



**UNIVERSIDADE ESTADUAL DO CEARÁ**  
**CENTRO DE CIÊNCIAS E TECNOLOGIA**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO**  
**MESTRADO ACADÊMICO EM CIÊNCIA DA COMPUTAÇÃO**

**JEFFERSON RODRIGO ALVES CAVALCANTE**

**UM MECANISMO DE ALERTAS PREVENTIVOS APOIADO EM SÉRIES  
TEMPORAIS PARA MONITORAMENTO DE DESEMPENHO EM REDES OTN**

**FORTALEZA – CEARÁ**

**2018**

JEFFERSON RODRIGO ALVES CAVALCANTE

UM MECANISMO DE ALERTAS PREVENTIVOS APOIADO EM SÉRIES TEMPORAIS  
PARA MONITORAMENTO DE DESEMPENHO EM REDES OTN

Dissertação apresentada ao Curso de Mestrado Acadêmico em Ciência da Computação do Programa de Pós-Graduação em Ciência da Computação do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de mestre em Ciência da Computação. Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Joaquim Celestino Júnior

FORTALEZA – CEARÁ

2018

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Sistema de Bibliotecas

Cavalcante, Jefferson Rodrigo Alves.

Um mecanismo de alertas preventivos apoiado em séries temporais para monitoramento de desempenho em redes OTN [recurso eletrônico] / Jefferson Rodrigo Alves Cavalcante. - 2018.

1 CD-ROM: il.; 4 ¾ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 57 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado acadêmico) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Acadêmico em Ciência da Computação, Fortaleza, 2018.

Área de concentração: Redes de Computadores.

Orientação: Prof. Dr. Joaquim Celestino Júnior.

1. Redes Ópticas de Transporte. 2. Séries Temporais. 3. Alisamento exponencial. 4. Cadeias de Markov. 5. Gerenciamento Preventivo. I. Título.

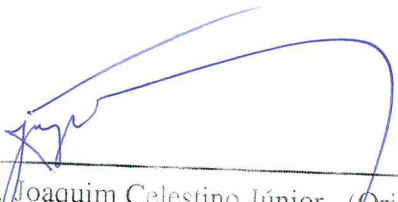
JEFFERSON RODRIGO ALVES CAVALCANTE

UM MECANISMO DE ALERTAS PREVENTIVOS APOIADO EM SÉRIES TEMPORAIS  
PARA MONITORAMENTO DE DESEMPENHO EM REDES OTN

Dissertação apresentada ao Curso de Mestrado Acadêmico em Ciência da Computação do Programa de Pós-Graduação em Ciência da Computação do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de mestre em Ciência da Computação. Área de Concentração: Ciência da Computação


Aprovada em: 20 de março de 2018

BANCA EXAMINADORA




---

Prof. Dr. Joaquim Celestino Júnior (Orientador)  
Universidade Estadual do Ceará - UECE



---

Prof. Dr. Rafael Lopes Gomes  
Universidade Estadual do Ceará - UECE



---

Prof. Dr. Maxwell Eduardo Monteiro  
Instituto Federal do Espírito Santo - IFES

À minha família, por sua capacidade de acreditar em mim e investir em mim. Mãe, seu cuidado e dedicação foi que deram, em alguns momentos, a esperança para seguir. Pai, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada.

## **AGRADECIMENTOS**

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida, e não somente nestes anos como universitário, mas que em todos os momentos é o maior mestre que alguém pode conhecer.

Aos meus pais Claudio e Aldinete e ao meu irmão Marcos, pelo amor, incentivo e apoio incondicional e que, durante os momentos de minha ausência dedicados ao estudo superior, sempre fizeram entender que o futuro é feito a partir da constante dedicação no presente!

A minha namorada Suzana, por ter me apoiado durante esta caminhada e ter sempre compreendido a importância do tempo dedicado aos estudos nos momentos de minha ausência.

À Universidade Estadual do Ceará, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presentes.

Ao meu professor orientador Celestino, por ter apoiado esta pesquisa e por ter proporcionado conhecimento e experiência não apenas acadêmicos, mas também de vida.

Agradeço a todos os professores não somente por terem me ensinado, mas por terem me feito aprender. a palavra mestre, nunca fará justiça aos professores dedicados aos quais sem nominar terão os meus eternos agradecimentos.

“É melhor lançar-se à luta em busca do triunfo mesmo expondo-se ao insucesso, que formar fila com os pobres de espírito, que nem gozam muito nem sofrem muito; E vivem nessa penumbra cinzenta sem conhecer nem vitória nem derrota.”

(Franklin Roosevelt)

## RESUMO

A Internet depende de redes de transporte com funções de entrega confiáveis e melhoradas para atender a atual demanda de seus usuários. Nessas redes, switches de Redes Ópticas de Transporte, ou Optical Transport Networks (OTN) em inglês, monitoram diferentes tipos de eventos em intervalos fixos de tempo, mantendo séries temporais de importantes métricas de desempenho. Através da exploração inteligente dessas séries temporais, operadores de rede podem antecipar falhas antes mesmo que elas ocorram, aprovisionar melhor os recursos da rede e garantir a qualidade e confiabilidade do serviço de transporte de dados. Neste trabalho, propõe-se um mecanismo de alertas que, apoiado na análise de séries temporais de Errored Blocks em intervalos de 1 segundo através do modelos de Holt e de cadeias de Markov, estima seu comportamento e avisa caso espere-se que a rede entre em estado de indisponibilidade nos próximos segundos de operação. O cenário simulado de testes foi baseado nos efeitos de variações reais de temperatura ocorridas na cidade de Curitiba sobre um laser usado em redes ópticas. Resultados em 9 simulações desse cenário mostraram que foi possível prever períodos de indisponibilidade com até 32 segundos de antecedência, tempo suficiente para ativação de um caminho protegido antes que a rede entrasse efetivamente em estado de indisponibilidade.

**Palavras-chave:** Redes Ópticas de Transporte. Séries Temporais. Alisamento exponencial. Cadeias de Markov. Gerenciamento Preventivo. Indisponibilidade de Rede



## ABSTRACT

The Internet depends on robust transport networks to meet user demands with improved and reliable managed delivery functions. In such networks, Optical Transport Network (OTN) switches are responsible for monitoring the occurrence of different types of performance events in fixed-time monitoring intervals, resulting in a set of time series. Exploring the occurrence of these events in an optimized intelligent way, enables operators to overcome faults before they actually take place, to perform better resource provisioning and assure quality of service and reliability. In this work we propose an alert mechanism for OTN which, from analysis of time series of Errored Blocks in 1-second intervals through Holt and Markov chain models, estimates its behavior and alerts if network unavailability is expected for next seconds of operation. The test scenario was based on effect of temperature variations occurred in Curitiba on a laser used in optical networks. From results based on 9 simulations of this scenario, the proposed mechanism alerted of network unavailability up to 32 seconds earlier, which is enough anticipation for activation of a protection path before unavailability could actually take place.

**Keywords:** Optical Transport Networks. Time series forecasting. Network performance monitoring. Exponential smoothing. Markov chains. Preventive Management. Network Unavailability

## LISTA DE ILUSTRAÇÕES

<b>Figura 1 – Organização dos cabeçalhos OPU, ODU e OTU em um quadro OTN. . . . .</b>	<b>19</b>
<b>Figura 2 – Ilustrando o transporte de tráfego Ethernet 10 Gigabit sobre uma OTN, incluindo um Operations System (OS) para gerência da rede e as trilhas ODU e OTU, onde o cabeçalho dessas camadas é criado/lido no caminho fim-a-fim. . . . .</b>	<b>20</b>
<b>Figura 3 – Funções de monitoramento de desempenho OTN. . . . .</b>	<b>21</b>
<b>Figura 4 – Indisponibilidade de caminhos em redes OTN. . . . .</b>	<b>22</b>
<b>Figura 5 – Série temporal na qual a tendência afeta a sazonalidade. . . . .</b>	<b>23</b>
<b>Figura 6 – A Função de Monitoramento de Desempenho UPAM e sua integração com as funções já padronizadas pela ITU-T. . . . .</b>	<b>26</b>
<b>Figura 7 – Intensidade do sinal transmitido pelo comprimento de onda no laser L1550P5DFB da Thorlabs. . . . .</b>	<b>33</b>
<b>Figura 8 – Relação entre Bit Error Rate e SNR medido em <math>E_b/N_0</math>, calculada através da Equação 5.3. . . . .</b>	<b>36</b>
<b>Figura 9 – Acurácias médias obtidas na detecção de Unavailable Seconds (UaS) para cada tamanho de amostra utilizando o modelo Holt com <math>\alpha</math> e <math>\beta</math> variando entre 0.3, 0.5 e 0.9. . . . .</b>	<b>38</b>
<b>Figura 10 – Taxa de falso-positivos médias obtidas na detecção de Unavailable Seconds (UaS) para cada tamanho de amostra utilizando o modelo Holt com <math>\alpha</math> e <math>\beta</math> variando entre 0.3, 0.5 e 0.9. . . . .</b>	<b>38</b>
<b>Figura 11 – Acurácias obtidas para cada tamanho de amostra utilizando o modelo de cadeia de Markov proposto na detecção de Unavailable Seconds (UaS). . . . .</b>	<b>39</b>
<b>Figura 12 – Taxa de falso-positivos obtidas para cada tamanho de amostra utilizando o modelo de cadeia de Markov proposto na detecção de Unavailable Seconds (UaS). . . . .</b>	<b>39</b>
<b>Figura 13 – Acurácia na detecção de Unavailable Seconds (UaS) por cada combinação de <math>\alpha</math> e <math>\beta</math> do modelo Holt em simulação do cenário de testes proposto. . . . .</b>	<b>40</b>
<b>Figura 14 – Taxa de falso-positivos na detecção de Unavailable Seconds (UaS) por cada combinação de <math>\alpha</math> e <math>\beta</math> do modelo Holt em simulação do cenário de testes proposto. . . . .</b>	<b>40</b>
<b>Figura 15 – Funcionamento do UPAM em simulação do cenário de testes. . . . .</b>	<b>42</b>

<b>Figura 16 – Funcionamento do UPAM em simulação do cenário de testes. . . . .</b>	<b>42</b>
<b>Figura 17 – Funcionamento do UPAM em simulação do cenário de testes. . . . .</b>	<b>43</b>
<b>Figura 18 – Antecipação à detecção de indisponibilidade em 9 simulações através do mecanismo UPAM. . . . .</b>	<b>43</b>

## LISTA DE TABELAS

<b>Tabela 2 – Mapeamento entre transições segundo-a-segundo e estados do modelo de cadeia de Markov proposto . . . . .</b>	<b>28</b>
<b>Tabela 3 – Parâmetros usados pelos modelos Holt e de cadeia de Markov no UPAM.</b>	<b>41</b>
<b>Tabela 4 – Estatísticas do UPAM aplicado a 9 simulações do cenário de testes. . . .</b>	<b>41</b>

## LISTA DE ALGORITMOS

**Algoritmo 1 – Retorna se um caminho ODU tende a permanecer em estado de degradação de desempenho utilizando a cadeia de Markov proposta** 29

## LISTA DE ABREVIATURAS E SIGLAS

BBE	Background Block Error
BER	Bit Error Rate
BUT	Begin of Unavailable Time
EB	Errored Block
EBC	Errored Blocks Counter
ES	Errored Second
EUT	End of Unavailable Time
FEC	Forwarding Error Correction
FMD	Funções de Monitoramento de Desempenho
MIB	Model Information Base
NE	Network Element
NES	Non-Errored Second
ODU	Optical Data Unit
OPU	Optical Payload Unit
OSNR	Optical Signal-to-Noise Ratio
OTN	Optical Transport Networks
OTU	Optical Transport Unit
SES	Severely Errored Second
SNR	Signal-to-Noise Ratio
TBC	Transmitted Blocks Counter
UaS	Unavailable Seconds
UPAM	Urgent Preventive Alert Mechanism
WDM	Wavelength Division Multiplexing

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	15
<b>2</b>	<b>TRABALHOS RELACIONADOS</b>	17
<b>3</b>	<b>FUNDAMENTAÇÃO TEÓRICA</b>	19
3.1	GERÊNCIA DE DESEMPENHO EM REDES OTN	19
3.2	PREVISÃO DE SÉRIES TEMPORAIS	22
3.3	CADEIAS DE MARKOV	24
<b>4</b>	<b>PROPOSTA</b>	26
4.1	MECANISMO DE ALERTA DE DESEMPENHO PARA REDES OTN	26
<b>4.1.1</b>	<b>O Urgent Preventive Alert Mechanism (UPAM)</b>	26
4.1.1.1	Cadeia de Markov Proposta	27
4.1.1.2	Os Alertas UPAM	29
<b>5</b>	<b>EXPERIMENTOS</b>	31
5.1	METODOLOGIA	31
<b>5.1.1</b>	<b>Seleção do Tamanho das Amostras</b>	31
<b>5.1.2</b>	<b>Seleção das Constantes <math>\alpha</math> e <math>\beta</math></b>	32
<b>5.1.3</b>	<b>Análise da Antecipação à Indisponibilidade</b>	32
5.2	CENÁRIO DE TESTES	32
5.3	SIMULAÇÃO DO CENÁRIO DE TESTES	34
<b>6</b>	<b>RESULTADOS</b>	37
6.1	ESCOLHA DO TAMANHO DA AMOSTRA	37
6.2	CONSTANTES DE ALISAMENTO $\alpha$ E $\beta$	39
6.3	APLICAÇÃO DO UPAM EM SIMULAÇÕES DO CENÁRIO DE TESTES	41
<b>7</b>	<b>CONCLUSÕES E TRABALHOS FUTUROS</b>	44
7.1	TRABALHOS FUTUROS	44
	<b>REFERÊNCIAS</b>	45
	<b>ANEXOS</b>	47
	ANEXO A – ALARM MECHANISM FOR ANTICIPATED DETECTION OF NETWORK UNAVAILABILITY IN IP NETWORKS THROUGH TIME SERIES ANALYSIS	48

## 1 INTRODUÇÃO

Com o propósito de melhorar o transporte de dados através de fibras ópticas, as Redes Ópticas de Transporte, ou Optical Transport Networks (OTN) em inglês, surgiram como uma evolução das tecnologias Synchronous Digital Hierarchy (SDH) e Synchronous Optical Networking (SONET), trazendo maior escalabilidade, menos overhead, transporte transparente do sinal cliente, topologias livres de formato, melhorias na padronização das funções de gerência para as camadas digitais e uso aprimorado de algoritmos de correção de erros, ou Forwarding Error Correction (FEC) em inglês, permitindo transmissões mais longas com menos regeneração.

Apesar dos diversos aprimoramentos ao longo dos anos, comunicações através de redes ópticas são suscetíveis a diversos tipos de degradação, que provocam conversões incorretas de sinais ópticos para elétricos no momento de sua recepção e podem levar à completa interrupção das comunicações caso seus efeitos sejam prolongados. As causas mais relevantes de degradação em redes ópticas são variações na temperatura dos lasers e multiplexadores, dispersão cromática e dos modos de polarização, acúmulo de ruído devido a conversões e ampliações do sinal óptico, não-linearidades das fibras, dentre outras (PAN; YU; WILLNER, 2010).

Nesse ínterim, a gerência de desempenho de redes OTN foi padronizada para medir a qualidade das comunicações, possibilitando que operadores de rede identifiquem caminhos ópticos degradados e tomem medidas corretivas. Os dados provenientes dessas medições, no entanto, podem ser usados também como entrada para modelos matemáticos, viabilizando análises automatizadas e inteligentes do desempenho, possivelmente até mesmo antecipando degradações inaceitáveis na qualidade da rede e permitindo correções antes mesmo que falhas aconteçam.

No caso de redes ópticas de longa distância, desde as terrestres a partir de 2000km às transpácificas de aproximadamente 10000km, o acúmulo de ruído gerado pelos vários amplificadores, as diferenças de temperatura entre multiplexadores localizados em diferentes regiões, os efeitos das dispersões e os efeitos das não-linearidades das fibras tornam-se problemas ainda mais ameaçadores para o desempenho dessas redes. Nesse contexto de maior suscetibilidade a interferências climáticas, à ação humana e até mesmo aos tipo de ambientes onde estão as fibras e os equipamentos, modelos probabilísticos capazes de se ajustar a séries temporais e estimar seu comportamento futuro são de especial interesse, pois podem ser usados para prever medições da gerência de desempenho de redes OTN e antecipar a abordagem de condições inaceitáveis na qualidade das comunicações, servindo como um nível adicional de segurança na prevenção da



indisponibilidade de serviço.

Neste trabalho, propõe-se o Urgent Preventive Alert Mechanism (UPAM), um mecanismo de alerta que, apoiado em dois modelos matemáticos para previsão e análise de séries temporais, sejam eles o modelo Holt e um modelo de cadeia de Markov proposto neste trabalho, é capaz de alertar com elevada acurácia que condições inaceitáveis de desempenho provavelmente ocorrerão num futuro próximo. De acordo com experimentos realizados em 9 simulações de um cenário de testes proposto, o mecanismo de alerta foi capaz de reportar períodos de indisponibilidade com antecedência média entre 6 e 12 segundos dependendo da simulação, chegando mesmo a alertar a chegada de um período de indisponibilidade com antecedência máxima de 32 segundos em uma das simulações. Sendo 10 segundos o tempo de detecção de indisponibilidade em redes OTN e 50 milisegundos o tempo de ativação de uma proteção, ou seja, uma rota alternativa, os resultados mostram que o mecanismo proposto seria plenamente capaz de evitar interrupção nas comunicações em cenários parecidos com o usado nos experimentos.

## 2 TRABALHOS RELACIONADOS

Como fruto da pesquisa que levou a este trabalho de dissertação de mestrado, recentemente publicamos o primeiro artigo que chama a atenção para o uso de modelos de séries temporais em redes OTN (CAVALCANTE; PATEL; CELESTINO, 2017). Nele, três famosos modelos de previsão baseados em alisamento exponencial foram comparados em um cenário de redução abrupta no desempenho da rede. Mediu-se a precisão dos modelos Simple Exponential Smoothing (SES), Holt e Holt-Winters em condições de alta estabilidade da rede, em seguida o número de frames recebidos incorretamente sofreu uma abrupta elevação e investigou-se quanto tempo cada modelo precisou para recuperar níveis de acerto tão acurados quanto antes da forte degradação. Esse tipo de degradação pode ocorrer em cenários de baixa estabilidade, como em cabos submarinos ou instalados em bueiros onde intercorrências acidentais podem provocar um esticamento ou dobra das fibras, causando pequenas rachaduras na fibra ou reduzindo a reflexibilidade de alguns comprimentos de onda, como reportado em (INTERNATIONAL TELECOMMUNICATION UNION, 2009). A ação humana durante manutenções também podem causar esse tipo de degradação por pressão sobre os cabos onde localizam-se as fibras ou pelos motivos já mencionados.

Neste trabalho de dissertação de mestrado, as degradações usadas nos experimentos são baseadas em variações reais na temperatura ambiente e acúmulo de ruído causado pelas dispersões e amplificações do sinal óptico. Além disso, propõe-se uma aplicação prática para modelos de previsão em redes OTN: um mecanismo de alerta capaz de antecipar que falhas provavelmente ocorrerão nos próximos segundos de operação. Nesse contexto, mesmo após uma extensiva busca na literatura, não encontramos nenhum outro trabalho que se propõe a prever indisponibilidade em redes OTN a partir da análise de séries temporais. No entanto, buscamos inspiração em um tópico próximo, o de detecção de anomalias em redes IP.

Trabalhos recentes na detecção de comportamentos anômalos em redes IP, como o Ant Colony Optimization for Digital Signature (ACODS) (CARVALHO *et al.*, 2016), baseado em um algoritmo bioinspirado e em técnicas de assinatura digital, e o trabalho reportado em (HAMAMOTO *et al.*, 2017), baseado em um algoritmo genético e lógica fuzzy, são exemplos de abordagens recentes para esse problema. De acordo com (BHUYAN; BHATTACHARYYA; KALITA, 2014), trabalhos nessa área são divididos em detecção de anomalias de desempenho ou segurança, e normalmente seguem uma abordagem baseada em duas etapas a cada iteração: (a) classificar o tráfego e computar o que deve ser considerado normal para cada classe, sejam

elas portas TCP, endereços IP de destino, dentre outras; (b) detectar quando o comportamento do tráfego desvia do que foi calculado como normal ou aceitável para cada classe, fazendo com que a detecção de anomalias aconteça o mais próximo possível do momento em que elas efetivamente começaram a ocorrer.

Nossa proposta difere em alguns sentidos das propostas para detecção de anomalias em redes IP, mas nos inspiramos em alguns de seus aspectos e métricas. Por exemplo, o mecanismo aqui proposto utiliza dois modelos matemáticos combinados, o modelo de Holt para prever o número de Errored Blocks, uma das métricas de desempenho em redes OTN, e um modelo de Cadeia de Markov para prever o comportamento da rede nas próximas iterações do monitoramento de desempenho. Além disso, os trabalhos recentemente publicados em (CARVALHO *et al.*, 2016) e (HAMAMOTO *et al.*, 2017), assim como em outros trabalhos, medem o desempenho de suas propostas através das métricas Acurácia e Taxa de Falso-Positivos. As propostas apresentadas nesse trabalho alcançaram entre 96.5% e 95.4% de Acurácia e entre 0.56% e 0.64% de Taxa de Falso-Positivos. Sendo assim, pretende-se atingir níveis similares ou melhores que esse no mecanismo de alerta proposto neste trabalho de mestrado.

Recentemente testamos uma versão modificada do mecanismo de alerta aqui proposto em redes IP com medições de perda de pacotes em redes reais, onde atingiu-se mais de 99% de acurácia e menos de 0.05% de Taxa de Falsos-Positivos na maioria das redes testadas, tendo essas métricas atingido 96.5% de acurácia e 2% de Taxa de Falsos-Positivos no pior cenário encontrado, onde a rede apresentava altos valores de Entropia Aproximada, indicando um alto grau de aleatoriedade nas medições, o que dificulta a ação de modelos de previsão. O artigo completo está incluído no anexo A, atualmente encontra-se em fase de publicação e serviu como prova de conceito para este trabalho de mestrado.

### 3 FUNDAMENTAÇÃO TEÓRICA

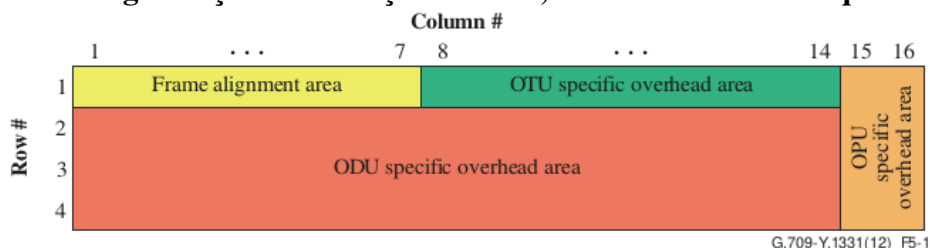
Para melhor compreender o mecanismo proposto, faz-se necessário entender o funcionamento do monitoramento de desempenho em redes OTN e os fundamentos de previsão baseada em séries temporais.

#### 3.1 GERÊNCIA DE DESEMPENHO EM REDES OTN

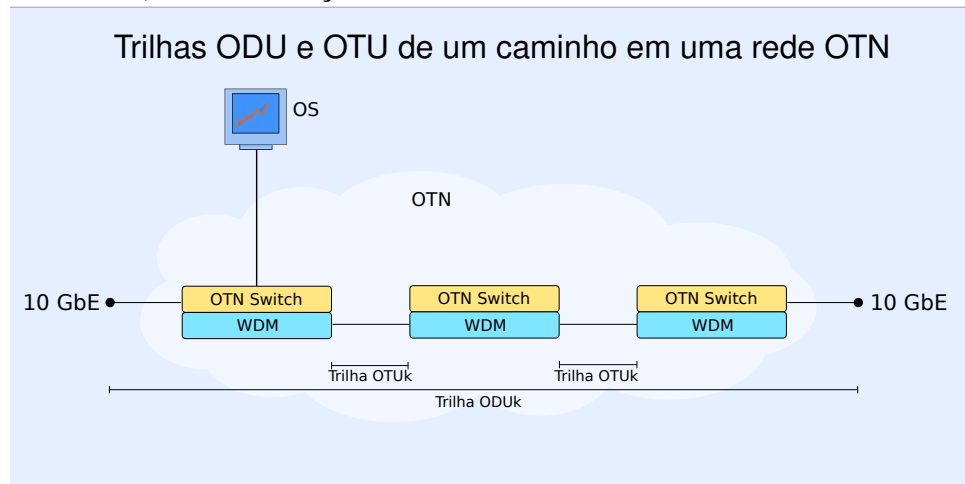
Para fornecer os recursos de gerenciamento e monitoramento desejados em redes OTN, a ITU-T padronizou as 3 camadas digitais das redes OTN, sejam elas a Optical Payload Unit (OPU), a Optical Data Unit (ODU) e a Optical Transport Unit (OTU), que servem como entrada para a camada óptica Optical Channel (OCh) onde o sinal digital é efetivamente modulado para transporte através da luz. Neste trabalho, aproveita-se a padronização para a gerência de desempenho da camada digital ODU, por isso apenas os aspectos das camadas digitais serão apresentados. Segue uma breve descrição do objetivo de cada camada digital das redes OTN.

A camada OPU é responsável pelo mapeamento entre o sinal cliente e a tecnologia OTN, seja ele advindo de redes Ethernet, SONET, dentre outras redes. A camada ODU é responsável pela supervisão de caminho de ponta a ponta, incluindo monitoramento de desempenho em pontos finais onde o sinal cliente entra e sai da rede. A camada OTU, por sua vez, é responsável pela supervisão do sinal entre seções do caminho fim-a-fim e provê a funcionalidade de correção de erros, ou seja, implementa algoritmos do tipo Forwarding Error Correction (FEC) que corrigem bits incorretos nos quadros OTN detectados no momento de sua recepção. A Figura 1 mostra a organização dos cabeçalhos das camadas digitais no quadro OTN. A figura 2 ilustra as seções da rede OTN na qual os cabeçalhos ODU e OTU são utilizados no transporte fim-a-fim do sinal cliente, sendo OTN Switch a parte responsável pela adaptação do sinal cliente e monitoramento do caminho fim-a-fim, e Wavelength Division Multiplexing (WDM) a parte responsável pela multiplexação/demultiplexação e transmissão/recepção do sinal óptico na fibra.

**Figura 1 – Organização dos cabeçalhos OPU, ODU e OTU em um quadro OTN.**



**Figura 2 – Ilustrando o transporte de tráfego Ethernet 10 Gigabit sobre uma OTN, incluindo um Operations System (OS) para gerência da rede e as trilhas ODU e OTU, onde o cabeçalho dessas camadas é criado/lido no caminho fim-a-fim.**

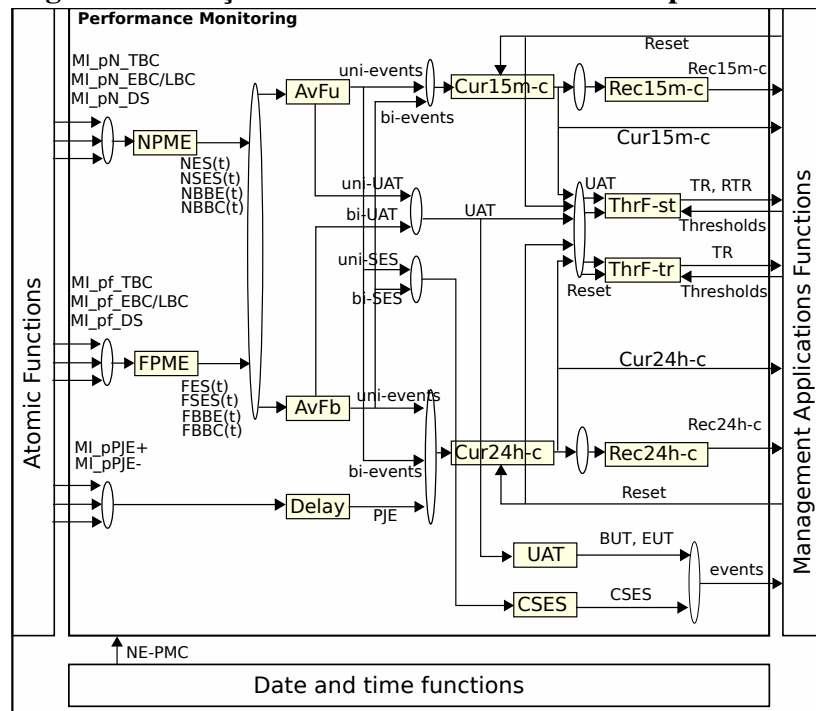


Fonte: Elaborado pelo autor

Cada camada digital possui um conjunto de funções atômicas responsáveis pelo processamento dos respectivos cabeçalhos no quadro OTN. Na camada ODU, a função atômica ODUk\_TT realiza verificações no campo BIP-8 de seu cabeçalho, que permite detectar a ocorrência de bits incorretos no quadro OTN (INTERNATIONAL TELECOMMUNICATION UNION, 2012b). As funções atômicas alimentam as Funções de Monitoramento de Desempenho (FMD), que processam as informações fornecidas pelas funções atômicas e, no caso das FMD, realizam o monitoramento e a gerência do desempenho de cada caminho ODU. Faz parte das atribuições das FMD a contagem de quadros incorretos por segundo, o armazenamento de objetos de monitoramento de desempenho em bases de dados, dentre outras. A Figura 3 apresenta as funções de monitoramento de desempenho padronizadas para as redes OTN e sua integração com as funções atômicas, bem como com as Função de Aplicações de Gerência, responsáveis por tomar ações referentes aos eventos produzidos pelas funções de monitoramento de desempenho.

Nas camadas ODU e OTU, cada quadro com bits incorretos é considerado um Errored Block (EB). Em intervalos de um segundo, o monitoramento de desempenho computa o contador Errored Blocks Counter (EBC), com o número de quadros com erros BIP-8 recebidos ou transmitidos nesse intervalo, juntamente com o Transmitted Blocks Counter (TBC), número de quadros recebidos ou transmitidos nesse intervalo. Se pelo menos um quadro (ou bloco) com erro foi detectado durante o último intervalo de um segundo, esse segundo é classificado como um Errored Second (ES). No entanto, se mais de 15% dos blocos recebidos ou transmitidos apresentarem bits incorretos, esse segundo é classificado como Severely Errored Second (SES) (INTERNATIONAL TELECOMMUNICATION UNION, 2003). Caso 10 SES consecutivos

**Figura 3 – Funções de monitoramento de desempenho OTN.**

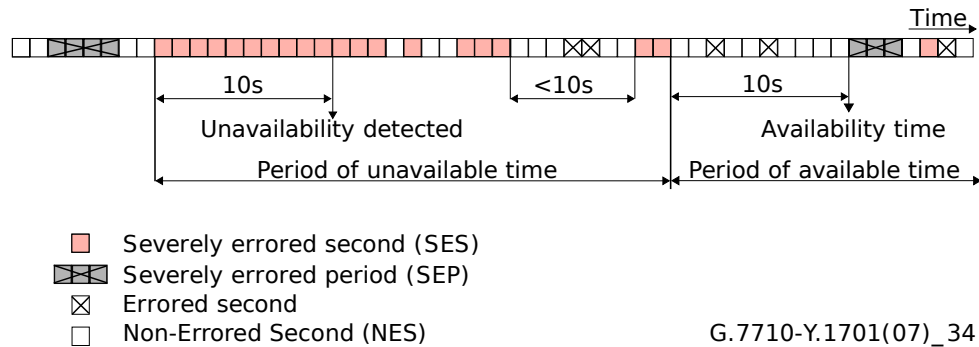


Fonte: Elaborado pelo autor, adaptado de ITU-T G.7710 (INTERNATIONAL TELECOMMUNICATION UNION, 2012a).

ocorram, o caminho ODU monitorado torna-se indisponível até que 10 segundos consecutivos sejam não-SES, como mostra a Figura 4 (INTERNATIONAL TELECOMMUNICATION UNION, 2012a). Deve-se observar que o monitoramento dos quadros transmitidos é feito separadamente dos quadros recebidos. A função de monitoramento de desempenho responsável por registrar o início e o fim de um período de indisponibilidade é a Unavailable Time (UAT), mostrada na Figura 3, que registra os eventos Begin of Unavailable Time (BUT) e End of Unavailable Time (EUT) a partir das informações providas pelas funções AvFu e AvFb. Na ocorrência de 10 SES seguidos, um alarme é disparado por ocasião do início de um período de indisponibilidade do caminho, ficando a cargo da gerência do equipamento e dos operadores da rede a tomada de ações corretivas. Faz parte do objetivo deste trabalho evitar que os efeitos da indisponibilidade afetem as comunicações, sendo os alertas responsáveis por sensibilizar o sistema de gerência a tomar ações corretivas antes que um alarme seja efetivamente disparado.

A gerência de desempenho em OTN acumula contadores de ES e SES durante intervalos de monitoramento de 15 minutos e 24 horas simultaneamente para cada caminho ODU. Além disso, o contador de Background Block Errors (BBE) acumula o número de Errored Blocks ocorridos enquanto o caminho ODU está disponível, e o contador Unavailable Second (UaS) conta por quantos segundos o caminho se manteve indisponível nesse intervalo. Assim que um intervalo de monitoramento termina, esses contadores são armazenados em uma Model

**Figura 4 – Indisponibilidade de caminhos em redes OTN.**



Fonte: Elaborado pelo autor, adaptado de ITU-T G.7710 (INTERNATIONAL TELECOMMUNICATION UNION, 2012a).

Information Base (MIB) (INTERNATIONAL TELECOMMUNICATION UNION, 2012c) em registros chamados de *recent registers*, com capacidade para os contadores dos 16 últimos intervalos de monitoramento de 15 minutos e do último intervalo de 24 horas. Enquanto um intervalo de monitoramento está em aberto, seus contadores são armazenados em um registro chamado *current register* da MIB da Gerência de Desempenho, e existe tanto para o monitoramento de 15 minutos quanto para o de 24 horas (INTERNATIONAL TELECOMMUNICATION UNION, 2012a).

Em resumo, Network Elements (NE) OTN compõem séries temporais de EBC a cada intervalo de um segundo e séries temporais de BBE e SES em intervalos de 15 minutos. Neste trabalho, exploramos técnicas de análise de séries temporais do contador EBC para tentar antecipar a ocorrência falhas em caminhos ODU antes que elas sequer ocorram.

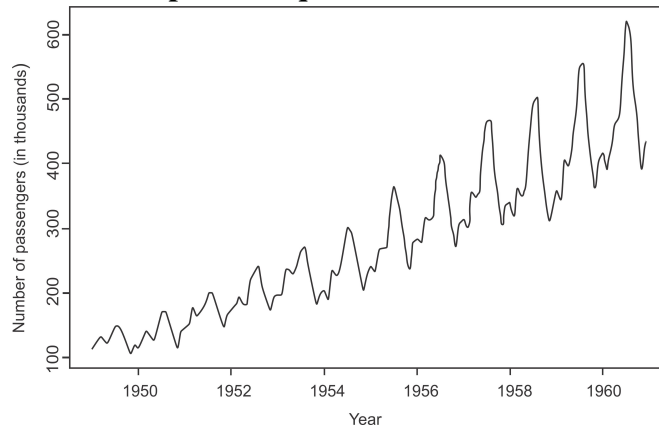
### 3.2 PREVISÃO DE SÉRIES TEMPORAIS

As séries temporais são um conjunto de observações ordenadas ao longo do tempo (JAŠEK; SZMIT; SZMIT, 2013) em que alguns componentes podem estar presentes, tais como: nível, tendência, sazonalidade e aleatoriedade, explicados a seguir. O nível é uma média acerca da qual as observações variam. Tendência é um aumento ou diminuição consistente de valores de uma série temporal ao longo do tempo. A sazonalidade é uma variação cíclica que pode ser observada. Por fim, a aleatoriedade é um comportamento que não é produzido por nenhum dos componentes acima mencionados.

Os componentes de uma série temporal também podem interagir umas com as outras,

produzindo comportamentos como mostrado na Fig. 5, em que tendência e sazonalidade estão presentes e têm uma interação multiplicativa, ou seja, o comportamento crescente nos valores induzidos pela tendência provocou variações sazonais mais fortes.

**Figura 5 – Série temporal na qual a tendência afeta a sazonalidade.**



Fonte: (CHATFIELD, 2000).

Para estimar valores em uma série temporal é importante entender como seus valores variam, encontrar um modelo matemático que se adapte a eles e usar esse modelo para prever valores alguns passos à frente no tempo. Por exemplo, se as observações variarem em torno de uma média e tais variações são fortes, um modelo apropriado pode ser o Alisamento Exponencial Simples, ou Simple Exponential Smoothing (SES) em inglês, que diminui exponencialmente os pesos de observações mais antigas. A previsão de uma observação através desse modelo é calculada através da equação  $\bar{Z}(t) = \alpha Z(t) + (1 - \alpha)\bar{Z}(t - 1)$ , onde  $Z(t)$  é uma observação da série temporal  $Z$  no tempo  $t$  e  $\bar{Z}(t)$  é a estimativa para valores de  $Z$  mais recentes que  $Z(t)$ . A constante  $\alpha$  dita a importância das observações mais recentes e seu valor reside no intervalo  $(0,1)$ .

Vários modelos de previsão importantes são baseados no alisamento exponencial, sendo Holt e Holt-Winters os mais proeminentes dessa classe por causa de seu bom desempenho comparado a outros modelos (MAKRIDAKIS *et al.*, 1982) (CHATFIELD; YAR, 1988). A diferença notável entre os dois modelos é que Holt-Winters propõe-se a estimar a variação sazonal da série temporal ao qual é aplicado. No entanto, neste trabalho exploraremos unicamente o modelo Holt, haja vista que as séries temporais abordadas nos experimentos não são longas o suficientes para permitir a detecção de sazonalidades.

O modelo Holt ajusta-se a séries temporais usando duas componentes exponencialmente alisadas: nível e tendência. Para estimar uma observação  $Z(t)$  de uma série temporal, computa-se  $\hat{Z}_t(h)$  através da Equação 3.1, sendo  $t$  um tempo conhecido na série temporal e  $h$  o



horizonte de previsão, ou seja, quantos passos à frente de  $t$  o modelo deverá estimar (MORETTIN; TOLOI, 1981). O nível  $L_t$  da série é calculado através da Equação 3.2. A tendência  $T_t$  da série, por sua vez, é calculada através da Equação 3.3. Holt usa duas constantes de alisamento exponencial,  $\alpha$  e  $\beta$ , uma para cada componente da série temporal a ser estimada. A tarefa de encontrar valores apropriados para essas constantes, no entanto, é algo que pode ser considerado uma desvantagem do modelo, pois adiciona um desafio ao seu uso (LAHIRI, 1979).

$$\hat{Z}_t(h) = L_t + hT_t \quad (3.1)$$

$$L_t = \alpha Z_t + (1 - \alpha)(L_{t-1} + T_{t-1}) \quad (3.2)$$

$$T_t = \beta(L_t - L_{t-1}) + (1 - \beta)T_{t-1} \quad (3.3)$$

Neste trabalho, o modelo Holt é explorado para estimar o nível de séries temporais de Errored Blocks Counter em intervalos de 1 segundo, e a partir da análise da tendência dos valores, ou seja, da detecção de um comportamento de aumento ou decréscimo na degradação do desempenho da rede, estima-se valores futuros de EBC. Caso estime-se que o número de EBC no próximo segundo ultrapassará o limiar de 15% dos blocos transmitidos, deve-se estar atento à possibilidade de esse comportamento se manter por tempo demais, o que provocaria a interrupção no serviço de transporte de dados da rede OTN.

Com a ajuda de modelos de previsão, a análise de séries temporais pode ser uma importante aliada no monitoramento preventivo de desempenho. Por isso, sendo o desenvolvimento de Errored Blocks em redes OTN uma das formas de medir o comportamento de seu desempenho, neste trabalho exploramos o uso de modelos matemáticos para determinar o comportamento futuro do desempenho dessas redes, visando detectar de forma suficientemente acurada e antecipada sérias degradações em seu desempenho, sendo essa uma forma de colaboração inteligente com as operações preventivas realizadas pelos profissionais responsáveis pela gerência de redes OTN e por mecanismos automáticos de recuperação.

### 3.3 CADEIAS DE MARKOV

Como explica Jeonghoon Mo em seu livro (MO, 2010), cadeias de Markov são poderosas ferramentas matemáticas para a modelagem de sistemas dinâmicos que mudam de estado ao longo do tempo, e sua popularidade atribui-se a sua simplicidade, flexibilidade e facilidade de processamento.

Cadeias de Markov são definidas por um espaço de estados  $G$  e uma matriz  $M$  de probabilidades de transição entre esses estados. Uma importante propriedade dessas matrizes é calcular a  $n$ -ésima potência de  $M$  com  $n$  tendendo ao infinito, dado por  $\lim_{n \rightarrow \infty} M^{(n)}$ , o que faz as probabilidades de transição convergirem, atingindo um equilíbrio independente do estado inicial, como exemplificado na Equação 3.4 (MO, 2010). Esse equilíbrio é conhecido como o estado estável  $\pi$  de uma cadeia de Markov. Na prática,  $\pi$  é um vetor de probabilidades e seu conteúdo é geralmente interpretado como o tempo que o sistema permanecerá em cada estado no longo prazo.

$$M = \begin{bmatrix} 0.6 & 0.4 \\ 0.25 & 0.75 \end{bmatrix} M^{16} = \begin{bmatrix} 0.3846 & 0.6154 \\ 0.3846 & 0.6154 \end{bmatrix} \quad (3.4)$$

Ao invés de elevar  $M$  a potências suficientemente altas para encontrar  $\pi$ , outros métodos podem ser usados para facilitar essa tarefa, e um deles é resolver o sistema de equações  $\pi M = \pi$  (MO, 2010). De acordo com um resultado derivado do teorema de Perron-Frobenius, seja ele que matrizes de cadeias de Markov sempre possuem o autovalor  $\lambda = 1$ , o problema de encontrar  $\pi$  pode ser reduzido ao problema de encontrar o autovetor associado ao autovalor  $\lambda = 1$  da matriz de probabilidades  $M$ . Esse vetor é às vezes referido como autovetor característico de uma matriz Markoviana  $M$ .

Neste trabalho de mestrado, propomos uma cadeia de Markov para determinar probabilisticamente se as comunicações em uma OTN permanecerão em um estado de degradação de desempenho, fornecendo uma avaliação qualitativa do desempenho da rede no longo prazo.

Com o uso dos modelos matemáticos apresentados, o mecanismo de alerta proposto pode analisar séries temporais de Errored Blocks Counter (EBC) e realizar inferências estatísticas para se antecipar a períodos de degradação intensa em redes OTN, ajudando operadores de rede a prevenir interrupções no serviço de transporte de dados de forma inteligente e automatizada.

## 4 PROPOSTA

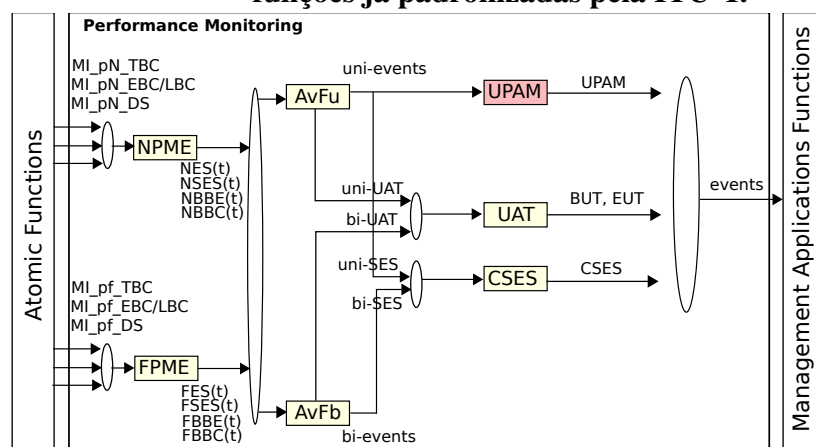
### 4.1 MECANISMO DE ALERTA DE DESEMPENHO PARA REDES OTN

Nesta seção apresentamos o mecanismo de alerta proposto, o Urgent Preventive Alert Mechanism (UPAM), que monitora o desempenho da rede e estima seu comportamento através de dois modelos matemáticos. Independentemente, cada modelo é responsável pela análise estatística e geração de previsões sobre o comportamento da rede e, em conjunto, eles são usados para fornecer um alerta confiável de duas etapas da provável ocorrência de degradação inaceitável de desempenho no futuro próximo.

#### 4.1.1 O Urgent Preventive Alert Mechanism (UPAM)

Nesta seção apresentamos o Urgent Preventive Alert Mechanism (UPAM), um mecanismo que computa informações estatísticas de desempenho no próprio Elemento de Rede OTN e dispara alertas preventivos de degradação do desempenho. Do ponto de vista funcional, esse mecanismo é implementado como uma Função de Monitoramento de Desempenho, que interage com funções atômicas para receber Contadores de Errored Blocks e Transmitted Blocks (EBC e TBC) em intervalos de um segundo, como mostrado na Figura 6. Quando um estado de degradação do desempenho é detectado, o UPAM gera um evento a ser registrado por aplicações de gerenciamento de rede, que podem pertencer à gerência de falhas ou desempenho, e que podem usar a ocorrência desse evento para ativar um caminho de proteção ou executar sua restauração através do cálculo de uma nova rota. A Figura 6 apresenta como o UPAM estende o

**Figura 6 – A Função de Monitoramento de Desempenho UPAM e sua integração com as funções já padronizadas pela ITU-T.**



Fonte: Elaborado pelo autor.

conjunto de Funções de Monitoramento de Desempenho padronizados pela ITU-T, mostrando como ele se relaciona com as outras funções e emite os eventos de alerta.

Para evitar problemas de escalabilidade com o uso do mecanismo, o UPAM foi projetado para analisar conjuntos curtos e de tamanho fixo de Errored Blocks Counter coletados em intervalos de um segundo, o que reduz a precisão de modelos de suavização exponencial que detectam a sazonalidade de uma série temporal, como o Holt-Winters. Por isso, o UPAM concentra-se na tendência de crescimento, decrescimento ou estabilidade dos contadores de Errored Blocks com o passar do tempo. O número de leituras de EBCs na série temporal usada pelos modelos é chamado de tamanho da amostra, ou *sample size* em inglês, e é efetivamente o tamanho das séries temporais usadas pelos modelos para gerar previsões. Tamanhos apropriados de amostra serão discutidos no Capítulo 5.

Após cada segundo de monitoramento, o modelo Holt analisa o passado recente dos EBCs e estima o número de Errored Blocks esperados para o próximo segundo de operação. O UPAM registra caso o valor estimado supere o limiar de 15% do total de blocos recebidos. Além disso, modelamos o monitoramento de desempenho em redes OTN como uma cadeia de Markov e, em paralelo com as estimativas fornecidas pelo modelo Holt, a cadeia de Markov estima qual a probabilidade de o desempenho da rede se manter em estado de degradação no longo prazo, e caso essa probabilidade exceda um limiar, o UPAM registra essa estimativa. Caso em um dado segundo de operação o UPAM registrar que ambos os modelos foram sensibilizados, isso indica que é alta a probabilidade de a rede entrar em estado de indisponibilidade nos próximos segundos de operação, e um alerta UPAM é disparado.

A seguir apresentamos o modelo de cadeia de Markov proposto para uso em conjunto com o modelo de previsão Holt, e mais adiante as ações recomendadas face às estimativas dos modelos e a um alerta UPAM.

#### 4.1.1.1 Cadeia de Markov Proposta

A partir de uma sequência de EBs contados nos últimos intervalos de um segundo, o UPAM classifica cada segundo como Non-Errored Second (NES), Errored Second (ES) ou Severely Errored Second (SES), seguindo a recomendação ITU-T G.7710 (INTERNATIONAL TELECOMMUNICATION UNION, 2012a). A partir de transições entre esses intervalos, o UPAM cria uma sequência  $S$  de estados de acordo com o mapeamento apresentado na Tabela 2. Esses estados formam o espaço de estado  $G$ : *Increasing Network Performance* ( $S_1$ ), *Stable*

**Tabela 2 – Mapeamento entre transições segundo-a-segundo e estados do modelo de cadeia de Markov proposto**

Transição	Estado	Descrição
NES to NES	Stable Network Performance ( $S_2$ )	Rede saudável e estável
NES to ES	Stable Network Performance ( $S_2$ )	Desempenho pouco degradado
NES to SES	Decreasing Network Performance ( $S_3$ )	Forte e súbito aumento no número de Errored Blocks
ES to NES	Increasing Network Performance ( $S_1$ )	Errored Blocks pararam de acontecer
ES to ES	Stable Network Performance ( $S_2$ )	Errored Blocks detectados em quantidade aceitável
ES to SES	Decreasing Network Performance ( $S_3$ )	Número de EBs cresceu para quantidades preocupantes
SES to NES	Increasing Network Performance ( $S_1$ )	Número de EBs decaiu substancialmente
SES to ES	Increasing Network Performance ( $S_1$ )	Número de EBs reduziu para níveis aceitáveis
SES to SES	Decreasing Network Performance ( $S_3$ )	Risco iminente de indisponibilidade

Fonte: Elaborado pelo autor

*Network Performance* ( $S_2$ ) e *Decreasing Network Performance* ( $S_3$ ). Foram utilizados nomes em inglês para os estados do modelo visando seu uso direto em publicações de alcance internacional.

A partir da sequência de estados em  $S$ , o UPAM cria uma matriz de transições de estados  $M$  com as probabilidades de transitar do estado  $S_p$  para  $S_q$ , sendo  $\{S_p, S_q\} \in \{S_1, S_2, S_3\}$ . No entanto, se nem todos os estados estiverem presentes em  $M$ , aplicam-se várias otimizações e deve-se ter cuidado para garantir que  $M$  seja uma matriz Markoviana. Se nenhuma transição conduzir ao estado  $S_3$ , nenhuma computação adicional é necessária e um alerta não é necessário. Se todas as transições levam a  $S_3$ , nenhuma outra computação é necessária e um alerta deve ser registrado imediatamente pelo sistema. Se nenhuma dessas circunstâncias for verificada e quando as transições para todos os estados estiverem presentes,  $M$  contém as probabilidades de transição entre todos os estados de  $G$ , caso contrário, apenas a transição entre estados  $S_3$  e  $S_1$  ou  $S_2$  estarão presentes.

Para estimar o estado futuro do sistema modelado de acordo com o espaço de estados  $G$ , é usada a abordagem da computação do autovetor característico de  $M$  para encontrar a probabilidade do estado estacionário  $\vec{\pi}$ . Se o vetor  $\vec{\pi}$  indicar que a probabilidade de o sistema estar no estado  $S_3$  no futuro for maior que 50%, então ela é maior que a soma das probabilidades de o sistema estar no estado  $S_2$  e  $S_3$ , sendo assim o UPAM registra que o modelo de cadeia de Markov indicou que uma degradação no desempenho da rede tende a continuar ocorrendo no longo prazo. Um pseudo-algoritmo mostrando como essa abordagem pode ser implementada é apresentada no Algoritmo 1.

---

**Algoritmo 1:** Retorna se um caminho ODU tende a permanecer em estado de degradação de desempenho utilizando a cadeia de Markov proposta

---

**Input:** Sequência de estados  $S$

**Output:** true or false

```

1: if  $S_{i+1} \neq S_3, \forall S_i \in S$  then
2:   return false
3: else if  $S_{i+1} == S_3, \forall S_i \in S$  then
4:   return true
5: end if
6:  $M \leftarrow \emptyset$ 
7: if  $(\exists S_{i+1} == S_2, \forall S_i \in S)$  and  $(\exists S_{i+1} == S_3, \forall S_i \in S)$  then
8:    $M \leftarrow \text{MarkovMatrix}_{3 \times 3}(S)$ 
9: else
10:   $M \leftarrow \text{MarkovMatrix}_{2 \times 2}(S)$ 
11: end if
12:  $\vec{p} \leftarrow \text{Eigenvector}(M, \lambda = 1)$ 
13: if  $\vec{p}[S_3] > 0.5$  then
14:   return true
15: end if
16: return false

```

---

#### 4.1.1.2 Os Alertas UPAM

Sempre que o modelo Holt registra que espera-se que um SES ocorra no próximo segundo de monitoramento, não há garantias de que essa circunstância se manterá por tempo suficiente para provocar indisponibilidade do caminho. O modelo de cadeia de Markov, por sua vez, pode registrar que espera-se um estado de queda de performance em duas situações: quando a rede passa a detectar a ocorrência de Errored Blocks ou de Severely Errored Blocks. Se esse modelo registra que o estado de queda de performance provavelmente predominará no longo prazo e o modelo Holt registra que um Severely Errored Second é esperado para o próximo minuto de operação, então a rede está diante de uma condição severa e um alerta UPAM é registrado pela função de monitoramento, onde é urgente a aplicação de medidas preventivas antes que a ocorrência de Severely Errored Seconds se mantenha por tempo suficiente para provocar a indisponibilidade do caminho monitorado e disparar um alarme correspondente a esse evento. Sendo assim, diante de um alerta UPAM propomos que o plano de controle ative o

caminho de proteção imediatamente, e que os operadores da rede procedam à manutenção de equipamentos ou fibras degradados.

## 5 EXPERIMENTOS

Para medir a antecipação promovida pelo mecanismo proposto, testamos os modelos com vários parâmetros e, após encontrar uma combinação que maximize a acurácia e minimize a taxa de falso-positivos na detecção de períodos de indisponibilidade, medimos com que antecedência o uso combinado dos modelos detectou a chegada de períodos de indisponibilidade na rede. Os parâmetros que serão utilizados para medir a acurácia e a taxa de falso-positivos serão: o tamanho da amostra, ou seja, com quantas medições recentes de Errored Blocks os modelos realizarão as previsões; e as constantes de alisamento  $\alpha$  e  $\beta$  do modelo Holt.

A probabilidade de ocorrer um Errored Block, ou seja, de haver pelo menos um bit incorreto em um quadro OTN, está diretamente ligada à relação sinal-ruído da luz na fibra, ou Signal-to-Noise Ratio (SNR). Quanto maior a potência do ruído gerado por amplificadores e dispersões em relação à potência do sinal transmitido, maior a probabilidade de a luz ser incorretamente convertida no bit efetivamente enviado pelo transmissor. As potências do sinal e do ruído são comumente apresentadas em dB e a probabilidade de um bit ser incorretamente traduzido no momento de sua recepção é denominada Bit Error Rate (BER). As relações entre o SNR de um caminho, a probabilidade Bit Error Rate e a consequente probabilidade de um Errored Block ocorrer serão apresentadas na Seção 5.3 deste capítulo.

### 5.1 METODOLOGIA

A seguir apresentamos a metodologia usada para a seleção da quantidade de tempo usada pelos modelos para gerar suas estimativas, que chamaremos de tamanho da amostra, além das constantes  $\alpha$  e  $\beta$  usadas pelo modelo Holt.

#### 5.1.1 Seleção do Tamanho das Amostras

A quantidade de observações em uma série temporal, ou o tamanho da amostra usada pelos modelos, é de suma importância, pois pouca informação pode limitar a precisão dos modelos de previsão, mas dispor de muitos dados pode tornar-se um problema de escalabilidade em equipamentos de rede. Sendo assim, nos experimentos desse trabalho medimos a partir de quantos segundos de monitoramento a acurácia e taxa de falso-positivos se estabilizam, ou seja, deixam de variar ao aumentarmos o tamanho da amostra. Objetiva-se encontrar um balanço entre o tamanho da amostra e a precisão dos alertas do UPAM. Os dois modelos foram testados com



tamanhos de amostra de 10, 20, 30, 40, 50 e 60 segundos.

No caso do modelo Holt, as métricas de acurácia e taxa de falso-positivos dependem não só do tamanho da amostra, mas também da combinação das constantes  $\alpha$  e  $\beta$ . Sendo assim, para entender como essas constantes influenciam nas métricas usadas, para cada tamanho de amostra, calculamos a média das acurácias obtidas com varias combinações de  $\alpha$  e  $\beta$  variando entre 0.1, 0.5 e 0.9. O mesmo procedimento foi usado para a taxa de falso-positivos. Assim, para cada tamanho de amostra apresentamos as médias das métricas com intervalo de confiança de 95%, o que permite entender o impacto da variação dos parâmetros nas métricas utilizadas.

### 5.1.2 Seleção das Constantes $\alpha$ e $\beta$

Após selecionar um tamanho de amostra apropriado para uso no UPAM, buscamos entender como a variação de cada parâmetro  $\alpha$  e  $\beta$  afeta a acurácia e a taxa de falso-positivos do modelo Holt para, por fim, selecionar a melhor combinação de  $\alpha$  e  $\beta$  para uso no UPAM.

### 5.1.3 Análise da Antecipação à Indisponibilidade

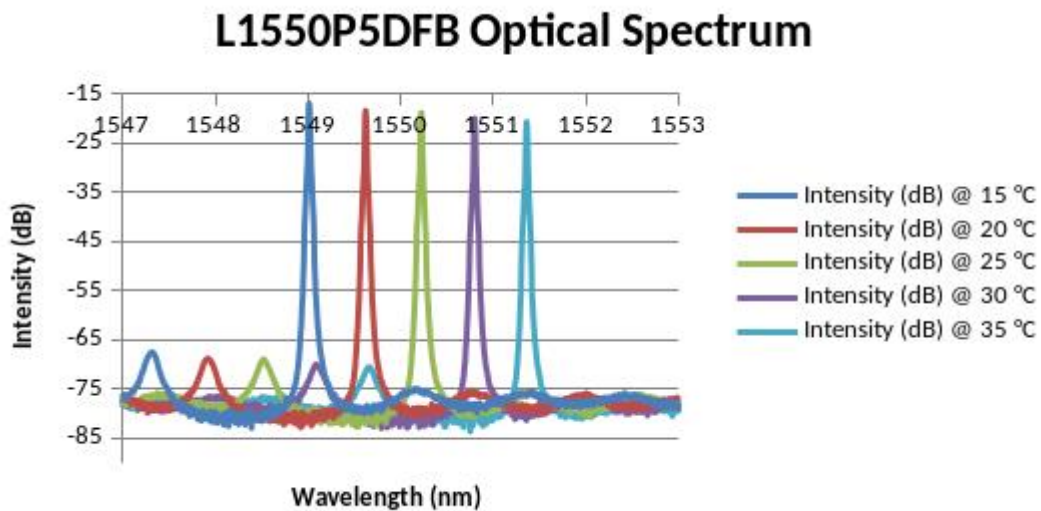
Após a seleção do tamanho das amostras e dos das constantes  $\alpha$  e  $\beta$ , apresentaremos a antecipação à falha promovida pelo mecanismo UPAM utilizando os modelos com os parâmetros selecionados.

## 5.2 CENÁRIO DE TESTES

Apesar de termos contatado diversas empresas para fornecimento de medições de Errored Blocks em redes reais, não obtivemos êxito em obter esses dados. Por isso, baseamo-nos na literatura especializada para produzir um cenário simulado onde o mecanismo de alertas proposto pudesse ser posto à prova.

O cenário de testes proposto basea-se na situação descrita na seção 5.9 do livro Optical Networks (RAMASWAMI; SIVARAJAN; SASAKI, 2009), na qual o laser transmissor é configurado para operar a uma temperatura, mas à medida que sua temperatura varia, o comprimento de onda transmitido também varia, comportamento conhecido como *wavelength-drift*. Como o receptor é configurado para operar de acordo com a configuração do laser, à medida que o comprimento de onda que chega ao receptor está diferente do configurado inicialmente, tem-se uma perda ou ruído em relação a como o sinal deveria estar. Quando pequeno, o *wavelength-drift* não causa tantos problemas e, na prática, como os lasers possuem um cooler

**Figura 7 – Intensidade do sinal transmitido pelo comprimento de onda no laser L1550P5DFB da Thorlabs.**



Fonte: Thorlabs

que controla sua temperatura, grandes variações no comprimento de onda não acontecem com grande frequência. No entanto, caso problemas nos resfriamento sejam acompanhados de variações na temperatura ambiente, esse pode tornar-se um severo problema para o desempenho da rede.

Nas cidades brasileiras, as variações de temperatura durante o dia podem ser grandes o suficiente para provocar indisponibilidade na rede por *wavelength – drift*. Para os experimentos, tomamos as variações de temperatura ocorridas no mês de setembro de 2016 na cidade de Curitiba, Paraná - Brasil, onde a temperatura chegou a variar 14 °C em relação à temperatura média do mês. Os dados de temperatura de diversas cidades brasileiras são disponibilizados pelo Instituto Nacional de Pesquisas Espaciais (INPE) em seu website.

Além disso, o efeito na variação da temperatura no comprimento de onda transmitido varia de acordo com o laser utilizado. Para efeito de testes, selecionamos o laser L1550P5DFB da fabricante Thorlabs, que transmite com um comprimento de onda de 1550nm, a uma largura de banda de 2.5Gbps e com coeficiente térmico de 0.12nm/°C, sendo essa a variação no comprimento de onda a cada grau Celsius a mais ou a menos da temperatura configurada de operação. A intensidade do sinal em dB de acordo com o comprimento de onda transmitido em cada temperatura é apresentado na Figura 7. A média da temperatura em Curitiba no período selecionado foi de 14.87 °C, por isso selecionamos a configuração de operação do laser em questão em 15 °C.

Em um dado momento de operação da rede, a perda em dB é medida como a

diferença entre a intensidade do sinal naquele momento e a intensidade do sinal operando nas condições ótimas, nesse caso com a temperatura do laser a 15°C. Para simplificar a simulação, assumimos que o laser opera à temperatura ambiente. Mesmo que a relação entre temperatura ambiente e de operação do laser seja diferente de 1, o objetivo do experimento é fazer o UPAM responder às variações de temperatura, e como a relação entre  $\text{nm}/^\circ\text{C}$  é a mesma independente da temperatura de operação do laser, essa assunção não traz prejuízos metodológicos. Com o uso de medições reais de temperatura de operação dos laser, no entanto, poderemos realizar experimentos com maior precisão nesse sentido.

### 5.3 SIMULAÇÃO DO CENÁRIO DE TESTES

Utilizando as medições de temperatura da cidade de Curitiba e os dados do laser L1550P5DFB da Thorlabs, simulamos 50 horas de operação de um caminho ODU, especificamente contemplando o intervalo onde houve a maior variação de temperatura na cidade. A relação sinal-ruído tomada foi estritamente óptica, ou seja, usando somente a intensidade do sinal transmitido e a intensidade do sinal no receptor, por isso essa relação é denominada Optical Signal-to-Noise Ratio (OSNR), e difere-se do SNR pois esse é medido após a conversão óptico-elétrica, mas possui o mesmo sentido para os propósitos desta pesquisa.

O simulador foi implementado na linguagem R. Inicialmente computou-se um OSNR de saída seguindo uma distribuição normal de média 60.53 e variância 0.1. Esse é o melhor caso, onde a potência do sinal é máxima, ou seja, com a temperatura em 15°C e transmitindo com comprimento de onda 1549.012nm, sendo o OSNR próximo a 0 quando a diferença entre a temperatura ambiente e a configurada (15°C) atinge os maiores picos ( $\Delta T$  até -14°C nesse cenário).

No livro *DWDM Network Designs and Engineering Solutions* (GUMASTE; ANTONY, 2003) discute-se o cálculo do OSNR em uma rede, desde a transmissão do sinal pelo laser até o fotoreceptor, passando pelos estágios ou seções, compostas por um trecho de fibra óptica e um amplificador, que adicionam perda ao sinal. Fazendo uso de algumas simplificações, a equação 4-13 de (GUMASTE; ANTONY, 2003) apresenta uma estimativa do OSNR em cada estágio  $i$  dada a intensidade do sinal que entra no estágio  $P_{in}$ , a potência do ruído adicionado pelo trecho  $NF_{stage}$ , a constante de Plank  $h = 6.6260 \times 10^{-34}$ , a frequência  $\nu$  e a largura de banda  $\Delta f$ .

Essa equação é aqui apresentada na Equação 5.1.

$$OSNR_i = \frac{P_{in}}{NF_{stage} h\nu \Delta f} \quad (5.1)$$

Uma importante medida usada em sistemas de telecomunicações é o  $E_b/N_0$ , definida como a energia por bit ( $E_b$ ) sobre a densidade espectral do ruído ( $N_0$ ), e é usada para medir a taxa de sinal ruído em sistemas de comunicação digitais. Essa medida é comumente utilizada para medir a taxa de bits incorretos, ou Bit Error Rate (BER), dada uma modulação do sinal digital. A equação 7.18 do livro *Optical Fiber Telecommunications* (KAMINOW; LI; WILLNER, 2013) apresenta uma relação entre o sinal-ruído óptico na forma de OSNR e digital na forma de  $E_b/N_0$ , que pode ser observada na Equação 5.2, onde  $R$  é a taxa de transmissão e  $\Delta\nu$  é a largura de banda do sinal. Nos experimentos aqui realizados foram utilizados os valores  $R = 2.5Gbps$  e  $\Delta\nu = 50GHz$ .

$$E_b/N_0 = 10\log_{10}(\Delta\nu/R) + OSNR_{dB} \quad (5.2)$$

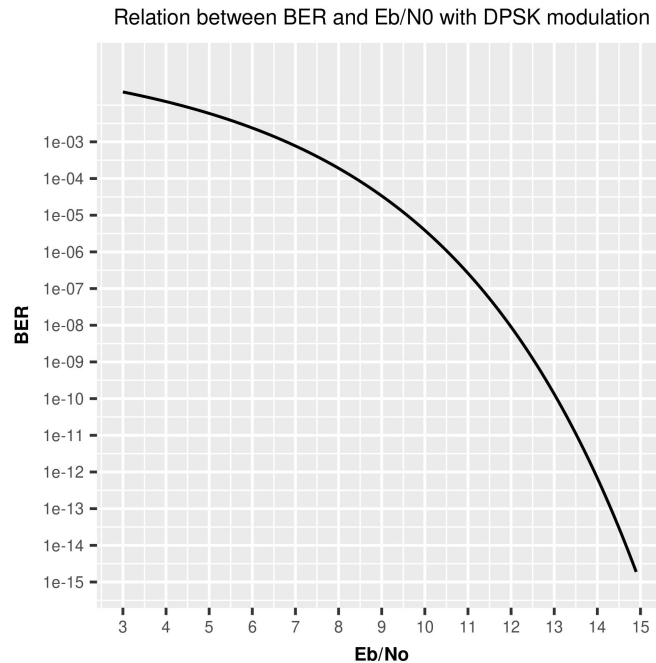
A partir das medidas de  $E_b/N_0$  e sabendo qual a modulação aplicada no sinal digital, pode-se calcular o Bit Error Rate correspondente e, a partir dessa medida, calcular a probabilidade de um bloco ODU conter bits incorretos e, conseqüentemente, ser um Errored Block. Neste trabalho assumimos a modulação Binary Phase-Shift Keying (BPSK), cuja relação entre BER e  $E_b/N_0$  é calculada pela Equação 5.3 e ilustrada na Figura 8. Normalmente configura-se uma rede óptica para operar com um BER de pelo menos  $1.0 \times 10E^{-12}$  e nunca maior que  $1.0 \times 10E^{-6}$ , pois a probabilidade de um Errored Block ocorrer torna-se demasiadamente elevada.

$$BER = \frac{1}{2} \operatorname{erfc}(\sqrt{E_b/N_0}) \quad (5.3)$$

Para computar o número de blocos com erro durante cada segundo de monitoramento, em vez de efetivamente gerar bits aleatórios para simular quadros OTN, utilizamos um gerador de eventos aleatórios onde cada evento é um quadro (ou bloco), e a probabilidade de um bloco conter pelo menos um bit errado é dada por:  $P_{EB} = 1 - (1 - BER)^N$ , sendo  $N$  o número de bits em um quadro.

Nos experimentos, considerou-se uma taxa de transmissão de 2.5Gbps, sendo a nomenclatura da camada ODU operando a essa taxa definida pela ITU-T como ODU1. Na

**Figura 8 – Relação entre Bit Error Rate e SNR medido em  $E_b/N_0$ , calculada através da Equação 5.3.**



Fonte: Elaborado pelo autor

camada ODU1 o número de bits cobertos pelo campo BIP-8 de seu cabeçalho contém  $N = 121920$  bits, e a essa taxa são enviados 20421 quadros ODU1 por segundo, sendo 3064 o limite de 15% dos quadros transmitidos necessários para indicar um segundo de operação como Severely Errored Second (INTERNATIONAL TELECOMMUNICATION UNION, 2003).

Por fim, a partir dos valores de OSNR e com o aparato matemático que nos permite computar a probabilidade de um quadro ODU1 ter sido recebido com bits incorretos, para cada simulação desse cenários geramos 20421 eventos aleatórios com probabilidade  $P_{EB}$  de ser um Errored Block para cada segundo de operação, totalizando 3 675 780 000 (aproximadamente 3.7 bilhões) de eventos durante toda a simulação. A partir desses dados, para cada simulação gerou-se uma série temporal com 50 horas informando o número de Errored Blocks em cada segundo de operação, sendo usado como entrada para os modelos de previsão usados no mecanismo de alertas UPAM.

## 6 RESULTADOS

Neste capítulo apresentamos a aplicação da metodologia proposta na Seção 5.1 para a escolha dos parâmetros usados pelos modelo Holt e pela cadeia de Markov proposta. Por fim apresentamos a antecipação promovida pela combinação dos modelos realizada pelo mecanismo UPAM, responsável por coletar a amostra de Errored Blocks Counter e aplicar os modelos para determinar quando espera-se que um período de indisponibilidade ocorrerá no futuro breve.

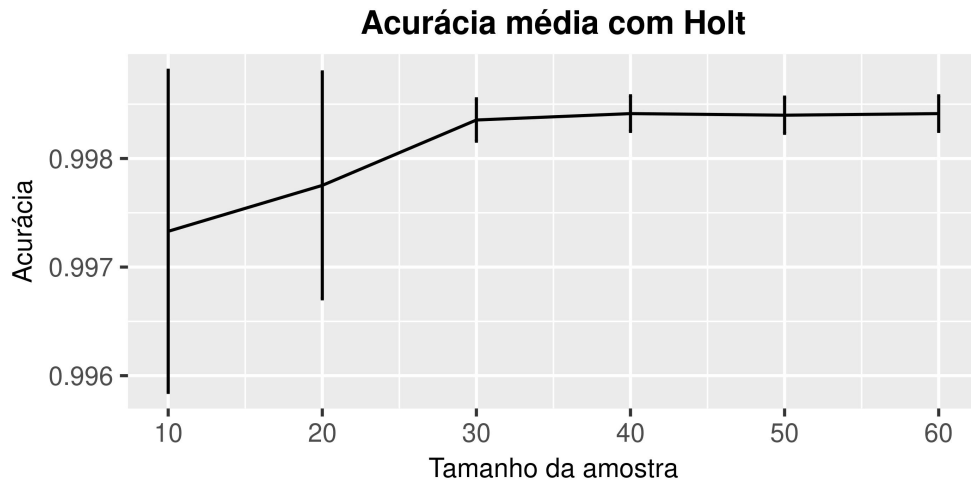
### 6.1 ESCOLHA DO TAMANHO DA AMOSTRA

A escolha do tamanho da amostra para uso pelo modelo Holt baseiou-se na análise da acurácia média e na taxa média de falso-positivos médios na detecção de Unavailable Seconds (UaS), para cada tamanho de amostra, seguindo a metodologia apresentada na Seção 5.1. A Figura 9 apresenta a acurácia média para cada tamanho de amostra com do intervalo de confiança de 95%. A Figura 10 apresenta o mesmo com a métrica taxa de falso-positivos, ou False-Positive Rate (FPR) em inglês. Da análise dessas figuras, observa-se que com 30 segundos de monitoramento as constantes de alisamento passam a influenciar pouco nas métricas. Além disso, a partir desse tamanho de amostra a quantidade de dados disponíveis para o modelo não causa impacto notável nas métricas utilizadas. Baseado nesses resultados, entendemos que um tamanho apropriado de amostra deve ter pelo menos 30 segundos de monitoramento, e para uso nos próximos passos deste experimento, escolhemos um tamanho de amostra igual a 40 segundos.

No caso do modelo de cadeia de Markov proposto, nas Figuras 11 e 12 não se nota uma convergência clara da acurácia de da taxa de falso-positivos ao aumentar-se o tamanho da amostra, mas nota-se claramente que essas métricas são melhores para tamanhos maiores de amostra. O problema encontrado, no entanto, é que ao selecionarmos um tamanho de amostra igual ao usado no modelo Holt, ou seja, os 40 segundos mais recentes de monitoramento, a antecipação a falha realizada pelo modelo UPAM era muito baixa.

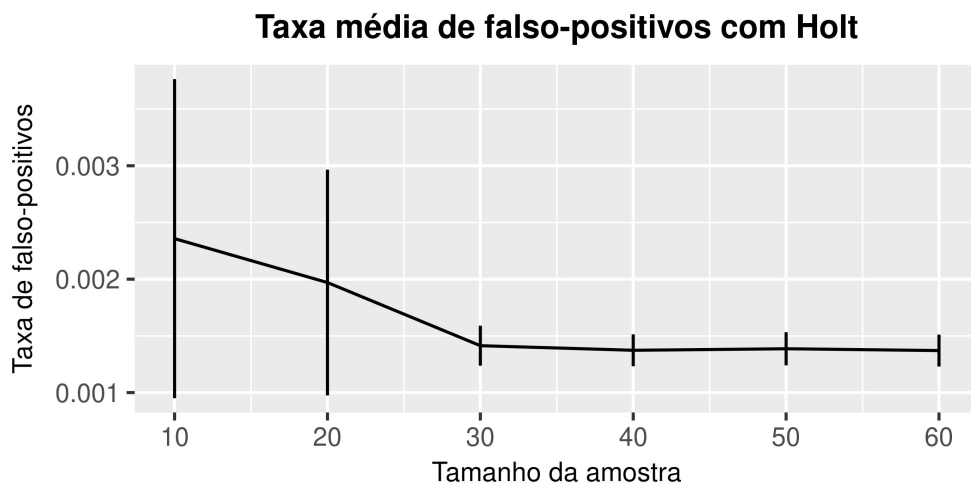
Isso ocorre porque, como o tempo hábil para a gerência de desempenho determinar um caminho como indisponível é 10 segundos, o modelo de cadeia de Markov não pode estar muito longe desse valor, caso contrário ele pode levar tempo demais para notar que a rede está em estado de redução de desempenho. Nesse modelo, quanto maior o tamanho da amostra, menos sensível ele é. Por isso, após alguns experimentos variando o tamanho da amostra para esse modelo com valores próximos, mas maiores que 10 segundos, selecionamos o tamanho da

**Figura 9 – Acurácias médias obtidas na detecção de Unavailable Seconds (UaS) para cada tamanho de amostra utilizando o modelo Holt com  $\alpha$  e  $\beta$  variando entre 0.3, 0.5 e 0.9.**



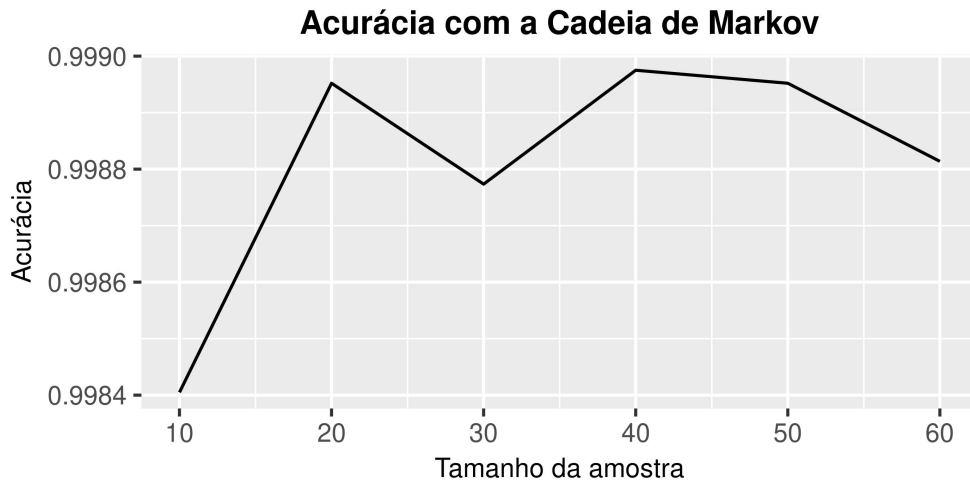
Fonte: Elaborado pelo autor.

**Figura 10 – Taxa de falso-positivos médias obtidas na detecção de Unavailable Seconds (UaS) para cada tamanho de amostra utilizando o modelo Holt com  $\alpha$  e  $\beta$  variando entre 0.3, 0.5 e 0.9.**



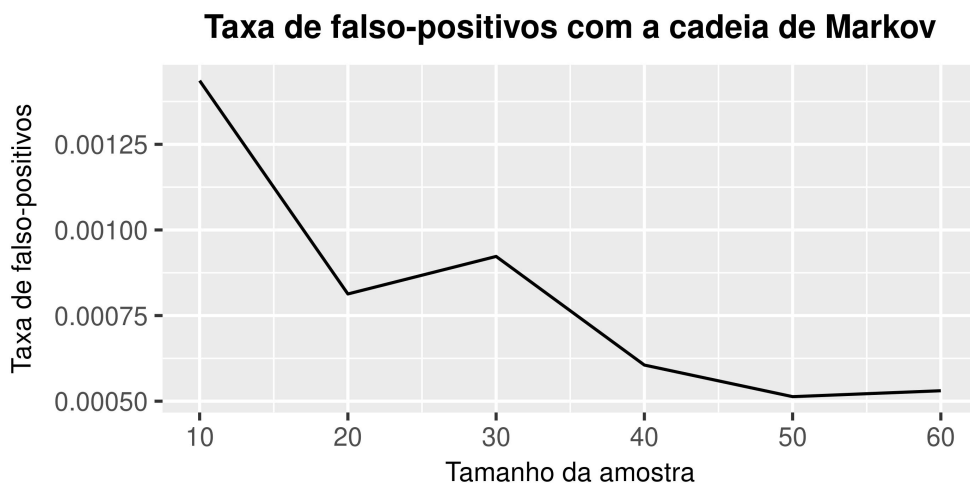
Fonte: Elaborado pelo autor.

**Figura 11 – Acurácias obtidas para cada tamanho de amostra utilizando o modelo de cadeia de Markov proposto na detecção de Unavailable Seconds (UaS).**



Fonte: Elaborado pelo autor.

**Figura 12 – Taxa de falso-positivos obtidas para cada tamanho de amostra utilizando o modelo de cadeia de Markov proposto na detecção de Unavailable Seconds (UaS).**



Fonte: Elaborado pelo autor.

amostra em 14 segundos de monitoramento recentes.

## 6.2 CONSTANTES DE ALISAMENTO $\alpha$ E $\beta$

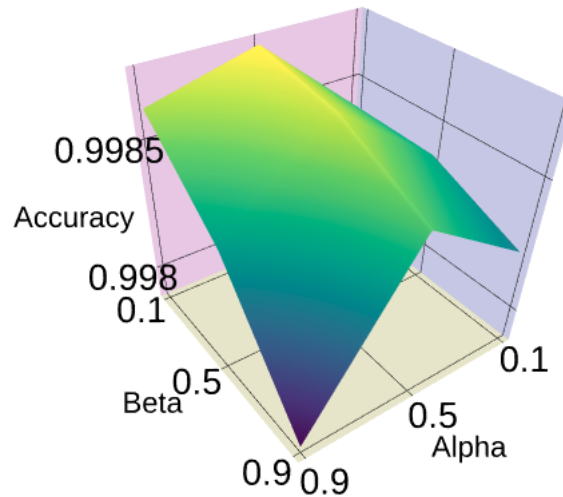
Após a selecção de um tamanho de amostra apropriado para aplicação do modelo Holt no UPAM, prosseguimos para a selecção dos parâmetros  $\alpha$  e  $\beta$  que maximizem a acurácia e minimizem a taxa de falso-positivos na detecção de Unavailable Seconds (UaS), ou seja, os segundos nos quais o caminho estava indisponível.

As Figuras 13 e 14 apresentam o impacto dessas constantes na acurácia e taxa de falso-positivos em uma simulação utilizando 40 segundos de tamanho de amostra. Da análise



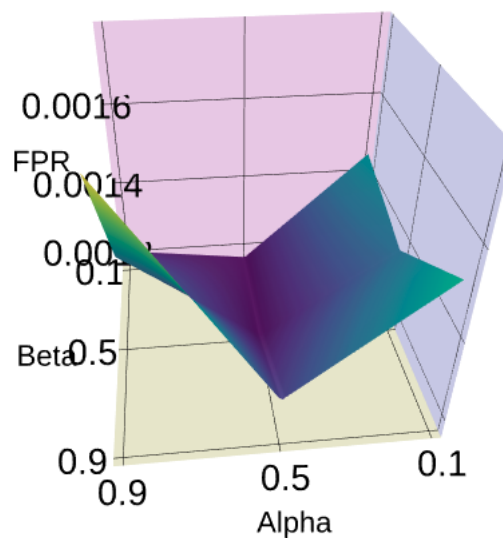
dessas figuras, nota-se que os melhores resultados foram obtidos quando  $\alpha = 0.5$  e  $\beta = 0.1$ , sendo esses os valores selecionados para uso no mecanismo UPAM. O comportamento foi muito similar em outras simulações do mesmo cenário, sendo essas figuras boas representantes gerais desse resultado.

**Figura 13 – Acurácia na detecção de Unavailable Seconds (UaS) por cada combinação de  $\alpha$  e  $\beta$  do modelo Holt em simulação do cenário de testes proposto.**



Fonte: Elaborado pelo autor.

**Figura 14 – Taxa de falso-positivos na detecção de Unavailable Seconds (UaS) por cada combinação de  $\alpha$  e  $\beta$  do modelo Holt em simulação do cenário de testes proposto.**



Fonte: Elaborado pelo autor.

### 6.3 APLICAÇÃO DO UPAM EM SIMULAÇÕES DO CENÁRIO DE TESTES

A Tabela 3 apresenta um resumo dos parâmetros usados pelos modelos do UPAM. A Tabela 4, por sua vez, apresenta as estatísticas de 9 simulações do cenário de testes, além da acurácia, taxa de falso-positivos e tempo em alerta com o uso do mecanismo proposto UPAM, onde verifica-se que ele foi capaz de manter a acurácia acima de 99.8% e a taxa de falso-positivos abaixo de 0.08% em todas as simulações na qual foi aplicado.

**Tabela 3 – Parâmetros usados pelos modelos Holt e de cadeia de Markov no UPAM.**

Modelo	Parâmetro	Valor
Holt	Tamanho das amostras	40 segundos
Holt	$\alpha$	0.5
Holt	$\beta$	0.1
Cadeia de Markov	Tamanho das amostras	14 segundos

Fonte: Elaborado pelo autor

**Tabela 4 – Estatísticas do UPAM aplicado a 9 simulações do cenário de testes.**

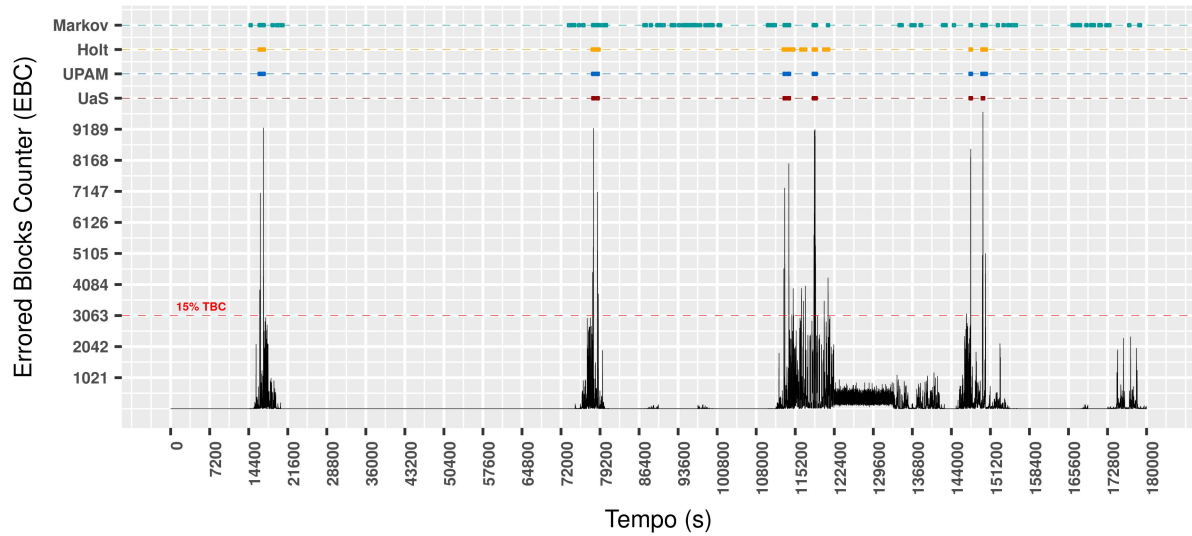
Simulação	Tempo Indisponível (UaS)	Acurácia	Taxa de Falso-Positivos	Tempo em Alerta
1	256	99.91247%	0.06286%	322
2	276	99.87345%	0.08585%	355
3	249	99.88198%	0.08821%	351
4	286	99.88254%	0.07036%	326
5	277	99.90739%	0.05243%	298
6	257	99.90322%	0.06923%	329
7	273	99.89070%	0.06050%	293
8	264	99.88317%	0.07839%	333
9	271	99.89522%	0.06516%	315

Fonte: Elaborado pelo autor

As Figuras 15, 16 e 17 mostram 3 simulações e o funcionamento dos alertas UPAM, além dos momentos nos quais os modelos Holt e de cadeia de Markov foram sensibilizados pela ocorrência de Errored e Severely Errored Seconds. Dessas figuras, observa-se como a combinação dos modelos torna precisa a emissão de alertas próximos ao início dos períodos de indisponibilidade, bem como durante o tempo de sua ocorrência.

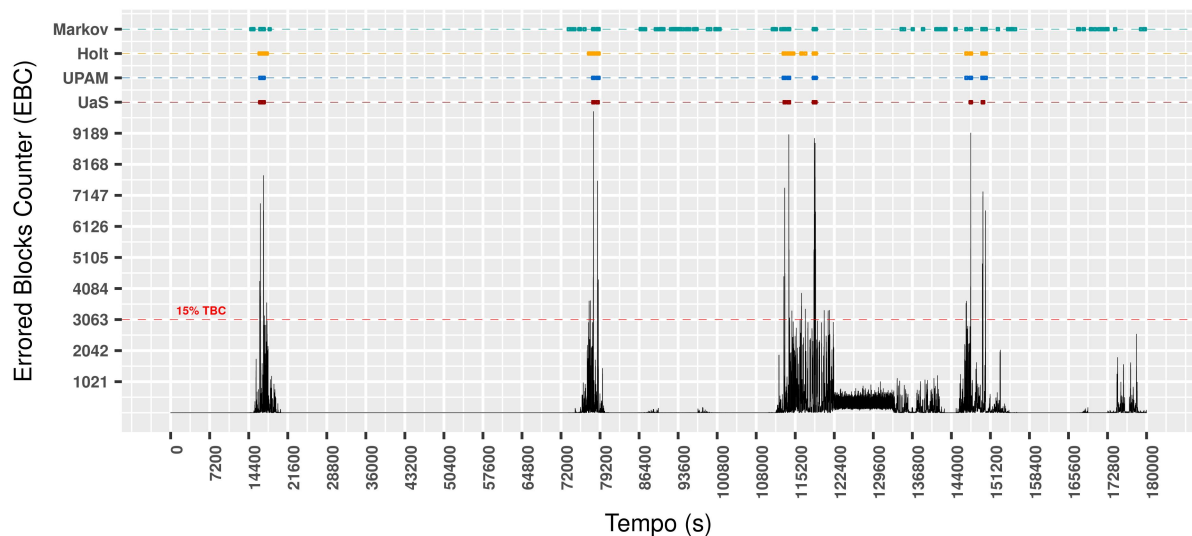
A Figura 18, por fim, apresenta a antecipação média, mínima e máxima para os períodos de indisponibilidade ocorridos nas 9 simulações do cenário de testes. A partir dessa figura observa-se que em todas as simulações houve antecipações maiores ou iguais a 15 segundos, tendo as médias das antecipações em cada simulação variando entre 6 no pior caso e 12 no melhor caso, tendo mesmo sido possível disparar um alerta com 32 segundos de antecedência em uma das ocorrências de indisponibilidade.

**Figura 15 – Funcionamento do UPAM em simulação do cenário de testes.  
Eventos de Desempenho e Alertas na Simulação #1**



Fonte: Elaborado pelo autor.

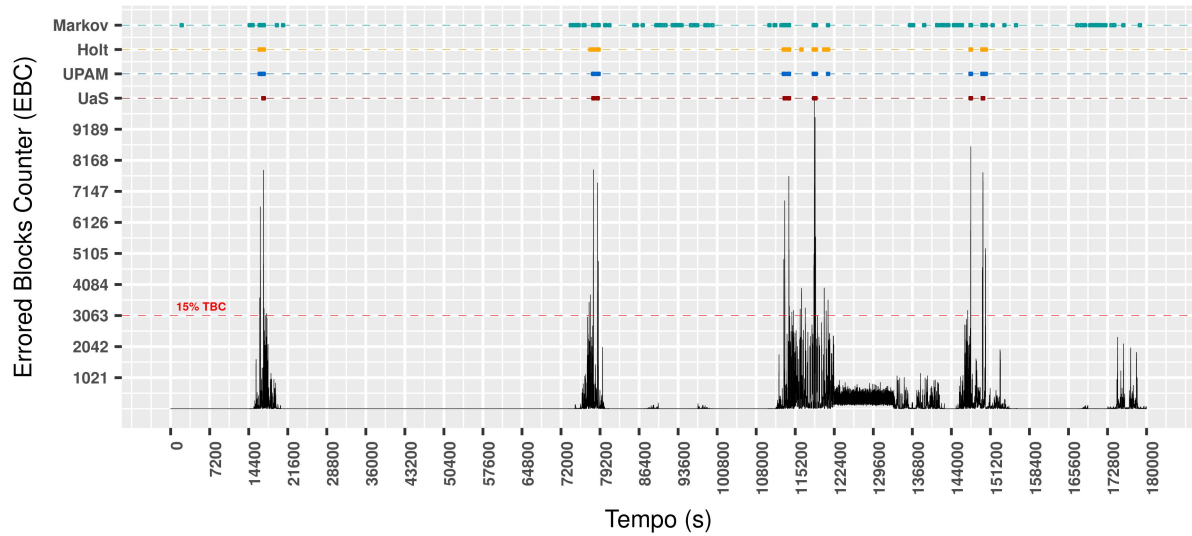
**Figura 16 – Funcionamento do UPAM em simulação do cenário de testes.  
Eventos de Desempenho e Alertas na Simulação #2**



Fonte: Elaborado pelo autor.

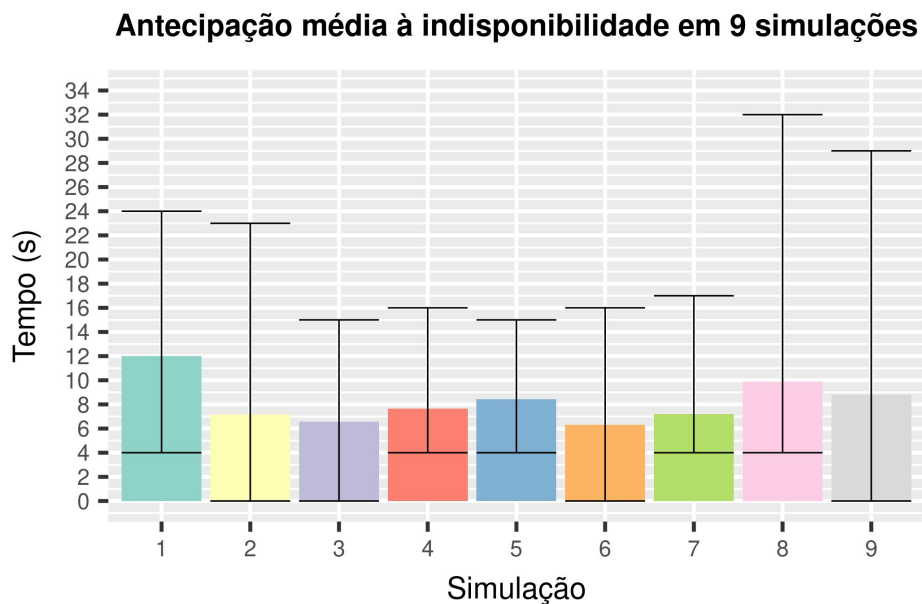
Considerando que a camada ODU leva ao menos 10 segundos para detectar a indisponibilidade do caminho quando a rede está fortemente degradada, **com o auxílio dos alertas UPAM teria sido possível, em média, ativar uma proteção com apenas 4 segundos de forte degradação no pior caso, tendo o melhor caso permitido ativar uma proteção 2 segundos antes mesmo de iniciar-se o período de 10 segundos consecutivos fortemente degradados, condição requerida para o disparo do alarme de indisponibilidade do caminho.** Como o

**Figura 17 – Funcionamento do UPAM em simulação do cenário de testes.  
Eventos de Desempenho e Alertas na Simulação #3**



Fonte: Elaborado pelo autor.

**Figura 18 – Antecipação à detecção de indisponibilidade em 9 simulações através do mecanismo UPAM.**



Fonte: Elaborado pelo autor.

tempo de ativação de uma proteção é de 50ms, a aplicação do mecanismo UPAM no cenário avaliado seria capaz de reduzir o impacto das variações de temperatura no desempenho das aplicações que utilizam a rede, chegando mesmo a evitar que o serviço de transporte fosse interrompido através da ativação de um caminho protegido antes da falha, eliminando o laser atingido por essas variações do caminho em questão até que a situação fosse normalizada.

## 7 CONCLUSÕES E TRABALHOS FUTUROS

A partir dos dados de desempenho coletados pela gerência de desempenho de redes OTN, séries temporais de Errored Blocks podem ser exploradas para detectar a chegada de períodos de indisponibilidade na rede. Por isso, este trabalho propõe o Urgent Preventive Alarm Mechanism (UPAM), que apoiado pelo modelo de previsão Holt, em conjunto com modelo de cadeia de Markov também proposto, tem como objetivo disparar alertas que visam prevenir o disparo de alarmes indicando o início de períodos de indisponibilidade, contribuindo assim com a sobrevivência da rede e evitando a interrupção de seus serviços de transporte.

Experimentos baseados na variação de temperatura na Cidade de Curitiba sobre o laser L1550P5DFB da Thorlabs mostraram que, em 9 simulações, o UPAM foi capaz de emitir alertas com antecedência suficiente para evitar a indisponibilidade em quase todas as ocorrências, muitas vezes segundos antes do início da contagem de 10 segundos usada pelas funções de monitoramento de desempenho para declaração de indisponibilidade da rede. Somado ao curto tempo de ativação de um caminho protegido, da ordem de 50 milissegundos, espera-se que o mecanismo UPAM proposto apoie as operações diárias das redes ópticas de transporte OTN, aumentando sua taxa de sobrevivência e auxiliando de forma inteligente e automática o trabalho dos operadores de rede.

### 7.1 TRABALHOS FUTUROS

Como trabalho futuro espera-se aplicar o mecanismo de alertas UPAM em redes reais e, a partir de um Sistema de Operações conectado aos switches OTN, realizar previsões de mais longo prazo utilizando os registros de desempenho coletados em intervalos de 15 minutos, possivelmente permitindo a detecção de sazonalidades no comportamento da rede e permitindo a emissão de alertas de queda de desempenho com maior antecedência.

## REFERÊNCIAS

- BHUYAN, M. H.; BHATTACHARYYA, D. K.; KALITA, J. K. Network anomaly detection: Methods, systems and tools. **IEEE Communications Surveys Tutorials**, v. 16, n. 1, p. 303–336, First 2014.
- CARVALHO, L. F.; BARBON, S.; MENDES, L. de S.; PROENÇA, M. L. Unsupervised learning clustering and self-organized agents applied to help network management. **Expert Systems with Applications**, v. 54, n. Supplement C, p. 29 – 47, 2016. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0957417416000555>>. Acesso em: 20 mar. 2018.
- CAVALCANTE, J.; PATEL, A.; CELESTINO, J. Performance management of optical transport networks through time series forecasting. p. 152–159, March 2017.
- CHATFIELD, C. **Time-series Forecasting**. [S.l.]: Chapman & C Hall/CRC, 2000.
- CHATFIELD, C.; YAR, M. Holt-winters forecasting: some practical issues. **The Statistician**, JSTOR, p. 129–140, 1988.
- GUMASTE, A.; ANTONY, T. **DWDM network designs and engineering solutions**. [S.l.]: Cisco Press, 2003.
- HAMAMOTO, A. H.; CARVALHO, L. F.; SAMPAIO, L. D. H.; ABRÃO, T.; PROENÇA, M. L. Network anomaly detection system using genetic algorithm and fuzzy logic. **Expert Systems with Applications**, v. 92, n. Supplement C, p. 390 – 402, 2017. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S095741741730619X>>. Acesso em: 20 mar. 2018.
- INTERNATIONAL TELECOMMUNICATION UNION. **ITU-T G.8201**: Error performance parameters and objectives for multi-operator international paths within the optical transport network (otn). [S.l.], 2003.
- INTERNATIONAL TELECOMMUNICATION UNION. **Optical Fibres,cables and systems**. [S.l.], 2009. 324 p.
- INTERNATIONAL TELECOMMUNICATION UNION. **ITU-T G.7710**: Common equipment management function requirements. [S.l.], 2012.
- INTERNATIONAL TELECOMMUNICATION UNION. **ITU-T G.806**: Characteristics of transport equipment - description methodology and generic functionality. [S.l.], 2012.
- INTERNATIONAL TELECOMMUNICATION UNION. **ITU-T G.874.1**: Optical transport network (otn): Protocol neutral management information model for the network element view. [S.l.], 2012.
- INTERNATIONAL TELECOMMUNICATION UNION. **ITU-T G.709**: Interfaces for the optical transport network. [S.l.], 2016.
- JAŠEK, R.; SZMIT, A.; SZMIT, M. Usage of modern exponential-smoothing models in network traffic modelling. **Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems**, Springer Science & Business Media, v. 210, p. 435, 2013.
- KAMINOW, I.; LI, T.; WILLNER, A. **Optical Fiber Telecommunications**. 6. ed. [S.l.]: Academic Press, 2013. VIB.

LAHIRI, S. B. Modified approach to trigg and leach's adaptive response rate model. **Computers & Operations Research**, Elsevier, v. 6, n. 1, p. 27–32, 1979.

MAKRIDAKIS, S.; ANDERSEN, A.; CARBONE, R.; FILDES, R.; HIBON, M.; LEWANDOWSKI, R.; NEWTON, J.; PARZEN, E.; WINKLER, R. The accuracy of extrapolation (time series) methods: Results of a forecast competition. **Journal of Forecasting**, v. 1, p. 111–153, 1982.

MO, J. **Performance Modeling of Communication Networks with Markov Chains**. Morgan & Claypool, 2010. 90- p. Disponível em: <<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6813555>>. Acesso em: 20 mar. 2018.

MORETTIN, P.; TOLOI, C. **Modelos para Previsão de Séries Temporais**. [S.l.]: Instituto de Matemática Pura e Aplicada, 1981.

PAN, Z.; YU, C.; WILLNER, A. E. Optical performance monitoring for the next generation optical communication networks. **Optical Fiber Technology**, v. 16, n. 1, p. 20 – 45, 2010. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S1068520009000686>>. Acesso em: 20 mar. 2018.

RAMASWAMI, R.; SIVARAJAN, K.; SASAKI, G. **Optical networks: a practical perspective**. [S.l.]: Morgan Kaufmann, 2009.

**ANEXOS**



ANEXO A – ALARM MECHANISM FOR ANTICIPATED DETECTION OF NETWORK UNAVAILABILITY IN IP NETWORKS THROUGH TIME SERIES ANALYSIS

Artigo submetido e aceito na conferência IEEE International Conference on Advanced Information Networking and Applications (AINA) 2018. O artigo está inserido na íntegra nas próximas páginas deste anexo.

# Alarm Mechanism for Anticipated Detection of Network Unavailability in IP Networks Through Time Series Analysis

Jefferson Cavalcante  
LARCES  
State University of Ceara  
Fortaleza - Ceara  
Email: jefferson.cavalcante@larces.uece.br

Joaquim Celestino Jr.  
LARCES  
State University of Ceara  
Fortaleza - Ceara  
Email: celestino@larces.uece.br

Ahmed Patel  
LARCES  
State University of Ceara  
Fortaleza - Ceara  
Email: whinchat2010@gmail.com

**Abstract**—With organizations and individuals increasingly depending on the Internet, failures in subnetworks may affect important services such as for economic, health, educational and governmental purposes. Also, as the complexity of the Internet increases, efficient monitoring and automatic preventive measures play vital roles in avoiding network services interruption. In this work, we propose an alarm mechanism based on time series analysis, which monitors entire IP networks with low overhead and anticipates strong degradation of network performance. When applied on 9 operational Internet Protocol (IP) networks with nodes spread worldwide, our mechanism was able to anticipate cases of 100% loss 15 minutes earlier with more than 99% of Accuracy and less than 0.05% of False-Positive Rate in the vast majority of the networks we tested with months of monitoring. In the worst case scenario we found, with Approximate Entropy (ApEn) indicating severely random behavior of loss measurements, our mechanism reached 96.5% of Accuracy and 2% of False-Positive Rate. Based on such encouraging results, we believe our alarm mechanism will support daily operations in IP networks, resulting in enhanced resiliency and enabling more intelligent service provisioning.

## I. INTRODUCTION

With the growing dependence on the Internet by the industry, government, universities and individuals in their daily life and operations, and with the growing complexities of either access and core networks, monitoring links and paths become more difficult and resource expensive. Also, a single link failure can interrupt communication among a large number of client networks.

To provide performance monitoring and fast recovery in case of failure in IP networks, various protocols has been proposed, such as One-Way and Two-Way Active Measurement Protocols (OWAMP [1] and TWAMP [2]) for network performance monitoring and measurements, Bidirectional Forwarding Detection (BFD) [3] and Virtual router Redundancy Protocol (VRRP) [4] for link or path failure detection. With the use of such protocols, networks can recover from failures even in sub-second to second delays. However, until a link or path failure happen, services which use the network can suffer with low Quality of Service (QoS), delivering poor services to network or application clients until a failure happens and a new

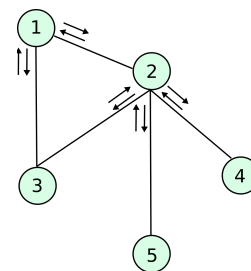


Fig. 1. A subset of all nodes in a network can be enough to monitor all links, reducing the overall number of test packets and avoiding links being monitored more than once.

route is established or links and routers repaired. Also, waiting until a path or link is unavailable to take corrective measures can end up with disruptive stoppage, even if temporarily, of essential and costly services such as those related to health care and financial applications, among others.

To reduce the overhead of monitoring large networks, work in [5] proposes that only a subset of all network elements should send performance monitoring packets, but it must be done in a way that guarantees monitoring of all links in the network. Fig. 1 illustrates the selection of a minimum set of nodes able to monitor all links of a network, and this allows, for example, delay measurement between pairs of nodes  $\{1, 4\}$  and  $\{3, 4\}$  measuring delay between nodes 2 and 4 only once. Authors in [5] reduces the problem of selecting such nodes to the Set Covering problem, which is NP-hard, and proposes a greedy algorithm for this task. In this work we extend [5] by adding intelligence to selected nodes, specifying protocols and algorithms, so they can collect performance statistics and estimate future network conditions, being able to trigger alarms and perform preventive rerouting when needed. We believe that the adoption of both approaches together will, at low computation cost, make IP networks more reliable and intelligent with low bandwidth overhead.

To empower network operators and devices with online statistical analysis for early detection of approach of network

unavailability, this paper proposes Alarm mechanism based on time series forecasting and probabilistic evaluation of packet loss rates, allowing for a steadier network performance recovery and preventive measures before failures even take place. Based on achieved results, we believe that adoption of our proposed mechanism will allow the avoidance of services interruption, more intelligent resource provisioning, better enforcement of QoS and increase IP networks survivability.

This work is organized as follows. Section II introduce related works which contributed to what is being proposed in this paper. Section III presents important background on techniques and tools used in our proposed mechanism. Section IV presents our proposed Alarm mechanism used to detect increasing network performance degradation on IP networks. Sections V and VI bring experiments performed on data of real operational networks and present obtained results. Section VII presents conclusions and discusses future works.

## II. RELATED WORKS

From serious research of related literature, we were not able to find works directly comparable to what is being proposed here, online analysis of time series of loss ratio measurements for alarms generation. While we are looking forward to find directly related and comparable works, we made use of metrics used in proposals of a somewhat related area: anomalous behavior detection.

Recent works in detection of anomalous behavior in networks, such as Ant Colony Optimization for Digital Signature (ACODS) [6] and one based on genetic algorithm and fuzzy logic [7] are examples of modern approaches to this problem. According to [8], works in this area are divided in detection of performance or security anomalies, and proposed techniques are divided in two phases: (a) classify traffic and compute what should be considered normal; (b) detect when traffic behavior deviates from what is being considered normal for its class, making detection of anomalous traffic as close as possible to the time they actually happened.

In this work, however, we follow a different approach to the problem of anomaly detection. Our proposal measures packet loss and isn't concerned on traffic classification, while this is a major feature in recent proposals for anomalous traffic detection, using combined information to produce alarms. Together with traffic characterization, other proposals in this field of research have a challenging update phase in which normal conditions re-evaluated [8], a phase that is not present in our proposed alarm mechanism as we consider that an anomaly occurs when 100% of all transmitted probe packets are lost. Our proposed mechanism triggers an alarm when all transmitted packets are **expected** to be lost and loss is **expected** to increase in next monitoring intervals. Since the aforementioned proposals for network anomaly detection in IP networks would require deep adaptations to be used in the context of this work, thus decharacterizing them, we compared results of our work with results recently reported with use of sophisticated approaches in anomaly detection applied in

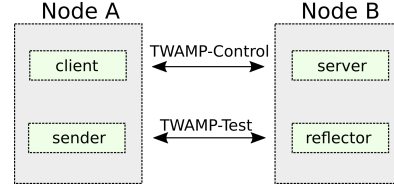


Fig. 2. Simplified roles of nodes which implement TWAMP protocols in a network.

other contexts, but still related to network performance, such as traffic load for specific IP addresses and protocols.

We set our performance objective to the levels reached in the recently published [7] and [6] in terms of Accuracy and False Positive Rates (FPR), which were achieved with introduction of abnormal traffic to test networks. In [6], the proposed ACODS approach reached 96.26% of Accuracy and beaten all other approaches compared in the study. In [7], the proposed technique reached 96.53% of Accuracy against 95.34% reached by ACODS in the database they tested. They also measured the False Positive Rate (FPR), which represents how much each technique erroneously reported an anomaly. The fuzzy approach reached 0.56% of FPR while ACODS reached 0.64%. During experiments in this work, our performance objective is to reach at least 95% of Accuracy and at most 0.6% of FPR to make our work comparable to good results achieved by these recently published techniques in detection of network performance anomalies.

## III. BACKGROUND

For the better understanding of our proposal on anticipated failure detection in IP networks, this section presents theoretical fundamentals on time series forecasting, Markov Chains and performance monitoring in IP networks.

### A. The TWAMP Protocol

Two-Way Active Measurement Protocol (TWAMP) [2] is a IETF standard [9] for computing round-trip measures between pairs of devices in IP networks. It is composed by two protocols: the Twamp-Control, which is used to set up sessions; and the Twamp-Test protocol, which defines test or probe messages sent by a sender and reflected by a reflector. Test packets are the ones actually used to measure network performance. Fig. 2 illustrates the roles of nodes that implement TWAMP protocols in a network. TWAMP-Control specifies that a TWAMP client initiates a TCP connection to a TWAMP server, than they exchange information such as security measures that will be employed, size of test packets and other details. Since a session is completely set up, a TWAMP sender starts sending UDP packets to its pair, a TWAMP reflector, which send them back allowing for delay, jitter, loss and other measurements.

### B. Time Series Forecasting

Time series are a set of observations sorted over time [10] in which components may be present, such as: level, trend, seasonality and randomness. Level is a mean observations vary

around. Trend is a consistent increase or decrease of values in a time series over time. Seasonality is a cyclical variation that might be noticed. Randomness is a behavior that is not produced by any of the aforementioned components.

In order to estimate values in a time series, it is important to understand how its values vary, find a mathematical model which fits to them, then use this model to forecast values steps ahead in time. To give an example, if observations vary around a mean, but such variations are strong, one appropriate model could be the Simple Exponential Smoothing, which exponentially decreasing weights older observations. This model, in particular, is written as  $\bar{Z}(t) = \alpha Z(t) + (1-\alpha)\bar{Z}(t-1)$ , where  $Z(t)$  is a time series observation at time  $t$ . The constant  $\alpha$  sets the importance of newer observations and is in range (0,1).

Various important forecasting models are based on exponential smoothing, with Holt and Holt-Winters being the most prominent because of their good performance compared to other models [11] [12], and thus used for series analysis in this work. One drawback is the need for proper selection of some constant parameters [13].

Holt model fits time series using two exponentially smoothed components: level and trend. Estimating an observation of  $Z$  at a time  $t+k$  is done by  $\hat{Z}_t(h) = L_t + hT_t$ , where  $t$  is a time for which there is a known observation  $Z_t$ , and  $h$  is a horizon for which the estimate will be computed [14]. Level is computed by equation  $L_t = \alpha Z_t + (1-\alpha)(L_{t-1} + T_{t-1})$ , and trend is computed by equation  $T_t = \beta(L_t - L_{t-1}) + (1-\beta)T_{t-1}$ . Holt uses two constant exponential smoothing parameters:  $\alpha$  and  $\beta$ , one for each component.

### C. Markov Chains

As stated by J. Mo in his book [15], Markov chain is a powerful mathematical tool for modeling of dynamic systems which change their states over time, with its popularity attributed to its simplicity, flexibility and easy of computation.

Markov chains are defined by a state space and a transition probability matrix. One important property of such matrices is that computing its  $n$ -th power  $M^{(n)}$  with  $\lim_{n \rightarrow \infty} M^n$  makes probabilities converge, reaching an equilibrium despite of the starting state, as exemplified in Eq. 1 [15]. This equilibrium is called the steady state distribution  $\pi$  of a Markov chain. In practice,  $\pi$  is a vector of probabilities, and is often interpreted as the time the modeled system will spend in each state in the long run.

$$M = \begin{bmatrix} 0.6 & 0.4 \\ 0.25 & 0.75 \end{bmatrix} M^{16} = \begin{bmatrix} 0.3846 & 0.6154 \\ 0.3846 & 0.6154 \end{bmatrix} \quad (1)$$

Instead of raising  $M$  to sufficiently high powers, other methods can be used to find the steady state distribution  $\pi$  more easily, and one of them is solving the system of equations  $\pi M = \pi$  [15]. According to a result derived from the Perron-Frobenius theorem, namely that Markov matrices always have the eigenvalue  $\lambda = 1$ , the problem of finding  $\pi$  can be seen as the problem of finding the left-eigenvalue associated to the eigenvalue  $\lambda = 1$  of a transition probability matrix  $M$ . This vector is often referred as the characteristic eigenvector of

a Markov matrix. In this work, we propose the use of the characteristic eigenvector of Markov matrices to statistically compute whether communications in IP networks will spend next time intervals in state of decreasing performance.

With use of presented mathematical models and protocol, our proposed Alarm mechanism can collect and perform statistical analysis anticipate possible periods of intense loss in IP networks, helping network operators in preventing service unavailability and Service Level Agreements breaches.

## IV. ALARM MECHANISM FOR ANTICIPATION OF NETWORK UNAVAILABILITY

Proactive monitoring of paths is when performance is indefinitely measured in fixed-time periods [16]. With the help of TWAMP, IP nodes carefully selected by the algorithm proposed in [5], and acting like a TWAMP-Test sender, can be used to monitor performance of an entire network inputting low overhead. Recent measurements of loss ratio obtained after each fixed-time period, called a monitoring interval, can be stored by each TWAMP-Test sender to form time series of loss ratios for further statistical analysis. In this section we present our proposed Alarm mechanism which, by analyzing time series of measurements collected by the TWAMP protocol, can indicate if service interruption might happen in near future and help preventing service unavailability and SLA breaches.

From the number of sent packets and the number of packets that have returned, TWAMP is able to compute loss ratio for each monitoring interval. Like other approaches to proactive network monitoring [17] [16], in this work we use of monitoring intervals with 15 minutes of duration.

Our approach uses Holt model to fit time series of loss ratios obtained in the last few monitoring intervals, thus producing an estimated loss ratio for the next 15 minutes. In parallel, we also use a Markov Chain model to estimate the time series behavior in the next monitoring intervals. when combined, both models are able to identify whether loss is expected to reach potentially dangerous levels, and whether it tends to keep growing, possibly reaching 100% loss and interrupting communications.

Holt model requires definition of its constants  $\alpha$  and  $\beta$ , which will be presented in Section V. For the Markov Chain used in this work, next paragraphs provide our proposed set of states and transition probability matrices which enable further statistical analysis for part our proposed Alarm mechanism.

TABLE I  
PERFORMANCE STATES FROM ANALYSIS OF CONSECUTIVE LOSS RATIO MEASUREMENTS

STATE	DESCRIPTION
$S_1$	Decreasing Loss
$S_2$	Stable Loss
$S_3$	Increasing Loss

Given the set  $L$  of consecutively measured loss ratios in  $n$  consecutive monitoring intervals, we define the set  $G$  of three states presented in Table-I, which reflects how loss ratio

evolves in  $L$ . The set  $Z$  is composed of states from transitions in  $L$  and is computed as follows:

$$Z(i) = \begin{cases} s1, & \text{for } L(i) > L(i+1) \\ s2, & \text{for } L(i) = L(i+1) \text{ and } L(i+1) \leq \theta\% \\ s3, & \text{for } L(i) < L(i+1) \text{ or } L(i+1) > \theta\% \end{cases}$$

The sequence of states  $Z$  is built from transitions of consecutive loss ratios and plays an important role in our model, since it is used to build the transition matrix  $M$ , which contains the computed probability of going from Network Performance State  $S_p$  to  $S_q$ , with  $\{S_p, S_q\} \in \{S_1, S_2, S_3\}$ . The constant  $\theta$  is set as a loss ratio which is considered too high to allow transition for other state other than  $S_3$  (Increasing Loss), even if even if consecutive loss ratios in  $L$  are decreasing or keeping stable.

With matrix  $M$  and by applying the Perron-Frobenius theorem, the equipment uses the higher eigenvalue  $\lambda = 1$  to compute its associated eigenvectors  $\vec{P}$ , the invariant vector of probabilities of having the network in each state  $S_1$ ,  $S_2$  and  $S_3$ . Markov matrix  $M$  contains the following state transitions probabilities:

$$M_{3 \times 3} = \begin{bmatrix} S_1 \Rightarrow S_1 & S_1 \Rightarrow S_2 & S_1 \Rightarrow S_3 \\ S_2 \Rightarrow S_1 & S_2 \Rightarrow S_2 & S_2 \Rightarrow S_3 \\ S_3 \Rightarrow S_1 & S_3 \Rightarrow S_2 & S_3 \Rightarrow S_3 \end{bmatrix}$$

In case there are no state transitions to  $S_1$  or  $S_2$  in  $M$ , the matrix is built as follows:

$$M_{2 \times 2} = \begin{bmatrix} S_i \Rightarrow S_i & S_i \Rightarrow S_3 \\ S_3 \Rightarrow S_i & S_3 \Rightarrow S_3 \end{bmatrix}, S_i \in \{S_1, S_2\}$$

Individually, each proposed model is responsible for estimate the future behavior os loss ratio after each monitoring interval, and trigger a warning if a predetermined threshold is crossed. In the context of our proposal, triggering a warning means setting a flag to *true* for the duration of the next monitoring interval, and we propose the flags  $H-FLAG$  and  $MC-FLAG$  for use with Holt and Markov Chain approaches respectively, which can be stored in a Model Information Base for integration with operation systems. With the Holt model, if the estimated loss ratio for the next monitoring interval exceeds a threshold  $\gamma$ , then the  $H-FLAG$  is to true and indicates that loss is expected to cross an alarming level in next monitoring interval. The impact of  $\gamma$  on accuracy and false positive ratios are presented in Section V. With the Markov Chain model, if the probability of state  $S_3$   $\vec{P}^i$  is higher than 50%, then the  $MC-FLAG$  is set to true and indicates that, based on how loss ratio has evolved in the last monitoring intervals, service interruption might be expected for the near future. Both  $H-FLAG$  and  $MC-FLAG$  are warnings which should make network operators aware of approach of degraded network performance, but they might not trigger urgent corrective measures for reasons presented in Section VI.

If, however, for a given current monitoring interval both  $H-FLAG$  and  $MC-FLAG$  are set to true, both models agree that

TABLE II  
CHARACTERISTICS OF NETWORK PATHS SELECTED FOR ANALYSIS.

Monitored path	Duration (months)	Failures	ApEn
Cape Town - Singapore	6.2	3239	1.5895
Cape Town - Columbia	6.2	1953	1.088692
Cape Town - Korea	6.2	236	0.3576688
Cape Town - Hyderabad	5.4	19	0.3252367
Cape Town - Hong-Kong	1.6	23	0.4399113
Zurich - Cape Town	6.2	156	0.1311798
Zurich - Spain	9.3	61	0.05634084
Zurich - Chile	5.7	8010	0.1456051
Zurich - Hong-Kong	0.9	24	0.1951773

loss is about to reach unacceptable levels and the monitored network path needs corrective measures in the short-term to prevent service interruption. In this case, we propose that an Alarm is logged into the Network Element system and it should be used to feed routing protocols such as RIP and IS-IS, for the establishment of alternative routes to affected destinations. Network operators should be also aware of this alarm so corrective measures can be taken on time, such as fixing cables, connectors, equipments, or environmental conditions that could cause such degraded performance.

## V. EXPERIMENTS

To assess the effectiveness of our proposal, we tested our alarm mechanism on various pairs of nodes on data of a real operational network. The WAND Research Group from the Waikato University, in New Zealand, developed the Active Measurement Project and deployed software for network performance monitoring in a large set of computers around the world, comprising 11 countries. All network performance monitoring data is made public by the WAND Research Group and can be accessed in [18]. Their database contains Two-Way network performance monitoring from the sending of 1 packet per minute for months. We based our analysis on 9 pairs of nodes distributed around the world with lossy paths shown in Table-II.

Most of the network paths we tested described a behavior similar to what was found in paths Cape Town-Korea and Zurich-Spain. The path Cape Town-Singapore, however, described a severe random behavior and poor network performance, and such complicated scenarios can be challenging to time series forecasting models, such as Holt. Cape Town-Columbia is in halfway between network performance found in Cape Town-Singapore and common cases such as Zurich-Spain. For this reason, we brought scenarios for analysis on both common and more complicated scenarios, which will help better understand how our proposed Alarm mechanism anticipates complete network unavailability in real operational networks under various circumstances.

To measure performance of our proposed Alarm mechanism, we compute Accuracy and False Positive Rates (FPR) in face of failures, it is 100% of packet loss. Accuracy increases whether there is an Alarm set for a monitoring interval which develops 100% of packet loss, and False-Positive Rate increases if there is an alarm set for a monitoring interval

which doesn't develop 100% of packet loss. Alarms are always set for the next monitoring interval after analysing time series of recent loss measurements, which means the proposed Alarm mechanism can be able to anticipate failures 15 minutes earlier. We computed these statistics from varying the following variables: sample size, which is the number of most recent monitoring intervals store in the network element; Constant  $\theta$  used by our proposed Markov Chain model to compute performance states; Constants  $\alpha, \beta$  used by Holt model, and the proposed constant  $\gamma$  to help this model deciding when to set a warning. Our research methodology for understanding the impact of such variables in accuracy and FPR is presented as follows:

- 1) **Sample Sizes:** We varied sample size from 4 to 96 intervals with increments of 4 intervals with 15 minutes of duration each. With Holt, for each sample size, we computed the average Accuracy and FPR from varying constants  $\alpha$  and  $\beta$  in Holt from 0.1 to 0.9 with increments of 0.2. For our proposed Markov Chain model, for each sample size we computed the Accuracy and FPR reached. As a final result of this experiment, we elected sample sizes which maximizes accuracy and minimizes FPR, yet finding a good balance between these metrics and the amount of space needed to store such time series in equipments.
- 2) **Holt constants  $\alpha$  and  $\beta$ :** After selection of an appropriate sample size, we analyzed the impact of Holt's  $\alpha$  and  $\beta$  constants on Accuracy and FPR. We selected values which maximizes Accuracy and minimizes FPR in most networks, or which allowed a good balance between these metrics.
- 3) **Tolerance constants  $\gamma$  and  $\theta$ :** During the 2 aforementioned experiments, we tried various values of these constants between 0.75 to 0.95 and selected the ones that provided higher accuracy and lower FPR.

After understanding the impact of all proposed and default parameters on Holt and Markov Chain models, we state which values better fit for use with loss measurements in IP networks. After presenting proper values for all parameters, we present analysis of our proposed Alarm performs in 9 world-wide network paths in terms of Accuracy and FPR.

## VI. RESULTS

In this section we present analysis of how our proposed Alarm mechanism performed with various world-wide network paths. For each pair of nodes, we present the Accuracy and False-Positive Rate of warnings generated by Holt and Markov Chain models separately for various values of sample size,  $\alpha, \beta, \gamma$  and  $\theta$ . After we understand the impact of all these parameters on performance of both models, we present final analysis on performance in terms of Accuracy and FPR of our proposed Alarm.

### A. Sample Size

During experiments to decide which sample size use with Holt and Markov Chain models, we found that 32 intervals

of 15 minutes each make a good balance between Accuracy, False-Positive Rate and storage size for use of Holt. We noted that with this model, higher sample sizes provided better results until stabilization, and 32 intervals was enough to reach stabilization in almost all tested network paths, as shown in Figs. 3 and 4.

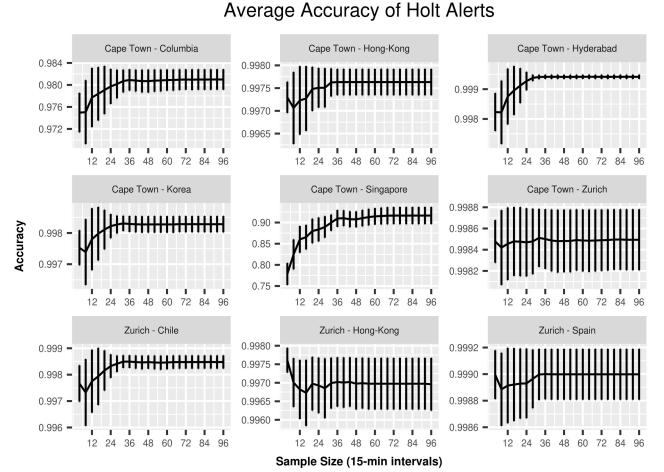


Fig. 3. Average Accuracy with 95% confidence intervals for various sample sizes with Holt.

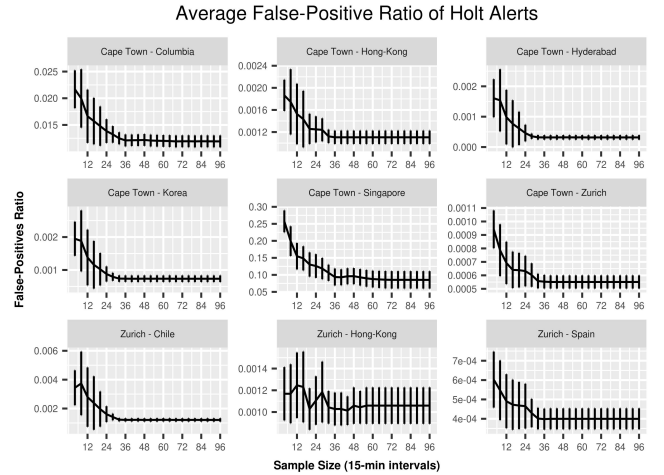


Fig. 4. False-Positive Ratio for various sample sizes with Holt.

With the proposed Markov Chain model, we noted that in general increasing the sample size decreases accuracy and increases FPR of its warnings, except for 2 cases as shown in Figs. 5 and 6. For this reason, we set sample size for use with Markov Chain to 12 monitoring intervals for a good balance between such metrics.

### B. Holt Exponential Smoothing Constants

From these experiments, as shown in Fig. 7, we noted that  $\alpha = 0.9$  and  $\beta = 0.1$  made Holt more accurate in most scenarios, and  $\beta$  tended to impact less than  $\alpha$  on accuracy. One

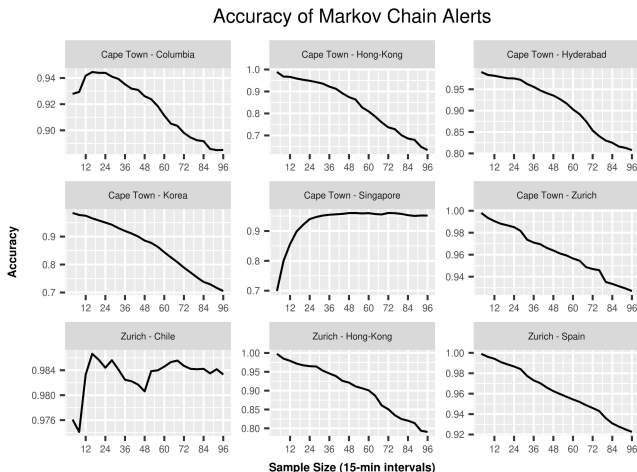


Fig. 5. Average Accuracy for various sample sizes with the Markov Chain.

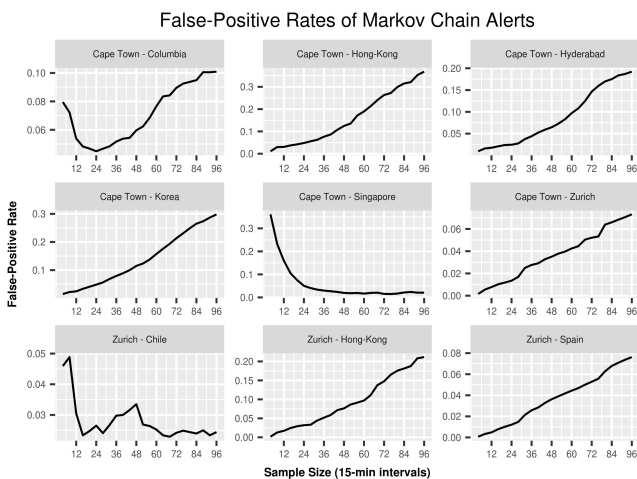


Fig. 6. False-Positive Ratio for various sample sizes with the Markov Chain.

exception was in the path between Cape Town and Singapore, in which lower values of  $\alpha$  produced higher accuracy, but the gain was small when compared to higher values of  $\alpha$ . Also, in this path  $\beta$  had more impact on accuracy than in most of other network paths we tested. for the sake of generality, we set  $\alpha = 0.9$  and  $\beta = 0.1$  for use with Holt to fit time series of loss measurements in IP networks.

### C. Tolerance constants

During the aforementioned experiments, we tested various values of tolerance constants  $\gamma$  and  $\theta$  in range between 0.75 and 0.90. Although not graphically presented here, we found good results with the following combination:  $\gamma = 0.9$  and  $\theta = 0.85$ .

After all experiments to select adequate parameters based on 9 world-wide IP network paths, we present in Table-Table-III a summary of selected constant parameters used by our Alarm mechanism for final results and analysis.

TABLE III  
PARAMETERS FOR USE IN OUR PROPOSED ALARM MECHANISM

Parameter	Value
Sample Size for Holt	32 intervals
Holt's $\alpha$	0.9
Holt's $\beta$	0.1
Holt's tolerance factor $\gamma$	0.9
Sample size for Markov Chain	12 intervals
Markov Chain's tolerance factor $\theta$	0.85

### D. Final Results

After stating values of parameters for use with Holt and our proposed Markov Chain models, we now compare in Table-IV the Accuracy (ACC) and False-Positive Rate (FPR) of warnings generated by each model, and for the combination of such warnings which makes our proposed Alarm. From presented results, we note the direct relationship between Approximate Entropy (ApEn) and performance of our alarm in accuracy and FPR. This is the expected behavior since higher ApEn indicates more unpredictable loss measurements.

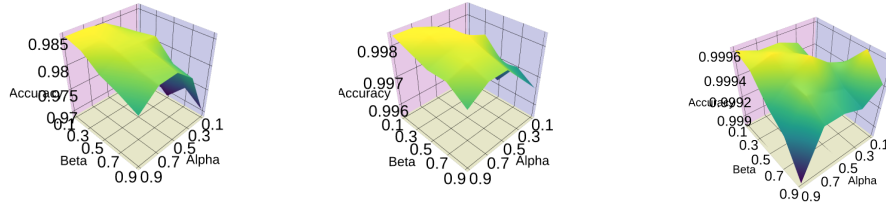
Holt provides overall good results in accuracy and FPR when ApEn is low, but with higher ApEn results are way below our performance objectives. When feedback provided by our proposed Markov Chain model is used, False-Positive Rates decreased by more than half in all tested network paths, and accuracy increased notably in scenarios with higher ApEn. Our Alarm mechanism, when uses combined time series analysis and warnings from Holt and Markov Chain models adjusted for the scenario of loss measurements in IP networks, resulted in more than 99% of accuracy and less than 0.1% of false-positive rates in almost all tested lossy world-wide paths we found in Waikato AMP database. From 9 network paths, in only two of them our Alarm mechanism presented less than 99% of accuracy, precisely 96.5% and 98.3%, and more than 0.1% of FPR, precisely 2% and 0.6%, but such scenarios suffered from strong random variations in loss measurements, and even under such circumstances our proposed mechanism developed acceptable performance.

We present in Figs. 8 and 9 a trace of loss measurements in some of the aforementioned network paths along with warnings and Alarms provided by our proposed mechanism.

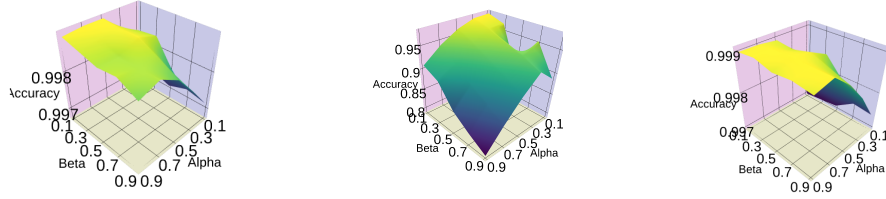
From analysis of presented results, we believe that our proposed Alarm mechanism can be an important allied to network operators and network service providers, proving itself very effective in preventive detection of network unavailability, providing opportune alarms to trigger corrective measures. We expect our proposed Alarm mechanism will part of and support daily operations of IP network operators and systems in the near future to improve survivability and service provisioning.

## VII. CONCLUSIONS

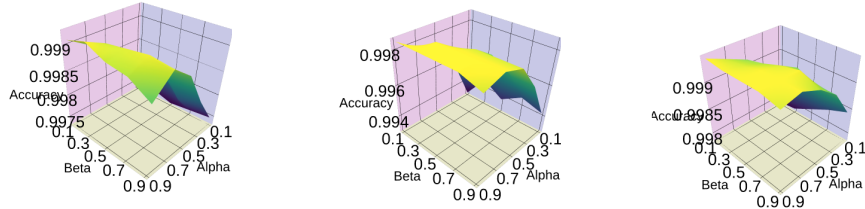
This study proposes an integrated mechanisms for efficient proactive and preventive detection of network service interruption, which, from analysis of loss ratio measurements, provide an *anticipated* Alarm mechanism for keeping the network healthy through preventive rerouting or maintenance.



(a) Cape Town - Columbia (b) Cape Town - Hong-Kong (c) Cape Town - Hyderabad



(c) Cape Town - Korea (d) Cape Town - Singapore (e) Zurich - Cape Town



(f) Zurich - Chile (g) Zurich - Hong-Kong (h) Zurich - Spain

Fig. 7. Impact of Holt exponential smoothing constants  $\alpha$  and  $\beta$  on Accuracy.

TABLE IV  
ACCURACY (ACC) AND FALSE-POSITIVE RATES (FPR) OF HOLT AND M. CHAIN MODELS AND THE COMBINED ALARM MECHANISM

Monitored path	Holt ACC%	Holt FPR%	Markov Chain ACC%	Markov Chain FPR%	Alarm ACC%	Alarm FPR%
Cape Town - Singapore	90.87010	95.76565	85.60606	15.93829	96.55192	2.20893
Cape Town - Columbia	98.54612	1.16882	94.17892	5.38159	98.24532	0.66254
Cape Town - Korea	99.88302	0.07903	97.45432	2.46105	99.84960	0.02822
Cape Town - Hyderabad	99.96166	0.02559	98.15951	1.77235	99.91692	0.01280
Cape Town - Hong-Kong	99.83211	0.10544	96.64218	3.05778	99.64323	0.04218
Zurich - Cape Town	99.89973	0.05619	99.05303	0.77546	99.79947	0.02248
Zurich - Spain	99.94048	0.03356	99.41964	0.48100	99.87723	0.02237
Zurich - Chile	99.90968	0.09305	98.33213	3.04722	99.87355	0.04652
Zurich - Hong-Kong	99.84568	0.07788	97.91667	1.71340	99.57562	0.03894

Also, analysis proposed in this work can help with more intelligent resource allocation, such as increasing bandwidth or making use of alternate routes in periods of higher network degradation.

For our current and future research, the proposed techniques will be used in context of network security and threat analysis for preventive detection of attacks to networks. Also, more sophisticated analysis will be proposed to increase the range of applications of our proposal.

## REFERENCES

- [1] S. Nadas, "A One-way Active Measurement Protocol (OWAMP)," Internet Requests for Comments, RFC Editor, RFC 7718, September 2006. [Online]. Available: <http://www.rfc-editor.org/rfc/rfc7718.txt>
- [2] A. M. K. Y. J. B. K. Hedayat, R. Krzanowski, "A Two-Way Active Measurement Protocol (TWAMP)," Internet Requests for Comments, RFC Editor, RFC 5357, October 2008. [Online]. Available: <http://www.rfc-editor.org/rfc/rfc5357.txt>
- [3] D. Katz and D. Ward, "Bidirectional Forwarding Detection (BFD)," Internet Requests for Comments, RFC Editor, RFC 5880, June 2010. [Online]. Available: <http://www.rfc-editor.org/rfc/rfc5880.txt>
- [4] S. Nadas, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6," Internet Requests for Comments, RFC



Loss Ratio Measurements and provided Alarms between Cape Town and Singapore

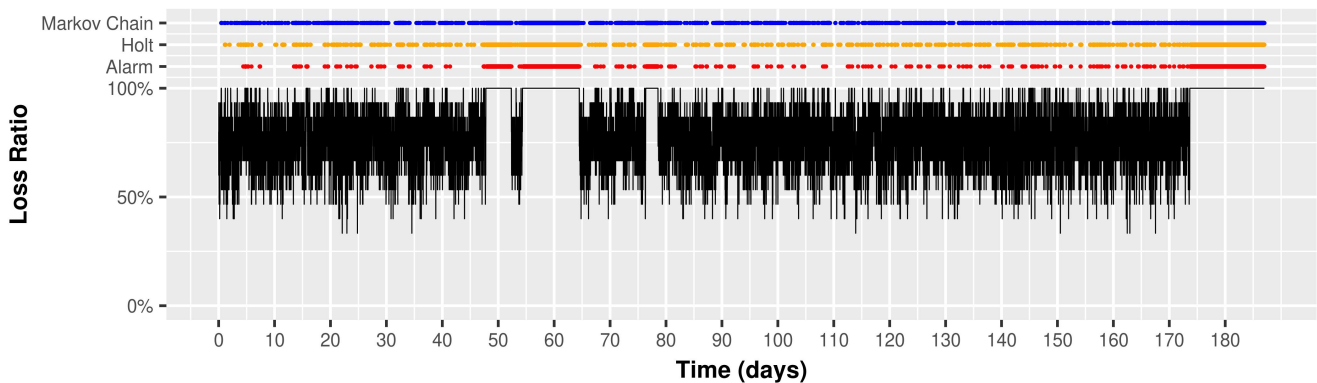


Fig. 8. Loss measurements between Cape Town and Singapore with Alarms provided by our proposed mechanism. This is the worst case scenario, with severe variations in loss measurements and high ApEn.

Loss Ratio Measurements and provided Alarms between Cape Town and Columbia

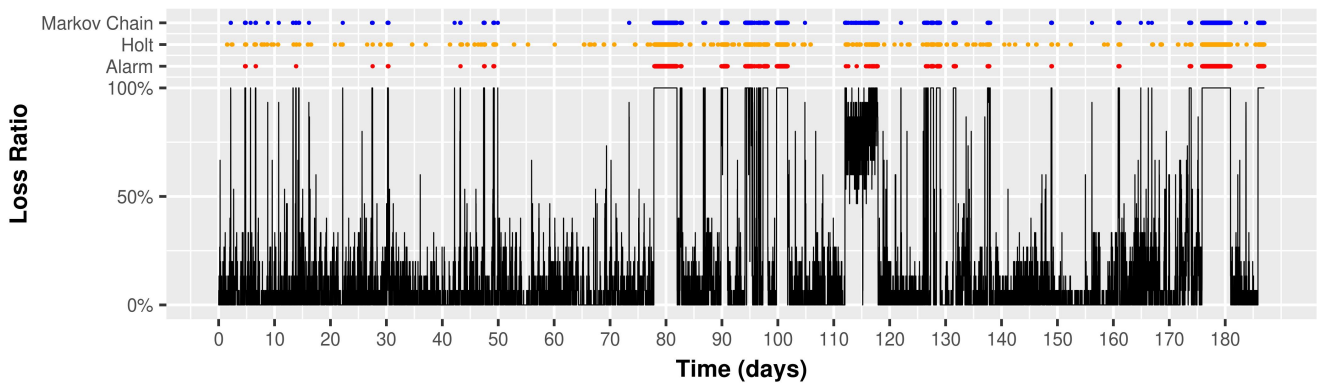


Fig. 9. Loss measurements between Cape Town and Columbia (US) with Alarms provided by our proposed mechanism.

Editor, RFC 5798, March 2010. [Online]. Available: <http://www.rfc-editor.org/rfc/rfc5798.txt>

[5] Y. Bejerano and R. Rastogi, "Robust monitoring of link delays and faults in ip networks," *IEEE/ACM Transactions on Networking*, vol. 14, no. 5, pp. 1092–1103, Oct 2006.

[6] L. F. Carvalho, S. Barbon, L. de Souza Mendes, and M. L. Proena, "Unsupervised learning clustering and self-organized agents applied to help network management," *Expert Systems with Applications*, vol. 54, no. Supplement C, pp. 29 – 47, 2016. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0957417416000555>

[7] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abro, and M. L. Proena, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Systems with Applications*, vol. 92, no. Supplement C, pp. 390 – 402, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S095741741730619X>

[8] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 303–336, First 2014.

[9] R. F. R. Geib, A. Morton and A. Steinmitz, "IP Performance Metrics (IPPM) Standard Advancement Testing," Internet Requests for Comments, RFC Editor, RFC 6576, March 2012. [Online]. Available: <http://www.rfc-editor.org/rfc/rfc6576.txt>

[10] R. Jašek, A. Szmit, and M. Szmit, "Usage of modern exponential-smoothing models in network traffic modelling," *Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems*, vol. 210, p. 435, 2013.

[11] S. Makridakis, A. Andersen, R. Carbone, R. Fildes, M. Hibon, R. Lewandowski, J. Newton, E. Parzen, and R. Winkler, "The accuracy of extrapolation (time series) methods: Results of a forecast competition," *Journal of Forecasting*, vol. 1, pp. 111–153, 1982.

[12] C. Chatfield and M. Yar, "Holt-winters forecasting: some practical issues," *The Statistician*, pp. 129–140, 1988.

[13] S. B. Lahiri, "Modified approach to trigger and leach's adaptive response rate model," *Computers & Operations Research*, vol. 6, no. 1, pp. 27–32, 1979.

[14] P. Morettin and C. Toloi, *Modelos para Previsão de Sries Temporais*. Instituto de Matematica Pura e Aplicada, 1981.

[15] J. Mo, *Performance Modeling of Communication Networks with Markov Chains*. Morgan & Claypool, 2010. [Online]. Available: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6813555>

[16] T. M. E. Forum, "Service OAM Performance Monitoring Implementation Agreement," MEF 35.1, Metro Ethernet Forum, MEF 35.1, May 2015.

[17] ITU, "Common equipment management function requirements," ITU-T G.7710, International Telecommunication Union, ITU-T G.7710, February 2012.

[18] T. McGregor. Active measurements project. [Online]. Available: <https://research.wand.net.nz/software/amp.php>