahrzeit verringert und damit auch die Reparaturzeit der Netzkomponenten verringert wird.

Die gesamte Reparaturzeit für das Degradationsmodell beträgt 2779 h und ist um 65,10 % geringer als bei dem FIT-Ratenmodell. Im Vergleich zu dem vorherigen Szenario mit zwei NOCs fällt der Unterschied in den Reparaturzeiten zwischen FIT-Ratenmodell und Degradationsmodell geringer aus. Dies liegt an der Definition der Reparaturzeit beider Modelle. Beim FIT-Ratenmodell zählt im Gegensatz zum Degradationsmodell, bei dem nur die Reparaturzeit als Ausfallzeit gilt, die Anfahrtszeit und

die Reparaturzeit zur Ausfallzeit. Daher wirkt sich die Verwendung der fünf NOCs bei Betrachtung der Ausfallzeit nur beim FIT-Ratenmodell aus. Die Ausfallzeiten des Degradationsmodells sind unabhängig von den Fahrzeiten und Anzahl der NOCs und daher konstant.

Der Vorteil von mehreren NOCs zeigt sich bei der Betrachtung der Fahrzeiten beider Modelle im Vergleich zu zwei NOCs. Beim FIT-Ratenmodell sinken die Fahrzeiten um 32,78 % und beim Degradationsmodell um 42,94 %. Durch die Planung des Reparaturprozesses konnten 1475,01 h Fahrzeit eingespart werden, was einer Verringerung um 24,54 % im Vergleich zu dem Modell mit zwei NOCs entspricht. Vergleicht man die Fahrzeiten zwischen FIT-Ratenmodell und Degradationsmodell für beide Simulationen so zeigt sich, dass diese bei der Verwendung von fünf NOCs beim Degradationsmodell nur um 1,13 % höher sind, obwohl die Anzahl der ausgetauschten Netzelemente um 27,30 % höher ist und dadurch zusätzliche Fahrzeiten entstehen. Bei der Betrachtung von zwei NOCs ist die Fahrzeit beim Degradationsmodell um 16,05 % höher. Während bei zwei NOCs sehr selten zwei oder mehrere Komponenten in einer Arbeitsschicht repariert werden, ist dies bei fünf NOCs deutlich häufiger möglich, wie man anhand der eingesparten Fahrzeiten erkennt.

Analyse der Betriebskosten

Für die Kosten des Reparaturprozesses werden dieselben Annahmen wie für den Fall mit zwei NOCs verwendet. Die Kosten für die Laser und Empfänger werden aus [VCP+06] entnommen und mit dem Faktor zwei skaliert [Kie10], um von den Kosten eines $2{,}5$ Gbit/s auf die Kosten eines 10 Gbit/s Transponders zu kommen. Mit den genannten Werten ergeben sich für einen Laser Kosten von 9000 $. Die Betriebskosten für den Reparaturprozess werden wieder mit Formel 5.5 berechnet, allerdings werden zusätzlich noch die Kosten für die Laser und die Empfänger betrachtet.

Für das FIT-Ratenmodell mit zwei NOCs ergeben sich mit den Werten aus Tabelle 5.2 Gesamtkosten von 151136,89 $. Beim Degradationsmodell betragen die Gesamtkosten 206514,10 $ und sind damit um 36,64 % höher. Die Kostensteigerung des Reparaturprozesses ist im Wesentlichen auf die größere Anzahl an ausgewechselten Netzelementen zurückzuführen. Des Weiteren trägt auch die Reparaturzeit der zusätzlich gewechselten Netzelemente zu den gestiegenen Kosten bei. Das Degradationsmodell reduziert allerdings die Ausfallzeit um 68 %, was einer höheren Verfügbarkeit des Weitverkehrsnetzes entspricht.

Zum Vergleich werden die Reparaturkosten bei der Verwendung von fünf NOCs betrachtet. In diesem Fall ergeben sich für das FIT-Ratenmodell Reparaturkosten von 150345,40 $ und beim Degradationsmodell 205279,19 $. Die Steigerung beträgt bei diesem Szenario 36,54 % und entspricht damit ungefähr dem Szenario mit zwei NOCs. Die Untersuchungen zeigen, dass sich die höhere Anzahl der NOCs und damit die Reduzierung der Fahrzeiten auf beide Szenarien gleichermaßen auswirkt.

Betrachtet man auch die Kosten für die Verletzung der Dienstgüte, verringert sich die Kostendifferenz der beiden untersuchten Modelle. Zur Berechnung der Kosten werden folgende Annahmen für Strafzahlungen verwendet. Die Strafzahlungen erhöhen sich pro drei Stunden Dienstausfall in einem Monat bei Verkehr mit zugesicherter Wiederherstellung der Verbindung. Im Fall eines Dienstes mit zugesichertem Schutzpfad erhöhen sich die Strafzahlungen pro 15 Minuten Dienstausfall, allerdings bei halben Strafzahlungen. Es wird vereinfachend angenommen, dass eine Wellenlänge auf einem Link einem Dienst entspricht und 40 % des Verkehrs auf einem Link Dienstgütekriterien besitzen. Die Verkehrsverteilung entspricht den berechneten Verkehrsmatrizen aus Kapitel 3. Es werden pro Link 100 Wellenlängen und eine durchschnittliche Auslastung des Weitverkehrsnetzes von 60 % angenommen. Die Kosten sind in Abbildung 5.9 und 5.10 zusammengefasst. Die Abszisse zeigt den Prozentsatz der Fehler an, bei dem SLA-Verletzungen auftreten.

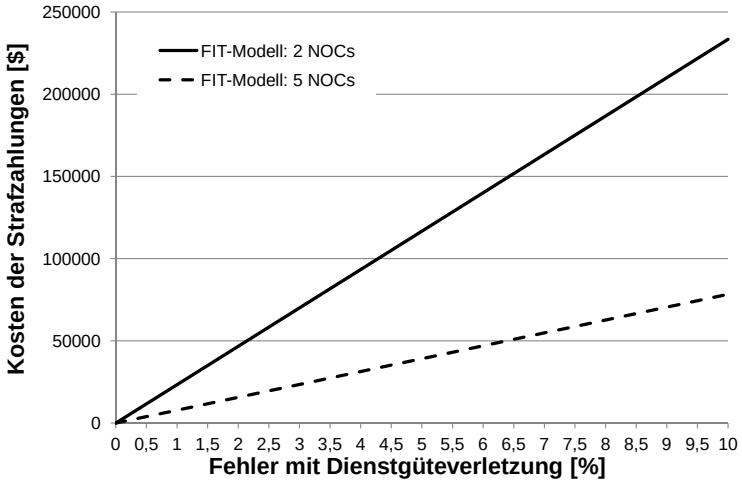


Abbildung 5.9: Auswirkung der Fehler auf die Höhe der Strafzahlungen (Restoration)

Nimmt man das oben beschriebene drei Stunden Intervall für Strafzahlungen, so ergibt sich der in Abbildung 5.9 dargestellte Kostenverlauf für das FIT-Ratenmodell. Das Simulationsszenario mit fünf NOCs weist, aufgrund der geringeren Anfahrtszeiten, geringere Kosten auf als das FIT-Ratenmodell mit zwei NOCs. Bei dem Degradationsmodell ergeben sich bei den oben genannten Annahmen keine zusätzlichen Kosten, da erst ab drei Stunden eine Strafzahlung erfolgt und der Austausch der optischen Elemente maximal zwei Stunden dauert. Sind bereits innerhalb der ersten drei Stunden Strafzahlungen vereinbart, fallen auch beim Degradationsmodell Strafzahlungen an. Derselbe Betrag addiert sich aber auch beim FIT-Ratenmodell, so dass die Differenz zwischen FIT-Modell und Degradationsmodell konstant bleibt. Aus den Kurven in Abbildung 5.9 und 5.10 erkennt man, dass die vorher berechneten Mehrkosten des Degradationsmodells ausgeglichen werden, sobald bei 2 % beziehungsweise 6 % der Fehler Strafzahlungen auftreten.

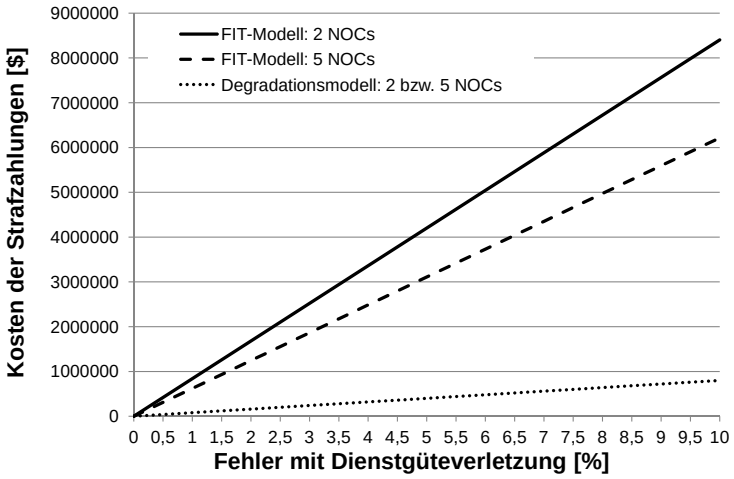


Abbildung 5.10: Auswirkung der Fehler auf die Höhe der Strafzahlungen (Protection)

In Abbildung 5.10 sind die Kurven für die Strafzahlungen für zugesicherte Ersatzpfade dargestellt. Da hier bereits nach 15 Minuten Strafzahlungen zu leisten sind, fallen auch für das Degradationsmodell Kosten an. Diese sind unabhängig von der Anzahl der NOCs, da beim Degradationsmodell nur die Austauschzeit der EDFAs zu den Zahlungen beiträgt. Im Vergleich zum FIT-Ratenmodell sind die Strafzahlungen beim Degradationsmodell wesentlich geringer, so dass die Gesamtkosten beim Degradationsmodell geringer ausfallen, wenn bereits 0,5 % der Fehler Strafzahlungen verursachen.

5.4.1 Diskussion der Ergebnisse

Wie bereits im Fall des untersuchten Links beschrieben, steigt die Anzahl der ausgewechselten Komponenten für das Degradationsmodell auch für das Referenznetz an. Gleichzeitig erreicht das Netz aber eine höhere Verfügbarkeit, da die Fahrzeiten zu den Komponenten nicht mehr zur Ausfallzeit zählen, sondern ausschließlich die Reparaturzeit der degradierten Komponenten. Die Hinzunahme von spontanen Ausfällen der Komponenten beim Degradationsmodell verringert die Verfügbarkeit, allerdings ist diese immer noch höher als im FIT-Ratenmodell. Die Ergebnisse treffen sowohl für die Verwendung von zwei beziehungsweise von fünf NOCs zu. Die Analyse der Betriebskosten ohne Strafzahlungen hat gezeigt, dass die höhere Anzahl an getauschten Komponenten zu deutlich höheren Kosten führt. Betrachtet man allerdings auch die Strafzahlungen aufgrund von ausgefallenen Diensten, weist das Degradationsmodell bereits die gleichen Kosten auf, wenn 2 % beziehungsweise 6 % der Fehler die Dienstgüte verletzen. Im Fall von zugesicherten Schutzpfaden für bestimmte Dienste, weisen die beiden Modelle die gleichen Kosten auf, wenn 0,5 %

der Fehler eine Strafzahlung verursachen.

Die Abschätzung der Strafzahlungen zeigt, dass bereits bei einem geringen Prozentsatz an Fehlern, die zu Strafzahlungen führen, das Degradationsmodell dieselben Betriebskosten aufweist wie das FIT-Modell und damit die Mehrkosten durch die höhere Anzahl an getauschten Netzelementen ausgleicht. Allerdings sind bei der Bewertung des Degradationsmodells nicht nur die Kosten ausschlaggebend, sondern auch die höhere Verfügbarkeit, die durch das frühzeitige Signalisieren erreicht wird. Bei einer gemeinsamen Betrachtung der Größen Verfügbarkeit und Betriebskosten, zeigt sich der Vorteil des Degradationsmodells, das bei gleichen oder geringfügigen höheren Kosten eine höhere Verfügbarkeit besitzt.

5.5 Zusammenfassung

In diesem Kapitel wurde der Einfluss eines Degradationsmodells auf die Verfügbarkeit eines Weitverkehrsnetzes und den Reparaturprozess untersucht. Dazu wurde zunächst die Degradation eines Pump-Lasers anhand eines Modells beschrieben, welches die zeitabhängige Degradation von optischen Netzkomponenten darstellt.

Mithilfe des Degradationsmodells erfolgten Untersuchungen zum Ausfallverhalten von EDFAs auf einem einzelnen Link. Die Ergebnisse des Degradationsmodells und des FIT-Ratenmodells wurden miteinander verglichen, um die Verfügbarkeit und die Reparaturzeit des Links zu bestimmen. Zusätzlich wurden noch zwei verschiedene Austauschstrategien betrachtet. Die Ergebnisse zeigen, dass der Austausch aller EDFAs auf einem Link die Anzahl der ausgetauschten EDFAs zwar erhöht, allerdings die Anzahl der Linkunterbrechungen reduziert und die Verfügbarkeit des Links erhöht. Das Degradationsmodell erlaubt zusätzlich die Planung der Wartungsphase eines Links oder Netzes.

Der zweite Teil des Kapitels befasst sich mit der Untersuchung des Degradationsmodells und einem FIT-Ratenmodell in einem Weitverkehrsnetz. Die aufgeführten Untersuchungsergebnisse zeigen, dass bei dem Degradationsmodell die Ausfallzeit des Weitverkehrsnetzes geringer und somit die Verfügbarkeit höher ist. Die Anzahl der ausgewechselten EDFAs steigt jedoch gegenüber dem FIT-Ratenmodell an, da diese vorzeitig gewechselt werden. Dadurch ergibt sich eine längere Fahrzeit, die allerdings durch das Austauschen von mehreren EDFAs in einer Arbeitsschicht wiederum verringert wurde.

Im letzten Abschnitt wurde das Degradationsmodell auf Laser und Empfangsdioden erweitert, welche eine ähnliche Alterungscharakteristik wie EDFAs besitzen. Zusätzlich wurden noch die Auswirkungen von zwei und fünf NOCs auf den Reparaturprozess analysiert. Die Ergebnisse haben gezeigt, dass bei einer höheren Anzahl von betrachteten Netzelementen die Ausfallzeiten im Vergleich zum FIT-Ratenmodell weiter verringert und die Verfügbarkeit des Weitverkehrsnetzes erhöht wird. Die Verwendung von zwei NOCs führt dazu, dass aufgrund der großen Entfernungen

zwischen den NOCs und den auszutauschenden Komponenten nur sehr selten mehrere Elemente gleichzeitig in einer Arbeitsschicht ausgewechselt wurden. Bei der Betrachtung von fünf NOCs nähern sich die Gesamtfahrzeiten der beiden Modelle weiter an, obwohl beim Degradationsmodell mehr Netzelemente ersetzt wurden. Dieser Effekt beruht auf der höheren Anzahl an degradierten Netzelementen die in einer Arbeitsschicht getauscht wurden. Allgemein ergibt sich, dass durch mehrere NOCs die Reparatur- und Ausfallzeit für beide Modelle verringert wird.

Um eine detailliertere Einschätzung zu den höheren Fahrzeiten im Vergleich zu der geringeren Ausfallzeit und der höheren Verfügbarkeit zu bekommen, wurde im letzten Abschnitt ein *OPerational EXpenditure* (OPEX)-Modell entwickelt, um die Kosten des Reparaturprozesses der beiden Modelle zu vergleichen. Es hat sich gezeigt, dass die Reparaturkosten für das Degradationsmodell höher sind als für das FIT-Ratenmodell, allerdings bei einer deutlich höheren Verfügbarkeit des Netzes. Die Betrachtung der Strafzahlungen haben ergeben, dass beide Modelle die gleichen Betriebskosten besitzen, wenn bereits 1 % der Fehler Strafzahlungen verursachen.

6 Teilautomatisiertes Netzmanagement

Wie im vorherigen Kapitel beschrieben, tritt in Weitverkehrsnetzen eine Vielzahl an Fehlern auf, die zum Ausfall von Netzkomponenten führen. Aufgrund der immer größeren transportierten Datenmenge und des gleichzeitigen Kostendrucks auf die Netzbetreiber, wird ein Netzmanagementsystem benötigt, das schnell auf eine veränderte Netzsituation reagiert und das Weitverkehrsnetz entsprechend anpasst.

Eine mögliche Verbesserung ist die Verwendung eines teilautomatisierten Netzmanagementsystems, welches ohne oder nur mit geringer manueller Interaktion des Netzbetreibers das Weitverkehrsnetz an die veränderte Netzsituation anpasst. In diesem Kapitel wird ein teilautomatisiertes Netzmanagementsystem realisiert, das basierend auf den Informationen in der Managementdatenbank, automatisch vorab definierte Ersatzkonfigurationen für potentielle Netzfehler berechnet und bereitstellt.

In Abschnitt 6.1 wird die Funktionsweise des teilautomatisierten Netzmanagementsystems beschrieben. Zunächst wird auf die Funktionen und das Zusammenspiel der einzelnen Managementmodule eingegangen. Anschließend erfolgt eine Beschreibung der jeweiligen Informationen, die in dem jeweiligen Managementmodul benötigt werden. Die Managementmodule werden kontinuierlich durchlaufen und passen das Weitverkehrsnetzes an die aktuelle Netzsituation an.

Jede Umkonfiguration des Netzes stellt aber einen kurzen Ausfall der betroffenen Netzbereiche dar und beeinträchtigt die Verfügbarkeit des Netzes. Damit das teilautomatisierte Netzmanagementsystem nicht ständig eine Umkonfiguration durchführt, wird in Abschnitt 6.2 ein Kostenmodell für Konfigurationswechsel des Weitverkehrsnetzes entwickelt. Anhand des Kostenmodells entscheidet das Netzmanagementsystem nach einer veränderten Netzsituation, ob sich die Umkonfiguration bestimmter Netzbereiche lohnt oder das Netz weiter mit der aktuellen Konfiguration betrieben wird.

In Abschnitt 6.3 erfolgt eine detaillierte Darstellung der zwei entwickelten Planungsprozesse des Netzmanagementsystems. Im fehlerfreien Fall werden mittels einer ganzzahligen linearen Optimierung definierte Ersatzkonfigurationen vorausberechnet. Die ganzzahlige lineare Optimierung wird durch einen heuristischen Lösungsansatz ergänzt, der im Fehlerfall zur Anwendung kommt, wenn keine geeignete Ersatzkonfiguration vorhanden ist. Das Ziel der Heuristik besteht darin, eine geeignete Lösung zur Behebung des Fehlers in wenigen Minuten oder sogar Sekunden zu berechnen.

6.1 Beschreibung des teilautomatisierten Netzmanagements

Heutige Weitverkehrsnetze werden mit Hilfe einer Steuerungs- oder Managementebene überwacht. Wie in Kapitel 2 beschrieben, besitzen beide Ebenen Schutzmechanismen, um einen Ausfall des Weitverkehrsnetz zu verhindern. Für den Betrieb eines Netzes müssen allerdings nicht beide Ebenen gleichzeitig vorhanden sein. Der Netzbetreiber entscheidet, ob er eine Steuerungs- und eine Managementebene oder nur eine Managementebene in seinem Weitverkehrsnetz verwendet. Für das in diesem Kapitel entwickelte teilautomatisierte Netzmanagementsystem wird davon ausgegangen, dass beide Ebenen vorhanden sind. Deshalb erfolgt zunächst eine Beschreibung der jeweiligen Aufgaben der beiden Ebenen.

6.1.1 Steuerungsebene

Die Steuerungsebene stellt eine verteilte Funktionalität zur Steuerung des Netzes zur Verfügung. Dabei werden Protokolle wie *Open Shortest Path First* (OSPF), *Resource reSerVation Protocol* (RSVP) und *Label Distribution Protocol* (LDP) benutzt, um die Topologie des Netzes zu erkennen und zu überwachen. Neben der Topologieerkennung ist die Steuerungsebene auch für die Informationsverteilung zuständig. Die weiteren Funktionalitäten sind Signalisierung, Routing, verteilte Wiederherstellung und Fehlerlokalisierung. Die Protokolle der Steuerungsebene tauschen mittels Signalisierungsnachrichten beispielsweise Informationen über die Kosten zwischen den Netzknoten aus, anhand derer die kürzesten Pfade zwischen den Netzknoten bestimmt werden. Die kürzesten Pfade werden für das Routing des Datenverkehrs benutzt und regelmäßig durch den Austausch von Statusinformationen erneuert. Neben der Berechnung der kürzesten Pfade kann die Steuerungsebene auch Ersatzpfade berechnen und reservieren, auf die im Fehlerfall umgeschaltet wird. Die Steuerungsebene verwaltet eine *Traffic Engineering Database* (TED), in der alle gesammelten Informationen über die Links und Netzknoten gespeichert werden. Die Informationen in der TED werden der Managementebene zur Verfügung gestellt und in der Managementdatenbank gespeichert. Zusätzlich kann in der Steuerungsebene noch ein PCE verwendet werden, das für die Berechnung der kürzesten Pfade und der Ersatzwege zuständig ist. Das *Path Computation Element* (PCE) wurde durch die IETF im RFC4655 [FV06] definiert und stellt eine Funktionseinheit dar, die einen Netzpfad basierend auf der Netztopologie berechnet. Für die Berechnung können verschiedene Nebenbedingungen verwendet werden. In dieser Arbeit wird das PCE als Berechnungsknoten für die Steuerungsebene verwendet, der für die Berechnung der kürzesten Pfade eingesetzt wird. Alle komplexeren Berechnungen wie die Optimierungen werden in der Managementebene durchgeführt.

6.1.2 Managementebene

Im Gegensatz zur Steuerungsebene gibt es bei der Managementebene sowohl verteilte als auch zentrale Architekturen. In dieser Arbeit wird ein zentrales Netzmanagementsystem betrachtet, da die zentrale Datenspeicherung eine globale Sicht und die globale Optimierung des Weitverkehrsnetzes ermöglicht. Die Managementebene überwacht das Weitverkehrsnetz mittels Überwachungsprotokollen und speichert die Informationen in der Managementdatenbank ab. Dabei müssen wesentlich mehr Informationen über das Netz gespeichert werden als bei der Steuerungsebene. Das Netzmanagementsystem benötigt beispielsweise neben den Verkehrsdaten auch noch die aktuellen Konfigurationsdaten des Weitverkehrsnetzes. Weiter unten werden die gespeicherten Informationen detaillierter beschrieben.

Neben der Überwachung des Netzes ist die Managementebene für die Visualisierung der Daten zur Vereinfachung der Überwachung und Fehlerfindung zuständig. Insbesondere bei dem vorgestellten teilautomatisierten Netzmanagementsystems müssen die automatisierten Teilschritte dem Netzbetreiber angezeigt werden, damit dieser gegebenenfalls auf das System einwirken kann. Ein weiteres Merkmal des Netzmanagement stellt die Konfiguration der Netzelemente, des PCE und der Steuerungsebene dar. Die Protokolle der Steuerungsebene werden durch die Managementebene konfiguriert und auf den Netzelementen wie in Kapitel 4 beschrieben aktiviert. Das Netzmanagement beeinflusst damit das Verhalten der Steuerungsebene, indem es die Randbedingungen für die Berechnung der Pfade und das Verhalten der Protokolle definiert. Neben den Protokollen der Steuerungsebenen ist die Managementebene auch für die Konfiguration weiterer Protokolle und Funktionalitäten der Netzkomponenten zuständig. Die von den Netzkomponenten gesendeten Alarmnachrichten werden ebenfalls von dem Netzmanagementsystem verarbeitet und analysiert. Verwendet ein Netzbetreiber keine Steuerungsebene in seinem Weitverkehrsnetz, so ist die Managementebene zusätzlich für die Aufgaben der Steuerungsebene zuständig.

6.1.3 Aufbau des teilautomatisierten Netzmanagementsystems

Die beschriebene Aufteilung der Funktionalitäten von Steuerungs- und Managementebene wird in dem Netzmanagementsystem in Abbildung 6.1 berücksichtigt. Wie bereits in Kapitel 2 beschrieben, besteht das Netzmanagement eines Weitverkehrsnetzes aus vier Phasen: Überwachung, Analyse, Planung und Konfiguration. Diese vier Phasen werden von dem teilautomatisierten Netzmanagement kontinuierlich durchlaufen, um auf Veränderungen im Netz schnell und geeignet zu reagieren. Alle notwendigen Managementmodule sind in Abbildung 6.1 dargestellt.

Alle gezeigten Module übernehmen einen bestimmten Aufgabenbereich des Netzmanagements und senden die relevanten Informationen an die anderen Module. Neben den Managementmodulen ist auch die Steuerungsebene abgebildet, die von dem Netzmanagement gesteuert wird. Das Netzmanagementsystem umfasst folgende Module

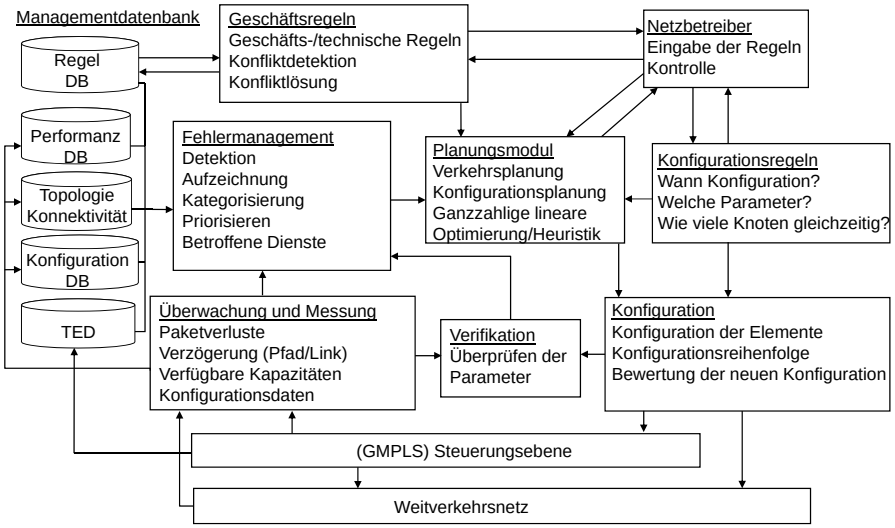


Abbildung 6.1: Darstellung des teilautomatisierten Netzmanagements

- Managementdatenbank
- Überwachung und Messung
- Verifikation
- Fehlermanagement
- Planungsmodul
- Geschäfts- und Konfigurationsregeln
- Konfiguration
- Schnittstelle zum Netzbetreiber

Die Interaktion der einzelnen Module entspricht einer Kontrollschleife, die kontinuierlich durchlaufen wird. Diese ist in Abbildung 6.2 veranschaulicht.

Das Überwachungsmodul liefert die aktuellen Informationen aus dem Weitverkehrsnetz und speichert diese in der Managementdatenbank. Die Managementdatenbank ist eine zentrale Datenbank, die in verschiedene Informationsbereiche aufgeteilt ist. Die Informationen aus der Überwachung werden dem Fehlermanagementmodul zur Verfügung gestellt, das eine Analyse anhand der Daten durchführt. Die festgestellten Veränderungen werden an das Planungsmodul übergeben, das mittels zweier in dieser Arbeit entwickelter Planungsprozesse eine Lösung für die Veränderung zur Verfügung stellt. Die Planungsprozesse werden später in diesem Kapitel eingehend behandelt. Das Planungsmodul berücksichtigt bei der Optimierung des Weitverkehrsnetzes die Geschäfts- und Konfigurationsregeln, die in den jeweiligen Modulen gespeichert sind. Die berechnete optimale Lösung wird anschließend an das Konfigurationsmodul übergeben, das die Konfiguration des Netzes durchführt. Dabei berücksichtigt das Konfigurationsmodul die Konfigurationsregeln, die vom Netzbetreiber vorgegeben werden. In dieser Arbeit liegt der Schwerpunkt auf der

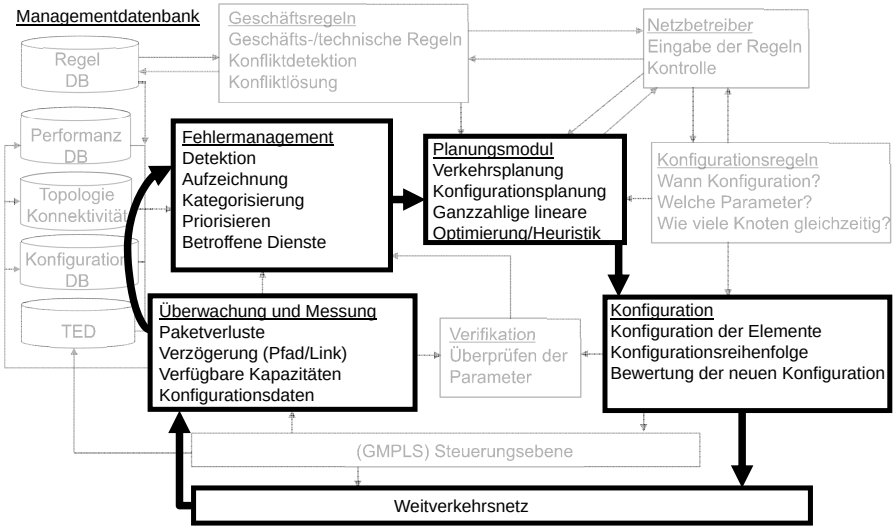


Abbildung 6.2: Managementschleife

Entwicklung und Implementierung des Planungsmoduls. Die entwickelten Planungsprozesse der Planungsmoduls sind in den Abschnitten 6.3 und 6.4 eingehender dargestellt. Im nächsten Abschnitt werden die Funktionen der einzelnen Module detailliert beschrieben.

6.1.4 Überwachungsmodul und Managementdatenbank

Das Überwachungsmodul enthält die Überwachungsprotokolle, mit denen die Informationen über den aktuellen Zustand des Netzes gesammelt und in der Managementdatenbank gespeichert werden. Für die Überwachung und Messung der Netzgüte kommen Werkzeuge wie Linktrace, Ping und Loopback zum Einsatz, die Informationen über die Linkauslastung und Konnektivität des Netzes liefern. Protokolle wie *Simple Network Management Protocol* (SNMP) werden anschließend zum Austausch der Managementinformationen und zur Konfiguration der Netzkomponenten genutzt. SNMP dient zum Konfigurieren und Abfragen der Daten auf den Netzkomponenten. In der *Management Information Base* (MIB) eines Netzknotens sind alle notwendigen Parameter gespeichert und können durch das Netzmanagementsystem verändert werden.

Die Informationen über das Netz werden in der Managementdatenbank gespeichert, die in verschiedene Bereiche aufgeteilt ist. In der Topologiedatenbank sind die Informationen über die Topologie und die Kapazitäten der Links abgelegt. Sie enthält die Konnektivität des gesamten Netzes und die aktuell konfigurierten Pfade der Verkehrsanforderungen. Ebenso enthält sie die Informationen über die berechneten Ersatzwege, die in einem Fehlerfall verwendet werden. Die Topologiedatenbank enthält ebenso die Informationen über die Pfade, die von der Steuerungsebene berechnet werden.

Die Konfigurationsdatenbank speichert die aktuelle Konfiguration aller Netzknoten und das momentane Routing der Verkehrsanforderungen. Zur aktuellen Konfiguration gehören beispielsweise die „Hallo"- und „Dead"-Timer bestimmter Protokolle, die Weiterleitungstabellen der Router, der Energieverbrauch der Netzkomponenten und die maximal erlaubte nutzbare Kapazität der Links. Darüber hinaus enthält die Konfigurationsdatenbank die Informationen über die aktuelle Auslastung der Links, die Prozessorauslastungen der Netzknoten, die Paketverlustraten, die Signalqualität und die Paketverzögerungen auf den Links und den Pfaden. Zusätzlich werden auch die Degradationswerte der optischen Netzkomponenten gespeichert, wie in Kapitel 5 beschrieben. Die Konfigurationsdatenbank enthält ebenfalls die vorab geplanten Ersatzkonfigurationen, die im Fehlerfall zur Anwendung kommen. Es werden aber nicht für alle potentiellen Fehlerfälle vorab optimale Ersatzkonfigurationen berechnet, sondern lediglich eine vorher definierte Anzahl an Ersatzkonfigurationen. In Abschnitt 6.3.3 wird genauer auf die Gründe für die begrenzte Anzahl an Ersatzkonfigurationen eingegangen.

Die Regeldatenbank setzt sich aus den Geschäfts- und Konfigurationsregeln zusammen. Die Geschäftsregeln definieren die *Service Level Agreement* (SLA) die bestimmen, welche Dienstgütekriterien die gerouteten Dienste einhalten müssen. Die Dienstgütekriterien werden vertraglich zwischen Netzbetreiber und Kunde festgehalten und enthalten ebenso die Höhe der Strafzahlungen, falls die Dienstgütekriterien nicht eingehalten werden. Die Konfigurationsdatenbank enthält die Konfigurationsregeln, die angeben, zu welchem Zeitpunkt eine Konfiguration durchgeführt wird und wie viele Netzkomponenten gleichzeitig neu konfiguriert werden. Die SLAs wirken sich direkt auf das Konfigurationsverhalten aus, da sie die maximale Ausfallzeit eines Dienstes definieren. Bestimmte Umkonfigurationen wie das Neustarten eines Routers verursachen kurze Ausfallzeiten der betroffenen Netzknoten und Kanten und müssen deshalb zur Unverfügbarkeit des Netzes addiert werden.

Die Alarmdatenbank ist für die Speicherung aller vom Netzmanagement empfangenen Alarmnachrichten zuständig. Die Alarmmeldungen werden mit einem Zeitstempel und dem Fehlertyp in einer Datei abgelegt und analysiert. Die TED der Steuerungsebene wird ebenfalls in der Managementdatenbank gespeichert. In der TED sind Informationen über die momentan benutzen Kapazitäten der Links, die reservierten Kapazitäten und die Verzögerungen pro Link gespeichert. Diese Daten werden von der Steuerungsebene gesammelt und zur Managementdatenbank weitergeleitet. In Tabelle 6.1 sind die wichtigsten in der Managementdatenbank gespeicherten Informationen zusammengefasst.

6.1.5 Fehlermanagement- und Verifikationsmodul

Im Fehlermanagementmodul werden die gespeicherten Informationen über das Netz analysiert und aktuell aufgetretene Netzfehler kategorisiert und priorisiert. Das Modul ist für die Alarmkorrelation zuständig mit deren Hilfe der Ursprungsalarm herausgefiltert wird [GH96], [SSC+03] und [YLC05]. Netzfehler erzeugen häufig

Teil der Managementdatenbank	Gespeicherte Inhalte
Topologie	Netzknoten, Links, Konnektivität
Konfiguration	„Hallo“- und „Dead“-Timer; Bandbreite; Weiterleitungstabellen; Energieverbrauch
Netzgüte	Paketverluste, Prozessorauslastung; eingehende Signalqualität; Linkauslastung; Wartezeiten
Regeln	Dienstgüteparameter; Konfigurationsregeln
Alarm	Log-Datei (Zeitstempel; Fehlertyp)
TED	Freie Bandbreite; reservierte Bandbreite; Wartezeit pro Link

Tabelle 6.1: Inhalt der Managementdatenbank

mehrere Alarmmeldungen auf den verschiedenen Schichten, weshalb es notwendig ist, die Anzahl der redundanten Alarmmeldungen zu verringern. Anschließend wird anhand des Zeitstempels, des Fehlertyps und der Ortsangabe die Fehlerquelle lokalisiert. Neben der Alarmkorrelation findet in dem Fehlermanagementmodul auch die Analyse der aktuellen Konfiguration des Weitverkehrsnetzes statt. Dazu wird das in Kapitel 4 entwickelte Bewertungsschema verwendet. Da Konfigurationsfehler häufig keine Alarmmeldung auslösen, müssen Netzanomalien untersucht werden, die auf einen Konfigurationsfehler hindeuten können. Anhand der beobachteten Auswirkungen und dem entwickelten Bewertungsschema lassen sich gegebenenfalls Rückschlüsse ziehen, ob es sich tatsächlich um einen Konfigurationsfehler handelt und welche Netzkomponenten betroffen sind.

Das Fehlermanagementmodul analysiert zusätzlich die Degradationswerte der optischen Komponenten. Auf Basis der Degradationswerte berechnet ein Algorithmus die Restlaufzeit der jeweiligen Netzkomponenten. Die Restlaufzeiten ermöglichen dem Netzbetreiber die Wartungsphasen in seinem Netz zu planen und das Netz auf die bevorstehenden Auswechslungen der Netzkomponenten vorzubereiten.

Anschließend an die Detektion werden die gefundenen Netzfehler kategorisiert und priorisiert. Die Netzfehler werden nach Hardware-, Software-, Konfigurationsfehler und sonstige Fehler aufgeteilt. In die Kategorie „sonstige Fehler“ fallen alle Netzfehler, die keiner anderen Kategorie zugeordnet werden können. Nach der Einordnung der Netzfehler erfolgt eine weitere Abstufung nach der Anzahl an betroffenen Links, Netzkomponenten und Diensten. Diese Informationen dienen zum Priorisieren der Fehler, um die Reihenfolge der Fehlerbehebung zu bestimmen. Die Priorität der Fehler ist umso höher, je mehr Netzkomponenten und Dienste mit Dienstgütekriterien betroffen sind. Aber auch die Auslastung der Links wirkt sich auf die Priorität des Fehlers aus.

Das Verifikationsmodul dient zur Überprüfung der aktuellen Netzkonfiguration. Es vergleicht die aktuelle Konfiguration des Netzes mit der geplanten Konfiguration, um Abweichungen festzustellen. Ebenso wird die Einhaltung der Dienstgütekriterien

wie Verzögerung der Pakete, Verlustrate und benutzte Kapazitäten überprüft. Ergibt sich hier eine Abweichung von den geplanten Vorgaben, wird dies an das Fehlermanagementmodul gesendet. Die Einrichtung eines neuen Dienstes wird ebenfalls im Verifikationsmodul durchgeführt. Das Modul überprüft, ob für den Dienst genügend freie Netzkapazitäten vorhanden sind. Die bestehenden Dienste dürfen durch den neuen Dienst nicht beeinträchtigt werden. Erfordert der neu einzurichtende Dienst bestimmte Dienstgütekriterien werden diese ebenfalls von dem Verifikationsmodul berücksichtigt. Stellt das Verifikationsmodul ein Fehlverhalten fest, übergibt es die Information an das Fehlermanagementmodul, das die Ursache für die Abweichung analysiert. Handelt es sich um eine Netzstörung, werden die entsprechenden Informationen an das Planungsmodul übergeben, um eine Lösung zur Behebung der Störung zu suchen.

6.1.6 Online-Planungsmodul

Das Online-Planungsmodul stellt die Intelligenz des teilautomatisierten Netzmanagements dar. Das Modul verwendet zwei Planungsprozesse, um das Verhalten des Netzes zu steuern.

- Eine ganzzahlige lineare Optimierung
- Einen heuristischen Lösungsansatz

Im fehlerfreien Fall werden kontinuierlich optimale Ersatzkonfigurationen für zukünftige Netzsituationen berechnet und in der Managementdatenbank abgelegt. Die Anzahl der vorab berechneten Ersatzkonfigurationen hängt von der Zeitdauer zwischen zwei Veränderungen der Netzsituation und der Degradation der Netzkomponenten ab. Eine längere stabile Netzsituation erlaubt es, eine größere Anzahl an Ersatzkonfigurationen vorab zu berechnen.

Kommt es zu einer Veränderung im Netz, die eine Umkonfiguration von bestimmten Netzbereichen erfordert, wird zuerst nach einer geeigneten vorab berechneten Ersatzkonfigurationen gesucht. Die Suche in der Managementdatenbank führt zu einer kürzeren Reaktionszeit der Managementebene und verringert die Ausfallzeit des Netzes. Der Algorithmus zur Vorausplanung der Ersatzkonfigurationen und der Prozess des Online-Planungsmoduls werden genauer in Abschnitt 6.3 und 6.4 beschrieben.

Der zweite Planungsprozess des Online-Planungsmoduls berechnet Lösungen für Netzfehler, wenn keine geeignete Ersatzkonfiguration gefunden wurde. Die für diesen Prozess verwendete Heuristik wird in Abschnitt 6.4 genauer beschrieben. Liefert einer der beiden Planungsprozesse eine Lösung, wird diese an das Konfigurationsmodul weitergeleitet.

6.1.7 Konfigurationsmodul

Das Konfigurationsmodul verwendet die Daten aus dem Planungsmodul und der Managementdatenbank und erstellt anhand der Informationen die Konfigurationsdateien für die jeweiligen Netzkomponenten. Die Konfigurationsdateien werden ebenfalls in der Managementdatenbank gespeichert. Anhand der Konfigurationsregeln, die vom Netzbetreiber festgelegt werden, bestimmt das Konfigurationsmodul, wann eine Konfiguration durchgeführt wird und wie viele Netzkomponenten gleichzeitig konfiguriert werden. Der Zeitpunkt der Konfiguration und die Anzahl der zu konfigurierenden Netzkomponenten bestimmen sich auch aus der Fehleranalyse und der entsprechenden Lösung, die durch das Planungsmodul geliefert wird.

6.1.8 Schnittstelle zum Netzbetreiber

Die Schnittstelle zum Netzbetreiber dient zur Überwachung des teilautomatisierten Netzmanagementsystems. Der Netzbetreiber ist für den Netzbetrieb und die Erfüllung der Dienstgütekriterien verantwortlich. Deshalb erfolgt ohne Zustimmung des Netzbetreibers keine automatische Neukonfiguration des Netzes. Das Managementsystem überwacht, analysiert und plant selbständig eine neue Konfiguration und teilt dem Netzbetreiber anschließend die aufgetretenen Fehler und die gefundene Lösung mit. Der Netzbetreiber entscheidet anhand der ihm zur Verfügung gestellten Information, ob das Weitverkehrsnetz umkonfiguriert wird. Das in dieser Arbeit entwickelte Netzmanagementsystem enthält allerdings eine Kostenfunktion, anhand derer das Netzmanagement eine Evaluierung durchführt und entscheidet, ob sich eine Umkonfiguration lohnt. Die Kostenfunktion wird in Abschnitt 6.2 genauer diskutiert. Mittels der Kostenfunktion ist auch eine automatische Umkonfiguration des Netzes vorstellbar, allerdings verfügt der Netzbetreiber in diesem Fall über eine geringere Kontrolle seines Netzes.

6.1.9 Geschäfts- und Konfigurationsregeln

Für die Planung der Ersatzkonfigurationen und der Konfiguration der Netzkomponenten gelten bestimmte Randbedingungen, die durch die Geschäfts- und Konfigurationsregeln festgelegt werden. Die Geschäftsregeln fließen als Nebenbedingung in den Planungsprozess ein und beeinflussen die Ergebnisse der Optimierungen. Die Geschäftsregeln enthalten unter anderem folgende Punkte:

- Die Dienstgütekriterien der einzelnen Dienste und die erforderlichen Strafzahlungen bei Nichterfüllung
- Die maximal benutzbare Kapazität pro Link
- Die maximal reservierbare Bandbreite pro Link

Die Konfigurationsregeln fließen sowohl in die Optimierung als auch in die Konfiguration des Netzes ein und bestimmen, wann eine Konfiguration ausgeführt wird und wie viele Netzkomponenten gleichzeitig konfiguriert werden. Die Konfigurationsregeln stellen keine unveränderlichen Regeln dar, sondern hängen unter anderem von der aktuellen Auslastung der Links und der Netzknoten des Weitverkehrsnetzes ab. Sie definieren beispielsweise, dass ein Konfigurationswechsel, bei dem viele Netzkomponenten gleichzeitig umkonfiguriert werden, in einer Zeitspanne mit geringer Auslastung der Netzkomponenten durchgeführt wird. Damit hat die Umkonfiguration nur eine geringe Auswirkung auf die Dienste eines Weitverkehrsnetzes.

Die Konfigurationsregeln bestimmen auch die Anzahl der Konfigurationswechsel, die innerhalb eines bestimmten Zeitraums erlaubt sind. Da einige Konfigurationsänderungen auf den Netzkomponenten zu kurzen Unterbrechungen des Routings führen, muss der Netzbetreiber die Konfigurationswechsel auf eine geeignete Anzahl reduzieren, so dass nicht bereits durch häufige Konfigurationswechsel die Dienstgütekriterien verletzt werden.

6.2 Kostenmodell zur Bewertung eines Konfigurationswechsels

Das Netzmanagementsystem verfügt über eine Schnittstelle zum Netzbetreiber, die es dem Betreiber ermöglicht, den Konfigurationszeitpunkt selbst zu bestimmen. Das Netzmanagement liefert in diesem Fall die Informationen über den Fehler und die gefundene Lösung an den Netzbetreiber, führt aber keine Neukonfiguration durch. Um auch den Konfigurationswechsel automatisch durch das Netzmanagementsystem durchführen zu lassen, erfolgt in diesem Abschnitt die Realisierung eines Kostenmodells, anhand dessen das Netzmanagement entscheidet, ob ein Konfigurationswechsel durchgeführt wird. Das entwickelte Kostenmodell analysiert und bewertet zunächst die Kosten eines Konfigurationswechsels und führt danach gegebenenfalls die Konfiguration aus. Ohne Verwendung eines Bewertungssystems führt jede Netzänderung zu einer Neukonfiguration des Netzes, wenn das Planungsmodul eine geeignete Ersatzkonfiguration bereithält. Zu häufige Umkonfigurationen des Netzes führen aber zu einem instabilen Netzzustand, da durch jede Konfiguration bestimmte Netzkomponenten nicht erreichbar sind und zur Blockierung von Diensten und Reduzierung der Verfügbarkeit des Netzes beitragen.

6.2.1 Kostenmodell

Das Kostenmodell betrachtet zum einen die tatsächlichen Kosten, die zum Beispiel durch die Verletzung der Dienstgütekriterien entstehen, zum anderen die virtuellen Kosten, die vom Zeitpunkt der Konfiguration und den bereits in der Vergangenheit erfolgten Neukonfigurationen abhängen. Der Zeitpunkt, wann eine Konfiguration

innerhalb eines Jahres durchgeführt wird, ist für die Verfügbarkeit eines Weitverkehrsnetzes und die definierten Dienstgütekriterien der gerouteten Dienste entscheidend. Die Umkonfigurationen von Netzkomponenten, wie zum Beispiel ein Software-Update oder die Konfiguration von Routingprotokollen, führen zu kurzen Netzunterbrechungen, die ebenfalls zur Ausfallzeit von Diensten mit Dienstgütekriterien beitragen. Zur Berechnung der Gesamtverfügbarkeit eines Dienstes muss deshalb zu den fehlerbedingten Ausfallzeiten auch die Ausfallzeiten durch Konfigurationswechsel addiert werden.

Die zeitliche Abhängigkeit der Konfigurationswechsel verdeutlicht das folgende Beispiel. In einem Weitverkehrsnetz wird ein Dienst angeboten, dessen Unverfügbarkeit pro Jahr maximal 10 Minuten betragen darf. Es wird angenommen, dass ein Konfigurationswechsel und der anschließende Neustart der Netzkomponenten zwei Minuten benötigen. Damit trägt eine Umkonfiguration zwei Minuten zur Ausfallzeit des Dienstes bei. Zwei verschiedene Szenarien werden im Folgenden betrachtet.

In den ersten vier Monaten eines Jahres erfolgen drei Konfigurationswechsel, die den Dienst beeinträchtigen und die Unverfügbarkeit des Dienstes auf sechs Minuten erhöhen. In der Mitte des Jahres kommt es zu einem Netzausfall der fünf Minuten dauert und ebenfalls den Dienst beeinträchtigt. Die gesamte Unverfügbarkeit des Dienstes liegt damit bei 11 Minuten und überschreitet den vertraglich festgesetzten Wert von 10 Minuten. Der Netzbetreiber muss in diesem Fall Strafzahlungen an den Kunden leisten.

Im zweiten Fall finden nur zwei Konfigurationen vor dem Netzausfall statt. Die Konfigurationswechsel und der Ausfall addieren sich zu einer Unverfügbarkeit des Dienstes von neun Minuten und liegen unterhalb der festgelegten Grenze. Am Ende des Jahres soll eine weitere Neukonfiguration durchgeführt werden, die den Dienst beeinträchtigen würde. Da es sich bei dem Konfigurationswechsel um eine Optimierung der Ressourcenauslastung und um keine Behebung eines Netzfehlers handelt, wird der Konfigurationswechsel nicht ausgeführt. Auf diese Weise wird die Verletzung des Dienstgütekriteriums vermieden.

Das Beispiel zeigt, dass ein Konfigurationswechsel abhängig von der Vorgeschichte und dem aktuellen Zeitpunkt unterschiedlich bewertet werden muss. Die Bewertung erfolgt anhand des Kostenmodells, das virtuelle Kosten abhängig vom Zeitpunkt eines Jahres einführt und anhand eines Schwellenwerts entscheidet, ob eine Netzkonfiguration verändert wird. Dazu werden zwei Szenarien unterschieden, die im Folgenden erläutert werden.

Nicht optimaler Netzzustand und Einhaltung der Dienstgütekriterien

Im ersten Szenario hat sich der Netzzustand verändert, ohne dass ein Fehler aufgetreten ist. Ein höheres Verkehrsaufkommen oder eine veränderte Verkehrsmatrix, die keine Linkkapazitäten überschreiten, entsprechen solch einem Fall. Aufgrund der veränderten Netzsituation, berechnet der Planungsalgorithmus des Planungsmoduls

eine neue optimale Konfiguration und leitet diese an das Konfigurationsmodul weiter. Das Kostenmodell entscheidet anschließend anhand der einzelnen Kostenparameter, ob es die neue Konfiguration anwendet.

Mit Formel 6.1 werden zunächst die Kosten einer Verletzung der Dienstgütekriterien berechnet. Das Zeitintervall t_{def} wird in den Geschäftsregeln festgelegt und gibt an, wie hoch die Strafzahlungen innerhalb eines definierten Zeitintervalls sind.

$$c_{SLA} = \frac{1}{t_{def}} \cdot c_{Strafe} \cdot t_{konfig} \tag{6.1}$$

Es wird davon ausgegangen, dass die Strafzahlungen c_{SLA}, abhängig von der maximal definierten Ausfallzeit pro Dienst und den Kosten für eine Verletzung der Dienstgüte c_{Strafe}, linear mit der Zeitdauer ansteigen. Zusätzlich zu den Kosten durch die Strafzahlungen entstehen noch virtuelle Kosten, die vom Zeitpunkt innerhalb eines Jahres abhängen.

$$c_{virtuell} = \sum_{\forall l \in P} l \cdot c_{SLA} \cdot (1 - \frac{t_{aktuell}}{t_{Jahr}}) \tag{6.2}$$

Die virtuellen Kosten $c_{virtuell}$ berechnen sich aus der Anzahl der von dem Konfigurationswechsel betroffenen Pfade, den Kosten einer Verletzung der Dienstgüte der betroffenen Dienste und dem Zeitpunkt innerhalb eines Jahres. Die Kosten entsprechen zu Beginn eines Jahres der Höhe der vereinbarten Strafzahlung und nehmen anschließend linear über die Zeit ab. Die höheren Kosten zu Beginn eines Jahres verhindern ein ständiges Neukonfigurieren des Netzes, wenn es sich um eine reine Optimierung der Lastverteilung innerhalb des Netzes handelt. Gegen Ende eines Jahres werden Umkonfigurationen zur Verbesserung der Lastverteilung kostengünstiger, wenn sie keine Verletzung der Dienstkriterien hervorrufen.

Die Gesamtkosten der Konfiguration berechnet sich schließlich aus der Summe der Kosten der Strafzahlungen und der virtuellen Kosten.

$$c_{neukonfig} = c_{SLA} + c_{virtuell} \tag{6.3}$$

Liegen die Gesamtkosten der Umkonfiguration unterhalb eines definierten Schwellwerts, wird die neue Konfiguration aktiviert, ansonsten wird die alte Konfiguration beibehalten. Eine nicht durchgeführte Umkonfiguration wird solange in der Managementdatenbank gespeichert, wie sich die aktuelle Netzsituation nicht verändert. Das Verifikationsmodul überprüft in regelmäßigen Intervallen die Netzkonfiguration und veranlasst gegebenenfalls zu einem späteren Zeitpunkt die Umkonfiguration. Die Gesamtkosten der Neukonfiguration reduzieren sich über die Zeit und ermöglichen daher die Umkonfiguration zu einem späteren Zeitpunkt.

Betriebseinschränkungen und Dienstgütekriterien verletzt

Ein anderes Verhalten ergibt sich, wenn ein Netzfehler aufgetreten ist, der zum Ausfall von Netzkomponenten führt und deshalb bestimmte Dienste im Weitverkehrsnetz beeinträchtigt. Die Neukonfiguration dient dann nicht zur Optimierung der Linkauslastung, sondern zur Behebung des Fehlers und zur Wiederherstellung der Verfügbarkeit der Dienste. In diesem Szenario müssen zwei Fälle zur Berechnung der Kosten eines Ausfalls unterschieden werden. Zum einen die Kosten, welche entstehen, wenn keine Neukonfiguration durchgeführt wird und zum anderen, die Kosten, die bei der Neukonfiguration des Netzes entstehen. Ein Vergleich der beiden Kosten entscheidet, ob sich eine Umkonfiguration lohnt oder der Netzbetreiber die alte Konfiguration bis zur Reparatur des Fehlers beibehält. Mit Formel 6.4 erfolgt die Berechnung der Strafzahlungen c_{SLA}.

$$c_{SLA} = \frac{1}{t_{def}} \cdot c_{Strafe} \cdot t_{reparatur} \tag{6.4}$$

Die Kosten für die Strafzahlungen setzen sich aus der festgeschriebenen Strafzahlung pro Zeitdauer für einen Dienstausfall und der tatsächlichen Reparaturdauer des Fehlers zustande. Die Höhe der Kosten werden maßgeblich durch die Reparaturdauer bestimmt.

Erfolgt aufgrund eines Fehlers ein Konfigurationswechsels von Teilbereichen des Weitverkehrsnetzes, entstehen sowohl Kosten durch den Ausfall des Dienstes als auch virtuelle Kosten für die Konfiguration wie bereits im ersten Szenario dargestellt. Die Kosten der Neukonfiguration werden mit Formel 6.5 berechnet.

$$c_{neukonfig} = \frac{1}{t_{def}} \cdot c_{Strafe} \cdot t_{reparatur} + \sum_{\forall l \in P} l \cdot c_{SLA} \cdot (1 - \frac{t_{aktuell}}{t_{Jahr}}) \tag{6.5}$$

Die Kosten der Neukonfiguration $c_{neukonfig}$ bestehen aus den Kosten für die Strafzahlungen durch die Verletzung der Dienstgüte multipliziert mit der Konfigurationsdauer. Im Unterschied zur Berechnung in Formel 6.4 zählt hier nur die Konfigurationsdauer, da angenommen wird, dass nach der Umkonfiguration die ausgefallenen Dienste wieder verfügbar sind. Die virtuellen Kosten der Konfiguration setzen sich wiederum aus den Kosten für die Strafzahlungen und dem Zeitpunkt der Konfiguration innerhalb eines Jahres zusammen.

Vergleich der Kosten der aktuellen und der neuen Konfiguration

Die im vorherigen Abschnitt betrachteten Kosten für einen Konfigurationswechsel werden mit den Kosten der aktuellen Konfiguration verglichen, um zu entscheiden, ob der Konfigurationswechsel durchgeführt wird. Für die Berechnung der Gesamtkosten der aktuellen und neuen Konfiguration des Weitverkehrsnetzes werden den

benutzten Linkkapazitäten Kosten zugeordnet. Dazu wird die in Abbildung 6.3 gezeigte Kurve verwendet, welche die Kosten der freien Linkkapazität in Abhängigkeit von der momentanen Auslastung des Links angibt.

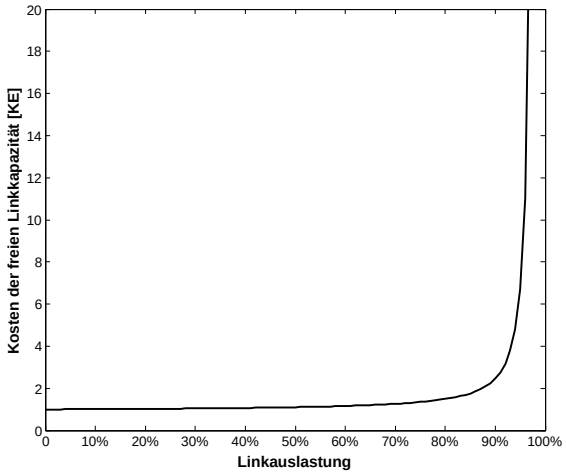


Abbildung 6.3: Kosten, um freie Kapazität eine Links zu benutzen

Die Kostenkurve ist an die Verkehrstheorie von Kommunikationsnetzen angelehnt und orientiert sich dabei an der mittleren Wartezeit der Anforderungen in einem M/M/1-Modell [Kle75]. Das bedeutet, je höher die Auslastung eines Links ist, desto höher sind für eine neue Anforderung die Kosten, die noch freie Kapazität zu verwenden. Basierend auf der Kostenkurve werden die Gesamtkosten der aktuellen Konfiguration $c_{NK,current}$ berechnet.

$$c_{NK,current} = \sum_{\forall l \in L} c_{l,cap} \tag{6.6}$$

Die Kosten der aktuellen Konfiguration setzen sich aus der Summe der Kosten der einzelnen Linkkapazitäten eines Weitverkehrsnetzes zusammen. Die Entscheidung, ob ein Konfigurationswechsel in einem Weitverkehrsnetz durchgeführt wird, erfolgt anhand eines Vergleichs der aktuellen und zukünftigen Kosten des Netzes.

$$c_{neukonfig} + c_{NK,Neu} \leq c_{NK,Aktuell} \tag{6.7}$$

Dazu werden die Konfigurationskosten $c_{neukonfig}$ und die Kosten für die neue Konfiguration $c_{NK,Neu}$ addiert und mit den Kosten der aktuellen Netzkonfiguration $c_{NK,Aktuell}$ verglichen. Fallen die Kosten für die Summe der Einzelkosten in Formel 6.7 kleiner aus als die Kosten der aktuellen Konfiguration, wird der Konfigurationswechsel durchgeführt. Erfolgt aufgrund der höheren Kosten keine Umkonfiguration, bleibt das Netz im alten Zustand, bis der Fehler repariert ist.

Ein Beispiel, bei dem ein Konfigurationswechsel nach dem Auftreten eines Fehlers höhere Kosten verursacht, ist der Ausfall eines oder mehrerer Links, auf denen Ver-

kehrsanforderungen ohne bestimmte Dienstgütekriterien geroutet werden. Besitzen die übrigen Links eine hohe Auslastung, ist ein umrouten der betroffenen Dienste nicht möglich, ohne die Dienste auf den intakten Links zu beeinträchtigen. Handelt es sich auf den intakten Links um Verkehrsanforderungen bestimmter Dienstgüte, führt eine Beeinträchtigung dieser Dienste zu Strafzahlungen. Abhängig von der Reparaturdauer bewirkt ein Konfigurationswechsel höhere Kosten und wird nicht durchgeführt.

6.2.2 Einfluss der Kostenfunktion auf die Konfigurationswechsel

In diesem Abschnitt wird der Einfluss des Kostenmodells auf die Konfigurationswechsel in einem Weitverkehrsnetz betrachtet. Als Referenznetz wird das Deutschland-50-Knotennetz verwendet. Zur Berechnung der Ersatzkonfigurationen werden die in Kapitel 6.3 und 6.4 entwickelten Optimierungsansätze verwendet. Zusätzlich wird das im vorherigen Abschnitt vorgestellte Kostenmodell zur Bewertung der Konfigurationen verwendet.

Es wird ein Simulationszeitraum von einem Jahr betrachtet, innerhalb dessen regelmäßig Netzveränderungen auftreten. Folgende Netzänderungen werden während der Simulation betrachtet:

- Erhöhung der Verkehrsanforderungen auf einem oder mehreren Links
- Erhöhung der Verzögerung auf einem oder mehreren Pfaden
- Erhöhung der Blockierung an einem oder mehreren Knoten

Die Fehlerereignisse sind zufällig zwischen Null und 10 innerhalb eines Monats verteilt. Die Konfigurationsdauer hängt von der Anzahl der zu konfigurierenden Netzknoten ab und liegt zwischen 30 Sekunden und 10 Minuten pro Konfigurationswechsel. Jedem Fehlerereignis wird eine zufällige Konfigurationsdauer mitgeliefert. Um eine statistische Aussage über die Anzahl der Konfigurationen und die tatsächlich aufgetretenen Veränderungen machen zu können, werden 50 Wiederholungen der Simulation durchgeführt. Die Mittelwerte als auch die Standardabweichung werden auf ganze Zahlen aufgerundet. Die Ergebnisse sind in Abbildung 6.4 dargestellt.

Darin sind die mittlere Anzahl an Fehlerereignissen und die tatsächlich durchgeführten Konfigurationen pro Monat dargestellt. Ohne Verwendung der Kostenfunktion führen 91,66% der Fehlerereignisse zu einer Neukonfiguration des Netzes. Nicht alle simulierten Fehlerereignisse führen zu einem Konfigurationswechsel, da trotz einer Veränderung des Netzzustandes die aktuelle Konfiguration optimal ist. Eine geringfügige Veränderung des Verkehrsaufkommens ist hierfür ein Beispiel.

Mit der Verwendung der Kostenfunktion reduziert sich die Anzahl der tatsächlich durchgeführten Konfigurationen. Vor allem zu Beginn eines Jahres finden deutlich weniger Konfigurationen statt als ohne Kostenfunktion. Am Ende des Jahres erhöht sich die Anzahl der Konfigurationen, da die virtuellen Kosten und damit die Gesamtkosten einer Konfiguration sinken. Damit erreicht die Kostenfunktion das Ziel,

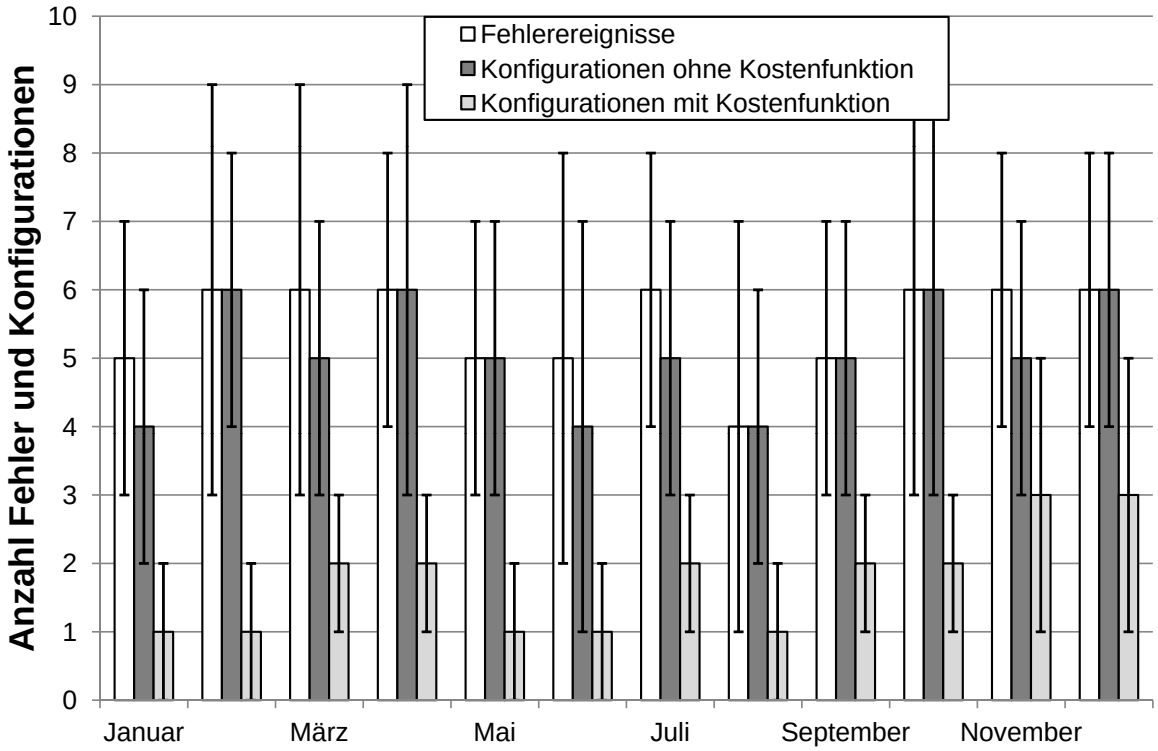


Abbildung 6.4: Anzahl der Fehlerereignisse und Anzahl der durchgeführten Konfigurationen

zu Beginn eines Jahres die Anzahl der Konfigurationen zu verringern und auf die notwendigen Konfigurationen zu begrenzen.

6.3 Planungsprozess und Optimierungsalgorithmen des Planungsmoduls

In diesem Abschnitt werden die entwickelten Planungsprozesse, die vom Planungsmodul des Netzmanagements verwendet werden, eingehend dargestellt. Das Planungsmodul verwendet drei unterschiedliche Prozesse. Zunächst gibt es einen übergeordneten Prozess, der durch jede veränderte Netzsituation angestoßen wird und eine Lösung finden soll. Daneben existieren zwei Planungsprozesse, die zur Berechnung einer optimalen Lösung verwendet werden. Der Langzeit-Planungsprozess berechnet mittels ganzzahliger linearer Optimierung Ersatzkonfigurationen für vorab definierte Netzänderungen. Der Kurzzeit-Planungsprozess verwendet zur schnellen Optimierung eine Heuristik, falls keine geeignete Ersatzkonfiguration in der Managementdatenbank vorhanden ist.

6.3.1 Prozessablauf bei Veränderung des Netzzustandes

In Abbildung 6.5 ist der Prozessablauf innerhalb des Planungsmoduls dargestellt, der nach einer veränderten Netzsituation angestoßen wird. Den Anfangszustand stellt die aktuelle fehlerfreie Konfiguration des Weitverkehrsnetzes dar. Die gestrichelten Pfeile bezeichnen empfangene Informationen von den anderen Modulen des Netzmanagements.

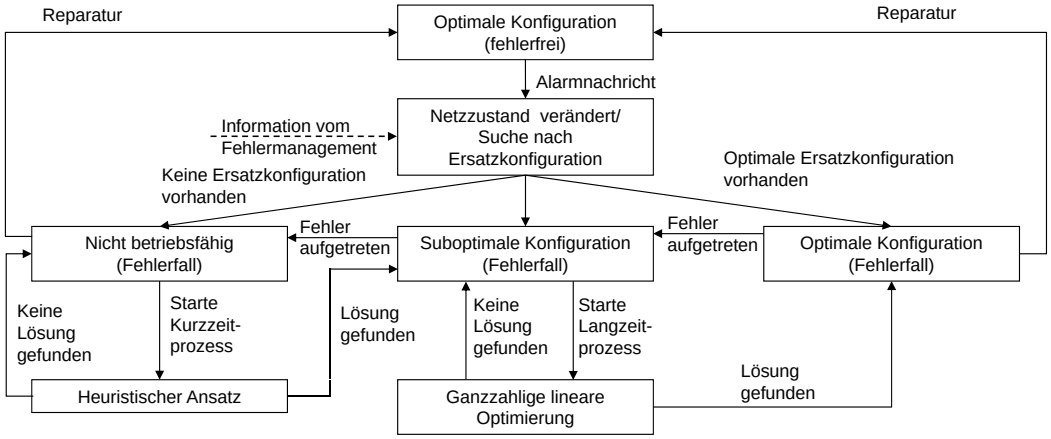


Abbildung 6.5: Prozessablauf nach einer Zustandsänderung des Netzes

Das Fehlermanagementmodul teilt dem Planungsmodul eine detektierte Änderung des Netzzustands mit. Daraufhin wird die Suche nach einer optimalen Ersatzkonfiguration angestoßen. Abhängig von dem aufgetretenen Ereignis erfolgt der Übergang in die Zustände „Optimal (Fehlerfall)“, „Suboptimal (Fehlerfall)“ oder „Nicht-Betriebsfähig (Fehlerfall)“.

In den Zustand „Optimal (Fehlerfall)“ gelangt der Prozess, wenn zu einem aufgetretenen Fehler die entsprechende optimale Ersatzkonfiguration vorhanden ist. Der Zustand „Suboptimal (Fehlerfall)“ bedeutet, dass eine Ersatzkonfiguration gefunden wurde, die aber nicht optimal ist. Ein Beispiel hierfür ist der Ausfall einer einzelnen Wellenlänge auf einem Link. Um den Fehler zu beheben, müssen nur die Verkehrsanforderungen einer Wellenlänge umgeleitet werden. Die Ersatzkonfiguration, die alle Verkehrsanforderungen von allen Wellenlängen umleitet, behebt ebenfalls den Fehler. Sie ist jedoch suboptimal, da der gesamte Verkehr auf dem Link umgeroutet wird und nicht nur der, der ausgefallenen Wellenlänge.

Befindet sich der Prozess in dem Zustand „Suboptimal (Fehlerfall)“ startet der Planungsprozess gegebenenfalls den Langzeitprozess, der die ganzzahlige lineare Optimierung beinhaltet. Findet die Optimierung eine Lösung, erfolgt jedoch keine automatische Umkonfiguration des Netzes, sondern anhand des entwickelten Kostenmodells wird zunächst evaluiert, ob sich eine Umkonfiguration lohnen würde. Eine Umkonfiguration wird durchgeführt, falls die Kosten der Umkonfiguration plus die Kosten der neuen Konfiguration niedriger als die Kosten der aktuellen Konfiguration sind. Bei einem betriebsfähigen Netz hängt der Übergang des Prozesses

von dem Zustand „Suboptimal (Fehlerfall)“ in den Zustand „Optimal (Fehlerfall)“ von verschiedenen Faktoren wie der Dauer des Fehlers, der Anzahl der betroffenen Dienste sowie der Anzahl der bereits erfolgten Umkonfigurationen innerhalb eines Jahres ab.

Findet der Planungsprozess nach einer Netzänderung keine geeignete Ersatzkonfiguration zur Behebung des Fehlers, geht der Prozess in den Zustand „Nicht-Betriebsfähig (Fehlerfall)“ über. Der Zustand „Nicht-Betriebsfähig (Fehlerfall)“ gibt an, dass ein oder mehrere Dienste nicht mehr geroutet werden können. In diesem Fall wird der Kurzzeit-Planungsprozess gestartet, der eine Heuristik verwendet, die basierend auf der letzten gültigen Netzkonfiguration eine Lösung für den aktuellen Fehlerfall sucht. Eine Heuristik findet bei geeigneten Startwerten in der Regel schneller eine Lösung als eine ganzzahlige lineare Optimierung. Allerdings kann nicht garantiert werden, dass die Heuristik die optimale Lösung findet. Hat die Heuristik eine Lösung gefunden, geht der Prozess in den Zustand „Suboptimal (Fehlerfall)“ über. Führt die Heuristik zu keiner Lösung, verweilt der Prozess im Zustand „Nicht-Betriebsfähig (Fehlerfall)“.

In den Zuständen „Optimal (Fehlerfall)“ und „Suboptimal (Fehlerfall)“ verweilt der Prozess bis der Fehler durch den Netzbetreiber behoben wird oder bis eine weitere Netzänderung auftritt. Tritt ein weiterer Fehler im Netz auf, geht der Prozess in den Zustand „Suboptimal (Fehlerfall)“ beziehungsweise „Nicht-Betriebsfähig (Fehlerfall)“ über und startet wiederum die Suche nach einer optimalen Ersatzkonfiguration. Durch eine physikalische Behebung des Fehlers durch den Netzbetreiber und der anschließenden Umkonfiguration des Netzes gelangt der Prozess wieder in den Ausgangszustand „Optimal (fehlerfrei)“ zurück.

Nach der Beschreibung des Prozessablaufs zur Behebung von detektierten Netzänderungen werden in den nächsten Abschnitten die zwei Planungsprozesse eingehend dargestellt, die zur Berechnung der optimalen Lösung verwendet werden.

6.3.2 Langzeitprozess zur Bestimmung der optimalen Ersatzkonfigurationen

Wie im Abschnitt 6.1 beschrieben, beinhaltet das Planungsmodul einen Langzeitplanungsprozess, der für die Vorausplanung der optimalen Ersatzkonfigurationen verantwortlich ist. Der Langzeit-Planungsprozess verwendet dafür eine ganzzahlige lineare Optimierung. Der Langzeit-Planungsprozess ist in Abbildung 6.6 dargestellt. Der Langzeit-Planungsprozess verwendet die Informationen über die aktuelle Netzsituation und berechnet optimale Ersatzkonfigurationen für potentielle zukünftige Netzsituationen. Zukünftige Netzsituationen sind alle Netzveränderungen, die in einem Weitverkehrsnetz auftreten können.

Wie später in Abschnitt 6.3.3 erläutert, wird aufgrund der Vielzahl unterschiedlicher zukünftiger Fehlerszenarien nicht für alle Fehlerszenarien eine Ersatzkonfiguration vorab berechnet. Daher werden die Ersatzkonfigurationen für zukünftige Szenarien

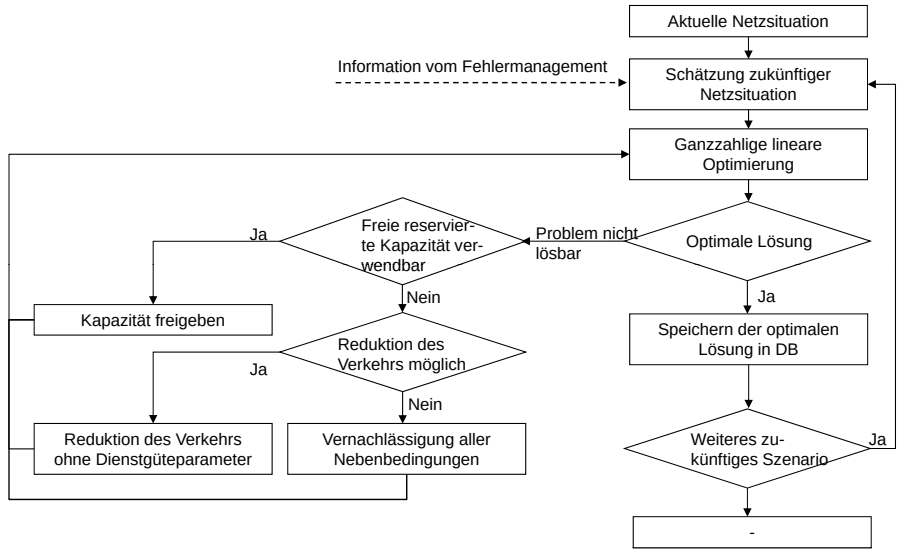


Abbildung 6.6: Langzeitprozess zur Planung der Ersatzkonfigurationen

nach der Wahrscheinlichkeit ihres Auftretens berechnet. Fehler die häufiger auftreten, wie zum Beispiel 1-Linkfehler oder Verkehrsveränderungen, werden zuerst berechnet. Anschließend erfolgt die Vorabberechnung für Knotenausfälle oder 2-Linkfehler.

Wie viele Ersatzkonfigurationen vorab berechnet werden können, hängt von der Optimierungszeit für die jeweiligen Fehlerszenarien und der Zeitdauer zwischen zwei Netzänderungen ab. Als weiterer Einflussparameter für die Berechnungsreihenfolge der Ersatzkonfigurationen dienen die Informationen aus dem Fehlermanagementmodul. Die Reihenfolge der vorab berechneten Ersatzkonfiguration ist allerdings nicht konstant, sondern wird durch die Auswertung der Konfigurationsfehler (Kapitel 4) und durch die aktuellen Degradationswerte der Netzkomponenten (Kapitel 5) beeinflusst. Wird ein Konfigurationsfehler identifiziert oder melden eine oder mehrere Netzkomponenten, dass sie ihre maximale Degradation erreicht haben, berechnet der Optimierungsalgorithmus zunächst für diese Fälle die Ersatzkonfigurationen.

Wie in Abbildung 6.6 dargestellt, berechnet der Langzeitprozess nacheinander die optimalen Ersatzkonfigurationen. Die verwendete ganzzahlige lineare Optimierung wird in Kapitel 7.1 detailliert beschrieben. Findet der Algorithmus eine optimale Lösung, speichert er diese in der Managementdatenbank ab und geht zum nächsten zukünftigen Szenario über. Sind keine weiteren Szenarien vorhanden, terminiert der Prozess bis er wieder durch ein neues Ereignis getriggert wird. Sind noch weitere Szenarien vorhanden, werden diese nacheinander abgearbeitet und für jedes zukünftige Netzszenario eine optimale Ersatzkonfiguration berechnet.

Abhängig von den Nebenbedingungen und dem zukünftigen Netzszenario kommt es in bestimmten Fällen vor, dass der Optimierungsalgorithmus keine Lösung findet. Ist das Optimierungsproblem nicht lösbar, verringert der Planungsprozess zunächst die Verkehrslast innerhalb des Netzes. Die Reduzierung betrifft allerdings nur Verkehr

ohne Dienstgütekriterien, um Strafzahlungen zu vermeiden. Ist eine Reduzierung des Verkehrs möglich, findet eine neue Optimierung mit den geänderten Verkehrswerten statt. Falls es eine optimale Lösung für das angepasste Szenario gibt, wird diese anschließend in der Managementdatenbank gespeichert und das nächste Szenario für die Optimierung ausgewählt.

Findet die Optimierung für eine Optimierungsaufgabe keine Lösung und kann der Verkehr ebenfalls nicht reduziert werden, versucht der Planungsprozess einzelne Nebenbedingungen des Optimierungsproblems zu lockern. Beispielsweise wird eine vorhandene Kapazitätsbegrenzung vernachlässigt und anschließend die Optimierung mit den veränderten Nebenbedingungen neu gestartet. Der Planungsprozess überprüft auf diese Weise sämtliche Nebenbedingungen des Optimierungsproblems und versucht sie gegebenenfalls zu relaxieren. Führt eine der Optimierungen zu einer Lösung, wird diese mit den Informationen über die veränderten Nebenbedingungen in der Managementdatenbank gespeichert.

Allerdings kann auch mit der Relaxierung von Nebenbedingungen nicht für alle zukünftigen Netzszenarien eine optimale Ersatzkonfiguration berechnet werden. Der gleichzeitige Ausfall von zwei oder mehreren Links reduziert die vorhandene Netzkapazität derart, dass eventuell nicht mehr alle Verkehrsanforderungen geroutet werden können. Da es sich bei dem Langzeit-Planungsprozess um eine Vorausplanung von zukünftigen Szenarien handelt, erfolgt im letzten Schritt des Planungsprozess eine Optimierung, bei der bestimmte Nebenbedingungen weggelassen werden, um eine optimale Lösung zu finden. So wird beispielsweise die maximal installierte Linkkapazität vernachlässigt. Die Lösung der vereinfachten Optimierung wird anschließend an den Netzbetreiber gesendet, um ihn darüber zu informieren, wie er das Netz aufrüsten muss, um die zukünftigen Änderungen zu bewältigen.

6.3.3 Vorab geplante Fehlerszenarien

Die Anzahl der vorausgeplanten Ersatzkonfigurationen hängt von zwei Faktoren ab. Zum einen wie lange die Optimierung einer Ersatzkonfiguration dauert, zum anderen wie viel Zeit insgesamt zur Optimierung zur Verfügung steht. Die gesamte verfügbare Optimierungszeit zur Berechnung aller Ersatzkonfigurationen hängt davon ab, wie häufig sich die Netzsituation in einem Weitverkehrsnetz verändert. Im Folgenden wird das Deutschland-17-Knoten-Netz als Referenznetz verwendet, um die Anzahl der Ersatzkonfigurationen und die benötigte Speichergröße zu berechnen.

Das Deutschland-17-Knotennetz besteht aus 17 Knoten und 26 Kanten. In Tabelle 6.2 sind sechs verschiedene zukünftige Szenarien aufgeführt, die für die Vorausplanung der Ersatzkonfiguration in Frage kommen. Die vorab berechneten Fehler bestimmen sich nach deren Auftrittswahrscheinlichkeiten, die anhand der gemessenen Fehler in [LAJ98] berechnet wurden.

1-Linkfehler stellen die häufigsten Fehler in heutigen Weitverkehrsnetzen dar, weshalb für alle potentiellen Linkausfälle die Ersatzkonfigurationen vorausgeplant wer-

Ersatzkonfiguration für	Anzahl
1-Linkfehler	26
2-Linkfehler	325
3-Linkfehler	2600
Knotenfehler	17
Knoten- und Linkfehler	4680
Verändertes Verkehrsaufkommen	544
Gesamtanzahl	8192

Tabelle 6.2: Mit Hilfe der linearen Optimierung vorausgeplante Fehlerszenarien

den. Für das Deutschland-17-Knotennetz ergeben sich 26 verschiedene Ersatzkonfigurationen. Erweitert man die Ersatzkonfigurationen auch auf 2- beziehungsweise 3-Linkfehler so ergeben sich weitere 2925 Ersatzkonfigurationen, die vorausberechnet werden. Neben den Linkfehlern werden auch für Knotenfehler vorab Ersatzkonfigurationen berechnet, da diese eine erhebliche Auswirkung auf das Netz haben und daher eine schnelle Reaktion erfordern. Im Vergleich zu Linkfehlern kommt es bei Knotenfehlern immer zu Verkehrsverlusten, da alle an diesem Knoten angeschlossenen Kunden nicht mehr mit dem Weitverkehrsnetz verbunden sind. Darüber hinaus werden auch die Kombinationen aus Knoten und 1-Linkfehler vorausgeplant. Ein weiteres zukünftiges Szenario ist der Anstieg der Verkehrsanforderungen in einem Weitverkehrsnetz. Der Abschätzung der benötigten Speicherkapazität erfolgt im nächsten Abschnitt.

6.3.4 Speicherkapazität der Ersatzkonfigurationen

Betrachtet man alle aufgezählten Ersatzkonfigurationen des vorangegangenen Beispiels, ergeben sich 8192 verschiedene Ersatzkonfigurationen. Um die benötigte Speichergröße aller Ersatzkonfigurationen zu berechnen, wird angenommen, dass eine Konfigurationsdatei für einen Router maximal 1 MByte benötigt. Die maximale Speichergröße für eine vollständige Ersatzkonfiguration benötigt somit 17 MByte im Fall des Deutschland-17-Knotennetzes. Zur Speicherung aller in Tabelle 6.2 aufgeführten zukünftigen Szenarien werden somit 139,26 GByte benötigt. Diese Datenmenge stellt für heutige Speichersysteme keine Herausforderung dar. Eine größere Rolle spielt die Optimierungszeit die für alle Ersatzkonfigurationen benötigt wird und die Frequenz mit der sich der Zustand eines Netzes ändert.

Liegt die mittlere Optimierungszeit pro Ersatzkonfiguration beispielsweise bei 10 Minuten, dauert der gesamte Optimierungsprozess für alle Ersatzkonfigurationen bei sequentieller Berechnung 57 Tage. Im Vergleich zur Frequenz der Veränderungen in einem Weitverkehrsnetz, die in wesentlich kürzeren Abständen eintreten, dauert der Planungszyklus damit sehr lange. Ändert sich die Netzsituation während der Planung der Ersatzkonfigurationen, sind alle bereits geplanten Ersatzkonfigurationen nicht mehr aktuell und müssen erneut berechnet werden. Es besteht die Herausforde-

rung, abhängig von der Änderungshäufigkeit in einem Weitverkehrsnetz, die Anzahl der Ersatzkonfigurationen zu bestimmen, die in einem vorgegebenen Zeitrahmen berechnet werden können. Findet die Planung der optimalen Ersatzkonfigurationen parallel statt, können weitaus mehr potentielle Fehlerfälle im Voraus geplant werden. Ein Netzbetreiber der für sein Netzmanagementsystem ein Rechenzentrum betreibt, verfügt über die Ressourcen, Optimierungen parallel durchführen zu können. Die in Kapitel 7 berechneten Werte werden deshalb als obere Zeitgrenze betrachtet.

In Kapitel 7 werden die Optimierungen aufgrund der verfügbaren Ressourcen sequentiell durchgeführt. Daher werden in dem Planungsmodul des Netzmanagementsystems die Netzsituationen vorausgeplant, die am wahrscheinlichsten sind. Zwei detaillierte Studien über Fehlerstatistiken in Netzen [LAJ98] und [Ati05] zeigen, dass Linkfehler die am häufigsten auftretenden Fehler in heutigen Weitverkehrsnetzen darstellen. Darüber hinaus treten ebenso Elektronik- und Wartungsfehler sowie Stromausfälle von Komponenten häufig auf. Wie in Grubers Dissertation [Gru07] gezeigt, können aus den Unverfügbarkeiten der Netzkomponenten und der Anzahl der Knoten und Kanten in einem Transportnetz die Fehlerwahrscheinlichkeiten für die einzelnen Fehlerereignisse berechnet werden. Das Fehlermanagementmodul verwendet die Auftrittswahrscheinlichkeiten zur Bestimmung der Berechnungsreihenfolge der Ersatzkonfigurationen. Die Reihenfolge kann aber durch einen auftretenden Fehler im Netz unterbrochen werden, um auf den aktuellen Fehler zu reagieren. Zum Beispiel das Auftreten von Netzanomalien, die den Netzbetrieb beeinträchtigen, aber nicht zu einem Ausfall führen, werden dann bevorzugt behandelt. Eine Untersuchung der Optimierungszeiten für verschiedene Fehlerszenarien erfolgt in Kapitel 7.

6.4 Online-Planung im Fehlerfall

Wie in Kapitel 6.3 dargestellt können nicht alle potentiellen Netzszenarien vorausgeplant werden. Für das Deutschland-17-Knotennetz ergeben sich bereits bei der Betrachtung von 1- und 2-Linkfehlern, Knotenfehlern und der Kombinationen aus den Einzelfehlern über 4000 Ersatzkonfigurationen. Ein geeigneter Optimierungsalgorithmus berechnet die erforderliche Anzahl an Ersatzkonfigurationen eventuell noch in einer adäquaten Zeit. Betrachtet man allerdings zusätzlich das gleichzeitige Auftreten von zwei Netzfehlern und die Unterscheidung von Wellenlängenfehlern auf den Links, steigt die Anzahl von Ersatzkonfigurationen in dem Beispielnetz auf über drei Millionen. Selbst mit parallel laufenden Optimierungen, die nur wenige Sekunden für eine Lösung benötigen, können in adäquater Zeit nicht alle Ersatzkonfigurationen berechnet werden.

Deshalb verwendet das Planungsmodul des teilautomatisierten Netzmanagements neben den Langzeit-Planungsprozess auch noch ein Kurzzeit-Planungsprozess, um schnell auf eine veränderte Netzsituation zu reagieren, für die keine geeignete Ersatzkonfiguration vorhanden ist. Der Kurzzeit-Planungsprozess ist in Abbildung 6.7 dargestellt und zeigt die einzelnen Zustände des Prozesses.

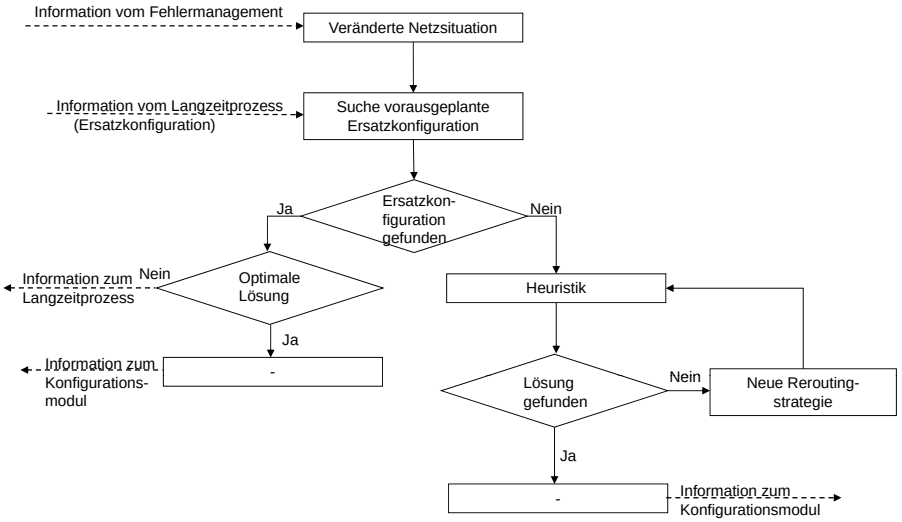


Abbildung 6.7: Kurzzeitprozess für die Online-Planung

Wenn eine Netzänderung durch das Fehlermanagementmodul mitgeteilt wird, sucht der Planungsprozess zunächst eine optimale Ersatzkonfiguration in der Managementdatenbank. Existiert eine geeignete Ersatzkonfiguration, wird diese an das Konfigurationsmodul des Netzmanagementsystems übergeben und der Kurzeitprozess terminiert. Findet der Suchalgorithmus eine Ersatzkonfiguration in der Managementdatenbank, die nicht die optimale Lösung für die veränderte Situation darstellt, aber den Fehler behebt, wird diese verwendet.

Nachdem die nicht optimale Ersatzkonfiguration an das Konfigurationsmodul übergeben wurde, erfolgt eine Planung mit Hilfe der ganzzahligen linearen Optimierung oder der Heuristik die im Kapitel 7 detailliert beschrieben werden. Welche Optimierungsmethode verwendet wird, hängt von dem aktuellen Fehler und der gefundenen Ersatzkonfiguration ab. Handelt es sich um einen physikalischen Fehler, dessen Reparatur aufwendiger ist und daher länger dauert, ist der Einsatz der ganzzahligen linearen Optimierung möglich. Findet eine der Optimierungsmethoden eine Lösung für die aktuelle Fehlersituation, die sich näher am Optimum befindet als die aktuell verwendete Ersatzkonfiguration, sendet das Planungsmodul die Information wiederum an das Konfigurationsmodul. Der Netzbetreiber entscheidet anschließend, ob die neue Ersatzkonfiguration aktiviert wird. Eine erneute Umkonfiguration hängt von verschiedenen Faktoren wie Dauer des Fehlers, Anzahl der neu zu konfigurierenden Netzkomponenten und die Auswirkung des Fehlers auf die Dienste ab.

Die Heuristik innerhalb des Kurzzeit-Planungsprozesses wird in Fehlerfällen angewandt, für die keine Ersatzkonfigurationen in der Managementdatenbank existieren. Mittels der Heuristik wird eine Lösung basierend auf der aktuellen Netzkonfiguration berechnet. Die neue Netzkonfiguration, die den aufgetretenen Fehler behebt, sollte sich nicht allzu sehr von der aktuellen Netzkonfiguration unterscheiden, so dass diese einen guten Startwert für die Heuristik liefert. Findet die Heuristik eine Ersatzkonfiguration, wird diese an das Konfigurationsmodul übergeben. Die Lösung wird

ebenfalls dem Langzeitprozess zur Verfügung gestellt, der abhängig vom Fehlerfall und der zur Verfügung stehenden Zeit eine optimale Ersatzkonfiguration berechnet. Findet die Optimierung eine Lösung, wird anhand des Kostenmodells oder durch den Netzbetreiber entschieden, ob der Konfigurationswechsel durchgeführt wird.

6.5 Zusammenfassung

In diesem Kapitel wurde das teilautomatisierte Netzmanagementsystem vorgestellt. Dieses besteht aus unabhängigen automatisierten Modulen, die alle Funktionalitäten eines Netzmanagements abbilden. Eine Kontrollschleife sorgt für eine kontinuierliche Überwachung des Netzes und gewährleistet eine schnelle Reaktion auf Veränderungen in einem Weitverkehrsnetz. Das Fehlermanagementmodul beinhaltet die Fehlersuche und Fehlerklassifizierung. Dazu verwendet es die Methoden aus den Kapiteln 4 und 5.

Für die Fehlerbehebung in einem Weitverkehrsnetz ist das Planungsmodul zuständig. Das Planungsmodul besteht aus drei Prozessen die eine schnelle Berechnung einer Lösung gewährleisten. Der Hauptprozess wird durch das Fehlermanagementmodul getriggert und ist für die Aktivierung des Langzeit- und Kurzzeit-Planungsprozesses zuständig. Des Weiteren leitet der Hauptprozess die berechneten Lösungen an das Konfigurationsmodul weiter und speichert die berechneten Ersatzkonfigurationen in der Managementdatenbank. Die Teilautomatisierung des Netzmanagements bezieht sich auf die manuelle Konfiguration durch den Netzbetreiber. Das Planungsmodul teilt dem Netzbetreiber die gefundenen Lösungen für einen Fehler mit und der Netzbetreiber entscheidet anschließend, ob die neue Konfiguration aktiviert wird.

Um die Konfiguration eines Netzes ebenfalls automatisch durchzuführen, wurde ein Kostenmodell für einen Konfigurationswechsel entwickelt. Anhand des Kostenmodells evaluiert das Netzmanagement die Kosten der aktuellen und der neuen Konfiguration und entscheidet anhand eines Vergleichs mit einem Schwellenwert, ob der Konfigurationswechsel durchgeführt wird. Die Ergebnisse der Simulationen zeigen, dass durch das Kostenmodell die Anzahl der Umkonfiguration reduziert und unnötige Konfigurationen verhindert werden.

Im letzten Abschnitt wurden die zwei Planungsprozesse zur Optimierung des Netzes entwickelt. Der Langzeit-Planungsprozess verwendet eine ganzzahlige lineare Optimierung zur Berechnung der Ersatzkonfigurationen und wird im fehlerfreien Fall des Weitverkehrsnetzes kontinuierlich durchlaufen. Die Ersatzkonfigurationen werden in der Reihenfolge der Auftrittswahrscheinlichkeiten der Fehler berechnet. Dabei gibt es keine Beschränkung der Anzahl der Ersatzkonfigurationen. Die maximale Anzahl an Ersatzkonfigurationen wird durch die Berechnungszeiten des Optimierungsalgorithmus und die Zeitdauer zwischen zwei Netzveränderungen bestimmt. Abschließend wurde der Langzeit-Planungsprozess durch einen Kurzzeit-Planungsprozess erweitert, der mittels einer Heuristik in adäquater Zeit eine Lösung für den Fehler berechnet.

7 Realisierung der Planungsprozesse

In diesem Kapitel werden die Planungsprozesse des Planungsmoduls beschrieben und anhand von Beispielnetzen untersucht. Als Eingangsparameter für die Planung werden die Verkehrsanforderungen verwendet, die in Kapitel 3 berechnet wurden. Zunächst erfolgt in Abschnitt 7.1 die Beschreibung der ganzzahligen linearen Optimierung, die für die Vorausplanung der Ersatzkonfigurationen zuständig ist. Anschließend werden anhand von Simulationen vorab definierte Konfigurationen vorausgeplant und die Zeitdauer der Optimierungen analysiert.

Im Abschnitt 7.2 wird auf den implementierten genetischen Algorithmus eingegangen. Dabei werden zunächst der Aufbau der Genome und deren Rekombinationsstrategien detailliert beschrieben. Anschließend wird die Fitnessfunktion und der Selektionsprozess erläutert, anhand derer die Kindgenerationen der Genome ausgewählt werden. Der letzte Teil des Abschnitts befasst sich mit der Simulation des genetischen Algorithmus in einem Weitverkehrsnetz. Anhand von verschiedenen Fehlerfällen wird die Fitness der Lösungen und die Zeitdauer bis eine gültige Lösung gefunden wird untersucht.

Der Abschnitt 7.3 untersucht das Zusammenspiel von Optimierung und Heuristik. Anhand von verschiedenen Fehlerszenarien wird die Reaktionszeit der Planungsprozesse simuliert und die gefundenen Lösungen analysiert. Zusätzlich wird die Stabilität des Netzmanagementsystems überprüft, indem in kurzen Zeitabschnitten unterschiedliche Fehler auftreten.

Im letzten Abschnitt des Kapitels wird eine Online-Planung auf *Reconfigurable Optical Add-Drop Multiplexer* (ROADM)s angewandt. In heutigen Weitverkehrsnetzen werden ROADMs eingesetzt, die ein flexibles Umschalten der Lichtpfade auf der optischen Ebene ermöglichen. Das flexible Hinzufügen eines Pfades, ermöglicht dem Netzbetreiber nachträglich Schutzpfade in einem Weitverkehrsnetz hinzuzufügen, ohne zusätzliche Hardware zu installieren. Die zusätzlichen Schutzpfade werden in der Online-Planung des Planungsmoduls verwendet, um im Fehlerfall eine schnelle Ersatzkonfiguration zu berechnen, die kein aufwendiges Umkonfigurieren erfordert. Die Optimierung und die Ergebnisse sind in Abschnitt 7.4 dargestellt.

7.1 Planungsalgorithmus zu Berechnung der Ersatzkonfigurationen

Zur Berechnung der vorausgeplanten Ersatzkonfigurationen wird eine ganzzahlige lineare Optimierung verwendet. Ziel der Optimierung ist es, das Routing aller Verkehrsanforderungen mit minimalen Kosten in einem veränderten Netzszenario zu finden. Der Optimierung stehen dabei nur die vorhandenen Netzressourcen zur Verfügung, die nach einem potentiellen Ausfall noch vorhanden sind.

Zunächst werden die kürzesten Pfade $p \in \mathbb{P}_D$ für alle Anforderungen $d \in \mathbb{D}$ nach dem Dijkstra Algorithmus [Dij59] berechnet und entsprechend ihrer Länge sortiert. Die verfügbaren Links des Netzes sind in der Menge $\mathbb{L}$ und die verfügbaren Knoten in der Menge $\mathbb{N}$ zusammengefasst. Über jeden Link wird eine bestimmte Anzahl an Wellenlängen w_l geroutet. Das Hauptziel der Optimierung ist die Minimierung der gesamten genutzten Kapazität eines Weitverkehrsnetzes.

$$\min \sum_{l \in \mathbb{L}} w_l, \quad w_l \in \{0; 1; 2; \dots\} \tag{7.1}$$

Das Optimierungsmodell beinhaltet folgende Nebenbedingungen, mit denen sichergestellt wird, dass beispielsweise die maximale Kapazität pro Link und die maximalen Verzögerungen bestimmter Verkehrsanforderungen eingehalten werden. Die binäre Variable $v_{d,p}$ bestimmt, welchen Pfad eine Verkehrsanforderung nimmt und die Bedingung 7.3 gewährleistet, dass jede Verkehrsanforderung zwischen einem Knotenpaar nur einen Pfad benutzt.

$$v_{d,p} \in 0{,}1, \quad \forall d \in \mathbb{D}, p \in \mathbb{P}_d \tag{7.2}$$

$$1 = \sum_{l \in \mathbb{L}} v_{d,p}, \quad \forall d \in \mathbb{D}, \tag{7.3}$$

Auf jedem Link dürfen maximal W_l Wellenlängen geroutet werden, was die Bedingung 7.4 sicherstellt.

$$\sum_{l \in \mathbb{L}} w_l \leq W_l \quad \forall l \in \mathbb{L} \tag{7.4}$$

In dem Weitverkehrsnetz existieren unterschiedliche Verkehrsklassen V_k, die eine bestimmte Dienstgüte besitzen. Die Bedingung 7.5 sorgt dafür, dass die maximal erlaubte Verzögerung v_{max} einer Verkehrsklasse nicht überschritten wird.

$$\sum_{p \in P_d : l \in p} v_l + \sum_{n \in p} v_k \leq v_{max} \quad \forall l \in \mathbb{L}, \forall v_k \in \mathbb{R}^+, v_{max} \in \mathbb{R}^+ \tag{7.5}$$

Die Verzögerungen auf einem Pfad setzen sich dabei aus den Verzögerungen der einzelnen Links v_l und den Verzögerungen innerhalb der Knoten v_k entlang eines Pfades zusammen. Für die Verzögerungen in den Knoten n wird abhängig von der Linklast eine konstante Verzögerung addiert, die sich an dem $M/M/1$ Wartemodell aus [Kle75] orientiert.

Auf bestimmten Links des Netzes existieren reservierte Kapazitäten beziehungsweise Wellenlängen W_r, die als Ersatzkapazitäten oder für bestimmte Verkehrsanforderungen mit garantierter Dienstgüte verwendet werden. Die Bedingung 7.6 stellt sicher, dass auf diesen Links nur die reduzierte Linkkapazität verwendet wird.

$$\sum_{l \in \mathbb{L}} w_l \leq (W_l - W_r) \quad \forall l \in \mathbb{L} \tag{7.6}$$

Findet der Optimierungsalgorithmus für bestimmte zukünftige Fehlerszenarien keine Lösung, da in dem Weitverkehrsnetz nicht genügend Kapazitäten für die Verkehrsanforderungen vorhanden sind, versucht der Planungsprozess bestimmte Nebenbedingungen zu relaxieren. Für die Relaxierung eignen sich die Nebenbedingungen 7.4 und 7.6, welche die maximale Kapazität pro Link bestimmen. Ist in einem potentiellen Fehlerszenario nicht ausreichend Kapazität vorhanden, verwendet der Optimierungsalgorithmus zunächst die freien reservierten Kapazitäten innerhalb des Weitverkehrsnetzes. Die reservierten Kapazitäten verursachen allerdings höhere Kosten für das Routen von Verkehrsanforderungen als die übrigen freien nicht reservierten Kapazitäten. Die Mehrkosten orientieren sich an dem aus der Verkehrstheorie bekannte Modell der Wartezeiten, die mit zunehmendem Angebot steigen. Nachdem eine oder mehrere Nebenbedingungen relaxiert wurden, findet eine erneute Optimierung statt. Führt die anschließende Optimierung wiederum zu keiner Lösung, reduziert der Planungsprozess diejenigen Verkehrsanforderungen, die keine Dienstgütekriterien besitzen, um den Faktor $rin\mathbb{R}^+$. Anschließend wird das vorherige Optimierungsmodell mit den reduzierten Verkehrsanforderungen verwendet.

Findet der Optimierungsalgorithmus auch mit den relaxierten Nebenbedingungen keine Lösung, erfolgt im letzten Schritt eine Optimierung ohne die Kapazitätsbegrenzungen auf den Links. Die Optimierung wird ohne Bedingung 7.4 durchgeführt, welche die Einhaltung der maximalen Linkkapazität der einzelnen Links beinhaltet. Die gefundene optimale Ersatzkonfiguration bezüglich der relaxierten Nebenbedingungen wird anschließend in der Managementdatenbank gespeichert. Zusätzlich sendet das Netzmanagementsystem eine Nachricht an den Netzbetreiber, um ihn darüber zu informieren, dass für einen potentiellen Fehlerfall nicht ausreichend Kapazität im Weitverkehrsnetz vorhanden ist.

7.1.1 Ergebnisse der Vorausplanung von Ersatzkonfigurationen

In diesem Abschnitt erfolgt die Evaluierung des Langzeitplanungsprozesses zur Vorausplanung der Ersatzkonfigurationen. Für die Simulationen werden drei ver-

schiedene Weitverkehrsnetze verwendet. Die Optimierung berechnet die optimalen Ersatzkonfigurationen für die in Tabelle 7.1 aufgeführten Fehler. Als Verkehrsanforderungen werden die berechneten Verkehrsmatrizen aus Kapitel 3 verwendet. Die Verkehrsmatrizen wurden so skaliert, dass auf jedem Link maximal 100 Wellenlängen benutzt werden und die Auslastung der Links im fehlerfreien Fall im Mittel bei 60 % liegt. Mit der angenommen mittleren Linkauslastung ist bei den meisten 1-Link-Ausfällen noch ausreichend Kapazität in den verwendeten Weitverkehrsnetzen vorhanden, um den Verkehr auf Ersatzwege umzuleiten.

	Anzahl der Konfigurationen		
Ersatzkonfiguration für	Deutschland-50	Nobel-US	Nobel-EU
1-Linkfehler	88	21	41
2-Linkfehler	3828	210	820
Knotenfehler	50	14	41
Knoten- und Linkfehler	4224	252	1066
Verändertes Verkehrsaufkommen	4900	364	1512
Gesamtanzahl	13090	861	3480
Benötigter Speicherbedarf	654,50 Gbyte	18,08 Gbyte	142,68 Gbyte

Tabelle 7.1: Mittels ganzzahliger linearer Optimierung vorausgeplante Fehlerszenarien

In der Tabelle sind die wahrscheinlichsten Fehler eines Weitverkehrsnetzes enthalten, für welche die Optimierung Ersatzkonfigurationen berechnet. Wie aus der Tabelle zu entnehmen ist, benötigt ein Weitverkehrsnetz mit steigender Anzahl an Knoten und Kanten mehr Speicherplatz in der Managementdatenbank. Entscheidend für die Anzahl an vorausberechneten Ersatzkonfigurationen ist weniger die benötigte Speicherkapazität als die dafür benötigte Berechnungszeit. Im nächsten Abschnitt erfolgt die Untersuchung der Optimierungszeit für die in Tabelle 7.1 aufgeführten Ersatzkonfigurationen.

7.1.2 Simulationsparameter

Zur Lösung des ganzzahligen Optimierungsproblems wurde CPLEX [ILO] und zur Datenrepräsentation und Berechnung der kürzesten Pfade wurde GRAPH [Gru] verwendet. Die Optimierungen wurden auf einem Computer mit Intel® Xeon® X5260 Quadcore Prozessor mit 3,33 GHz und 16 GByte Hauptspeicher berechnet, wobei für eine Optimierung nur jeweils ein Kern des Prozessors genutzt werden konnte.

Die Ergebnisse für die Vorausplanung für alle drei Weitverkehrsnetze sind in Abbildung 7.1 zusammengefasst. In den Diagrammen sind die mittleren Optimierungszeiten für ein Fehlerszenario und die Optimierungszeit für alle Szenarien aufgeführt. Die Berechnungszeiten ergeben sich aus einer sequentiellen Berechnung der einzelnen Optimierungsprobleme. Das Netzmanagementsystem eines Netzbetreibers, welches über ausreichend Rechenkapazitäten verfügt, ist in der Lage, die Optimierungen

parallel durchzuführen und erreicht damit kürzere Optimierungszeiten für alle Ersatzkonfigurationen. Die Lösungszeiten werden somit als obere Schranke betrachtet.

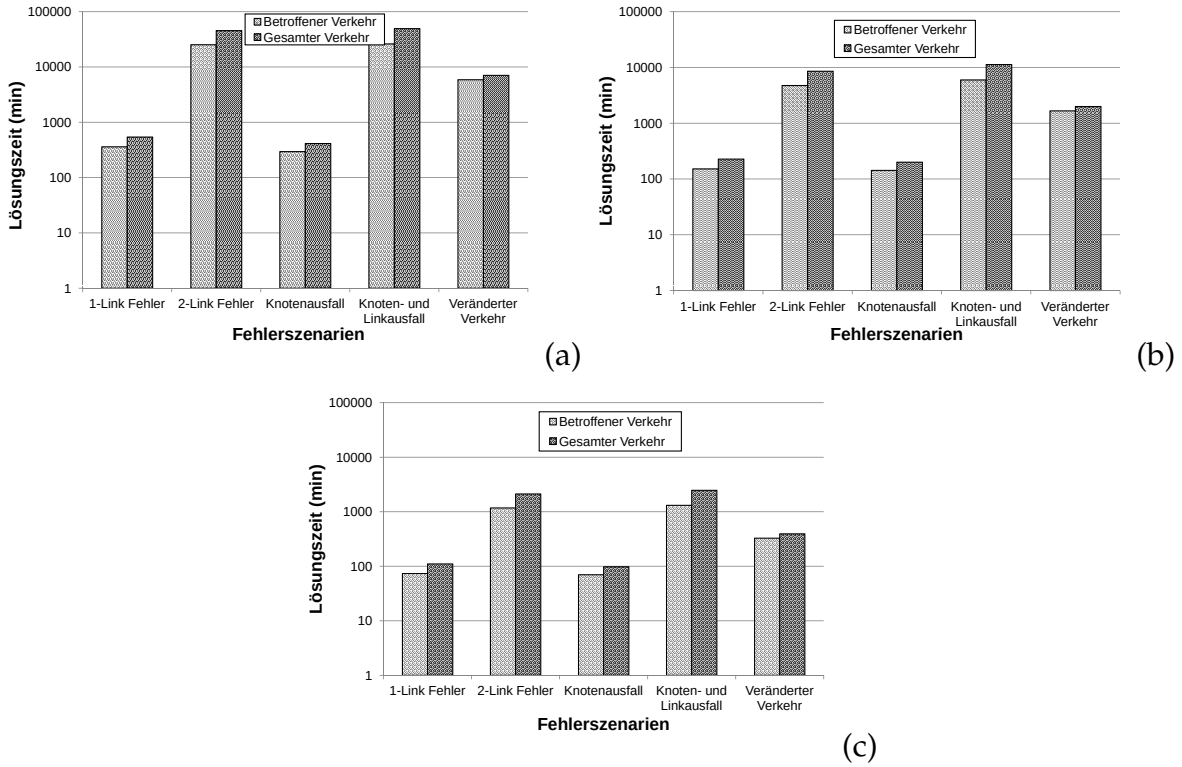


Abbildung 7.1: Zeitdauer zur Vorausplanung der Ersatzkonfigurationen für (a) Deutschland-50-Knotennetz (b) Nobel-EU-Netz (c) Nobel-US-Netz

Es wurden zwei verschiedene Re-Routingstrategien betrachtet und die Optimierungszeiten miteinander verglichen. Das erste Optimierungsziel besteht darin, nur die von einem Fehler betroffenen Verkehrsanforderungen neu zu routen. Durch diese Nebenbedingung soll möglichst wenig Verkehr im Weitverkehrsnetz umgeleitet werden. Führt die erste Optimierungsstrategie zu keinem Ergebnis, werden anschließend alle Verkehrsanforderungen betrachtet und gegebenenfalls neu geroutet. Die Optimierungszeiten für die Berechnung der Ersatzkonfigurationen sind in Abbildung 7.1 logarithmisch dargestellt. Bei allen drei Weitverkehrsnetzen berechnet die Optimierung mit dem ersten Optimierungsziel, nur die betroffenen Verkehrsanforderungen zu routen, die Lösungen in der kürzesten Zeit. Allerdings ist die Verkehrslast bei der zweiten Optimierungsstrategie gleichmäßiger im Weitverkehrsnetz verteilt, da alle Verkehrsanforderungen betrachtet werden.

Die längste Optimierungszeit besitzen die Fehlerszenarien mit zwei Linkfehlern. Um alle Kombinationen an 2-Linkfehler vorab zu planen, benötigt die Optimierung bis zu 18 Tage (nur betroffene Verkehrsanforderungen) beziehungsweise 32 Tage für das Deutschland-50-Knotennetz. Die Vorausplanung aller beschriebenen Fehlers-

zenarien dauert für das Deutschland-50-Knotennetz bis zu 41 beziehungsweise 72 Tage. Deutlich kürzere Optimierungszeiten ergeben sich für das Nobel-EU- und das Nobel-US-Weitverkehrsnetz. Die Optimierungszeiten für die Vorabberechnung aller Fehlerszenarien betragen 16 Tage für das Nobel-EU-Netz beziehungsweise vier Tage für das Nobel-US-Netz. Allerdings wirkt sich beim Nobel-EU-Netz und Nobel-US-Netz die geringere Linkdichte auf die Optimierungsstrategie aus. Vor allem beim Nobel-US-Netz findet häufiger eine Relaxation der Nebenbedingungen statt, da mit den restlichen Linkkapazitäten nicht alle Verkehrsanforderungen geroutet werden können. Dies zeigt sich insbesondere bei den 2-Linkfehlerszenarien.

Wie in Kapitel 6 beschrieben, vernachlässigt die Optimierung im letzten Schritt die Kapazitätsbegrenzungen der Links, falls mit den Nebenbedingungen keine Lösung gefunden wurde. Durch die Relaxierung soll die Optimierung auf jeden Fall eine Lösung finden und dem Netzbetreiber mitteilen. Wie viele Fehlerszenarien schließlich zu einer Relaxierung führen, ist in Abbildung 7.2 dargestellt.

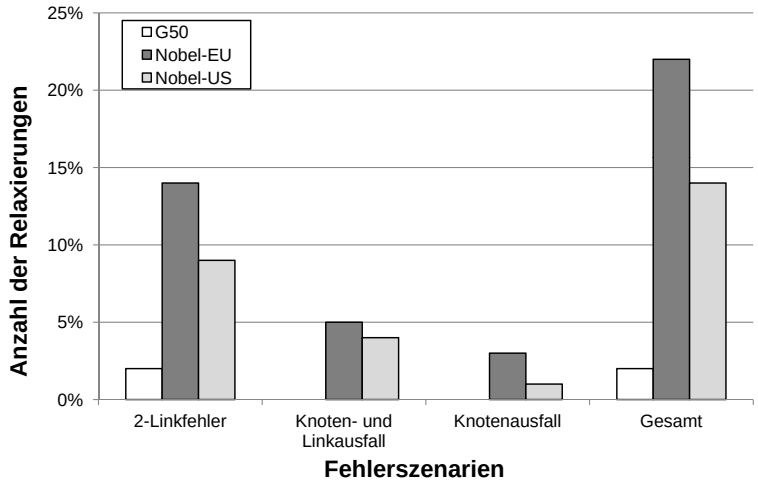


Abbildung 7.2: Anzahl der Relaxierungen pro Fehlerszenario

Im Fall des Nobel-EU-Netzes werden in 22 % und beim Nobel-US-Netz in 14 % der Fehlerszenarien die Nebenbedingungen relaxiert, um eine optimale Ersatzkonfiguration zu finden. Insbesondere die 2-Linkfehler und die Kombination aus Knoten- und Linkausfall führen zu einer Relaxierung der Nebenbedingungen. Das Deutschland-50-Knotennetz besitzt den höchsten Knotengrad und daher stehen auch beim gleichzeitigen Ausfall von zwei Links noch ausreichend Alternativwege zur Verfügung. Nur in 2 % der 2-Linkfehler wird eine Relaxierung durchgeführt, wobei die verbleibende Linkkapazität ausreicht, um alle Verkehrsanforderungen zu routen. Durch die hohe Linkanzahl existieren weniger Links mit einer sehr hohen Kapazitätsauslastung und es sind keine zentralen Links vorhanden, über die eine Vielzahl der Verkehrsanforderungen geroutet werden muss.

Abschließend lässt sich feststellen, dass für die meisten vorab definierten Fehlerszenarien eine optimale Ersatzkonfiguration berechnet wird. Allerdings hängt deren Anzahl von der Netzgröße und der Zeitdauer zwischen zwei Fehlerereignissen ab. Für das Nobel-EU- und Nobel-US-Netz lassen sich in adäquater Zeit die Ersatzkonfigurationen berechnen. Für das Nobel-EU-Netz findet man in 62 % der Fälle und für das Nobel-US in 71 % der Fälle eine optimale Ersatzkonfiguration ohne Relaxierung der Nebenbedingung. Das Deutschland-50-Knotennetz weist im Vergleich zu den beiden anderen Weitverkehrsnetzen eine längere Optimierungszeit auf, da die Anzahl der vorab geplanten Fehlerszenarien um ein Vielfaches höher ist. Die Optimierungszeit der Einzelfehler ist dagegen nicht wesentlich länger als für die anderen beiden Netze. Für das Deutschland-50-Knotennetz findet man in 92 % der Fälle eine optimale Ersatzkonfiguration.

Für alle drei untersuchten Weitverkehrsnetze gilt, dass die Reihenfolge der Vorausplanung entscheidend für die maximale Anzahl der Ersatzkonfigurationen ist. Je mehr Ersatzkonfigurationen mittels der ganzzahligen linearen Optimierung im Voraus berechnet werden, desto höher ist die Wahrscheinlichkeit, dass eine geeignete Ersatzkonfiguration für einen auftretenden Netzfehler vorhanden ist. Die Ergebnisse dazu sind in Abschnitt 7.3 beschrieben, in dem das Zusammenspiel von Vorausplanung und Heuristik beschrieben wird. Die im Netzmanagement verwendete Heuristik wird im nächsten Abschnitt dargestellt.

7.2 Genetischer Algorithmus

Wie in Abschnitt 7.1.1 gezeigt, ist es in einem Weitverkehrsnetz nicht möglich alle potentiellen Fehlerszenarien vorauszuplanen. Die Optimierungszeit aller Fehlerszenarien zusammen ist um ein Vielfaches größer als der Zeitraum zwischen zwei Netzänderungen. Für die nicht vorausgeplanten Fehlerfälle wird in diesem Abschnitt deshalb ein *Genetischer Algorithmus* (GA) entwickelt, der eine schnelle Lösungszeit ermöglicht.

Wissenschaftliche Untersuchungen in [DAS97], [Che98] und [LI00] zeigen gute Ergebnisse bei der Anwendung des GA auf die Minimierung der Kosten eines Weitverkehrsnetzes unter der Bedingung der Zuverlässigkeit des Netzes. Zur schnellen Planung wird deshalb ein GA [Bar57], [Fra57], [Bre62], [Gol89] eingesetzt. Der GA gehört zur Klasse der heuristischen Optimierungsverfahren und ist ein evolutionärer Algorithmus. Wie bei allen heuristischen Optimierungsverfahren kann nicht garantiert werden, dass eine gefundene Lösung dem Optimum entspricht. Die Untersuchungen in [EH91] bestätigen die Konvergenz der evolutionären Algorithmen zu einem globalen Optimum. GA basiert auf der Idee der natürlichen Selektion und Vererbung, die dazu führen, dass über viele Generationen nur die „guten“ Gene überleben und somit die Lösung gegen das Optimum strebt.

Die Vorteile des GA sind dessen Geschwindigkeit mit welcher eine Lösung gefunden wird und die Anzahl der Lösungen, die am Ende des Prozesses zur Verfügung

stehen. Jede Generation besteht aus einer bestimmten Anzahl von Populationen, die eine gültige Lösung darstellen. Somit stehen dem Netzbetreiber mehrere Lösungen gleichzeitig zur Verfügung.

Der GA startet mit einer initialen Population und durchläuft anschließend, wie in Abbildung 7.3 gezeigt, die Schritte Rekombination, Mutation und Selektion. Am Ende eines Durchlaufs steht eine neue Generation zur Verfügung. Die Schleife wird solange durchlaufen, bis sich über eine bestimmte Anzahl an Generationen keine Verbesserung der Fitness einstellt. In diesem Fall wird der Durchlauf der Schleife abgebrochen und die aktuelle Generation gespeichert. Die zuletzt berechnete Generation stellt damit eine stabile Lösung des Optimierungsproblems dar.

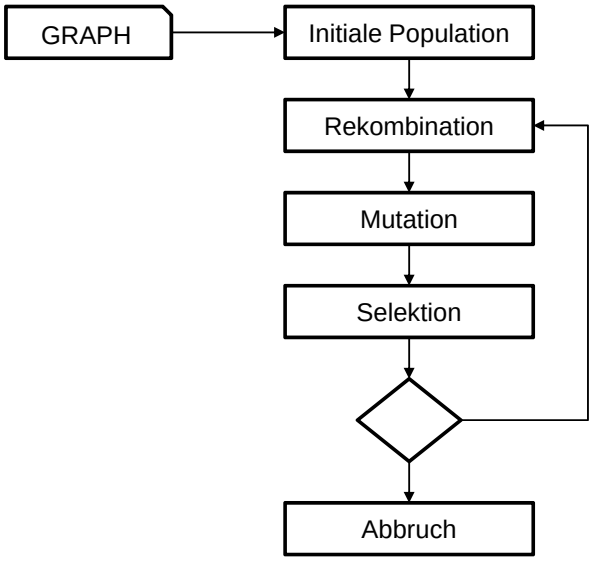


Abbildung 7.3: Ablaufdiagramm des Genetischen Algorithmus

Die initiale Population basiert auf der letzten gültigen Konfiguration des Weitverkehrsnetzes, da diese eine gute Ausgangsbasis für den GA darstellt. Eine neue Netzkonfiguration nach einer Veränderung in einem Weitverkehrsnetz sollte in den meisten Fällen keine großen Abweichungen von der letzten gültigen Konfiguration besitzen.

Die initiale Population wird mit Hilfe von GRAPH erzeugt. Zunächst werden die physikalische Topologie und die aktuelle Verkehrsmatrix eingelesen und die k-kürzesten Pfade für alle Verkehrsanforderungen berechnet. Für die kürzesten Pfade wird wiederum der Algorithmus von Dijkstra verwendet. Die Neuberechnung der kürzesten Pfade nach einem Fehler im Netz ist erforderlich, da durch den Ausfall von Kanten oder Knoten eine neue Topologie entsteht und die alten kürzesten Pfade ihre Gültigkeit verlieren.

Anschließend werden die von einem Fehler betroffenen Verkehrsanforderungen bestimmt. Fällt ein Knoten in einem Netz aus, können die Verkehrsanforderungen von und zu diesem Knoten nicht mehr bedient werden und werden im Algorithmus

blockiert. Die Genome werden zufällig initialisiert, um eine erste Generation an Lösungen zu haben. Die erste Population kann auch ungültige Lösungen enthalten, welche durch die Rekombination, Mutation und Selektion aussortiert werden.

Genom

Das Genom muss ein bestimmtes Format besitzen, so dass Rekombinationen und Mutationen möglich sind. Die Genome müssen zum Beispiel alle die gleiche Größe besitzen, um sie miteinander kombinieren zu können. Der Aufbau der Genome leitet sich aus der in Abbildung 7.4 dargestellten Matrix der kürzesten Pfade ab.

	0	1	2	...	k-1
0	A-B	A-C-B	A-D-B	...	A-D-E-B
1	A-C	A-D-C	A-E-C	...	A-F-C
⋮	⋮	⋮	⋮	⋮	⋮
$D_{xy}-1$	Z-A	Z-B-A	Z-C-A	...	Z-D-A

Abbildung 7.4: Tabelle der kürzesten Pfade

Zu Beginn berechnet der Algorithmus die k-kürzesten Pfade für alle Anforderungspaare und speichert diese in einer Matrix. In der vertikalen Richtung werden alle Anforderungspaare und in der horizontalen Richtung ihre k-kürzesten Pfade gespeichert. Aus dieser Zuordnung wird das Genom, wie in Abbildung 7.5 dargestellt, gebildet.

1	4	...	3
0	1	...	$D_{xy}-1$

Abbildung 7.5: Repräsentation des Genoms

Das Genom besteht aus den Routenzuweisungen für jede Verkehrsanforderung. Die Position im Genom spiegelt die entsprechende Verkehrsanforderung wieder und die Zahl innerhalb des Genoms steht für den gewählten kürzesten Pfad dieser Verkehrsanforderung. In Abbildung 7.5 wird die Verkehrsanforderung an Position 1 über den kürzesten Pfad 4 geroutet. Das genaue Routing des kürzesten Pfads 4 findet sich in der Matrix der kürzesten Pfade wieder. Die Länge des Genoms entspricht somit der Anzahl der Verkehrsanforderungen in einem Weitverkehrsnetz.

Fitnessfunktion

Zur Bewertung der gefundenen Lösungen benutzt der GA eine Fitnessfunktion, die entweder minimiert oder maximiert wird. Die Hauptaufgabe des Algorithmus

besteht darin, alle Anforderungen der Verkehrsmatrix nach dem Auftreten eines Fehlers in dem Weitverkehrsnetz zu routen. Dies gilt insbesondere für die Verkehrsanforderungen mit Dienstgütekriterien. Die Fitnessfunktion in Formel 7.7 setzt sich aus drei Termen zusammen, welche die Dienstgütekriterien berücksichtigen.

$$c = k_1 \cdot p_{SLA} + k_2 \cdot d_{nr} + k_3 \cdot d \tag{7.7}$$

Die Kosten der Fitnessfunktion setzen sich aus den Strafzahlungen p_{SLA}, den blockierten Verkehrsanforderungen d_{nr} und den Verzögerungen der Verkehrsanforderungen d zusammen. Die Parameter sind normiert und können Werte zwischen Null und eins annehmen. Alle drei Terme werden zusätzlich noch mit den Koeffizienten k_1, k_2 und k_3 gewichtet, um den Einfluss der einzelnen Parameter zu bestimmen. Der Parameter k_1 für die Strafzahlungen hat einen höheren Einfluss auf die Kosten und wird deshalb auch höher gewichtet als die restlichen Terme.

Die blockierten Verkehrsanforderungen d_{nr} berechnen sich aus der Anzahl der Verkehrsanforderungen n_d und der Blockierung pro Verkehrsanforderung b_d.

$$d_{nr} = \frac{\sum_{d \in \mathbb{D}} n_d \cdot b_d}{\sum_{d \in \mathbb{D}} n_d} \tag{7.8}$$

Die Kosten für die Strafzahlungen setzen sich aus zwei Termen zusammen. Der erste Summand bestimmt die Kosten durch Verkehrsanforderungen, die nicht geroutet werden können. Der zweite Summand beinhaltet dagegen die Kosten, welche durch Verkehrsanforderungen entstehen, die zwar geroutet werden, aber nicht die geforderten Dienstgütekriterien einhalten.

$$p_{SLA} = \sum_{d \in \mathbb{D}_S} n_d \cdot \bar{b}_d + \sum_{d \in \mathbb{D}_S} n_d \cdot b_d \cdot \frac{max(0, t_d - t_{max})}{t_w - t_{max}} \tag{7.9}$$

t_d gibt die Ende-zu-Ende-Verzögerung einer Verkehrsanforderung an und besteht aus den Knoten- und Kantenverzögerung entlang eines Pfades. Die Kantenverzögerungen berechnet sich aus der Länge einer Kante und der Ausbreitungsgeschwindigkeit des Lichts in der Glasfaser. Die Knotenverzögerung hängt dabei von der Auslastung der Knoten entlang des Pfades $p \in P_d$ ab und orientieren sich an dem Wartemodell in [PMF+02] und an den Werten von heutigen Cisco Routern [JC09].

Der dritte Term d in der Fitnessfunktion dient dazu, die Wartezeiten an Knoten zu reduzieren, indem eine Lastteilung der Verkehrsanforderungen berücksichtigt wird, um das Weitverkehrsnetz fehlertoleranter zu machen und die Flexibilität beim Routing im Fehlerfall zu steigern. Durch ein gleichmäßiges Routen der Verkehrsanforderungen sinkt die maximale Auslastung einzelner Kanten, welche dann noch Kapazitäten zur Verfügung haben, falls ein Fehler auftritt und Verkehr über diese Kante umgeleitet wird.

$$d = \sum_{d \in \mathbb{E}} cost(e) \tag{7.10}$$

Nach [PMF+02] und [HVD04] sind Kantenauslastungen über 80 % in heutigen Netzen unüblich und werden bei diesen Auslastungen als überlastet betrachtet. Für die Kosten pro Kante abhängig von der Auslastung der Kante wird wiederum die Kurve aus Abbildung 6.3 verwendet.

Rekombination

In der Rekombinationsphase des GA werden die Populationen einer Generation miteinander kombiniert, um bessere Lösungen zu erzeugen. Die Rekombination ist mit der Kreuzung des Erbguts in der Natur vergleichbar. Der Algorithmus verwendet die 2-Punkt-Rekombination, die im Vergleich zur 1-Punk-Rekombination und zum gleichmäßigen Kreuzungsverfahren [Syw89] bessere Werte liefert.

Für die 2-Punk-Rekombination werden zufällig zwei Genome aus dem Pool ausgewählt. Dabei ist eine Gleichverteilung von Bedeutung. Das bedeutet, dass nicht nur die besten Lösungen einer Generation miteinander kombiniert werden, sondern auch schlechtere Genome mit der besten Lösung. Bei der 2-Punkt-Rekombination werden zwei Kreuzungspunkte $kp1$ und $kp2$ zweier Genome so ausgewählt, dass gilt

$$1 \leq kp1 \tag{7.11}$$
$$kp2 \leq L \tag{7.12}$$
$$kp1 < kp2 \tag{7.13}$$

L stellt die Länge des Genoms dar und entspricht der Anzahl der gerouteten Verkehrsanforderungen. Wie in Abbildung 7.6 gezeigt, wird mit Hilfe von zwei Kreuzungspunkten die Länge der zwei Genome bestimmt, die rekombiniert werden.

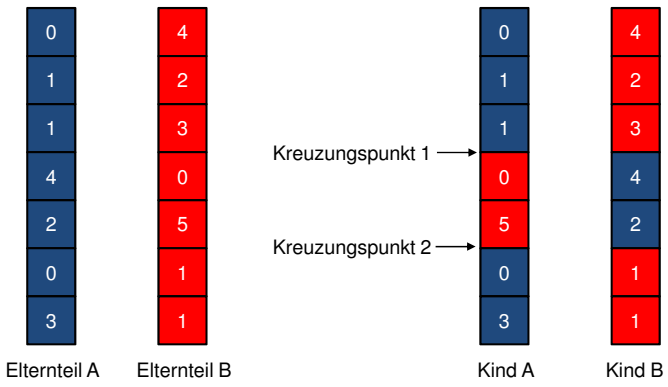


Abbildung 7.6: 2-Punkt-Rekombination

Mutation

Die Mutation ist eine weitere Möglichkeit, um neue Genome in eine Evolution einzubringen. Hierbei werden einzelne Einträge eines Genoms zufällig verändert. Durch die Mutation wird eine neue Variabilität in eine Population eingeführt, die durch das reine Rekombinieren der Elterngenome eventuell nicht vorhanden wäre. Für die Mutation werden die Einträge aller Genome durchlaufen und mit der Wahrscheinlichkeit P ausgewählt und mutiert. Durch die Mutation sollen lokale Maxima oder Minima als endgültige Lösung der Heuristik vermieden werden.

Selektion

Die Selektion entscheidet welche Genome in die neue Generation übernommen werden. Diese Entscheidung wird anhand der Fitness der einzelnen Genome getroffen. Beim Selektionsprozess werden diejenigen Genome ausgewählt, die am ehesten dafür geeignet sind, in der nächsten Generation noch bessere Lösungen zu generieren. In der Literatur gibt es verschiedene Selektionsmechanismen, beispielsweise Roulette-Wheel-Selektion, Stochastic Universal Sampling und Stochastic Tournament, für die Auswahl der nächsten Generation [Gol89] und [Mic96].

In dieser Arbeit wurde als Auswahlkriterium die Roulette-Wheel-Selektion [GD91], [DJPS08], [BTS09] verwendet. Bei dieser Selektion wird jedem Genom ein Feld auf einem Roulette-Rad zugewiesen, das von der Fitness des Genoms abhängt. Dabei bekommt die schlechteste Lösung nur ein Feld und die beste Lösung a Felder zugewiesen, wobei a der aktuellen Populationsgröße entspricht. Aus dem Pool der Felder werden solange Genome zufällig entnommen, bis die nächste Generation vollständig gebildet ist. Genome die bereits selektiert wurden, werden aus dem Pool für die nächste Ziehung entfernt. Der Vorteil der Roulette-Wheel-Selektion besteht darin, dass auch Genome mit einer schlechteren Fitness eine geringere Wahrscheinlichkeit besitzen, für die nächste Generation selektiert zu werden.

Bei der Auswahl der Genome muss deren Gültigkeit gewährleistet sein. Die Genome müssen einen der vorher berechneten kürzesten Pfade enthalten und dürfen die Kapazität der einzelnen Links nicht überschreiten. Eine Verkehrsanforderung die entlang eines Pfades geroutet wird, darf auf den gerouteten Links nur dieselbe Wellenlänge verwenden. Ein weiteres Gültigkeitskriterium ist die Ende-zu-Ende Verzögerung des ausgewählten Routings für bestimmte Verkehrsanforderungen, die einen Maximalwert nicht überschreiten darf.

Abbruchbedingung

Der Nachteil eines GA und allgemein heuristischer Optimierungsverfahren besteht darin, dass keine analytische Schranke angegeben und auch nicht garantiert werden kann, dass die zu einem bestimmten Zeitpunkt gefundene Lösung der optimalen

Lösung entspricht. Deshalb muss für den GA ein Abbruchkriterium angegeben werden, welches die Qualität der Lösungen evaluiert und entsprechend der Kriterien den Algorithmus terminiert.

Als Abbruchkriterium wird die mittlere Fitness aller Genome einer Generation betrachtet. Bleibt die mittlere Fitness über eine bestimmte Anzahl von Generationen stabil, hat der Algorithmus seine Sättigung erreicht und wird abgebrochen. In Abbildung 7.7 ist ein beispielhafter Fitnessverlauf gezeigt, in dem die Abbruchbedingung nach 100 Generationen erreicht wird. In dem Diagramm ist zusätzlich noch der Verlauf der Fitness des besten Genoms jeder Generation eingezeichnet.

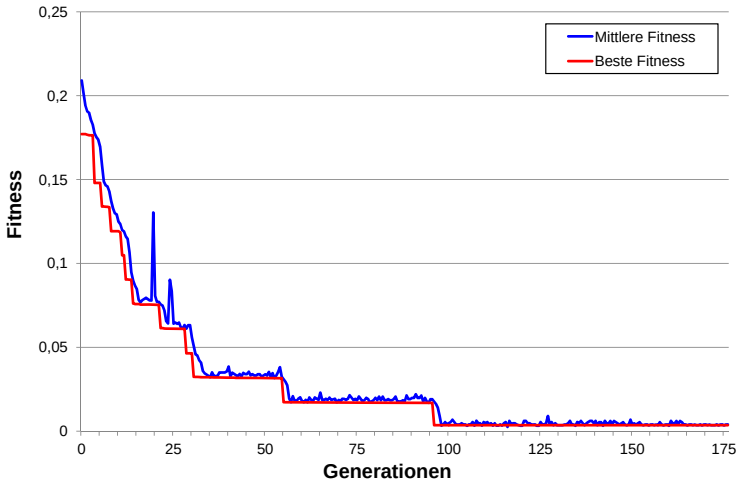


Abbildung 7.7: Fitness des besten Genoms und durchschnittliche Fitness über alle Genome

Man erkennt einen sehr ähnlichen Kurvenverlauf für die durchschnittliche Fitness aller Genome und die Fitness des besten Genoms und sich diese nach 100 Generationen nur geringfügig unterscheiden. Allerdings kann keine Aussage darüber getroffen werden, ob es sich dabei um ein lokales oder globales Maximum beziehungsweise Minimum handelt. Für die Online-Planung ist das Auffinden einer schnellen Lösung entscheidend. Diese sollte wenn möglich optimal sein, allerdings primär die Betriebsfähigkeit des Netzes garantieren. Daher akzeptiert das Netzmanagementsystem bereits die erste gültige Lösung des GA.

7.2.1 Ergebnisse der Optimierung und Diskussion

In diesem Abschnitt erfolgt die Evaluierung des realisierten GA. Dazu werden verschiedene Netztopologien verwendet, um die Auswirkung der Knoten- und Linkanzahl sowie der Anzahl der Verkehrsanforderungen auf den Algorithmus zu untersuchen. Für die Simulationen werden das Deutschland-17-Knotennetz, das Nobel-EU- und das Nobel-US-Netz verwendet. Für diese Transportnetze werden verschiedenen

Fehlerszenarien betrachtet und die Performanz des Algorithmus evaluiert. Es werden keine Wellenlängenkonverter verwendet und für jede Verkehrsanforderung zwischen zwei Knotenpaaren werden sechs verschiedene kürzeste Pfade vorausberechnet.

Die Online-Planung mittels eines GA wird angewandt, um nach dem Auftreten eines Fehlers schnell eine Lösung zu finden, falls keine Ersatzkonfiguration existiert. Daher ist die Optimierungszeit des GA eine entscheidende Größe, die im Folgenden analysiert wird. In Tabelle 7.2 sind die Berechnungszeiten für die kürzesten Pfade aller Verkehrsanforderungen für die verschiedenen Netztopologien aufgeführt.

Weitverkehrsnetz	Neuberechnung aller kürzesten Pfade	Neuberechnung betroffener kürzester Pfade
Deutschland-17-Knotennetz	8 s	3 s
Nobel-EU-Netz	26 s	5 s
Nobel-US-Netz	3 s	2 s

Tabelle 7.2: Berechnungszeit der kürzesten Pfade aller Verkehrsanforderungen

Die Tabelle enthält Berechnungszeiten sowohl für die Neuberechnung der kürzesten Pfade alle Verkehrsanforderungen als auch für die Neuberechnung der kürzesten Pfade der betroffenen Verkehrsanforderungen. Diese zählen zur gesamten Optimierungszeit des GA. Die vollständige Neuberechnung dauert vor allem beim Nobel-EU-Netz mit 26 s sehr lange. Für eine endgültige Aussage müssen allerdings die Lösungszeiten des GA für die einzelnen Fehlerszenarien betrachtet werden, um das Verhältnis zwischen Berechnung der kürzesten Pfade und vollständiger Lösungszeit zu bewerten. Die Berechnungszeiten der beiden anderen Beispielnetze sind aufgrund der geringeren Knoten- und Linkanzahl deutlich geringer.

Die Berechnungszeiten der kürzesten Pfade sind deutlich kürzer, wenn die bereits berechneten kürzesten Pfade wiederverwendet werden und nur für die betroffenen Verkehrsanforderungen neu berechnet werden. Insbesondere für große Netze wie dem Nobel-EU-Netz ergeben sich deutlich geringere Berechnungszeiten.

Nach der Berechnung der kürzesten Pfade verwendet der GA drei verschiedene Re-Routingstrategien für die Verkehrsanforderungen:

- Das ausschließliche Umleiten der betroffenen Verkehrsanforderungen (1)
- Das Umleiten der betroffenen Verkehrsanforderungen und der Verkehrsanforderungen ohne Dienstgütekriterien (2)
- Das Umleiten aller Verkehrsanforderungen (3)

Nach einem Fehlerereignis startet der Algorithmus die Optimierung unter Verwendung der ersten Re-Routingstrategie (1). Da das primäre Ziel die schnelle Berechnung von gültigen Lösungen ist, versucht der Algorithmus zunächst nur die betroffenen

Verkehrsanforderungen neu zu routen. Die Strategie soll auch vermeiden, dass sämtliche Verkehrsanforderungen in einem Weitverkehrsnetz neu geroutet werden müssen. Findet der GA mit der ersten Routingstrategie keine Lösung, erfolgt im nächsten Schritt das Umleiten der betroffenen Verkehrsanforderungen und der Verkehrsanforderungen ohne Dienstgüteparameter. Die zweite Strategie verfolgt das Ziel, Verkehr mit Dienstgütekriterien nicht umzuleiten, um zu vermeiden, dass durch die Neukonfiguration eine kurze Ausfallzeit auftritt. Der GA versucht deshalb zunächst nur Verkehrsanforderungen ohne Dienstgütekriterien umzuleiten. Führt auch diese Strategie nicht zum Erfolg, startet der GA eine Suche, bei der sämtliche Verkehrsanforderungen innerhalb des Weitverkehrsnetzes neu geroutet werden. Diese Option bietet die meisten Freiheitsgrade bezüglich des Routings dauert aufgrund der Komplexität der Aufgabe aber entsprechend länger.

In den nächsten Abschnitten werden anhand verschiedener Fehlerszenarien die Performanz des GA untersucht. Dabei werden diejenigen Fehlerfälle verwendet, die von der ganzzahligen linearen Optimierung aufgrund der hohen Anzahl an Möglichkeiten nicht voraus geplant werden.

Vergleich der Auswirkungen der Wellenlängenzuweisungen

Für die folgenden Untersuchungen wird angenommen, dass in den untersuchten Weitverkehrsnetzen keine Wellenlängenkonverter vorhanden sind. Eine Verkehrsanforderung besitzt deshalb entlang des Pfades von Quell- zu Zielknoten dieselbe Wellenlänge. Zunächst werden drei verschiedene Wellenlängenzuweisungsstrategien anhand der verschiedenen Netztopologien verglichen, um die geeignete Wellenlängenzuweisungsstrategie für die Heuristik zu finden. Die Ergebnisse sind in Abbildung 7.8 dargestellt.

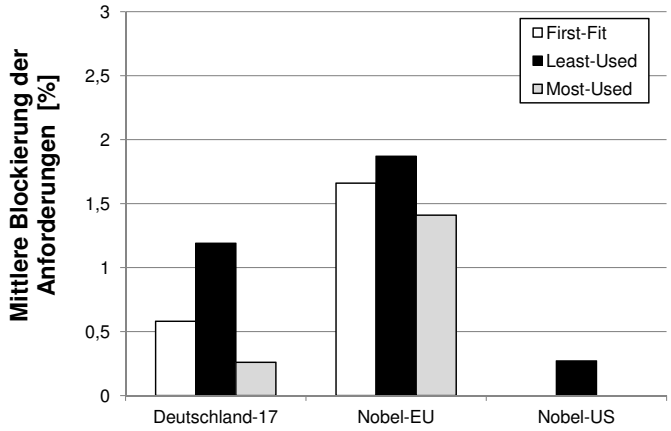


Abbildung 7.8: Auswirkung der Wellenlängenzuweisungen

In der Abbildung sind die Anzahl der durchschnittlich blockierten Verkehrsanforderungen für 1-Kantenfehler unter Verwendung der drei unterschiedlichen Zuwei-

sungsstrategien gezeigt. Dabei ist ersichtlich, dass die „First Fit“- und „Most Used“-Methode zu einer geringeren Anzahl an blockierten Verkehrsanforderungen in den verwendeten Netztopologien führen. Die Ergebnisse stimmen mit denen in [RS02] überein, dass die „Most Used“-Methode eine höhere Wahrscheinlichkeit besitzt, eine freie Wellenlänge zu finden. Für das Nobel-US-Netz traten bei Verwendung der „First Fit“- und „Most Used“-Methode keine Blockierungen auf. Da die „Most Used“-Methode im Vergleich zur „First Fit“-Methode eine geringere Anzahl an blockierten Verkehrsanforderungen aufweist, wird die „Most Used“-Methode für alle weiteren Betrachtungen verwendet.

1-Kantenfehler

Im Folgenden werden verschiedene Fehlerszenarien auf die beschriebenen Netztopologien angewendet. Zunächst werden 1-Kantenfehler betrachtet, um die Ergebnisse des GA mit der ganzzahligen linearen Optimierung zu vergleichen. Der Fitnessverlauf des GA ist in Diagramm 7.9 für die Verwendung der Re-Routingstrategien (1) und (2) dargestellt, um die Auswirkung der Re-Routingstrategien auf die Lösungszeit zu verdeutlichen.

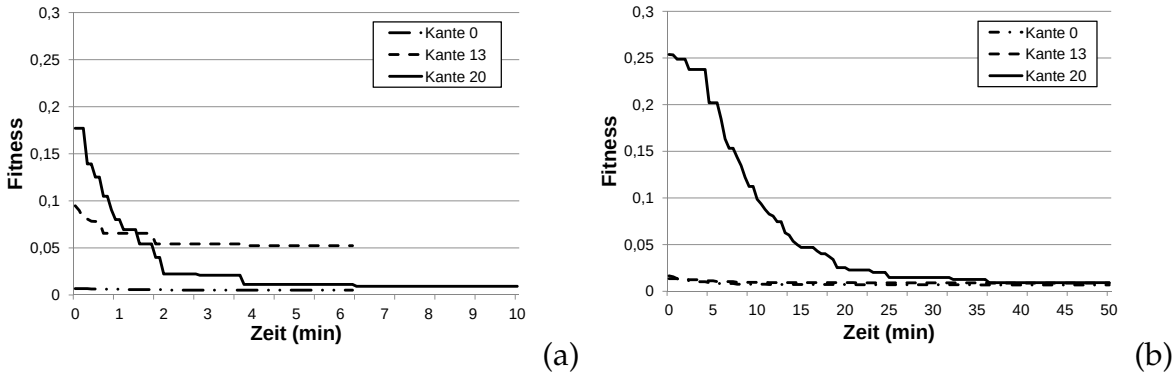


Abbildung 7.9: Konvergenz des GA unter Verwendung der (a) Re-Routingstrategien (1) (b) Re-Routingstrategien (2)

Das Diagramm zeigt den zeitlichen Verlauf der Fitness der Generationen für drei 1-Kantenfehler im Deutschland-17-Knotennetz. Die exemplarisch ausgewählten Kantenfehler zeigen den Verlauf der Fitness der Lösungen für die Kanten mit der höchsten Verkehrsauslastung (gestrichelte Linie), die Kante mit der schnellsten Lösungszeit (gestrichelte/gepunktete Linie) und die Kante mit der längsten Optimierungszeit (schwarze Linie). In Diagramm 7.9 (a) wurden nur die betroffenen Verkehrsanforderungen umgeroutet. Unter der Verwendung der Re-Routingstrategie (1) findet der GA innerhalb von vier Minuten eine Lösung für 24 von 26 Kanten. Für zwei 1-Kantenfehler findet der GA keine gültige Lösung. Die gestrichelte Kurve in Diagramm 7.9 (a) zeigt den Fitnessverlauf für eine der beiden Kanten. Die Fitness konvergiert zwar gegen einen bestimmten Wert, aber es können nicht alle Verkehrsanforderungen geroutet werden, wenn das Abbruchkriterium erreicht wird.

Zum Vergleich ist das Ergebnis des GA mit der zweiten Re-Routingstrategie in Diagramm 7.9 (b) eingezeichnet. Es ist wiederum der Verlauf der Fitnesswerte über die Zeit für die drei 1-Kantenfehler dargestellt. Wie der Verlauf der schwarzen Kurve veranschaulicht, besitzt der GA mit der zweiten Re-Routingstrategie eine höhere Lösungszeit für alle 1-Kantenfehler. Im Gegensatz zur ersten Re-Routingstrategie findet der GA allerdings für alle 26 1-Kantenfehler eine Lösung. Aus den beiden Diagrammen zeigt sich, dass für eine Lösung aller 1-Kantenfehler in möglichst kurzer Zeit eine Kombination der drei oben genannten Strategien notwendig ist.

Für eine genauere Untersuchung sind die Optimierungszeiten für alle 1-Kantenfehler in den Diagrammen 7.10 (a) und (b) dargestellt. Der GA wendet alle drei Re-Routingstrategien in der im vorherigen Abschnitt erwähnten Reihenfolge an.

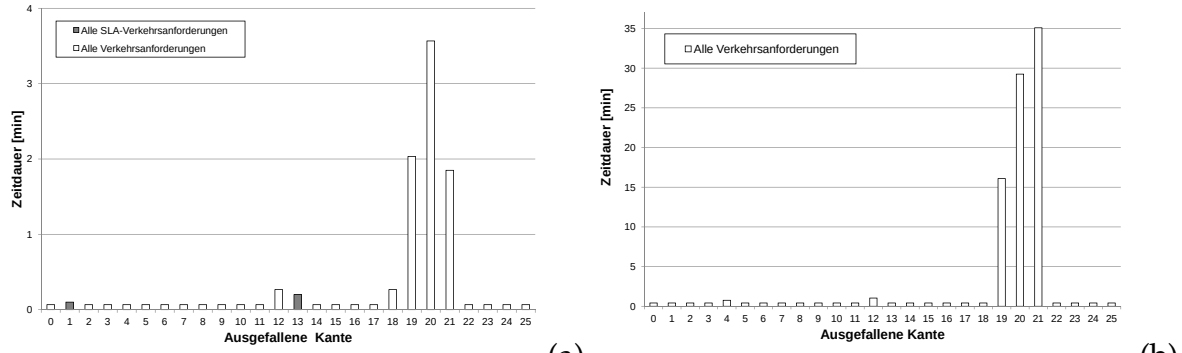


Abbildung 7.10: Optimierungszeiten für alle 1-Kantenfehler (a) nur betroffener Verkehr umgeroutet (b) betroffener und nicht SLA-Verkehr umgeroutet

Wie zu erwarten ist in Abbildung 7.10 (a) die Optimierungszeit für Re-Routingstrategie (1) (nur betroffene Verkehrsanforderungen) geringer als für Re-Routingstrategie (2) (betroffener und Nicht-SLA Verkehr). Der Algorithmus muss bei dem ausschließlichen Re-Routing der betroffenen Verkehrsanforderungen wesentlich weniger Pfade umrouten und benötigt daher weniger Zeit. In beiden Diagrammen fällt auf, dass die Kanten 19, 20 und 21 eine besonders lange Optimierungszeit benötigen. Dies liegt an den angeschlossenen Knoten, die einen geringen Knotengrad besitzen. Im fehlerfreien Fall besitzen die Knoten einen Knotengrad von 2, der sich im Fehlerfall auf 1 reduziert. Die Verkehrsanforderungen von den entsprechenden Knoten können somit nur über einen verbleibenden kürzesten Pfad geroutet werden.

In Diagramm 7.11 sind die vollständigen Optimierungszeiten für alle 1-Kantenfehler dargestellt. Die Lösungszeiten berechnen sich aus der Summe der einzelnen Optimierungszeiten aller verwendeten Strategien. In Diagramm 7.11 ist zu erkennen, dass 24 1-Kantenfehler bereits mit der ersten Re-Routingstrategie gelöst werden können. Für die Kanten 1 und 13 werden mittels Re-Routingstrategie (2) alle Verkehrsanforderungen geroutet.

Die Ergebnisse zeigen, dass für 84 % der 1-Kantenfehler innerhalb einer Minute eine Lösung vorhanden ist. Bei den Kanten 19, 20 und 21 verhindert der geringe

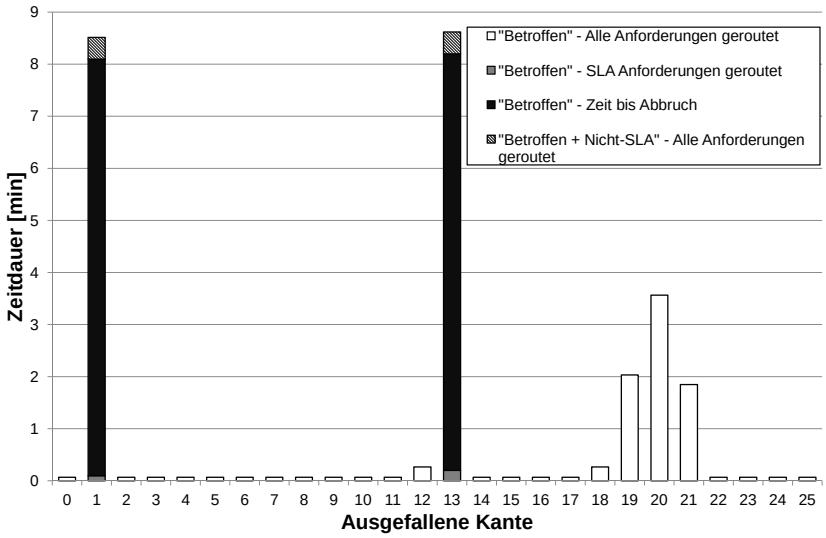


Abbildung 7.11: Optimierungszeit bis alle Verkehrsanforderungen geroutet werden

Knotengrad eine schnelle Lösungszeit. Nur bei zwei 1-Kantenfehlern muss die Re-Routingstrategie (2) verwendet werden, die innerhalb einer Minute eine Lösung findet. Hier zeigt sich eine erste mögliche Verbesserung der Verwendung der drei Re-Routingstrategien. Insgesamt benötigt der GA für die Kanten 1 und 13 ungefähr neun Minuten bis eine gültige Lösung vorhanden ist. Allerdings ergibt sich die lange Lösungsdauer aufgrund Re-Routingstrategie (1). Der GA erreicht mit der ersten Re-Routingstrategie nach circa acht Minuten die Abbruchbedingung ohne eine gültige Lösung gefunden zu haben. Anschließend startet der GA die Optimierung mit Re-Routingstrategie (2) und finden innerhalb von 30 Sekunden eine Lösung. Ein frühzeitiger Abbruch des ersten Optimierungslaufs und Wechsel auf Re-Routingstrategie (2) ergibt für die zwei 1-Kantenfehler eine wesentlich kürzere Optimierungszeit. Bricht der GA den ersten Optimierungslauf nach 30 Sekunden ab und startet anschließend die Optimierung mit Re-Routingstrategie (2), ergibt sich eine gesamte Lösungszeit von einer Minute für die Kanten 1 und 13.

2-Kantenfehler

Wie in Abschnitt 7.1.1 gesehen, benötigt die Optimierung für zwei Kantenfehler abhängig von dem Weitverkehrsnetz bis zu 32 Tage. Treten Änderungen in einem Weitverkehrsnetz in kürzeren Abständen auf, kann die ganzzahlige lineare Optimierung nicht für alle 2-Kantenfehler Ersatzkonfigurationen berechnen. Die Optimierungszeiten des GA für 2-Kantenfehler sind in den Diagrammen 7.12 (a)-(c) dargestellt.

Für das Deutschland-17-Knotennetz findet der GA in 85 % der Fälle innerhalb von fünf Minuten eine Lösung. Der geringe Knotengrad des Netzes bewirkt wiederum,

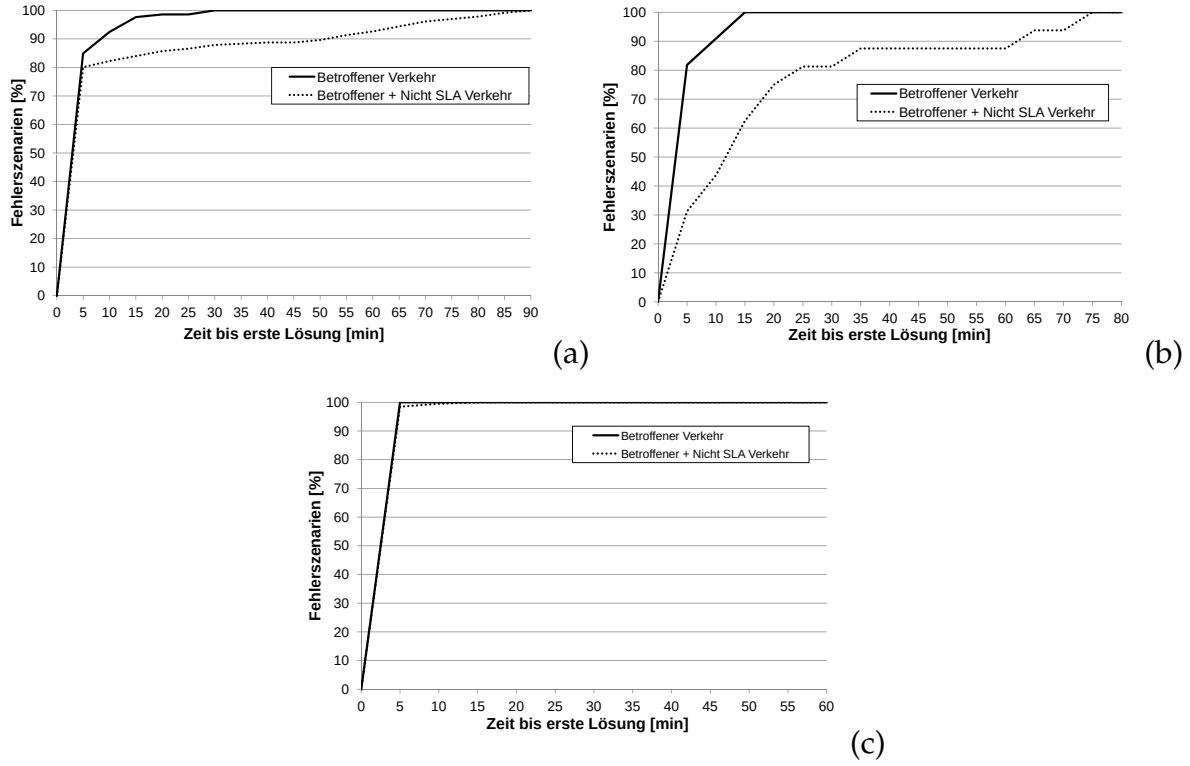


Abbildung 7.12: Kumulierte Optimierungsdauer für alle 2-Kantenfehler unter Verwendung der Re-Routingstrategien (a) Deutschland-17-Knotennetz (b) Nobel-EU-Netz (c) Nobel-US-Netz

dass beim Ausfall bestimmter Kanten die Optimierungszeit aufgrund der geringen Anzahl an Ersatzpfaden ansteigt. Fallen zwei Kanten zur selben Zeit aus, erhöht sich auch der Anteil der blockierten Verkehrsanforderungen. Mit Re-Routingstrategie (1) werden 3 % der Verkehrsanforderungen mit Dienstgütekriterien nicht geroutet. Mit Re-Routingstrategie (2) beträgt der Anteil 2 %.

Ähnliche Ergebnisse ergeben sich auch für das Nobel-EU-Netz in Abbildung 7.12 (b). 82 % der 2-Kantenfehler werden innerhalb von 5 Minuten gelöst. Allerdings existieren wiederum Kanten deren angeschlossene Knoten einen Knotengrad von 2 besitzen und daher die Optimierung verhältnismäßig lange dauert. Bei den verbleibenden 2-Kantenfehlern (18 %) benötigt der Algorithmus maximal 15 Minuten bis er eine Lösung findet. Bricht der GA die Lösungssuche frühzeitig nach 30 Sekunden ab und wechselt auf die nächste Re-Routingstrategie, benötigt er in diesen Fällen ebenfalls maximal 5 Minuten für eine erste gültige Lösung. Insgesamt können 3,49 % der Verkehrsanforderungen nicht geroutet werden.

Für das Nobel-US-Netz in Abbildung 7.12 (c) zeigt der GA die besten Ergebnisse bei 2-Kantenfehlern. Die Mehrheit der Fehlerszenarien (94 %) kann innerhalb von 5 Minuten gelöst werden. Weitere 5 % der 2-Kantenfehler können in maximal 15 Minuten gelöst werden. Aber auch in dem Nobel-US-Netz können nicht alle Verkehrs-

anforderungen mit Dienstgütekriterien geroutet werden. Insgesamt werden 1 % der Verkehrsanforderungen blockiert.

Die Ergebnisse machen deutlich, dass durch einen frühzeitigen Abbruch des Algorithmus die Optimierungszeit des GA bei denjenigen Fehlern weiter reduziert wird, die zur Lösung mindestens zwei der drei Re-Routingstrategien einsetzen.

Wellenlängenfehler

Der Online-Planungsalgorithmus kommt vor allem bei Fehlerszenarien zum Einsatz, die aufgrund der Komplexität oder der Vielzahl an Möglichkeiten eine ganzzahlige lineare Planung in adäquater Zeit nicht zulassen. Ein Beispiel für die hohe Anzahl an Möglichkeiten stellt der Ausfall von Wellenlängen dar. Die Diagramme 7.13 (a)-(c) zeigen vier unterschiedliche Ausfallszenarien für Wellenlängen in drei Weitverkehrsnetzen.

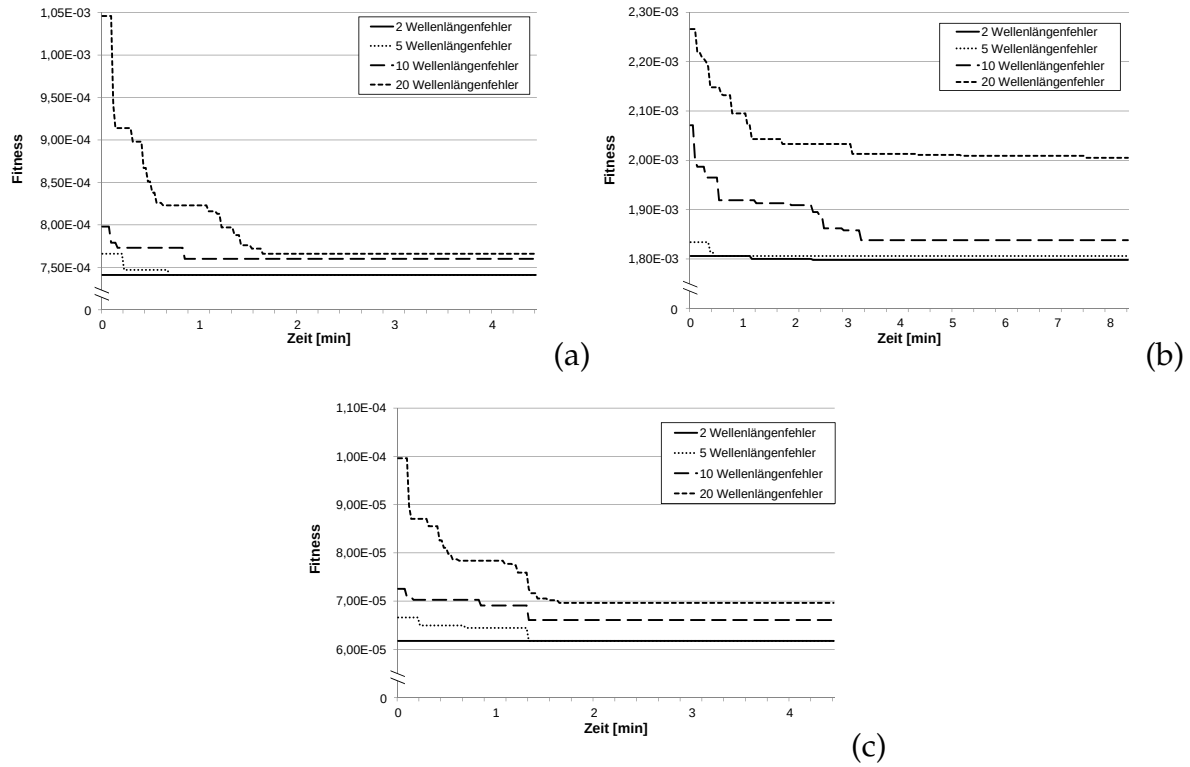


Abbildung 7.13: Anzahl der Wellenlängenfehler für (a) Deutschland-17-Knotennetz (b) Nobel-EU-Netz (c) Nobel-US-Netz

Wie auch bei den Kantenfehlern, kommen verschiedene Re-Routingstrategien zum Einsatz. Zunächst wird versucht, nur den Verkehr der ausgefallenen Wellenlänge neu zu routen. Führt dies nicht zum Erfolg, werden auch bestehende Verbindungen umgeleitet. In den Diagrammen erkennt man die schnelle Konvergenz des GA für alle Simulationsszenarien. Bereits nach fünf Sekunden findet der Algorithmus eine

Lösung bei bis zu 5 Wellenlängenfehlern für das Deutschland-17-Knotennetz. Bei 20 gleichzeitig ausgefallenen Wellenlängen existiert bereits nach 10 Sekunden eine erste gültige Lösung. Die Lösung verbessert sich im Deutschland-17-Knotennetz um 5 % nach einer Minute bei 10 Wellenlängenausfällen und um 26,67 % nach 1,7 Minuten bei 20 ausgefallenen Wellenlängen. Wie zu erwarten, werden keine Verkehrsanforderungen blockiert und das ausschließliche Re-Routing der betroffenen Verkehrsanforderungen führt zu einer Lösung.

Ähnliche Resultate erhält man für die anderen beiden Transportnetze. Für das Nobel-EU-Netz 7.13 (b) existieren für alle gezeigten Wellenlängenausfälle gültige Lösungen bereits nach 10 Sekunden. In einigen wenigen Fällen (4 %) dauert es 1 Minute bis eine gültige Lösung gefunden wird. Auch für das Nobel-US-Netz ergeben sich gültige Lösungen innerhalb von 10 Sekunden für alle in 7.13 (c) gezeigten Fehlerszenarien. Innerhalb von 1,7 Minuten verbessert sich die Fitness der Genome bei 20 Wellenlängenfehlern maximal um 30,10 %. Da aber bei der Online-Planung das schnelle Finden einer Lösung im Vordergrund steht, lohnt sich die Verbesserung im Verhältnis zum Zeitaufwand nicht.

Veränderung der Verkehrsmatrix

Eine weitere häufige Situation in einem Transportnetz ist die Veränderung des Verkehrsaufkommens. In diesem Abschnitt wird nur die Zunahme des Verkehrs betrachtet, da eine Verkehrsabnahme für das Weitverkehrsnetz keine Schwierigkeit darstellt, wenn bereits der gesamte initiale Verkehr geroutet werden kann. Für die Ergebnisse in den Diagrammen 7.14 (a)-(c), wurde eine unterschiedlich hohe Anzahl an neuen Verkehrsanforderungen betrachtet. Die zusätzlichen Verkehrsanforderungen sind in Wellenlängen gegeben und entsprechen damit einer Vergrößerung des Verkehrsaufkommens von 100 Gbit/s pro Wellenlänge. Alle neu hinzugefügten Verkehrsanforderungen besitzen Dienstgüteparameter wie eine maximale Verzögerung oder eine minimale Bandbreite.

Die Verkehrsmatrix wurde für alle Netze um 20, 40 beziehungsweise 60 Wellenlängen erhöht. Für das Deutschland-17-Knotennetz und das Nobel-EU-Netz bedeuten die zusätzlichen gerouteten Verkehrsanforderungen einen Zuwachs des transportierten Verkehrs um 4 %, 7 % beziehungsweise 11 %. Für das Nobel-US-Netz entspricht dies einer Erhöhung von 6 %, 11 % und 17 %.

Die Diagramme zeigen, dass der GA für die Veränderung der Verkehrsanforderungen um 20 beziehungsweise 40 neuen Wellenlängen in allen Beispielnetzen innerhalb von 10 Sekunden eine Lösung findet. Einige wenige neue Verkehrsanforderungen, die einen der zentralen Links benutzen, führen zu einer Optimierungszeit von maximal drei Minuten. Erhöht man die Anzahl der neuen Verkehrsanforderungen auf 60 Wellenlängen, so erhöht sich die Optimierungszeit des GA deutlich. Die Zeit bis zur ersten Lösung beträgt maximal fünf Minuten für das Deutschland-17-Knotennetz und das Nobel-US-Netz. Die Mehrheit der Lösungen findet der Algorithmus innerhalb von zwei Minuten. Beim Nobel-EU-Netz erhöht sich die Optimierungszeit dagegen

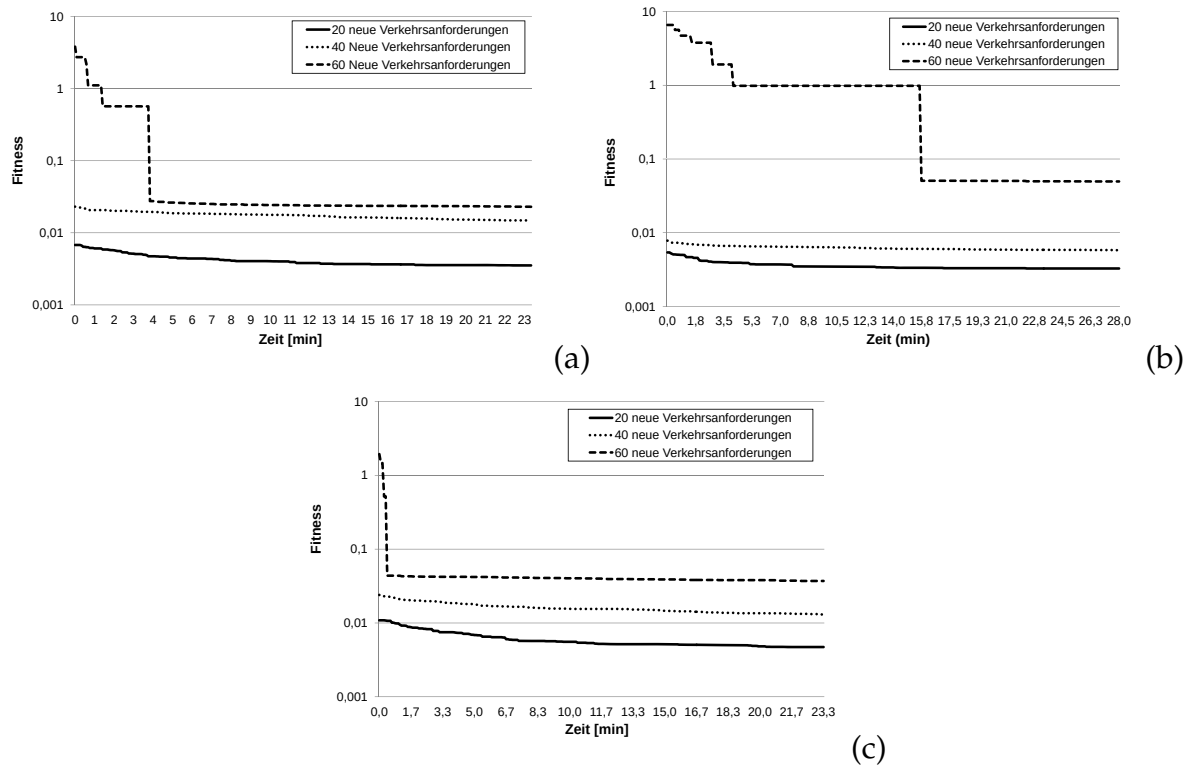


Abbildung 7.14: Hinzufügen von neuen Verkehrsanforderungen für (a) Deutschland-17-Knotennetz (b) Nobel-EU-Netz (c) Nobel-US-Netz

auf 16 Minuten. Dies liegt wie bereits erwähnt an der hohen Anzahl der Knoten mit einem Knotengrad von 2. Dies reduziert die Möglichkeit den Verkehr mit Dienstgüte durch das Transportnetz zu routen.

7.2.2 Diskussion der Ergebnisse des GA

Der entwickelte GA wurde anhand typischer Fehler in einem Weitverkehrsnetz auf seine Performanz untersucht. Für Wellenlängenausfälle und Verkehrsveränderungen findet der Algorithmus bereits nach 30 Sekunden eine gültige Lösung. Selbst für den gleichzeitigen Ausfall von 20 Wellenlängen oder das Hinzufügen von 40 zufälligen neuen Verkehrsanforderungen (Wellenlängen) berechnet der GA eine Lösung innerhalb von 50 Sekunden. Bei dem Ausfall von Wellenlängen werden alle Lösungen mit dem Re-Routing der betroffenen Anforderungen erreicht.

Für 1-Kantenfehler ergibt sich ein ähnliches Ergebnis wie bei den Wellenlängenfehlern. Allerdings muss der GA bei bestimmten Fehlern die zweite Re-Routingstrategie verwenden, um alle Verkehrsanforderungen routen zu können. Für die Mehrheit der Fehler (circa 80%) kann innerhalb von einer Minute eine Lösung gefunden werden.

Bei 2-Kantenfehlern erhöht sich die Lösungszeit für die Mehrheit der Fehler (circa 75 %) auf fünf Minuten. Allerdings variieren die einzelnen Optimierungszeiten

stark voneinander und einige 2-Kantenfehler lassen sich ebenfalls innerhalb einer Minute berechnen. Für die übrigen Fehler muss der GA auch die anderen Re-Routingstrategien verwenden, um eine Lösung zu finden. Dadurch erhöht sich die Lösungszeit. Bereits bei 2-Kantenfehlern ist nicht mehr genügend Kapazität vorhanden, um alle Verkehrsanforderungen zu routen.

Es hat sich gezeigt, dass bei der Verwendung von mehreren Re-Routingstrategien, ein frühzeitiger Abbruch die Lösungszeit erheblich reduzieren kann. Häufig findet der GA mit der neuen Re-Routingstrategie bereits nach wenigen Sekunden bis Minuten eine Lösung. Da aber bereits vorher eine Optimierung mit der alten Re-Routingstrategie stattgefunden hat, ist die gesamte Optimierungszeit deutlich höher. Die Untersuchungen zeigen, dass es für eine schnelle Lösung hilfreich ist, die Suche nach einer Lösung vorzeitig abzubrechen, um auf eine neue Re-Routingstrategie zu wechseln. Die Lösungszeit kann vor allem bei 2-Kantenfehler noch weiter verkürzt werden, wenn der GA die drei Re-Routingstrategien nicht sequentiell verwendet, sondern gleich mit einer der Re-Routingstrategien beginnt, die beim Umrouten alle Verkehrsanforderungen betrachtet. Allerdings existieren auch 2-Kantenfehler, die nur mit dem Umrouten der betroffenen Verkehrsanforderungen (erste Re-Routingstrategie) eine Lösung finden. Wie die Ergebnisse zeigen, weist die Lösungszeit des GA mit der ersten Re-Routingstrategie die kürzesten Lösungszeiten auf.

7.3 Kombination von Voraus- und Online-Planung

In den vorangegangenen Kapiteln erfolgte die Untersuchung der einzelnen Planungsalgorithmen des Netzmanagementsystems. Die Ergebnisse haben ergeben, dass die Vorausplanung von Ersatzkonfigurationen ein wesentlicher Bestandteil zum schnellen Auffinden von Ersatzwegen im Fehlerfall darstellt. Ergänzt mit der Online-Planung besteht die Möglichkeit, auch für nicht vorausgeplante Fehler eine Ersatzkonfiguration in wenigen Sekunden zu finden. Die Leistungsfähigkeit der teilautomatisierten Netzmanagementarchitektur wird in diesem Kapitel untersucht. Dazu wird in einer Simulation das Verhalten der Netzmanagementarchitektur bei verschiedenen Netzveränderungen und das Zusammenspiel von ganzzahliger linearer Optimierung und Heuristik untersucht.

Für die Simulationen wird das Deutschland-50-Knotennetz mit denselben Verkehrsanforderungen wie bei den vorherigen Untersuchungen verwendet. Beide Planungsalgorithmen werden zu Beginn der Simulation gestartet. Die ganzzahlige lineare Optimierung berechnet daraufhin die Ersatzkonfigurationen für die vorab definierten Fehlerfälle. Anschließend werden in bestimmten Zeitabständen 100 Fehlerfälle simuliert und die Reaktion des teilautomatisierten Netzmanagements analysiert. Die Auftrittswahrscheinlichkeit der einzelnen Fehler in der Simulation orientiert sich an den untersuchten Fehlerereignissen in [MIB+04]. Das bedeutet, dass 1-Linkfehler und Verkehrsveränderungen häufiger auftreten als 2-Linkfehler oder komplette Knotenausfälle. In den Untersuchungen werden auch die Degradationswerte der opti-

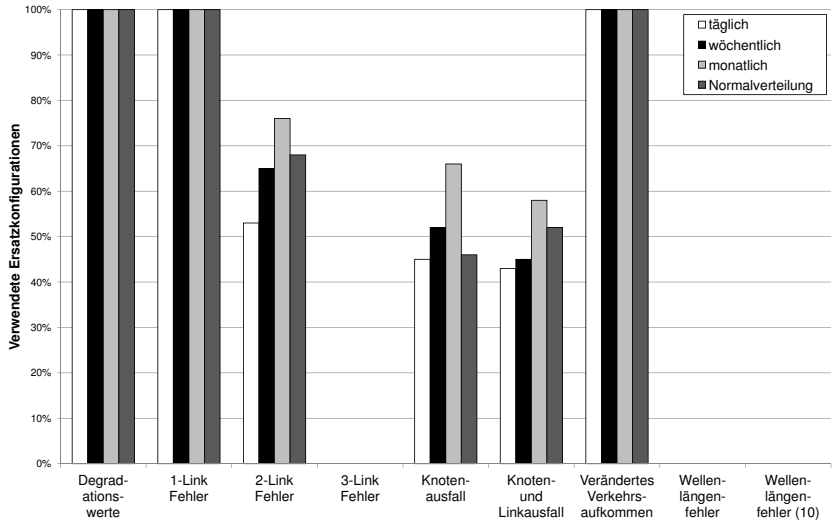
schen Netzkomponenten berücksichtigt. Wie in Kapitel 5 beschrieben, senden die Netzkomponenten eine Warnnachricht an das Netzmanagementsystem, sobald sie degradiert sind. Nach dem Empfang einer Degradationsnachricht, berechnet das Netzmanagement eine optimale Ersatzkonfiguration für die Kanten, entlang derer sich die degradierten Komponenten befinden.

Es werden zwei verschiedene Simulationen durchgeführt. Bei der ersten Simulation tritt der erste Fehler erst nach einer Woche auf, um dem Netzmanagement eine gewisse Zeit für die Vorausberechnung der Ersatzkonfigurationen zu geben. In der zweiten Simulation treten Fehler sofort nach Beginn der Simulation auf. Auf diese Weise wird die Stabilität des teilautomatisierten Netzmanagement bei einer geringen Anzahl vorab berechneten Ersatzkonfigurationen untersucht. Die Ergebnisse der ersten Simulation mit Vorlaufzeit sind in Abbildung 7.15 dargestellt.

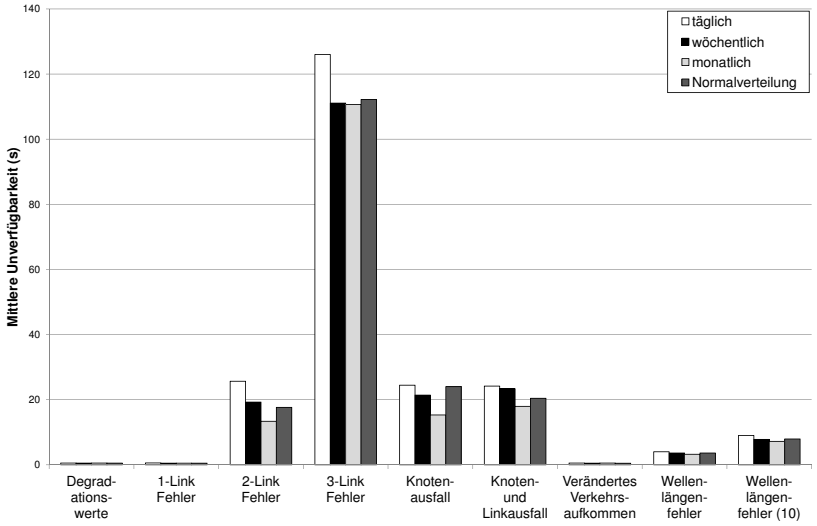
Zur Evaluierung des teilautomatisierten Netzmanagements wurden vier verschiedene Fehlerintervalle verwendet. Wie aus der Abbildung 7.15 (a) ersichtlich ist, nimmt die Trefferquote bei den vorab berechneten Ersatzkonfigurationen mit abnehmender Fehlerhäufigkeit zu. Beim Auftreten von Degradationen, 1-Linkfehlern und verändertem Verkehrsaufkommen findet das Netzmanagement unabhängig von der Fehlerfrequenz zu 100 % eine Ersatzkonfiguration. Beim Empfang von Degradationswerten liegt dies am Algorithmus zur Vorausplanung der Ersatzkonfigurationen. Erhält das Netzmanagementsystem Degradationsnachrichten von Netzkomponenten, berechnet der Algorithmus gleich im Anschluss eine Ersatzkonfiguration, die er in der Managementdatenbank speichert. Die Konfiguration erfolgt dann zu einem späteren Zeitpunkt.

Die Ersatzkonfigurationen für 1-Linkfehler und für ein verändertes Verkehrsaufkommen berechnet das Netzmanagement vor den anderen Fehlerfällen. Da der erste Fehler erst nach einer Woche auftritt, hat das Netzmanagement bereits für diese beiden Fehlerszenarien alle Ersatzkonfigurationen vorab geplant. 3-Linkfehler beziehungsweise Wellenlängenfehler werden aufgrund der hohen Anzahl an Kombinationen und der kurzen fehlerfreien Zeit nicht vorab berechnet. Bei diesen Fehlern verwendet das Netzmanagement zur Berechnung einer Ersatzkonfiguration den GA. Bei den restlichen Fehlerszenarien zeigt sich der Einfluss des Fehlerintervalls auf die Trefferquote der Ersatzkonfigurationen. Treten täglich Fehler auf, sinkt die Trefferquote auf 52 % für die 2-Linkfehlerszenarien. Bei Knotenausfällen fällt die Trefferquote weiter ab. Der vollständige Ausfall eines Netzknotens ereignet sich relativ selten und wird daher erst geplant, wenn wahrscheinlichere Fehlerszenarien vorausgeplant wurden. Bei einem wöchentlichen oder monatlichen Fehlerereignis steigt die Trefferquote auf über 50 % an. Allerdings ist die Zeit zwischen zwei Fehlern zu gering, um eine ausreichende Anzahl an Knotenfehlern vorab zu planen.

Abbildung 7.15 (b) zeigt die Unverfügbarkeit des Weitverkehrsnetzes pro Fehlerszenario für 100 aufgetretene Fehler an. In den Fehlerszenarien bei denen immer eine geeignete Ersatzkonfiguration vorhanden ist, findet das Netzmanagement innerhalb einer halben Sekunde eine Lösung. Entscheidend für die Lösungszeit ist die Suchdauer des Algorithmus für die Ersatzkonfigurationen in der Managementda-



(a)



(b)

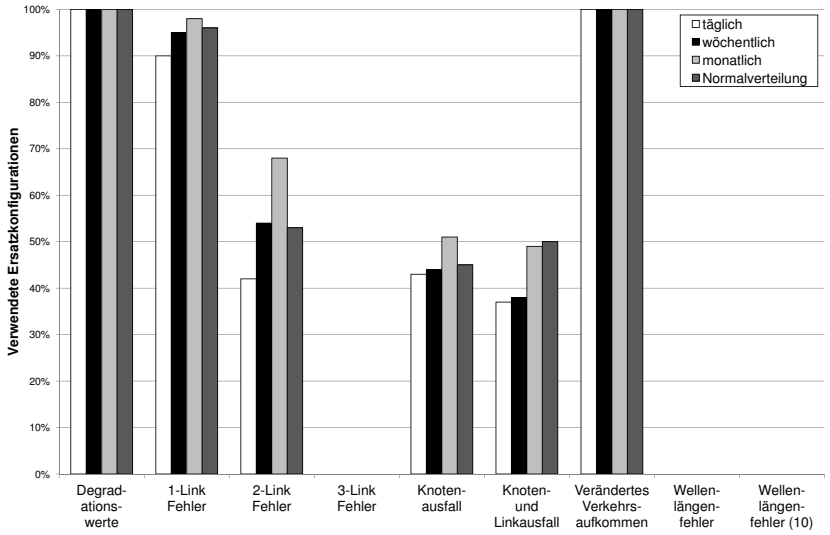
Abbildung 7.15: Deutschland-50-Knotennetz mit Vorlaufzeit (a) Anzahl verwendeter Ersatzkonfiguration (b) Unverfügbarkeit des Netzes

tenbank. Je geringer die Trefferquote bei den Ersatzkonfigurationen, desto höher ist die Unverfügbarkeit des Netzes. Für 2-Linkfehler benötigt der Planungsalgorithmus im Mittel zwischen 13 und 25 Sekunden, um eine Lösung zu finden. Die Knotenausfälle liegen in der gleichen Größenordnung wie die 2-Linkfehler. Wellenlängenfehler werden aufgrund der hohen Anzahl nicht vorausberechnet. Die Ergebnisse zeigen, dass auch ohne die Existenz einer Ersatzkonfiguration Lösungen innerhalb von wenigen Sekunden durch den GA gefunden werden. Der gleichzeitige Ausfall von 10 Wellenlängen führt zu einer Unverfügbarkeit von maximal 10 Sekunden. 3-Linkfehler führen zur höchsten Unverfügbarkeit des Weitverkehrsnetzes, da diese nicht vorausgeplant werden und die restliche Linkkapazität häufig nicht ausreicht, um alle Verkehrsanforderungen zu routen. Der Algorithmus versucht daher primär die Verkehrsanforderungen mit Dienstgütekriterien zu routen. Dadurch steigt die Komplexität des Optimierungsproblems und erhöht dementsprechend die Optimierungszeit.

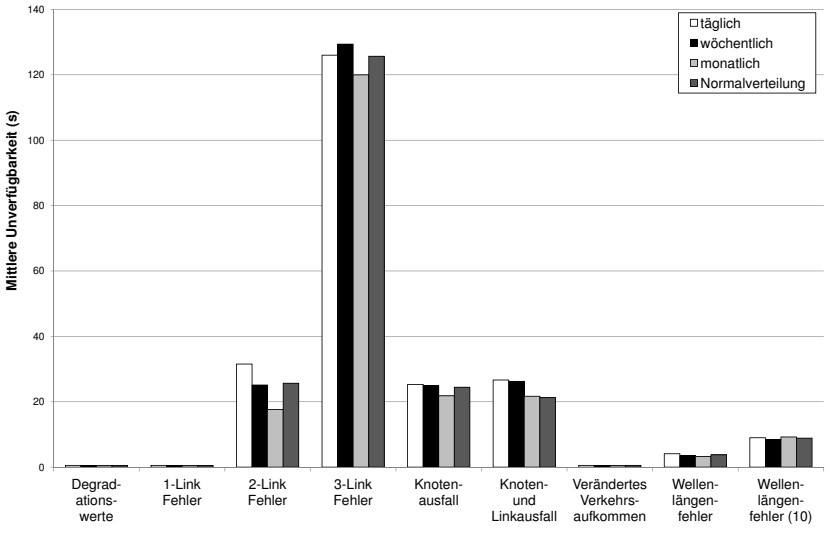
In Abbildung 7.16 sind die Ergebnisse für das gleiche Simulationsszenario dargestellt, allerdings entfällt die Vorlaufzeit von einer Woche für das Netzmanagementsystem. Die Fehlerereignisse treten somit sofort nach dem Start der Simulation auf.

Eine Trefferquote von 100% ergibt sich nur noch für Degradationsfehler und ein verändertes Verkehrsaufkommen, da die Vorausberechnung dieser Fehlerszenarien innerhalb eines Tages erfolgt. Im Vergleich zur vorherigen Simulation sinkt die Trefferquote bereits bei 1-Linkfehlern geringfügig ab. Hierfür sind 1-Linkfehler verantwortlich, die bereits an den ersten beiden Tagen auftreten und für die noch keine Ersatzkonfiguration vorab geplant wurde. Besonders deutlich wird die Reduktion der Trefferquote anhand des täglichen Fehlerszenarios. Die Unverfügbarkeit steigt um fünf Sekunden auf maximal 55 Sekunden an. Ähnliche Resultate ergeben sich für die übrigen Fehlerszenarien. Die Trefferquote für Ersatzkonfigurationen nimmt geringfügig ab und führt zu einer Erhöhung der Unverfügbarkeit des Netzes. Für die Fehlerereignisse ohne vorhandene Ersatzkonfiguration ergeben sich im Vergleich zur vorherigen Simulation keine Unterschiede.

Vergleicht man die beiden Simulationsszenarien, lässt sich zusammenfassend feststellen, dass die Vorausplanung von Ersatzkonfigurationen insbesondere bei den häufig auftretenden Fehlern zu einer schnellen Lösung führt. Vor allem die Veränderung des Verkehrsaufkommens, die Mitteilung von Degradationswerten und 1-Kantenfehlern lassen sich beinahe zu 100 % durch eine Ersatzkonfiguration lösen. Ebenso zeigt der GA bei Fehlerfällen, für die keine Ersatzkonfiguration existiert, eine geringere Unverfügbarkeit des Weitverkehrsnetzes. Eine höhere Ausfallzeit ergibt sich vor allem bei Fehlerereignissen, bei denen eine hohe Kapazität auf einmal ausfällt, wie dies bei 3-Linkfehlern der Fall ist. Die verbleibende Kapazität in dem Weitverkehrsnetz reicht häufig nicht aus um alle Verkehrsanforderungen zu routen. Beide Planungsalgorithmen, insbesondere der GA, versuchen in diesem Fall alle Verkehrsanforderungen mit Dienstgütekriterien zu routen. Die dadurch erhöhte Komplexität verlängert die Lösungszeit des GA und damit auch die Unverfügbarkeit des Netzes. Allerdings vermindert diese Strategie die vereinbarten Strafzahlungen des Netzbetreibers an



(a)



(b)

Abbildung 7.16: Deutschland-50-Knotennetz ohne Vorlaufzeit (a) Anzahl verwendeter Ersatzkonfiguration (b) Unverfügbarkeit des Netzes

seine Kunden.

Im nächsten Abschnitt werden *Reconfigurable Optical Add-Drop Multiplexer* (ROADM)s und deren Möglichkeit, die Flexibilität der Online-Planung zu erhöhen, betrachtet. Durch die optische Weiterleitung einer bestimmten Wellenlänge auf mehrere Ausgänge, werden in einem Weitverkehrsnetz zusätzliche Schutzpfade hinzugefügt, ohne dass neue Kapazitäten installiert werden.

7.4 Anwendung der Online-Planung auf heutige ROADMs

Die im vorherigen Kapitel entwickelte Heuristik berücksichtigt bei der Berechnung von Lösungen drei verschieden Re-Routingstrategien, allerdings wurden bei den Simulationen keine Wellenlängenkonverter betrachtet. Die Optimierung zeigt trotz der Einschränkung gute Ergebnisse für die untersuchten Fehlerfälle. Um die Flexibilität der Online-Planung bei Fehlerfällen weiter zu erhöhen, werden deshalb in diesem Abschnitt ROADMs betrachtet. In heutigen Weitverkehrsnetzen werden optische neu konfigurierbare Multiplexer ROADMs eingesetzt, die es während des Netzbetriebs erlauben, bestimmte Wellenlängen zu terminieren (drop) oder hinzuzufügen (add). In [GBS+10] werden unterschiedliche Arten von ROADMs und ihre spezielle Charakteristik beschrieben. Im Wesentlichen werden ankommende Lichtsignale mit Hilfe eines Splitters aufgeteilt und entweder über einen Multiplexer am Ausgang des ROADMs weitergeleitet oder über einen weiteren Splitter terminiert. Ein weiterer Splitter/Koppler wird zum Hinzufügen von neuen Wellenlängen genutzt. Jedoch besitzen ROADMs noch eine weitere interessante Eigenschaft, die für die Voraus- und Online-Planung verwendet werden kann: die Broadcast- & Select (B&S)-Funktionalität. Diese Eigenschaft wird in Abbildung 7.17 anhand eines ROADMs mit Knotengrad drei erläutert.

Ein optisches Signal, das am Eingang des Splitters (NW) ankommt, wird zu allen Ausgangs-*Wavelength Selective Switch* (WSS)s und zu dem lokalen Drop-Port gebroadcastet. Nur in diesen Komponenten wird selektiert, ob die Wellenlänge blockiert oder weitergeleitet wird. Im Fall des WSS können mehrere Signale der selben Wellenlänge ankommen, weshalb sichergestellt sein muss, dass nur ein Signal weitergeleitet wird, während die anderen blockiert werden. Ein Überblick über die zugrundeliegende Technologie findet sich in [Key05]. Zukünftige Entwicklungen, wie flexiblere Splitter und WSSs, zur Erweiterung der ROADM-Architektur werden in [TS07], [PKO+09], [Per10], [MKV10] und [GBS+10] eingehend dargestellt.

Das Ziel der Online-Planung ist, einen Routing- und Wellenlängenzuweisungs-Algorithmus für ROADMs zu entwickeln, der den Schutz von Diensten erhöht, indem die B&S-Eigenschaften von heutigen ROADMs ausgenutzt werden. Der Algorithmus fügt zusätzliche Schutzpfade zu den Arbeitspfaden in ein Transportnetz ein, ohne den aktuell gerouteten Verkehr zu beeinflussen. Teile der Ergebnisse finden sich in [Sch11].

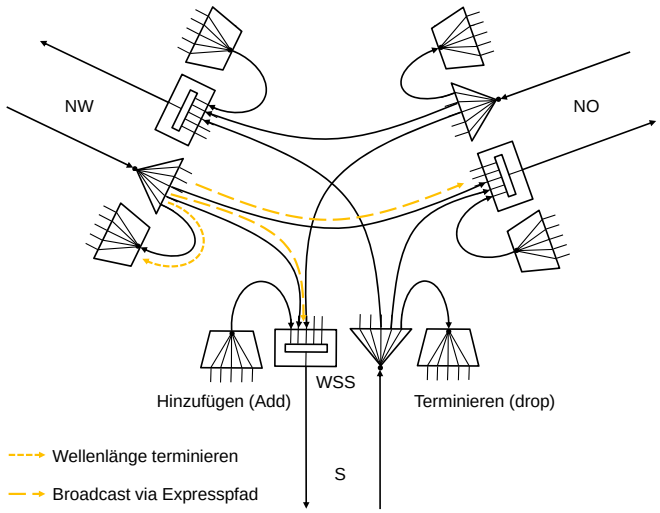


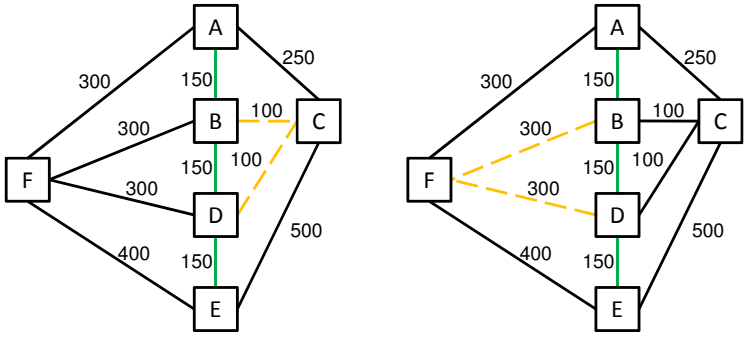
Abbildung 7.17: Broadcast- und Select-Funktionalität eines ROADMs mit Knotengrad 3

7.4.1 RWA-Ansätze für zusätzliche ROADM-basierende Schutzpfade

Es liegt die Idee zugrunde, auf ungenutzten Kapazitäten von Glasfasern zusätzlich Wellenlängen zu routen, die auf diesen Glasfasern noch nicht benutzt werden. Dadurch werden zusätzliche Schutzpfade geschaltet, ohne zusätzliche Transponder zu installieren. Diese können dann im Fehlerfall genutzt werden und verursachen nur sehr kurze Verzögerungen, da sie bereits beschaltet sind. Um diesen Schutzpfad zu nutzen, wird mit Hilfe von B&S eines ROADMs eine eingehende Wellenlänge nicht nur auf den Expressausgang weitergeleitet, sondern zusätzlich noch an weitere Ausgänge, auf der die Wellenlänge noch nicht benutzt wird.

Das Beispiel in Abbildung 7.18 stellt die beiden Möglichkeiten dar, die in einem Weitverkehrsnetz vorkommen.

Der grüne Pfad stellt den Arbeitspfad dar, der durch einen zusätzlichen Pfad geschützt werden soll. Die Gesamtlänge des Arbeitspfades beträgt 450 km, das bedeutet, dass ein Transponder mit einer Reichweite von 750 km ausreicht, um diese Verkehrsanforderung zu bedienen. Die maximale Übertragungsdistanz (MTD) von Transpondern ist aus [HGMS08] entnommen und es wird angenommen, dass für eine Verkehrsanforderung zwischen zwei Netzknoten der Transponder mit der minimal notwendigen MTD verwendet wird. In Abbildung 7.18 (a) befindet sich der Schutzpfad (gelb) innerhalb der Länge des installierten Transponders, während bei (b) der Schutzpfad die Transponderreichweite von 750 km überschreitet. In Weitverkehrsnetzen existieren beide Möglichkeiten und der Netzbetreiber muss entscheiden, ob ein neuer Transponder installiert wird oder der Weg verwendet wird, der keine zusätzlichen Kosten verursacht. Für die Untersuchungen in dieser Arbeit werden zwei verschiedene Szenarien angenommen, die im Folgenden dargestellt sind.



(a) Ersatzpfad innerhalb der Transponderreichweite

(b) Ersatzpfad außerhalb der Transponderreichweite

Abbildung 7.18: Hinzufügen eines zusätzlichen Schutzpfades

Schaltung von Schutzpfaden im laufenden Netzbetrieb

In diesem Szenario wird davon ausgegangen, dass das *Routing and Wavelength Assignment* (RWA) bereits erfolgt ist und keine blockierten Anforderungen existieren. Alle Verkehrsanforderungen sind damit geroutet, allerdings besitzen sie keinen Schutzpfad. Somit erhält man ein ungeschütztes Weitverkehrsnetz. Im zweiten Schritt werden Schutzpfade zu den Arbeitspfaden hinzugefügt, indem bereits geroutete Wellenlängen im ersten ROADM entlang des Pfades auf einen weiteren Ausgangsport umgelenkt und am letzten ROADM wieder terminiert werden.

Der Algorithmus für die nachträglich eingefügten Schutzpfade berechnet zunächst die ungeschützten RWAs für das Weitverkehrsnetz. Anschließend werden für alle Verkehrspaare, bei denen es möglich ist, Schutzpfade hinzugefügt. Alle Verkehrspaare, für die kein Schutzpfad gefunden werden kann, bleiben ungeschützt. Somit werden die bereits gerouteten Verkehrsanforderungen nicht beeinflusst, was die Vorgabe für den Algorithmus ist.

Planung der Schutzpfade zusammen mit den Arbeitspfaden

Um die Ergebnisse bezüglich der nachträglich eingefügten Schutzpfade zu vergleichen, wird noch ein weiterer Ansatz untersucht, bei dem die Schutzpfade nicht nachträglich eingefügt werden, sondern von Beginn an zusammen mit der Planung der Arbeitspfade. Es gelten die gleichen Bedingungen für die B&S-Architektur der ROADMs wie bereits bei dem vorhergehenden Szenario, so dass sich Arbeitspfad und Schutzpfade jeder Verkehrsanforderung den ersten und letzten Glasfaserlink teilen. Dazu wird der in [Bha97] vorgestellte Algorithmus zur Berechnung von kürzesten disjunkten Pfade zwischen zwei Knoten verwendet. Wenn keine disjunkten Pfade gefunden werden, bleiben die entsprechenden Arbeitspfade ungeschützt.

7.4.2 Simulationsparameter und Ergebnisse für die ROADM-Szenarien

Für die Simulation wurden drei unterschiedliche Weitverkehrsnetze verwendet. Die Topologien wurden wiederum aus der SNDlib [OPTW07] entnommen, um eine Vergleichbarkeit mit anderen Simulationsergebnissen zu erzielen. Dabei werden drei verschiedene Netzarten untersucht, die sich in ihrer Größe und Linkdichte unterscheiden: Ein Metronetz (Atlanta, Newyork), ein Weitverkehrsnetz (Deutschland-50-Knotennetz) und ein Ultra-Weitverkehrsnetz (Nobel-US-Netz).

Die Verkehrsanforderungen für die Beispielnetze sind so gewählt, dass die maximale Wellenlängenanzahl auf einem Link gleich 96 ist. Alle Verkehrsanforderungen zwischen zwei Knoten sind in Wellenlängen angegeben. Es werden wieder die Verkehrsmatrizen aus Kapitel 3 verwendet und entsprechend den Vorgaben skaliert und in Wellenlängen umgerechnet. Als zweites wird eine gleichmäßige Verteilung benutzt, die jedem Knotenpaar eine zufällige Anzahl an Wellenlängen zuordnet.

Für die Berechnung der Verfügbarkeit der Netze werden die mittlere Zeit zwischen zwei Fehlern *Mean Time Between Failure* (MTBF) und die mittlere Reparaturzeit *Mean Time To Repair* (MTTR) benötigt. Die notwendigen Werte dafür sind aus [SAF01] entnommen. Die Verfügbarkeit eines Pfades wird mit folgender Formel berechnet:

$$a_p = \frac{MTBF_p}{MTBF_p + MTTR} \tag{7.14}$$

Für die MTTR wird angenommen, dass sie für alle Glasfasern in den Beispielnetzen gleich ist. Die $MTBF_p$ für einen ungeschützten Pfad entspricht der Länge des Pfades multipliziert mit der Verfügbarkeit pro Kilometer. Für geschützte Pfade berechnet sich die Verfügbarkeit entsprechend aus Arbeitspfad und Schutzpfad.

Zunächst wird die maximale Anzahl an möglichen Schutzpfaden mit den aktuell tatsächlich aufgebauten verglichen. Dies wird anhand des Newyork-Netzes für die vorausgeplanten und die nachträglich hinzugefügten Schutzpfade evaluiert. Für die Simulationen wurden sowohl die SNDlib Verkehrsmatrizen (S-H und S-L) als auch die gleichförmig verteilten Verkehrsmatrizen (U-H und U-L) verwendet. „H“ steht dabei für hohes Verkehrsaufkommen und „L“ für halbes Verkehrsaufkommen im Vergleich zum Hochlastszenario.

In Abbildung 7.19 erkennt man, dass im vorausgeplanten Fall die Anzahl der potentiellen als auch der tatsächlichen Schutzpfade höher ist als im nachträglich hinzugefügten Fall. Dies liegt daran, dass bei der Vorausplanung der Algorithmus die Arbeits- und Schutzpfade frei wählen kann.

Allerdings ist im vorausgeplanten Fall auch die Anzahl der blockierten Verkehrsanforderungen höher. Der Unterschied in der Wellenlängenblockierung ergibt sich aufgrund von Blockierungen auf den Kanten. Bei der Betrachtung des erreichbaren Schutzlevels lässt sich feststellen, dass das nachträgliche Hinzufügen von Schutzpfa-

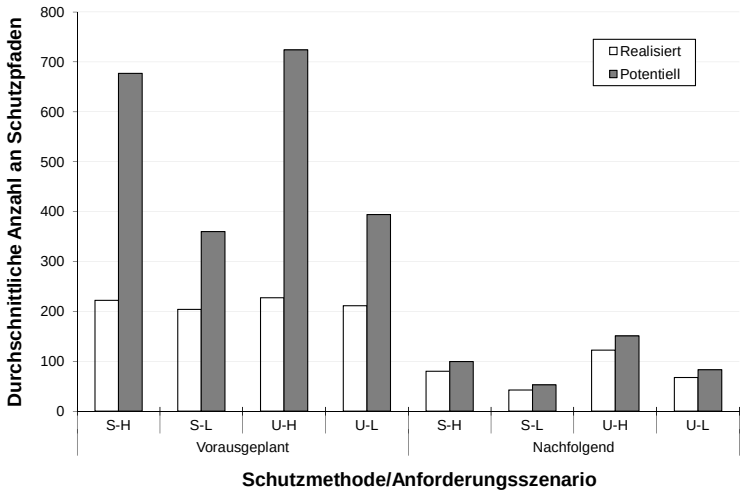
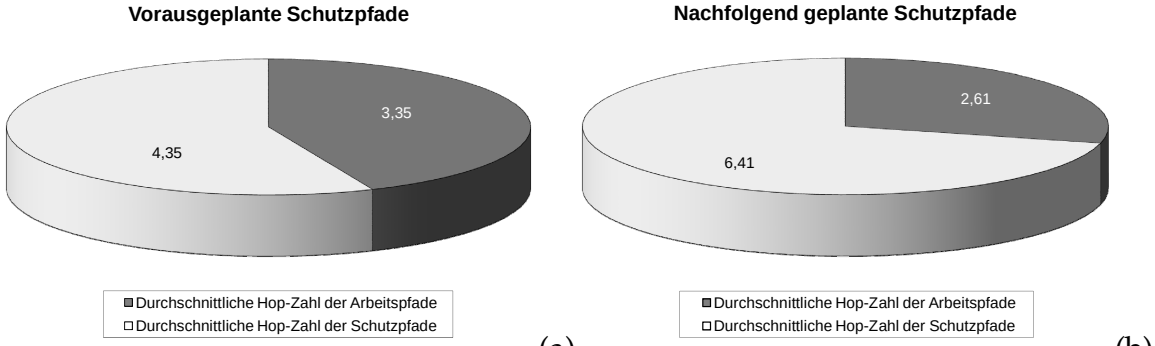


Abbildung 7.19: Verfügbarkeit

den für das Deutschland-50-Knotennetz in beiden Lastszenarien aufgrund des hohen Knotengrads funktioniert. Im Fall des Atlanta- und Nobel-US-Netzes, ist das geringe Lastszenario für das nachträgliche Hinzufügen von Schutzpfaden geeignet.

Bei der Betrachtung der Pfadlängen in Hops in Abbildung 7.20 stellt man fest, dass die durchschnittliche Pfadlänge der Arbeitspfade bei dem vorausplanenden Szenario um einen Hop länger ist, während bei dem nachträglich hinzugefügten Szenario die Schutzpfade länger sind.



(a) (b)

Abbildung 7.20: Durchschnittliche Hop-Länge der Pfade für (a) Vorausgeplante Pfade (b) Nachfolgend geplante Pfade

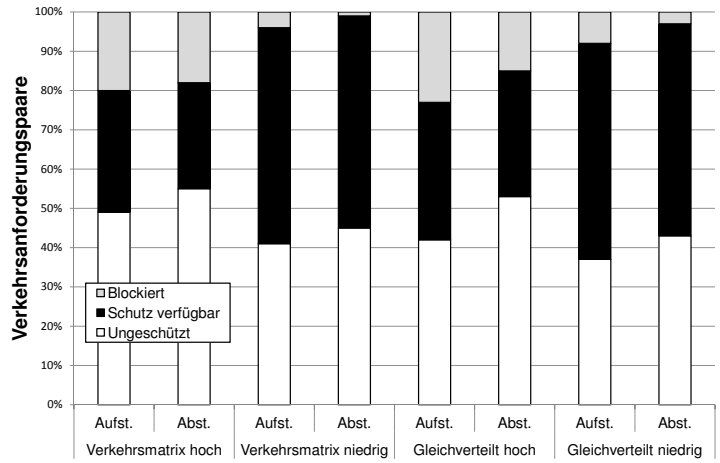
Dies lässt sich darauf zurückführen, dass bei dem vorausplanenden Szenario die Kombination aus Arbeits- und Schutzpfad optimiert wird, während bei nachträglich hinzugefügten Schutzpfaden nur die restlich vorhandenen Kapazitäten genutzt werden können. Die Schutzpfade sind deshalb beim nachträglichen Hinzufügen nicht zwingend die kürzesten Pfade, sondern abhängig von der Verfügbarkeit der freien Wellenlängen.

Im Folgenden wird der Einfluss der Zuweisung der Verkehrsanforderungen und der Wellenlängenzuweisung betrachtet. Die Ergebnisse in Abbildung 7.21 (a) für den vorausgeplanten Fall zeigen die Abhängigkeit der blockierten Anforderungen und der geschützten und ungeschützten Anforderungen von ihrer Zuweisung. Das geringere Lastszenario weist allgemein eine geringere Blockierung und damit eine höhere Anzahl an geschützten Pfaden auf. Die Anzahl der möglichen Schutzpfade hängt stark von den Netzeigenschaften ab. Ein Knotengrad von zwei erlaubt es einem ROADM nicht, einen Pfad auf zwei Expresspfade umzulenken, um einen nachträglichen Schutzpfad hinzuzufügen.

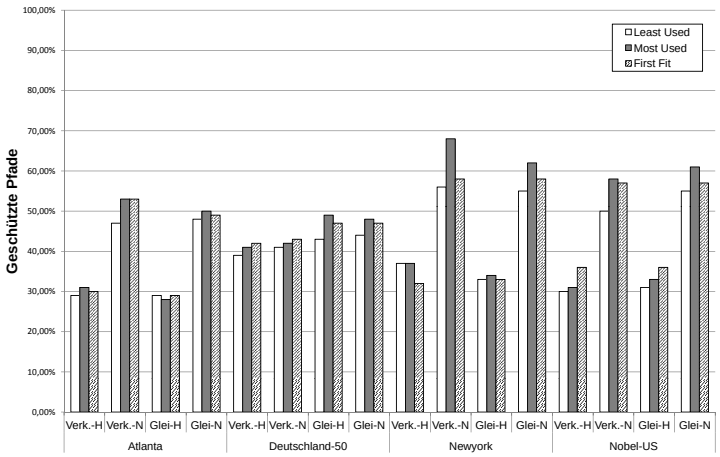
Für das Hochlastszenario stellt sich heraus, dass die Routingzuweisungen von Anforderungen in absteigender Reihenfolge eine geringere Blockierung verursachen. Werden die kürzeren Anforderungspfade zuerst zugewiesen, verursachen diese eine Blockierung der langen Anforderungspfade auf einigen Links. Für das Routing von längeren Pfaden existieren unter Beibehaltung der selben Wellenlänge weniger alternative Pfade. Deshalb steigt die Blockierung an, wenn die potentiellen Pfade bereits durch kurze Anforderungspaare blockiert sind.

Bei der Zuweisung der Wellenlängen in Abbildung 7.21 (b) ergeben sich keine großen Unterschiede bei der Vorausplanung der Schutzpfade für die verschiedenen Topologien. Wie in [ZJM00] beschrieben, besitzt die Zuweisung der am meisten genutzten Wellenlänge („Most Used“) etwas bessere Ergebnisse, als die zwei anderen Zuweisungsstrategien. Diese Zuteilung verhindert Blockierungen dadurch, dass freie Wellenlängen so lange wie möglich aufgehoben werden. Jedoch zeigen die Ergebnisse des Nobel-US-Hochlastszenarios, dass die Zuweisung der zuerst passenden Wellenlänge („First Fit“) bessere Ergebnisse als die Zuweisung der am meisten genutzten Wellenlängen liefert. Dies kann zum Beispiel für Router oder bei einer gefordert kleinen Berechnungszeit eingesetzt werden, da keine Bewertung von verwendeten Wellenlängen erfolgen muss und der Algorithmus eine kürzere Laufzeit besitzt.

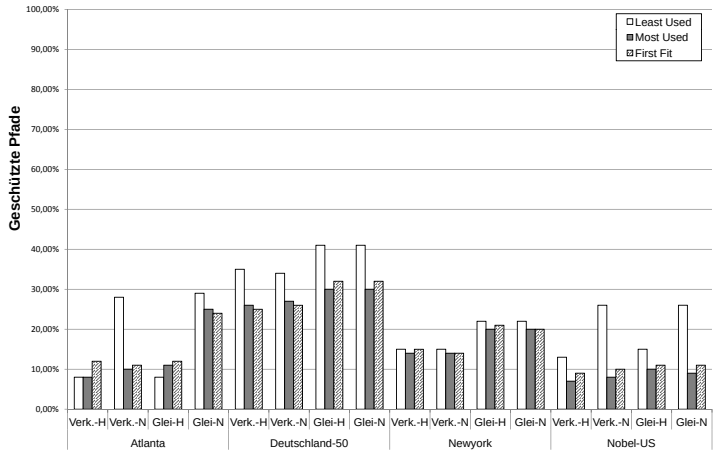
Bei den nachträglich hinzugefügten Schutzpfaden wirkt sich die Art der Wellenlängenzuweisung auf die Blockierung und die Anzahl der Schutzpfade stärker aus (Abbildung 7.21 (c)). Im Fall des nachträglich hinzugefügten Schutzes hängt die benutzte Wellenlänge für den Schutzpfad von der Wellenlänge des Arbeitspfades ab. Deshalb führt die „Most Used“-Methode zu den schlechtesten Ergebnissen, da die selbe Wellenlänge wie beim Arbeitspfad nicht mehr für einen Schutzpfad genutzt werden kann, da sie bereits auf den meisten Links verwendet wird. Die Zuweisung der zuerst gefundenen freien Wellenlänge („First Fit“) führt zu einem ähnlichen Ergebnis wie die „Most Used“-Methode. Nur im Fall der Atlanta-Topologie mit hohem Lastszenario erzielt die Zuweisung der am meisten genutzten Wellenlängen eine geringere Blockierung und eine höhere Anzahl an geschützten Pfaden. Dies liegt an der hohen Linkdichte in dieser Topologie und der damit verbundenen größeren Anzahl an Ersatzpfaden.



(a)



(b)



(c)

Abbildung 7.21: Einfluss der (a) Anforderungszuweisungen und Wellenlängenzuweisung für (b) Vorausgeplante Schutzpfade (c) Nachträglich hinzugefügte Schutzpfade

Auswirkungen der verschiedenen Netztopologien auf den Algorithmus

Um den Einfluss des Knotengrads und der Linklänge auf den RWA-Algorithmus für ROADMs zu bestimmen, werden in diesem Abschnitt die verschiedenen Netztopologien genauer untersucht. Ein entscheidender Parameter ist dabei die erreichte Anzahl der Schutzpfade im Vergleich zur maximal möglichen Anzahl der Schutzpfade. Das theoretische Maximum für die mögliche Anzahl an Schutzpfaden ist gleich der Anzahl der Arbeitspfade der Länge größer gleich drei, da diese Pfade als Schutzpfade geeignet sind, vorausgesetzt es existiert eine freie Wellenlänge. In Abbildung 7.22 wird das erreichte Schutzpotential, welches die Anzahl der hinzugefügten Schutzpfade geteilt durch das theoretische Maximum darstellt, für alle verwendeten Topologien veranschaulicht.

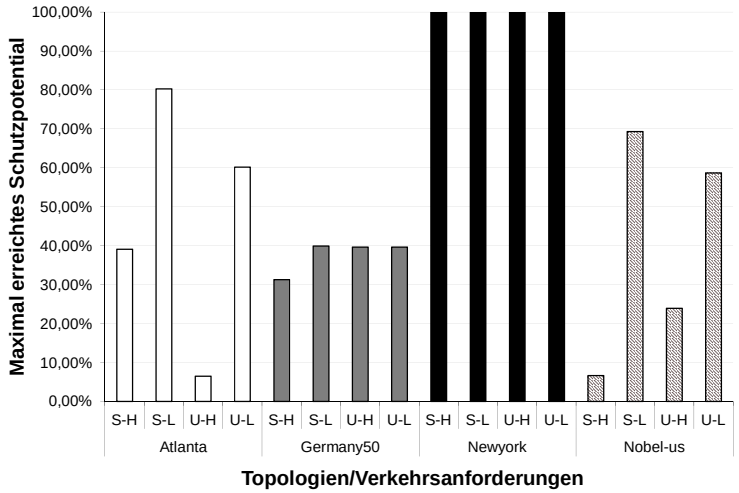


Abbildung 7.22: Verwendetes Schutzpotential für alle simulierten Topologien und Anforderungen

Für die Atlanta- und Nobel-US-Topologie sind die Ergebnisse sehr stark abhängig von dem benutzten Anforderungsszenario, sowohl bei der Zuweisung als auch beim Volumen der Anforderungen. Der Grund dafür liegt in der geringen Linkanzahl der beiden Topologien. Mit steigenden Anforderungen sinkt die Wahrscheinlichkeit einen Pfad für eine bestimmte Wellenlänge zu finden. Das Deutschland-50-Knotennetz zeigt eine interessante Charakteristik, da das Schutzpotential nicht die 40 % Marke überschreitet und für drei der vier Verkehrsszenarien gleich groß ist. Dies liegt an dem geringen Knotengrad des Netzes, der an bestimmten Knoten zu einer Engstelle führt, über die eine große Anzahl an Verkehrsanforderungen geroutet werden. Newyork stellt die Topologie mit dem höchsten mittleren und maximalen Knotengrad dar. Diese Topologie erreicht dadurch ein Schutzpotential von 100 %, da ausreichend Links vorhanden sind, auf denen nachträglich dieselbe Wellenlänge des Arbeitspfades geschaltet werden kann.

Ein weiterer wichtiger Parameter für Weitverkehrsnetze ist deren Verfügbarkeit,

die im Folgenden für die verschiedenen Netztopologien betrachtet wird. In Abbildung 7.23 sind die Verfügbarkeiten für die vier verwendeten Beispielnetze vor und nach dem Hinzufügen von Schutzpfaden dargestellt.

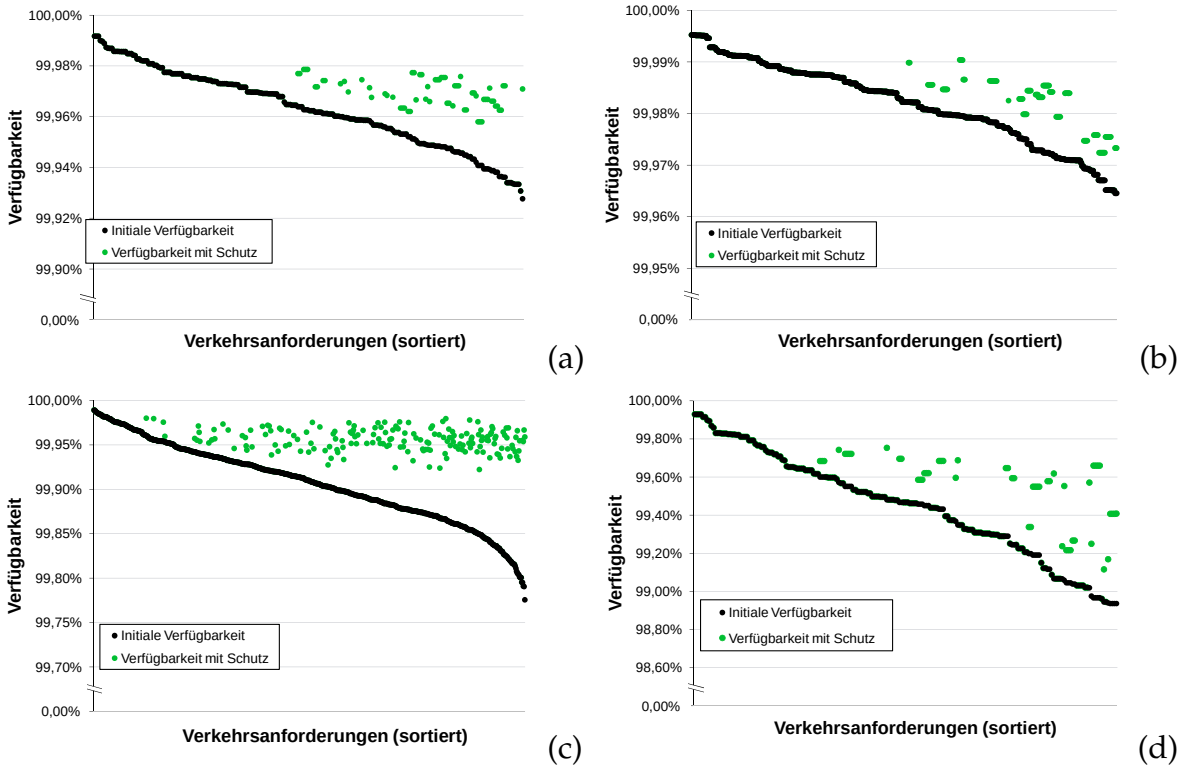


Abbildung 7.23: Verfügbarkeit vor und nach dem Hinzufügen von Schutzpfaden: (a) Atlanta mit uniform-low (b) Newyork mit uniform-high (c) Deutschland-50-Knotennetz mit uniform-high (d) Nobel-US mit uniform-low

Die Verfügbarkeiten sind aufsteigend nach der Länge der Verkehrsanforderungspaare sortiert. Allgemein lässt sich für alle vier Topologien feststellen, dass die kürzeren Verkehrsanforderungen eine identische Verfügbarkeit vor und nach dem Hinzufügen von Schutzpfaden besitzen. Dies liegt an der geringen Anzahl von Hops, die bei bestimmten Pfaden kleiner als drei ist, und der daraus resultierenden Begrenzung, dass der B&S-Schutz der ROADMs nicht verwendet werden kann. Bei längeren Anforderungspfaden steigt die Verfügbarkeit durch zusätzliche Schutzpfade an.

Die Ergebnisse der Atlanta- und Newyork-Topologie zeigen eine Vergrößerung der Verfügbarkeit um 31 Minuten beziehungsweise um weniger als 10 Minuten pro Jahr und Verkehrsanforderung. Dies entspricht einer Reduzierung der Ausfallzeit des gesamten Netzes um 118 h beziehungsweise 114 h, was einer Reduzierung der Unverfügbarkeit um 1,34 % entspricht. Für das Atlanta-Netz bedeutet dies, dass ohne Transponderaufrüstung 28,38 % der Anforderungen nachträglich mit der nicht verkehrsbeeinflussenden Methode geschützt werden und dabei die jährliche Ausfallzeit um 16 % reduziert wird. In Abbildung 7.23 (c) ist die Verfügbarkeit für

das Deutschland-50-Knotennetz dargestellt. Im Durchschnitt wird die Verfügbarkeit pro Pfad und Verkehrsanforderung um mehr als 2 h erhöht. Das ergibt insgesamt eine Reduzierung der Ausfallzeit um 1246,5 h pro Jahr. Die Unverfügbarkeit des Netzes wird damit um 26 % reduziert. Auch hier wurden wiederum nur Schutzpfade betrachtet, die keine zusätzlichen Kosten verursachen.

In Abbildung 7.24 sind die Anzahl der notwendigen Transponderaufrüstungen dargestellt, um den maximalen nachträglichen Schutz für die jeweilige Topologie zu erreichen.

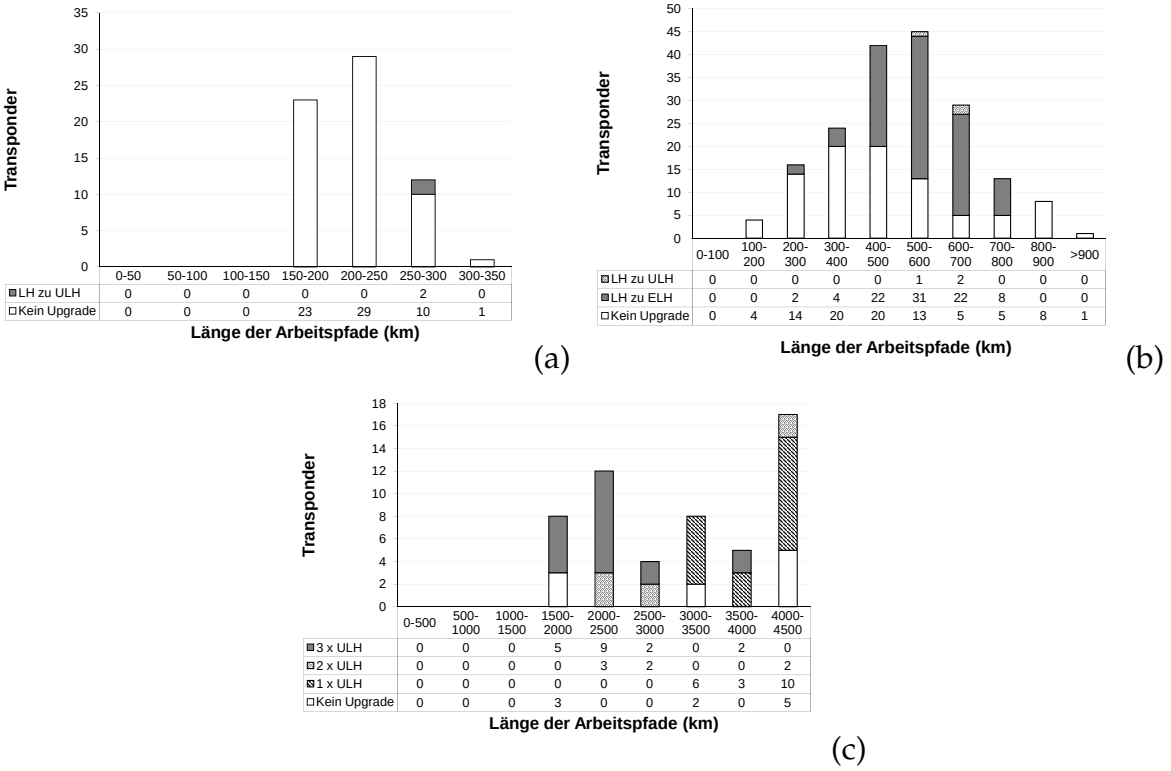


Abbildung 7.24: Transponderaufrüstung, um maximalen nachträglichen Schutz zu erreichen: (a) Atlanta mit uniform-low (b) Deutschland-50-Knotennetz mit uniform-high (c) Nobel-US mit uniform-low

Anhand der Diagramme sieht man die Abhängigkeit der nachträglichen Schutzmethode von der Pfadlänge und damit die Abhängigkeit von der Topologie. In einem Metronetz wie Atlanta wird nur in wenigen Fällen eine Umrüstung von einem *Long Haul* (LH) auf einen *Ultra Long Haul* (ULH) benötigt, um Schutzpfade nachträglich zu installieren. Für das Atlanta-Netz benötigt man nur für Pfade der Länge 250 bis 300 km eine Umrüstung. Anders sieht es bei Weitverkehrsnetzen aus, die längere Anforderungspfade aufweisen.

Im Fall des Deutschland-50-Knotennetzes werden 90 von 182 Schutzpfaden mit dem ursprünglich installierten Transponder bedient. Um die anderen Schutzpfade zu installieren, muss eine Aufrüstung von einem LH- zu einem *Extra Long Haul*

(ELH)-Transponder erfolgen. Bei drei Verkehrsanforderungen wird eine Umrüstung auf eine ULH benötigt, da die Ersatzpfade eine Länge von über 1500 km besitzen. Die Verwendung dieser langen Ersatzwege kommt durch die Definition des Algorithmus zustande, der alle möglichen Pfade für den Schutz betrachten soll, ohne Einschränkung der Entfernung. Bei einer zusätzlichen Betrachtung von SLAs für bestimmte Verkehrsanforderungen sind unter Umständen solch lange Ersatzpfade nicht möglich, da sie die Dienstgütekriterien verletzten.

Noch deutlicher wird die Abhängigkeit des nachträglichen Schutzes bei der Betrachtung des Nobel-US-Netzes in Abbildung 7.24 (c). In dieser Topologie sind nur wenige Links vorhanden, die aber sehr große Distanzen aufweisen. Die geringe Linkanzahl limitiert die Anzahl der möglichen Schutzpfade auf zwei Arten. Zum einen gibt es nur wenige disjunkte Ersatzpfade zum gerouteten Arbeitspfad und gleichzeitig sind die Links sehr stark belastet. Das bedeutet, dass auf den stark belasteten Links bereits viele Wellenlängen verwendet werden, die nicht mehr für den Schutzpfad zur Verfügung stehen. In der Nobel-US-Topologie ergeben sich deshalb nur 10 Schutzpfade, die keine Transponderumrüstung benötigen und ohne zusätzliche Kosten realisiert werden können. Die Mehrheit der möglichen Schutzpfade kann erst mit einer Umrüstung auf zwei beziehungsweise drei ULH realisiert werden. Die Ergebnisse zeigen, dass der Zuwachs an Schutzpfaden im Fall des Nobel-US-Netzes sehr gering ist und durch die Umrüstung der Transponder sehr hohe Kosten verursacht. Obwohl die Anzahl der zusätzlichen Schutzpfade und die Erhöhung der Verfügbarkeit dem Atlanta-Netz ähneln, ist das nachträgliche Hinzufügen von Ersatzpfaden bei der Nobel-US-Topologie aus finanzieller Sicht nicht lohnenswert.

7.5 Zusammenfassung

In diesem Kapitel wurden die Planungsprozesse des teilautomatisierten Netzmanagementsystems untersucht. Dazu wurden unterschiedlich große Weitverkehrsnetze und verschiedene Fehlerszenarien verwendet. Im ersten Teil erfolgte eine Evaluierung der linearen ganzzahligen Optimierung. Es hat sich gezeigt, dass für die Referenznetze Nobel-EU und Nobel-US eine Vorausplanung aller definierten Fehlerszenarien in adäquater Zeit möglich ist. Im Fall des Deutschland-50-Knotennetzes dauert die Vorausplanung im Verhältnis zu den Fehlerintervallen zu lange, weshalb die Reihenfolge der Vorausplanung einen großen Einfluss auf die maximal mögliche Anzahl an vorausgeplanten Ersatzkonfigurationen hat.

Der zweite Teil des Kapitels befasst sich mit einem GA, der zur schnellen Planung verwendet wird, wenn keine Ersatzkonfiguration gefunden wurde. Der GA verwendet drei unterschiedliche Re-Routingstrategien, um eine Lösung zu berechnen. Ist nach einem aufgetretenen Fehler die verbleibende Kapazität in dem Weitverkehrsnetz zu gering, versucht der GA primär die Verkehrsanforderungen mit Dienstgütekriterien zu routen. Für die meisten Fehlerszenarien findet der GA innerhalb von wenigen Sekunden eine Lösung. Allerdings steigt die Optimierungszeit auf mehrere Minuten,

wenn die verbleibende Netzkapazität zu gering ist. Für diese Fälle hat sich gezeigt, dass ein vorzeitiger Abbruch des GA und der anschließende Wechsel zu einer neuen Re-Routingstrategie schneller zu einer Lösung führt, als wenn der GA bis zum Abbruchkriterium arbeitet. Insbesondere bei 2-Linkfehlern und Knotenausfällen führte der zeitgesteuerte Abbruch zu einer Lösung in kürzerer Zeit.

Anschließend wurde das Zusammenspiel der beiden Planungsprozesse anhand von verschiedenen Fehlerszenarien und Auftrittszeitpunkten untersucht. Es hat sich gezeigt, dass durch die Vorausberechnung der Ersatzkonfigurationen eine hohe Trefferquote bei den wahrscheinlicheren Fehlerszenarien erzielt wird. Auch für 2-Linkfehlerszenarien findet der Planungsprozess abhängig von dem Fehlerintervall noch in über 50 % der Fälle eine geeignete Ersatzkonfiguration. Existiert keine geeignete Ersatzkonfiguration, findet der GA in den meisten Fällen innerhalb einer Minute eine Lösung.

Der letzte Teil des Kapitels hat sich mit ROADMs und deren Möglichkeit beschäftigt, nachträglich Schutzpfade hinzuzufügen ohne den bereits gerouteten Verkehr zu beeinflussen und ohne zusätzliche Kosten zu verursachen. Die Ergebnisse zeigen, dass in allen untersuchten Topologien Anforderungen durch das nachträgliche Hinzufügen von Ersatzpfaden geschützt werden, wenn ausreichend Restkapazität vorhanden ist. Der Erfolg der nachträglich hinzugefügten Schutzpfade hängt dabei von der Topologie und den installierten Transpondern ab. In Metronetzen können alle nachträglich möglichen Schutzpfade ohne Zusatzkosten geschaltet werden. Bei Weitverkehrsnetzen führt das nachträgliche Hinzufügen von Schutzpfaden zu geringen Kosten. Dagegen sind Ultra-Weitverkehrsnetze für das nachträgliche Hinzufügen von Schutzpfaden nicht geeignet.

8 Zusammenfassung

Die steigenden Anforderungen heutiger und zukünftiger Dienste bezüglich Verfügbarkeit und Bandbreite sowie die hohen Wachstumsraten des Datenverkehrs erfordern flexible und hoch verfügbare Weitverkehrsnetze. Dem steigenden Datenverkehr stehen auf Seiten des Netzbetreibers sinkende Einnahmen pro Netzanschluss gegenüber, was den Netzbetreiber dazu zwingt, die Betriebskosten des Weitverkehrsnetzes zu reduzieren. Ein viel versprechender Ansatz ist die Teilautomatisierung des Netzmanagements, um auf veränderte Anforderungen an das Netz schnell und flexibel reagieren zu können.

In dieser Arbeit wurden deshalb verschiedene Aspekte eines teilautomatisierten Netzmanagementsystems untersucht. Teilautomatisiert bezieht sich in dieser Arbeit auf die Tatsache, dass das Netzmanagementsystem die Überwachung und die Planung des Netzes selbständig durchführt, die Ergebnisse aus den beiden Schritten allerdings dem Netzbetreiber mitteilt. Der Netzbetreiber entscheidet anschließend, ob und wann die Konfiguration durchgeführt wird.

Um eine robuste Planung des Routings durchzuführen, wurden zunächst heutige Dienste anhand ihrer Verkehrsverteilung und ihrem Verkehrsanteil am bestehenden Datenaufkommen untersucht. Das entwickelte Verkehrsmodell basiert auf einem populationsbasierten Ansatz, bezieht aber zusätzlich noch Netzaustauschknoten, die Verteilung von Servern und die Verteilung von Unternehmensstandorten mit ein. Die Ergebnisse zeigen, dass abhängig von der Verteilung der Netzaustauschknoten und den Servern eine asymmetrische Verkehrsmatrix entsteht. Mittels eines Hypothesentests wurde bestätigt, dass die entwickelten Verkehrsmodelle ähnliche Charakteristiken wie real gemessene Verkehrsmatrizen besitzen und deshalb für die Planung von Weitverkehrsnetzen geeignet sind.

Damit das Netzmanagement automatisiert nach Fehlern suchen kann, wurden die Auswirkungen von Konfigurationsfehlern untersucht. Die Schwierigkeit bei Konfigurationsfehlern besteht darin, dass sie häufig ein ähnliches Fehlermuster wie physikalische Fehler aufweisen und daher schwer zu erkennen sind. In einem ersten Schritt erfolgte eine detaillierte Beschreibung häufiger Fehlermuster von Konfigurationsfehlern. Dabei stellte sich heraus, dass die Konfiguration von Filterregeln und Sicherheitsregeln eine häufige Fehlerquelle darstellt und im schlechtesten Fall zum Ausfall eines oder mehrerer Links führt. Im Anschluss erfolgte zum Priorisieren der Konfigurationsfehler die Entwicklung eines Bewertungsschemas, welches vom teilautomatisierten Netzmanagementsystem verwendet wird. Das Bewertungssystem basiert auf verschiedenen Einflussgrößen wie der Anzahl der Konfigurationsbefehle und der Anzahl der konfigurierten Netzelemente.

Die Analyse von Konfigurationsfehlern reicht allerdings nicht aus, um die Verfügbarkeit eines Weitverkehrsnetzes zu erhöhen. Im nächsten Schritt wurde deshalb ein proaktives Verfahren entwickelt, um Fehler zu finden, bevor sich diese auf ein Netz auswirken. Dazu wurden die physikalischen Werte verschiedener optischer Netzelemente betrachtet, welche die Degradation der optischen Netzelemente beschreiben. Zunächst wurde ein Alterungsmodell für die optischen Elemente entwickelt, welches es ermöglicht, festzustellen, wann die optischen Netzelemente ihre maximale Degradation erreicht haben und ausgetauscht werden müssen. Anschließend erfolgte die Untersuchung verschiedener Austauschstrategien für *Erbium dopted Fiber Amplifier* (EDFA)s anhand eines einzelnen Links, wie er in Weitverkehrsnetzen häufig vorkommt. Die Ergebnisse zeigen, dass der Austausch aller EDFAs auf einem Link im Vergleich zum Austausch der degradierten EDFAs die Verfügbarkeit des Links steigert. Allerdings wird bei Verwendung dieser Strategie innerhalb der gleichen Zeitdauer eine größere Anzahl an EDFAs ausgetauscht.

Im zweiten Schritt wurde das Degradationsmodell anhand eines Referenznetzes untersucht und mit einem *Failures in Time* (FIT)-Modell verglichen, weil der Ausfall von optischen Komponenten nicht vorhergesehen werden kann. Die Untersuchungen wurden zusätzlich noch auf optische Laser und Empfänger ausgeweitet. Des Weiteren wurde die Auswirkung der Anzahl der Betriebszentren auf die Reparaturzeit und Reparaturkosten analysiert. Die Ergebnisse zeigen, dass die Überwachung der Degradationsparameter die Verfügbarkeit des Netzes deutlich steigert. Die Reparaturzeit des Degradationsmodells liegt um 62% niedriger als beim FIT-Ratenmodell. Allerdings kommt es, bei dem untersuchten Link, zu einer höheren Anzahl an ausgetauschten optischen Komponenten. Aus diesem Grund ist die Fahrtzeit der Techniker beim Degradationsmodell höher als beim FIT-Ratenmodell. Die Planung der Wartungsphase und eine höhere Anzahl von Betriebszentren ermöglichen allerdings eine Reduzierung der Fahrzeiten der Techniker, so dass sich diese denen des FIT-Ratenmodells annähern. Um die Auswirkungen der beiden Modelle auf die Betriebskosten zu untersuchen, wurden neben den Reparaturkosten zusätzlich noch die Kosten für Strafzahlungen betrachtet. Die Untersuchungen haben gezeigt, dass abhängig davon, ob ein Netzbetreiber eine Wiederherstellung des Pfades oder zusätzliche Schutzpfade zusichert, die beiden Modelle die gleichen Betriebskosten aufweisen, wenn 6 Prozent beziehungsweise 0,5 Prozent der Fehler die Dienstgüte verletzen.

Der letzte Teil der Arbeit befasst sich mit dem teilautomatisierten Netzmanagementsystem. Zunächst erfolgten die Beschreibung der Komponenten des Netzmanagementsystems und der Austausch der Informationen zwischen diesen. Anschließend erfolgte eine eingehende Darstellung der Planungsprozesse, die abhängig von der aktuellen Netzsituation verwendet werden. Der Langzeit-Planungsprozess verwendet eine ganzzahlige lineare Optimierung und ist für die Vorabberechnung der optimalen Ersatzkonfigurationen zuständig. Daneben wurde zusätzlich ein Kurzzeit-Planungsprozess entwickelt, der im Fehlerfall verwendet wird, falls keine geeignete Ersatzkonfiguration existiert. Für den Kurzzeitplanungsprozess wurde ein *Genetischer Algorithmus* (GA) entwickelt. Zusätzlich wurde ein Kostenmodell vorgestellt, welches

ein ständiges Neukonfigurieren des Netzes verhindert, indem es die Kosten der Neukonfiguration mit den Kosten der aktuellen Konfiguration vergleicht.

Die entwickelten Planungsprozesse wurden anhand von unterschiedlichen Referenznetzen und Fehlerszenarien evaluiert. Die Ergebnisse zeigen, dass die am häufigsten auftretenden Fehler wie 1-Linkfehler und 2-Linkfehler in adäquater Zeit vorausgeplant werden. Allerdings existieren Fehlerfälle, bei denen die Optimierung nicht in adäquater Zeit gelöst werden konnte. Solche Fehler konnten aber mit dem GA in wenigen Sekunden bis Minuten gelöst werden. Im letzten Schritt wurde die Kombination aus Vorausplanung und Online-Planung untersucht. Für Verkehrsveränderungen und Degradationsfehler konnte zu 100 Prozent eine vorab berechnete Ersatzkonfiguration gefunden und verwendet werden. Auch bei 1-Linkfehlern wurde eine Trefferquote von über 90 Prozent erreicht. Bei den übrigen vorausberechneten Ersatzkonfigurationen ergab sich abhängig von der Fehlerhäufigkeit eine Trefferquote zwischen 40 Prozent und 80 Prozent.

Zum Abschluss wurde die Online-Planung auf *Reconfigurable Optical Add-Drop Multiplexer* (ROADM)s angewandt, um zu evaluieren, ob nachträglich die Verfügbarkeit des Netzes erhöht werden kann, ohne zusätzliche Infrastruktur zu verbauen. In den Untersuchungen stellte sich heraus, dass in Metronetzen alle potentiellen Schutzpfade nachträglich geschaltet werden konnten. Bei Weitverkehrsnetzen ist dies ebenfalls zu geringen Kosten möglich, allerdings konnten nicht alle potentiellen Schutzpfade geschaltet werden. Dagegen sind Ultra-Weitverkehrsnetze für das nachträgliche Hinzufügen von Schutzpfaden nicht geeignet.

Als weiterführende Arbeiten sei in diesem Zusammenhang die Untersuchung von statistischen Methoden erwähnt, die zum Auffinden von Konfigurationsfehlern die beschriebenen Fehlermuster verwenden. Methoden wie Data Mining und bayessche Algorithmen bieten hierfür einen interessanten Ansatzpunkt. Die Weiterentwicklung des vorgestellten proaktiven Mechanismus auf nicht optische Komponenten stellt des Weiteren einen aussichtsreichen Ansatz dar, um die Verfügbarkeit des Netzes durch rechtzeitiges Signalisieren von bevorstehenden Ausfällen zu erhöhen.

Ein weiterer Aspekt für zukünftige Betrachtungen, ist die Verwendung der Ergebnisse des GA als Eingangsparameter für die ganzzahlige Optimierung. Die ganzzahlige Optimierung berechnet in kürzerer Zeit eine Lösung, so dass mehr Ersatzkonfigurationen vorausgeplant werden können. Dadurch steigt die Verfügbarkeit des Netzes weiter an.

Zusätzlich sollte in weiterführenden Arbeiten die automatisierte Konfiguration von Netzkomponenten untersucht werden. Diese Konfiguration eines Netzes ermöglicht die komplette Automatisierung des Netzmanagementsystems ohne Eingriff des Netzbetreibers. Als Grundlage könnte das in dieser Arbeit entwickelte Kostenmodell dienen, mithilfe dessen die Gesamtkosten einer Neukonfiguration berechnet werden, um ein ständiges Umkonfigurieren zu verhindern.

Abkürzungen

Abkürzungen

AS *Autonomes System*
ATM *Asynchronous Transfer Mode*
BGP *Border Gateway Protocol*
CD *Chromatische Dispersion*
CDN *Content Delivery Networks*
CLI *Command Line Interface*
DSL *Digital Subscriber Line*
DWDM *Dense Wavelength Division Multiplexing*
EDFA *Erbium dopted Fiber Amplifier*
ELH *Extra Long Haul*
FCAPS *Fehler, Konfiguration, Abrechnung, Leistungsmerkmale und Sicherheit*
FIT *Failures in Time*
FR *Frame Relay*
FTP *File Transfer Protocol*
GA *Genetischer Algorithmus*
GbE *Gigabit-Ethernet*
HDTV *High Definition Television*
IETF *Internet Engineering Task Force*
IGP *Interior Gateway Protocol*
ILP *Ganzzahligen linearen Optimierung*
IP *Internet Protocol*
IPTV *Internet Protocol Television*
IS-IS *Intermediate System to Intermediate System*
ISO *Internationale Organisation für Standardisierung*

ITU *International Telecommunication Union*
LAN *Local Area Network*
LDP *Label Distribution Protocol*
LH *Long Haul*
LO *lokalen Oszillatorlaser*
LoS *Loss of Signal*
LP *Lineare Optimierung*
MIB *Management Information Base*
MPLS *Multi-Protocol Label Switching*
MTBF *Mean Time Between Failure*
MTU *Maximum-Transmission-Unit*
MTTR *Mean Time To Repair*
MZI *Mach-Zehnder-Interferometer*
NMS *Netzmanagementsystemen*
NOC *Netzbetriebszentrum*
OAM *Betrieb, Administration und Wartung*
OPEX *OPerational EXpenditure*
OSPF *Open Shortest Path First*
OSI *Open Systems Interconnection*
P2P *Peer to Peer*
PCE *Path Computation Element*
PMD *Polarisationsmodendispersion*
QPSK *Quadratur Phase Shift Keying*
ROADM *Reconfigurable Optical Add-Drop Multiplexer*
RSVP *Resource reSerVation Protocol*
RWA *Routing and Wavelength Assignment*
SDH *Synchronous Digital Hierarchy*
SDTV *Standard Definition Television*
SHO *Super Hub Office*
SLA *Service Level Agreement*
SNMP *Simple Network Management Protocol*
SONET *Synchronous Optical Network*

TED *Traffic Engineering Database*
TMN *Telekommunikationstechnik Managementnetz*
TX *Transmitter*
ULH *Ultra Long Haul*
VHO *Video Hub Office*
VoD *Video On Demand*
VoIP *Voice-over-IP*
VPN *Virtual Private Networks*
WDM *Wavelength Division Multiplexing*
WSS *Wavelength Selective Switch*
100GET 100 *Gbit/s Carrier Ethernet Transport*

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Veröffentlichungen des Autors

[FGH+08] Hannu Flinck, Claus Gruber, Marco Hoffmann, Andreas Kirstädter, Christian Merkle, Thomas Michaelis, and Dominic Schupke, *Packet transport for the future internet*, it - Information Technology **50** (2008), no. 6, 351–357.

[Mer08a] Christian Merkle, *Part i: Configuration failures of the ip layer*, Forschungsbericht, Lehrstuhl für Kommunikationsnetze, 2008.

[Mer08b] Christian Merkle, *Part ii: Configuration failures of the ethernet and the wdm layer*, Forschungsbericht, Lehrstuhl für Kommunikationsnetze, 2008.

[Mer10] Christian Merkle, *Degradation model for erbium-dopted fiber amplifiers to reduce network downtime*, 16th Eunice, June 2010.

[PMKS07] Eleni Palkopoulou, Christian Merkle, Andreas Kirstädter, and Dominic Schupke, *Service oriented traffic models for future backbone networks*, 8. ITG-Fachtagung Photonische Netze, May 2007.

[PMS+11] Eleni Palkopoulou, Christian Merkle, Dominic Schupke, Claus Gruber, and Andreas Kirstädter, *Traffic models for future backbone networks - a service-oriented approach*, European Transaction on Telecommunications **22** (2011), 137–150.

[uCM06] Stephan Eichler und Christian Merkle, *Data aggregation system for distributing inter-vehicle warning messages*, 31st IEEE Conference on Local Computer Networks, November 2006.

Allgemeine Veröffenlichungen

[ABB+06] Nazime Agoulmine, Sasitharan Balasubramaniam, Dimitri Botvich, John Strassner, Elyes Lehtihet, and William Donnelly, *Challenges for autonomic network management*, First Conference on Modelling Autonomic Communication Environment, 2006.

[ABMR06] David Allan, Nigel Bragg, Alan McGuire, and Andy Reid, *Ethernet as carrier transport infrastructure*, IEEE Communications Magazine **44** (2006), 95 – 101.

[AGR06] Siddhartha Annapureddy, Christos Gkantsidis, and Pablo Rodriguez,

Providing video on demand using peer to peer networks, IPTV Workshop, International World Wide Web Conference, May 2006.

[AIK+03] Achim Autenrieth, Andreas Iselt, Andreas Kirstädter, Bernhard Edmaier, Robert Prinz, and Dominic Schupke, *Cost structures of transport networks*, ITG Networkshop 2003, 2003.

[AKA09] Mouhammd Al-Kasassbeh and Mo Adda, *Network fault detection with wiener filter-based agent*, Network and computer Applications **32** (2009), 824–833.

[Ati05] Atis, *Annual report 2005*, Forschungsbericht, Network Reliability Steering Committee (NRSC), 2005.

[Aut03] Achim Autenrieth, *Differentiated resilience in ip-based multilayer transport networks*, Ph.D. thesis, Technische Universität München, 2003.

[Bar57] Nils A. Barricelli, *Symbiogenetic evolution processes realized by artificial methods*, Methodos **9** (1957), 143–182.

[BDL+01] Ayan Banerjee, John Drake, Jonathan P. Lang, Brad Turner, Kireeti Kompella, and Yakov Rekhter, *Generalized multiprotocol label switching: An overview of routing and management enhancements*, IEEE Communications Magazine **39** (2001), 144 – 150.

[BEGE06] E. Bert Basch, Roman Egorov, Steven Gringeri, and Stuart Elby, *Architectural tradeoffs for reconfigurable dense wavelength-division multiplexing systems*, IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS **12** (2006), 615– 626.

[BGH+03] Andreas Betker, Christoph Gerlach, Ralf Hülsermann, Monika Jäger, Marc Barry, Stefan Bodamer, Jan Späth, Christoph Gauger, and Martin Köhn, *Reference transport network scenarios*, MultiTeraNet Report, July 2003.

[Bha97] Ramesh Bhandari, *Optimal physical diversity algorithms and survivable networks*, Symposium on Computer and Communications, 1997.

[Bre62] Hans-Joachim Bremermann, *Optimization through evolution and recombination*, Self-Organizing Systems, 1962.

[BTS09] Ravi S. Barpanda, Ashok K. Turuk, and Bibhudatta Sahoo, *A new cost function to solve rwa problem in wavelength routed optical network using genetic algorithms*, Nature & Biologically Inspired Computing, 2009.

[CCY+06] Meeyoung Cha, Gagan Choudhury, Jennifer Yates, Aman Shaikh, and Sue Moon, *Case study: Resilient backbone design for iptv services*, Workshop on IPTV Services over World Wide Web, Mai 2006.

[CdPB+05] Roberto Clemente, Andrea del Pistoia, Maurizio Bartoli, Giancarlo D'Orazio, and Bruno Pennestri, *Short term strategies for carrier class ip over optics network*, Design of Reliable Communication Networks (DRCN), 2005.

[CFV08] Pedro Casas, Lionel Fillatre, and Sandrine Vaton, *Multi hour robust*

routing and fast load change detection, IEEE International Conference on Communications, May 2008.

[CGG+04] Don Caldwell, Anna Gilbert, Joel Gottlieb, Albert Greenberg, Gisli Hjalmtysson, and Jennifer Rexford, *The cutting edge of ip router configuration*, ACM Special Interest Group on Data Communication (SIGCOMM) Computer Communication Review **34** (2004), 21–26.

[Cha06] Rayane Chahine, *Business case for ason*, Master's thesis, Technische Universität München, 2006.

[Che98] Sheng-Tzong Cheng, *Topological optimization of a reliable communication network*, IEEE Transactions on Reliability **47** (1998), no. 3, 225–233.

[CHK+10] Tarik Cicic, Audun Fosselie Hansen, Amund Kvalbein, Matthias Hartmann, Ruediger Martin, Michael Menth, Stein Gjessing, and Olav Lysne, *Relaxed multiple routing configurations: Ip fast reroute for single and correlated failures*, Transactions on Network and Service Managment **6** (2010), 1–14.

[Cis] Cisco, *Cisco configuration guidelines*.

[CKIP05] Rayane Chahine, Aandreas Kirstädter, Andreas Iselt, and Sandrine Pasqualini, *Operational cost reduction using ason/astn*, Optical Fiber Communication Conference and Exposition (OFC), 2005.

[CS03] Angela L. Chiu and John Strand, *An agile optical layer restoration method for router failures*, IEEE Network **17** (2003), 38–42.

[CVFC09] Pedro Casas, Sandrine Vaton, Lionel Fillatre, and Thierry Chonavel, *Efficient methods for traffic matrix modeling and on-line estimation in large-scale ip networks*, 21st conference on International Teletraffic Congress, September 2009.

[Dan63] George B. Dantzig, *Linear programming and extensions*, Princeton, 1963.

[DAS97] Berna Dengiz, Fulya Altiparmak, and Alice E. Smith, *Search genetic algorithm for optimal design of reliable networks*, IEEE Transactions on Evolutionary Computation **1** (1997), no. 3, 179–188.

[DC09] Robert Doverspike and Bruce Cortez, *Restoration in carrier networks*, DRCN, 2009.

[DDF+06] Simon Dobson, Spyros Denazis, Antonio Fernandez, Dominique Gaiti, Erol Gelenbe, Fabio Massacci, Paddy Nixon, Fabrice Saffre, Nikita Schmidt, and Franco Zambonelli, *A survey of autonomic communications*, ACM Transactions on Autonomous and Adaptive Systems **1** (2006), 223–259.

[DG06] Elias A. Doumith and Maurice Gagnaire, *Traffic grooming in multi-layer wdm networks: Meta-heuristics versus sequential algorithms*, Proceedings of the European Summer School, 2006.

[Dij59] Edsger W. Dijkstra, *A note on two problems in connexion with graphs*, Numerische Mathematik **1** (1959), 269–271.

[DJPS08] Tanmay De, Puneet Jain, Ajit Pal, and Indranil Sengupta, *A genetic algorithm based approach for traffic grooming, routing and wavelength assignment in optical wdm mesh networks*, Networks, 2008.

[DKL06] Rainer H. Derksen, Aandreas Kirstädter, and Gottfried Lehmann, *100 gbit/s ethernet for true end-to-end carrier-grade ethernet networks*, European Conference on Networks and Optical Communications, July 2006.

[DPGM+02] Nick G. Duffield, Albert Greenberg Pawan Goyal, Partho Mishra, K. K. Ramakrishnan, and Jacobus E. van der Merwe, *Resource management with hoses: Point-to-cloud services for virtual private networks*, IEEE/ACM Transaction on Networking **10** (2002), 679–692.

[DW00] Anurag Dwivedi and Richard E. Wagner, *Traffic model for usa long-distance optical network*, Optical Fiber Communication Conference, March 2000.

[EAK05] Khalid El-Arini and Kevin Killourhy, *Bayesian detection of router configuration anomalies*, Joint International Conference on Measurement and Modeling of Computer Systems, 2005.

[EGDH08] Moez Esseghir, Samir Ghamri-Doudane, and Kamel Haddadou, *First steps towards an autonomic management system*, Network Operations and Management Symposium, 2008.

[EH91] Aarts Eiben and Kees Van Hee, *Global convergence of genetic algorithms: A markov chain analysis*, Parallel Problem Solving from Nature, 1991.

[EIAK03] Dr. Bernhard Edmaier, Dr. Andreas Iselt, Dr. Achim Autenrieth, and Dr. Andreas Kirstädter, *Gmpls: Wegbereiter zu dynamischen optischen transportnetzen*, ONLINE 2003, 2003.

[EIP06] David Erman, Dragos Ilie, and Adrian Popescu, *Bittorrent traffic characteristics*, International Multi-Conference on Computing in the Global Information Technology - (ICCGI'06), 2006.

[Ela05] Anush Elangovan, *Efficient multicasting and broadcasting in layer 2 provider backbone networks*, IEEE Communication Magazine **43** (2005), 166–170.

[EWAD88] A.F Elrefaie, R.E. Wagner, D.A. Atlas, and D.G. Daut, *Chromatic dispersion limitations in coherent lightwave transmission systems*, Journal of Lightwave Technology **6** (1988), no. 5, 704 – 709.

[FA08] Don Fedyk and David Allan, *Ethernet data plane evolution for provider networks*, IEEE Communications Magazine **46** (2008), 84–89.

[FB05] Nick Feamster and Hari Balakrishnan, *Detecting bgp configuration faults with static analysis*, Symposium on Networked Systems Design & Implementation, 2005.

[FML+03] Chuck Fraleigh, Sue Moon, Bryan Lyles, Chase Cotton, Mujahid Khan, Deb Moll, Rob Rockell, Ted Seely, and Christophe Diot, *Packet-level traffic measurements from the sprint ip backbone*, IEEE Network **17** (2003), 6–16.

[FR01] Anja Feldmann and Jennifer Rexford, *Ip network configuration for intradomain traffic engineering*, IEEE Network Magazine **15** (2001), 46–57.

[Fra57] Alex S. Fraser, *Simulation of genetic systems by automatic digital computers*, Australian Journal of Biological Sciences **10** (1957), 484–491.

[FT00] Bernard Fortz and Mikkel Thorup, *Internet traffic engineering by optimizing ospf weights*, INFOCOM, 2000.

[FZT08] Luyuan Fang, R. Zhang, and M Taylor, *The evolution of carrier ethernet services-requirements and deployment case studies*, IEEE Communication Magazine **46** (2008), 69–76.

[Gal06] Denis Gallant, *Optical network foundation for triple play services roll-out*, National Fiber Optic Engineers Conference, March 2006.

[Gar06] Fernando Fajardo Garcia, *Techno-economic aspects of carrier-grade ethernet for backbone networks*, Master's thesis, Escola Politècnica Superior de Castelldefels, 2006.

[GBD03] Yashar Ganjali, Supratik Bhattacharyya, and Christophe Diot, *Limiting the impact of failures on network performance*, RR04-ATL-020666, Sprint ATL Research, 2003.

[GBS+10] Steven Gringeri, Bert Basch, Vishnu Shukla, Roman Egorov, and Tiejun J. Xia, *Flexible architectures for optical transport nodes and networks*, IEEE Communication Magazine **48** (2010), no. 7, 40–50.

[GD91] David E. Goldberg and Kalyanmoy Deb, *A comparative analysis of selection schemes used in genetic algorithms*, Foundations of Genetic Algorithms, 1991.

[GD11] Alexandre Gerber and Robert Doverspike, *Traffic types and growth in backbone networks*, Optical Fiber Communication Conference and Exposition, 2011.

[GH96] Robert D. Gardner and David A. Harle, *Methods and systems for alarm correlation*, Global Telecommunications Conference, 1996.

[GLFP+06] Andrea Di Giglio, Jesus F. Lobo, Juan Fernandez-Palacios, Angel Ferreiro, Francois Dorgeuille, Bela Berde, Joachim Fritz Westphal, Ralf Herber, Sergio Bellotti, Gert Eilemberger, Stefan Bunse, Matthieu Clouqueur, Sandrine Pasqualini, Luca Valcarenghi, Nicola Andriolli, Alessio Giorgetti, Didier Colle, Wouter Tavernier, Hisao Nakajima, Marco Quagliotti, Marcello Potenza, Peter Tomsu, Gunnar Edwall, Hans Mickelsson, Anders Berntson, Loa Anderson, Jonas Martensson, Martine Herpers, and Javier Jimenez, *Nobel phase 2 - document deliverable d 1.1 - architectural vision of network evolution*, D11, IST IP NOBEL Phase 2, 2006.

[GLW+06] M. Gunkel, R. Leppla, M. Wade, A. Lord, D. Schupke, G. Lehmann, C. Fürst, S. Bodamer, B. Bollenz, H. Haunstein, H. Nakajima, and J. Martensson, *A cost model for the wdm layer*, International Conference on Photonics in Switching (PS), October 2006.

[Gol89] David E. Goldberg, *Genetic algorithms in search, optimization, and machine learning*, Addison-Wesley Publishing Company, 1989.

[GPdSV03] Luís Gouveia, Pedro Patrício, Amaro F. de Sousa, and Rui Valadas, *Mpls over wdm network design with packet level qos constraints based on ilp models*, INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, vol. 1, 2003, Seiten 576 – 586.

[Gru07] Claus Günter Gruber, *Design and optimization of resilient multipath networks*, Ph.D. thesis, Technische Universität München, 2007.

[HBB+04] Ralf Hülsermann, Stefan Bodamer, Marc Barry, Andreas Betker, Christoph Gauger, Monika Jäger, Martin Köhn, and Jan Späth, *A set of typical transport network scenarios for network modelling*, 5. ITG-Fachtagung Photonische Netze, May 2004, Seiten 65–72.

[HGMS08] Ralf Huelsermann, Matthias Gunkel, Clara Meusburger, and Dominic A. Schupke, *Cost-modeling and evaluation of capital expenditures in optical multilayer networks*, Journal of Optical Networking **7** (2008), no. 9, 814–833.

[HJ97] Cynthia S. Hood and Chuanyi Ji, *Proactive network fault detection*, INFOCOM, 1997.

[HKP+08] F. Hauske, M. Kuschnerov, K. Piyawanno, M. Alfiad, T. Wuth, E. D. Man, E.-D. Schmidt, B. Spinnler, H. de Waardt, and B. Lankl, *Simultaneous monitoring of cd, dgd and osnr from fir filter coefficients in coherent receivers*, Photonische Netze, 2008.

[HLL+06] Xiaojun Hei, Chao Liang, Jian Liang, Yong Liu, and Keith W. Ross, *Insights into pplive: A measurement study of a largescale p2p iptv system*, IPTV Workshop, International World Wide Web Conference, May 2006.

[HQY+06] Junqiang Hu, Dayou Qian, Haijun Yang, Ting Wang, S. Weinstein, M. Cvijetic, and S. Nakamura, *Triple play services over a converged optical/wireless network*, National Fiber Optic Engineers Conference, March 2006.

[HS99] Qiming He and Mark A. Shayman, *Using reinforcement learning for proactive network fault management*, International Conference on Communication Technologies, 1999.

[HS06] Markus Hidell and Peter Sjödin, *Performance of nack-oriented reliable multicast in distributed routers*, 2006 Workshop on High Performance Switching and Routing Program (HPSR), 2006.

[HVD04] Nicolas Hohn, Darryl Veitch, and Christoph Diot, *Bridging router performance and queuing theory*, ACM Joint international conference on Measurement and modeling of computer systems, 2004.

[ICBD04] Gianluca Iannaccone, Chen-Nee Chuah, Supratik Bhattacharyya, and Christophe Diot, *Feasibility of ip restoration in a tier 1 backbone*, IEEE Network **18** (2004), 13–19.

[IEEa] IEEE Draft Standard for Information technology, *802.1q - virtual lans*,

Institute of Electrical and Electronics Engineers, Inc., .

[IEEb] IEEE Draft Standard for Information technology, *802.1qay - provider backbone bridge traffic engineering*, Institute of Electrical and Electronics Engineers, Inc., .

[IEEc] IEEE Draft Standard for Information technology, *Draft standard for local and metropolitan area networks - virtual bridged local area networks - amendment 4: Provider bridges*, Institute of Electrical and Electronics Engineers, Inc., , ieee p802.1ad/d6.0 ed.

[IEEd] IEEE Draft Standard for Information technology, *Ieee 802.3 ethernet working group*, Institute of Electrical and Electronics Engineers, Inc., .

[IEEe] IEEE Draft Standard for Information technology, *Virtual bridged local area networks - amendment 6: Provider backbone bridges*, Institute of Electrical and Electronics Engineers, Inc., .

[IHU+04] Atsushi Iwata, Yoichi Hidaka, Masaki Umayabashi, Nobuyui Enomoto, and Akira Arutaki, *Global open ethernet (goe) system and its performance evaluation*, IEEE Journal on Selected Areas in Communications **22** (2004), 1432–1442.

[IKC04a] Andreas Iselt, Andreas Kirstaedter, and Rayane Chahine, *The role of ason and gmpls for the bandwidth trading market - bandwidth brokerage under the influence of novel control*, ICETE 2004, 1st International Conference on E-Business and Telecommunication Networks, 2004.

[IKC04b] Andreas Iselt, Andreas Kirstädter, and Rayane Chahine, *Ason for bandwidth trading*, ITG/VDE Photonische Netze, 2004.

[InCM+02] Gianluca Iannaccone, Chen nee Chuah, Richard Mortier, Supratik Bhattacharyya, and Christophe Diot, *Analysis of link failures in an ip backbone*, Proceedings of the 2nd ACM Special Interest Group on Data Communication (SIGCOMM) Workshop on Internet measurement, 2002.

[Int85] International Telecommunication Union, *Tmn: Telecommunications management network model*, International Telecommunication Union, , 1985.

[Iwa06] Atsushi Iwata, *Carrier-grade ethernet technologies for next generation wide area ethernet*, IEICE Transactions on Communication **3** (2006), 651 – 660.

[Jaj05] Andrzej Jajszczyk, *Automatically switched optical networks: Benefits and requirements*, Communications Magazine, IEEE **43** (2005), 10– 15.

[JC09] Vinod Joseph and Brett Chapman, *Deploying qos for cisco ip and next generation networks: The definitive guide*, Morgan Kaufmann Publishers, 2009.

[JCS+03] Yang Ji, Yunchul Chung, D. Sprinzak, M. Heiblum, D. Mahalu, and Hadas Shtrikman, *An electronic mach-zehnder interferometer*, Letters to Nature **422** (2003), 415–418.

[JP98] Norleyza Jailani and Ahmed Patel, *Fms: A computer network fault management system based on the osi standards*, Malaysian journal of computer

Science **11** (1998), no. 1, 22–31.

[Jun] Juniper, *Juniper networks configuration guidelines*.

[JvdMB+07] Brendan Jennings, Sven van der Meer, Sasitharan Balasubramaniam, Dmitri Botvich, Micheal O. Foghlu, William Donnelly, and John Strassner, *Towards autonomic management of communications networks*, IEEE Communications Magazine **45** (2007), 112–121.

[JZ04] Ulf Jennehug and Tingting Zhang, *Increasing bandwidth utilization in next generation iptv networks*, International Conference on Image Processing **3** (2004), 2075–2078.

[KC03] Jeffrey O. Kephart and David M. Chess, *The vision of autonomic computing*, Computer **36** (2003), no. 1, 41–50.

[KCG07] Amund Kvalbein, Tarik Cicic, and Stein Gjessing, *Post-failure routing performance with multiple routing configurations*, IEEE INFOCOM, 2007.

[KDL97] Jasmine Kemtchou, Monique Duhamel, and Pierre Lecoy, *Gain temperature dependence of erbium-doped silica and fluoridefiber amplifiers in multichannel wavelengthmultiplexed transmissionsystems*, Lightwave Technology **15** (1997), 2083–2090.

[Key05] Barrie P. Keyworth, *Roadm subsystems and technologies*, Optical Fiber Communication Conference, 2005.

[KFY02] Alexander V. Konstantinou, Danilo Florissi, and Yechiam Yemini, *Towards self-configuring networks*, DARPA Active Networks Conference and Exposition, 2002.

[KGL+09] Charles R. Kalmanek, Gihui Ge, Seungjoon Lee, Carsten Lund, D an Pei, Joseph Seidel, Jacobus van der Merwe, and Jennifer Gates, *Darkstar: Using exploratory data mining to raise the bar on network reliability and performance*, DRCN, 2009.

[KGRB06] Aandreas Kirstädter, Claus Gruber, Johannes Riedl, and Thomas Bauschert, *Carrier-grade ethernet for packet core networks*, International Conference Asia Pacific Optical Communications (APOC), September 2006.

[KHC+09] Amund Kvalbein, Audun Fosselie Hansen, Tarik Cicic, Stein Gjessing, and Olav Lysne, *Multiple routing configurations for fast ip network recovery*, Transactions on Networking **17** (2009), 473–486.

[KHKC06] J.Y. Kim, J.H. Hahm, Y.S. Kim, and J.K. Choi, *Ngn architecture for iptv service without effect on conversational services*, International Conference on Advanced Communication Technology (ICACT) **1** (2006), 465 – 469.

[KIA+05] Andreas Kirstaedter, Andreas Iselt, Achim Autenrieth, Dominic A. Schupke, Robert Prinz, and Bernhard Edmaier, *Business models for next generation transport networks*, Photonic Network Communications, 2005.

[Kie10] Moritz Kiese, *Efficient optimization methods for communication network planning and assessment*, Ph.D. thesis, Technische Universität München, 2010.

[KIP+06] Andreas Kirstädter, Andreas Iselt, Sandrine Pasqualini, Rayane Chahin, Monika Jäger, and Fritz-Joachim Westphal, *A quantitative study on the influence of ason/gmpls on opex*, International Journal of Electronics and Communication (AEÜ) **60** (2006), 30–44.

[KJdWD01] Ton Koonen, Geert Morthierand Jean Jennen, Huug de Waardt, and Piet Demeester, *Optical packet routing in ip-over-wdm networks deploying two-level optical labeling*, 27th European Conference on Optical Communications, 2001.

[Kle75] Leonard Kleinrock, *Queuing systems*, John Wiley & Sons, Inc, 1975.

[KlP05] Eligijus Kubilinskas and Micha l Pioro, *An ip/mpls over wdm network design problem*, The 5th International Workshop on Design of Reliable Communication Networks, 2005.

[KR07] Ralf Kornberger and Helmut Reiser, *"die suche nach der nadel im heuhaufen nyx - ein system zur lokalisierung von rechnern in großen netzwerken anhand ip- oder mac-adressen*, 21. DFN Arbeitstagung über Kommunikationsnetze, 2007.

[KW04] Emre Kiciman and Yi-Min Wang, *Discovering correctness constraints for self-management of system configuration*, International Conference on Autonomic Computing, 2004.

[LADL06] Gottfried Lehmann, Achim Autenrieth, Rainer H. Derksen, and Patrick Leisching, *Die neue ethernet generation: 100-gigabit-ethernet mit integrierten elektrisch-optischen hochgeschwindigkeitsschaltkreisen*, Photonik, 2006.

[LAJ98] Craig H. Labovitz, Abha Ahuja, and Farnman Jahanian, *Experimental study of internet stability and wide-area backbone failures*, Forschungsbericht, Technical Report CSETR-382-98, University of Michigan, 1998.

[LBBSS02] Nathaniel Leibowitz, Aviv Bergman, Roy Ben-Shaul, and Aviv Shavit, *Are file swapping networks cacheable? characterizing p2p traffic*, Proc. of the 7th Int. WWW Caching Workshop, August 2002.

[LBC03] Jean-François Labourdette, Eric Bouillet, and Sid Chaudhuri, *Role of optical network and spare router strategy in resilient ip backbone architecture*, Design of Reliable Communication Networks (DRCN), October 2003.

[LDWJ06] Wu Linping, Meng Dan, Gao Wen, and Zhan Jianfeng, *A proactive fault-detection mechanism in large-scale cluster systems*, 0th international conference on Parallel and distributed processing, 2006.

[lGDW00] lvasir Ghani, Sudhir Dixit, and Tidhiang Wang, *On ip-over-wdm integration*, Communications Magazine, IEEE **38** (2000), 72–84.

[LGXR04] Robert Love, Amitava Ghosh, Weimin Xiao, and Rapeepat Ratasuk, *Performance of 3gpp high speed downlink packet access (hsdpa)*, Vehicular Technology Conference, vol. 5, 2004, Seiten 3359–3363.

[LI00] Baoding Liu and K. Iwamura, *Topological optimization model for communication network with multiple reliability goals*, Computer and Mathematics

with Applications **39** (2000), 59–69.

[LIJOJ10] Craig Labovitz, Scott Iekel-Johnson, Jon Oberheide, and Farnam Jahanian, *Internet inter-domain traffic*, ACM SIGCOMM 2010, 2010.

[LLW+06] Franck Le, Sihyung Lee, Tina Wong, Hyong S. Kim, and Darrell Newcomb, *Minerals: using data mining to detect router misconfigurations*, SIGCOMM, 2006.

[LM02] Jun Li and Constantine Manikopoulos, *Network fault detection: Classifier training method for anomaly fault detection in a production network using test network information*, 27th Annual IEEE International Conference on Local Computer Networks, 2002.

[LTWG05] Haiying Liang, Guowen Teng, Hongjun Wang, and Yuan Gao, *Detecting bgp misconfiguration for bgp/mpls vpns*, Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005.

[MBRM96] Biswanath Mukherjee, Dhritiman Banerjee, Ramu S. Ramamurthy, and Amarnath Mukherjee, *Some principles for designing a wide-area wdm optical networks*, IEEE/ACM Transactions on Networking **4** (1996), no. 5, 684–696.

[MC96] Theodore W. Manikas and J. T. (Tom) Cain, *Genetic algorithms vs simulated annealing: A comparison of approaches for solving the circuit partioning problem*, Forschungsbericht, Department of Electrical Engineering, The University of Pittsburgh, 1996.

[Med05] Aref Meddeb, *Why ethernet wan transport?*, IEEE Communications Magazine **43** (2005), 136–141.

[MHR11] Stefan Metzger, Wolfgang Hommel, and Helmut Reiser, *Integriertes management von sicherheitsvorfällen*, 18. DFN-Workshops Sicherheit in vernetzten Systemen, 2011.

[MIB+04] Athina Markopoulou, Gianluca Iannaccone, Supratik Bhattacharyya, Chen-Nee Chuah, and Christophe Diot, *Characterization of failures in an ip backbone*, Annual IEEE Conference on Computer Communications, INFOCOM, vol. 4, March 2004, Seiten 2307–2317.

[Mic96] Zbigniew Michalewicz, *Genetic algorithms + data structures = evolution programs*, Springer Berlin Heidelberg, 1996.

[MK06] Richard Mortier and Emre Kiciman, *Autonomic network management: some pragmatic considerations*, Special Interest Group on Data Communication, 2006, Seiten 89–93.

[MKV10] Konstantinos Manousakis, Panagiotis Kokkinos, and Emmanouel Varvarigos, *Performance evaluation of node architectures with color and direction constraints in wdm networks*, IEEE Globecom, 2010.

[MSSW05] Darli A. A. Mello, Dominic A. Schupke, Matthias Scheffel, and Helio Waldman, *Availability maps for connections in wdm optical networks*, Design

of Reliable Communication Networks, October 2005.

[MTB99] Carmen Mas, Patrick Thiran, and Jean-Yves Le Boudec, *Fault localization at the wdm layer*, Photonic Network Communications, 1999.

[MWA02] Ratul Mahajan, David Wetherall, and Tom Anderson, *Understanding bgp misconfiguration*, SIGCOMM, August 2002.

[Naj05] Marianne Najm, *Influence of bandwidth-on-demand concepts on the high-speed packet market*, Master's thesis, Technische Universität München, 2005.

[Net06] Nokia Siemens Networks, *High quality and resilient iptv multicast architecture - an overview of resip multicast architecture design guidelines*, , Nokia Siemens Networks, 2006.

[NST05] Aantonio Nucci, Ashwin Sridharan, and Nina Taft, *The problem of synthetically generating ip traffic matrices: Initial recommendations*, ACM SIGCOMM Computer Communication **35** (2005), 19–32.

[OGP03] David Oppenheimer, Archana Ganapathi, and David A. Patterson, *Why do internet services fail, and what can be done about it?*, 4th Usenix Symposium on Internet Technologies and Systems, 2003.

[OIS07] Eiji Oki, Ichiro Inoue, and Kohei Shiomoto, *Path computation element (pce)-based traffic engineering in mpls and gmpls networks*, IEEE Sarnoff Symposium, 2007.

[OPK+06] Michael J. O'Mahony, Christina Politi, Dimitrios Klonidis, Reza Nejabati, and Dimitra Simeonidou, *Future optical networks*, Journal of Lightwave Technology **24** (2006), 4684–4696.

[OPTW07] Sebastian Orlowski, Michal Pioro, Artur Tomaszewski, and Roland Wessäly, *Sndlib 1.0 - survivable network design library*, Proceedings of the 3rd International Network Optimization Conference, 2007.

[Per09] Radia Perlman, *Folklore of robust network routing*, DRCN, 2009.

[Per10] Sterling Perrin, *The need for next-generation roadm networks*, Forschungsbericht, Heavy Reading, 2010.

[PKI+05] Sandrine Pasqualini, Andreas Kirstädter, Andreas Iselt, R. Chahine, Sofie Verbrugge, Didier Colle, Mario Pickavet, and Piet Demeester, *Influence of gmpls on network providers operational expenditures: A quantitative study*, IEEE Communications Magazine **43** (2005), 28 – 38.

[PKO+09] G. Prasanna, B. S. Kishore, G. K. Omprasad, K. S. Raju, R. Gowrishankar, K. Venkataramaniah, Ron Johnson, and Pavan Voruganti, *Versatility of a colorless and directionless wss based roadm architecture*, Communication Systems and Networks and Workshops, 2009.

[PMF+02] Konstantina Papagiannaki, Sue Moon, Chuck Fraleigh, Patrick Thiran, Fouad Tobagi, and Christophe Diot, *Analysis of measured single-hop delay from an operational backbone network*, IEEE Infocom, 2002.

[PSB+07] Aiko Pras, Jürgen Schonwalder, Mark Burgess, Olivier Festor, Gregorio M. Perez, Rolf Stadler, and Burkhard Stiller, *Key research challenges in network management*, IEEE Communications Magazine **45** (2007), 104–110.

[Ram06] Rajiv Ramaswami, *Optical networking technologies: What worked and what didn' t*, IEEE Communications Magazine **44** (2006), 132–139.

[Rap05] Lutz Rapp, *Quality surveillance algorithm for erbium-doped fiber amplifiers*, Design of Reliable Communication Networks, 2005.

[Rei01] Helmut Reiser, *Sicherheitsarchitektur für ein managementsystem auf der basis mobiler agenten*, Ph.D. thesis, Fakultät für Mathematik und Informatik der Ludwig-Maximilians-Universität München, 2001.

[Rei07] John P. Reilly, *Getting started with the sid: A sid modeler's guide*, TeleManagement Forum, , 2007.

[Rei08] Helmut Reiser, *Ein framework für föderiertes sicherheitsmanagement*, Habilitation, 2008.

[Ric00] K.W. Richardson, *Umts overview*, Electronics & Communication Engineering Journal, vol. 12, June 2000, Seiten 93–100.

[Rie03] Anton Riedl, *Routing optimization and capacity assignment in multi-service ip networks*, Ph.D. thesis, Technische Universität München, 2003.

[Rou05] Matthew Roughan, *Simplifying the synthesis of internet traffic matrices*, SIGCOMM Computer Communication, 2005.

[RR00] Byrav Ramamurthy and Ashok Ramakrishnan, *Virtual topology reconfiguration of wavelength-routed optical wdm networks*, GLOBECOM, 2000.

[RR07] Satish Raghunath and K. K. Ramakrishnan, *Resource management for virtual private networks*, IEEE Comunications Magazine **45** (2007), 38–44.

[RRG04] Dirk Reichelt, Franz Rothlauf, and Peter Gmilkowsky, *Designing reliable communication networks with a genetic algorithm using a repair heuristic*, EvoCOP 2004 (J. Gottlieb and G.R. Raidl, eds.), LNCS 3004, Springer-Verlag Berlin Heidelberg, 2004, Seiten 177–187.

[RS96] Rajiv Ramaswami and Kumar N. Sivarajan, *Design of logical topologies for wavelength-routed optical networks*, IEEE Journal on Selected Areas in Communications **14** (1996), no. 5, 840–851.

[RS02] Rajiv Ramaswami and Kumar N. Sivarajan, *Optical networks - a practical perspective*, Morgan Kaufmann Publishers, 2002.

[RSPJ08] Jeong-Dong Ryoo, Jongtae Song, Jaewoo Park, and Bheom-Soon Joo, *Oam and its performance monitoring mechanisms for carrier ethernet transport networks*, IEEE Communication Magazine **46** (2008), 97–103.

[SAF01] Dominic A. Schupke, Achim Authenried, and Thomas Fischer, *Survivability of multiple fiber duct failures*, International Workshop on the Design of Reliable Communication Networks, 2001.

[SAL06] John Strassner, Nazim Agoulmine, and Elyes Lehtihet, *Focale: A novel autonomic networking architecture*, Latin American Autonomic Computing Symposium, 2006.

[SBG+05] Jan Späth, Stefan Bodamer, Christoph Glingener, Marconi, and Backnang, *Next-generation transport solutions for ip backbone networks - benefits of an astn-based multi-layer otn network*, Optical Transmission, Switching, and Subsystems II. Edited by Lam, Cedric F.; Gu, Wanyi; Hanik, Norbert; Oguchi, Kimio. Proceedings of the SPIE **5626** (2005), 371–381.

[Sch11] Thilo Schoendienst, *Utilizing the broadcast and select architecture of today's roadms*, Master's thesis, Institute of Communication Networks (LKN), 2011.

[SEK05] Arno Schmid-Egger and Andreas Kirstädter, *Ethernet in core networks: A technical and economical analysis*, Workshop on High Performance Switching and Routing, 2005.

[SGD+02] Stefan Saroiu, Krishna P. Gummadi, Richard J. Dunn, Steven D. Gribble, and Henry M. Levy, *An analysis of internet content delivery systems*, Proceedings of the 5th symposium on Operating systems design and implementation, 2002.

[SI04] Roberto Sabella and Paola Iovanna, *Traffic engineering in next generation multi-layer networks based on the gmpls paradigm*, Second International Working Conference: Performance Modelling And Evalution Of Heterogeneous Networks, 2004.

[SJH03] Dominic A. Schupke, Monika Jäger, and Ralf Hülsermann, *Comparison of resilience mechanisms for dynamic services in intelligent optical networks*, Fourth International Workshop on the Design of Reliable Communication Networks, 2003.

[SPG+06] Matthias Scheffel, Robert Prinz, Claus G. Gruber, Achim Authenried, and Dominic A. Schupke, *Optimal routing and grooming for multilayer networks with transponders and muxponders*, IEEE Global Communications Conference, 2006.

[SS03] Galen H. Sasaki and Ching-Fong Su, *The interface between ip and wdm and its effect on the cost of survivability*, IEEE Communications Magazine **41** (2003), 74–79.

[SSC+03] Sava Stanic, Suresh Subramaniam, Hongsik Choi, Gokhan Sahin, and Hyeong-Ah Choi, *Efficient alarm management in optical networks*, DARPA Information Survivability Conference and Exposition, 2003.

[SSH06] Stefan Schmid, Manolis Sifalakis, and David Hutchison, *Towards autonomic networks*, 3rd Annual Conference on Autonomic Networking, LNCS 4195, Springer Berlin / Heidelberg, 2006, Seiten 1–11.

[Str02] John Strassner, *Den-ng: Achieving business driven network management*, 8th IEEE/FIP Network Operations and Management Symposium, 2002.

[SW04] Subhabrata Sen and Jia Wang, *Analyzing peer-to-peer traffic across large networks*, IEEE/ACM TRANSACTIONS ON NETWORKING **12** (2004), 219 – 232.

[Syw89] G. Sywerda, *Uniform crossover in genetic algorithms*, Proceedings of the third international conference on Genetic algorithms table of contents, Morgan Kaufmann Publishers, 1989, Seiten 2–9.

[TB00] Dale R. Thompson and Griff L. Bilbro, *Comparison of a genetic algorithm with a simulated annealing algorithm for the design of an atm network*, IEEE Communication Letters **4** (2000), no. 8, 267–269.

[TLG08] Ali Tizghadam and Alberto Leon-Garcia, *Aorta: Autonomic network control and management system*, INFOCOM Workshop, 2008.

[TPC+09] Wouter Tavernier, Dimitri Papadimitriou, Didier Colle, Mario Pickavet, and Piet Demeester, *Optimizing the ip router update process with traffic-driven updates*, DRCN, 2009.

[TR06] Renata Teixeira and Jennifer Rexford, *Managing routing disruptions in internet service provider networks*, IEEE Communications Magazine **44** (2006), 160–165.

[TS07] Onur Turkcu and Suresh Subramaniam, *Blocking in reconfigurable optical networks*, IEEE International Conference on Computer Communications, 2007.

[TSB97] Surat Tanterdtid, Worawit Steanputtanagul, and Watit Benjapolakul, *Optimizing atm network configuration based on virtual path concept using genetic algorithm*, Communications, Computers and Signal Processing, 1997.

[TZI+07] Zhenning Tao, Hao Zhang, Akihiko Isomura, Lei Li, Takeshi Hoshida, and Jens C. Rasmussen, *Simple, robust, and wide-range frequency offset monitor for automatic frequency control in digital coherent receivers*, European Conference on Optical Communication, 2007.

[VCP+06] S. Verbrugge, D. Colle, M. Pickavet, P. Demeester, S. Pasqualini, A. Iselt, A. Kirstaedter, R. Huelsermann, F. J. Westphal, and M. Jaeger, *Methodology and input availability parameters for calculating opex and capex costs for realistic network scenarios*, Journal of Optical Networking **5** (2006), no. 6, 509–520.

[VK00] Malathi Veeraraghavan and Mark Karol, *Using wdm technology to carry ip traffic*, 34th Annual Conference on Information Sciences and Systems, March 2000.

[VKK06] Sundar Vedantham, Seong-Hwan Kim, and Deepak Kataria, *Carrier-grade ethernet challenges for iptv deployment*, IEEE Communications Magazine **44** (2006), 24–31.

[VL03] Sascha Vorbeck and Ralph Leppla, *Dispersion and dispersion slope tolerance of 160-gb/s systems, considering the temperature dependence of chromatic di-*

spersion, IEEE PHOTONICS TECHNOLOGY LETTERS **15** (2003), 1470–1472.

[VZ04] Malathi Veeraraghavan and Xuan Zheng, *A reconfigurable ethernet/sonet circuit based metro network architecture*, IEEE Journal on Selected Areas in Communication **22** (2004), 1406–1418.

[Wat91] R. Waters, *Diode laser degradation mechanisms: A review*, Progress in Quantum Electronics **15** (1991), no. 3, 153–174.

[WE06] P.J. Winzer and R.-J. Essiambre, *Advanced optical modulation formats*, Proceedings of the IEEE **95** (2006), 952–985.

[Woo04] A. Wool, *A quantitative study of firewall configuration errors*, IEEE Computer **37** (2004), no. 6, 62–67.

[WTKD04] William E. Walsh, Gerald Tesauro, Jeffrey O. Kephart, and Rajarshi Das, *Utility functions in autonomic systems*, First International Conference on Autonomic Computing, 2004.

[Yem93] Y. Yemini, *The osi network management model*, Communications Magazine, IEEE **31** (1993), no. 5, 20–29.

[YLC05] Ming Yu, Wenjui Li, and Lijin Chong, *A new hybrid alarm correlation scheme for mpls-enabled backbone networks*, IEEE Conference on Networks, 2005.

[ZFB04] Lothar Zier, Wolfgang Fischer, and Frank Brockners, *Ethernet-based public communication services: Challenge and opportunity*, IEEE Communications Magazine **42** (2004), 88 – 95.

[ZJM00] H. Zang, J. P. Jue, and B. Mukherjee, *A review of routing and wavelength assignment approaches for wavelength-routed optical wdm networks*, Optical Networks Magazine **1** (2000), no. 1, 47–60.

[ZM02] K. Zhu and B. Mukherjee, *Traffic grooming in an optical wdm mesh network*, IEEE Journal on Selected Areas in Communications **20** (2002), no. 1, 122–133.

Webseiten

[Aka11] Akamai, *Akamai*, www.akamai.com, 2011.

[Bac09] Daniel Bachfeld, *Heise news - fehlkonfigurierter router beeinträchtigt teile des internet*, February 2009.

[Cis08] Cisco, *White paper - the exabyte era*, January 2008.

[Exc] Frankfurt Internet Exchange, *Frankfurt internet exchange*.

[Fora] Distributed Management Task Force, *Common information model*.

[FV06] A. Farrel and J.-P. Vasseur, *A path computation element (pce)-based architecture*, Network Working Group, 2006.

[Gmb06] Ipoque GmbH, *Press release*, October 2006.

[Gmb09] Detecon GmbH, *Press release*, Februar 2009.

[Gru] Claus Gruber, *C++ bibliothek GRAPH*.

[Hei09] Heise, *Heise news - kombination aus bedienfehler und cisco-bug legte beinahe das internet lahm*, February 2009.

[Hei10] Heise, *Heise news - chinesischer provider ëntführt"kurzzeitig teile des internets*, April 2010.

[Hut05] J. Huter, *Statistisches monatsheft baden-würtemberg*, April 2005.

[ILO] ILOG Inc., *CPLEX*.

[LIJM+09] S. Craig Labovitz, D. Iekel-Johnson, J. McPherson, Oberheide, and F. Jahanian, *Internet traffic and content*, October 2009.

[Pay11] Payscale, *Payscale: Salary survey for job: Computer/network support technician*, 2011.

[SM09] Hendrik Schulze and Klaus Mochalski, *Internet study 2008/2009*, 2009.

[SND11] SNDlib, *Sndlib: Germany 50 node reference network*, 2011.

[Wil09] Andreas Wilkens, *Heise news - stau auf googles datenautobahn*, May 2009.