Wallace Rodrigues de Santana

Estudo sobre Modelagem e Avaliação de Confiabilidade em Redes Óticas

Santo André, SP – Brasil
Junho de 2010

Universidade Federal do ABC – UFABC
Mestrado em Engenharia da Informação

Estudo sobre Modelagem e Avaliação de Confiabilidade em Redes Óticas

Autor: Wallace Rodrigues de Santana
Orientador: Prof. Dr. Guiou Kobayashi

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia da Informação da Universidade Federal do ABC como requisito parcial para obtenção do título de Mestre em Engenharia da Informação, Área de Concentração Redes de Informação, Linha de Pesquisa Redes de Comunicação.

Santo André, SP – Brasil
Junho de 2010

Ficha catalográfica elaborada pela Biblioteca da Universidade Federal do ABC

SANTANA, Wallace Rodrigues de
Estudo sobre modelagem e avaliação de confiabilidade em redes óticas / Wallace Rodrigues de Santana — Santo André : Universidade Federal do ABC, 2010.

109 fls. il.

Orientador: Guiou Kobayashi

Dissertação (Mestrado) — Universidade Federal do ABC, Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, Engenharia da Informação, 2010.

1. Redes ópticas 2. Diagramas de Decisão Binária 3. KyaTera I. KOBAYASHI, Guiou. II. Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, Engenharia da Informação, 2010, III. Título.

CDD 004.6

Dissertação de Mestrado apresentada no Curso de Mestrado em Engenharia da Informação da Universidade Federal do ABC, como requisito parcial para obtenção do título de Mestre em Engenharia da Informação.

Avaliada em 10 de junho de 2010 pela seguinte Banca Examinadora:

_____

Prof. Dr. Guiou Kobayashi
Orientador

_____

Prof. Dr. José Artur Quilici Gonzalez
Universidade Federal do ABC

_____

Prof. Dr. Wagner Luiz Zucchi
Universidade de São Paulo

Em memória de Geni Aranha Araújo.

Agradecimentos

Agradeço primeiramente a Deus, pela sabedoria que tem me dado e pelas bênçãos que tem derramado sobre mim.

Agradeço em especial meu orientador Prof. Dr. Guiou Kobayashi, pela paciência e confiança depositada em mim.

Agradeço aos meus ex-superiores Roberto Eduardo Leon e Paulo Fernando Loesch, por terem permitido que eu conciliasse os estudos com o meu trabalho na CEAGESP.

Agradeço os professores Salvador Giaquinto (IPT), Humber Furlan (FATEC-SP), Ricardo Andrian Capozzi (FATEC-Mauá), Maria Fátima Baptista Marques (Camicado), Jarbas Thaunahy Santos de Almeida (FATEC-Mauá) e Osmil Aparecido Morselli (FATEC-Mauá), por terem me recomendado ao programa de Mestrado da Universidade Federal do ABC.

Agradeço os colegas de classe Alaelson de Castro Jatobá Neto, Fátima Dias Machado, Kelly Cristina da Cruz Silva, Patrícia Dias dos Santos, Robson dos Santos França, Rodrigo Campos Bortoletto, Samuel Perfidio D'Attilio e Telmo Claudinei Machado, e aos amigos Oliver Guerino e Thiago Angelini, pelos momentos que passamos juntos estudando.

Agradeço a todos os professores da Pós-Graduação em Engenharia da Informação da UFABC, pelos ensinamentos e orientações passados a nós.

Agradeço também minha esposa Carla, pelo carinho e compreensão.

Resumo

Nos dias de hoje, as redes de comunicação têm se mostrado cada vez mais vitais e importantes, pois provêm conexões locais, regionais e internacionais para voz, dados e vídeo. Num mundo globalizado, elas desempenham um papel importante na economia e nas relações humanas, de tal maneira que a sua indisponibilidade, ainda que por pouco tempo, pode causar uma série de transtornos e inconvenientes.

As redes de comunicação são baseadas principalmente em enlaces de fibra ótica, que estão distribuídas geograficamente, enterradas ao longo de rodovias, ferrovias, junto a gasodutos e oleodutos, e por conseqüência, expostas aos mais variados tipos de sinistros que podem acarretar a sua indisponibilidade, como escavações, enchentes, terremotos, falhas humanas, falhas de equipamento, etc.

Assim, este trabalho procura discutir e apresentar uma metodologia para modelar e avaliar a confiabilidade das redes óticas, de modo a construir um modelo de confiabilidade que possa ser usado por provedores de serviços para adequar suas operações aos acordos de níveis de serviço estabelecidos com seus clientes.

Palavras-chave: Redes Óticas, Confiabilidade, Disponibilidade, Tolerância a Falhas, MTTF, MTBF, Proteção, Sobrevivência, Diagramas de Decisão Binária, KyaTera.

Abstract

Nowadays, communication networks have proved increasingly vital and important as they come from local connections, regional and international voice, data and video. In a globalized world, they play an important role in the economy and human relationships, so that its unavailability, even for a short time, can cause a lot of trouble and inconvenience.

Communication networks are mainly based on optical fiber links, which are distributed geographically, buried along highways, railways, along with gas and oil pipelines, and consequently exposed to all kinds of accidents which may lead to its unavailability, as excavations, floods, earthquakes, human error, equipment failures, etc.

Thus, this paper discusses and presents a methodology to model and evaluate the reliability of optical networks in order to construct a model of reliability that can be used by service providers to tailor their operations to service level agreements established with their customers.

Keywords: Optical Networks, Reliability, Availability, Fault Tolerance, MTTF, MTBF, Protection, Survivability, Binary Decision Diagrams, KyaTera.

Sumário

Lista de Acrônimos

1R – Re-amplified

2R – Re-shaped

3R – Re-timed

A – Availability

ADD – Algebric Decision Diagram

ARP – Address Resolution Protocol

ATM – Asynchronous Transfer Mode

BDD – Binary Decision Diagram

CAE – Composition after Expansion

CCE – Centro de Computação Eletrônica

CEAGESP – Companhia de Entrepostos e Armazéns Gerais de São Paulo

CUDD – Colorado University Decision Diagram

CWDM – Coarse Wavelength Division Multiplexing

DAG – Directed Acyclic Graph

DWDM – Dense Wavelength Division Multiplexing

EDFA – Erbium-doped Fiber Amplifier

EE – Entangled Expansion

FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo

FATEC-Mauá – Faculdade de Tecnologia de Mauá

FATEC-SP – Faculdade de Tecnologia de São Paulo

FIT – Failures in Time

FMEA – Failure Mode and Effects Analysis

FMECA – Failure Mode, Effects and Criticality Analysis

Gbps – Gigabit per second

HALT – Highly Accelerated Life Testing

HRD5 – Handbook for Reliability Data for Electronic Components

INCOR – Instituto do Coração

IP – Internet Protocol

IPT – Instituto de Pesquisas Tecnológicas

ITE – IF-Then-Else

ITU – International Telecommunication Union

LTE – Line Terminating Equipment

MAC – Media Access Control

MIL-HDBK 217 – Military Handbook 217

MTBF – Mean Time between Failures

MTTF – Mean Time to Failure

MTTR – Mean Time To Repair

NARA – Núcleo de Apoio à Rede Acadêmica

NGN – Next-Generation Networks

NP – Non Polynomial

OA – Optical Amplifier

OADM – Optical Add and Drop Multiplexer

OBDD – Ordered Binary Decision Diagram

OLA – Optical Line Amplifiers

OLT – Optical Line Terminal

OSC – Optical Supervisory Channel

OTM – Optical Terminal Multiplexer/Demultiplexer

OTMX – Optical Terminal Multiplexer/Demultiplexer

OXC – Optical Cross Connect

PTE – Path Terminating Equipment

PUC – Pontifícia Universidade Católica

QoS – Quality of Service

R – Reliability

RARP – Reverse Address Resolution Protocol

RBD – Reliability Block Diagram

RG – Dispersion Compensation components and Regenerators

ROADM – Reconfigurable Optical Add and Drop Multiplexer

ROBDD – Reduced Ordered Binary Decision Diagram

RWA – Routing and Wavelength Assignment

Rx – Receiver

SAN – Storage Area Network

SDH – Synchronous Digital Hierarchy

SLA – Service Level Agreement

SLU – Sub-loop Unbundling

SM – Single Mode Fiber

SONET – Synchronous Optical Networking

SONET ADM – Synchronous Optical Networking Add and Drop Multiplexer

STE – Section Terminating Equipment

Tbps – Terabit per second

TCP – Transmission Control Protocol

TCP/IP – Internet Protocol Suite

TPD – Telefônica Pesquisa e Desenvolvimento

Tx – Transmitter

U – Unavailability

UFABC – Universidade Federal do ABC

UNI – User to Network Interface

UNICAMP – Universidade Estadual de Campinas

UNIFESP – Universidade Federal de São Paulo

USP – Universidade de São Paulo

VoIP – Voice over IP

WDM – Wavelength Division Multiplexing

ZDD – Zero-suppressed Binary Decision Diagram

Lista de Tabelas

Lista de Figuras

1. Introdução

Nos dias de hoje, as redes de comunicação têm se mostrado cada vez mais vitais e importantes, tanto em termos humanos como financeiros. Elas são a infraestrutura "invisível" que provê conexões locais, regionais e internacionais para voz, dados e vídeo. Num mundo cada vez mais globalizado, as redes de comunicação desempenham um papel muito importante, pois por ela trafegam notícias, pedidos de compra e venda, transações bancárias, reservas de voos, etc. As rede de comunicação são tão importantes que a sua indisponibilidade, ainda que por pouco tempo, pode causar sérios transtornos, prejuízos e muitos inconvenientes [1] [2].

Uma rede de comunicação é formada a partir da interligação de elementos menores capazes de transmitir e receber dados. O menor elemento de uma rede é conhecido como nó. Se este nó for um computador, podemos chamá-lo também de *host*.

Para interligar os nós, é necessário o uso de enlaces de comunicação (*links*) por onde trafegam os dados de um nó a outro. Estes enlaces podem ser elétricos, óticos, de ondas eletromagnéticas, entre outros.

Uma rede ideal seria aquela que se recupera de erros dinamicamente, de modo que o usuário final não perceba sua indisponibilidade, ou que esta seja de tal forma muito pequena para não ser percebida.

Desta forma, a rede deveria detectar onde a falha ocorre, sinalizar as demais partes da rede e iniciar os procedimentos de correção [1]. No entanto, a maior dificuldade é como transportar a sinalização da falha em uma rede que tem seu tráfego interrompido por uma. Este problema pode ser contornado de várias formas, seja instalando rotas alternativas de tráfego, com o uso de *links* sobressalentes dedicados ou compartilhados, seja combinando diferentes mídias, como fibra ótica e microondas, entre outros.

Independente do sistema de proteção empregado, sempre haverá uma contrapartida inerente ao tipo de proteção. Uma rede com uma grande diversidade de caminhos pode resultar numa rede complexa e de resposta lenta, ao passo que uma rede mais simples pode ser mais suscetível a falhas.

Os sistemas de proteção compartilhados têm a vantagem do menor custo de instalação, mas no momento da falha o tráfego tem que ser balanceado de modo a acomodar as necessidades de largura de banda de todos os usuários. Até mesmo o tráfego de alta prioridade em redes que possuem esquemas de priorização de tráfego QoS (*Quality of Service*) pode ser prejudicado.

Um dos principais inconvenientes da maioria dos sistemas de proteção é que eles dependem de canais de sinalização para que as rotas sejam reconfiguradas, mas o canal de sinalização também pode falhar. Uma alternativa é que o nó monitore o tempo de resposta para detectar se o *link* está em falha. No entanto, isso pode resultar em tempos de resposta mais lentos [1].

Anéis óticos SONET e SDH funcionam de forma relativamente rápida. A topologia em anel faz com que a seleção da rota seja mais rápida do que na topologia em malha. O tempo gasto por anéis SONET para detectar falhas e realizar a mudança de linha é normalizada em menos de 60 ms (10 ms para detectar e falha e 50 ms para rotear um novo caminho). Apesar de ser uma arquitetura que oferece um alto nível de proteção e um tempo baixo para recuperação, é pouco flexível para se ajustar a topologias dispersas geograficamente [1].

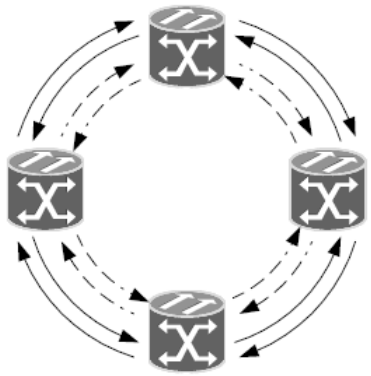


Figura 1 – Rede em anel duplo bidirecional [3]

Já as redes com topologia em malha são mais adequadas a topologias dispersas geograficamente, já que não precisam, necessariamente, ter todos os nós interconectados. Por outro lado, a complexidade e a redundância aumentam na mesma medida em que aumenta o número de ligações ou conexões possíveis. Apesar disso incrementar a diversidade de rotas disponíveis, isso também dificulta a tarefa de escolher rapidamente a rota mais adequada no caso de falha. Os algoritmos para calcular novas rotas dinamicamente podem ser complexos e dispendiosos, e sua execução pode ser inviável mesmo se executados em supercomputadores. A rede da Figura 2 não é

uma rede real, mas demonstra como a complexidade aumenta à medida que novos nós são introduzidos na rede.

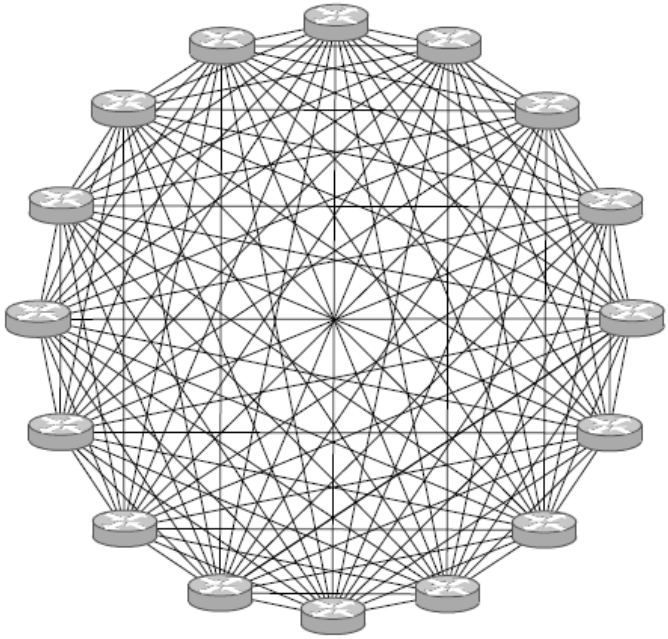


Figura 2 – Rede em malha totalmente conectada [3]

Deve-se levar em conta também que os métodos de proteção podem se dar desde o nível físico da rede até o nível lógico, o que impede que seja adotada uma abordagem única. Ainda que se implemente a proteção de rotas no nível lógico, não podemos esquecer que o rompimento de um cabo que carrega várias fibras irá indisponibilizar todos os usuários que trafegam por aquele enlace, de modo que a avaliação da proteção no nível físico deve ser priorizada.

São vários os tipos de falhas que podem ocorrer, seja devido a falhas humanas, falhas de equipamento, desastres naturais, entre outros.

As falhas humanas podem ser acidentais ou propositais. As falhas acidentais podem ser causadas por imprudência, omissão ou negligência. As falhas propositais podem ser motivadas por atos de vandalismo, espionagem e sabotagem.

Quanto às falhas de equipamentos, o mais freqüente é o rompimento de dutos e cabos de fibra ótica. Se o cabeamento estiver enterrado, escavações sem supervisão podem ocasionar o rompimento dos cabos. Se o cabeamento estiver suspenso em postes, o rompimento pode ser causado pela queda de árvores, por exemplo.

Emendas mal conectadas também causam a interrupção na transmissão dos dados na fibra. Já as falhas de *hardware* e *software* também são possíveis de ocorrerem, mas são menos comuns.

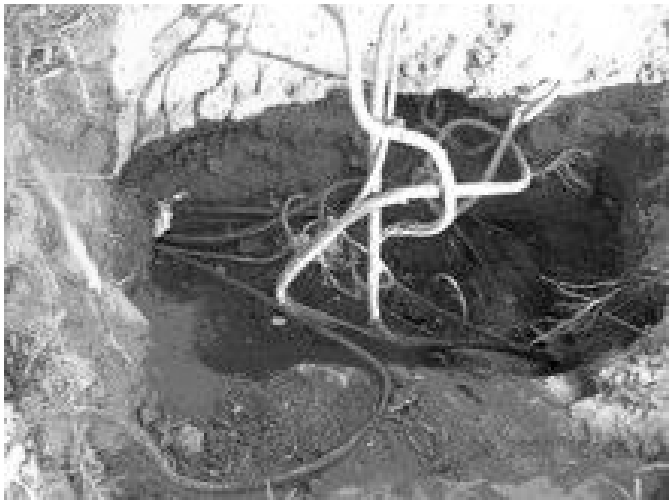


Figura 3 – Rompimento de cabos de fibra ótica causados por escavação [4]

Os cabos de fibra ótica estão mais sujeitos a falhas porque, em sua maioria, estão enterradas ao longo de rodovias, ferrovias, junto a gasodutos e oleodutos, e por conseqüência, expostas aos mais variados tipos de sinistros que podem acarretar a sua indisponibilidade, como escavações, enchentes, terremotos, erosões, etc. [5].

Figura 4 – Erosão em rodovia causada por fortes chuvas [6]

Além dos tipos de sinistros descritos acima, aplicáveis a fibras óticas terrestres, temos ainda os que se aplicam às fibras óticas submersas, que interligam os continentes e carregam uma grande quantidade de tráfego de dados.

A confiabilidade é um parâmetro importante no projeto de fibras óticas submarinas, pois o tempo de vida útil esperado é da ordem de décadas e o seu custo para reparo é excessivamente alto [7]. O projeto de cabos submarinos de fibra ótica deve levar em conta que a operação se dará em águas profundas e em alta pressão, e que os cabos estarão tensionados. A concepção mecânica do cabo submarino deve levar em conta também as forças que são aplicadas ao cabo pelo movimento do navio em resposta à ação das ondas, além de seu próprio peso. A experiência tem demonstrado que um cabo deve ter uma força de ruptura maior do que o peso de 19 km do cabo na água [8].

1.1. Motivação

A confiabilidade de uma rede é um parâmetro fundamental a ser considerado nas aplicações e serviços a serem ofertados nas redes óticas que compõem as redes atuais e as redes da próxima geração (NGN – *Next-Generation Networks*). Entender as características e limites destas redes a partir da perspectiva da confiabilidade da rede permitirá um melhor planejamento e manutenção das redes óticas. Como o atributo de confiabilidade é transparente para o usuário do serviço – que só se dá conta do nível de confiabilidade da rede quando esta fica indisponível – torna-se difícil para o usuário avaliar o quanto deve ser pago para se garantir um nível de entrega de serviço (SLA – *Service Level Agreement*) que atenda suas necessidades. Assim, o usuário não tem como mensurar o custo do serviço relacionado com o nível de proteção requerido.

Por exemplo, uma empresa com serviços baseados na Internet sabe da necessidade de se ter uma rede tolerante a falhas e com baixo tempo de recuperação para manter seus negócios 24 horas por dia, 7 dias por semana. Nestes casos, a interrupção do fornecimento de serviços causada por falhas na comunicação podem significar a queda no volume de negócios e prejudicar a imagem da empresa. Para se proteger disso, a empresa pode contratar enlaces de comunicação de diferentes provedores, e imaginar que isso seja suficiente para garantir a disponibilidade do acesso à Internet. No entanto, como os enlaces de grande distância são caros para instalar e manter, muitos provedores compartilham a mesma infra-estrutura de rede, de modo que o rompimento de um enlace irá indisponibilizar ambos. A

empresa então irá notar que pagar o dobro (ou mais) pelos enlaces não é suficiente para garantir a disponibilidade do serviço.

De maneira geral, o contrato de SLA é um acordo entre o cliente e o prestador de serviços que estabelece parâmetros claros que especificam o tempo máximo em que os serviços podem ficar indisponíveis e o tempo máximo para repará-los. Tempos de indisponibilidade muito baixos requerem sistemas muito confiáveis, o que significa custos elevados de equipamentos e instalações, ou tempos de reparo muito baixos. Prazos curtos de atendimento para reparo requerem disponibilidade de peças de reposição e equipamentos de manutenção, bem como equipes de suporte que estejam sempre à disposição, pois de acordo com as necessidades do cliente, o atendimento pode ser realizado apenas em dias úteis durante o horário comercial ou 24 horas por dia, 7 dias por semana.

Diante disto, vê-se que quanto menor for a indisponibilidade da rede requerida pelo cliente, maior será o custo com o contrato de SLA. Sendo assim, como avaliar o custo da confiabilidade e da disponibilidade requerido por um determinado usuário? Para tal devemos responder algumas questões: O que é confiabilidade e quais os conceitos associados a ela, e como aplicar estes conceitos aos serviços de rede? Como medir a confiabilidade da rede, desde o nível de componentes até o nível de sistema? Como melhorar a confiabilidade, e quanto isso irá custar? Como manter os atributos originais de confiabilidade?

Para responder estas e outras perguntas, este trabalho será focado nos seguintes aspectos:

- Identificar os componentes que compõem os nós e os enlaces de uma rede;
- Obter os dados de MTTF de cada componente;
- Estudar as configurações de recuperação da rede;
- Aplicar modelos de confiabilidade.

Esperamos assim, ao final deste trabalho de pesquisa, levantar qual o nível de confiabilidade e disponibilidade da rede KyaTera.

1.2. Objetivos

Este trabalho tem como objetivo realizar um estudo sobre a confiabilidade e disponibilidade de redes óticas, discutindo os seus efeitos na prestação de serviços de rede. Na sua parte aplicada avaliou-se uma rede real, a rede KyaTera, aplicando-se algumas técnicas de avaliação de confiabilidade.

1.3. Escopo

Estudar os modelos de rede existentes e suas técnicas de proteção que estejam as mais próximas possíveis da camada física da rede ótica. Analisar a teoria de confiabilidade na rede ótica e estudar alternativas para o problema NP completo na avaliação em modelagem da confiabilidade da rede. Por fim, aplicar um modelo na avaliação da confiabilidade da rede ótica KyaTera no nível da camada física, uma vez que uma falha em um duto ou cabo já é suficiente para indisponibilizar uma parte da rede para um grande número de usuários, independente das abordagens de proteção das camadas superiores.

1.4. Trabalhos relacionados

O ponto de partida para se entender e compreender a confiabilidade de uma rede é que a análise da falha de um componente não é suficiente para entender o seu comportamento em nível de sistema. A falha de um roteador ou o rompimento de um cabo de fibra devem ser analisados no contexto da comutação de circuitos ou de pacotes em uma rede ótica, de modo a analisar seus efeitos na confiabilidade e disponibilidade dos serviços da rede.

Durante décadas muitos pesquisadores concentraram esforços para modelar a confiabilidade de uma rede, seja algebricamente e numericamente, usando Teoria dos Grafos, algoritmos e mais recentemente Árvores de Decisão Binária [9], [10], [11], [12] e [13].

Em 1986 [14] mostrou que o cálculo da confiabilidade da rede era um problema exponencial do tipo NP completo (Tempo Polinomial não Determinístico), o que dificulta sua análise para redes com muitos nós e vértices. Desde então muitos algoritmos e soluções foram propostas.

A complexidade da rede aumenta na mesma medida em que aumenta o número de ligações ou conexões possíveis entre os nós. Como isso incrementa a diversidade de rotas disponíveis, também dificulta a análise da rota mais adequada para comutar o tráfego de dados.

Em 2002 [12] apresentou uma aproximação para determinar a confiabilidade de *k* terminais em uma rede não orientada. O cálculo da confiabilidade k-terminal é o problema mais genérico encontrado na literatura. Dado um conjunto de nós alvo $k \in V$ com $k = |K|$, onde *V* é o número total de vértices (ou nós) da rede e |*K*| representa um subconjunto de vértices, a confiabilidade k-terminal é a probabilidade de que para um dado nó $s \in |K|$ deverá existir pelo menos um caminho de *s* para todos os outros nós em *k*. A confiabilidade será então a soma das probabilidades de sucesso dos caminhos disjuntos [12]. O problema, no entanto, está no fato de que a complexidade de identificar todos os caminhos disjuntos de sucesso é exponencial (problema NP-completo). Para contornar este problema, foi usada uma técnica que consiste em derivar funções de pares de terminais baseado no diagrama de expansão de *links* (*edge expansion diagram*) usando diagrama de decisão binária ordenada (OBDD). No entanto, esta técnica levava em consideração que a rede deveria ser modelada como um grafo não direcionado e que os nós eram livres de falhas.

Para efeitos de cálculo da confiabilidade, consideram-se três tipos de situação [9] [10]:

1. Quando se deseja calcular a probabilidade de que k terminais (ou nós) de uma rede estejam conectados;
2. Quando se deseja calcular a probabilidade de que todos os terminais (ou nós) de uma rede estejam conectados;
3. Quando se deseja calcular a probabilidade de que um par de terminais (ou nós) de uma rede esteja conectado.

O cálculo da confiabilidade da rede pode ser dividido em duas classes: a do cálculo aproximado e a do cálculo exato. No cálculo exato há duas categorias: a primeira usa algoritmos que enumeram a quantidade mínima de caminhos, e a segunda usa algoritmos que reduzem o gráfico que representa a rede removendo alguns de seus componentes [11].

Há ainda, na literatura, discussões sobre como aumentar a confiabilidade sem necessariamente calculá-la [15], [16] e [17].

1.5. Contribuições

Descrever uma metodologia capaz de orientar a determinação dos níveis de confiabilidade de uma rede ótica qualquer. A partir de um caso concreto de medição e avaliação de confiabilidade baseado em uma rede real, acreditamos ser possível validar um modelo de confiabilidade que possa ser usado por provedores de serviços para que estes possam oferecer melhores serviços baseados em SLA.

1.6. Organização do texto

No capítulo 2 é apresentado o modelo de rede ótica, seus equipamentos e suas particularidades, bem como a topologia e os equipamentos usados para conectar a rede. No capítulo 3 são discutidos os métodos para avaliação dos níveis de confiabilidade e disponibilidade dos equipamentos e elementos que compõem a rede. No capítulo 4 são apresentados os métodos usados na proteção e restauração dos enlaces de rede ótica, com o objetivo de restabelecer o tráfego de dados em caso de falhas. No capítulo 5 é dada uma visão geral das técnicas de modelagem para avaliação de confiabilidade em redes óticas. No capítulo 6 é descrita a arquitetura da rede KyaTera. No capítulo 7 é demonstrada a avaliação da confiabilidade da rede KyaTera, e no capítulo 8 são apresentadas as conclusões finais e os trabalhos futuros.

2. Modelo de rede

2.1. Rede local

Uma rede é formada por nós e por enlaces que os conectam. Se considerarmos uma rede local, teremos como nós da rede os seguintes elementos: servidores, estações de trabalho e *switches*. Estes nós são conectados por meio de cabos ou ondas de rádio (*wireless*). Cada um destes elementos possui pontos de falha, que podem comprometer toda a rede ou apenas parte dela.

No caso do comprometimento dos cabos, servidores ou estações de trabalho, apenas parte da rede será afetada. Falhas nos cabos afetam equipamentos ligados a eles. Falhas nos servidores afetam o funcionamento de alguns serviços, e falhas nas estações geralmente afetam apenas elas mesmas.

Entretanto, no caso do comprometimento do *switch*, serão afetados todos os equipamentos ligados a ele. Se o *switch* for único na rede, esta será totalmente afetada. Se o *switch* estiver cascateado com outros *switches*, a falha poderá afetar uma parte da rede apenas.

Outro detalhe importante das redes locais é quanto à forma como os nós se comunicam. A troca de informações muitas vezes se dá por meio da difusão de pacotes (*broadcasting*). Essa difusão pode ocorrer tanto no nível físico – quando o *switch* precisa mapear os endereços MAC em cada porta de rede, por exemplo – quanto no nível lógico, quando se usa os protocolos ARP e RARP da camada de rede para resolver endereços físicos e lógicos, se considerarmos uma rede baseada em TCP/IP.

2.2. Rede abrangente

Uma rede abrangente nada mais é que a interligação em larga escala das redes locais. Para interligar estas redes locais, usa-se um novo elemento: o roteador. Este é responsável por duas atividades: encontrar as melhores rotas entre duas redes e impedir o tráfego de difusão.

Como as redes abrangentes cobrem uma vasta área geográfica, uma forma de conectar as diversas redes locais é através dos enlaces de fibra ótica de longa distância. Estes enlaces comportam uma grande quantidade de dados trafegando a taxas de transmissão muito altas.

2.3. Modelo de rede ótica

Uma rede ótica é caracterizada por ter seus enlaces baseados em fibra ótica. Os enlaces de fibra ótica podem também ser usados em implementações de redes locais do tipo SAN (*Storage Area Network*). No entanto, neste trabalho, trataremos redes óticas a partir do ponto de vista das redes abrangentes.

Sendo assim, do ponto de vista do domínio elétrico, cada nó de uma rede ótica será formado pelo roteador de borda e pelos *transceivers* dos enlaces óticos que chegam e saem do roteador. Para garantir a alta disponibilidade da rede, um dos métodos mais usados é o uso de rotas múltiplas, que permitem que em caso de falha de um enlace, uma rota alternativa entre os nós possa ser estabelecida a partir de outros enlaces.

Já do ponto de vista do domínio ótico, devemos considerar todos os componentes que permitem que sejam estabelecidos caminhos de comunicação em uma malha de rede ótica. Isso é necessário pois o roteamento de dados no domínio ótico é bastante peculiar e difere totalmente da forma como é feito o roteamento de dados no domínio elétrico. O estudo destes componentes óticos e a análise de sua confiabilidade serão estudados a parte.

Além do *hardware* envolvido na construção da rede ótica, devemos considerar também o *software* embarcado nos roteadores e demais elementos gerenciáveis. Nos roteadores, por exemplo, o *software* é responsável por selecionar, por meio de algoritmos e protocolos, as melhores rotas para encaminhamento dos pacotes de dados. Nos demais elementos óticos gerenciáveis, o *software* é responsável por permitir a configuração dos componentes de forma remota.

2.3.1. Topologia de rede

Além dos detalhes em nível de equipamentos, devemos levar em conta também a topologia que a rede pode assumir. Assim, o modelo de rede ótica consiste em nós interconectados por enlaces que podem acomodar uma ou mais fibras, e cada fibra pode acomodar um ou mais canais. A conexão entre os nós é satisfeita quando é estabelecido um caminho de luz entre o nó origem e o nó destino. O caminho de luz, ou simplesmente caminho, é um canal ótico entre dois nós, formando assim uma rota, que possui o mesmo comprimento de onda por todos os nós e segmentos da rede em que passa.

Dependendo da disponibilidade de comprimentos de onda em um determinado segmento da rede, pode haver ou não a necessidade de se usar a conversão de comprimentos de onda. Independente do que ocorre fisicamente, um caminho que atravessa uma parte da rede pode ser encarado como uma conexão de circuito comutado que pode ser reconfigurada. Assim, um conjunto de caminhos lógicos irá constituir a topologia lógica da rede, independente do que ocorre na topologia física [18].

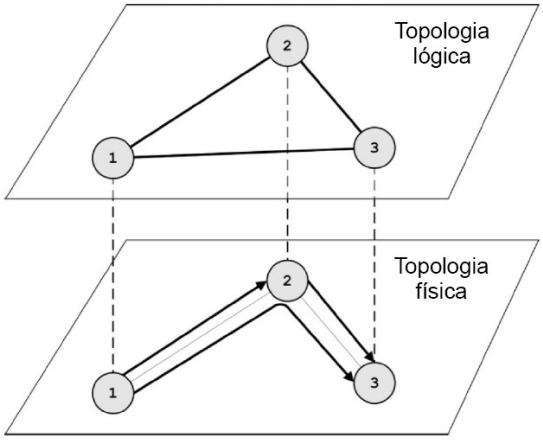
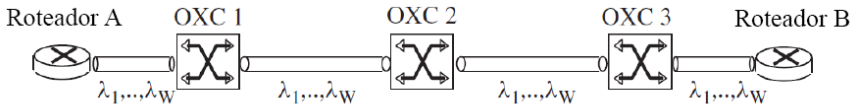
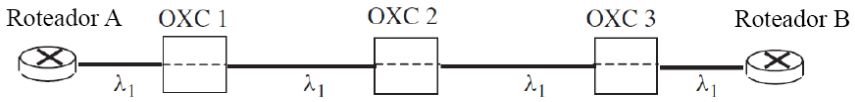


Figura 5 – Camadas física e lógica de uma rede ótica [18]

Cada nó na topologia física consiste de um comutador ótico e de um equipamento de terminação do sinal ótico, a menos que o nó funcione apenas como retransmissor do sinal. Um canal ótico que passa por um comutador pode ser roteado de uma fibra na entrada do equipamento para outra fibra na saída. Se isso for feito puramente no domínio ótico, o mesmo comprimento de onda na entrada deverá estar disponível também na saída e em todos os outros nós por onde este canal passar. Na Figura 6(a), por exemplo, entre os roteadores A e B há três comutadores, com diversos comprimentos de onda disponíveis. Na Figura 6(b) é estabelecido um caminho de luz onde é atribuído o mesmo comprimento de onda em cada um dos comutadores.



(a) Comprimentos de onda disponíveis em cada comutador



(b) Um caminho de luz estabelecido entre os roteadores A e B

Figura 6 – Estabelecimento de um caminho de luz [19]

Caso seja necessário, poderá ser usada a conversão de comprimentos de ondas, de forma a acomodar o canal no comprimento de onda disponível no segmento, mesmo que ele seja diferente do comprimento de onda do segmento de origem [18].

2.3.2. Roteamento e atribuição de comprimentos de onda

Os caminhos de luz são a peça chave para a construção da topologia lógica da rede. Assim, o estabelecimento de rotas otimizadas e o melhor aproveitamento possível dos comprimentos de onda disponíveis são cruciais para se implementar uma rede ótica que possa usar o máximo dos recursos disponíveis. No entanto, em redes que não possuem a capacidade de conversão de comprimentos de onda, não é nada fácil estabelecer uma rota que passe por vários nós onde é necessário selecionar determinado comprimento de onda entre os diversos disponíveis. Ao se estabelecer uma rota, corre-se o risco de que em determinado segmento da rede, comprimentos de onda não possam ser usados porque nos segmentos adjacentes o mesmo comprimento não está mais disponível [20]. Isto é conhecido como problema de roteamento e atribuição de comprimentos de onda, ou RWA (*Routing and Wavelength Assignment*).

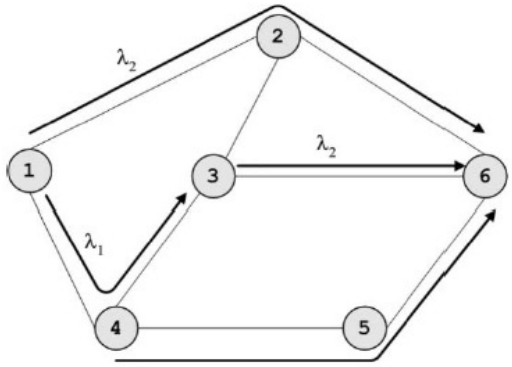


Figura 7 – Diferentes esquemas de atribuição de comprimentos de onda [18]

Há extensa pesquisa na literatura sobre o assunto, e algoritmos RWA têm sido estudados para permitir uma seleção adequada de rotas e comprimentos de onda entre as muitas escolhas possíveis para o estabelecimento de uma conexão [18].

2.4. Componentes de uma rede ótica

Os enlaces de uma rede ótica são formados por diversos elementos, que têm por principal objetivo permitir que o sinal chegue a grandes distâncias e que se possa selecionar e configurar caminhos alternativos para o tráfego de dados.

Se considerarmos um enlace ponto-a-ponto que interligue dois nós, teremos os seguintes componentes [21]:

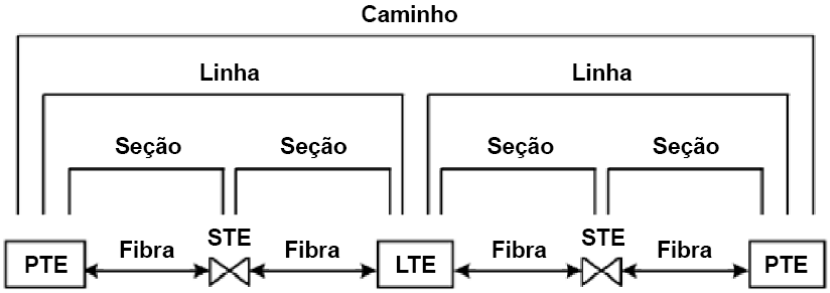


Figura 8 – Componentes de uma rede ótica ponto-a-ponto [21]

Onde:

- PTE (*Path Terminating Equipment*): pode ser um ponto de origem ou destino de um caminho ótico completo. Pode conter os componentes OLT, OADM ou OXC;
- LTE (*Line Terminating Equipment*): é o ponto de origem ou destino de um enlace. Pode conter os componentes OADM ou OXC;
- STE (*Section Terminating Equipment*): neste ponto são colocados os repetidores e/ou regeneradores de sinal. Pode conter um componente OLA do tipo OA ou RG.

O OLT (*Optical Line Terminal*), que também pode ser referenciado na literatura como OTM (*Optical Terminal Multiplexer/Demultiplexer*) ou OTMX, é a porta de entrada (ou saída) que um cliente deve usar para poder se conectar a uma rede ótica. Redes clientes que queiram enviar (ou receber) dados em uma rede ótica devem usar o OLT como interface para a conversão de diferentes tecnologias. Um OLT contém até três elementos funcionais: um multiplexador/demultiplexador de comprimentos de onda, um *transponder* responsável por adaptar a freqüência do sinal e, opcionalmente, um amplificador ótico. A capacidade de multiplexar e demultiplexar vários comprimentos de onda de diferentes canais é muito útil na construção de redes óticas WDM

(*Wavelength Division Multiplexing*), CWDM (*Coarse Wavelength Division Multiplexing*) ou DWDM (*Dense Wavelength Division Multiplexing*) [22] [23] [24].

Figura 9 – Motorola AXS2200 Optical Line Terminal (OLT) [25]

Em uma rede WDM, o OADM (*Optical Add and Drop Multiplexer*) é o elemento responsável por adicionar ou retirar canais seletivamente em um enlace ótico.

Já o OXC (*Optical Cross Connect*) é um comutador de sinais óticos, onde N canais na entrada podem ser comutados para N canais na saída, permitindo assim que novos caminhos alternativos para o tráfego de dados possam ser criados e configurados [19] [21].

O OLA (*Optical Line Amplifier*) é responsável por amplificar e/ou regenerar o sinal ótico, de forma que o enlace possa cobrir longas distâncias. Pode ser um amplificador OA (*Optical Amplifier*), que trabalha puramente no domínio ótico, ou um regenerador RG (*Dispersion Compensation Components and Regenerators*), que trabalha no domínio ótico-elétrico e faz o trabalho de resincronizar, reconverter e rerotear os dados (*retiming, reconversion e reroute*) [23].

Todos estes elementos são usados em arquiteturas que podem suportar várias topologias, incluindo as topologias em anel e em malha. Os OLT's multiplexam vários comprimentos de onda em uma única fibra ótica e também demultiplexam um sinal WDM composto em comprimentos de onda individuais. É importante frisar que a tecnologia WDM também se refere às tecnologias DWDM e CWDM. Já os OADM's são usados nos locais onde se queira extrair comprimentos de onda específicos para serem terminados localmente ou introduzir novos comprimentos de onda a serem

roteados para outros destinos. Por sua vez, os OXC's desempenham funções semelhantes aos OADM's, mas em uma escala muito maior em termos de portas e comprimentos de onda suportados, pois em uma rede distribuída são usados para interconectar diversos anéis ou malhas, que podem ter como clientes roteadores IP, comutadores ATM e terminais SONET, entre outros [22]. A Figura 10 mostra um exemplo de rede em anel que usa OADM´s para inserir e retirar comprimentos de onda da rede.

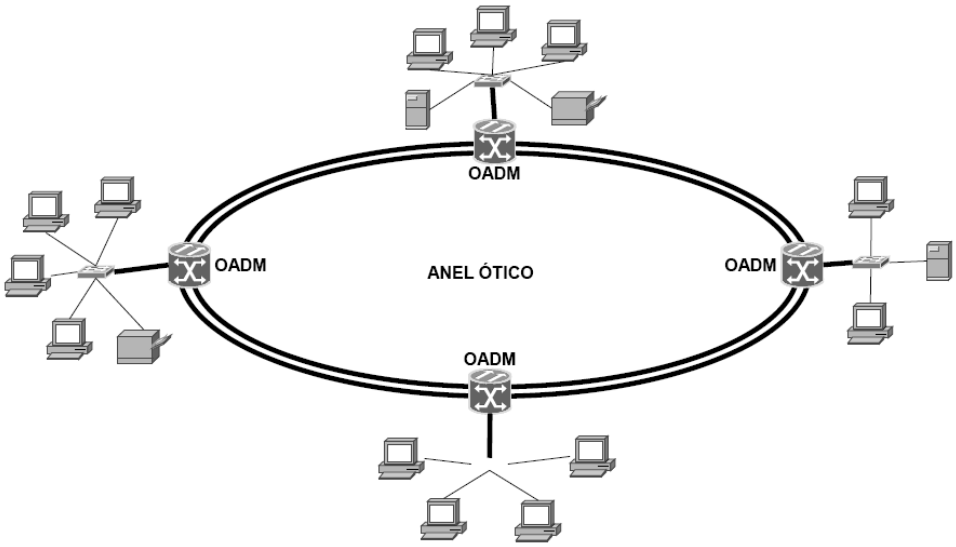


Figura 10 – Rede em anel com dispositivos OADM [26]

Há ainda inúmeras características importantes que são desejáveis em uma rede ótica. A reutilização de comprimentos de onda, por exemplo, permite suportar uma grande quantidade de caminhos de dados ao longo de uma rede usando-se uma quantidade limitada de comprimentos de onda disponíveis em cada enlace. Para isso, é necessário que a rede suporte a conversão de comprimentos de onda. Imaginemos a comunicação entre dois nós em duas redes distintas, mas adjacentes, que atravessa um caminho ótico qualquer entre elas. Na primeira rede este caminho ótico usa um dado comprimento de onda, mas quando entra na segunda rede pode ser que o mesmo comprimento de onda não esteja disponível. Assim, a conversão permitirá que um diferente comprimento de onda que esteja disponível naquela rede possa ser utilizado para completar o caminho [22].

A Figura 11 mostra um exemplo de rede em malha com diversos tipos de clientes, representados pelos quadrados nomeados de A a F. Cada caminho de luz que interliga estes clientes aloca comprimentos de onda conforme sua disponibilidade. Note que o caminho que passa pelo nó X e

que interliga os clientes E e F precisou utilizar o recurso de conversão de comprimento de onda para estabelecer a comunicação.

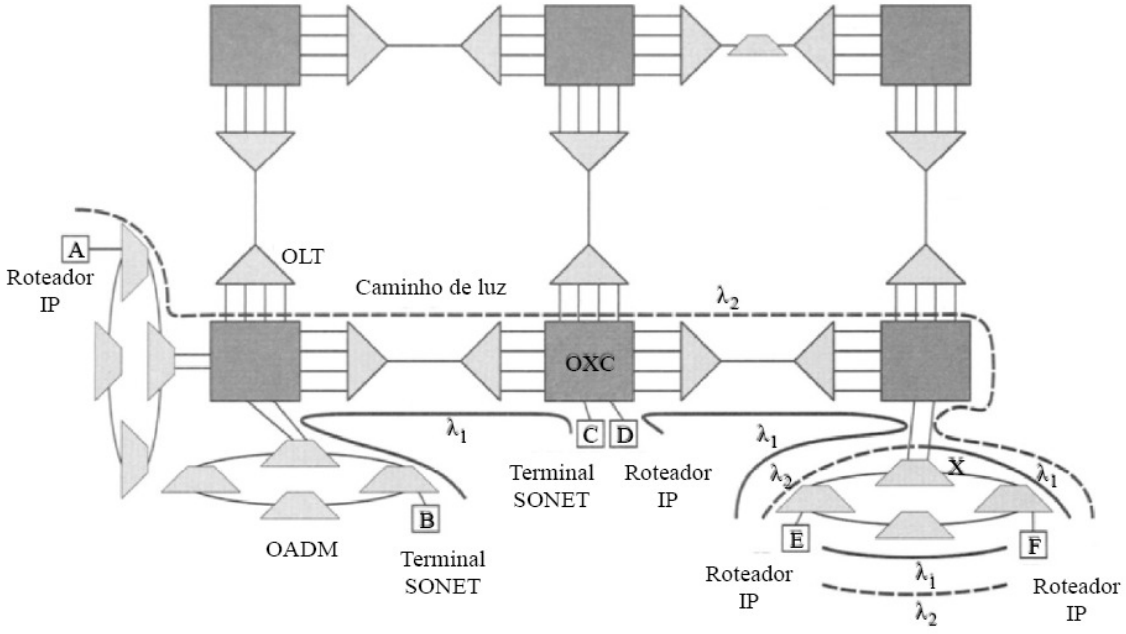


Figura 11 – Componentes de uma rede ótica em malha [22]

Outras características importantes são a transparência, o chaveamento de circuitos, a capacidade de sobrevivência e a topologia de caminhos óticos.

A transparência diz respeito ao fato de que os caminhos óticos podem transportar dados com taxas de transferência de bits variadas e diferentes protocolos de rede. O chaveamento de circuitos é a capacidade de se configurar caminhos óticos sob demanda, localmente ou remotamente. Capacidade de sobrevivência é quando a rede pode suportar o roteamento por caminhos alternativos quando um dado enlace encontra-se em falha. A topologia de caminhos óticos é a visão que as camadas mais altas têm da configuração da rede no nível da camada ótica. Enquanto que na camada ótica um caminho de dados pode percorrer vários equipamentos, nas camadas mais altas este caminho pode ser visto como um único enlace que interliga roteadores IP, por exemplo [22].

2.4.1. Optical line terminal

O OLT é um componente de rede relativamente simples comumente usado para multiplexar e demultiplexar comprimentos de onda. Podem ser formados por *transponders*, responsáveis por adaptar

o sinal de entrada para ser transportado no domínio ótico, bem como por multiplexadores de comprimentos de onda e, opcionalmente, amplificadores óticos [22]. A Figura 12 mostra o esquema de um OLT onde o sinal dos clientes não compatíveis com a norma ITU é convertido primeiramente no *transponder*, antes de ser encaminhado para o multiplexador/demultiplexador, que na sua saída ainda possui um canal separado de supervisão OSC (*Optical Supervisory Channel*).

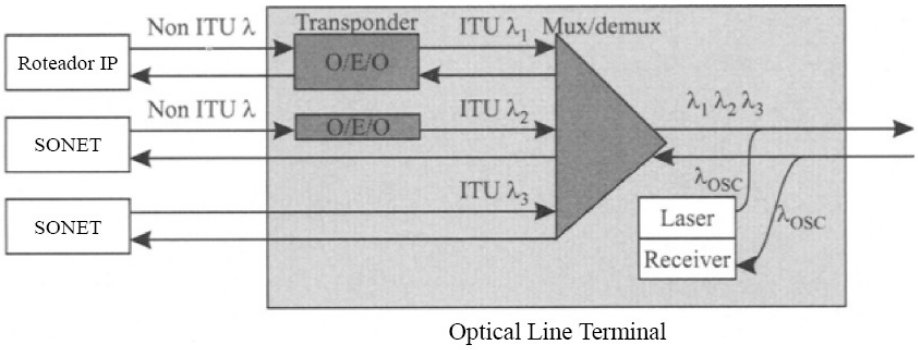


Figura 12 – Esquema de um OLT (*Optical Line Terminal*) [22]

2.4.2. Optical line amplifier

O sinal ótico, quando transmitido, perde potência ao longo do caminho e dificulta sua detecção após percorrer longas distâncias. Os amplificadores ou regeneradores são usados então para restaurar o sinal e colocá-los num nível de potência que possa ser detectado nos estágios seguintes. Tipicamente, são instalados ao longo de um enlace ótico a cada 80-120 quilômetros [22]. No caso dos amplificadores, eles podem ser usados como amplificadores de potência, em linha ou como pré-amplificadores. No primeiro e no último caso, o sinal pode ser reforçado quando sai do multiplexador ou antes que entre no receptor. Amplificadores em linha são usados em enlaces WDM de longa distância para reforçar o sinal e compensar o que foi perdido ao longo do caminho [19].

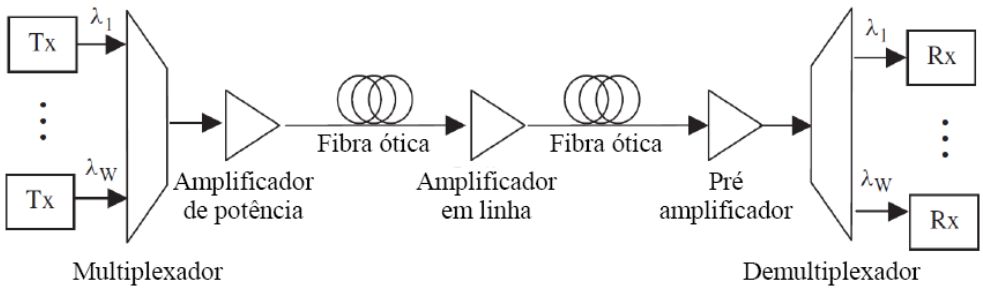


Figura 13 – Um típico enlace WDM [19]

Antes do advento dos amplificadores puramente óticos (OA), a única opção existente era usar os regeneradores (RG), que convertem o sinal do domínio ótico para o domínio elétrico, regeneram-no e então convertem-no novamente para o domínio ótico [22].

Figura 14 – Infinera Optical Line Amplifier (OLA) [27]

No regenerador, antes de o sinal ser retransmitido, o sinal é convertido do domínio ótico para o domínio elétrico, e então é aplicado o que se chama de 1R, 2R ou 3R, e novamente o sinal é convertido para o domínio ótico. No domínio elétrico, 1R significa que o sinal é novamente amplificado (re-amplified); 2R significa que o sinal é novamente amplificado e transformado (re-shaped) e 3R que o sinal é novamente amplificado, transformado e sincronizado (re-timed) [19].

Também é possível amplificar o sinal totalmente no domínio ótico, como o uso de amplificadores óticos (OA), usando fibras amplificadoras dopadas com érbio (EDFA - *Erbium-doped fiber amplifier*), amplificadores do tipo RAMAN ou baseados em semicondutores [22]. No domínio ótico, não é possível aplicar o 2R e o 3R [19].

Na Figura 15 é mostrado o esquema de um amplificador do tipo OA baseado em fibra dopada com érbio. Este tipo de amplificador consiste de um comprimento de fibra de sílica cujo núcleo é dopado com átomos ionizados de érbio. Esta fibra é bombeada por meio de um sinal gerado a partir de um *laser*, geralmente no comprimento de onda de 980 nm ou 1.480 nm. A fim de combinar a saída do *laser* da bomba com o sinal de entrada, a fibra dopada é precedida por um acoplador de comprimento de onda seletivo. Na saída, outro acoplador pode ser usado para separar o sinal amplificado de

qualquer sinal remanescente do bombeamento. Geralmente, um isolador é usado na entrada ou na saída do amplificador para evitar reflexos no sinal [22].

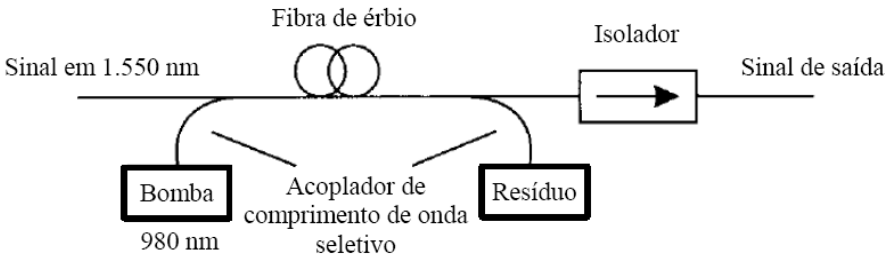


Figura 15 – OLA do tipo OA baseado em fibra dopada com Érbio [22]

O amplificador OA é um dispositivo analógico, o que significa que ele amplifica todos os canais existentes em uma fibra ótica e qualquer ruído que esteja presente no sinal. Já no regenerador RG, cada canal é individualmente demodulado e convertido para o domínio elétrico, onde os bits são amostrados e sincronizados, quando então são novamente modulados e convertidos para o domínio ótico [21].

2.4.3. Optical add and drop multiplexer

O OADM tem a capacidade de adicionar e retirar seletivamente determinados comprimentos de onda em um enlace de fibra ótica. Geralmente ele é configurado para adicionar ou retirar um grupo fixo de canais, permitindo que os demais passem diretamente por ele [22] [28].

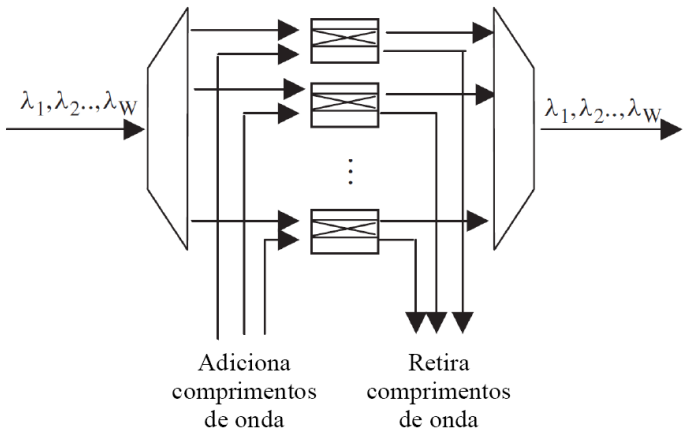


Figura 16 – OADM (*Optical Add and Drop Multiplexer*) [19]

O OADM pode ser usado em topologias de rede linear ou anel, e pode operar no modo fixo ou reconfigurável. No modo fixo, os canais que poderão ser adicionados ou retirados são previamente fixados e só podem ser configurados manualmente. Já no ROADM (*Reconfigurable Optical Add and Drop Multiplexer*), os canais podem ser configurados dinamicamente e de forma remota [28].

2.4.4. Optical cross-connect

Um OXC é um comutador ótico do tipo N x N, com N fibras de entrada por N fibras de saída. O OXC pode comutar oticamente todos os comprimentos de onda de uma dada fibra na entrada em comprimentos de onda de uma dada fibra na saída. O OXC também pode ser usado como um OADM (*Optical Add and Drop Multiplexer*) [19].

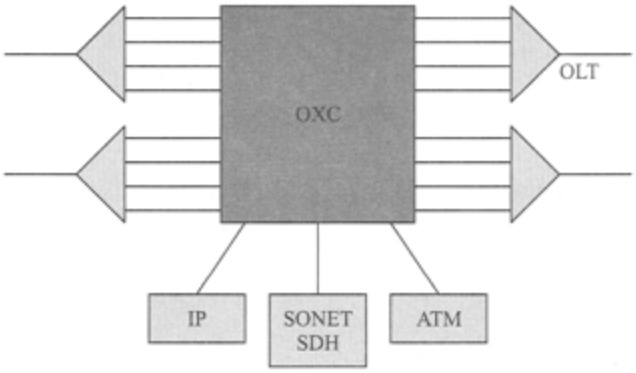


Figura 17 – OXC (*Optical Cross-connect*) [22]

3. Análise da confiabilidade dos elementos que formam uma rede ótica

Uma das formas de se estudar a confiabilidade das redes óticas é através da mensuração da sua vida útil e da probabilidade de falhas ocorrerem durante este período. Durante a operação de um sistema real, se um equipamento falha, ele é reparado ou substituído por um novo. Assim, o equipamento, durante sua vida útil, poderá estar em dois estados distintos: funcionando ou em reparo. Conforme vão ocorrendo falhas, o sistema alterna entre estes dois estados. Podemos então dizer que a vida útil de um equipamento é a soma do tempo médio até apresentar falhas e do tempo médio para reparos. Para fins de disponibilidade do sistema, devemos considerar também o tempo de parada planejado para manutenção preventiva.

Na literatura, a confiabilidade é definida como a habilidade de um sistema ou equipamento exercer sua função sob uma determinada condição durante um período específico de tempo, e a disponibilidade é o quanto um sistema ou equipamento está operacional e acessível quando solicitado [29].

3.1. Princípios de tolerância a falhas

De forma simplificada, a tolerância é a capacidade de um sistema resistir a falhas que possam causar a interrupção de sua operação [30].

Os conceitos de tolerância a falhas, resistência a falhas e alta disponibilidade se diferenciam quanto à quantidade de transações que podem ser perdidas em um evento de falha, quanto ao nível de indisponibilidade oferecido e quanto ao nível de degradação do sistema experimentado pelo usuário enquanto o sistema se recupera da falha [30].

A disponibilidade do sistema está fortemente associada ao tempo requerido para reparos após os eventos de falhas. Assim, quanto menor o tempo para reparos ou paradas planejadas para manutenção, maior será a disponibilidade.

As empresas podem definir vários níveis de disponibilidade, de acordo com a criticidade de suas operações [30]:

- Nível 1: usuários e serviços são interrompidos e os dados são corrompidos;
- Nível 2: usuários e serviços são interrompidos e os dados são preservados;
- Nível 3: usuários interrompidos, serviços permanecem funcionando;
- Nível 4: não há interrupções, mas o desempenho degrada;
- Nível 5: não há interrupções, e a recuperação de falhas é implementada.

Quanto maior o nível de disponibilidade, maior será o custo incremental para se atingir uma pequena melhora. Adicionar componentes redundantes (ou em paralelo) aumenta significativamente a disponibilidade do sistema, enquanto que a adição de componentes em série reduz a disponibilidade geral, já que todos os sistemas ligados em série devem funcionar para o serviço continuar em operação [30].

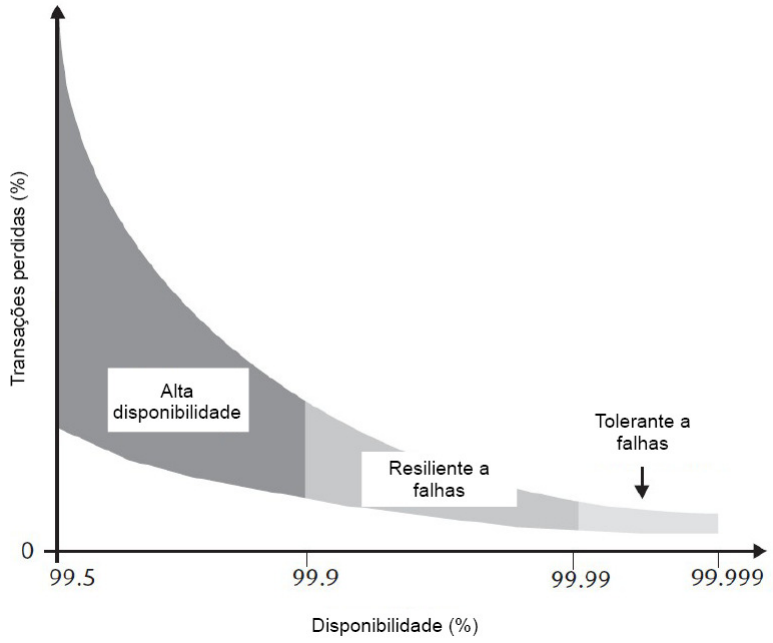


Figura 18 – Tolerância *versus* disponibilidade [30]

3.1.1. Sistemas tolerantes a falhas

Sistemas tolerantes a falhas possuem a habilidade de se recuperar automaticamente de falhas de modo a não impactar os serviços oferecidos pelo sistema. Está associada a disponibilidades que vão de 99,99% a 99,999%.

Em outras palavras, sistemas tolerantes a falhas necessitam que sejam identificados quais processos do sistema são críticos para sua operação. Uma vez identificados estes processos, então o sistema é projetado para se comportar de uma determinada maneira quando ocorrem os eventos de falhas. Assim, uma falha simples não irá causar uma interrupção de todo o sistema [30]

A capacidade de tolerância a falhas pode ser alcançada de várias formas, através do emprego de componentes redundantes, checagem de erros contínua e mecanismos de recuperação automática, entre outros.

3.1.2. Sistemas resilientes a falhas

Sistemas resilientes a falhas são semelhantes a sistemas tolerantes a falhas, mas com a diferença de que podem não preservar o estado de todas as transações durante o evento de falhas. Nestes sistemas o usuário pode perceber uma degradação dos serviços oferecidos [30].

3.1.3. Sistema de alta disponibilidade

Sistemas de alta disponibilidade geralmente estão associados a disponibilidades que vão de 99,5% to 99,9%. Estes sistemas são projetados assumindo-se que dados do estado das transações terão uma grande chance de serem perdidos durante o evento de falhas. O objetivo principal dos sistemas de alta disponibilidade não é prevenir a interrupção da operação, mas sim minimizar seus efeitos [30].

3.2. Medidas de tolerância a falhas

Todo equipamento em uma rede ótica atende a uma função específica e tem um tempo de vida útil estimado, e se espera que ele desempenhe corretamente suas funções neste intervalo de vida útil sem apresentar defeitos. No entanto, o desempenho ideal de um equipamento não é igual ao da vida real. Por causa de uma série de fatores, o equipamento sempre terá uma certa probabilidade de apresentar defeitos, o que poderá resultar na indisponibilidade do sistema.

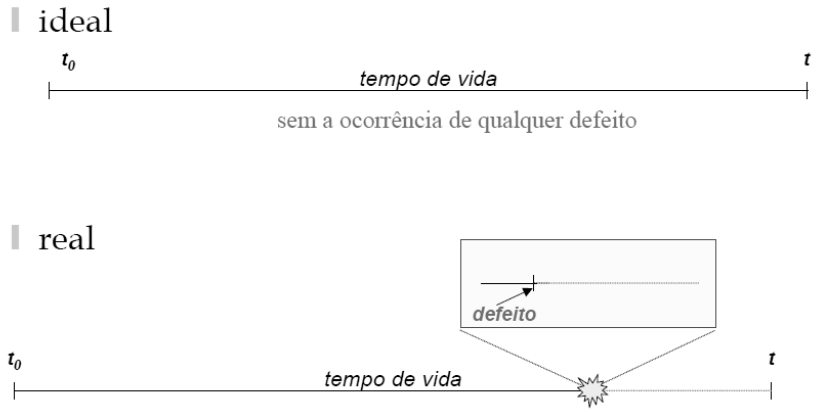


Figura 19 – Comportamento ideal e real de um componente [31]

A vida útil de um equipamento ou de uma população de equipamentos pode ser dividida em três períodos distintos, que são melhor visualizados em um gráfico conhecido como "curva da banheira", mostrado na Figura 20. Neste gráfico, existem três períodos distintos: o período de taxa de falhas decrescente, também conhecido como período de mortalidade infantil; o período de vida útil, ou de taxa de falhas constante; e o período de taxa de falhas crescente, no final da vida útil do componente.

O primeiro período é caracterizado por uma taxa de falhas decrescente. É o que ocorre durante o início da vida de uma população de equipamentos. Após a fabricação do equipamento, é aplicada uma técnica de *burn-in*, que consiste em expor os equipamentos a um ritmo de trabalho intenso e acelerado para eliminar os componentes mais fracos e que possuem alguma falha em seu processo de fabricação.

O próximo período é a parte plana do gráfico, que é chamado de vida normal do equipamento. As falhas neste período costumam acontecer em uma seqüência aleatória durante este tempo. Apesar de ser difícil de prever, a taxa com que as falhas acontecem neste período é previsível.

O terceiro período começa no ponto em que a inclinação começa a aumentar e se estende até o final do gráfico. Isto é o que acontece quando as unidades ficam velhas e começam a falhar em uma taxa crescente, pois já ultrapassaram o seu período de vida útil e as falhas passam a serem vistas como uma conseqüência natural do desgaste dos componentes [31] [32] [33].

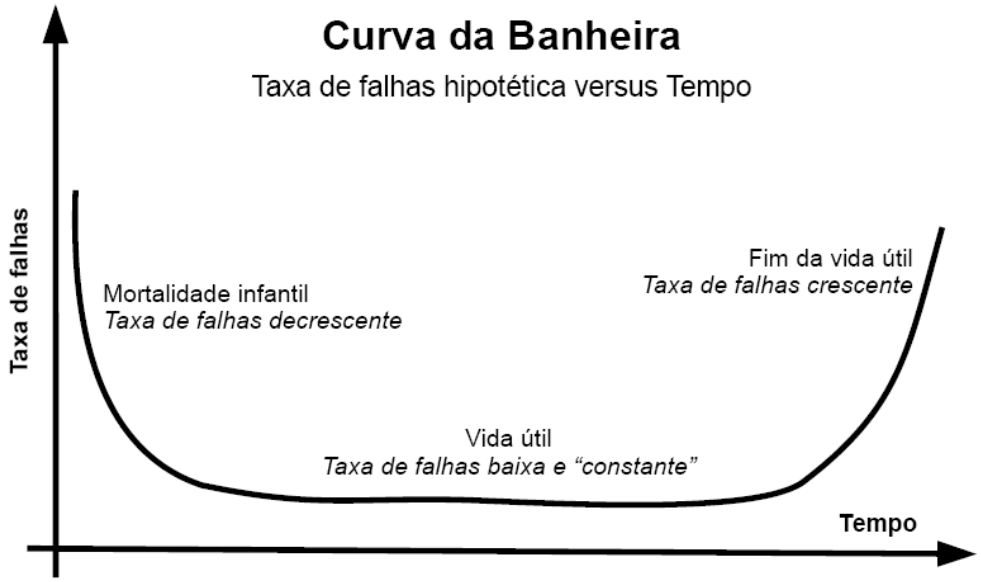


Figura 20 – Gráfico da Curva da banheira [31] [32] [33]

Assim, é extremamente importante conhecer o momento em que a taxa de falhas de um equipamento começa a crescer aceleradamente, pois assim é possível estimar seu tempo de vida útil e programar a troca do equipamento de forma a evitar uma indisponibilidade do sistema.

Durante a vida útil do equipamento ou produto, a taxa de falhas λ é praticamente constante, e a unidade de medida é a quantidade de falhas por unidade de tempo. Esta unidade de medida é a FIT, ou Falhas no Tempo (*Failures in Time*), que é o número de falhas por bilhão de horas. Assim:

$$1\ FIT = 1\ falha\ em\ 10^9\ horas \tag{1}$$

Como um ano tem 365 dias e ¼, o total de horas por ano é de 8.766 horas. Assim, o FIT em anos é dado por:

$$1\ FIT \approx 1\ falha\ em\ 114.077\ anos \tag{2}$$

Exemplo: Suponha que se deseja estimar a taxa de falhas λ de um determinado componente. Tomemos então dez componentes idênticos que são testados até que cada um falhe ou chegue a 1.000 horas de operação, momento em que o ensaio será terminado para aquele componente. Os resultados poderiam ser os seguintes:

Tabela 1 – Dados de ensaio para um componente hipotético

Componente	*Horas*	*Falhas*
1	1000	Não falhou
2	1000	Não falhou
3	467	Falhou
4	1000	Não falhou
5	630	Falhou
6	590	Falhou
7	1000	Não falhou
8	285	Falhou
9	648	Falhou
10	882	Falhou
Total	**7.502**	**6**

O cálculo da taxa de falhas λ é dado por:

$$\lambda = \frac{número\ de\ falhas}{tempo\ de\ observação \times tamanho\ da\ amostra} \tag{3}$$

Substituindo, temos:

$$\lambda = \frac{6}{7502 \times 10} \approx 0{,}0000799787 \approx 79.979 \times 10^{-9}\ \frac{falhas}{hora}$$

O que significa 79.979 falhas a cada 1 bilhão de horas.

Já o cálculo do MTTF é dado por:

$$MTTF = \frac{tempo\ de\ observação \times tamanho\ da\ amostra}{número\ de\ falhas} \tag{4}$$

Substituindo, temos:

$$MTTF = \frac{7.502 \times 10}{6} \approx 12.503\ horas$$

Para relacionar o FIT com o MTTF usamos a seguinte relação:

$$FIT = \frac{10^9}{MTTF\ (horas)} \tag{5}$$

Substituindo, temos:

$$FIT = \frac{10^9}{12.503} \approx 79.981$$

Na tabela abaixo são mostrados alguns valores típicos de taxa de falhas λ e taxa de reparos μ para equipamentos óticos e cabos de fibra ótica:

Tabela 2 – Taxa de falhas e taxa de reparos [21] [34] [35]

Equipamento ou serviço	*Taxa de falhas e taxa de reparos*
Emendas de cabos	FIT=30 ou MTTF=3.803 anos
Conectores	FIT=100 ou MTTF=1.141 anos
Rompimento de cabos	FIT=311 ou MTTF=367 anos para cada 1 km de fibra
Conjunto de circuitos lógicos de média complexidade	FIT=1.500 ou MTTF=76 anos
Circuito ótico de recepção	FIT=4.311 ou MTTF=26 anos
Comutadores de proteção	FIT=6.007 ou MTTF=19 anos
Circuito ótico de transmissão	FIT=10.867 ou MTTF=10 anos
Substituição de equipamento	MTTR=2 horas
Reparo de cabos	MTTR=12 horas

As redes de comunicação, em especial as redes óticas, estão sujeitas não só a falhas de equipamentos, mas a uma grande variedade de falhas que podem ou não ser acidentais, ou que ainda podem ser causadas por fenômenos naturais ou falhas humanas.

Se considerarmos os momentos em que um equipamento pode falhar em uma dada linha do tempo, teremos o seguinte gráfico:

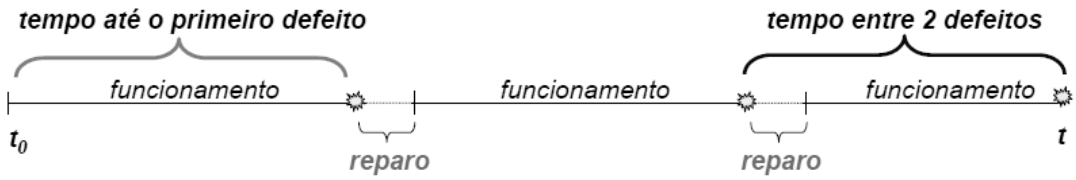


Figura 21 – Linha do tempo para falhas de um equipamento [31]

O tempo para ocorrer o primeiro defeito durante a vida útil de um equipamento ou produto é chamado de MTTF (*Mean Time to Failure*). O tempo de reparo (ou troca) deste equipamento é conhecido como MTTR (*Mean Time to Repair*), que inclui o tempo necessário para a notificação da falha, o tempo gasto com o deslocamento do técnico de campo, o tempo gasto com o transporte da nova peça do almoxarifado até o local de instalação e o tempo gasto no reparo ou troca propriamente dito. No MTTR devemos considerar também as paradas planejadas para manutenção. O intervalo entre as falhas do equipamento é chamado MTBF (*Mean Time Between Failures*) [31].

Tabela 3 – MTBF para alguns equipamentos óticos [36] [37] [38] [39]

Equipamento	*MTBF*
OLT SmartOptics Mux/Demux T-3004	4.383.000 horas ou 500 anos
OLA RAMAN Cisco C-Band	319.014 horas ou 36 anos
OLA EDFA Greatway Technology GWA3530	150.000 horas ou 17 anos
OADM CTC SML	57.000 horas ou 7 anos

Como os tempos de operação do sistema são muito maiores que os tempos de reparo, os valores de MTTF e de MTBF são muito próximos, o que faz com que seja possível usar um ou outro na análise de confiabilidade. Assim, temos que a relação entre estas três medidas se dá da seguinte forma:

$$MTBF = MTTF + MTTR \tag{6}$$

A taxa de falhas (λ) se relaciona com o MTTF através da seguinte equação:

$$\lambda = \frac{1}{MTTF} \tag{7}$$

Da mesma forma, a taxa de reparos (μ) se relaciona com o MTTR através da seguinte equação:

$$\mu = \frac{1}{MTTR} \tag{8}$$

Na tabela abaixo são mostrados alguns valores típicos de MTBF:

Tabela 4 – Valores típicos de MTBF e MTTR para falhas em equipamentos de comunicação [40]

Equipamento	*Faixa de MTBF (horas)*	*MTTR típico (horas)*
Servidor Web	$10^4 – 10^6$	1
Interface de rede	$10^4 – 10^5$	2
Interface de Roteador	$10^5 – 10^6$	2
Comutador ATM	$10^5 – 10^6$	2
Comutador SONET	$10^5 – 10^6$	4
Comutador SDH	$10^5 – 10^6$	4
Comutador WDM	$10^5 – 10^6$	6

Para medir a confiabilidade de uma rede ótica, o termo confiabilidade é definido como a probabilidade de um elemento da rede estar em plena operação durante um período de tempo [30] [41], e disponibilidade é a probabilidade de um elemento da rede estar operacional em um ponto particular do tempo [30].

A confiabilidade ou *reliability* (R) de um sistema ou equipamento é dada pela equação abaixo:

$$R = 1 - \frac{1}{MTTF} \tag{9}$$

Ou

$$R = 1 - \lambda \tag{10}$$

Quando o componente está sujeito apenas às falhas que ocorrem em intervalos aleatórios, e o número esperado de falhas é o mesmo para longos períodos de tempo, a confiabilidade pode ser definida pela equação exponencial [42]:

$$R(t) = e^{-\lambda t} \tag{11}$$

ou

$$R(t) = e^{\frac{-t}{MTTF}} \tag{12}$$

Onde:

λ=taxa de falhas, t=tempo de operação (ou tempo de vida útil) e MTTF=tempo médio até apresentar falhas.

Exemplo: dado um equipamento com MTTF de 500 mil horas e com vida útil esperada de aproximadamente 5 anos (ou tempo de operação), teremos:

$$R(t) = e^{\frac{-t}{MTTF}} = e^{\frac{-5\ anos \times 8.766\ horas}{500.000}} \approx 0{,}91607 = 91{,}61\%$$

De forma simplificada, diz-se que a disponibilidade ou *availability* (A) de um sistema é a fração de tempo em que ele está disponível para operação [43]. Isto pode ser representado pelas equações abaixo na forma:

$$A = \frac{MTTF}{MTTF + MTTR} \tag{13}$$

Ou

$$A = \frac{\mu}{\mu + \lambda} \tag{14}$$

Onde:

μ=taxa de reparos, λ=taxa de falhas, MTTF=tempo médio até apresentar falhas e MTTR=tempo médio para reparos.

Por sua vez, a indisponibilidade ou *unavailability* (U) do sistema é a probabilidade complementar da disponibilidade, e é dada pela equação:

$$U = 1 - A \tag{15}$$

Exemplo: dado um equipamento com MTTF de 500 mil horas e com MTTR de 4 horas, teremos:

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{500.000}{500.000 + 4} \approx 0{,}999992 \approx 99{,}9992\%$$

$$U = 1 - A = 1 - 0{,}999992 = 0{,}00008\%$$

Na tabela abaixo são mostrados alguns valores típicos de disponibilidade:

Tabela 5 – Classes de Disponibilidade [30]

Disponibilidade (%)	*Indisponibilidade Anual*	*Descrição*
98	175,2 horas	Falhas são freqüentes
99	87,6 horas	Falhas são raras
99,5	43,8 horas	Considerado alta disponibilidade
99,9	8,8 horas	Considerado resiliente a falhas
99,99	52,6 minutos	Considerado tolerante a falhas
99,999	5,3 minutos	Cinco noves
99,9999	31,5 segundos	Seis noves
100	0	Disponibilidade contínua

De acordo com [30], quanto maior o valor de MTBF (ou MTTF), maior será a disponibilidade do sistema:

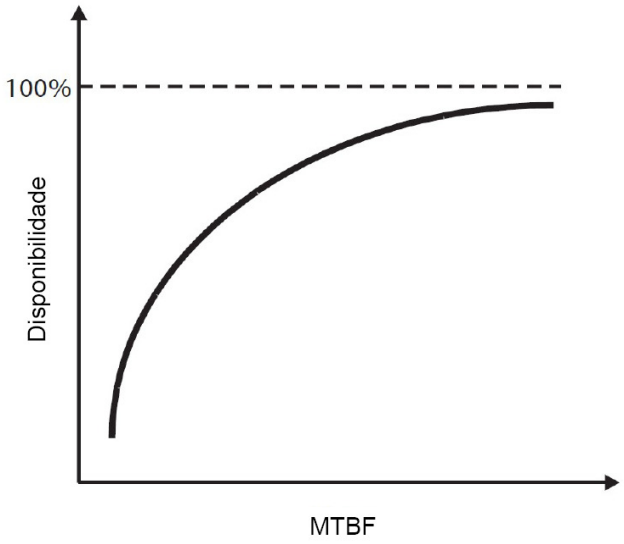


Figura 22 – Disponibilidade *versus* MTBF [30]

De modo análogo, quanto menor o MTTR, menor será o impacto no valor da disponibilidade do sistema:

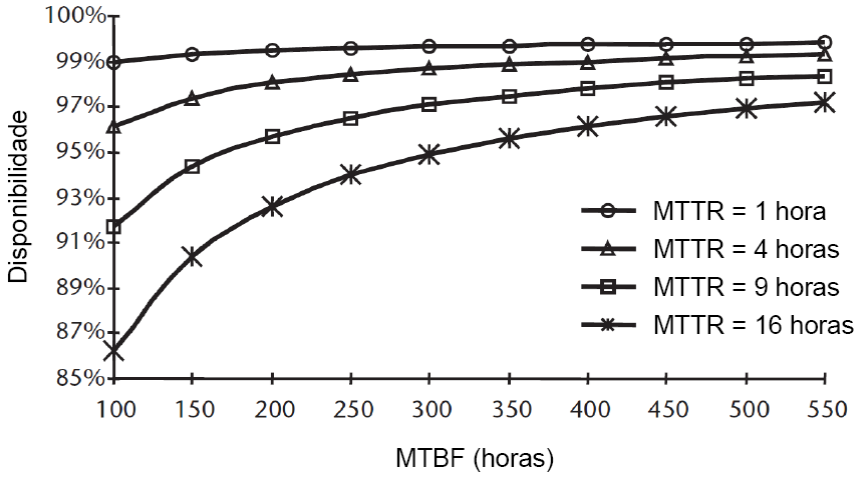


Figura 23 – Efeito do valor de MTTR na disponibilidade [30]

Assim, as empresas tomadoras de serviço podem querer estabelecer que os fornecedores de assistência técnica ofereçam os menores tempos de reparos possíveis. Este tipo de exigência é estabelecido em um contrato denominado Acordo de Nível de Serviço, ou Service Level Agreement (SLA).

3.3. Métodos para predizer e estimar o MTTF

Para calcular os valores de MTTF de um dado equipamento ou produto, podem-se usar dois métodos: o da predição e o da estimação. No método de predição o valor do MTTF é calculado levando-se em conta o projeto do sistema e os componentes usados na sua construção. Este método é útil quando o projeto dos componentes que compõem o produto é novo e não existe histórico de seu comportamento. Já o método de estimação é usado quando já existe um histórico considerável de dados a respeito das características e propriedades dos componentes que compõem o equipamento ou produto. Como o segundo método é baseado em dados concretos, equipamentos que usam o método de estimação possuem um valor de MTTF mais próximo do valor real [44].

3.3.1. Métodos para predizer a confiabilidade

Os primeiros métodos usados para o cálculo de confiabilidade usando o predição surgiram na década de 1940, com o cientista alemão Wernher von Braun e o matemático alemão Eric Pieruschka, durante a tentativa de melhorar a confiabilidade dos foguetes V-1. Pieruschka ajudou Braun a modelar a confiabilidade dos foguetes V-1 e assim documentar os primeiros modelos preditivos de confiabilidade modernos. Posteriormente, com o avanço da indústria nuclear e aeroespacial, a área de análise da confiabilidade foi crescendo e se aperfeiçoando cada vez mais [44].

3.3.1.1. MIL-HDBK 217

Publicado pelo exército dos Estados Unidos em 1965, o Military Handbook 217 foi criado para oferecer um procedimento padrão para calcular a confiabilidade dos equipamentos e sistemas militares que usam componentes eletrônicos.

O documento descreve duas formas para predizer a confiabilidade: *Parts Count Prediction* e *Parts Stress Analysis Prediction*. A primeira forma é usada quando o equipamento ou produto está na sua fase inicial de desenvolvimento. Consiste em agrupar componentes similares e contá-los. O número de componentes em cada grupo é então multiplicado por uma taxa de falhas genérica e por um fator de qualidade tabelados no MIL-HDBK 217. Então, a taxa de falhas de todos os diferentes grupos

é somada para se obter a taxa de falhas final. Por definição, é assumido que todos os componentes estão em série e é necessário o cálculo separado para os componentes que não estão em série.

A segunda forma é usada já na fase final do desenvolvimento do equipamento ou produto, quando o projeto dos circuitos e a relação dos componentes sofrerão pouca ou nenhuma mudança. É similar à primeira forma de predição, mas o taxa de falhas é calculada individualmente para cada componente baseado nas condições de funcionamento e operação a que cada componente estará sujeito, como umidade, temperatura, vibrações, tensão, corrente, etc. Normalmente a taxa de falhas calculada na segunda forma é menor que na primeira.

Atualmente, o MIL-HDBK 217 é raramente usado. Em 1996, o exército dos Estados Unidos anunciou que o MIL-HDBK 217 seria descontinuado. Em parte porque hoje, com a confiabilidade cada vez maior dos componentes eletrônicos, pesquisas apontam que as falhas ocorrem mais por problemas na operação, no controle do processo de produção e no projeto do produto.

3.3.1.2. Telcordia

O modelo de predição Telcordia nasceu na indústria de telecomunicações e passou por uma série de mudanças ao longo dos anos. Foi desenvolvido inicialmente pela Bellcore Communications Research sob o nome de Bellcore para calcular a confiabilidade de equipamentos de telecomunicações. Apesar de ser baseado no MIL-HDBK 217, o modelo de confiabilidade e os métodos de predição foram alterados em 1985 para refletir as novas características dos equipamentos da época. A SAIC comprou a Bellcore em 1997 e mudou seu nome para Telcordia. A última revisão do Telcordia Prediction Model é a SR-332 Issue 1, publicada em maio de 2001, e continua a ser aplicada pela indústria como ferramenta para cálculo da confiabilidade [44].

3.3.1.3. HRD5

O HRD5 é a sigla para *Handbook for Reliability Data for Electronic Components*, usado para o cálculo da confiabilidade em sistemas de telecomunicações. Foi desenvolvido pela British Telecom e é usado principalmente na Inglaterra. É similar ao MIL-HDBK 217, porém não cobre todas as variáveis

ambientais, mas provê um modelo de predição que engloba uma quantidade muito maior de componentes eletrônicos [44].

3.3.1.4. RBD

O RBD (*Reliability Block Diagram*) é uma ferramenta gráfica usada para modelar a confiabilidade e a disponibilidade de um sistema. A estrutura do diagrama de bloco de confiabilidade define as interações lógicas das falhas em um sistema e não necessariamente as conexões físicas e lógicas dos componentes. Cada bloco representa um componente, um subsistema ou outra falha representativa. O diagrama pode representar um sistema inteiro, um subsistema ou qualquer combinação que requeira análise de falhas, de confiabilidade ou de disponibilidade. Esta ferramenta também serve para mostrar como cada componente do sistema interfere na operação de todo o sistema [45].

3.3.1.5. FMEA/FMECA

O FMEA (*Failure Mode and Effects Analysis*) é um processo usado para analisar os modos de falha de um produto. A informação do modo de falha é então usada para determinar o impacto que cada falha terá sobre a operação do equipamento ou produto. Além disso, a análise do modo de falha pode atribuir um nível de gravidade de cada um dos modos, o que é chamado de FMECA (*Failure Mode, Effects and Criticality Analysis*). O FMEA utiliza uma abordagem de baixo para cima (*bottom-up*), ou seja, começa analisar desde o nível de componente até o nível de circuitos e posteriormente de suas funções no equipamento. Os dados de probabilidade necessários para se calcular a confiabilidade podem ser de difícil obtenção para vários componentes, principalmente se estes tiverem múltiplos estados ou modos de operação [44].

3.3.1.6. Árvore de falhas

A árvore de falhas é uma técnica que foi desenvolvida pela Bell Telephone Laboratories para avaliar a segurança do Minuteman Launch Control System, que são sistemas de lançamento e monitoramento de mísseis balísticos intercontinentais que carregam ogivas nucleares. Posteriormente, foi aplicada para análise de confiabilidade de sistemas [45].

A árvore de falhas se utiliza da abordagem de cima para baixo (*top-down*), baseando-se numa lista de eventos relacionados tanto à operação normal quanto a uma falha. A árvore é então montada desde o nível de funções e circuitos até o nível de componentes. A confiabilidade é então calculada convertendo-se a árvore de falhas em um conjunto de equações equivalentes. Assim como o FMEA, os dados de probabilidade necessários para se calcular a confiabilidade podem ser de difícil obtenção [44].

3.3.1.7. HALT

O HALT (*Highly Accelerated Life Testing*) é um método utilizado para aumentar a confiabilidade global do projeto de um equipamento ou produto. Através do HALT, pode-se predizer quanto tempo é necessário para que o equipamento ou produto chegue ao final de sua vida útil. Para isso, o equipamento ou produto é submetido a testes intensivos que são cuidadosamente medidos e controlados. Um modelo matemático é então utilizado para calcular a quantidade real de tempo que teria levado o equipamento ou produto a falhar em campo. Embora HALT possa estimar o MTBF, sua função principal é melhorar a confiabilidade do projeto [44].

3.3.2. Métodos para estimar a confiabilidade

Os métodos para estimar a confiabilidade usam dados reais de falhas em campo e, portanto, fornecem uma medida mais precisa da taxa de falhas. Estes dados podem não estar disponíveis para novos produtos ou equipamentos, e nem mesmo para aqueles fabricados em baixa escala [46].

3.3.2.1. Similar item prediction method

Este método provê uma forma rápida de se estimar a confiabilidade de um produto ou equipamento baseado no histórico de dados de confiabilidade de um item similar. A eficácia deste método depende da similaridade entre o produto em análise e o produto existente o qual possui dados de campo disponíveis. A semelhança deve se estender aos processos de fabricação, ambientes operacionais, funções do produto, etc. Para os produtos ou equipamentos que seguem um caminho evolutivo, este método de estimação é especialmente útil, uma vez que aproveita a experiência de

campo passado. No entanto, as diferenças entre os projetos devem ser cuidadosamente investigadas e levadas em conta na previsão final [46].

3.3.2.2. Field data measurement method

O método de medição de dados em campo é baseado na experiência de campo real dos produtos, desde o momento em que é fabricado e distribuído até o momento em que alguns produtos retornam para serem reparados. Este é um dos métodos mais utilizados pelos fabricantes, pois é parte integrante do seu programa de controle de qualidade, que são geralmente referidos como Gestão de Crescimento da Confiabilidade.

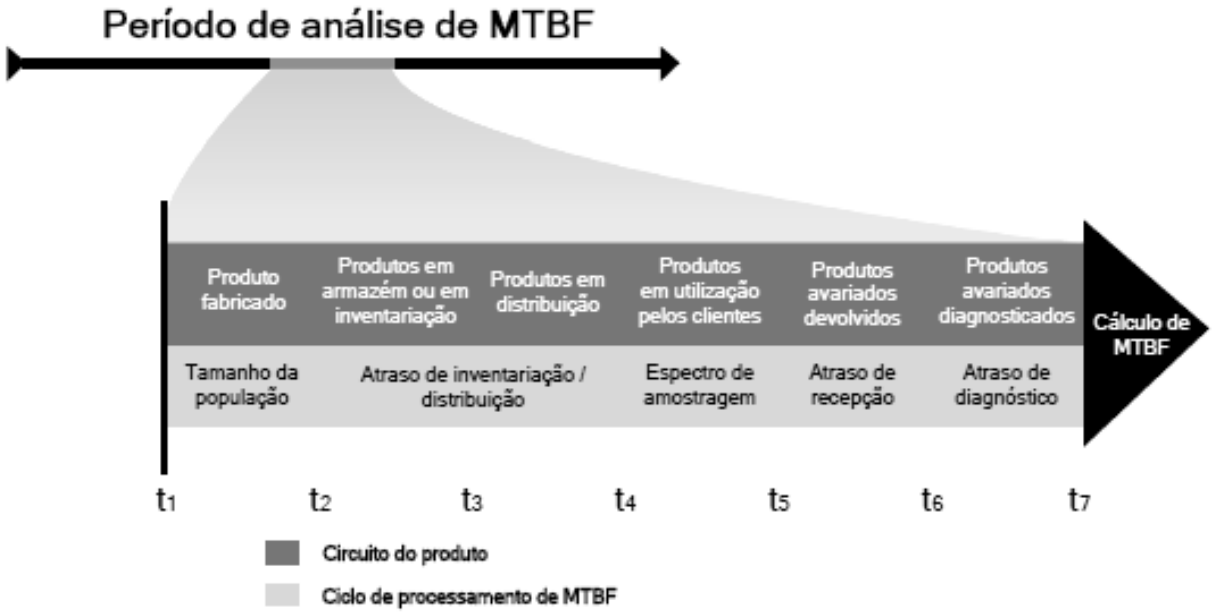


Figura 24 – Processo de medição de dados em campo [46]

Ao coletar as estatísticas de taxa de falhas de produtos ou equipamentos em uso no campo, um fabricante pode rapidamente identificar os defeitos mais comuns do produto. Pelo fato de ser baseado em falhas reais que de fato acontecem em campo, este método consegue identificar falhas que não são detectáveis nos métodos de predição.

Este método consiste em avaliar uma amostra populacional de novos produtos e coletar os dados de falha. Uma vez reunidos estes dados, é então calculado a taxa de insucesso e o MTTF. A taxa de falhas será então a porcentagem de uma população de unidades que se espera que "falhe" em um

dado ano calendário. Além de se utilizar estes dados para controle de qualidade, são usados também para fornecer aos clientes informações sobre a confiabilidade dos produtos e dos processos de qualidade. Como este método é de certa forma amplamente utilizado pela indústria, ele acaba fornecendo uma base comum para comparar valores de MTTF de produtos e equipamentos de diferentes fabricantes. Essas comparações permitem aos usuários avaliar as diferenças em relação à confiabilidade entre os produtos, e oferecem uma ferramenta na tomada de decisões de compra ou especificação. Como em qualquer comparação, é imperativo que as variáveis críticas sejam as mesmas para todos os sistemas que estão sendo comparados [46].

3.4. Avaliação de confiabilidade e disponibilidade

Para sistemas de comunicações óticas ponto a ponto, algumas equações podem ser usadas para se obter a disponibilidade equivalente de um sistema [43] [45] [47]. Se considerarmos a associação de elementos em série como na figura abaixo:

Figura 25 – Associação de elementos em série [43] [45]

Valerão as seguintes equações:

$$\lambda = \lambda_a + \lambda_b + \ldots + \lambda_n \tag{16}$$

$$MTTF = \frac{1}{\frac{1}{MTTF_a} + \frac{1}{MTTF_b} + \ldots + \frac{1}{MTTF_n}} \tag{17}$$

$$R = R_a \times R_b \times \ldots \times R_n \tag{18}$$

$$A = A_a \times A_b \times \ldots \times A_n \tag{19}$$

$$U = 1 - A = 1 - \left(A_a \times A_b \times \ldots \times A_n\right) \tag{20}$$

Considerando a associação de elementos em paralelo:

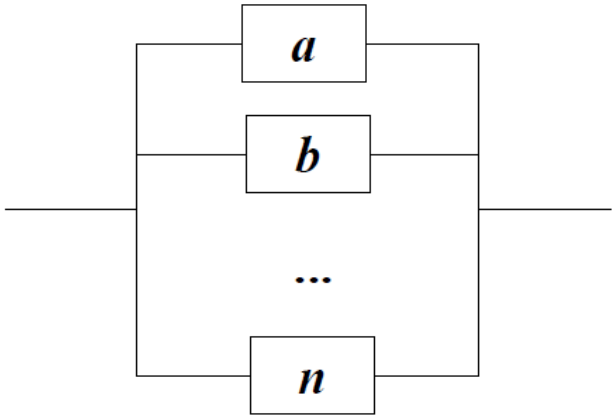


Figura 26 – Associação de elementos em paralelo [43] [45]

Valerão as seguintes equações:

$$\lambda = \lambda_a \times \lambda_b \times \ldots \times \lambda_n \tag{21}$$

$$MTTF = MTTF_a \times MTTF_b \times \ldots \times MTTF_c \tag{22}$$

$$R = 1 - \left[\left(1 - R_a\right) \times \left(1 - R_b\right) \times \ldots \times \left(1 - R_n\right)\right] \tag{23}$$

$$A = 1 - \left[\left(1 - A_a\right) \times \left(1 - A_b\right) \times \ldots \times \left(1 - A_n\right)\right] \tag{24}$$

$$U = U_a \times U_b \times \ldots \times U_n \tag{25}$$

Quando na associação em paralelo temos apenas dois elementos, as equações para calcular a confiabilidade *R* e a disponibilidade *A* podem ser simplificadas [48]:

$$R = R_a + R_b - R_a \times R_b \tag{26}$$

$$A = A_a + A_b - A_a \times A_b \tag{27}$$

3.4.1. Exemplo de aplicação

As falhas em uma rede ótica podem ocorrer ao nível do *link* de acesso, o que é chamado de falha de *link* simples, ou ao nível do nó, que é chamado de falha do nó simples. A diferença é que a falha de um nó afeta todos os *links* que chegam ou saem dele. E quando se considera que dois *links* podem falhar simultaneamente, esta falha é chamada de falha de *link* duplo.

Conforme demonstrado por [48], tomemos como exemplo o cálculo da confiabilidade entre dois nós numa rede em anel, formado por cinco nós e também por cinco *links* que os interligam. Neste exemplo iremos assumir que a origem é o nó A e o destino o nó D. A distância de cada *link* é dada em metros, e a parte em negrito que sai de cada nó são os *links* que compartilham o mesmo duto. Ou seja, para o nó E, os dois *links* que vão para os nós A e D compartilham um mesmo duto de 8.500 metros antes de serem separados. Assim, a falha neste trecho será mutuamente dependente.

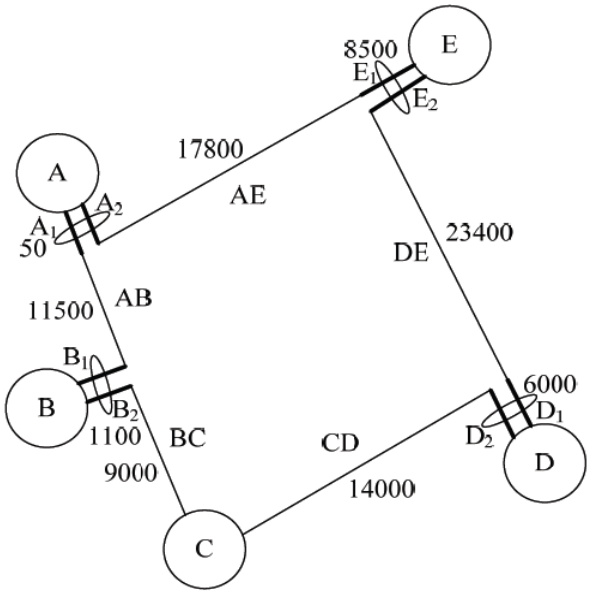


Figura 27 – Topologia em anel [48]

As partes dos *links* mutuamente dependentes são denotadas por (A_1, A_2), (B_1, B_2), (D_1, D_2) e (E_1, E_2).

Entre a origem A e o destino D existem dois caminhos possíveis. O primeiro caminho passa por B e C e o segundo caminho passa por E. Usando-se as associações em série e em paralelo temos o seguinte esquema:

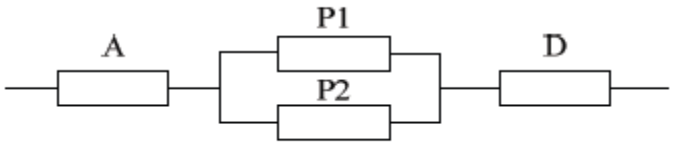


Figura 28 – Modelo de disponibilidade para os nós A-D [48]

Que pode ser calculado da seguinte forma:

$$A_{AD} = A_A \times A_P \times A_D \tag{28}$$

Onde A_P é a disponibilidade dos caminhos paralelos entre A e D:

$$A_P = A_{P1} + A_{P2} - A_{P1} \times A_{P2} \tag{29}$$

Onde A_{P1} é a disponibilidade do primeiro caminho:

$$A_{P1} = A_{A1} \times A_{AB} \times A_{B1} \times A_B \times A_{B2} \times A_{BC} \times A_C \times A_{CD} \times A_{D2} \tag{30}$$

E A_{P2} é a disponibilidade do segundo caminho:

$$A_{P2} = A_{A2} \times A_{AE} \times A_{E1} \times A_E \times A_{E2} \times A_{DE} \times A_{D1} \tag{31}$$

3.5. Acordo de nível de serviço

O Acordo de Nível de Serviço, ou *Service Level Agreement* (SLA), para o reparo de redes óticas varia de acordo com o tipo de usuário que utiliza o serviço ou o tipo de serviço que é transportado pela rede [40].

Como tipos de usuários, de acordo com [49], temos: usuários críticos de segurança, usuários críticos de negócios, usuário de baixo custo e usuários de nível básico.

A tabela abaixo mostra alguns tipos de serviços:

Tabela 6 – Serviços de aplicação e requerimentos típicos [40]

Aplicação	*Taxa de bits*	*Variação da Taxa de bits*	*Sensibilidade ao atraso*	*Necessidade de recuperação*
Serviços de telefonia	32-64 kbps	Constante	5	5
Voz sobre IP	8-32 kbps	Constante	5	5
Videofone	256-1920 kbps	Alta	5	5
Videoconferência	pelo menos 256 kbps	Alta	5	5
Trabalho à distância	de 64 kbps a 2 Mbps	Muito alta	5	4
Transmissão de TV	2-8 Mbps	Alta	4	4
Ensino à distância	de 64 kbps a 2 Mbps	Muito alta	5	5
Filmes sob demanda	de 750 kbps a 4 Mbps	Alta	4	3
Notícias sob demanda	64 kbps	Muito alta	2	2
Acesso Internet	de 64 kbps a 2 Mbps	Muito alta	1	2
Comércio eletrônico	de 64 kbps a 2 Mbps	Muito alta	2	2

Os níveis de SLA se dão em termos do tempo máximo que um sistema pode ficar indisponível. Assim, quanto maior o nível de SLA requerido (ou menor o tempo de indisponibilidade), maior será o custo.

4. Sobrevivência em redes óticas

Em uma rede ótica, uma rota que liga dois pontos geográficos pode conter muitos cabos de fibra, que por sua vez, pode conter muitas fibras. Uma rota com 10 milhas (ou quilômetros) usando 3 cabos de fibra é chamada de rota de 10 milhas ou rota de 30 milhas de cabos. Se cada cabo contiver 20 fibras, a mesma rota poderá ser chamada de rota de 600 milhas de fibras. Só nos Estados Unidos, até o final dos anos 1990, foram instaladas mais de 355 mil milhas de cabos, contendo mais de 16 milhões de milhas de fibras [22]. Só a rede KyaTera, por exemplo, possui cerca de 6.130 quilômetros de fibra, entre fibras próprias implantadas nos campus universitários e fibras apagadas cedidas pelas companhias de telefonia nos estados de São Paulo e Minas Gerais [4].

As redes óticas provêm uma infraestrutura por onde trafegam uma grande quantidade de dados, desde serviços de voz a tráfego multimídia. Muitos canais de dados podem trafegar por um único enlace de fibra, com o uso de técnicas de multiplexação, por exemplo. E a grande abrangência e uso das redes de fibra fazem com que sejamos cada vez mais dependentes delas.

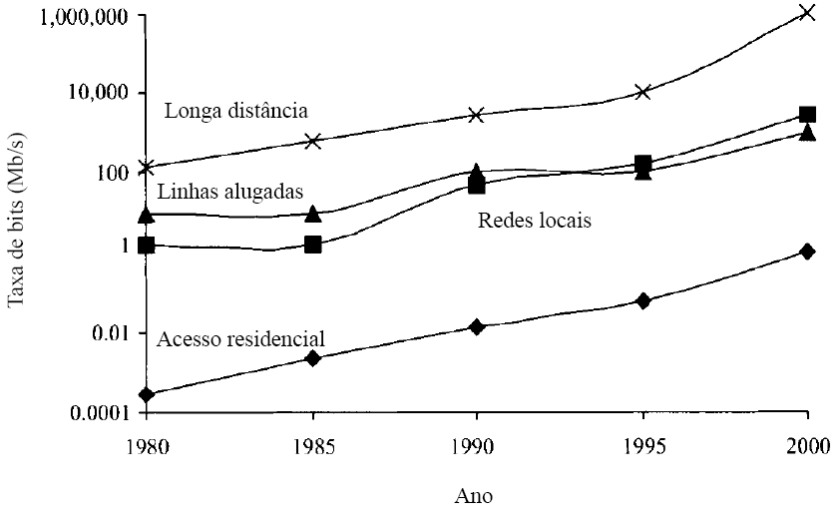


Figura 29 – Crescimento da largura de banda em diferentes tipos de redes [22]

A preocupação em prover métodos rápidos de recuperação de falhas se dá porque a largura de banda de uma fibra ótica excede dezenas de Tbps, e uma simples falha pode fazer com que milhões de usuários fiquem desconectados e, conseqüentemente, fazer com que muitas empresas percam dinheiro. Assim, melhorar os esquemas de proteção da rede é fundamental para assegurar a sobrevivência e a disponibilidade de uma rede ótica [19] [22].

São muitos os tipos de falhas que podem ocorrer em uma rede ótica, e o mais comum ainda é o rompimento de cabos, mas nem por isso os outros tipos de falhas devam ser desprezados. Em [28] são descritos alguns outros tipos, como falhas do nó, falhas no canal, falhas nas portas dos *switches* e roteadores, entre outros.

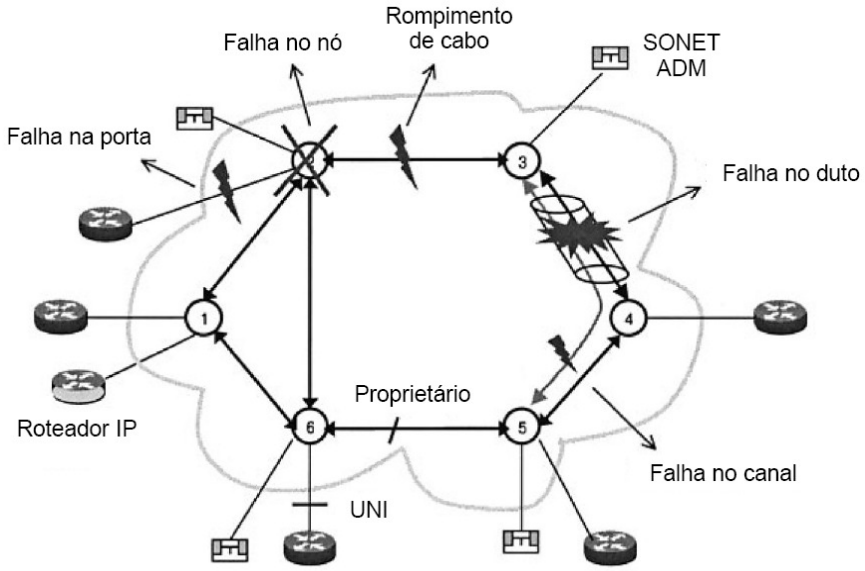


Figura 30 – Diferentes tipos de falha em uma rede ótica [28]

4.1. Visão geral sobre proteção e sobrevivência

O grau de sobrevivência ou disponibilidade de uma rede pode ser definido como a habilidade desta rede continuar a prover serviços mesmo num estado de falhas. No exemplo da Figura 31(a), os nós B e D têm dois caminhos possíveis de comunicação, seja pela rota BCD ou pela rota BAD. Já no caso da Figura 31(b), não há nenhuma rota alternativa entre os nós B e D.

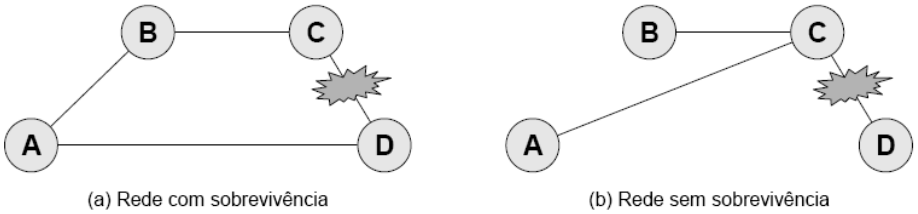


Figura 31 – Uma rede com disponibilidade e outra sem [50]

Assim, a proteção tem por objetivo prover redundância numa rede, de modo que os dados possam ser roteados por caminhos alternativos e restabelecer o tráfego existente mesmo quando ocorre uma falha.

4.1.1. Esquemas de proteção

Da mesma forma que existem vários tipos de falhas, também há diversos modos de se implementar a sobrevivência em redes óticas. A proteção de enlaces em redes óticas é uma delas, e este item irá focar na proteção das falhas decorrentes do rompimento do cabo, que é a falha mais comum do enlace. A proteção de enlaces pode ser classificada em esquemas de proteção, que usa uma reserva de recursos para poder implementar a sobrevivência, ou em esquemas de restauração, que usa uma capacidade excedente de recursos para garantir a operação da rede em casos de falha [51].

Redes óticas com esquemas de proteção são aquelas que possuem rotas alternativas de tráfego. Estas rotas alternativas podem ser dedicadas ou compartilhadas, e permitem que a velocidade com que a rede é restaurada seja maior. Já no esquema de restauração, novas rotas devem ser descobertas dinamicamente. A vantagem é que a utilização da rede torna-se mais eficiente, mas a velocidade com que a rede é restaurada é menor se comparada com as redes que possuem esquemas de proteção [51].

Uma visão ampliada dos esquemas de proteção de redes óticas pode ser vista em [52] [53] [54] [55]:

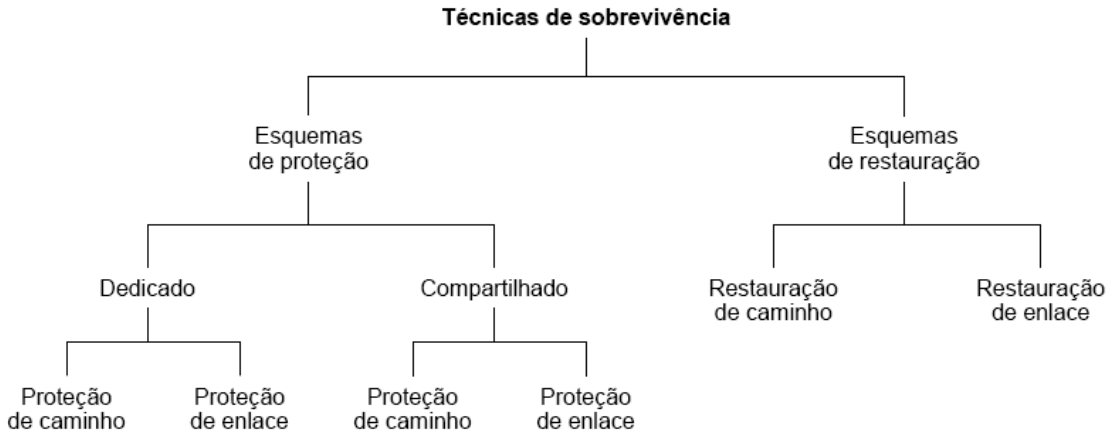


Figura 32 – Técnicas de sobrevivência [52] [53] [54] [55]

A proteção pode ser feita no nível de um caminho de luz individual ou no nível de uma simples fibra. A proteção de caminho está associada aos meios de proteção que visam restaurar a transmissão de dados por outro caminho de luz alternativo. A proteção de enlace se refere aos meios de proteção aplicados a uma fibra, que invariavelmente irá aplicar-se a todos os canais ou aos comprimentos de onda existentes nela [19]. A diferença aqui é que um caminho pode atravessar vários nós da rede, enquanto um enlace sempre liga dois nós [51]. A proteção de caminho procura uma rota alternativa para substituir uma rota com falha. A proteção do enlace procura restabelecer a conexão entre os dois nós afetados, que compartilham o enlace.

4.1.2. Caminhos de proteção e caminhos de trabalho

Caminhos de trabalho servem para transmitir o tráfego de dados sob o modo de operação normal da rede. Caminhos de proteção são uma alternativa para transmitir o tráfego de dados quando o modo de operação da rede está em estado de falha. Estes caminhos são disjuntos de modo que uma falha física não interrompa ambos.

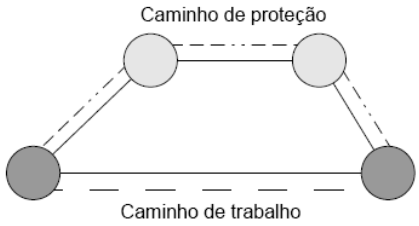


Figura 33 – Caminho de proteção e caminho de trabalho [50]

4.1.3. Proteção dedicada e proteção compartilhada

A proteção dedicada provê para cada caminho de trabalho um caminho de proteção dedicado, conforme exemplificado na Figura 34.

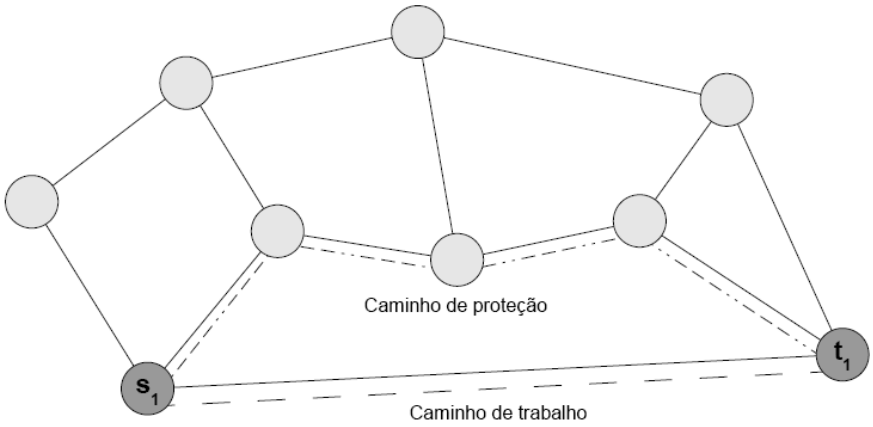


Figura 34 – Proteção dedicada [50]

Por sua vez, a proteção compartilhada provê para cada grupo de caminhos de trabalho um único caminho de proteção. Isso economiza recursos, mas somente um caminho de trabalho poderá falhar por vez.

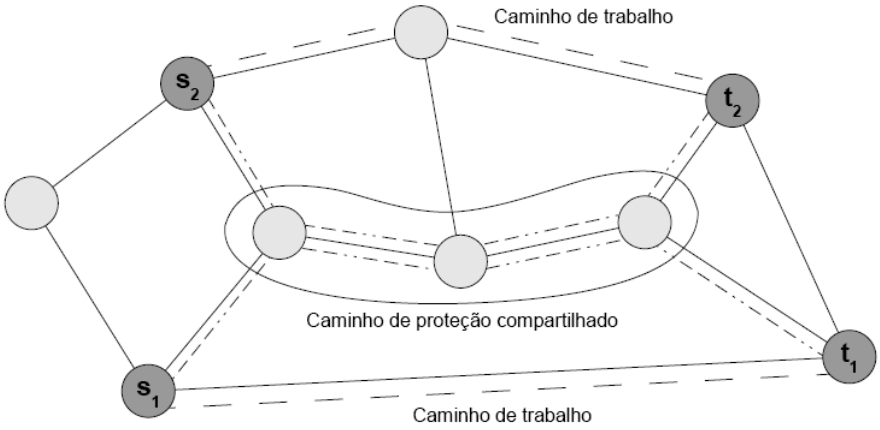


Figura 35 – Proteção compartilhada [50]

4.1.4. Proteção reversiva e não reversiva

A proteção reversiva faz com que o caminho do tráfego seja comutado novamente para o caminho restaurado após a ocorrência de uma falha. Em redes onde a proteção não é reversiva, a comutação para o caminho restaurado deve ser feita manualmente.

4.1.5. Chaveamento de proteção unidirecional e bidirecional

A proteção unidirecional é o esquema no qual, sob um evento de falha do enlace, apenas uma direção do tráfego é redirecionada, ficando a outra direção do tráfego operando na fibra original, conforme exemplificado na Figura 36(b). Nos esquemas de proteção bidirecional, ambos os sentidos são comutados para os enlaces de proteção, conforme exemplificado na Figura 36(c).

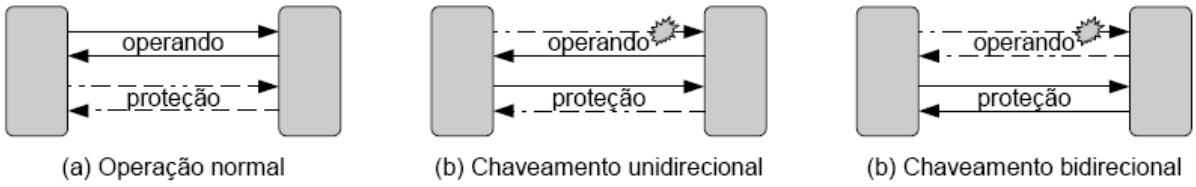


Figura 36 – Chaveamento de proteção unidirecional e bidirecional [50]

O chaveamento de proteção unidirecional é mais adequado para os esquemas de proteção dedicada, enquanto que o chaveamento de proteção bidirecional é mais adequado para os esquemas de proteção compartilhada [50].

4.1.6. Chaveamento de caminho, de enlace e de anel

O chaveamento de caminho faz com que uma nova rota seja criada usando-se um caminho alternativo, e é típico em redes do tipo malha. Já os chaveamentos de enlace e de anel são mais apropriados para redes em anel [50] [52] [56].

O chaveamento de enlace cria uma nova rota a partir de um enlace adjacente ao enlace com falha, conforme mostrado na Figura 37(b).

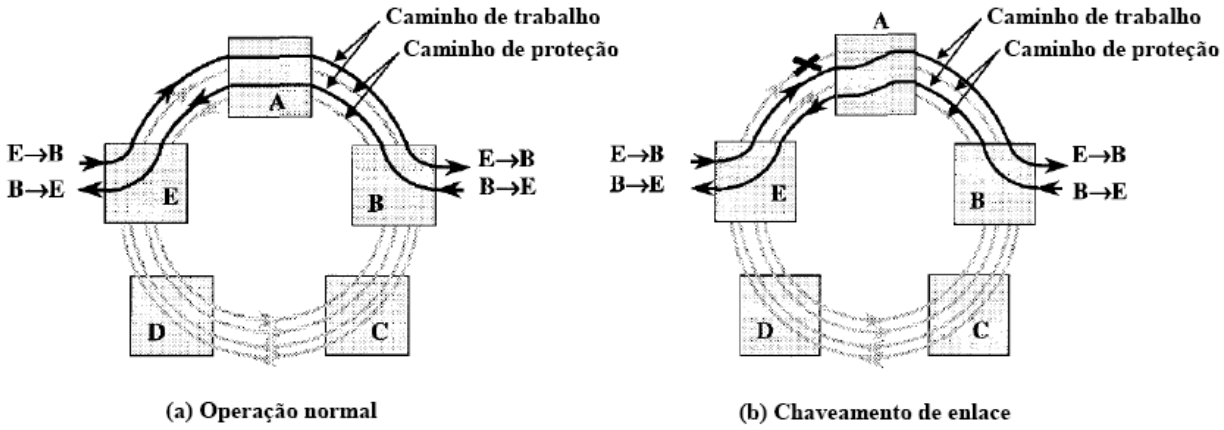


Figura 37 – Chaveamento de enlace [56]

Por sua vez, o chaveamento de anel cria uma nova rota a partir de um caminho ou enlace que percorre os nós adjacentes ao enlace com falha, conforme mostrado na Figura 38(b).

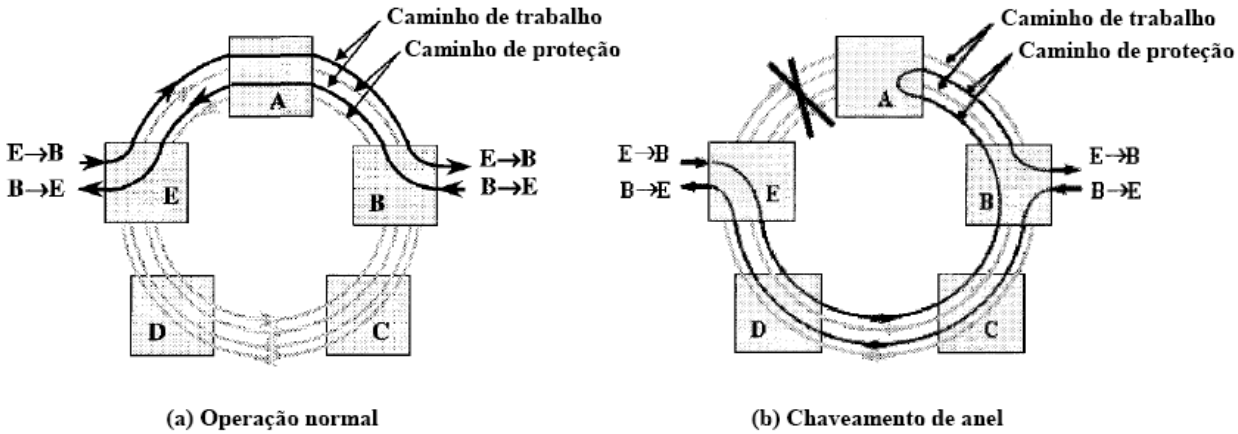


Figura 38 – Chaveamento de anel [56]

4.1.7. Proteção 1+1

Na proteção 1+1, o tráfego de dados é transmitido simultaneamente por duas fibras separadas desde a origem até o destino, e o destino se encarrega de selecionar uma das duas fibras para receber os dados baseado na qualidade do sinal. Se uma das fibras se romper, o destino simplesmente comuta da fibra com falha para a fibra operante. Este tipo de proteção é o mais rápido [19].

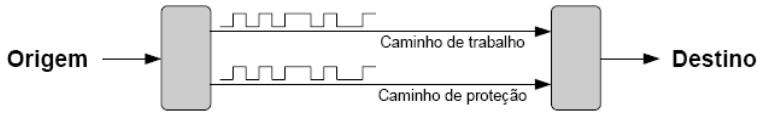


Figura 39 – Proteção 1+1 [50]

4.1.8. Proteção 1:1

A proteção 1:1 é semelhante à proteção 1+1, com a diferença de que a fibra de proteção só começará a transmitir quando a fibra primária falhar.

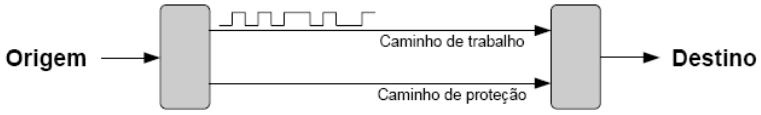


Figura 40 – Proteção 1:1 [50]

4.1.9. Proteção 1:N

A proteção 1:N é uma generalização da proteção 1:1, onde N fibras em operação compartilham N fibras de proteção.

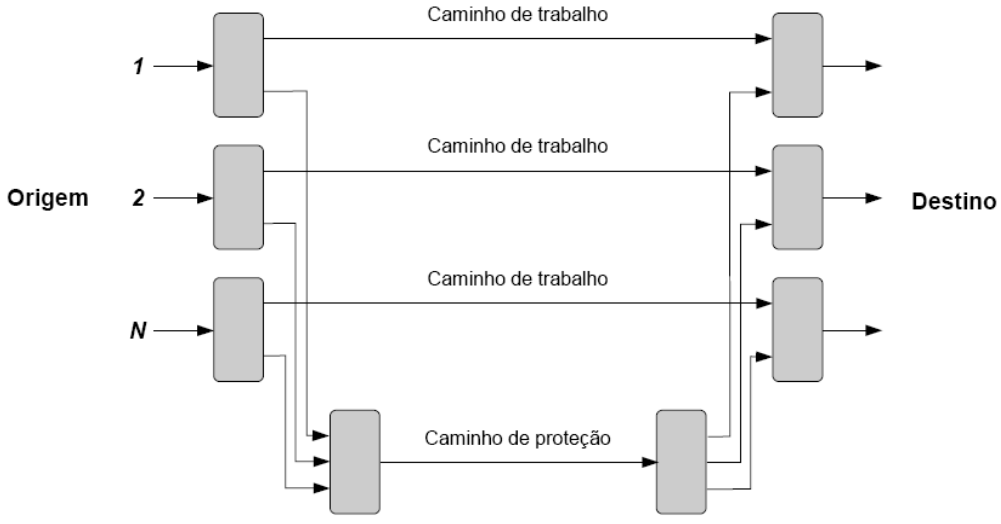


Figura 41 – Proteção 1:N [50]

4.2. Proteção e restauração de caminhos de dados

Na proteção de caminho, os recursos de proteção são reservados durante a configuração da conexão, enquanto que na restauração de caminho as rotas de proteção são descobertas dinamicamente após a falha. Quando um segmento da rede falha, o nó origem e o nó destino de cada caminho que atravessa o segmento são informados sobre a falha por meio de mensagens oriundas dos nós adjacentes ao segmento que falhou.

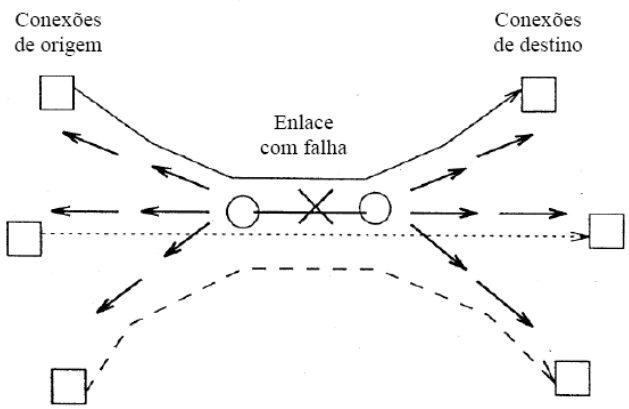


Figura 42 – Mensagens enviadas pelos nós adjacentes à falha para nós origem e destino [53]

4.2.1. Proteção de caminho dedicado

Na proteção de caminho dedicado, também chamada de proteção 1:1, os recursos destinados para proteção são exclusivos a uma única conexão (ou caminho) e não são compartilhados com nenhuma outra.

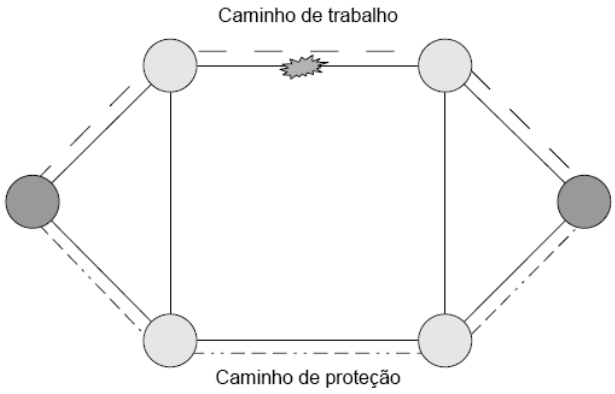


Figura 43 – Proteção de caminho [53]

4.2.2. Proteção de caminho compartilhado

Na proteção de caminho compartilhado, também chamada de proteção 1:N, os recursos destinados para proteção podem ser usados por diferentes conexões ou caminhos, mas é desejável que mais de uma conexão não falhe ao mesmo tempo, o que poderia acarretar uma indisponibilidade de recuperação da rede por falta de recursos de proteção disponíveis. A proteção de caminho compartilhado utiliza a capacidade de transmissão da rede de forma mais eficiente se comparada com a proteção de caminho dedicado.

4.2.3. Restauração de caminho

Na restauração de caminho, os nós origem e destino de cada conexão que atravessam um segmento da rede em falha utilizam-se de um algoritmo distribuído que descobre dinamicamente uma rota alternativa. Se não houver rotas alternativas disponíveis, então a conexão é encerrada.

4.3. Proteção e restauração de enlaces

Na proteção de enlace, os recursos de proteção ao redor do enlace são reservados durante a configuração da conexão, enquanto que na restauração de enlace os nós ao redor do enlace em falha procuram descobrir dinamicamente uma nova rota.

4.3.1. Proteção de enlace dedicado

Na proteção de enlace dedicado, para cada enlace é configurada uma rota de proteção com um comprimento de onda reservado em torno do enlace. Pode acontecer de não ser possível atribuir uma rota de proteção dedicada ao redor de cada elo da conexão primária e no mesmo comprimento de onda. Como em geral este método de proteção não usa de forma eficiente os comprimentos de onda disponíveis, a proteção de enlace dedicado é pouco utilizada [19].

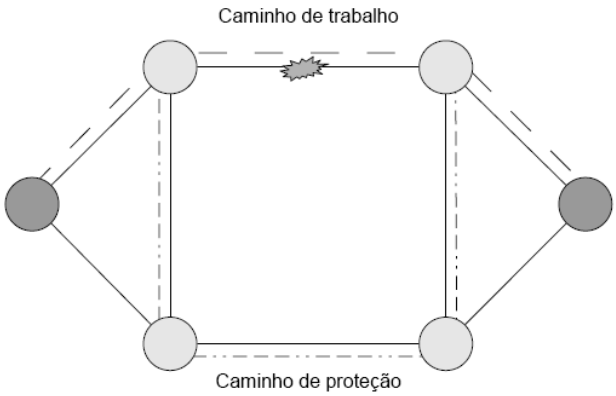


Figura 44 – Proteção de enlace [53]

4.3.2. Proteção de enlace compartilhado

Na proteção de enlace compartilhado, os recursos destinados para proteção podem ser usados por diferentes enlaces, mas é desejável que mais de um enlace não falhe ao mesmo tempo, o que poderia acarretar uma indisponibilidade de recuperação da rede por falta de recursos de proteção disponíveis. A proteção de enlace compartilhado utiliza a capacidade de transmissão da rede de forma mais eficiente se comparada com a proteção de enlace dedicado.

4.3.3. Restauração de enlace

Na restauração de enlace, os nós origem e destino de cada conexão que atravessam um enlace da rede em falha utilizam-se de um algoritmo distribuído que descobre dinamicamente uma rota alternativa ao redor do enlace. Se não houver rotas alternativas disponíveis, então a conexão é encerrada.

5. Modelagem da confiabilidade de rede

Para modelar a confiabilidade de uma rede ótica, partimos do princípio de que o estudo das falhas de cada componente ou elemento da rede individualmente não é suficiente para compreender e analisar o comportamento da rede como um todo. A falha de um nó ou a queda de um enlace de fibra ótica devem ser estudadas no contexto de uma rede dinâmica com comutação de circuitos ou de pacotes, de modo que nas últimas décadas muitos estudos nessa área foram concentrados na análise de múltiplas rotas aplicando Teoria dos Grafos. O trabalho recente de [10] apresenta importantes considerações acerca deste problema.

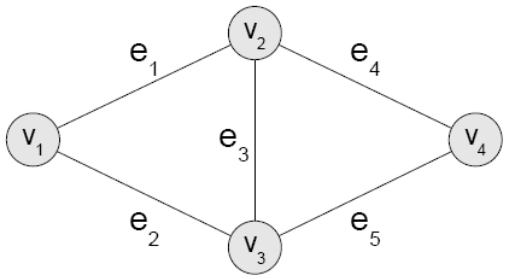


Figura 45 – Grafo de uma rede [57] [58]

De acordo com [10], para um grafo $G(V, E)$, onde V denota o conjunto de vértices (ou nós) e E o conjunto de enlaces, sendo k a quantidade de vértices com $k = |K|$, onde $|K|$ representa um subconjunto de vértices, a confiabilidade k-terminal $R(G_{(k)})$ será a probabilidade de que k vértices em $|K|$ estão conectados e em operação. A confiabilidade all-terminal $R(G_{(|V|)})$ será a probabilidade de que todos os vértices estão conectados e em operação, e a confiabilidade terminal-pair $R(G_{(2)})$ será a probabilidade de que um par de terminais esteja conectado e em operação.

O cálculo da confiabilidade de uma rede é um problema não-polinomial, o que faz com que o cálculo para redes com um grande número de nós seja computacionalmente inviável [10].

Para simplificar o cálculo, muitos artigos na literatura consideravam os nós como perfeitos, uma vez que a maioria das falhas ocorre nos enlaces de fibra ótica. Desta forma muitas soluções e algoritmos foram desenvolvidos, tanto numericamente quanto algebricamente [57] [59] [60].

No entanto, mesmo que as falhas nos enlaces de fibra ótica sejam mais comuns, as falhas nos nós — que incluem uma série de equipamentos de conversão, amplificação e outros — também são responsáveis pela indisponibilidade de serviços, de forma que outros artigos na literatura consideraram as falhas dos nós no cálculo da confiabilidade das redes [10] [58] [61].

Para uma dada rede, qualquer caminho ou enlace adicional faz com que o cálculo da confiabilidade cresça fatorialmente, e seja muito difícil de ser executado mesmo em supercomputadores.

Se considerarmos o modelo de rede da figura abaixo, poderemos modelar uma rede simples onde o nó de origem (*s*) e o nó de destino (*t*) são colocados nos vértice v_1 e v_4. Os enlaces são representados por setas que vão de (*s*) até (*t*). O enlace e_3 é bidirecional, já que os dados podem caminhar em ambas as direções.

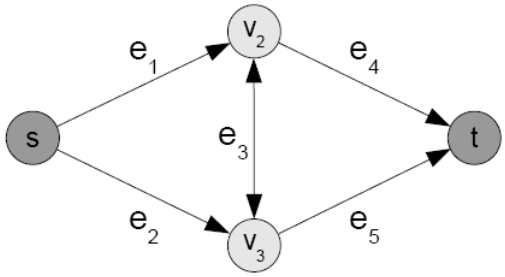


Figura 46 – Grafo direcionado de uma rede [57] [58]

A Figura 47 representa uma parte da árvore de eventos da rede quando dados são transferidos da origem (*s*) para o destino (*t*). As caixas de linhas sólidas representam as conexões com sucesso e as caixas com linhas tracejadas as conexões que falharam. A barra sobre o elemento (nó ou enlace) significa que este elemento não está funcionando, ou seja, está num estado de falha.

A primeira caixa sólida nos mostra que se os enlaces e_1 e e_4 e o nó v_1 estiverem funcionando corretamente, a transferência de dados da origem (*s*) para o destino (*t*) será realizada com sucesso. No primeiro nível, se considerarmos que todos os elementos estão funcionando corretamente, teremos quatro caminhos possíveis para a transferência de dados. Devido à simetria da rede, iremos decompor apenas uma de suas ramificações.

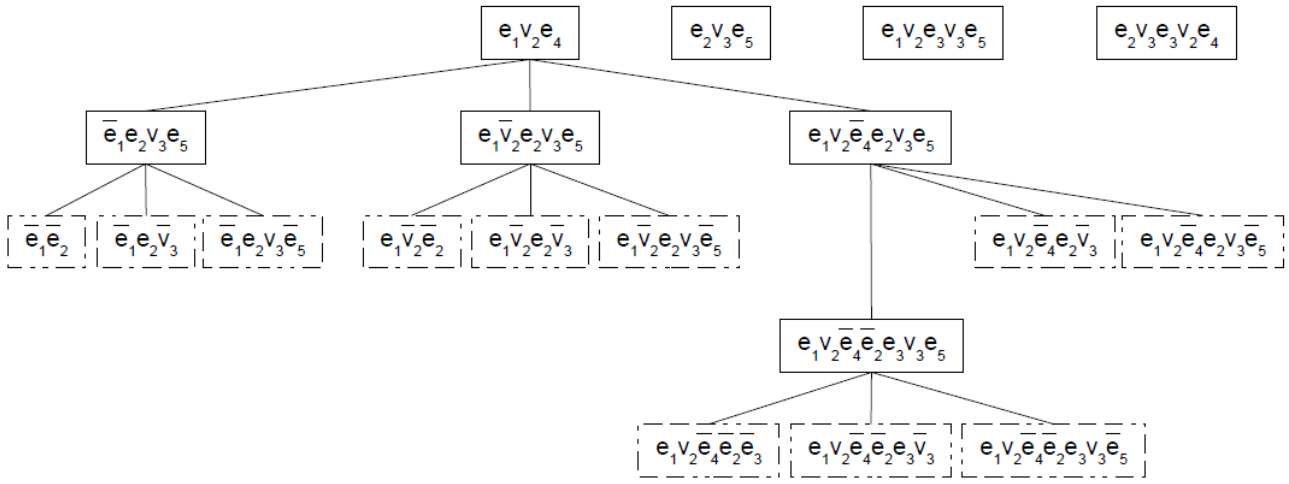


Figura 47 – Árvore de eventos de confiabilidade [58]

A expressão simbólica para a confiabilidade de cada par pode ser obtida a partir dos eventos com sucesso. Assim, R_1 representa a confiabilidade da primeira ramificação, e e_i e v_j representam a confiabilidade do enlace i e do nó j, onde teremos:

$$\begin{aligned} R_1 = {} & (e_1 \times v_1 \times e_4) + (\bar{e}_1 \times e_2 \times v_3 \times e_5) + (e_1 \times \bar{v}_1 \times e_2 \times v_3 \times e_5) + \\ & + (e_1 \times v_1 \times \bar{e}_4 \times e_2 \times v_3 \times e_5) + (e_1 \times v_1 \times \bar{e}_4 \times \bar{e}_2 \times e_3 \times v_3 \times e_5) \end{aligned} \tag{32}$$

Onde $\bar{e}_i$ representa a não confiabilidade de e_i, ou seja, $\bar{e}_i = 1 - e_i$.

Aplicando este mesmo raciocínio para todos os outros ramos, a confiabilidade de cada par poderá ser obtida a partir de:

$$R = s \times (R_1 + R_2 + R_3 + R_4) \times t \tag{33}$$

A partir do tamanho das expressões para esta rede extremamente simples, podemos verificar como este problema, que é basicamente um problema combinatório, poderá crescer fatorialmente (n!) ao invés de exponencialmente, à medida que enlaces adicionais são acrescentados. Para contornar este problema, várias técnicas foram desenvolvidas.

5.1. Simplificando a complexidade da rede

Apresentamos a seguir três métodos que podem ser usados para simplificar a complexidade da rede e permitir o cálculo da confiabilidade mesmo para redes grandes.

5.1.1. Redução em série e em paralelo

A idéia básica desta abordagem é reduzir a topologia da rede resolvendo a confiabilidade em série e em paralelo da rede, já apresentados no item 3.4 deste trabalho. Consideremos as seguintes expressões de confiabilidade:

- Conexão em série de elementos $A + B : R_{A+B} = R_A \times R_B$
- Conexão em paralelo de elementos $A \parallel B : R_{A\parallel B} = R_A + R_B - R_A \times R_B$

A figura abaixo apresenta um exemplo onde a técnica de redução é demonstrada [21]:

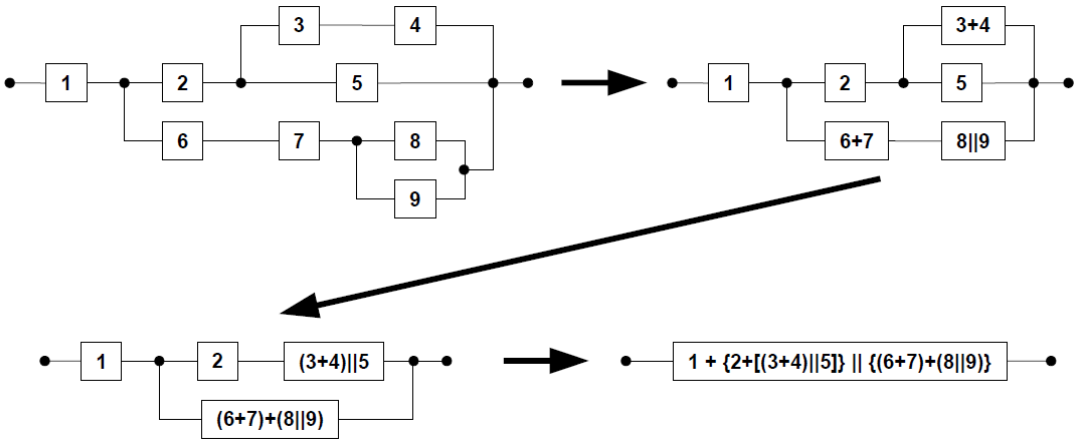


Figura 48 – Redução em série e em paralelo [21]

No entanto, algumas topologias como a da Figura 49 não podem ser facilmente reduzidas, sendo necessária a aplicação de outras técnicas.

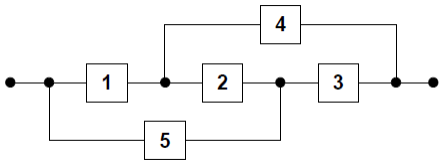


Figura 49 – Topologia de rede que não pode ser facilmente reduzida [21]

5.1.2. Simplificação triângulo-estrela

A simplificação triângulo-estrela consiste em converter uma configuração de três nós que estejam conectados na forma de triângulo para uma configuração equivalente no formato de estrela [62] [63] [64].

Como se pode ver na Figura 50(a), os nós *abc* formam um triângulo, que pode ser convertido para uma estrela conforme mostrado na Figura 50(b). No entanto, notemos que um quarto elemento aparece na rede, o nó *u.*

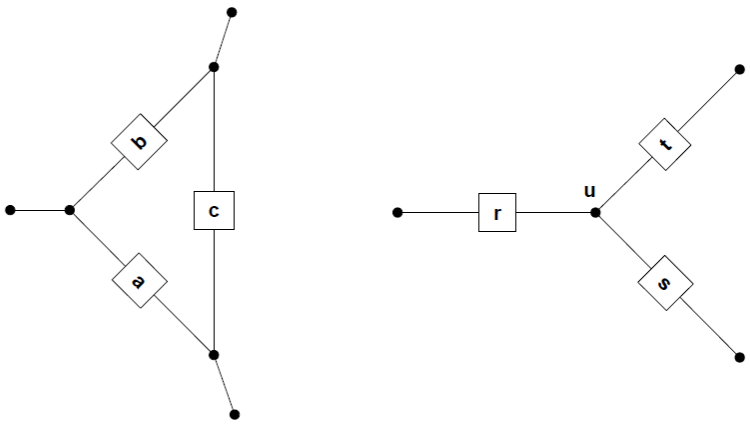


Figura 50 – Simplificação triângulo-estrela [62] [63] [64]

Assim, a confiabilidade dos nós *abc* será equivalente a confiabilidade dos nós *rstu*, que é dada pelas seguintes equações:

$$\alpha = a + b + c - ab - ac - cc + abc \tag{34}$$

$$\delta = c + ab - abc \tag{35}$$

$$\gamma = b + ac - abc \tag{36}$$

$$\beta = a + bc - abc \tag{37}$$

$$r = \frac{\alpha}{\delta},\ s = \frac{\alpha}{\gamma},\ t = \frac{\alpha}{\beta},\ u = \frac{\delta\gamma\beta}{\alpha^2} \tag{38}$$

5.1.3. Cut-graph

A técnica *cut-graph* consiste em dividir uma rede grande em redes menores onde a solução para o cálculo da confiabilidade seja conhecida para cada uma destas redes menores. O grande problema aqui é como selecionar o conjunto de nós e enlaces que serão abstraídos como sendo um enlace único.

A figura abaixo mostra dois nós onde a rede intermediária foi abstraída para um enlace simples. Neste caso, é possível avaliar a confiabilidade e a disponibilidade da rede a partir de parâmetros conhecidos da sub-rede abstraída.

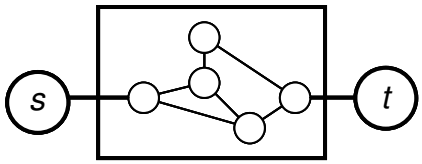


Figura 51 – Abstração de enlace simples

Porém, no mundo real, um nó nem sempre é um nó terminal ou possui uma conexão simples. Como exemplificado na figura a seguir, não é possível analisar a confiabilidade $R(t)$ sem avaliar a outra rede subjacente.

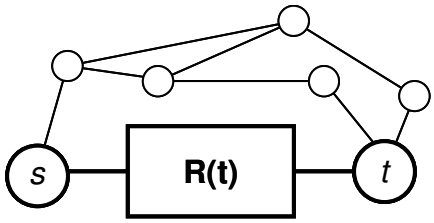


Figura 52 – Conexão "externa"

5.2. Aplicando diagramas de decisão binária

Em [10] foi desenvolvida uma solução de modelagem da confiabilidade usando funções com ROBDD (*Reduced Ordered Binary Decision Diagrams*), onde foram propostos dois algoritmos: EE (*Entangled Expansion*) e CAE (*Composition after Expansion*). O algoritmo EE é um método de decomposição recursiva da rede, que é similar mas diferente da operação de contração do teorema de fatoração. Já o algoritmo CAE se beneficia do método de substituição do *link* incidente [59]. Mas para isso, necessita que as variáveis do BDD sejam ordenadas. Em muitos trabalhos, apesar de os autores se referirem ao uso de diagramas de decisão binária simplesmente como BDD, muitas vezes eles estarão se referindo aos diagramas com variáveis ordenadas, chamados de BDD ordenado ou OBDD [11].

Considerando que os nós também podem falhar, o método de substituição do *link* incidente é o método mais comumente usado para calcular a confiabilidade nestes casos. Consiste em considerar os *links* adjacentes ao nó com falha como se também estivessem em estado de falha [59]. Este método será usado por [10] em conjunto com BDD para o cálculo da confiabilidade considerando que os nós também podem falhar.

Em seu trabalho, [11] demonstra como implementar BDD computacionalmente usando um pacote baseado em software livre chamado CUDD – Colorado University Decision Diagram. O pacote CUDD, escrito em C++, provê funções para manipular BDD e suas variantes, como ADD (*Algebric Decision Diagram*) e ZDD (*Zero-suppressed Binary Decision Diagram*). BDD é usado para representar funções de chaveamento; ADD é usado para representar funções para um conjunto de dados arbitrário, e ZDD é usado para representar funções de chaveamento assim como o BDD, mas com a vantagem de ser mais eficiente quando o conjunto de dados está no formato de cubo [65].

5.2.1. Diagramas de decisão binária

Diagramas de Decisão Binária ou BDD (*Binary Decision Diagram*) são uma estrutura de dados que representam funções booleanas em um gráfico acíclico. Os BDDs foram originalmente concebidos por C.Y. Lee em 1959 [66] e posteriormente aprimorados por Akers em 1978 [67].

De acordo com [68], por definição, um BDD de uma função booleana $f:\{0,1\}^n \rightarrow \{0,1\}$ é um grafo acíclico direcionado DAG (*Directed Acyclic Graph*) e enraizado, com dois tipos de vértices: terminais e não terminais. Cada vértice terminal v tem como atributo um valor valor(v) $\in \{0,1\}$. Dos vértices não terminais v saem dois arcos para dois vértices-filhos, zero(v) e um(v). Cada vértice v não-terminal é rotulado pelo índice de uma variável booleana, índice(v) $\in \{1, 2, \ldots, n\}$.

O BDD é um conjunto de funções decompostas disjuntas, que nada mais é que a decomposição de funções booleanas, também conhecido como expansão de Shannon. Assim, um BDD pode ser reconhecido como um conjunto de produtos disjuntos baseado em grafo [12]. A representação do BDD também pode ser explicada usando o conectivo *IF-Then-Else* (ITE), onde x é a variável de decisão booleana [10] [12]:

$$f = (x \wedge f_{x=1}) \vee (\bar{x} \wedge f_{x=0}) = ite(x, f_{x=1}, f_{x=0}) \tag{39}$$

Tomemos um exemplo mais simples, considerando a seguinte expressão [67]:

$$f = A \vee \bar{B}C \tag{40}$$

Neste exemplo, conforme diagrama da Figura 53, para determinar o valor binário de f, basta olhar o valor de A. Se A=1, então f=1. Se A=0, deveremos então olhar para B. Se B=1, então f=0. Mas se B=0, então f será igual ao valor de C.

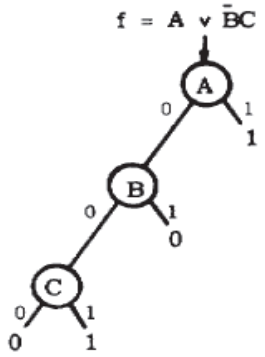


Figura 53 – Diagrama para $f = A \vee \overline{B}C$

Outro detalhe importante na construção de BDD é a ordenação das variáveis, pois dela dependem o tamanho do BDD e a complexidade de sua manipulação [9]. Diferentes funções terão diferentes níveis de sensibilidade de ordenação [11].

Para exemplificar, dada uma função:

$$f = (a_1 \wedge b_1) \vee (a_2 \wedge b_2) \vee (a_3 \wedge b_3) \tag{41}$$

É possível ter dois gráficos distintos, mudando-se apenas a ordem de ordenação das variáveis:

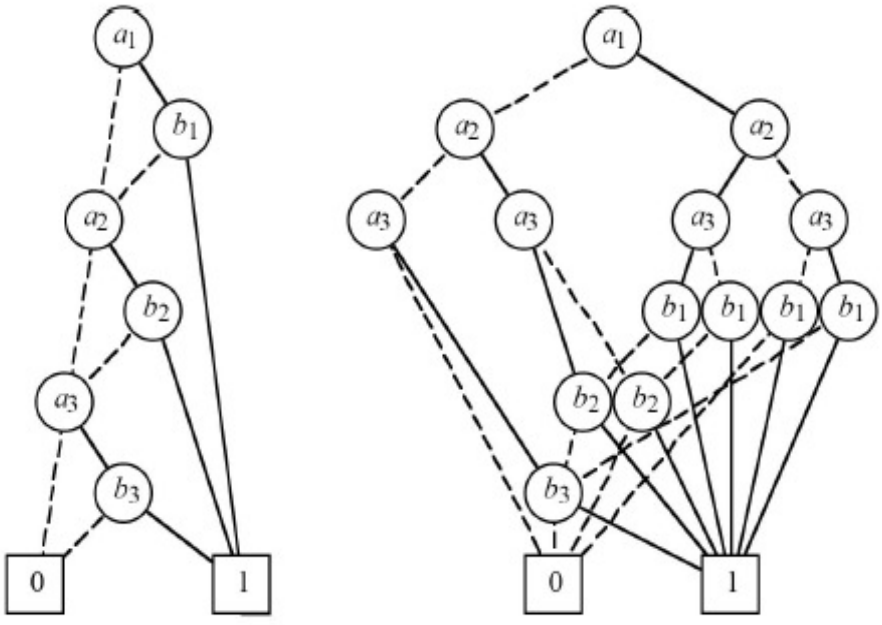


Figura 54 – Efeito da ordenação da variável no tamanho do diagrama [69]

5.2.2. Exemplo de aplicação

Dada uma função booleana $f = x_1 \wedge x_2 \vee x_3$, podemos aplicar a expansão de Shannon como demonstrado abaixo:

$$f = x_1 \wedge x_2 \vee x_3$$

$$\begin{aligned} f_{(x_1=1)} &= x_2 \vee x_3 \\ f_{(x_1=0)} &= x_3 \end{aligned} \tag{42}$$

$$\therefore f = x_1(x_2 \vee x_3) \vee x_1'(x_3)$$

Assim que é aplicada a expansão de Shannon para x_1, continua-se a expandir as funções, agora para g_1 e g_2:

$$g_1 = x_2 \vee x_3$$

$$\begin{aligned} g_{1(x_2=1)} &= 1 \\ g_{1(x_2=0)} &= x_3 \end{aligned} \tag{43}$$

$$\therefore g_1 = x_2(1) \vee x_2'(x_3)$$

$$g_2 = x_3$$

$$\begin{aligned} g_{2(x_3=1)} &= 1 \\ g_{2(x_3=0)} &= 0 \end{aligned} \tag{44}$$

$$\therefore g_2 = x_3(1) \vee x_3'(0)$$

Uma vez finalizada as expansões, podemos então construir o diagrama de decisão binária, e simplificá-la, quando for o caso:

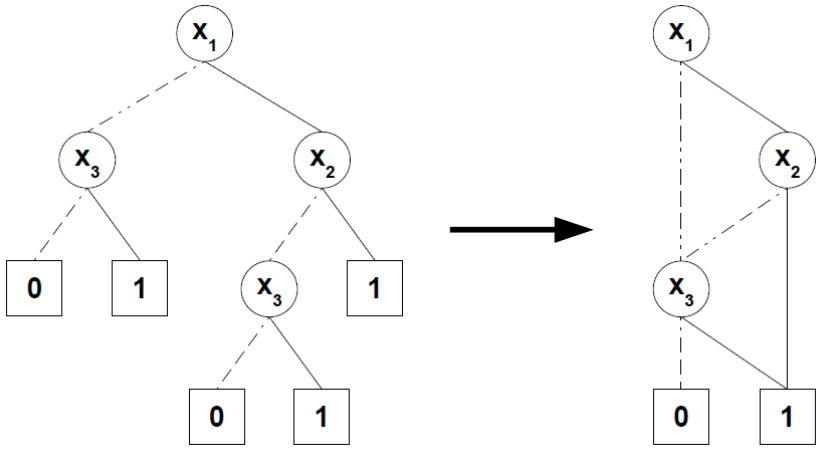


Figura 55 – Simplificação de uma árvore de decisão binária

6. Rede KyaTera

O KyaTera nasceu com a missão de reunir as competências e recursos laboratoriais necessários para desenvolver ciência, tecnologias e aplicações da Internet do futuro.

Construída para a pesquisa, esta rede conta com mais de 600 pesquisadores do estado de São Paulo em diversas áreas do conhecimento, que estão trabalhando interligados por uma rede ótica de alta capacidade para usá-la como plataforma de testes de tecnologias [4].

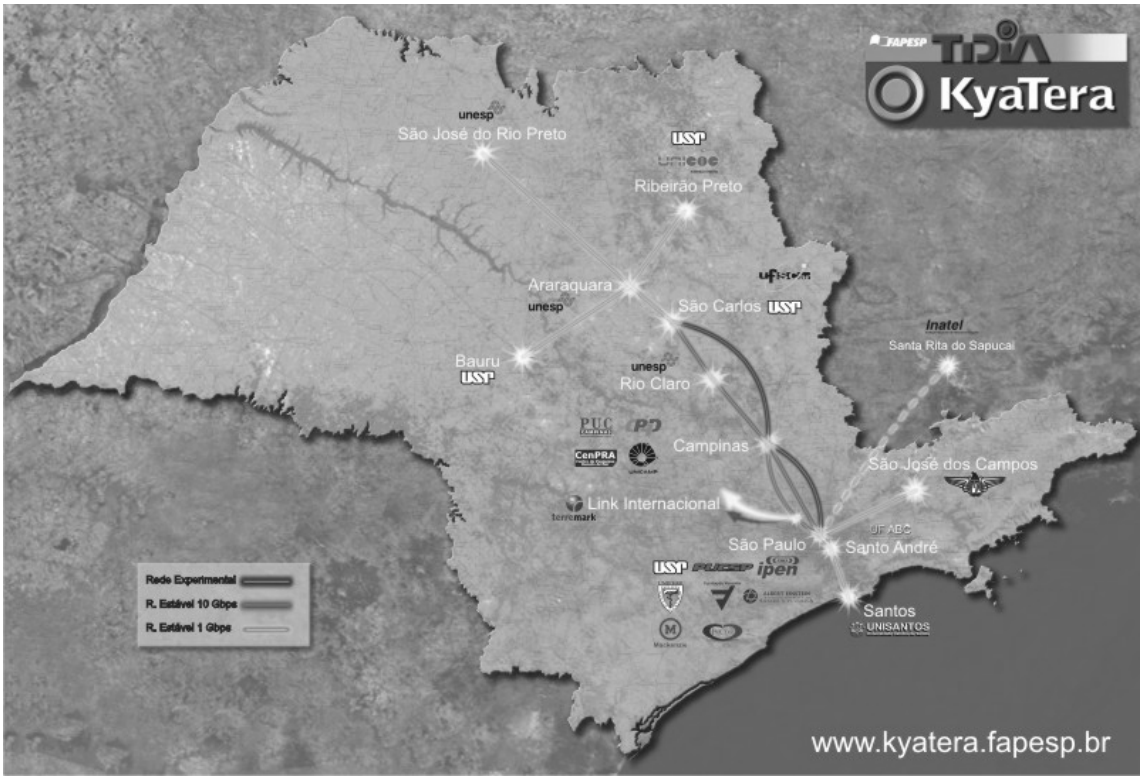


Figura 56 – Rede KyaTera no estado de São Paulo [4]

O KyaTera conecta diversas instituições acadêmicas e empresas através da sua rede ótica dedicada, formando um ambiente de trabalho colaborativo à distância para a geração de conhecimento e inovações tecnológicas. Ela possui duas redes: a experimental e a estável. A primeira é usada para pesquisas que envolvem as camadas física e de rede. A segunda é usada para pesquisas que envolvem aplicações de Internet avançadas [4].

6.1. Rede experimental

A rede experimental interliga os laboratórios da Rede KyaTera que desejam realizar experimentos colaborativos e distribuídos de transmissão ótica e de redes sob condições reais. Esta rede oferece uma quantidade variável de fibras apagadas do tipo monomodo e multimodo, e a máxima taxa de transmissão já alcançada foi de 320 Gbps [4].

Nessa rede são realizados os experimentos da camada física e da camada de redes. Na camada física os pesquisadores estudam a transmissão física em fibra ótica. Tendo acesso direto às fibras óticas apagadas, eles podem instalar e configurar todo o equipamento necessário. Exemplos de temas de pesquisa: sistemas de transmissão de alta capacidade por fibra ótica, sistemas DWDM, amplificadores óticos, dispositivos para redes fotônicas, entre outros.

Já na camada de redes os pesquisadores estudam a melhoria do transporte da informação que percorre a infra-estrutura de fibras óticas do projeto. São desenvolvidas pesquisas em assuntos como: redes óticas, redes de computadores, protocolos, segurança, baixa latência, padrões de interface e interoperabilidade em comunicações óticas. Os pesquisadores desta camada também são responsáveis pela Rede Estável.

6.2. Rede estável

A rede estável do KyaTera interliga todos os laboratórios associados ao projeto através de uma malha ótica de fibras SM (*Single Mode Fiber*) dedicada, usando a tecnologia de transmissão DWDM. A principal função da rede estável é oferecer serviços para promover a pesquisa colaborativa entre os participantes do projeto, como por exemplo, acesso à videoconferência de alta definição, laboratórios virtuais (WebLabs), VoIP, Internet2, etc. A rede estável oferece, para cada laboratório, uma taxa de transmissão mínima de 1 Gbps, através de um *backbone* de 10 Gbps que interconecta os três grandes centros concentradores da rede, localizados nas cidades de São Paulo (USP), Campinas (UNICAMP) e São Carlos (USP São Carlos).

Os pesquisadores desta rede trabalham em aplicações de Internet avançada pensadas para promover a pesquisa colaborativa, como os WebLabs (laboratórios disponíveis na Web para controle e monitoramento) e a videoconferência de alta definição. Eles desenvolvem *software* e *hardware* para o

controle de instrumentos através da Internet e para integração de mídias avançadas de alta resolução. Para eles, a rede ótica não é objeto de estudo; ela é um meio de transporte para grandes quantidades de dados.

A topologia da rede estável do KyaTera não obedece a uma topologia específica do ponto de vista físico, mas do ponto de vista lógico foi adotada a topologia em estrela, pois é a mais apropriada para a interconexão dos laboratórios que geralmente estão concentrados dentro dos campi universitários [4].

Já para interligar fisicamente os diferentes campi, foi adotada a configuração apropriada a cada caso. É por este motivo que são encontrados enlaces ponto-a-ponto, anel metropolitano e estrela (dentro dos campi). Esta combinação de topologias também é conhecida com *Mesh (*malha) ou *Mixed* (mista), dependendo da literatura consultada.

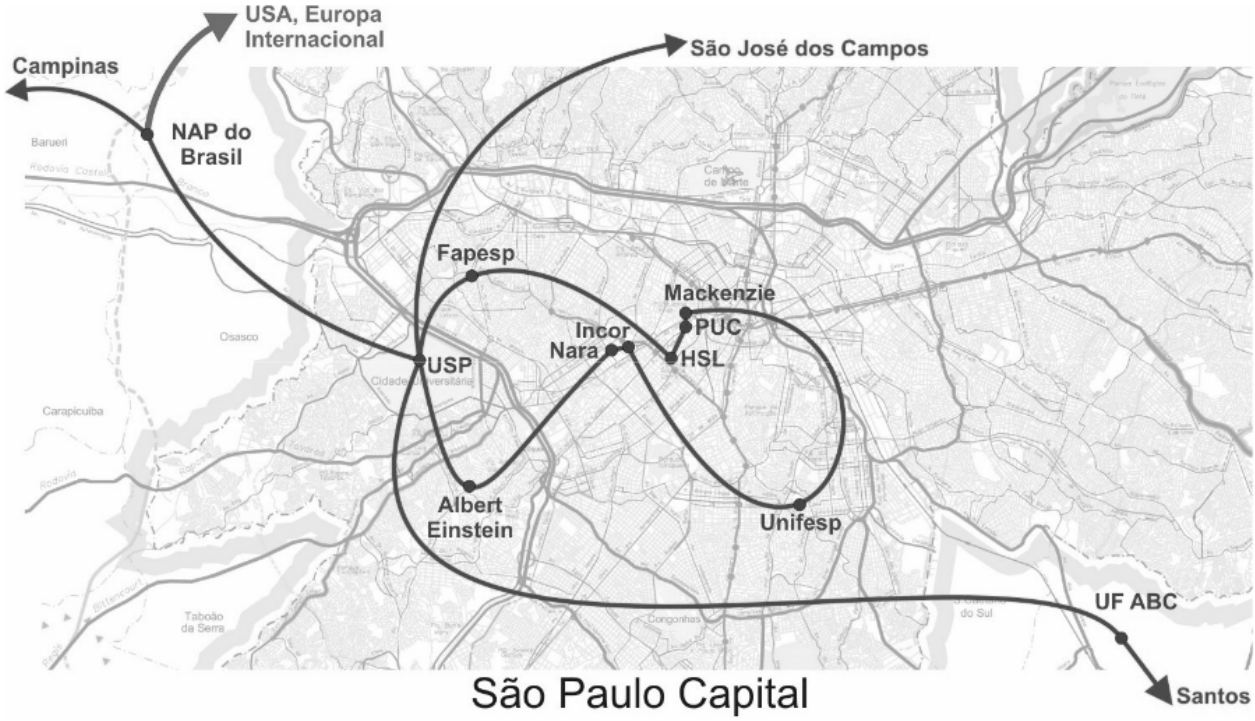


Figura 57 – Rede KyaTera na região metropolitana de São Paulo [4]

O planejamento e a manutenção da rede estável estão a cargo da equipe do NARA (Núcleo de Apoio à Rede Acadêmica).

6.3. Anel ótico metropolitano

O anel ótico metropolitano do KyaTera é responsável por interligar os diversos centros de pesquisa da cidade de São Paulo, incluindo hospitais, universidades e empresas privadas. Dentre os projetos que rodam sobre a plataforma do KyaTera, podemos destacar o WebLab para um Banco Abrangente de Imagens Médicas, coordenado por pesquisadores do INCOR, que tem por objetivo criar uma base de imagens para poder ser usada no desenvolvimento, teste e avaliação de novos *softwares* para radiologia. Adicionalmente, seu uso pode ser igualmente importante para agências governamentais que certificam equipamentos e produtos médicos. E esta base também pode ser usada em conjunto com outras informações clínicas, como uma fonte de materiais para treinamento de novos radiologistas ou para educação continuada [4].

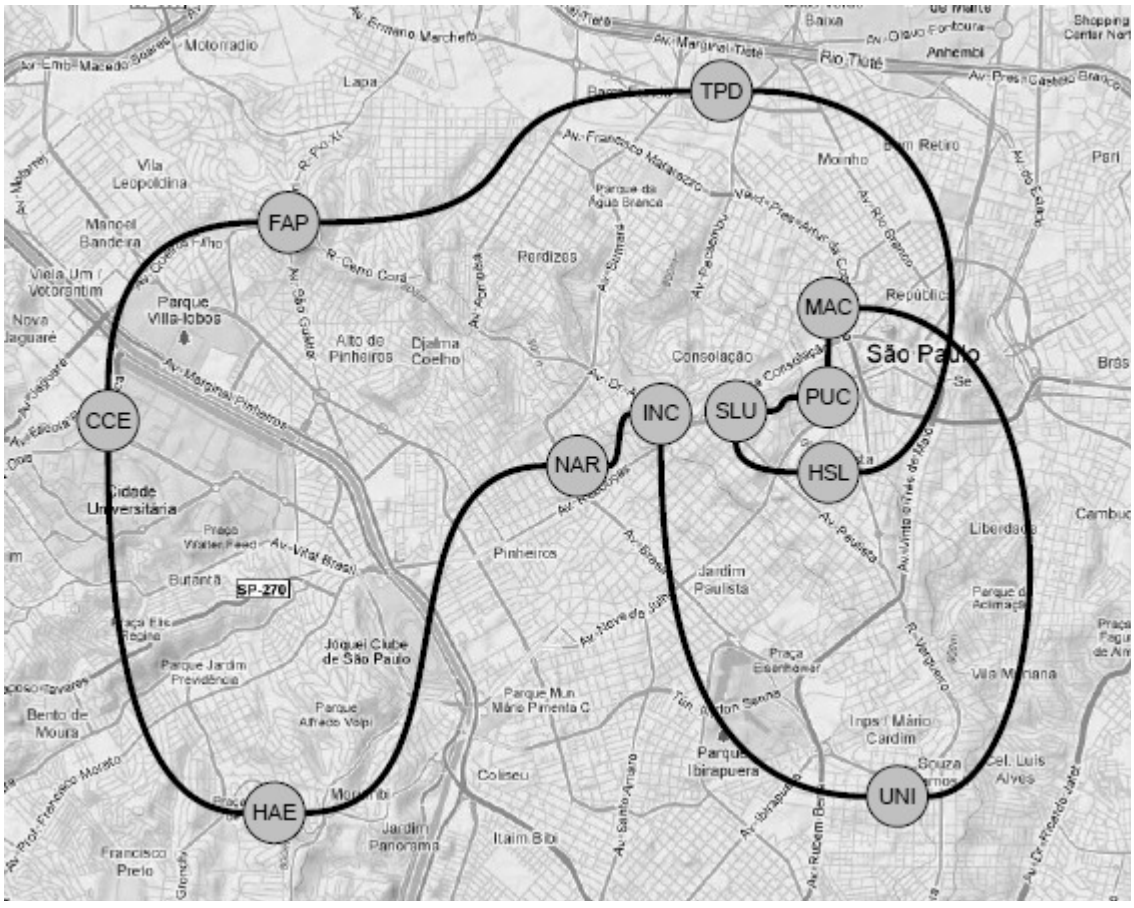


Figura 58 – Mapa do anel da Rede KyaTera em escala aproximada [4]

O anel ótico metropolitano possui 118,5 km de comprimento, e interliga onze centros de pesquisa. A figura acima ilustra a disposição geográfica aproximada dos nós da rede. Os enlaces são formados por dutos e caixas de passagens (não mostradas na figura) enterradas ao longo de ruas e

avenidas. Na figura abaixo, é mostrado um mapa esquemático para fins da análise de confiabilidade da rede.

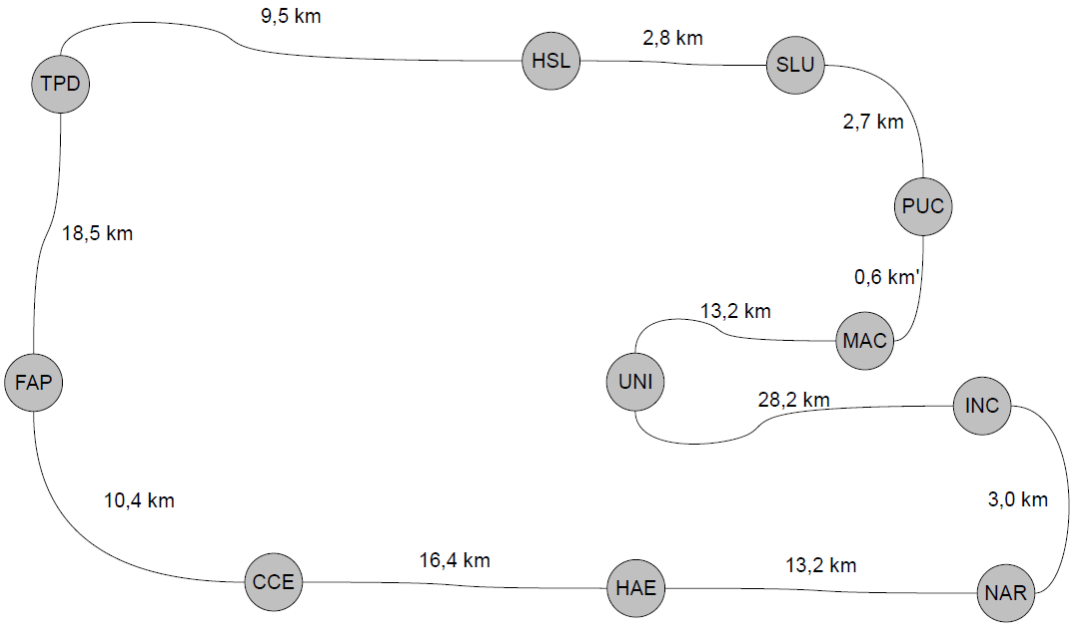


Figura 59 – Mapa esquemático do anel da Rede KyaTera sem escala [4]

Na tabela a seguir, estão as siglas e os nomes dos centros de pesquisa:

Tabela 7 – Nós do anel ótico KyaTera [4]

Sigla do Nó	*Descrição do nó*
TPD	Laboratório da Telefônica Pesquisa e Desenvolvimento – TPD
HSL	Hospital Sírio Libanês
SLU	SLU (*Sub-loop Unbundling*) da Telefônica Pesquisa e Desenvolvimento - TPD
PUC	Pontifícia Universidade Católica – PUC
MAC	Universidade Presbiteriana Mackenzie
UNI	Universidade Federal de São Paulo – UNIFESP
INC	Instituto do Coração – INCOR
NAR	Núcleo de Apoio à Rede Acadêmica – NARA
HAE	Hospital Albert Einstein
CCE	Centro de Computação Eletrônica da Universidade de São Paulo – CCE/USP
FAP	Fundação de Amparo à Pesquisa do Estado de São Paulo - FAPESP

Na tabela acima, o termo *unbundling* (fragmentar, separar) é utilizado para descrever o acesso oferecido por operadoras de serviço telefônico local de modo que outros provedores de serviço possam

comprar ou alugar porções de seus elementos de rede para prover serviço a assinantes. É o chamado compartilhamento da última milha das redes telefônicas [70].

7. Modelando e avaliando a confiabilidade e a disponibilidade da rede KyaTera

Calcular a confiabilidade *R* e a disponibilidade *A* da rede KyaTera é um problema do tipo NP completo, o que dificulta sobremaneira a sua resolução mesmo em termos computacionais.

Para efeitos de cálculo da confiabilidade e disponibilidade, consideram-se três tipos de situação [9] [10]:

1. Confiabilidade e disponibilidade entre k terminais (ou nós);
2. Confiabilidade e disponibilidade entre todos os terminais (ou nós);
3. Confiabilidade e disponibilidade entre um par de terminais (ou nós).

Neste estudo iremos considerar o cálculo da confiabilidade e da disponibilidade para um par de terminais sujeitos a falhas de nó simples e falhas de *link* simples. Tomaremos como exemplo o cálculo entre os terminais A (Telefônica Pesquisa e Desenvolvimento) e G (Instituto do Coração). O comprimento total do anel é de 118,5 km, sendo que o comprimento no sentido AG é de 57 km e no sentido GA é 61,5 de km.

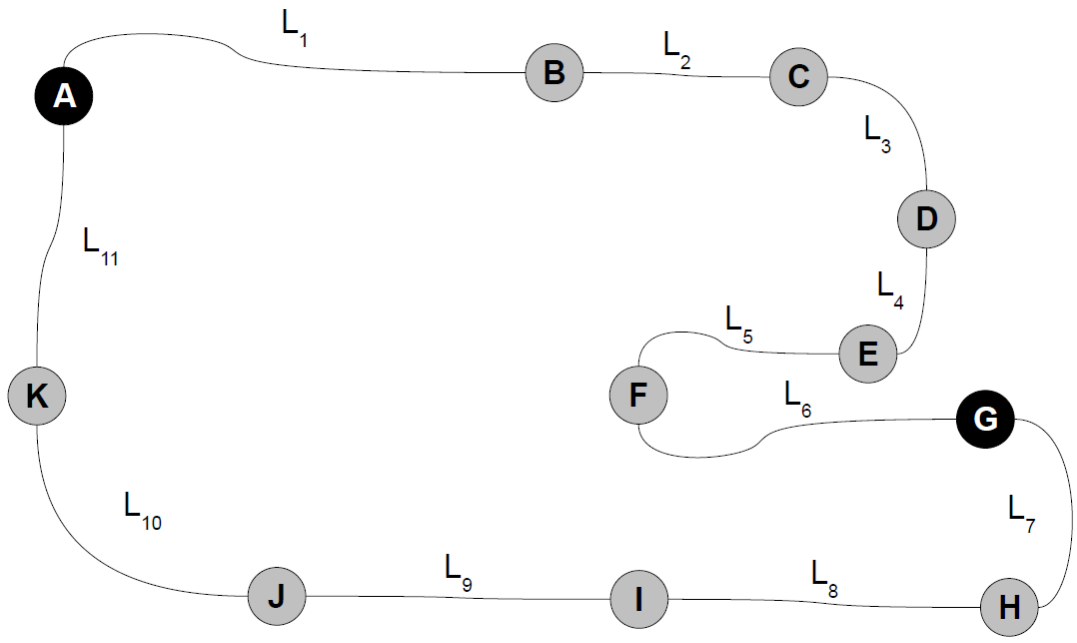


Figura 60 – Mapa esquemático do anel ótico para cálculo da confiabilidade e disponibilidade

7.1. Confiabilidade e disponibilidade do nó

Cada nó do anel metropolitano da rede KyaTera é formado tipicamente por um multiplexador/demultiplexador e por um amplificador do tipo EDFA.

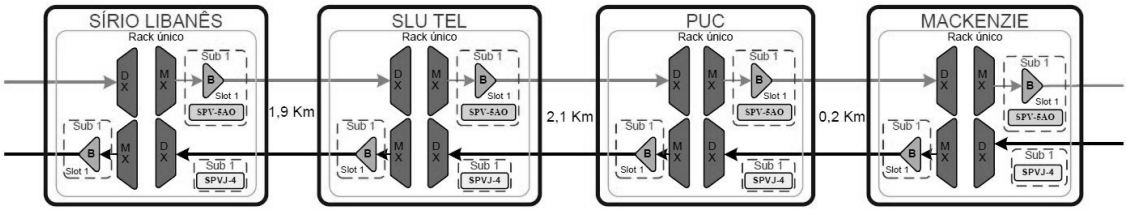


Figura 61 – Detalhe da interligação entre os nós do KyaTera [4]

Além destes componentes, cada nó possui um supervisor dos amplificadores (SPV-5AO) e um supervisor dos *transponders* (SPVJ-4), responsáveis pelo gerenciamento remoto dos elementos do nó.

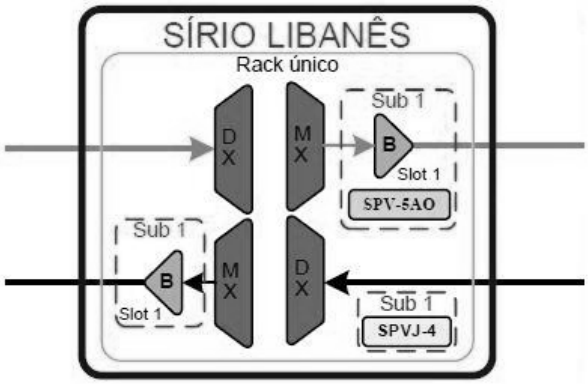


Figura 62 – Detalhe de um nó do KyaTera [4]

Ao contrário do que a figura acima possa sugerir, a configuração é em série entre todos os elementos. Assim, a confiabilidade e a disponibilidade do nó serão dadas pela configuração abaixo:

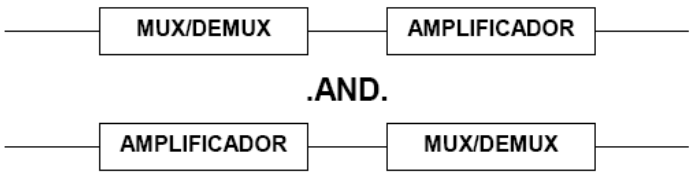


Figura 63 – Configuração da confiabilidade e disponibilidade do nó

Como não tivemos acesso ao modelo dos equipamentos que compõem o nó, usaremos as especificações de equipamentos similares no mercado. Para o multiplexador/demultiplexador, temos os dados do SmartOptics Mux/Demux T-3004 [36], e para o amplificador, os dados do Shenzhen Greatway Technology GWA3530 Fiber Amplifier [37].

Tabela 8 – Dados para cálculo da confiabilidade e da disponibilidade do nó [36] [37]

Equipamento	*MTTF (horas)*	*FIT*	*MTTR (horas)*
SmartOptics Mux/Demux T-3004	4.383.000	228	2
Shenzhen Greatway Technology GWA3530 Fiber Amplifier	150.000	6.667	2

7.1.1. Cálculo da confiabilidade do nó

A confiabilidade do nó será dada pela expressão:

$$R_{NÓ} = R_{MUX\,/\,DEMUX}{}^{2} \times R_{AMPLIFICADOR}{}^{2}$$

Como

$$R = 1 - \frac{1}{MTTF} = 1 - \lambda$$

Então

$$R_{NÓ} = (1 - \lambda_{MUX\,/\,DEMUX})^2 \times (1 - \lambda_{AMPLIFICADOR})^2$$

Substituindo os valores, teremos que:

$$R_{NÓ} = 99{,}9986\%$$

7.1.2. Cálculo da disponibilidade do nó

A disponibilidade do nó será dada pela expressão:

$$A_{NÓ} = A_{MUX\,/\,DEMUX}{}^{2} \times A_{AMPLIFICADOR}{}^{2}$$

Como

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{\mu}{\mu + \lambda}$$

Então

$$A_{NÓ} = \left(\frac{\mu_{MUX\,/\,DEMUX}}{\mu_{MUX\,/\,DEMUX} + \lambda_{MUX\,/\,DEMUX}} \right)^{2} \times \left(\frac{\mu_{AMPLIFICADOR}}{\mu_{AMPLIFICADOR} + \lambda_{AMPLIFICADOR}} \right)^{2}$$

Substituindo os valores, teremos que:

$$A_{NÓ} = 99{,}9972\%$$

7.2. Confiabilidade e disponibilidade do enlace

Para calcular a confiabilidade e a disponibilidade dos enlaces é necessário conhecer as taxas de falhas e de reparos dos cabos de fibra ótica, das emendas e dos conectores. A taxa de falhas dos cabos não é um dado que está disponível no fabricante, pois as falhas com eles ocorrem, na maioria das vezes, devidas a fatores externos, como escavações, por exemplo.

A melhor forma de se obter a taxa de falhas para cabos de fibra ótica é observar o seu histórico de falhas. Conhecer os locais onde as fibras estão instaladas também é fundamental para se entender como fatores externos poderão interferir na sua disponibilidade.

Para o cálculo da confiabilidade dos enlaces devemos considerar também a taxa de falhas das emendas e dos conectores. Dependendo do fabricante de fibra ótica, cada segmento de fibra pode ter em média 4 km de comprimento [35]. Assim, o número aproximado de segmentos na fibra será dada pela expressão:

$$quantidade\ de\ segmentos = \frac{comprimento\ do\ enlace}{4\,[km]} \tag{45}$$

Como para cada fibra temos dois conectores, a configuração de uma fibra sem emendas seria a seguinte:

Figura 64 – Configuração de uma fibra sem emendas

Já para o caso de fibras com emendas, a configuração seria a seguinte:

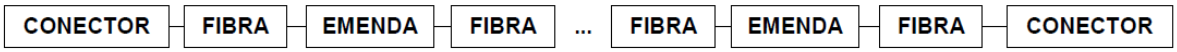


Figura 65 – Configuração de uma fibra com emendas

Não podemos esquecer que para cada enlace existe pelo menos um par de fibras, para fazer as funções de transmissão (Tx) e recepção (Rx) de dados. Se tivermos então um enlace com uma emenda, teremos duas fibras com duas emendas e quatro conectores. Como o par de fibras é acondicionado em um único cabo físico, e as falhas mais freqüentes com cabos são o seu rompimento, podemos considerar o par de fibras como sendo uma única fibra. Como as emendas são feitas separadamente e esta parte do cabeamento fica acondicionado em caixas de passagens, as emendas terão de ser contadas em separado.

Assim, o cálculo da confiabilidade para o enlace será dado pela equação:

$$R_{ENLACE} = R_{CONECTOR}{}^{4} \times R_{FIBRA}{}^{comprimento[km]} \times R_{EMENDA}{}^{2(n-1)} \tag{46}$$

Ou

$$R_{ENLACE} = (1-\lambda_{CONECTOR})^4 \times (1-\lambda_{FIBRA})^{comprimento[km]} \times (1-\lambda_{EMENDA})^{2(n-1)} \quad (47)$$

Onde *n* é igual ao número de segmentos do enlace.

E para o cálculo da disponibilidade do enlace teremos:

$$A_{ENLACE} = A_{CONECTOR}{}^4 \times A_{FIBRA}{}^{comprimento[km]} \times A_{EMENDA}{}^{2(n-1)} \quad (48)$$

Ou

$$A_{ENLACE} = \left(\frac{\mu_{CONECTOR}}{\mu_{CONECTOR}+\lambda_{CONECTOR}}\right)^4 \times \left(\frac{\mu_{FIBRA}}{\mu_{FIBRA}+\lambda_{FIBRA}}\right)^{comprimento[km]} \times \left(\frac{\mu_{EMENDA}}{\mu_{EMENDA}+\lambda_{EMENDA}}\right)^{2(n-1)} \quad (49)$$

No caso do KyaTera, o tamanho dos segmentos de fibra não segue necessariamente um padrão, pois isto depende principalmente do local por onde as fibras irão passar. Na tabela abaixo, temos a quantidade de emendas e segmentos de fibra para cada enlace da rede [4].

Tabela 9 – Distância dos enlaces [4]

Enlace	*Localização*	*Emendas*	*Segmentos*	*Distância (km)*
L_1	TPD-HSL	3	4	9,5
L_2	HSL-SLU	0	1	2,8
L_3	SLU-PUC	0	1	2,7
L_4	PUC-MAC	0	1	0,6
L_5	MAC-UNI	2	3	13,2
L_6	UNI-INC	4	5	28,2
L_7	INC-NAR	0	1	3,0
L_8	NAR-HAE	3	4	13,2
L_9	HAE-CCE	2	3	16,4
L_{10}	CCE-FAP	2	3	10,4
L_{11}	FAP-TPD	3	4	18,5
	Comprimento total do anel			**118,5**

Como não temos o histórico de falhas de cabos do KyaTera e nem acesso aos dados de falhas das emendas e conectores, usaremos os dados encontrados na literatura [21] [34] [35].

Tabela 10 – Dados para cálculo da confiabilidade do enlace [21] [34] [35]

Equipamento	*MTTF (horas)*	*FIT*	*MTTR (horas)*
Emendas de cabos	33.333.333	30	2
Conectores	10.000.000	100	2
Rompimento de cabos	3.213.556 por km	311 por km	12

Assim, substituindo os dados para cada enlace da rede, teremos os seguintes valores de confiabilidade e disponibilidade de nosso modelo:

Tabela 11 – Confiabilidade e disponibilidade do modelo

Enlace	*Localização*	*R (%)*	*A (%)*
L_1	TPD-HSL	99,9996	99,9963
L_2	HSL-SLU	99,9999	99,9989
L_3	SLU-PUC	99,9999	99,9989
L_4	PUC-MAC	99,9999	99,9997
L_5	MAC-UNI	99,9995	99,9950
L_6	UNI-INC	99,9991	99,9893
L_7	INC-NAR	99,9999	99,9988
L_8	NAR-HAE	99,9995	99,9950
L_9	HAE-CCE	99,9994	99,9938
L_{10}	CCE-FAP	99,9996	99,9960
L_{11}	FAP-TPD	99,9994	99,9930

7.3. Confiabilidade e disponibilidade da rede

Para calcular a confiabilidade e a disponibilidade de qualquer par de terminais da rede, basta calcular a função booleana de um par de nós qualquer. Para os nós AG, por exemplo, iremos usar a seguinte função booleana:

$$R_{AG} = R_A \wedge \begin{bmatrix} \left(R_{L_1} \wedge R_B \wedge R_{L_2} \wedge R_C \wedge R_{L_3} \wedge R_D \wedge R_{L_4} \wedge R_E \wedge R_{L_5} \wedge R_F \wedge R_{L_6}\right) \vee \\ \left(R_{L_7} \wedge R_H \wedge R_{L_8} \wedge R_I \wedge R_{L_9} \wedge R_J \wedge R_{L_{10}} \wedge R_K \wedge R_{L_{11}}\right) \end{bmatrix} \wedge R_G \qquad (50)$$

A partir da função booleana acima, podemos então construir o diagrama de decisão binária correspondente [9] [10] [11] [67], conforme mostrado na Figura 66.

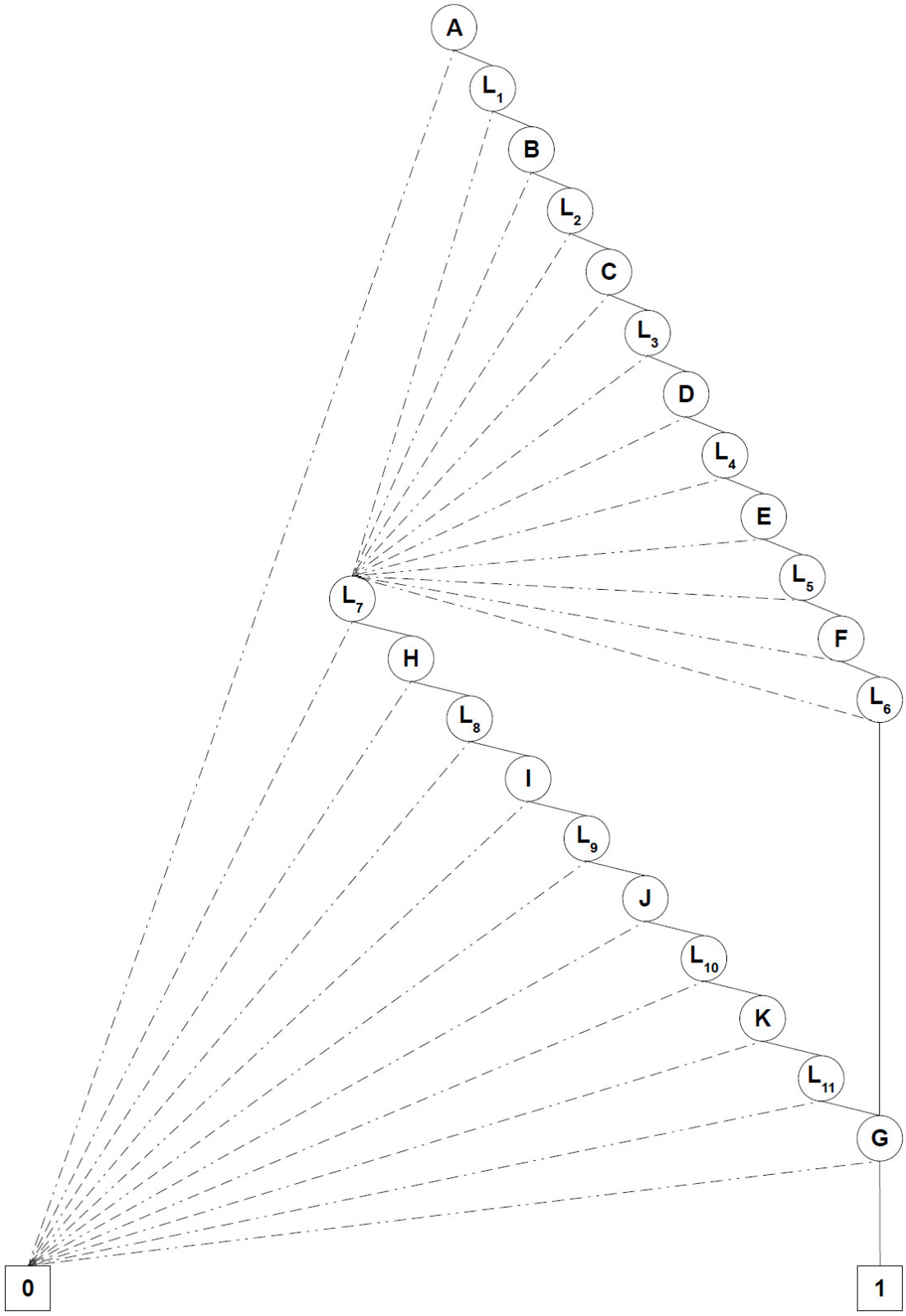


Figura 66 – Árvore de decisão binária

Com os dados de confiabilidade e disponibilidade de cada nó e de cada enlace, e com a função booleana correspondente, podemos agora calcular a confiabilidade e a disponibilidade para qualquer

par de terminais da rede. Neste estudo, vamos avaliar estes parâmetros para os nós AG, considerando que os mesmos estão sujeitos apenas a falhas de nó ou falhas de *link* simples.

A confiabilidade entre os nós A e G será dada pela seguinte equação:

$$R_{AG} = R_A \times \left(R_{L_1L_6} \parallel R_{L_7L_{11}}\right) \times R_G \tag{51}$$

A confiabilidade dos caminhos em paralelo é dada pela equação:

$$R_{L_1L_6} \parallel R_{L_7L_{11}} = 1 - \left(1 - R_{L_1L_6}\right) \times \left(1 - R_{L_7L_{11}}\right)$$

Ou

$$R_{L_1L_6} \parallel R_{L_7L_{11}} = R_{L_1L_6} + R_{L_7L_{11}} - R_{L_1L_6} \times R_{L_7L_{11}}$$

Já para cada um dos caminhos teremos:

$$R_{L_1L_6} = R_{L_1} \times R_B \times R_{L_2} \times R_C \times R_{L_3} \times R_D \times R_{L_4} \times R_E \times R_{L_5} \times R_F \times R_{L_6}$$

E

$$R_{L_7L_{11}} = R_{L_7} \times R_H \times R_{L_8} \times R_I \times R_{L_9} \times R_J \times R_{L_{10}} \times R_K \times R_{L_{11}}$$

De modo análogo, as equações para o cálculo da disponibilidade serão idênticas.

Assim, substituindo os valores, teremos:

$$R_{L_1L_6} = 99{,}9910\% \; e \; A_{L_1L_6} = 99{,}9643\%$$

$$R_{L_7L_{11}} = 99{,}9923\% \; e \; A_{L_7L_{11}} = 99{,}9655\%$$

$$R_{L_1L_6} \parallel R_{L_7L_{11}} = 100{,}0000\% \; e \; A_{L_1L_6} \parallel A_{L_7L_{11}} = 100{,}0000\%$$

Por fim, a confiabilidade e a disponibilidade da rede entre os nós A e G é:

$$R_{AG} = 99{,}9972\% \; e \; A_{AG} = 99{,}9945\%$$

Para o cálculo da indisponibilidade temos que:

$$U_{AG} = 1 - A_{AG}$$

Logo,

$$U_{AG} = 1 - 99{,}9945\% = 0{,}0055\%$$

O que significa uma indisponibilidade de aproximadamente 29 minutos por ano, sendo então considerado como tolerante a falhas, conforme mostrado na Figura 18 e na Tabela 5 [30].

Calculando a confiabilidade para todos os pares de nós teremos:

Tabela 12 – Matriz calculada de confiabilidade

NÓS	B	C	D	E	F	G	H	I	J	K
A	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%
B	-	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%
C		-	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%
D			-	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%
E				-	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%
F					-	99,9972%	99,9972%	99,9972%	99,9972%	99,9972%
G						-	99,9972%	99,9972%	99,9972%	99,9972%
H							-	99,9972%	99,9972%	99,9972%
I								-	99,9972%	99,9972%
J									-	99,9972%

E calculando a disponibilidade para todos os pares de nós teremos:

Tabela 13 – Matriz calculada de disponibilidade

NÓS	B	C	D	E	F	G	H	I	J	K
A	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%
B	-	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%
C		-	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%
D			-	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%
E				-	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%
F					-	99,9945%	99,9945%	99,9945%	99,9945%	99,9945%
G						-	99,9945%	99,9945%	99,9945%	99,9945%
H							-	99,9945%	99,9945%	99,9945%
I								-	99,9945%	99,9945%
J									-	99,9945%

Para encontrar a confiabilidade e a disponibilidade para qualquer par de nós nas Tabelas 12 e 13, basta na primeira coluna (NÓS) selecionar o nó origem e na intersecção com a coluna do nó destino (B-K) verificar o valor encontrado.

Os valores de confiabilidade e disponibilidade para todos os pares de nós do modelo aparecem iguais nas Tabelas 12 e 13 porque foram arredondados na quarta casa decimal. No entanto, os cálculos foram feitos usando-se 14 casas decimais. Os valores mínimo e máximo para a confiabilidade e disponibilidade do modelo estudado são mostrados na tabela abaixo:

Tabela 14 – Valores mínimo e máximo de confiabilidade e disponibilidade do modelo

Valores	*R (%)*	*A (%)*
Mínimo	99,99724140819050%	99,99447202648860
Máximo	99,99724209103730%	99,99448411862700

Outra justificativa é que como a rede é em anel, à medida que um nó destino se distancia do nó origem em um sentido, no sentido oposto ele vai se aproximando. E como os dois caminhos possíveis entre os pares de nós devem ser considerados como em paralelo, os valores calculados de confiabilidade e disponibilidade em um sentido mais curto acabam compensando os valores calculados do sentido mais longo.

7.4. Avaliação do impacto do MTTR na disponibilidade da rede

Ainda que a rede possa ter uma confiabilidade alta, as paradas para manutenção são inevitáveis, seja para prevenção ou para corrigir falhas. Assim, o tempo gasto para manutenção pode influenciar de forma decisiva nos valores finais de indisponibilidade da rede.

Pelo fato dos enlaces estarem distribuídos geograficamente, sejam enterrados ao longo de rodovias ou suspensos em postes junto com a rede elétrica, eles estão mais sujeitos a falhas e o seu tempo para reparo costuma ser alto, pois o reparo das fibras depende da disponibilidade de equipes de técnicos em campo, da correta localização da falha, da facilidade de acesso ao local, entre outros. Nestes casos, é o contrato de SLA quem irá estabelecer os valores de MTTR a serem praticados, e como um baixo tempo de MTTR implica um alto custo de serviços de suporte e manutenção, é necessário estabelecer um tempo de MTTR que ofereça uma boa relação custo *versus* benefício.

O valor de disponibilidade calculado para o modelo entre o par de nós AG levou em consideração um MTTR de 12 horas para manutenção dos enlaces. O gráfico da Figura 67 mostra como o incremento do MTTR para o reparo de cabos de fibra influencia na diminuição gradual dos níveis de disponibilidade. Foram usados valores de MTTR de 2 a 48 horas, com incremento de duas horas.

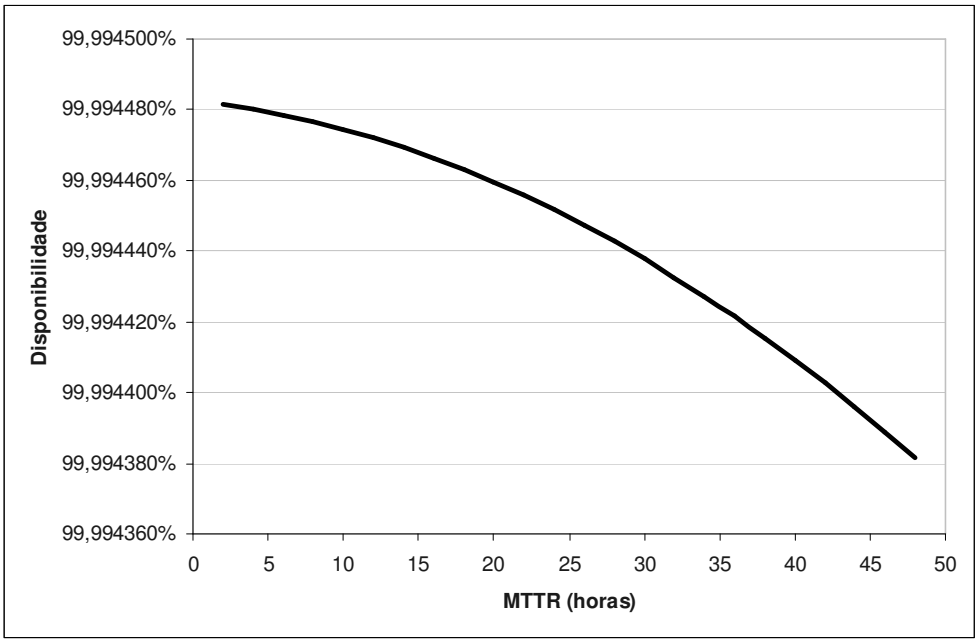


Figura 67 – Gráfico da disponibilidade *versus* MTTR para o par AG

É importante notar que no gráfico da Figura 67, mesmo variando o MTTR de 2 a 48 horas, a disponibilidade para os nós AG variou apenas de 99,9944% a 99,9945%. Isso se dá porque estamos considerando apenas as falhas de nó simples e de *link* simples. As falhas de *link* simples consideram que um segundo enlace não deverá falhar até que o primeiro seja reparado. Isso é importante de ser considerado, já que nas redes em anel sempre existem dois caminhos disjuntos entre um par de nós.

Neste caso, considerando os dados do gráfico da Figura 67, o cliente poderia contratar um nível de SLA junto ao provedor de serviços que tivesse um custo mais adequado ao seu orçamento, haja vista que tempos curtos de MTTR em nosso modelo contribuem muito pouco para o aumento da disponibilidade.

Raciocínio semelhante podemos aplicar quando plotamos em um gráfico os valores de disponibilidade de todas as 55 combinações possíveis de pares de nós em nosso modelo. No gráfico da Figura 68, foram usadas medidas de MTTR de 4, 8 e 12 horas, e os valores de disponibilidade dos pares foram colocados em ordem crescente.

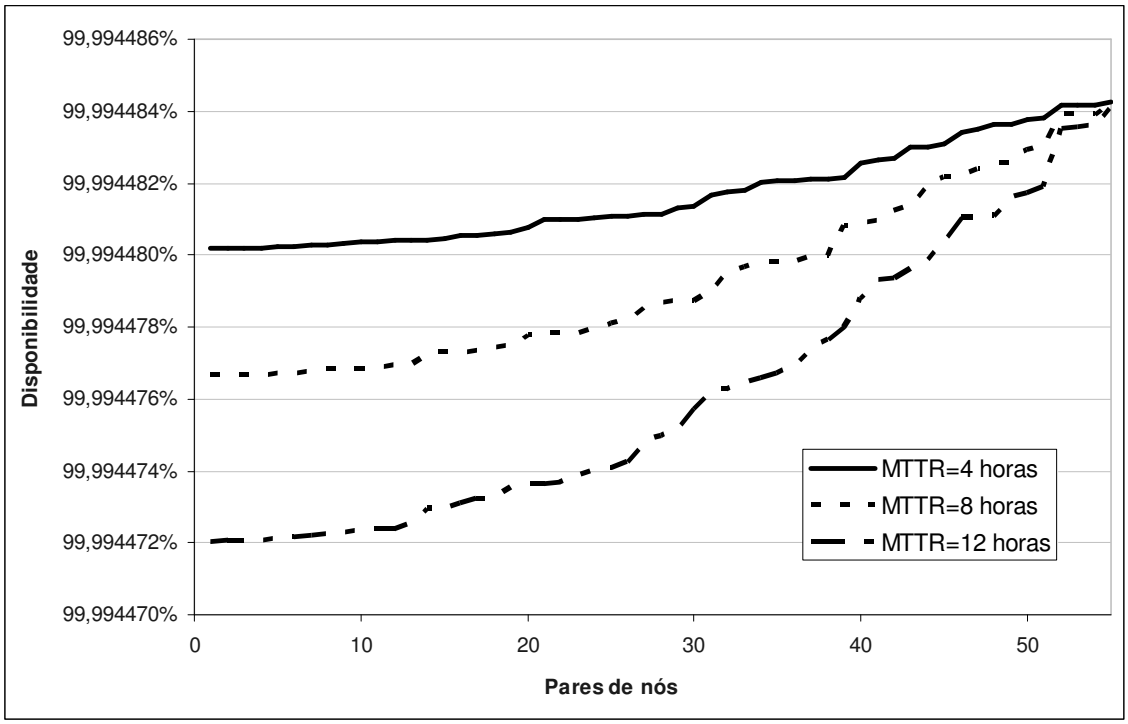


Figura 68 – Gráfico da disponibilidade *versus* MTTR para todos os pares de nós

Também neste caso, tempos curtos de MTTR contribuem muito pouco para o aumento da disponibilidade.

8. Conclusões e trabalhos futuros

Este trabalho teve por objetivo principal estudar as questões que envolvem a modelagem e a avaliação da confiabilidade e disponibilidade em redes óticas.

Estudar os aspectos que envolvem a confiabilidade é muito importante para que possamos avaliar o seu impacto na indisponibilidade da rede. Entender as características e os limites destas redes a partir da perspectiva da confiabilidade permitirá desenvolver melhores técnicas de implantação, planejamento e manutenção das redes óticas. Assim, a confiabilidade passa a ser um parâmetro fundamental a ser considerado nas aplicações e serviços a serem ofertados nas redes atuais e na Internet do futuro, e que poderá ser requerido em futuros contratos de prestação de serviços entre provedores e usuários finais.

Na parte teórica deste trabalho, procurou-se demonstrar a importância da análise da confiabilidade, apresentando os conceitos associados a ela e como aplicá-los, levando-se em conta os modelos de rede existentes e suas técnicas de proteção, bem como a aplicação de modelos de avaliação da confiabilidade. Demonstrou-se também como medir a confiabilidade da rede, desde o nível de componentes até o nível de sistema.

Na sua parte aplicada, avaliou-se uma rede real, identificando-se os componentes que compõem os nós e os enlaces da rede e aplicando-se algumas técnicas de avaliação de confiabilidade, com destaque para o uso de diagramas de decisão binária, que tem se mostrado uma ferramenta importante para contornar o problema NP-completo. Mesmo para redes com um grande número de nós e enlaces, é possível automatizar o cálculo usando-se implementações de classes em linguagens de programação orientada a objetos.

A partir da avaliação da confiabilidade do modelo da rede KyaTera, pode-se concluir que a confiabilidade diminui a medida que o nó fica mais complexo ou o enlace mais longo. Como isso pode ser inevitável em redes complexas, é imprescindível a implementação de sistemas redundantes e com caminhos alternativos para rotear o tráfego de dados. A escolha entre caminhos alternativos dedicados ou compartilhados deverá levar em conta os custos envolvidos e a criticidade dos serviços demandados.

No caso da rede KyaTera, a implementação de um anel ótico na região metropolitana pode ser suficiente para falhas de nó ou falhas de *link* simples, mas no modelo estudado a rede teria dificuldades em sobreviver a falhas de *link* duplo. Assim, a única forma de aumentar a confiabilidade do modelo estudado seria aumentar o número de caminhos alternativos entre os nós, ou instalar um segundo anel ótico, desde que não fosse implantado nos mesmos dutos.

Quanto à disponibilidade do modelo de rede estudado, pode-se concluir que diminuir o valor do MTTR contribui muito pouco no aumento da disponibilidade. Neste caso específico, o cliente poderia contratar um SLA com um tempo de atendimento maior sem prejudicar a qualidade do serviço, desde que seja considerada apenas as falhas de nó ou falhas de *link* simples. Se for considerada a possibilidade de suportar falhas de *links* duplo, o tempo de MTTR deverá ser o menor possível, o que demandará um custo maior.

Na atualidade, a melhor forma de oferecer proteção às redes óticas ainda é a instalação de caminhos alternativos disjuntos. Devido ao elevado custo de instalação destes caminhos, nem sempre esta opção é viável. Assim, acreditamos que se a KyaTera estiver próxima do modelo de rede estudado, ela não está totalmente preparada para prover a confiabilidade requerida para sistemas de missão crítica, como para algumas aplicações na área de telemedicina, por exemplo.

8.1. Proposta de trabalhos futuros

Como proposta de trabalhos futuros, pode-se expandir este estudo considerando-se uma gama maior de tipos de falha, além das falhas de nó simples e de *link* simples. Para isso é necessário modelar as falhas e verificar como elas influenciam na modelagem e avaliação da confiabilidade e da disponibilidade das redes óticas. Além disso, seria importante analisar também os principais parâmetros de desempenho requeridos pelas aplicações e serviços de tempo real, de modo a mapear os requisitos de confiabilidade, disponibilidade e segurança destas aplicações. As aplicações deveriam ser analisadas também, incluindo a análise dos diversos tipos de serviços que serão demandados nas redes de próxima geração, bem como seus parâmetros de desempenho, como largura de banda, latência, entre outros.

Referências Bibliográficas

[1] Marchant, Nils, *Network Reliability – The Quest for the Ideal Robust Network*, 2000

[2] M. N. Ellanti, S. S. Gorshe, L. G. Raman, and W. D. Grover, *Next Generation Transport Networks: Data, Management, and Control Planes*, Springer, April 2005

[3] Shepard, S., *Optical Networking Crash Course: The Market Place, The Fundamentals, The Market Players, Solutions and Applications*, McGraw-Hill, 2001

[4] Fundação de Amparo à Pesquisa do Estado de São Paulo, *Projeto KyaTera*. Disponível em: http://www.kyatera.fapesp.br. Acesso em 20 de fevereiro de 2009

[5] Hines, Annlee A., *Planning for Survivable Networks: Ensuring Business Continuity*, Wiley Publishing, 2002

[6] Henrique, Thiago, Futura Press, *Portal UOL Notícias*, 26 de janeiro de 2010. Disponível em: http://noticias.uol.com.br/cotidiano/2010/01/26/ult5772u7176.jhtm. Acesso em 10 de fevereiro de 2010

[7] Wu, P.S.; , "Undersea lightguide cable reliability analyses," *Reliability and Maintainability Symposium, 1990. Proceedings.*, Annual , vol., no., pp.157-159, 23-25 Jan 1990

[8] Yoshizawa, N.; Yabuta, T.; , "Study on submarine cable tension during laying," *Oceanic Engineering, IEEE Journal of* , vol.8, no.4, pp. 293- 299, Oct 1983

[9] Hardy, G.; Lucet, C.; Limnios, N.; , "K-Terminal Network Reliability Measures With Binary Decision Diagrams," *Reliability, IEEE Transactions on* , vol.56, no.3, pp.506-515, Sept. 2007

[10] Sy-yen Kuo; Fu-Min Yeh; Hung-Yau Lin; , "Efficient and Exact Reliability Evaluation for Networks With Imperfect Vertices," *Reliability, IEEE Transactions on* , vol.56, no.2, pp.288-300, June 2007

[11] Ghasemzadeh, M.; Meinel, C.; Khanji, S.; , "K-terminal Network Reliability Evaluation Using Binary Decision Diagram," *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on* , vol., no., pp.1-5, 7-11 April 2008

[12] Fu-Min Yeh; Shyue-Kung Lu; Sy-Yen Kuo; , "OBDD-based evaluation of k-terminal network reliability," *Reliability, IEEE Transactions on* , vol.51, no.4, pp. 443- 451, Dec 2002

[13] Liudong Xing; , "An Efficient Binary-Decision-Diagram-Based Approach for Network Reliability and Sensitivity Analysis," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* , vol.38, no.1, pp.105-115, Jan. 2008

[14] Ball, Michael O.; , "Computational Complexity of Network Reliability Analysis: An Overview," *Reliability, IEEE Transactions on* , vol.35, no.3, pp.230-239, Aug. 1986

[15] Changcheng Huang; Minzhe Li; Srinivasan, A.; , "A Scalable Path Protection Mechanism for Guaranteed Network Reliability Under Multiple Failures," *Reliability, IEEE Transactions on* , vol.56, no.2, pp.254-267, June 2007

[16] Sivakumar, M.; Sivalingam, K.M.; , "A Routing Algorithm Framework for Survivable Optical Networks Based on Resource Consumption Minimization," *Lightwave Technology, Journal of* , vol.25, no.7, pp.1684-1692, July 2007

[17] Kwok Shing Ho; Kwok Wai Cheung; , "Generalized Survivable Network," *Networking, IEEE/ACM Transactions on* , vol.15, no.4, pp.750-760, Aug. 2007

[18] Somani, Arun. Survivability and Traffic Grooming in WDM Optical Networks. Cambridge University Press, 2006

[19] Perros, Harry G., *Connection-Oriented Networks - SONET, SDH, ATM, MPLS and Optical Networks*, Wiley.

[20] Ozdaglar, A. E. and Bertsekas, D. P. 2003. Routing and wavelength assignment in optical networks. *IEEE/ACM Trans. Netw.* 11, 2 (Apr. 2003), 259-272.

[21] Grover, W. D., *Mesh-Based Survivable Transport Networks: Options and Strategies for Optical, Mpls, SONET and ATM Networking*. Prentice Hall PTR., 2003.

[22] Ramaswami, R., Sivarajan, K. N., *Optical Networks – A Practical Persperctive*, Second Edition, Morgan Kaufmann Publishers, 2002.

[23] Grote, N., Venghaus, H., *Fibre Optic Communication Devices,* Springer-Verlag, New York, 2001

[24] Kaminow, I. P., Li, T., and Willner, A. E. 2008 *Optical Fiber Telecommunications: Systems and Networks*. 5th. Academic Press.

[25] Motorola, Inc., © 2007, *Motorola AXS2200 Optical Line Terminal Datasheet*. Disponível em: http://www.motorola.com/staticfiles/Business/Products/Cable%20Broadband/Optical%20Access/AXS2200/_Documents/Static%20Files/Datasheet%20AXS2200.pdf?localeId=33. Acesso em 10 de fevereiro de 2010

[26] Ghip Systems GmbH, © 2006, *Express OADM Datasheet*. Disponível em: http://www.ghipsystems.com/Download/express-OADM-en.pdf. Acesso em 10 de fevereiro de 2010

[27] Infinera Corporation, © 2007, *Infinera Optical Line Amplifier Datasheet*. Disponível em: http://www.infinera.com/pdfs/ola/infinera_ola_data_sheet.pdf. Acesso em 10 de fevereiro de 2010

[28] Mukherjee, B., *Optical WDM Networks (Optical Networks).* Springer-Verlag New York, Inc., 2006

[29] IEEE 90 – Institute of Electrical and Electronics Engineers, "*IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*". New York, NY: 1990

[30] Liotine, M., *Mission-Critical Network Planning*, Artech House, 2003

[31] Weber, Taisy Silva. *Tolerância a falhas: conceitos e exemplos*. Disponível em: <http://www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF>

[32] Shooman, M. L., *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. John Wiley & Sons, Inc., 2002

[33] Speaks, Scott, "*Reliability and MTBF Overview*", Vicor Reliability Engineering, www.vicorpower.com.

[34] M. To, P. Neusy, *Unavailability analysis of long-haul networks*, IEEE J. on Sel. Areas in Comm., vol. 12, no. 1, January 1994, pp100-109.

[35] Rados, I.; Sunaric, T.; Turalija, P.; , "Suggestions for availability improvement of optical cables," *Circuits and Systems for Communications, 2002. Proceedings. ICCSC '02. 1st IEEE International Conference on* , vol., no., pp. 234- 239, 2002

[36] SmartOptics AS, *T-Series Optical CWDM Multiplexers Datasheet*. Disponível em: http://www.smartoptics.com/files/282-1234359443-0.pdf/T*Series%20CWDM%20R1.3.pdf. Acesso em 10 de fevereiro de 2010

[37] Shenzhen Greatway Technology Co., Ltd., *GWA3530 Series 1550nm Fiber Amplifier Datasheet*. Disponível em: http://www.greatwaytech.com/HFC/GWA3530.pdf. Acesso em 10 de fevereiro de 2010

[38] Cisco Systems, Inc., © 2008, *Raman C-Band Optical Amplifier Datasheet*, Disponível em: http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/data_sheet_c78-500925.pdf. Acesso em 10 de fevereiro de 2010

[39] CTC Union Technologies Co., Ltd., *SML-OADM Optical Add-Drop Multiplexer Datasheet*, Disponível em: http://www.ctcu.com.tw/download/catalogs/2010/SML-OADM.pdf. Acesso em 10 de fevereiro de 2010

[40] Vasseur, J., Pickavet, M., and Demeester, P. 2004 *Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Morgan Kaufmann Publishers Inc.

[41] ITU-T Recommendation E.800, "*Terms and definitions related to quality of service and network performance including dependability*", ITU-T Standardization Organization, August 1994.

[42] Stapelberg, R. F., *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design*, Springer, 2008

[43] Amazonas, José Roberto de Almeida, "*Projeto de Sistemas de Comunicações Ópticas*", Editora Manole, Barueri-SP, 2005.

[44] Torell, Wendy, Avelar, Victor, "*Mean Time Between Failure: Explanation and Standards*". White Paper #78. APC, www.apc.com.

[45] Reliasoft Publishing, *System Analysis Reference: Reliability Availability and Optimization*, 2003

[46] Torell, Wendy, Avelar, Victor, "*Performing Effective MTBF Comparisons for Data Center Infrastructure*". White Paper #112. APC, www.apc.com.

[47] Mukherjee, D.S.; Assi, C.; Agarwal, A., *An Alternative Approach for Enhanced Availability Analysis and Design Methods in p-Cycle-Based Networks*, Selected Areas in Communications, IEEE Journal on , vol.24, no.12, pp.23-34, Dec. 2006

[48] Lapcevic, O.; Lackovic, M.; Mikac, B.; , "Impact of dependent failures on the availability of the optical network," *Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on* , vol., no., pp.423-427, 25-25 July 2008

[49] C. O'Shea, "*Requirements and reference configurations for survivability*", European RACE project end-to-end Survivable Broadband Networks (IMMUNE), deliverable D2, June 1994.

[50] Xiaohong, Jiang. *Optical Networks Lectures Notes*. Disponível em: http://www.hori.ecei.tohoku.ac.jp/

[51] Ou, Canhui Sam, Mukherjee, Biswanath, "*Survivable Optical WDM Networks*", Springer, 2005.

[52] Dongyun Zhou; Subramaniam, S., *Survivability in optical networks*, Network, IEEE, vol.14, no.6, pp. 16-23, Nov/Dec 2000

[53] Ramamurthy, S.; Sahasrabuddhe, L.; Mukherjee, B., "Survivable WDM mesh networks," *Lightwave Technology, Journal of* , vol.21, no.4, pp. 870-883, April 2003

[54] Ramamurthy, S.; Mukherjee, B., “Survivable WDM mesh networks. Part I - Protection,” *INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE* , vol.2, no., pp.744-751 vol.2, 21-25 Mar 1999

[55] Ramamurthy, S.; Mukherjee, B., “Survivable WDM mesh networks. Part II - Restoration,” *Communications, 1999. ICC '99. 1999 IEEE International Conference on* , vol.3, no., pp.2023-2030 vol.3, 1999

[56] El-Bawab, Tarek S., *Optical Switching*, Springer-Verlag New York, Inc., Secaucus, NJ, 2006

[57] Wei-Jenn Ke; Sheng-De Wang; , "Reliability evaluation for distributed computing networks with imperfect nodes," *Reliability, IEEE Transactions on* , vol.46, no.3, pp.342-349, Sep 1997

[58] V. A. Netes and B. P. Filin, *Consideration of node failures in network-reliability calculation*, IEEE Transactions on Reliability, vol. 45, no. 1, pp. 127–128, Mar. 1996.

[59] K. K. Aggarwal, J. S. Gupta, and K. B. Misra, “A simple method for evaluation of a communication system,” *IEEE Trans. Communications*, vol. 23, pp. 563–566, May 1975.

[60] Yoo, Y.B.; Deo, N., *A comparison of algorithms for terminal-pair reliability*, Reliability, IEEE Transactions on , vol.37, no.2, pp.210-215, Jun 1988

[61] D. Torrieri, *Calculation of node-pair reliability in large networks with unreliable nodes*, IEEE Transactions on Reliability, vol. 43, no. 3, pp. 375–377, Sep. 1994.

[62] W. Kuo and M. J. Zuo. Optimal Reliability Modeling: Principles and Applications. Wiley, 2002.

[63] C. Lucet and J.-F. Manouvrier, “Exact methods to compute network reliability,” in *Statistical and Probabilistic Models in Reliability*, D. C. Ionescu and N. Limnios, Eds. Birkhauser Boston: , 1999, pp. 279–294.

[64] Tittmann, P.: *Combinatorial Methods in Network Reliability*, ATH Bielsko-Biała, Polen, 30. Mai 2007.

[65] Fabio Somenzi. CUDD Package. ftp://vlsi.colorado.edu/pub/.

[66] C. Y. Lee. Representation of Switching Circuits by Binary-Decision Programs. *Bell Syst. Tech. Journal*, 38:985-999, 1959

[67] Akers, S.B.; , "Binary Decision Diagrams," *Computers, IEEE Transactions on* , vol.C-27, no.6, pp.509-516, June 1978

[68] Maciel França Madeira, Heraldo, *Diagramas de Decisão Binária - Levantamento Bibliográfico*, USP/IME, 2000

[69] Randal E. Bryant. Graph-Based Algorithms for Boolean Function Manipulation. *IEEE Transactions on Computers*, 35(8):677–691, 1986.

[70] Odling, P.; Mayr, B.; Palm, S.; , "The technical impact of the unbundling process and regulatory action," *Communications Magazine, IEEE* , vol.38, no.5, pp.74-80, May 2000