UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Rodrigo Costa Duarte

Avaliação do Impacto de Falhas no Tráfego da Rede da Universidade Federal de Juiz de Fora

Juiz de Fora
2014

UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Rodrigo Costa Duarte

Avaliação do Impacto de Falhas no Tráfego da Rede da Universidade Federal de Juiz de Fora

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação, do Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora como requisito parcial para obtenção do título de Mestre em Ciência da Computação.

Orientador: Alex Borges Vieira
Coorientador: Ítalo Fernando Scotá Cunha

Juiz de Fora
2014

Ficha catalográfica elaborada através do Programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Duarte, Rodrigo Costa.
Avaliação do Impacto de Falhas no Tráfego da Rede da Universidade Federal de Juiz de Fora / Rodrigo Costa Duarte. -- 2014.
71 f.

Orientador: Alex Borges Vieira
Coorientador: Ítalo Fernando Scotá Cunha
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação, 2014.

1. Redes de computadores. 2. Impacto de falhas. 3. Caracterização. I. Vieira, Alex Borges, orient. II. Cunha, Ítalo Fernando Scotá, coorient. III. Título.

Rodrigo Costa Duarte

Avaliação do Impacto de Falhas no Tráfego da Rede da Universidade Federal de Juiz de Fora

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Computação da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de Mestre.

Aprovada em 01 de Agosto de 2014.

BANCA EXAMINADORA

_____

Prof. D.Sc. Alex Borges Vieira – Orientador
Universidade Federal de Juiz de Fora

_____

Prof. D.Sc. Ítalo Fernando Scotá Cunha – Coorientador
Universidade Federal de Minas Gerais

_____

Prof. D.Sc. Artur Ziviani
Laboratório Nacional de Computação Científica

_____

Prof. D.Sc. Eduardo Barrére
Universidade Federal de Juiz de Fora

A Deus, que guiou meus passos em mais esta jornada. Aos meus pais pelo exemplo, o carinho e a inspiração. Para Eliete e Gustavo, sem os quais esta conquista nunca seria completa.

AGRADECIMENTOS

Agradeço primeiramente a Deus e a Nossa Senhora, por estarem presentes em todos os meus momentos.

A meus familiares, principalmente a meus pais, João e Cidinha, por nunca se cansarem de me ensinar tudo aquilo que aprenderam em suas jornadas e por me mostrar que todas as conquistas devem ser acompanhadas de muito esforço, dedicação e comprometimento. A minhas irmãs, meus cunhados e cunhadas, sobrinhos e sobrinhas por estarem sempre prontos a ajudar.

A minha esposa Eliete, pelo total apoio e compreensão, por estar ao meu lado mesmo nos momentos mais díficeis e pelo carinho constante que me dedicou ao longo deste desafio. Tudo é possível com você ao meu lado!

Ao meu querido filho Gustavo, pelo amor incondicional mesmo nas horas não brincadas ou nos momentos de cansaço. Seu sorriso e sua alegria me abasteceram de energia para conquistar este objetivo.

Aos meus orientadores, Alex e Ítalo por todas as lições, pelo apoio constante, a confiança emprestada, os puxões de orelha necessários e o incentivo sempre presente. A amizade e consideração que dedico a vocês vai muito além de qualquer título.

A todos os professores que dedicaram seu tempo me mostrando a importância de crescer sempre, em especial aos mestres Custódio, Ely, Guilherme e Rubens pela confiança inicial depositada em mim. Aos colegas de curso e funcionários do ICE, por sua generosidade e disposição constante em compartilhar o conhecimento e oferecer ajuda e palavras de incentivo sempre que necessário.

A meus amigos, parte fundamental de minha vida mesmo que o tempo não nos brinde com tantos encontros quanto merecemos. Aos colegas de trabalho pelo suporte constante nos momentos em que tive que focar nos estudos. E a todos aqueles que, mesmo silenciosamente, torceram por mim e acreditaram na minha conquista.

A todos aqueles que, mesmo estando em outro plano, fizeram parte da construção do meu ser e estão sempre presentes em minhas preces e pensamentos, e pelos quais espero sempre lutar as boas batalhas, honrando toda a aprendizagem compartilhada e os bons exemplos recebidos.

"Enquanto a sociedade feliz não chega, que haja pelo menos fragmentos de futuro em que a alegria é servida como sacramento, para que as crianças aprendam que o mundo pode ser diferente. Que a escola, ela mesma, seja um fragmento do futuro..."

Rubem Alves

RESUMO

Neste trabalho caracterizamos o impacto de falhas na Rede Nacional de Ensino e Pesquisa (RNP) no tráfego de dados da rede da Universidade Federal de Juiz de Fora. Nós estudamos o impacto das falhas no comportamento do tráfego, dos usuários e das aplicações na rede da universidade. As falhas estudadas se dividem em falhas parciais e problemas de desempenho. As falhas parciais são interessantes pois persistem por várias horas e afetam apenas enlaces internacionais da RNP, sem impedir acesso a destinos no Brasil. Por outro lado, as falhas de desempenho são causadas por queda de conectividade entre links importantes do núcleo de rede da RNP, sem causar no entanto perda de conectividade fim-a-fim entre a universidade e destinos no Brasil e no exterior. Nossos resultados mostram que falhas nos enlaces internacionais da RNP tem impacto desprezível no desempenho de conexões nacionais e que usuários modificam seu comportamento em função da indisponibilidade de serviços hospedados fora do Brasil. Por exemplo, o tráfego de entretenimento migra do Facebook para o YouTube, que permanece ativo durante as falhas; e a fração de tráfego interativo reduz gradativamente durante a falha, indicando evasão dos usuários da rede. Mostramos também que, durante as falhas parciais, aplicações assíncronas com servidores fora do Brasil, como Dropbox e SMTP, acumulam tarefas durante a falha e causam rajadas de tráfego quando a falha é restaurada. Durante falhas de desempenho, verificamos que estas impactam principalmente o volume de dados transmitidos e métricas como o RTT das conexões. Observamos também que em alguns momentos, ao contrário do esperado, há melhoras de algumas métricas de desempenho para alguns destinos. Isso ocorre pois alterações nas rotas utilizadas como caminho principal pelas transmissões podem melhorar seu desempenho. Nossos resultados podem ser aplicados na melhoria da infraestrutura de redes do backbone da RNP e na definição de parâmetros de configuração de rotas para minimizar o impacto de alguns tipos de falhas.

Palavras-chave: Caracterização. Redes de computadores. Impacto de Falhas.

ABSTRACT

In this paper we characterize the impact of failures in the RNP´s (Rede Nacional de Ensino e Pesquisa) network on data traffic at UFJF (Universidade Federal de Juiz de Fora). In particular, we study the impact of failures on traffic, user, and application behavior. We classify the failures we study into partial failures and performance problems. Partial failures are interesting in that they persist for several hours and impact only international links, so destinations hosted in Brazil remain reachable. On the other hand, performance problems, caused by the disruption of connectivity between important links in the RNP backbone, without causing loss of end-to-end connectivity between the university and destinations in Brazil and abroad. Our results show that, during partial failures, although failures in international links have negligible impact on the performance of national traffic, users do adapt their behavior to the unavailability of services hosted abroad. For example, entertainment traffic migrates from Facebook to YouTube, which remains reachable during the analyzed failures; and the fraction of interactive traffic gradually decreases during failures, indicating that users may leave the campus early. We also show that, during partial failures, asynchronous applications hosted abroad, like Dropbox and SMTP, queue up tasks during the failure and cause traffic bursts when the failure is restored. We found that performance failures primarily impact the volume of data transmitted and metrics such as RTT. We have observed that when performance problems occurs, contrary to expectations, the performance improves for some destinations, due to changes in the routes used as primary path for transmissions. Our results can be used to guide improvements in the infrasctruture of the RNP backbone and assist in better defining parameters of route configurations to minimize the impact of some kind of failures.

Keywords: Characterization. Computer Networks. Failures Impact.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Falhas de comunicação na Internet podem ser causadas por problemas de *hardware*, como rompimento de cabos, ou erros de *software*, como configuração inadequada de um roteador. A maioria destas falhas passa despercebida graças às mudanças automáticas de roteamento que as contornam usando rotas alternativas (MARKOPOULOU et al., 2008). No entanto, falhas causadas por erros de configuração de equipamentos ou ausência de rotas alternativas requerem intervenção humana e podem levar horas para serem solucionadas (KOMPELLA et al., 2007).

Embora a literatura seja rica em esforços para caracterizar anomalias e falhas na Internet (e.g., (MARKOPOULOU et al., 2008; TURNER et al., 2010; KOMPELLA et al., 2007; ZHANG et al., 2008; LAKHINA et al., 2004b)), o impacto desses problemas no tráfego e no comportamento dos usuários ainda é pouco conhecido (MARKOPOULOU et al., 2008). Além disso, o comportamento dos usuários e o tráfego da Internet mudaram ao longo dos anos. O volume de tráfego P2P, antes fração dominante do tráfego total, reduziu frente à popularização da distribuição de vídeo sob demanda via HTTP (SANDVINE, 2013). Aplicações interativas, como redes sociais, ferramentas colaborativas de edição de documentos e serviços bancários, são cada vez mais utilizadas pelos usuários de Internet. Novas aplicações estão disponíveis na nuvem e só podem ser utilizadas com acesso à rede. Em geral, a maior dependência da Internet para realização de várias tarefas diárias agrava o impacto de falhas de conectividade nos usuários.

Neste trabalho, investigamos o impacto de falhas no tráfego de um campus universitário. Para tal, caracterizamos o tráfego capturado do roteador de borda da Universidade Federal de Juiz de Fora (UFJF), instituição conectada à Internet por meio da Rede Nacional de Ensino e Pesquisa (RNP). Nossa base de dados contém sumários da grande maioria dos fluxos de entrada e saída da rede da universidade entre janeiro e novembro de 2013, compreendendo cerca de 65 mil arquivos de registros de log, que compactados ocupam um volume de aproximadamente 450 GB. Estes arquivos cobrem conexões por onde trafegaram mais de 250 TB de dados (seção 4.2). Em particular, caracterizamos mudanças no comportamento—volume, padrões e características do tráfego—dos usuários e das aplicações durante períodos em que, sabidamente, ocorreram falhas no Backbone da

RNP. Dividimos nosso estudo em dois tipos distintos de falhas descritas em nosso trabalho como falhas parciais e falhas de desempenho. As falhas parciais ocorreram em janeiro de 2013 e representam um cenário onde houve queda de comunicação com enlaces internacionais da RNP, impedindo totalmente o acesso à Internet comercial fora do Brasil. Um dos diferenciais deste tipo de falha é que as mesmas são parciais: apesar de destinos fora do Brasil terem ficado inacessíveis, destinos no Brasil praticamente não foram afetados. Os outros tipos de falha estudados são as falhas de desempenho, ocorridas entre julho e novembro de 2013, onde apesar da ocorrência de quebras de *links* importantes entre Pontos de Presença de RNP, a comunicação fim-a-fim não foi interrompida completamente e sim afetada pela utilização de rotas alternativas.

Nossos resultados, mesmo limitados a uma universidade, representam mais um passo na direção da melhor compreensão do impacto de falhas no comportamento dos usuários. Acreditamos que os resultados apresentados são particularmente interessantes para a comunidade de pesquisa em redes de computadores e podem motivar mudanças práticas do uso e do gerenciamento dos recursos de rede existentes.

Parte do trabalho desenvolvido nessa dissertação foi apresentado no XXXII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) , sob o título "Avaliação do Impacto de Falhas na Rede Nacional de Pesquisa no Tráfego de uma Universidade Federal", no dia 07 de maio de 2014.

1.1 CONTRIBUIÇÕES

As principais contribuições dessa dissertação são:

- Caracterização do tráfego de uma instituição de ensino brasileira.
- Descrição de diferentes aspectos observados durante a ocorrência de falhas, como impacto no tráfego agregado e no comportamento dos usuários e de algumas aplicações utilizadas.
- Análise da ocorrência de falhas em links de acesso Internet observada das perspectivas das estações finais e do comportamento dos usuários.
- Avanço no estado da arte dos estudos de monitoração de tráfego para observação de falhas, mostrando comportamentos e configurações desejáveis por parte de provedores de acesso e administradores de rede antes e durante os incidentes com perda de conectividade ou desempenho para evitar alguns efeitos negativos dos mesmos.

1.2 ORGANIZAÇÃO DA DISSERTAÇÃO

A dissertação está organizada da seguinte forma: o capítulo 2 apresenta conceitos teóricos importantes para o bom entendimento deste trabalho. O capítulo 3 mostra uma análise sucinta de alguns trabalhos que serviram de base para nossos estudos. No capítulo 4 mostramos o cenário onde foram realizados nossos estudos e a metodologia utilizada para coleta dos dados utilizados em nossa pesquisa. No capítulo 5 apresentamos os resultados de nossas análises dos dados coletados e inferências obtidas com o estudo dos mesmos. Finalizando, no capítulo 6 apresentamos a conclusão do trabalho, com algumas discussões sobre os resultados obtidos e indicações para trabalhos futuros que consideramos pertinentes.

2 CONCEITOS TEÓRICOS

Neste capítulo são apresentados conceitos importantes para o bom entendimento deste trabalho. Na seção 2.1 descrevemos as características gerais de sistemas de monitoração de tráfego e conceituamos as monitorações do tipo ativa (seção 2.1.1) e passiva (seção 2.1.2). Finalizamos o capítulo, apresentando na seção 2.1.3 uma descrição do projeto e funcionamento da ferramenta de coleta e análise Tstat (*TCP STatistic and Analysis Tool*) utilizada em nossos estudos.

2.1 MONITORAÇÃO DE TRÁFEGO

A área de monitoração do tráfego Internet é considerada de grande interesse para o estudo de redes desde os primórdios da Internet. Com a criação da ARPANET, as primeiras transmissões de dados utilizando suas estruturas já eram monitoradas (THOMPSON et al., 1997). Mesmo durante o período em que a administração da ARPANET era centralizada (realizada pela NSFNET), pontos de medição já estavam disponíveis na rede permitindo a caracterização do tráfego.

Com o tempo, a Internet cresceu exponencialmente em vários aspectos, como o número de usuários e hospedeiros, aplicações e serviços fornecidos e também em sua complexidade. Este crescimento, aliado à grande dependência da Internet em diversos setores da sociedade demandam uma infraestrutura cada vez mais funcional e robusta de monitoramento e medição para seu bom funcionamento e para a pesquisa e descoberta de melhorias e avanços na área de redes de computadores.

Encontramos na literatura inúmeros trabalhos que buscam caracterizar anomalias e falhas na Internet através de análise de tráfego nos mais variados ambientes e sistemas espalhados pelo mundo. A organização CAIDA[1] (The Cooperative Association for Internet Data Analysis) conduz regularmente medições no tráfego da Internet, além de desenvolver ferramentas de análises e analisar amostras disponíveis de tráfego com o intuito de obter perspectivas sobre a composição, propriedades e evolução da carga de trabalho na Internet. Além disso disponibiliza links para um grande número de publicações técnicas e científicas na área de monitoração e análise de dados.

[1] `http://www.caida.org`

Uma infraestrutura de monitoramento de tráfego pode facilitar a pronta detecção e diagnóstico de muitos problemas endereçando alguns dos seguintes objetivos:

- Estabelecer linhas base de utilização para a modelagem de atividades normais ou anormais;
- Detectar e localizar problemas específicos da Internet;
- Identificar gargalos na rede;
- Manter arquivo de dados para análises de períodos longos e
- Possibilitar coletas de dados para fins específicos, como experimentos ou análises da rede.

Através da análise de dados obtidos com a estrutura de monitoramento é possível detalhar ocorrências consideradas anômalas nas redes de computadores, indicando falhas de diversos tipos ou até ataques que podem comprometer o bom funcionamento da rede. Entre os eventos detectados podemos citar (MURRAY et al., 2001):

- Falhas de dimensionamento, como falta de largura de banda;
- Falhas físicas, como mau funcionamento de hardware ou defeitos no cabeamento;
- Falhas de software ou má configuração de equipamentos críticos (como roteadores);
- Vulnerabilidades provocadas por usuários, como instalação de propagadores e ataques de negação de serviço.

Os impactos provocados por estes eventos tem dimensão variada, podendo muitas vezes passar despercebidos pelos usuários e em outros momentos serem catastróficos, interrompendo serviços e causando danos de difícil dimensionamento para os usuários servidos pela rede afetada.

Conforme (BARFORD; CROVELLA, 1999) técnicas para estudos do tráfego da rede podem ser divididas entre aquelas que usam técnicas de monitoramento passivo, que consistem tipicamente da coleta de pacotes de dados em algum ponto da rede, ou as que usam monitoramento ativo que injetam algum tipo de estímulo na rede e medem as respostas a este estímulo.

As características de técnicas de monitoramento ativo e passivo são detalhadas nas subseções seguintes. Vemos ainda em (MURRAY et al., 2001) que as metodologias de monitoramento, ativas ou passivas, em uma escala utilizável envolvem grande quantidade de dados, e alguns problemas devem ser confrontados. Entre estes problemas podemos citar os seguintes:

- Fato de a velocidade da coleta dos dados ser substancialmente maior que a análise dos mesmos;
- Inexistência de uma definição padrão de como obter uma cobertura de medições representativa de toda a Internet e
- Indefinição sobre uma correta identificação de taxas de amostragem suficientes para pesquisas.

Além disso a questão da confidencialidade dos dados coletados, removendo informações como os dados transmitidos e informações de identificação de usuários, é um pré-requisito fundamental, tanto para evitar vulnerabilidades de segurança, quanto para encorajar a cooperação e o compartilhamento de dados pesquisados.

2.1.1 MONITORAMENTO ATIVO

O monitoramento ativo (CLAFFY; MCCREARY, 1999) geralmente envolve injetar na rede pacotes de dados (também descritos como sondas). Estes pacotes são necessários para as medições esperadas com destino a um ou mais dispositivos alvos. Geralmente são esperadas, como reação a estes envios, respostas contendo informações sobre a rota utilizada para alcançar o destino e métricas de desempenho. Dentre as métricas de desempenho obtidas estão (PAXSON et al., 1998):

- Caminho percorrido entre dispositivos de roteamento;
- Atraso;
- Perda de pacotes e
- Características da largura de banda entre *hosts* entre outras.

Algumas vezes, as informações obtidas podem incluir ainda dados sobre o hospedeiro de destino, tais como:

- Estado do hospedeiro;
- Serviços disponíveis;
- Sistema operacional, etc.

No modelo apresentado na figura 2.1 observamos uma estação de origem enviando uma sonda para um destino específico. Conforme vai seguindo a rota para o destino, a sonda pode disparar, nos dispositivos por onde trafega, a emissão de pacotes de resposta que chegando ao emissor trazem informações coletadas em cada um dos dispositivos.

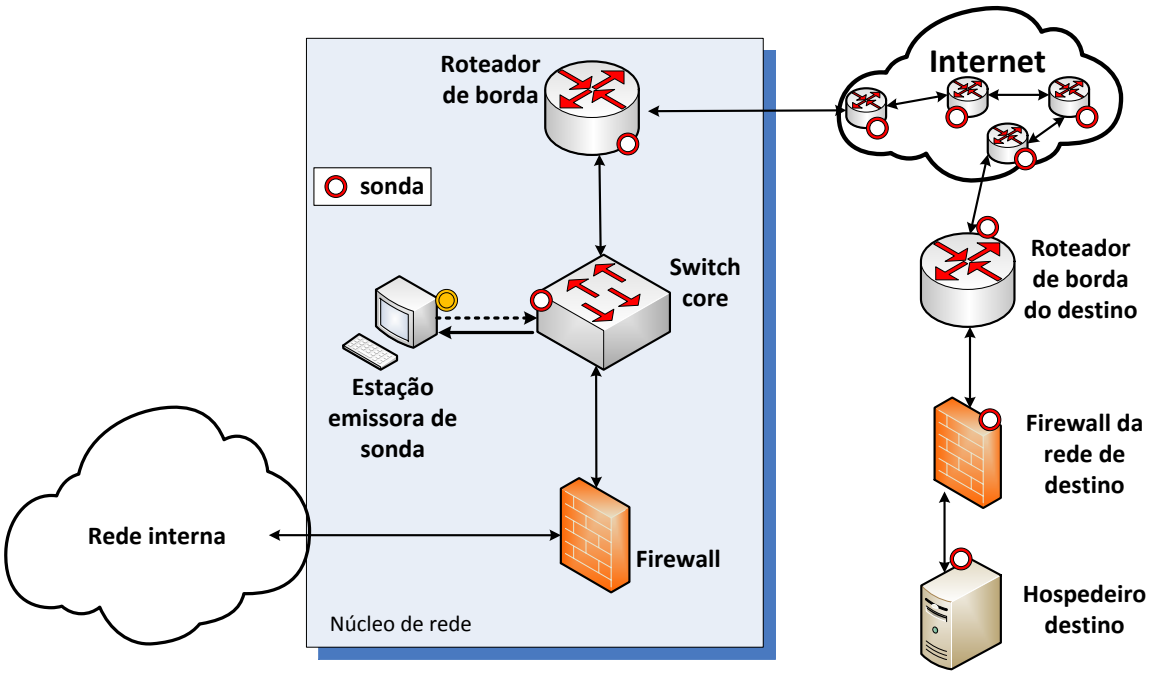


Figura 2.1: Modelo de coleta ativa.

O monitoramento ativo, por possuir características intrusivas, está sujeito a ser detectado por dispositivos como *firewalls* como tráfego hostil causando seu bloqueio antes da entrada no perímetro da rede local de destino. Como resposta a estas medidas de proteção, técnicas de monitoramento ativo têm sido aperfeiçoadas para acompanhar os crescentes níveis de segurança requeridos pelas instituições ligadas à Internet, tornando possível mapear os dispositivos e serviços oferecidos dentro de uma rede e assim descobrir vulnerabilidades que possam afetá-la.

Existem várias ferramentas de monitoramento ativo que podem ser utilizadas para medir a largura de banda em um caminho fim-a-fim, entre elas estão pathchar (JACOBSON, 1997), bprobe (CARTER; CROVELLA, 1996) e nettimer (LAI; BAKER, 2001). O aplicativo Traceroute (JACOBSON, 1989) é uma ferramenta que permite obter algumas métricas simples de caminhos entre *hosts*. TReno (MATHIS; ALLMAN, 1988) é utilizada para medir a capacidade de transmissão TCP em massa sobre um caminho Internet.

A maior vantagem deste tipo de monitoramento é a independência da existência de comunicações reais entre *hosts* para obtenção de dados sobre as conexões. No entanto é importante ressaltar que, apesar de oferecer visões sobre as condições da rede, as medições ativas podem afetar o desempenho da rede dependendo da quantidade de dados injetados

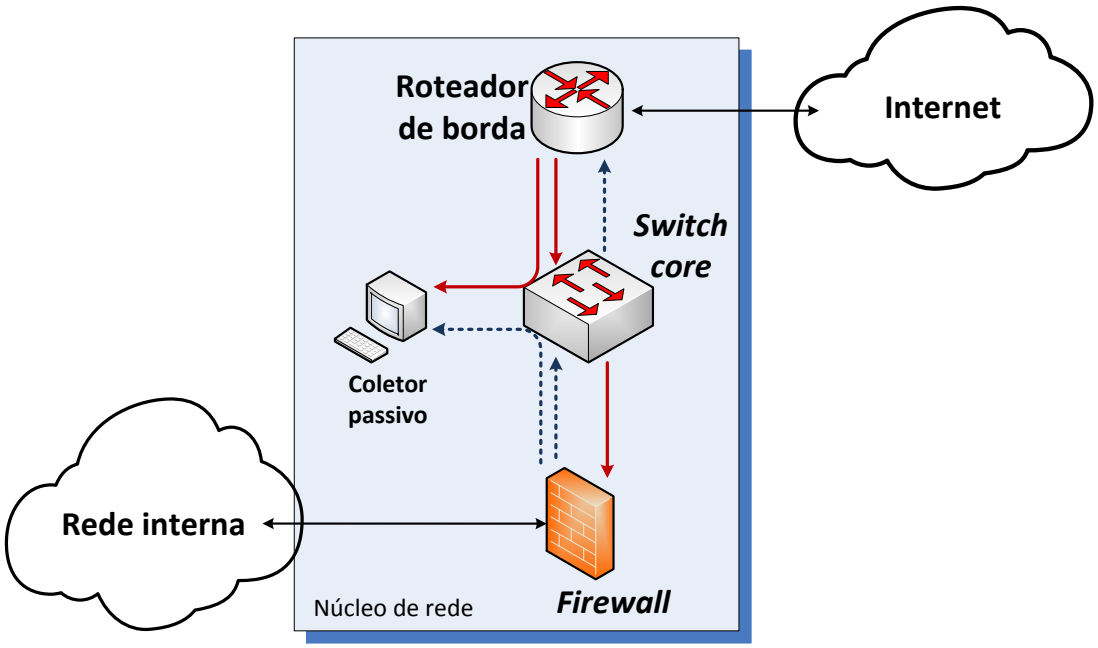


Figura 2.2: Modelo de coleta passiva.

na mesma, sendo esta uma desvantagem a ser observada.

2.1.2 MONITORAMENTO PASSIVO

Técnicas de monitoramento passivo, também referenciadas na literatura como medições de carga de trabalho (*workload*) (CLAFFY; MCCREARY, 1999), se baseiam na coleta de tráfego através de dispositivo(s) interno(s) a uma rede, como roteadores, switches ou até dispositivos independentes de monitoramento coletando passivamente informações ou até o próprio tráfego enquanto o mesmo trafega pela rede.

Observamos no modelo apresentado na figura 2.2 uma estação de coleta que recebe de um *switch* por onde passam os dados de entrada e saída para a Internet de uma rede específica, cópias de todos os pacotes trafegados entre a rede a Internet. É interessante observar que nenhum tráfego adicional que possa afetar o desempenho da rede é gerado, com exceção para as cópias dos pacotes que dependem apenas do desempenho da estação coletora e do *switch*, que deve estar habilitado para suportar o espelhamento de tráfego.

A grande vantagem apresentada por esta técnica de medição é não afetar o tráfego transportado pela rede durante o período de monitoramento. No entanto por depender absolutamente da presença do tráfego apropriado na rede estudada, pode ser muito mais

difícil ou até impossível extrair algumas informações desejadas dos dados disponibilizados pela coleta.

Os resultados obtidos com medições passivas vão desde taxas de utilização de banda e distribuição de uso de diversos protocolos até a detecção de intrusões (MOHAN et al., 2011). Ferramentas como o *Wireshark* (OREBAUGH et al., 2006) (evolução do *Ethereal*) e o *tcpdump* (JACOBSON et al., 1989) estão atualmente entre as ferramentas mais utilizadas para monitoramento passivo (FUENTES; KAR, 2005).

A organização CAIDA desenvolve e mantém o projeto *CoralReef* (MOORE et al., 2001) para coleta e análise de dados obtidos através de monitores passivos de tráfego Internet, tendo inclusive desenvolvido um pacote de *software* com a colaboração e o apoio da comunidade de *Internet Measurement*.

2.1.3 FERRAMENTA TSTAT

Em meados de 2001 uma equipe do Grupo de telecomunicações em redes da *Politecnico di Torino* iniciou o desenvolvimento de uma ferramenta, o Tstat (*TCP STatistic and Analysis Tool*) (MELLIA et al., 2001). Com seu núcleo baseado no código fonte do *TCPtrace* (OSTERMANN, 2000), esta ferramenta permite que o tráfego seja avaliado em um *host* de borda de forma a possibilitar que os fluxos de entrada e saída sejam correlacionados buscando por conexões bidirecionais cliente-servidor (MELLIA et al., 2003). Outro objetivo do desenvolvimento do Tstat é permitir a produção de dados estatísticos a partir de traces de pacotes de rede. Em nosso trabalho utilizamos o Tstat como ferramenta de coleta de dados.

O Tstat possibilita a análise de pacotes capturados em tempo real, utilizando computadores pessoais com hardware padrão ou placa de redes desenvolvidas especificamente para a captura de dados, bem como a análise de pacotes previamente capturados, importando vários formatos de arquivos de coletas, como os suportados pela biblioteca *libpcap* além de vários outros.

A ferramenta captura as informações de cabeçalho dos pacotes trafegados na rede, armazenando-as em arquivos de log contendo uma linha de registros para cada fluxo de dados estabelecido entre dois *hosts*. Conforme o posicionamento da estação de coleta, é possível capturar os dados internos ou externos à rede que se deseja estudar. A figura 2.3 mostra um modelo de coleta similar ao utilizado em nosso trabalho com o coletor

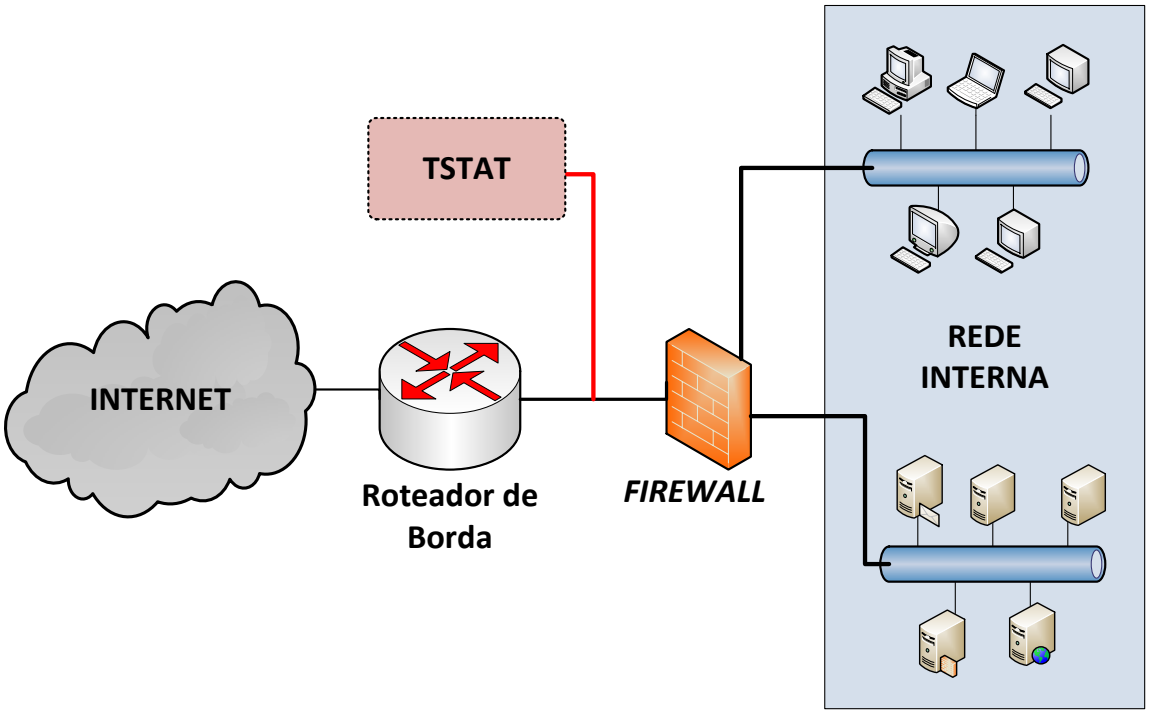


Figura 2.3: Modelo de posicionamento de um coletor Tstat.

posicionado entre o roteador de borda e o *firewall* que protege uma rede interna.

Nos registros capturados, são identificadas as estações que iniciaram os fluxos (clientes) e as que receberam as solicitações (servidores) identificando separadamente as informações referentes a cada sentido do fluxo. Além disso, com base em informações passadas na configuração da ferramenta, é possível identificar se cliente e servidor estão posicionados dentro ou fora da rede estudada. Outra informação obtida pelo Tstat é o protocolo da camada de transporte utilizado nos fluxos, TCP ou UDP, sendo esta informação utilizada para dividir os registros gravados em diferentes arquivos dependendo do protocolo.

Também é permitida pela ferramenta, a criação de padrões diferentes de captura, dependendo do tipo de fluxo a ser estudado gerando então arquivos personalizados de log com informações relevantes ao formato definido. Na tabela 2.1 vemos alguns exemplos de arquivos de logs específicos gerados pelo Tstat. Destacamos a linha 5 da tabela, onde é mostrado o arquivo padrão de captura de fluxos relacionados a conexões de vídeo, sendo os registros deste arquivo um subconjunto dos registros do log gravado em log_tcp_complete com colunas adicionais que possuem maior relevância para conexões do *YouTube* e outros *streams* de vídeo.

Para nosso estudo, em razão da predominância absoluta tanto em volume quanto em

Tabela 2.1: Exemplos de arquivos padrões de log gerados pelo Tstat

Arquivo	Fluxos	Descrição
log_tcp_complete	TCP completos	fluxos TCP corretamente encerrados
log_tcp_nocomplete	TCP incompletos	fluxos TCP não finalizados
log_udp_complete	UDP	fluxos UDP capturados
log_skype_complete	Skype	fluxos Skype capturados
log_video_complete	vídeo	fluxos TCP relacionados a conexões de vídeo

número de conexões do tráfego utilizando o TCP, utilizamos nas análises as conexões identificados pelo Tstat como TCP completo, ou seja, estabelecidas através do *Three-way Handshake* e encerradas de forma normal conforme os padrões do protocolo.

Alguns dos campos gravados pelo aplicativo nos arquivos log_tcp_complete gerados são mostrados na tabela 2.2. Na tabela 2.2(a) vemos as métricas sumarizadas em pares por direção do fluxo (uma métrica para enviados pelo cliente e outra para os enviados pelo servidor), sendo consideradas por padrão pela ferramenta as máquinas que iniciam a conexão como clientes e as que respondem à conexão como servidores. Na tabela 2.2(b) apresentamos métricas globais para as conexões.

Na tabela 2.2(c) mostramos alguns tipos de conexões identificados pela ferramenta (através de um banco de assinaturas do próprio Tstat), representados pelo campo Tipo de conexão e alguns exemplos de subtipos de conexões HTTP que são registrados no campo Tipo HTTP dos arquivos de log. É possível obter maiores detalhes sobre cada um dos campos, bem como sobre outros tipos de arquivos de log gerados pela ferramenta no *site* do projeto Tstat[2], existindo ainda a possibilidade da customização de novos tipos de registros baseados em informações de outras aplicações ou protocolos conforme os requisitos dos estudos.

[2] `http://tstat.polito.it/measure.shtml#LOG`

descrição abreviada	unidade	descrição detalhada
Endereço IP do Cliente/Servidor	-	-
Porta TCP do Cliente/Servidor	-	-
Pacotes	-	número total de pacotes enviados pelo cliente/servidor
bytes únicos	bytes	número de bytes de dados enviados pelo cliente/servidor
bytes de dados	bytes	número de bytes de dados enviados pelo cliente/servidor, incluindo retransmissões
pacotes retransmitidos	-	número de segmentos retransmitidos
bytes retransmitidos	bytes	número de bytes retransmitidos
rtt médio	ms	RTT médio computado medindo o tempo decorrido entre o segmento de dados e o ACK correspondente
rtt min	ms	RTT mínimo observado durante a conexão
rtt max	ms	RTT máximo observado durante a conexão
Desvio padrão do rtt	ms	desvio padrão do RTT

(a) Pares de métricas separados por direção do fluxo (C2S ou S2C).

descrição abreviada	unidade	descrição detalhada
Duração	ms	duração do fluxo do primeiro ao último pacote
Tempo de início (abs)	ms	Tempo absoluto (*epoch*) do primeiro pacote do fluxo
C Interno	0/1	1 = cliente tem IP interno, 0 = cliente tem IP externo
S Interno	0/1	1 = servidor tem IP interno, 0 = servidor tem IP externo
Tipo da conexão	-	Bitmask do tipo de conexão conforme identificado pelo mecanismo de inspeção do TCP
Tipo HTTP	-	Para fluxos HTTP, o conteúdo HTTP identificado

(b) Exemplos de métricas únicas para todo o fluxo.

tipo de conexão
HTTP
RTSP
RTP
MSN
P2P
SKYPE
SMTP
POP3
IMAP4
SSL/TLS
SSH 2.0/1.99
RTMP
Bittorrent MSE/PE

tipo HTTP	descrição
HTTP_GET	comando GET não classificado
HTTP_POST	comando POST não classificado
HTTP_MSN	Chat MSN tunelado sobre HTTP (POST)
HTTP_YOUTUBE_VIDEO	Download de vídeo YouTube (GET)
HTTP_VIDEO_CONTENT	Download de vídeo genérico FLV ou MP4 (GET)
HTTP_WIKI	Wikipedia (GET)
HTTP_RAPIDSHARE	Download de arquivo RapidShare (GET)
HTTP_FACEBOOK	Conexões *Facebook-related* (GET/POST)
HTTP_ADV	*Site advertisement* (GET)
HTTP_FLICKR	Download de fotos Flickr (GET)
HTTP_YOUTUBE_SITE	Download de conteúdo do site YouTube (GET)
HTTP_TWITTER	Tráfego não criptografado Twitter (GET/POST)
HTTP_DROPBOX	Tráfego Dropbox (GET)

(c) Tipo da conexão por protocolo e subtipos HTTP identificada pelo Tstat.

Tabela 2.2: Exemplos de métricas sumarizadas pelo Tstat.

3 TRABALHOS RELACIONADOS

A área de monitoramento de redes de computadores surgiu devido à necessidade básica de se verificar e mensurar o funcionamento das redes e detectar e corrigir erros em seu funcionamento de forma ágil e precisa. Conforme vemos em (STINE, 1990) já no início da década de 90, inúmeras ferramentas de monitoramento já existiam e eram utilizadas por administradores, operadores e até usuários de redes.

Com o passar do tempo e a evolução das redes, ficou clara a necessidade de se analisar e caracterizar cuidadosamente o tráfego como forma de se propor melhorias na configuração e operação das redes e se preparar de forma adequada para as tendências apontadas pelas análises. Em (ANAGNOSTAKIS et al., 2002) os autores apontam a crescente importância do monitoramento como parte vital das infraestruturas de rede modernas.

Entre 1988 e 1995, período em que a NSFNET (uma das precursoras da Internet atual) possuía administração centralizada e um *backbone* de Internet único com pontos de medição disponíveis, vários estudos foram publicados no sentido de caracterizar o tráfego (THOMPSON et al., 1997). Em 1993, (CLAFFY et al., 1993) apresentou uma série de características do tráfego da NSFNET, que era na época um *backbone* T1, como a predominância das aplicações utilizando protocolos como FTP e SMTP sobre outros protocolos e uma distribuição bimodal dos tamanhos de pacote indicando uma mistura de transferências em massas de dados com aplicações interativas.

Ainda nesta época, (Heimlich, HEIMLICH; FRAZER, 1996) mostraram as tendências de crescimento do tráfego da NSFNET. (FRAZER, 1996) aponta ainda um crescimento exponencial do tráfego em 1994 e o aparecimento de aplicações como *Gopher* e a *Web*, iniciando a tendência de uma futura superação dos tráfegos de e-mail e transferência de arquivo pelo tráfego *web* na mistura de tráfego.

Com o fim da NSFNET em 1995, surgiram vários *backbones* comerciais e estudos em larga escala de medições de tráfego passaram a ser publicados em menor frequência neste ambiente mais competitivo, conforme (THOMPSON et al., 1997). Por outro lado, alguns provedores comerciais de Internet aproveitaram a capacidade de fazer medições em seus próprios *backbones* com alto nível de detalhes (MCROBB; HAWKINSON, 1997).

A dificuldade em se obter medições fim-a-fim em escalas maiores que sites únicos foi

explicitada por Paxson, entre 1994 e 1999, através de uma série de estudos (PAXSON, 1999), percorrendo por áreas como patologias de roteamento, características de perdas de dados, comportamento de implementações TCP específicas, variações de atrasos e enfileiramento de pacotes.

Vários estudos de caracterização de tráfego publicados concentram seu foco no núcleo da rede utilizando dados de grandes *backbones* como em (MARKOPOULOU et al., 2008) onde é feita uma análise, classificação e caracterização de falhas e seus tipos baseado no *backbone* da Sprint que utilizando atualizações de roteamento IS-IS. Ainda utilizando como objeto de estudo o *backbone* da *Sprint* (IANNACCONE et al., 2002) analisa a ocorrência de falhas no *backbone* e impactos em serviços emergentes na época, como VoIP, buscando endereçar deficiências através da análise das falhas.

Seguindo a tendência de utilizar o core da rede como (KATZ-BASSETT et al., 2008) combinou o monitoramento passivo através de "*feeds*" BGP de toda a rede com monitoramento ativo das bordas da Internet, disparando *probes* em casos de suspeitas de falhas para descobrir e localizar *black holes* (problemas de acessibilidade na Internet onde rotas existem para um destino, mas os pacotes não conseguem chegar até ele) e classificá-los. Desta forma, os autores identificaram entre outras coisas que os problemas possuem extensão bem maior que o esperado e que a maioria dos problemas detectados são ligados à topologia das redes e de acessibilidade parcial (apresentando vários casos onde um Sistema Autônomo está inacessível através de um de seus provedores, mas não de outros).

O estudo anomalias é recorrente nas publicações relacionadas a monitoramento, como em (ZHANG et al., 2004) que direciona seus estudos para serviços com grande área de abrangência como sistemas P2P e redes de distribuição de conteúdo. Combinando monitoramento passivo para detectar anomalias no comportamento da rede com *probes* de múltiplos nós para quantificar e caracterizar o escopo destas anomalias.

Em (LAKHINA et al., 2004b,a) os autores propõem um método para identificação de anomalias baseado em volume de tráfego separando o espaço de medição do tráfego em dois subespaços determinados "normal" e "anômalo" e aplicam o método em uma grande rede acadêmica americana (Abiliene) definindo, caracterizando e exemplificando os tipos de anomalias encontrados.

(NGUYEN; THIRAN, 2004) definem em seu artigo uma estratégia para se obter informações da rede através de medições fim-a-fim, denominada "tomografia da rede" e

determina as falhas através de alterações observadas nos caminhos seguidos pelo tráfego.

Nos últimos anos observamos alguns trabalhos que utilizaram mineração "oportunística" de fontes de dados de "baixa qualidade" (como arquivos de configuração de roteadores, arquivos de *syslog* e anúncios de listas de e-mail operacionais) para apresentar um método de reconstrução do histórico de eventos de falhas em um sistema autônomo (AS) (TURNER et al., 2010).

Os autores (GILL et al., 2011) realizaram análises em larga escala de falhas de redes de datacenters, buscando caracterizar padrões de falhas neste tipo específico de rede e entender sua confiabilidade global em três dimensões, caracterizando elementos de redes mais suscetíveis a falhas, estimando o impacto destas falhas e analisando a efetividade da redundância de rede.

Algumas publicações acompanham tendências específicas e fatos históricos. Algumas publicações apresentam análises de quedas de rede causadas por motivos políticos, como em (DAINOTTI et al., 2011), onde os autores analisam quedas de rede causadas por episódios de censura na Líbia e no Egito onde os governos utilizaram o botão "matar a Internet" durante protestos ocorridos nestes países. Os autores utilizam fontes de dados diversificadas, como dados coletados do projeto *UCSD network telescope*[1], dados BGP do *Routeviews*[2] e do *RIPE NCC's Routing Information Service*[3] e *probes* do projeto Ark[4] para documentar as interrupções. Além disso, os autores demonstram o uso de tráfego para identificar os bloqueios e detalhar eventos prévios, como filtragem de pacotes indicando a possibilidade da formação de uma base para automação de alerta prévio de detecção de supressão de serviços Internet.

Destacamos ainda o estudo (TURNER et al., 2013) que apresenta uma comparação da fidelidade dos dados sobre falhas obtidos de mensagens de e-mails trocadas entre operadores e *syslog* com dados de "alta-qualidade" derivados de análises de mensagens do protocolo de roteamento IS-IS. O estudo mostra que os dados de *syslog* e e-mails são considerados de baixa qualidade necessitando de contabilização mais precisa falha-a-falha, porém possuem um custo de obtenção muito inferior, detectando-se ainda grandes diferenças (desacordos) entre os dois tipos de fontes comparados, sendo as obtidas por IS-IS mais apuradas.

[1] `http://www.caida.org/projects/network_telescope/`
[2] `http://www.routeviews.org`
[3] `http://www.ripe.net/data-tools/stats/ris`
[4] `http://www.caida.org/projects/ark`

A ferramenta de coleta e análise Tstat (MELLIA et al., 2003) foi utilizada para análises no tráfego TCP da *Politecnico di Torino* (MELLIA et al., 2005) e para o estudo de anomalias no tráfego TCP (MELLIA et al., 2006).

O Tstat também foi utilizado em estudos específicos sobre comportamento do tráfego em tecnologias ou aplicações de redes específicas, como tráfego TCP em redes WiFi (FRANCESCHINIS et al., 2005), tráfego do Skype (BONFIGLIO et al., 2009), IPTV (MELLIA; MEO, 2010) e utilização de tráfego DNS para identificação de serviços e conteúdo na web (BERMUDEZ et al., 2012). Mais recentemente, foram publicados ainda, estudos sobre serviços de armazenamento em nuvem (DRAGO et al., 2013) como o *Dropbox* (DRAGO et al., 2012) entre diversos outros.

Apontamos como diferenciais de nosso estudo em relação a outras publicações, o foco das análises nos "end-points" das comunicações de rede, a observação do tráfego mais próximo do usuário e a análise, entre outros fatores, de suas mudanças de comportamento, bem como do comportamento indesejado de algumas aplicações assíncronas utilizadas nas redes internas.

4 CONJUNTO DE DADOS E METODOLOGIA DE COLETA

Esta seção detalha o conjunto de dados analisados e a metodologia utilizada para obtenção dos dados. Na subseção 4.1 detalhamos o ambiente de coleta, representado pela UFJF e seus *links* de acesso à Internet, descrevemos ainda, de forma uma pouco mais sucinta, o Backbone da RNP. Na subseção 4.2 descrevemos a metodologia adotada na coleta dos dados.

4.1 AMBIENTE DE COLETA

A rede da UFJF, onde foram coletados os dados deste estudo, integra 22 unidades e provê conectividade para aproximadamente 6.000 computadores, conectados por rede cabeada em laboratórios de pesquisa, escritórios de administração, salas de aula e pontos de acesso sem fio. A UFJF possui aproximadamente 19.000 alunos, 1.500 funcionários e 1.400 professores. A coleta realizada não captura o tráfego interno da universidade. Apesar de o tráfego interno ser interessante para análise, coletá-lo exigiria uma infraestrutura de coleta significativamente mais extensa, com um servidor de coleta em cada rede local.

Todo o tráfego de dados da UFJF com destino à Internet é enviado ao PoP-MG (ponto de presença da RNP em Minas Gerais), em Belo Horizonte, por dois enlaces ponto-a-ponto OC-3 com total de 310 Mbps de banda. A partir do PoP-MG, o tráfego da UFJF entra no *backbone* da RNP, que se encarrega de rotear o tráfego ao seu destino.

A RNP interliga praticamente todas as instituições públicas de ensino do Brasil, bem como algumas instituições governamentais (e.g., EMBRAPA). A infraestrutura da RNP é gerenciada em colaboração com pontos de troca de tráfego regionais operados por universidades, como o PoP-MG em Belo Horizonte. Empresas e redes comerciais podem se ligar à RNP nos pontos de troca de tráfego regionais, na maioria das vezes, via acordos de troca livre de tráfego (*peering*). O tráfego na RNP destinado a computadores fora do Brasil passa por enlaces internacionais. Atualmente, o mais importante desses enlaces liga São Paulo a Miami e tem banda de 20 Gbps. O tráfego da RNP destinado a empresas e redes conectadas aos pontos de troca de tráfego não utiliza os enlaces internacionais.

Neste trabalho nós avaliamos o impacto de falhas na Rede Nacional de Ensino e Pesquisa (RNP) em dados trafegados entre a Universidade Federal de Juiz de Fora (UFJF) e

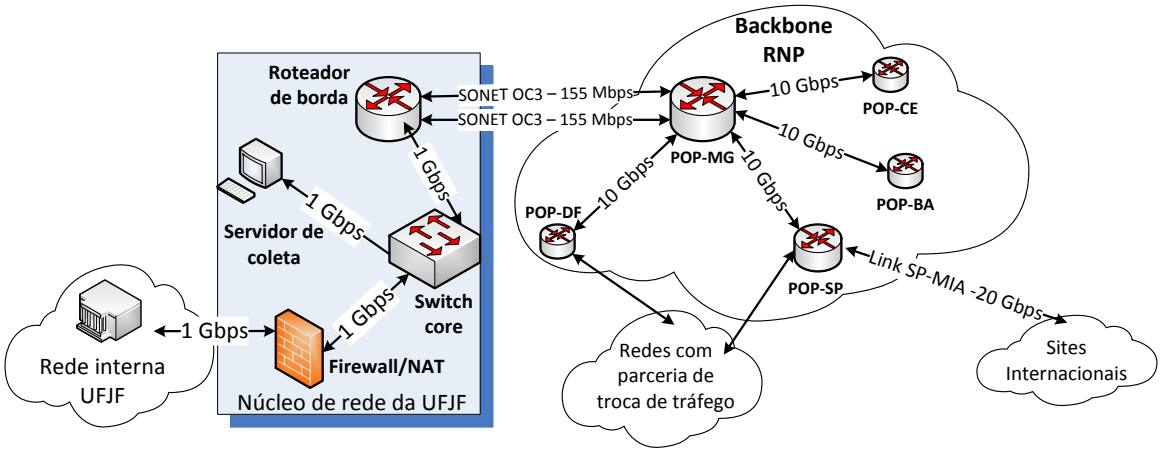


Figura 4.1: Ambiente de coleta de dados.

a Internet. A figura 4.1 apresenta uma visão geral do ambiente de coleta de dados. Considerando que todo o tráfego Internet da universidade passa pelo *Datacenter* da instituição, instalamos um chaveador (*switch*) entre o roteador de borda e o *firewall* da UFJF. O roteador de borda e o *firewall* são responsáveis por rotear e filtrar, respectivamente, todo o tráfego de entrada e de saída do campus. O *firewall* da UFJF também faz tradução de endereços (NAT) para alguns nós da rede interna. Adicionamos então à rede um servidor de coleta, ligando-o a uma porta no *switch* configurada para receber o espelhamento de todo o tráfego de entrada e saída para a Internet. O servidor de coleta, captura de forma contínua o tráfego, sumarizando as informações de cada conexão entre dispositivos da rede da Universidade com dispositivos externos usando o Tstat (FINAMORE et al., 2011). Os pacotes capturados são descartados após sumarização, preservando a privacidade dos usuários.

4.2 METODOLOGIA DE COLETA

Para as coletas realizadas em nosso trabalho foi posicionado um servidor de coleta entre o roteador de borda da UFJF e seu *firewall*. Este posicionamento permitiu que fossem coletados os tráfegos de entrada da Internet e também de saída viabilizando o correlacionamento dos pacotes e identificação dos fluxos pertencentes a conexões iguais pela ferramenta de coleta.

O servidor ficou diretamente conectado a um *switch* presente na infraestrutura da instituição e também ligado diretamente ao roteador e ao *firewall*. O tráfego foi direcionado para o servidor através de espelhamento de portas, onde foi espelhada a porta que recebia o tráfego vindo do roteador de borda com direção ao *firewall* e a porta que recebia o tráfego em sentido inverso, ou seja, partindo do *firewall* com destino ao roteador de borda.

Como servidor de coleta foi utilizado um computador com dois processadores Intel Xeon de 3.40GHz, 4 GB de memória RAM, um disco rígido com 300 GB e duas interfaces de rede Ethernet 10/100/1000 Mbps (uma conectada à porta recebendo o espelhamento do switch e a outra ligada à rede interna para acesso administrativo ao computador). Como sistema operacional utilizamos a distribuição Ubuntu do Linux, em sua versão 12.04.1 LTS por sua compatibilidade com a ferramenta de coleta (TSTAT). Este dimensionamento de *hardware* atendeu de forma satisfatória nossas expectativas, permitindo que a coleta de tráfego ocorresse com descarte de pacotes, por problemas de capacidade de processamento, praticamente nulo. O servidor utilizado foi dedicado exclusivamente às tarefas de captura e sumarização dos pacotes trafegados, evitando a concorrência por recursos com outros serviços de *software* ou aplicações.

Como ferramenta de coleta foi utilizado o Tstat, que efetuou ainda a sumarização do tráfego coletado, descartando os pacotes espelhados após este processo, de forma a preservar a privacidade dos usuários. As informações armazenadas no servidor de coleta se resumem portanto, a registros de cada fluxo de dados, contendo as métricas obtidas pelo Tstat, sem a retenção dos dados trafegados.

Após o processamento pela ferramenta, uma nova pasta é criada por hora no servidor, contendo os arquivos correspondentes à última hora de coleta. Em cada pasta é gravado, em tempo real, um conjunto de arquivos de texto em que cada linha corresponde a um fluxo diferente e cada coluna é associada a uma métrica específica. Cada arquivo na pasta apresenta colunas referentes ao tipo de tráfego sumarizado no log, como exemplo temos arquivos contendo a sumarização de fluxos TCP, fluxos UDP, fluxos de vídeo, entre outros.

Apesar de a coleta nos fornecer informações detalhas para fluxos de variados tipos, concentramos nossos estudos nos fluxos TCP completos, ou seja, aqueles fluxos TCP onde ocorre o processo de *three way handshake* e a conexão é fechada corretamente, através de segmentos FIN/ACK ou RST. Os fluxos sem indicação correta de fechamento da conexão

são armazenados em outro arquivo de log e não foram analisados em nosso estudo.

Maiores detalhes sobre o formato dos arquivos de log gerados pelo Tstat e cada métrica sumarizada pela ferramenta podem ser obtidos na página do projeto [1].

Optamos em nosso estudo por analisar somente os fluxos do tipo TCP pela expressiva predominância representada por este tipo de fluxo em relação aos fluxos UDP, correspondendo em média a cerca de 95% do volume de dados trafegado conforme observado em (MELLIA et al., 2005) e mantido no ambiente da UFJF.

O período de coleta compreendeu todo o ano de 2013, onde acumulamos cerca de 453 Gb de arquivos compactados contendo os logs, sendo cerca de 85% deste volume correspondente aos logs do tipo TCP completo.

Na tabela 4.1 mostramos algumas estatísticas aproximadas sobre os dados coletados e em 4.2 apresentamos os períodos de falha estudados indicando alguns detalhes sobre cada período e o tipo de falha relacionado. Apesar do processo de coleta ser contínuo, algumas interrupções do servidor ocorreram devido a falhas de hardware e de fornecimento de energia, fazendo com que a coleta fosse interrompida em alguns períodos. No entanto, as ocorrências de interrupções da coleta foram em pouca quantidade e raramente ultrapassavam o período de um dia, não afetando os resultados de nosso estudo.

Após a coleta dos logs, os mesmos foram processados de forma a gerar arquivos contendo somente os dados referentes aos períodos que foram objeto de nossas análises e alguns campos dos registros coletados pelo Tstat diretamente relacionados ao trabalho de pesquisa. Assim, conseguimos reduzir o volume total das informações coletadas, permitindo uma análise mais profunda dos dados mais importantes para nossos estudos.

As informações de localização geográfica e de domínios foram obtidas com a utilização de uma base de dados de geolocalização (MaxMind), que nos forneceu a localização geográfica por país, além de dados de domínio dos endereços IP participantes das conexões capturadas. Desta forma conseguimos identificar se as conexões eram feitas com sites nacionais ou internacionais e a quais domínios correspondiam os IPs externos à UFJF.

[1] `http://tstat.polito.it/measure.shtml#LOG`

Tabela 4.1: Dados sobre a pesquisa

Dados da coleta	
Período de coleta	de 01/01/2013 a 30/11/2013
Número de horas de coleta	aproximadamente 7500 horas
Volume compactado dos arquivos de log	aproximadamente 453 GB
Volume total trafegado	aproximadamente 252 TB
Número de conexões TCP sumarizadas	aproximadamente 2.8 trilhões

Tabela 4.2: Dados sobre as falhas estudadas

Início da falha	**Duração**	**Impactos**	**Tipo de falha**
07/01/2013 - 14:45 BRST	9 hs	volume e sessões	parcial
09/01/2013 - 08:05 BRST	12 hs	volume e sessões	parcial
10/01/2013 - 12:35 BRST	7 hs	volume e sessões	parcial
09/07/2013 - 08:48 BRT	5 hs	volume	desempenho
19/08/2013 - 08:10 BRT	4.5 hs	volume	desempenho
28/08/2013 - 15:10 BRT	3.5 hs	volume	desempenho
21/11/2013 - 09:00 BRST	7.5 hs	volume	desempenho

5 AVALIAÇÕES

Neste capítulo são apresentados os resultados obtidos em nossas análises. Focamos as análises em dias de falhas anunciadas pela RNP. Em particular, estudamos dos tipos específicos de falhas. Na subseção 5.1 analisamos falhas parciais onde o acesso à Internet não é totalmente interrompido. De acordo com relatórios publicados pela RNP,[1] nos dias 7, 9 e 10 de janeiro de 2013 ocorreram falhas na infraestrutura de fibra óptica de algumas operadoras de telecomunicação. Essas falhas impossibilitaram o acesso aos enlaces internacionais da RNP. Consequentemente, destinos e serviços hospedados fora do Brasil ficaram inacessíveis, mas destinos conectados aos pontos de troca de tráfego da RNP continuaram acessíveis. Argumentamos que falhas globais têm impacto forte mas simples no tráfego - interrompendo-o por completo - e que falhas parciais são mais interessantes de analisar.

Na subseção 5.2 analisamos falhas de desempenho, caracterizadas por interrupções em enlaces internos do backbone, afetando apenas a troca de tráfego entre POPs intermediários, tornando indisponíveis poucos links sem redundância de rotas. Estudamos quatro falhas deste tipo ocorridas nos meses de julho, agosto (duas ocorrências) e novembro de 2013. Em geral, estas falhas foram documentadas pela RNP como rompimentos de fibras de operadoras, causando interrupção do link entre um ou mais pares de POPs no backbone da RNP.

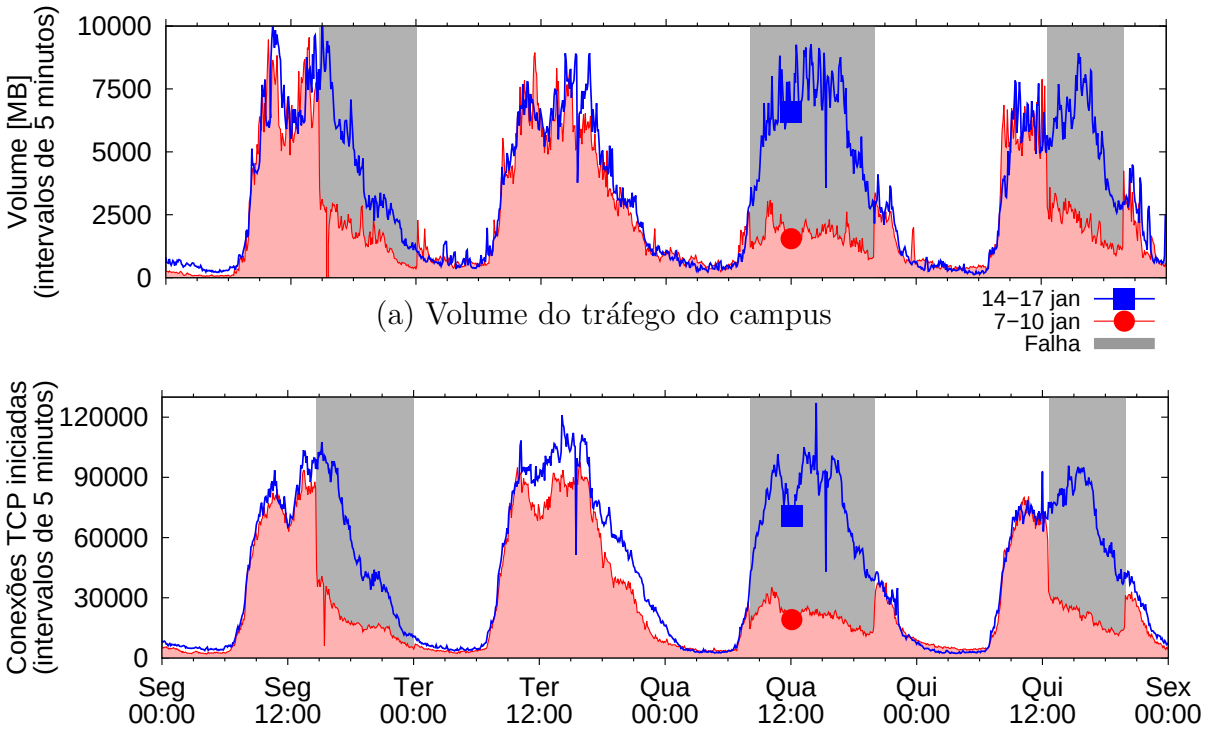
5.1 FALHAS PARCIAIS

Inicialmente, iremos estudar falhas parciais. Iremos verificar o impacto dessas falhas no tráfego do campus, no comportamento dos usuários e nas aplicações.

5.1.1 IMPACTO DAS FALHAS NO TRÁFEGO AGREGADO

A figura 5.1 apresenta uma visão geral do tráfego na rede da UFJF durante dois períodos distintos, cada um cobrindo quatro dias consecutivos, correspondentes a dias letivos do calendário acadêmico. A sazonalidade do tráfego durante o período letivo explica a opção por comparar o tráfego dos dias de falha com o tráfego de dias de semana imediatamente

[1] `http://www.rnp.br/backbone/weblog/arquivo/arquivo_2013-m01.php`



(a) Volume do tráfego do campus

(b) Número de conexões TCP no campus

Figura 5.1: Visão geral do tráfego de dados na rede da UFJF.

anteriores ou posteriores, uma vez que buscamos comparar períodos que possuam maior similaridade. A figura 5.1(a) mostra o tráfego total, agregado em intervalos de cinco minutos. Como o TSTAT grava apenas o total de bytes trafegados e a duração de cada fluxo, nós distribuímos os bytes de um fluxo uniformemente ao longo de sua duração. A figura 5.1(b) mostra o número de conexões TCP iniciadas em intervalos de cinco minutos. As linhas azuis, marcadas com um quadrado, mostram o tráfego total e o número de conexões iniciadas no período de 14 a 17 de janeiro de 2013, quando nenhuma falha foi reportada pela RNP. As linhas vermelhas, marcadas com um círculo, mostram o tráfego e o número de conexões iniciadas entre os dias 7 e 10 de janeiro de 2013, quando a RNP reportou três falhas. Todos os períodos cobrem dias de semana de segunda a quinta-feira (optamos por não incluir nos gráficos as sextas-feiras, por apresentarem padrão de tráfego similar aos outros dias de semana mostrados). As falhas ocorreram de 14:45 do dia 7 às 00:05 do dia 8 de janeiro, de 08:05 à 20:00 do dia 9 de janeiro e de 12:35 à 19:55 no dia 10 de janeiro (horários de verão de Brasília); nós sombreamos estes períodos na figura 5.1. Note que, devido à greve de 2012 e consequente adaptação do calendário acadêmico, as aulas na UFJF foram retomadas dia 7 de janeiro, fazendo com que o período estudado corresponda a dias intermediários do período letivo.

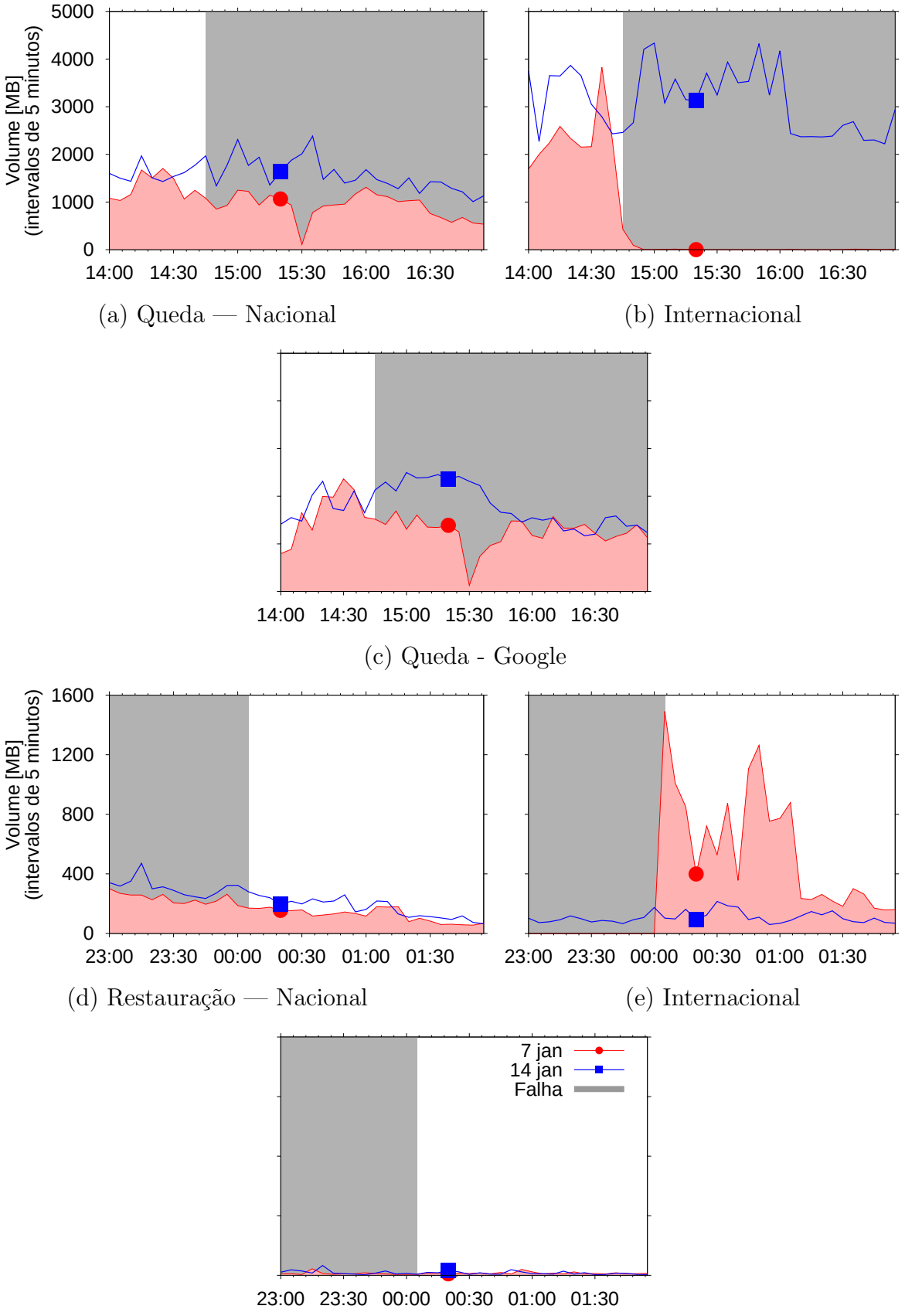
Em geral, o tráfego apresenta o típico padrão de uso diurno, com pico entre 10 e 16 horas e mínimo durante a madrugada. O aumento do tráfego a partir das 7 horas é mais acentuado que sua redução a partir das 18 horas. Isso ocorre devido à existência de cursos noturnos com quantidade de alunos menor que os cursos diurnos. Note que o impacto das falhas no volume total é imediato devido à interrupção do tráfego internacional. O volume de tráfego aumenta imediatamente após a restauração das falhas.

O comportamento do número de conexões TCP iniciadas é qualitativamente similar. Tentativas de conexões a destinos fora do Brasil durante a falha nunca são completadas com sucesso, são marcadas como conexões incompletas pelo TSTAT e não são contabilizadas na figura 5.1(b). O comportamento do número de conexões TCP ativas (ao contrário de iniciadas), também é qualitativamente similar pois as conexões internacionais também são interrompidas pelas falhas (não mostrado).

5.1.2 IMPACTO DAS FALHAS POR GEOLOCALIZAÇÃO DOS DESTINOS

Nós separamos o tráfego total em três conjuntos: tráfego nacional, com destino no Brasil, tráfego internacional, com destino fora do Brasil, e tráfego para serviços do Google. Nós separamos tráfego para serviços do Google porque eles continuam acessíveis durante as falhas através do Ponto de Troca de Tráfego em São Paulo; além disso, grande parte do tráfego do campus é do *YouTube* (seção 5.1.4). Nós classificamos tráfego entre nacional e internacional usando a base de dados livre do *MaxMind*. Apesar das limitações conhecidas para bases de dados de geolocalização, a precisão é suficiente para a granularidade da nossa classificação (POESE et al., 2011). Para classificar o tráfego do Google, nós resolvemos os endereços IPs associados a domínios de serviços do *Google* (e.g., youtube.com, gmail.com, google.com). Nós classificamos como tráfego para o Google qualquer conexão com endereço de origem ou destino nos prefixos referentes a estes IPs nas tabelas de roteamento do PTT-Metro em São Paulo.

A figura 5.2 mostra a variação dos tráfegos nacional, internacional e para serviços do Google durante períodos de três horas que cobrem o início (figuras 5.2(a–c)) e o término (figuras 5.2(d–f)) da falha do dia 7 de janeiro. Para fins de comparação, a figura mostra curvas correspondentes também para o dia 14 de janeiro, mesmo dia da semana mas sem falha reportada. Como na figura 5.1, nós mostramos o volume em intervalos de cinco minutos e o período de falha está sombreado.



(a) Queda — Nacional

(b) Internacional

(c) Queda - Google

(d) Restauração — Nacional

(e) Internacional

(f) Restauração - Google

Figura 5.2: Detalhe do impacto da falha no tráfego durante o início da falha (linhas 1 e 2) e durante a recuperação da falha (linhas 3 e 4) no dia 7 de janeiro.

As figuras 5.2(a) e (c) mostram que o início da falha não causa impacto imediato significativo nos tráfegos nacional e para o Google. Porém, o tráfego internacional rapidamente cai para zero. O vale mostrado em ambas as curvas por volta das 15:30 do dia 7 de janeiro foi causado por uma falha local na UFJF (reinício do roteador de borda). No momento de restauração da falha ocorre uma rajada de tráfego internacional (figura 5.2(e)) gerada por aplicações assíncronas, como detalharemos na seção 5.1.6. Observamos impacto semelhante no número de conexões TCP (não mostrado).

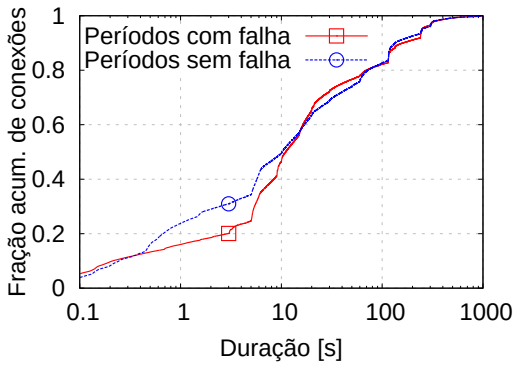
5.1.3 IMPACTO DAS FALHAS EM CARACTERÍSTICAS E DESEMPENHO DE CONEXÕES

Durante períodos de falha, as conexões TCP podem apresentar características diferentes das encontradas em períodos sem falha. A figura 5.3 mostra a distribuição acumulada da duração, latência fim-a-fim e taxa de transmissão das conexões durante um período que inclui do início à recuperação de uma falha e, para fins comparativos, um período de igual duração sem falhas. Os períodos mostrados são de 14:45 às 00:05 dos dias 7 (linha com quadrado) e 14 (linha com círculo) de janeiro.

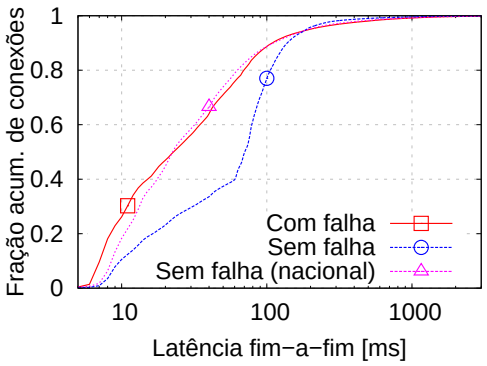
A Figura 5.3(a) mostra as distribuições acumuladas das durações das conexões TCP durante os períodos considerados. As distribuições são, em geral, similares exceto pela redução (em 54%) da fração de conexões com duração entre 0,5 e 3 segundos durante falhas e pelo aumento (em 16%) da fração de conexões com duração maior que 3 segundos. Como discutiremos na seção 5.1.4, uma causa para esse efeito está na mudança de comportamento dos usuários.

A figura 5.3(b) mostra as distribuições acumuladas da latência fim-a-fim das conexões TCP nos mesmos períodos. A diferença na latência entre os períodos com e sem falha resulta dos destinos acessados durante a falha estarem localizados em redes no Brasil e geograficamente mais próximos. Para uma comparação mais justa, mostramos também a latência fim-a-fim das conexões para destinos no Brasil durante o dia 14 (sem falha, linha marcada com um triângulo). Vemos que a falha não tem impacto na latência fim-a-fim das conexões com destino no Brasil.

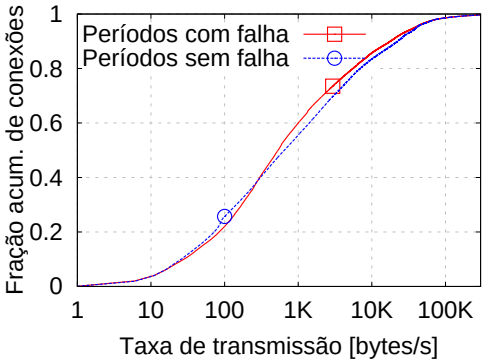
A figura 5.3(c) mostra que a distribuição acumulada da taxa de transmissão das conexões TCP durante o período considerado não é significativamente impactada pela falha. Isto indica que os enlaces não ficaram sobrecarregados durante a falha. Analisamos também a taxa de perda de pacotes das conexões TCP e não observamos diferenças signifi-



(a) Duração



(b) Latência fim-a-fim



(c) Taxa de transmissão

Figura 5.3: Comparação do desempenho das conexões TCP durante a falha do dia 7 de janeiro com o mesmo período do dia 14 de janeiro (sem falha).

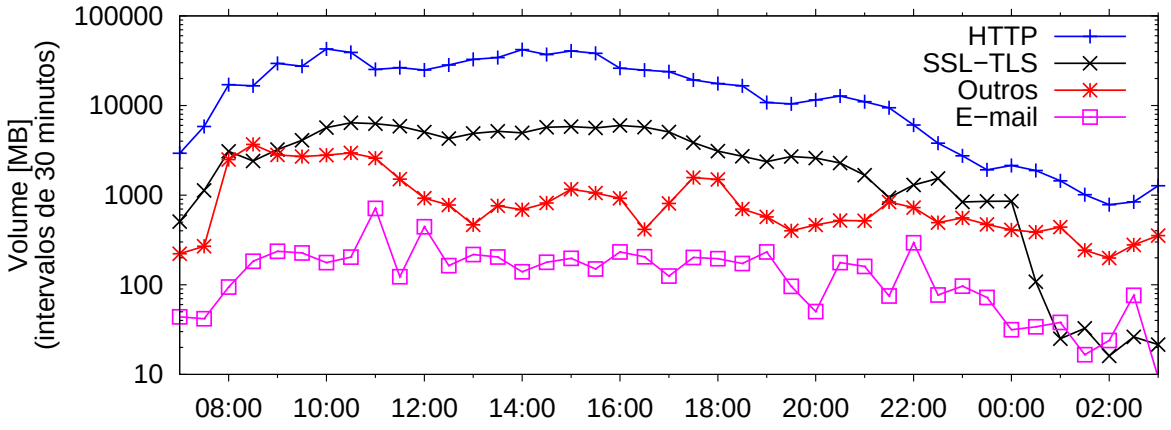
cativas entre períodos com e sem falhas. Em ambos os casos, a porcentagem de tráfego transferido em retransmissões é menos de 1,5% do tráfego total.

5.1.4 IMPACTO DAS FALHAS NO COMPORTAMENTO DOS USUÁRIOS

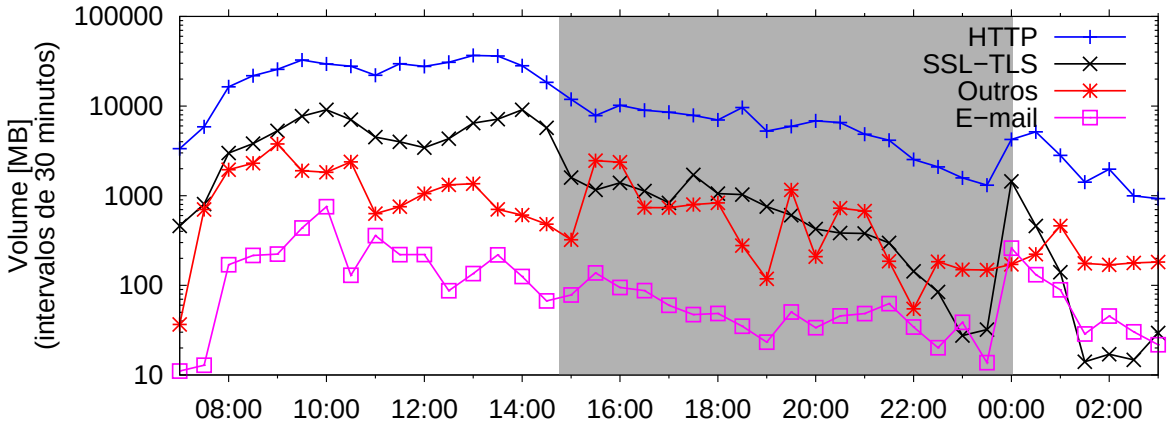
Nesta seção analisamos o impacto das falhas em características do tráfego para inferir modificações no comportamento dos usuários da rede. Discutimos redução da quantidade de tráfego interativo e modificações da mistura de aplicações utilizadas durante falhas.

Iniciamos a sessão analisando a ocorrência de redução no tráfego interativo durante as falhas. A figura 5.4 mostra o volume total de tráfego de diferentes protocolos, segundo classificação do TSTAT, em intervalos de trinta minutos. A linha “E-mail” combina os protocolos POP, IMAP e SMTP. Os demais protocolos são agrupados na linha “Outros”.

Nós mostramos na figura 5.4(a) tráfego normal no dia 14 de janeiro, sem falha, e na figura 5.4(b) o tráfego no dia 7 de janeiro, com falha. O comportamento da quantidade de conexões TCP por protocolo ao longo do tempo é qualitativamente similar (não mostrado).



(a) Dia sem falha, 14 de janeiro



(b) Dia com falha, 7 de janeiro

Figura 5.4: Volume de tráfego por protocolo.

Apesar de mostrarmos apenas resultados para a falha do dia 7, os resultados apresentados também são válidos para as falhas dos dias 9 e 10 de janeiro.

Durante o período sem falhas, o volume de tráfego de cada protocolo se mantém relativamente estável entre 7:00 e 22:00 horas (figura 5.4(a)). O volume de tráfego criptografado (protocolo "SSL/TLS") diminui significativamente durante a madrugada. Em períodos de falhas, o volume de tráfego criptografado diminui gradativamente a partir do início da falha (figura 5.4(b)); compare, por exemplo, a quantidade de tráfego criptografado entre 20:00 e 20:30 dos dias 7 e 14 de janeiro (425 MB e 1.3 GB, respectivamente). Discutiremos os picos de tráfego criptografado e de e-mail após a restauração da falha na seção 5.1.6.

Como o tráfego criptografado é resultante primariamente de atividades dos usuários na rede,[2] acreditamos que os usuários deixam suas estações de trabalho para se dedicar a

[2]Por exemplo, um dos destinos com maior quantidade de conexões criptografadas em nossos dados é o site da Prefeitura de Juiz de Fora (http://pjf.mg.gov.br).

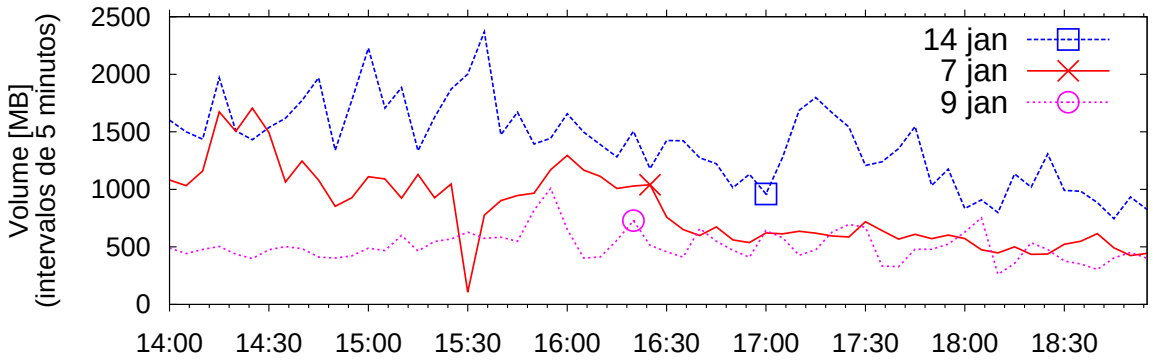


Figura 5.5: Modificação no volume de tráfego nacional devido às falhas.

outras atividades ou até deixam o campus prematuramente em função da falha de conectividade. Para testar a hipótese acima nós estimamos o número de usuários pela quantidade de conexões realizadas a serviços do Google. Não consideramos serviços como *Twitter* e *Facebook* porque estão hospedados fora do Brasil e, diferentemente de serviços do Google, ficam inacessíveis durante falhas. Às 17:00 horas do dia 7 de janeiro, aproximadamente 2 horas após o início da falha, a quantidade de conexões para serviços do Google era 45% menor que durante o mesmo período no dia 14, sem falha.

A figura 5.5 compara o volume de tráfego nacional nos dias 7 e 9 de janeiro (com falha) e no dia 14 de janeiro (sem falha). As falhas começaram às 14:45 e 8:05 nos dias 7 e 9 de janeiro, respectivamente (nesta figura não sombreamos as falhas). Vemos que mesmo o tráfego nacional, cujos serviços continuam acessíveis durante a falha, diminui no dia 7; mais um indicativo que usuários alteram seu comportamento. Além disso, no dia 9 o tráfego nacional nunca alcança o volume normal em dias sem falha; indicando que alguns usuários, que dependam da Internet para execução de suas atividades, talvez nem vão ao campus ao receber de colegas a notícia da falha de rede.

5.1.5 MODIFICAÇÕES DA MISTURA DE APLICAÇÕES

A tabela 5.1 compara tráfego das aplicações entre o período de falha de 14:45 à 00:05 dos dias 7 e 8 de janeiro com o mesmo período dos dias 14 e 15 de janeiro. O tráfego foi classificado em aplicações pelo TSTAT. Nós sumarizamos os resultados agregando aplicações como *Twitter*, MSN e *Flickr* em "Social", aplicações como *MegaUpload*, *HotFile* e *RapidShare* em "Hospedagem de Arquivos", aplicações como *BitTorrent* e *eDonkey* em "P2P" e provedores de anúncios em "Propaganda". Para cada conjunto de aplicações, nós

mostramos: a fração de suas conexões relativas ao total de conexões no período, a fração de seu tráfego relativo ao tráfego total no período, o volume de tráfego e o volume médio de suas conexões.

Como o *Facebook* é hospedado fora do Brasil, seu tráfego é reduzido a zero durante a falha. Em contrapartida, a fração de tráfego e conexões para o *YouTube* aumenta significativamente. Isso indica adaptabilidade dos usuários e uma migração das conexões de entretenimento para serviços que continuam disponíveis durante a falha. Notamos que a fração de conexões e tráfego nem sempre aumenta para aplicações que continuam ativas durante a falha (e.g., *Google Maps*).

Notamos que a fração do tráfego para serviços de hospedagem de arquivos é pequena. O tráfego de aplicações P2P como *Bittorrent* e *eDonkey* também é pequeno, em parte devido a regras de bloqueio no *firewall* da UFJF. Como o tráfego dessas aplicações é pequeno com e sem falha, não conseguimos observar mudança de comportamento. Por último, a redução da proporção de conexões HTTP POST corrobora nosso resultado anterior de redução do tráfego interativo e possível evasão dos usuários da rede.

Nós também analisamos as frações de conexões e tráfego associadas a cada conjunto de aplicações 30 minutos após a restauração das falhas (não mostrado). Nós observamos que um intervalo de 30 minutos é suficiente para que usuários percebam a restauração da falha e retornem para o comportamento normal. Por exemplo, 30 minutos é suficiente para que a fração de conexões ao *Facebook* se normalize. Para as falhas analisadas, o volume de tráfego fica alterado por algumas horas, devido a modificações no comportamento de aplicações (seção 5.1.6). Infelizmente todas as falhas analisadas foram restauradas durante a madrugada e não pudemos analisar nenhuma falha restaurada em horário de pico.

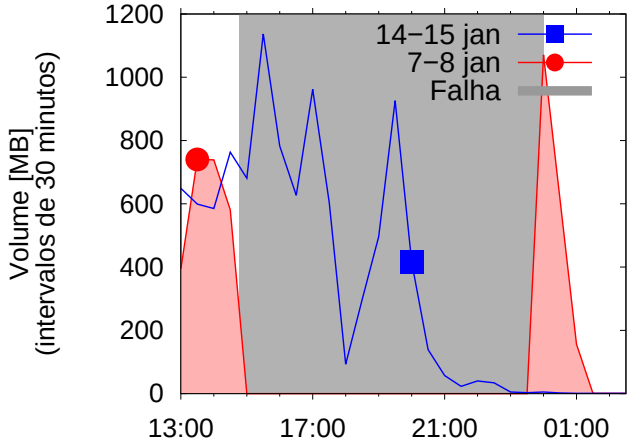
5.1.6 IMPACTO DAS FALHAS NO COMPORTAMENTO DE APLICAÇÕES

Falhas têm impacto imediato no comportamento do tráfego e impacto gradativo no comportamento do usuário. Nesta seção avaliamos o impacto de falhas no comportamento de aplicações assíncronas que executam constantemente em plano de fundo.

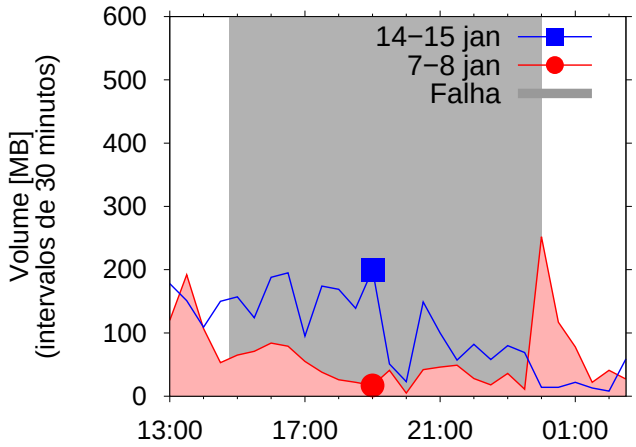
A figura 5.6 mostra o volume de tráfego, em intervalos de trinta minutos para conexões *Dropbox*[3] e SMTP (*Simple Mail Transport Protocol*), segundo classificação do TSTAT. Como anteriormente, as linhas azuis marcadas com um quadrado mostram o tráfego dos dias 14 e 15, sem falhas, e as linhas vermelhas marcadas com um círculo mostram o tráfego

Tipo de Tráfego	% das conexões		% do tráfego		Volume de tráfego (GB)		Volume por conexão (KB)	
	07/01/13	14/01/13	07/01/13	14/01/13	07/01/13	14/01/13	07/01/13	14/01/13
HTTP GET	63,86	44,93	41,03	53,51	317,08	592,85	34,98	48,68
HTTP POST	2,20	2,77527	0,44	1,12	3,41	12,46	10,97	16,57
Youtube	3,06	1,07	39,43	17,53	304,72	194,24	702,29	668,79
Propaganda	2,23	2,15	0,33	0,41	2,59	4,54	8,18	7,79
Social	0,057	0,50	0,03	0,08	0,25	0,89	31,03	6,52
Facebook	0,007	6,46	0	4,21	0	46,65	0,00	26,62
Hospedagem	0	0,01	0	2,76	0	30,62	0,00	0,00
P2P	0,47	1,25	3,34	1,72	25,81	19,06	662,19	119,57
Email	1,38	0,82	0,66	0,78	5,10	8,64	44,56	82,66
SSL/TLS	10,83	20,6	9,26	15,21	71,56	168,53	79,67	64,16
Demais	15,90	19,44	0,9	0,8	6,95	8,86	5,39	3,81

Tabela 5.1: Comparação do tráfego de aplicações entre 14:45 e 00:05 dos dias 7 e 8 de janeiro (período de falha) e o mesmo período nos dias 14 e 15 de janeiro (sem falha).



(a) Dropbox



(b) SMTP

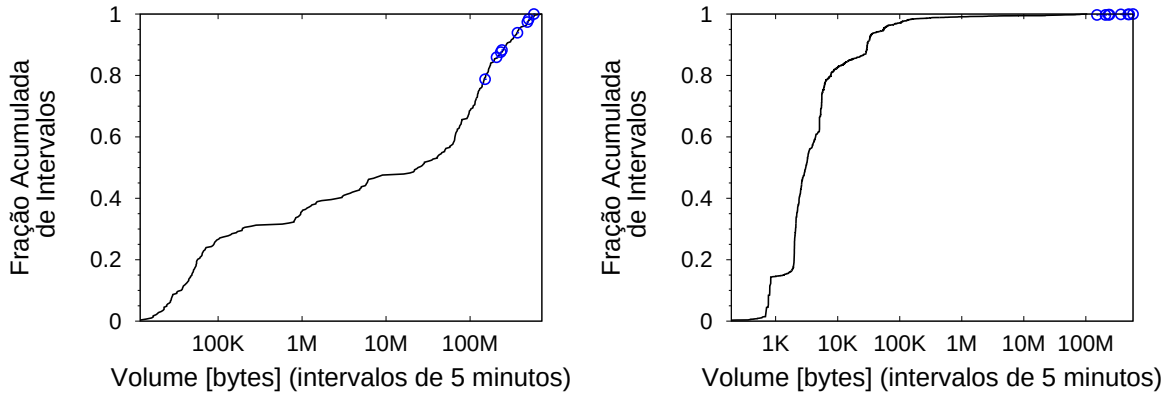
Figura 5.6: Impacto das falhas no volume de tráfego de aplicações assíncronas.

dos dias 7 e 8, com falha.

Como o *Dropbox* é hospedado em uma plataforma da *Amazon Web Services*, todo o tráfego é interrompido durante a falha. De forma similar, parte do tráfego SMTP é internacional e interrompido durante a falha. Quando a falha é restaurada às 00:05 do dia 8, as tarefas acumuladas pelas duas aplicações ao longo da falha (i.e., arquivos criados e modificados no *Dropbox* bem como e-mails enfileirados) são disparadas. Para ambas as aplicações, percebemos uma rajada de tráfego após a restauração da falha. A rajada aumenta o tráfego enviado pela aplicação e tem duração relativamente curta, entre 30 e 60 minutos.

A linha na figura 5.7(a) mostra a distribuição acumulada do volume de tráfego Dropbox durante o dia 17 de janeiro de 2013 (sem falha), em intervalos de cinco minutos. Nós

[3]Na figura 5.4 e na tabela 5.1 a maior parte do tráfego Dropbox está classificado como “SSL/TLS”.



(a) Tráfego no dia 17 de janeiro (b) Intervalos entre 19:55 e 20:35

Figura 5.7: Distribuição do volume de tráfego Dropbox em intervalos de 5 minutos em diferentes períodos. Pontos em destaque são o volume de tráfego Dropbox nos 40 minutos seguintes à falha do dia 10 de janeiro, em intervalos de 5 minutos.

também calculamos o tráfego Dropbox durante a rajada de tráfego após restauração de uma falha. Em particular, calculamos o tráfego em intervalos de cinco minutos durante os 40 minutos seguintes à restauração da falha do dia 10 de janeiro (i.e., oito intervalos de cinco minutos entre 19:55 e 20:35). Nós marcamos o tráfego relativo aos intervalos com rajada de tráfego com círculos azuis sobre a distribuição de tráfego Dropbox do dia 17 de janeiro. Focamos na falha do dia 10 de janeiro pois foi a falha restaurada mais cedo (às 19:55), de forma que uma comparação com o tráfego *Dropbox* em dias normais fosse mais realista. Os resultados mostram que os intervalos seguintes à falha têm volume de tráfego Dropbox maior que a maioria dos intervalos ao longo do dia, e comparável ao tráfego *Dropbox* em horários de pico.

A figura 5.7(b) é similar, mas a linha mostra a distribuição acumulado do volume de tráfego *Dropbox* apenas nos intervalos de 5 minutos entre 19:55 e 20:35 dos dias 14, 15, 16, 17 e 18 de janeiro (sem falhas). A figura 5.7(b) mostra que a rajada de tráfego *Dropbox* após restauração de uma falha é significativamente maior que o tráfego típico do horário, até sete vezes maior no período de 40 minutos analisado.

Atualmente, aplicações de armazenamento de arquivos em nuvem (*cloud storage*) são responsáveis por uma fração não desprezível do tráfego do campus. Apenas o Dropbox, uma das aplicações mais populares para tal fim, consome na média 4% da banda da universidade. Rajadas de tráfego combinadas a um possível aumento do volume de tráfego destas aplicações podem comprometer o desempenho da rede em períodos pós-falha e degradar o desempenho de aplicações interativas como teleconferências.

5.2 FALHAS DE DESEMPENHO

Nesta seção mostramos nossas análises sobre falhas com características distintas das mostradas na seção anterior. Enquanto as falhas da seção anterior são caracterizadas por perda total de acesso do *backbone* RNP aos *links* internacionais, as falhas de desempenho representam falhas em enlaces internos do *backbone*. Ou seja, as falhas de desempenho afetam a troca de dados (tráfego) apenas na rede da RNP, sem interromper o tráfego geral como um todo. Consideramos portanto, para esta seção, as falhas ocasionadas por quedas de *links* entre Pontos de Presença (PoPs) no *backbone* da RNP, reportados pela instituição em seu site como causadores de lentidão no acesso. Para nossos estudos, observamos detalhadamente quatro períodos apresentando falhas com estas características ocorridos entre os meses de julho e novembro de 2013. Nossa análise se concentra em observar como as características do tráfego e o comportamento dos usuários se alteram nestas condições.

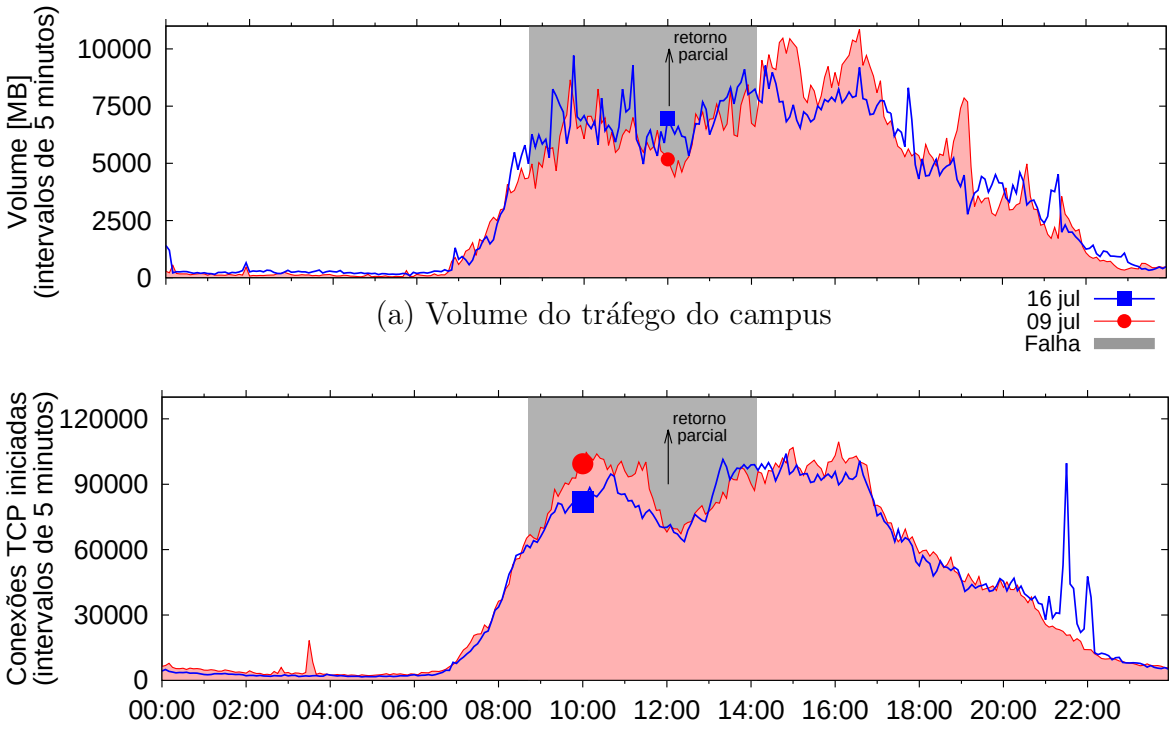
5.2.1 IMPACTO DAS FALHAS NO TRÁFEGO AGREGADO

A figura 5.8 apresenta uma visão geral do tráfego na rede da UFJF durante dois dias distintos sendo um deles com a ocorrência de falha e o outro, correspondente à semana posterior, sem a ocorrência de falhas reportadas. A figura 5.8(a) mostra o volume total de tráfego, agregado em intervalos de cinco minutos. A figura 5.8(b) mostra o número de conexões TCP iniciadas em intervalos de cinco minutos. As linhas azuis, marcadas com um quadrado, mostram o tráfego total e o número de conexões iniciadas no dia 16 de julho de 2013, quando nenhuma falha foi reportada pela RNP. As linhas vermelhas, marcadas com um círculo, mostram o tráfego e o número de conexões iniciadas no dia 09 de julho de 2013, quando a RNP reportou lentidão no acesso à rede acadêmica brasileira devido a quedas ocasionadas por rompimentos de fibras[4].

Ambos os períodos representados no gráfico correspondem a terças-feiras. As falhas ocorreram de 08:48 às 12:02 do dia 9 de julho para o link que conecta o POP-SP com o POP-MG e no mesmo dia das 08:42 às 14:08 no link entre os POPs SP e SC (horário de Brasília); nós sombreamos estes períodos na figura 5.8. Note-se que ambas as datas representam dias letivos normais no calendário acadêmico da universidade.

Note que em geral há pequena redução no volume de tráfego durante todo o período

[4]rompimentos praticamente simultâneos identificados na rede da operadora Oi, entre os estados de São Paulo e Santa Catarina e entre Minas Gerais e São Paulo.



(a) Volume do tráfego do campus

(b) Número de conexões TCP no campus

Figura 5.8: Visão geral do tráfego de dados na rede da UFJF - 09 e 16 de julho.

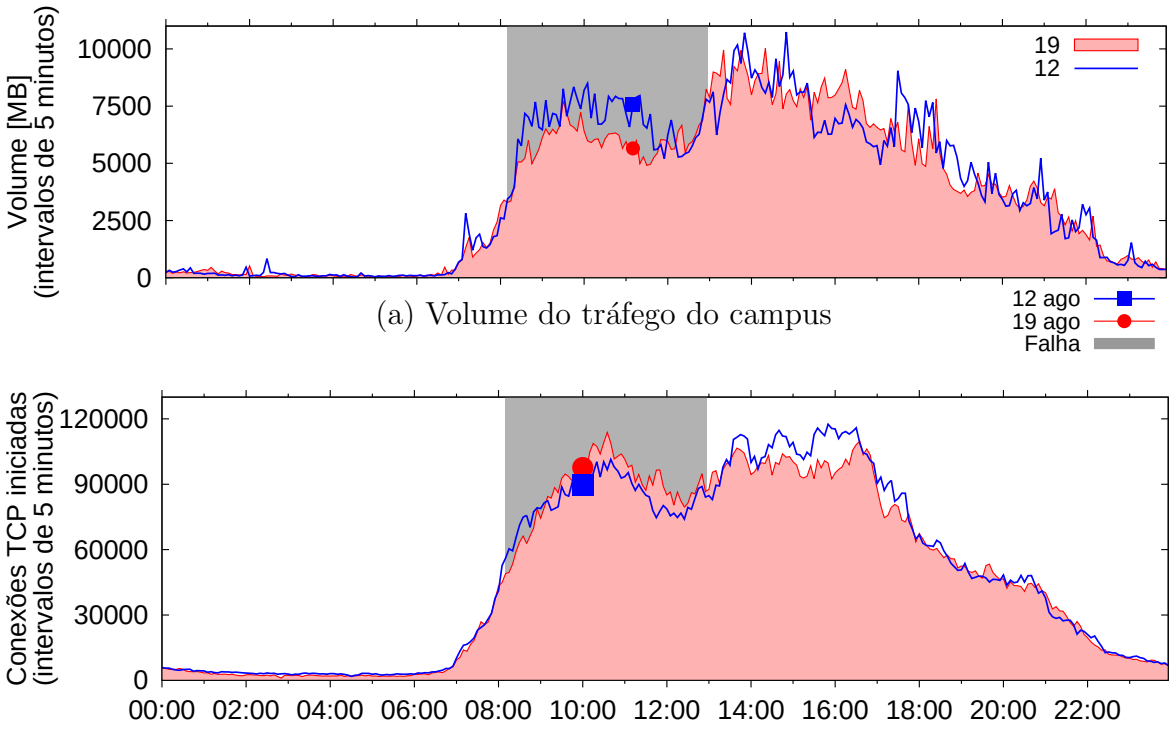
de interrupção e, em contrapartida, um aumento no número de conexões TCP iniciadas (principalmente antes do retorno parcial identificado na figura).

De forma semelhante, a falha ocorrida no dia 12 de agosto também não apresenta impactos significativos. A figura 5.9 apresenta a visão geral do tráfego na rede da UFJF durante os dias 19 de agosto (quando ocorreram falhas de desempenho) e 12 de agosto (sem falhas reportadas). A figura 5.9(a) mostra o volume de tráfego total, agregado em intervalos de cinco minutos. A figura 5.9(b) mostra o número de conexões TCP iniciadas em intervalos de cinco minutos. A falha do dia 19 foi reportada pela RNP como resultado de um novo rompimento de fibras[5].

O problema de rompimento persistiu entre 08:10 e 12:57 do dia 19 de agosto; nós sombreamos este período na figura 5.9. Ambos os períodos representados no gráfico correspondem a segundas-feiras, dias letivos normais no calendário acadêmico.

O comportamento observado nas figuras 5.8 e 5.9 é bastante similar, demonstrando pequenas variações, de diminuição em relação ao volume trafegado e aumento em relação ao número de conexões iniciadas. Consideramos que a pequena diferença entre volume trafegado pode ser explicada pelo fato dos links interrompidos não causarem grande im-

[5]na operadora Oi, entre os estados de São Paulo e Rio de Janeiro.



(a) Volume do tráfego do campus

(b) Número de conexões TCP no campus

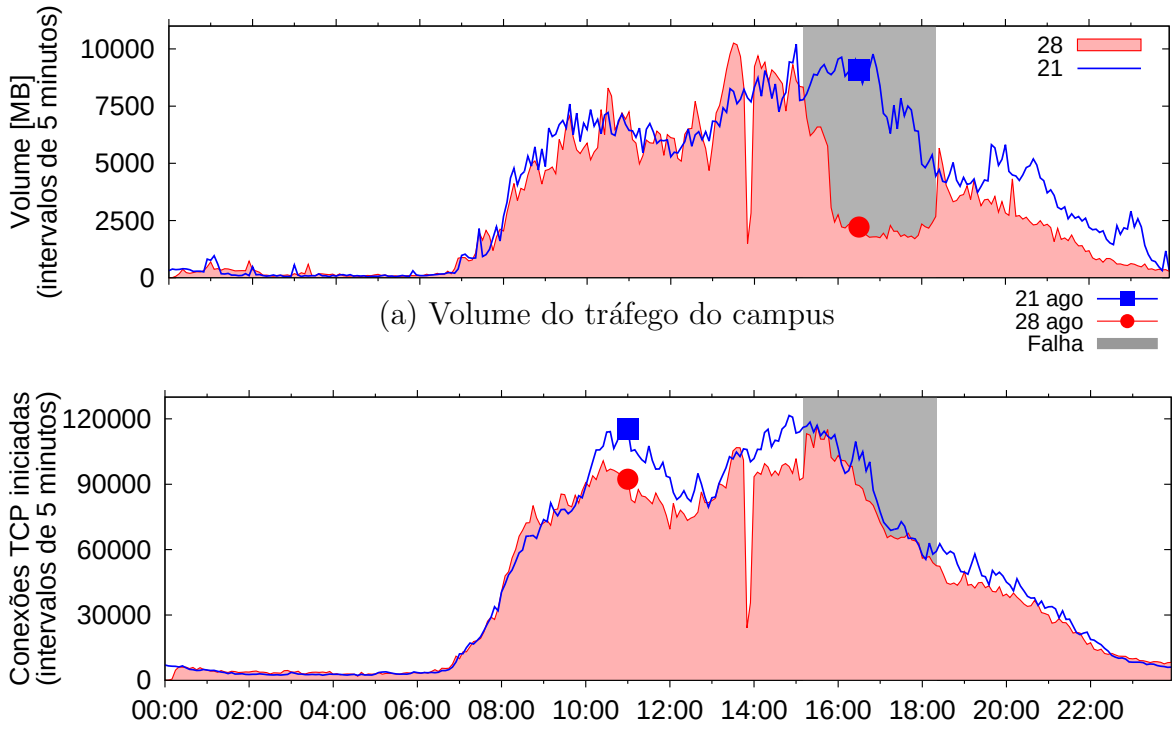
Figura 5.9: Visão geral do tráfego de dados na rede da UFJF - 19 e 12 de agosto.

pacto por existirem rotas alternativas, com largura de banda adequada, para o tráfego dos dados. Acreditamos ainda que o aumento de conexões TCP iniciadas durante as falhas tenha sido causado pela interação de usuários, abrindo novas sessões concorrentes, ao perceber alguma demora no recebimento das informações solicitadas na rede.

De forma geral, as falhas de desempenho reportadas acima não causaram grande impacto no tráfego do campus.

O tráfego, nestes dias, apresenta padrões similares aos de dias normais, como apresentado na seção anterior (sec. 5.1). Com crescimento acentuado a partir das 8 horas da manhã, redução e posterior recuperação no período de almoço (aproximadamente entre 11 e 13 horas) e redução paulatina a partir das 17 horas até aproximadamente às 22 horas, quando se mantêm em patamares baixos durante o resto da noite e madrugada do dia seguinte. Conforme também observamos na seção anterior o comportamento do número de conexões TCP iniciadas é qualitativamente similar.

A figura 5.10 apresenta uma visão geral do tráfego na rede da UFJF durante os dias 28 de agosto (quando ocorreram falhas) e 21 de agosto (sem falhas reportadas). A figura 5.10(a) mostra o tráfego total, agregado em intervalos de cinco minutos. A figura 5.10(b) mostra o número de conexões TCP iniciadas em intervalos de cinco minutos.



(a) Volume do tráfego do campus

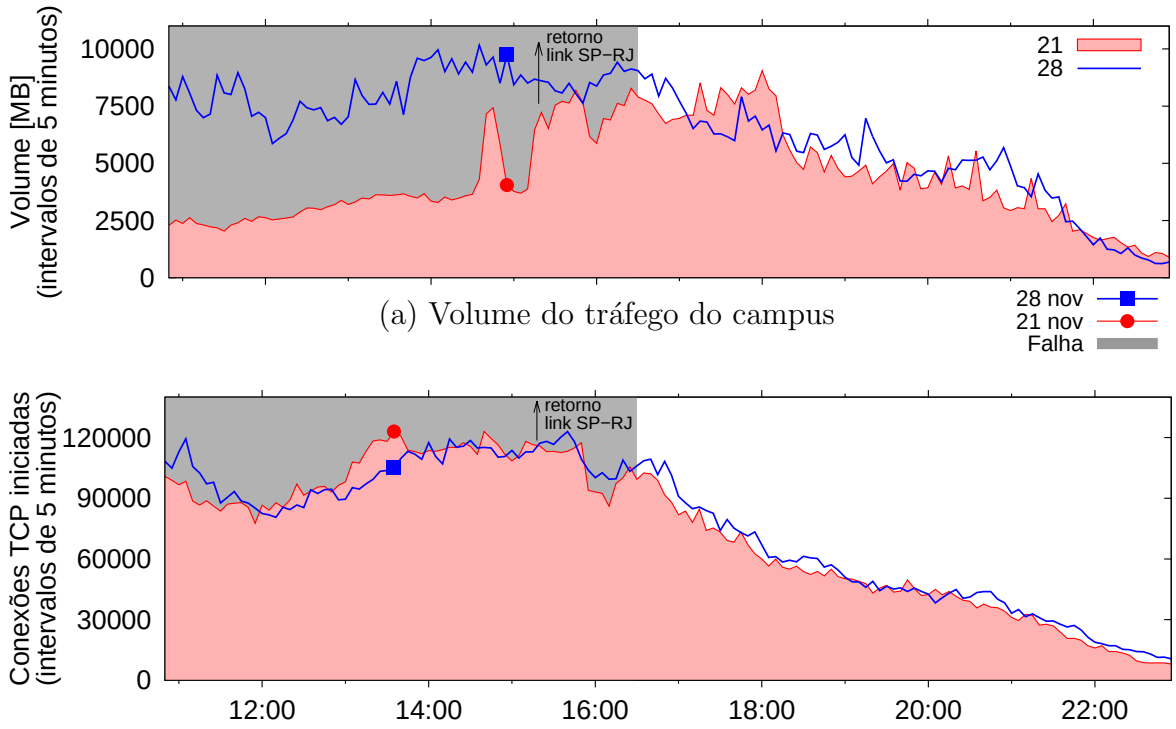
(b) Número de conexões TCP no campus

Figura 5.10: Visão geral do tráfego de dados na rede da UFJF - 28 e 21 de agosto.

Nesta ocasião, as falhas ocorreram no dia 28 de agosto de 2013, quando foi reportada pela RNP lentidão na rede acadêmica devido a diversas quedas identificadas na rede de uma operadora, entre os estados de Minas Gerais e Ceará, Maranhão e Pará, Bahia e Espírito Santo, São Paulo e Minas Gerais, Paraná e São Paulo e Rio Grande do Sul e Santa Catarina, causando congestionamento de outros circuitos de backbone. Os períodos representados no gráfico correspondem a quartas-feiras, dias letivos normais no calendário acadêmico.

Os maiores impactos da queda são facilmente identificados, na figura 5.10 aproximadamente entre as 15:10 e 18:20 do dia 28 de agosto. Essa falha, entre todas as falhas de desempenho estudadas, foi a que apresentou maior disparidade entre os níveis de volume de tráfego. Uma possível explicação para este comportamento é a grande quantidade de ligações entre POPs afetadas pelas falhas. É interessante observar que, apesar de todo o impacto no volume trafegado, praticamente não se nota disparidade em relação ao número de conexões TCP iniciadas no período no dia com falha e no dia sem a presença de falhas.

A figura 5.11 apresenta uma visão do tráfego na rede da UFJF durante os dias 21 de novembro (quando ocorreram falhas) e 28 de novembro (sem falhas reportadas). Nessa figura apresentamos o tráfego agregado e o número de conexões TCP iniciadas. Nesse dia,



(a) Volume do tráfego do campus

(b) Número de conexões TCP no campus

Figura 5.11: Visão geral do tráfego de dados na rede da UFJF - 21 e 28 de novembro.

a RNP reportou lentidão na rede acadêmica devido a falhas nos circuitos entre os estados de São Paulo e Rio de Janeiro e São Paulo e Minas Gerais. Os períodos representados no gráfico correspondem a quintas-feiras, dias letivos normais no calendário acadêmico. As quebras de link ocorreram próximo às 9 horas da manhã (não mostrado na figura)[6] e foram recuperadas às 15:18 para o link SP-RJ e 16:30 para o link SP-MG.

O número de conexões TCP iniciadas é qualitativamente similar assim como o comportamento relacionado ao volume trafegado conforme vemos nas figuras 5.8 a 5.11 (b). Entretanto o comportamento quantitativo do volume de tráfego apresenta diferenças consideráveis como observado na figura 5.11(a). Curiosamente, observamos ainda que a diferença quantitativa em relação ao número de conexões é muito pequena.

Ao observar os gráficos 5.8 a 5.11, vemos que em todos os períodos analisados nesta seção ocorrem diminuições, mais ou menos significativas, do volume de tráfego trocado externamente pela UFJF nos dias com falhas, destacando-se os dias 28 de agosto (figura 5.10(a)) e 21 de novembro, (figura 5.11(a)), onde as diferenças são mais claras.

Acreditamos que a considerável diferença de volume apresentada nos períodos de falhas, mostrada nas figuras 5.10(a) e 5.11(a), pode ser explicada pela grande quantidade

[6]Durante a falha deste dia específico, a coleta foi iniciada somente às 10:45 devido a problemas com o servidor, motivo pelo qual o gráfico apresentado tem início aproximadamente neste mesmo horário.

de links afetados, como ocorreu no dia 28 de agosto e pela importância da localização dos links afetados para a rede estudada, no caso da falha de 21 de novembro.

Entendemos que a falha de um link diretamente na rota do tráfego, conforme ocorreu nas falhas de 9 de julho e 16 de agosto, traz um impacto pouco relevante pela possibilidade de adaptação do roteamento utilizando rotas alternativas. Já no caso das duas falhas de desempenho posteriores (28/08 e 21/11), a adaptabilidade se vê comprometida. Levamos em consideração que possíveis caminhos alternativos também se encontram comprometidos, impactando fortemente o tráfego dos dados e consequentemente o volume relacionado ao mesmo. Entretanto, o número de conexões TCP iniciadas nos períodos com falhas geralmente sofre poucas alterações em relação aos dias de tráfego normal e em alguns períodos chega a ser superior ao número de conexões iniciadas em períodos sem falhas como podemos observar nas figuras 5.8(b) e 5.9(b).

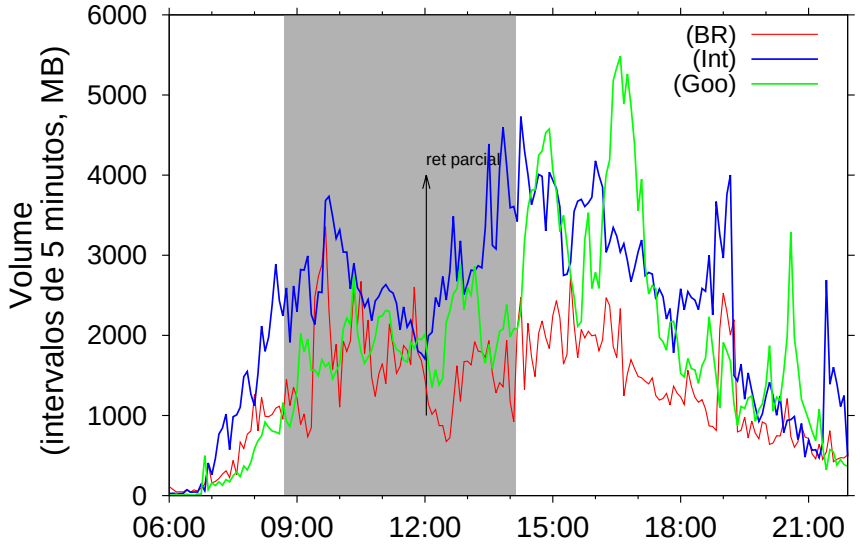
Esta particularidade observada neste tipo de falha pode ser explicada por uma maior interação dos usuários, tentando abrir novas sessões para um mesmo conteúdo devido à lentidão presente na rede nos momentos de falha. Este tipo de comportamento do usuário pode sobrecarregar ainda mais a infraestrutura de redes de computadores, potencializando o efeito da falha em si.

5.2.2 IMPACTO DAS FALHAS DE DESEMPENHO POR GEOLOCALIZAÇÃO DOS DESTINOS

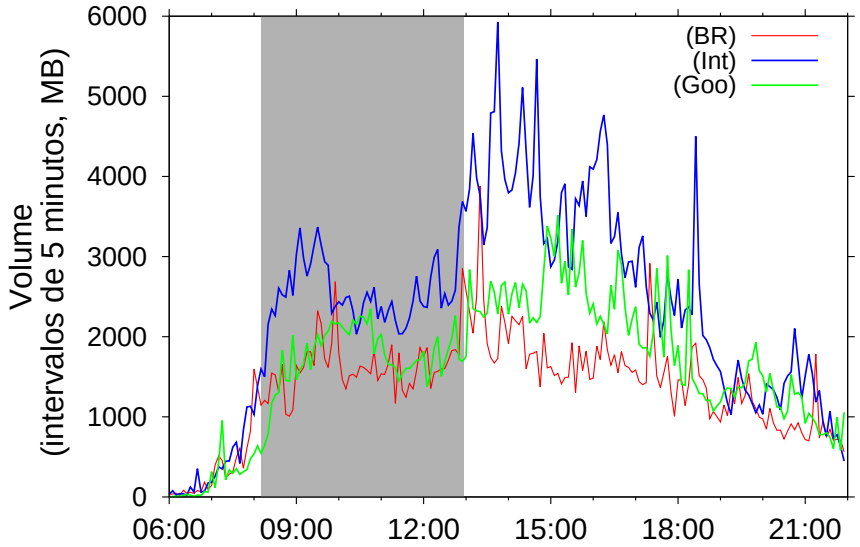
As figuras 5.12(a) e 5.12(b) mostram a variação do tráfego trocado com sites nacionais, internacionais e serviços do Google em dias onde ocorreram falhas de desempenho.

De forma distinta do que ocorreu com as falhas parciais mostradas na seção 5.1, desta vez não observamos perda total de acesso a nenhum dos três tipos de destino estudados. Verificamos ainda que geralmente as quedas nos volumes que ocorrem nos períodos de falha aparentam ser proporcionais entre os três tipos de geolocalização estudados. O volume é mostrado em intervalos sumarizados de cinco minutos e os períodos onde ocorreram falhas estão sombreados.

Concluímos portanto que a geolocalização dos destinos não exerce grande influência no impacto nas falhas de desempenho estudadas, afetando proporcionalmente os três tipos de destino analisados.



(a) 09/07



(b) 19/08

Figura 5.12: Detalhe dos impactos de falhas de performance por geolocalização

5.2.3 IMPACTO DAS FALHAS EM CARACTERÍSTICAS E DESEMPENHO DE CONEXÕES

Para identificar possíveis diferenças em características do tráfego e desempenho realizamos a comparação entre os períodos com falha e os períodos normais para algumas métricas de desempenho. A figura 5.13 mostra a distribuição acumulada da duração, latência fim-a-fim e taxa de transmissão das conexões durante períodos de igual duração com falhas (linha com quadrado) e sem falhas (linha com círculo).

Observamos na figura 5.13 que nas falhas de desempenho do dia 09 de julho a maior alteração ocorre em relação à latência fim-a-fim entre as conexões, onde nos períodos com falhas ocorre aumento considerável da latência (5.13(b)). Percebemos também, uma

discreta alteração na fração das conexões com duração menor que 10 segundos, conforme vemos na figura 5.13(a), em dias com falhas temos uma fração de conexões com duração de até 9 segundos pouco menor que nos dias normais. A figura 5.13(c) mostra que a alteração em relação à taxa de transmissão dos dados é insignificante.

Para o período de ocorrência de falha do dia 19 de agosto (não mostrado), a distribuição é perfeitamente similar à do dia 09 descrita acima, não demandando maior detalhamento.

Para as falhas do dia 28 de agosto (figura 5.14) e do dia 21 de novembro (não mostrado) verificamos a ampliação dos impactos das falhas nas métricas estudadas. Acompanhando o aumento queda de volume trafegado mostrada na seção 5.2.1, nessas falhas a latência aumenta consideravelmente mais que nas duas falhas anteriores evidenciando a dificuldade de se encontrar caminhos para os destinos com o mesmo desempenho das rotas principais.

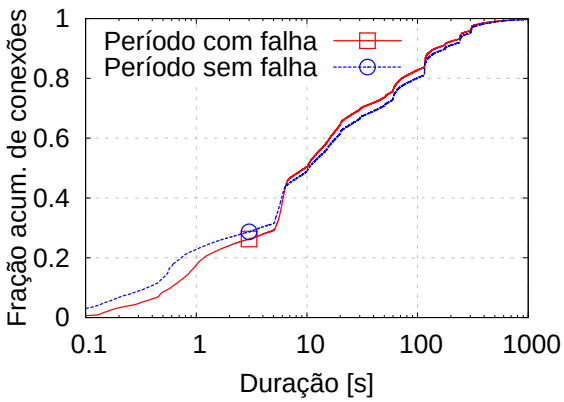
Ocorre também uma diferença (diminuição) mais acentuada na fração de conexões com duração de até 9 segundos, como exemplo, vemos na figura 5.14(a), que as conexões com duração de até 3 segundos representam cerca de 10% das conexões em dias com falhas e cerca de 27% em dias sem falhas. Esta diferença evidencia maior demora no estabelecimento e encerramento de conexões.

Observamos também que, nas falhas de 28/08 e 21/11, é visível e significativa a alteração na distribuição das taxas de transmissão das conexões, ocorrendo aumento considerável na fração de conexões com taxa de transmissão na faixa de até 1 Kbps nos dias de falha. Conforme vemos na figura 5.14(c) o percentual de conexões com taxa de até 1 Kbps é de cerca de 80% nos dias com falha e de 60% nos dias normais evidenciando maiores taxas de transmissão em dias sem falhas.

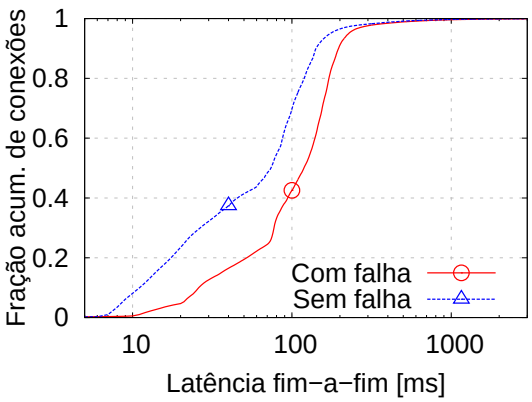
5.2.4 IMPACTO DAS FALHAS DE DESEMPENHO NO COMPORTAMENTO DOS USUÁRIOS

Nesta seção avaliamos o impacto das falhas de desempenho no comportamento dos usuários. Para isto analisamos o comportamento do tráfego em relação aos conjuntos de protocolos e aplicações mais utilizados.

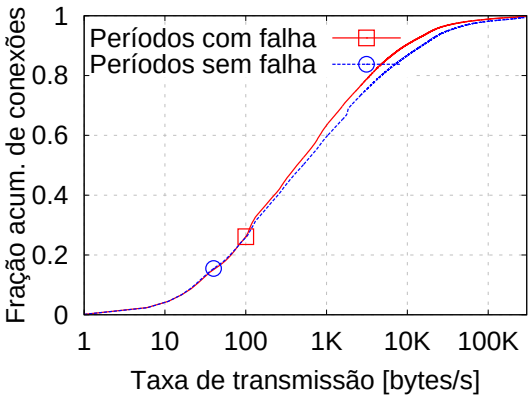
As figuras 5.15 e 5.16 mostram o impacto das falhas de desempenho respectivamente no volume e no número de conexões TCP iniciadas por tipo de protocolo utilizado. Mostramos nas figuras os protocolos HTTP, notadamente de maior volume e número de conexões entre os protocolos avaliados; protocolos SSL e TLS (relacionados a tráfego através de conexões criptografadas) e tráfego utilizando protocolos relacionados a troca de e-mails,



(a) Duração



(b) Latência fim-a-fim



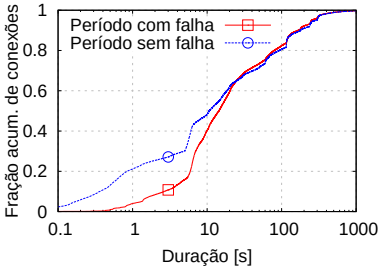
(c) Taxa de transmissão

Figura 5.13: Comparação do desempenho das conexões TCP durante a falha do dia 9 de julho com o mesmo período do dia 16 de julho (sem falha).

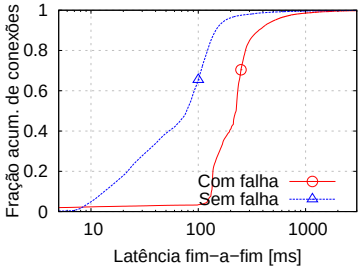
como SMTP, POP e IMAP. Comparamos os tráfegos de dias com falhas e sem falhas para fins de observação de parâmetros normais de tráfego e de períodos com falhas, apresentando portanto dois gráficos, sendo um do dia com falha e o outro com o dia de semana imediatamente anterior.

Podemos observar que as falhas não afetam substancialmente os padrões de tráfego em relação aos protocolos utilizados. Na figura 5.15 verificamos que a variação de volume de dados por tipo de aplicação não apresenta, ao longo do período de falha, diferenças consideráveis do padrão para dias normais no mesmo período. Os outros dias com falhas de desempenho estudados não foram mostrados por evidenciar praticamente o mesmo padrão de utilização dos protocolos avaliados, ou seja, mesmo ocorrendo diferença nos volumes, os mesmos caem proporcionalmente para cada protocolo analisado.

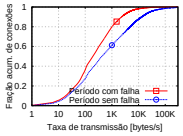
Na figura 5.16 observamos que a quantidade de conexões iniciadas nos dias de falha também não difere em grande escala da quantidade observada para um dia sem falhas (figura 5.16(b)). Comportamento similar foi observado nas outras falhas de desempenho



(a) Duração



(b) Latência fim-a-fim



(c) Taxa de transmissão

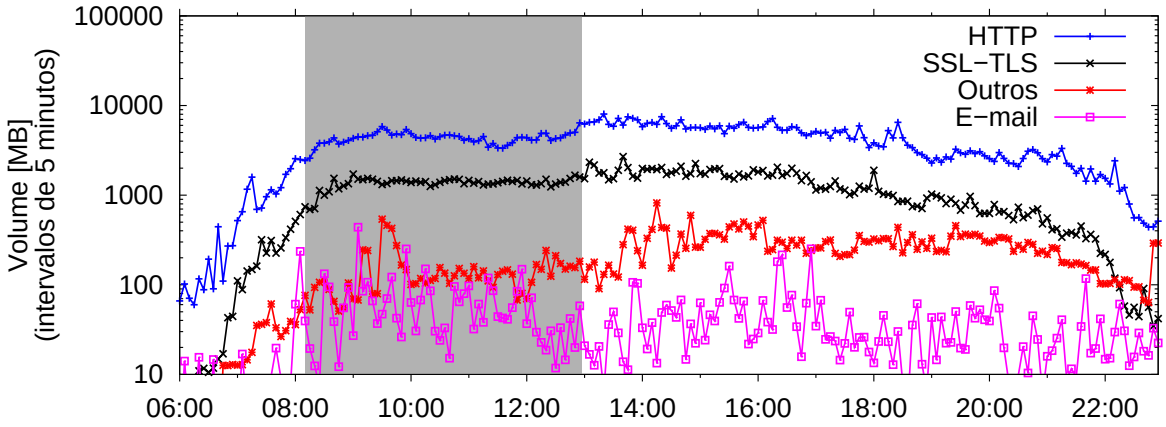
Figura 5.14: Comparação do desempenho das conexões TCP durante a falha do dia 28 de agosto com o mesmo período do dia 21 de agosto (sem falha).

estudadas (não mostrado), onde a ausência de mudança no comportamento entre os protocolos reflete a pouca modificação observada para a quantidade de fluxos TCP durante um dia com falhas de desempenho.

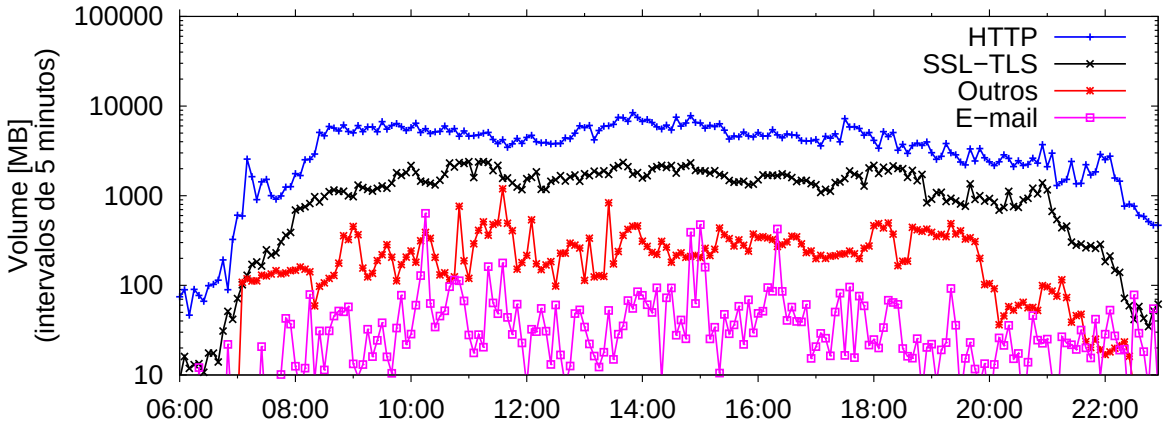
Procuramos observar também o comportamento da mistura de aplicações utilizada nos momentos de falhas de desempenho, através da análise do volume de dados e do número de conexões relacionados a alguns tipos de aplicações que rodam na rede utilizando o protocolo HTTP segundo classificação realizada pela ferramenta Tstat.

Observamos nas figuras 5.17 e 5.18, respectivamente, o volume trafegado e a quantidade de conexões iniciadas associadas a alguns tipos específicos de aplicações HTTP. Analisamos conexões relacionadas a aplicações POST e GET do HTTP sem destino classificado, tráfego relacionado ao *YouTube*, tráfego relacionado a anúncios (por exemplo, propagandas e *banners* de *sites*) e relacionado a aplicações de redes sociais bastante utilizadas no Brasil, como *Facebook* e *Twitter*. Nas figuras citadas, comparamos novamente o tráfego de dias com e sem falhas, apresentando para cada figura dois gráficos para a falha reportada, sendo um do dia com falha e o outro com o dia de semana imediatamente anterior correspondente (sem falha).

Conforme observamos em relação aos protocolos no começo desta seção, o volume trafegado e o número de conexões não parecem sofrer impacto diretamente relacionado às falhas. Detectamos nos dias de falha apenas variações proporcionais na participação de cada tipo de aplicação nos conjuntos de tráfego estudados. Apesar de mostrarmos somente as figuras referentes aos dias 19 de agosto (com falha) e 12 de agosto (sem falha)



(a) 19/08



(b) 12/08

Figura 5.15: Impacto das falhas de 19/08 no volume de tráfego por tipo de aplicação.

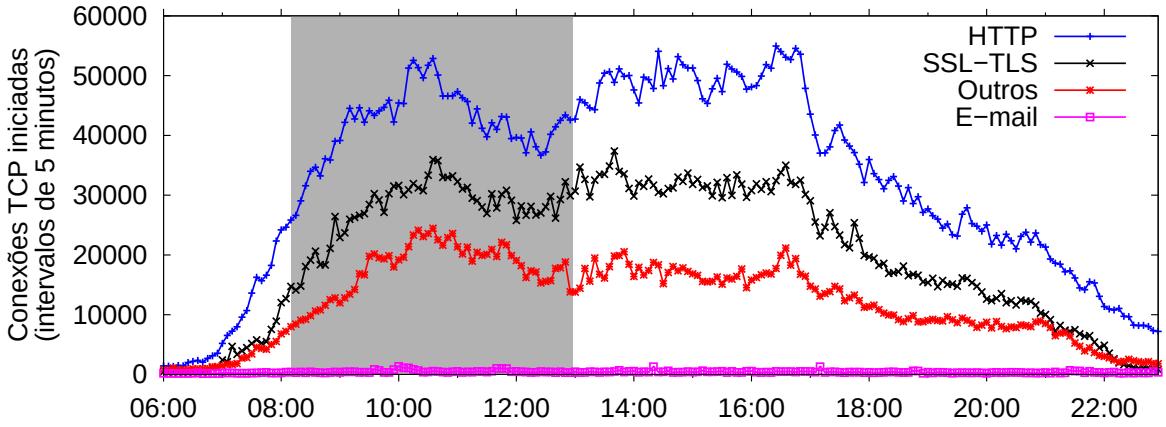
verificamos nos outros dias de falha de desempenho estudados comportamento similar.

As análises realizadas e descritas acima nos levam a crer que as falhas de desempenho pesquisadas neste estudo não provocaram alterações significativas no comportamento dos usuários, em relação aos protocolos de rede e aplicações acessadas, distintamente do que observamos para falhas parciais na seção 5.1.4.

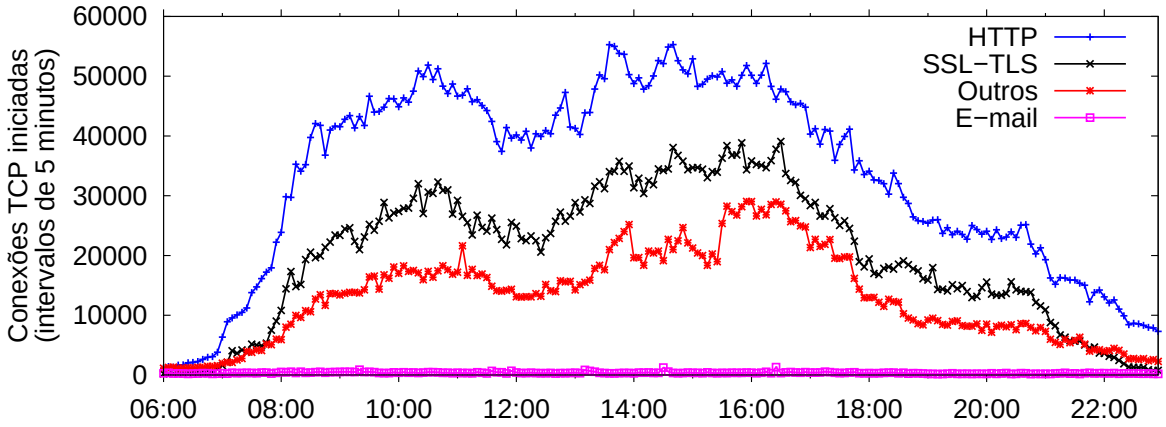
5.2.5 COMPORTAMENTO DO TRÁFEGO HTTP POR ROTAS UTILIZADAS

Nesta seção detalhamos o comportamento do tráfego HTTP durante falhas de desempenho. Nós escolhemos detalhar o tráfego HTTP por este possuir maior volume de tráfego e número de conexões, em relação às rotas seguidas pelos dados principalmente através de Pontos de Presença da RNP no Brasil.

Com a intenção de detectar indícios de melhora ou piora nos indicadores de desem-



(a) 19/08



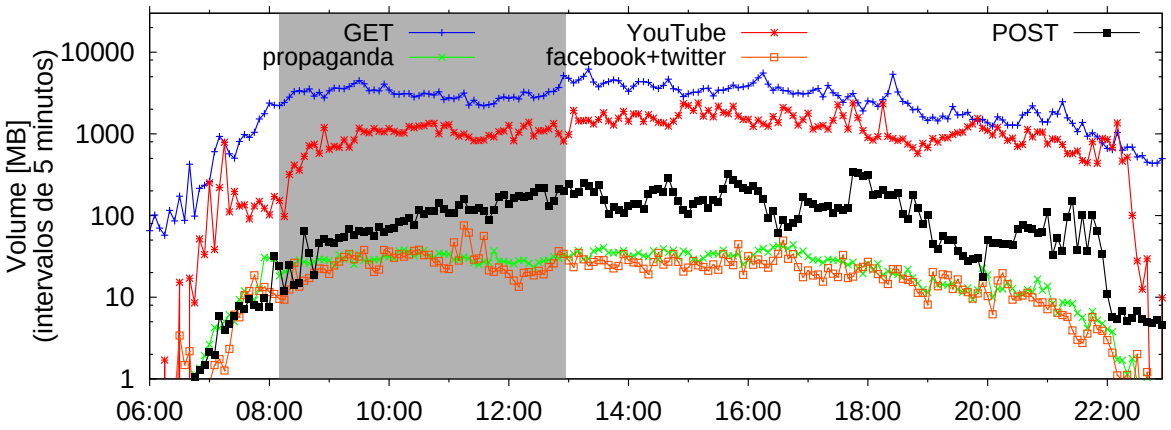
(b) 12/08

Figura 5.16: Impacto das falhas de 19/08 no número de conexões por tipo de aplicação.

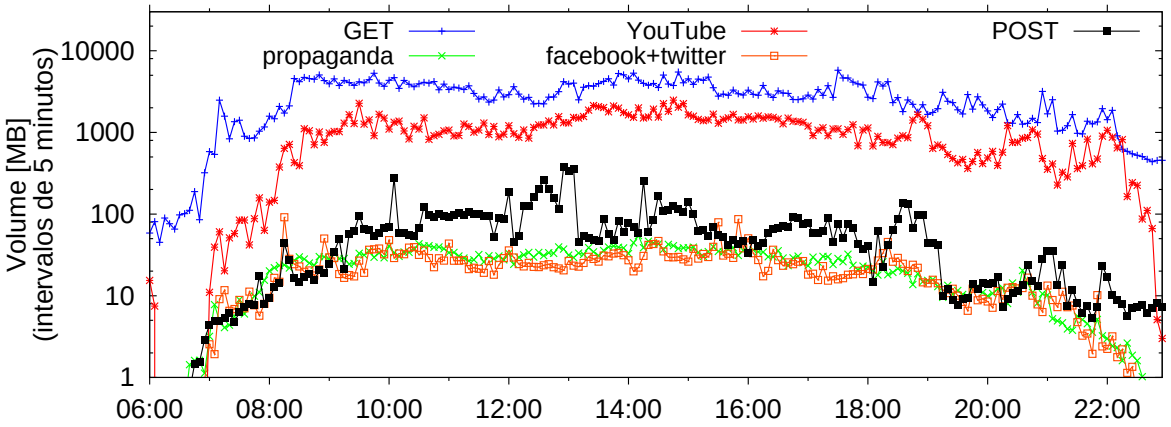
penho de caminhos específicos seguidos pelo tráfego, mostramos nas tabelas 5.2 a 5.5 métricas do tráfego partindo ou chegando de instituições ligadas diretamente a Pontos de Presença da RNP em vários estados do país. Para fins de comparação mostramos também o tráfego trocado entre a UFJF e o site internacional da *Amazon* e entre a universidade e uma empresa brasileira de conteúdo e serviços internet alocada na Internet comercial brasileira (UOL).

As tabelas mostram dados de períodos de falha e do mesmo período sem falha exatamente uma semana antes ou após as falhas. Os dados observados são o número absoluto de conexões entre a UFJF e sites diretamente ligados aos POPs do backbone da RNP, o volume trafegado nestas conexões, o percentual de volume de dados retransmitidos nas conexões e o RTT médio destas conexões.

Na tabela 5.2 analisamos o período de falha do dia 09 de julho, onde conforme citado anteriormente a RNP apontou falhas nos circuitos entre os POPs MG-SP e SP-SC e



(a) 19/08

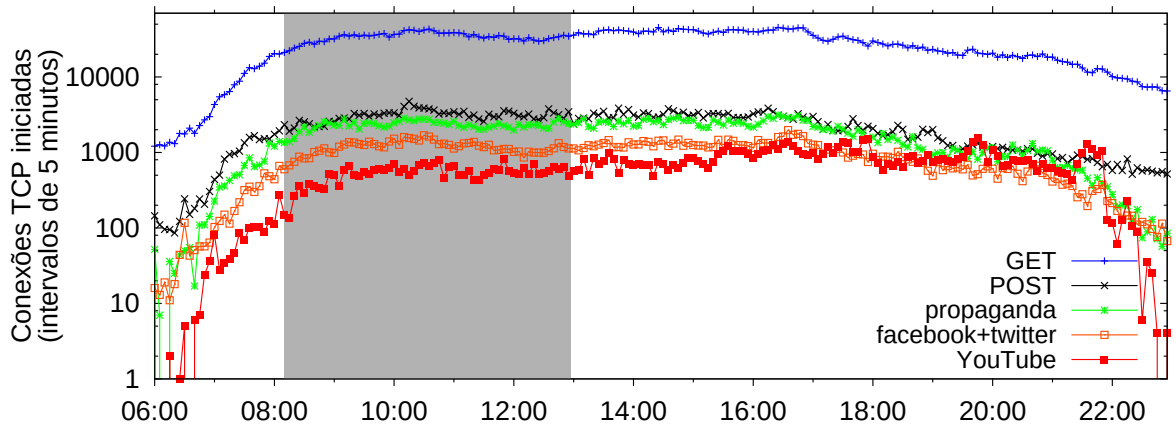


(b) 12/08

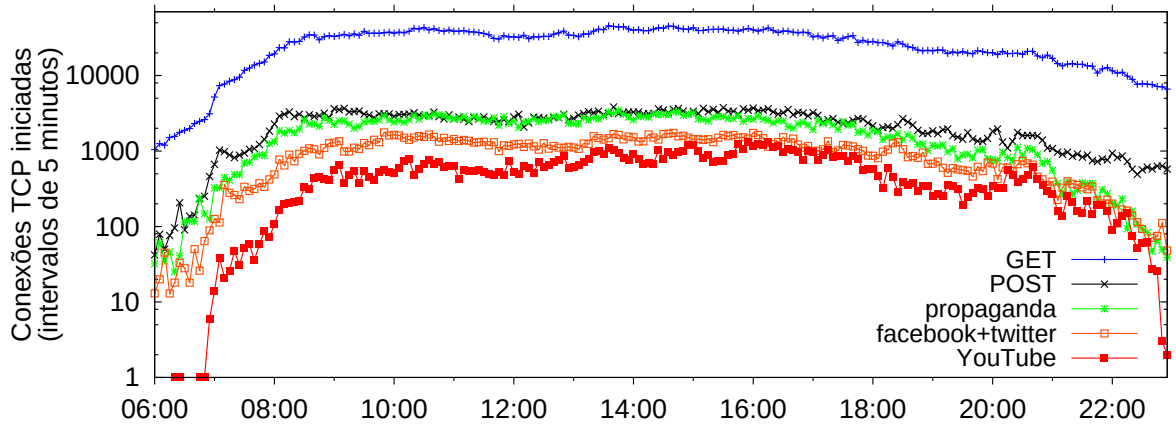
Figura 5.17: Impacto das falhas de 19/08 no volume de tráfego por tipo de aplicação HTTP.

mostramos ainda as mesmas métricas para o dia 16 de julho (sem falhas reportadas), no mesmo período. Conforme esperado para o período com falhas vemos um aumento no RTT da maioria das conexões, no entanto as conexões com sites ligados ao POP-DF, POP-PR e alguns POPs do Nordeste (PB, RN e SE) apresentaram RTT reduzido neste período. Explicações plausíveis para esta alteração seriam a troca da rota principal com o POP-MG ter sido transferida de SP para o DF durante a queda impactando numa melhora de desempenho e na ligação direta também com os POPs CE e BA presentes no caminho entre a UFJF e os POPs do nordeste com melhora citados. O percentual de retransmissão de forma geral também apresentou piora (aumento do percentual) nos momentos de falha, porém, novamente em alguns casos específicos, ocorreu diminuição no percentual de retransmissão mesmo com as falhas.

Na tabela 5.3 observamos o período de falha do dia 19 de agosto, onde a RNP reportou



(a) 19/08



(b) 12/08

Figura 5.18: Impacto das falhas de 19/08 no número de conexões por tipo de aplicação HTTP.

falhas nos circuitos entre os POPs SP-RJ e mostramos com fins comparativos as mesmas métricas para o dia 12 de agosto (sem falhas), no mesmo período do dia. Novamente vemos um aumento no RTT da maioria das conexões e algumas exceções, dentre elas, novamente as para o DF e PR, os mesmos POPs do Nordeste que melhoram o desempenho na falha de 09 de julho. Desta vez detectamos melhora também para o acesso ao PoP-RJ.

O impacto no link para o Rio de Janeiro pode ter sido causado pelo redirecionamento de rota, deixando de ser feita a transmissão do tráfego direcionado ao estado através de São Paulo, passando por outra rota. Curiosamente, o percentual de retransmissão de tráfego apresentou um aumento para metade e diminuição para a outra metade de destinos estudados.

Na tabela 5.4 apresentamos os dados relativos ao período de falha do dia 28 de agosto. Nesse dia, a RNP reportou falhas em vários circuitos, entre eles os que ligam os POPs

MG-CE, MA-PA, BA-ES, SP-MG, PR-SP, RS-SC. Na mesma tabela mostramos ainda as mesmas métricas para o dia 21 de agosto (sem falhas reportadas), no mesmo período do dia. Durante esta falha o aumento no RTT ocorreu para praticamente todos os destinos, com exceção para alguns sites do norte e nordeste, mais especificamente, os links de PE e SE, que apresentaram diminuição considerável do RTT durante as falhas, indicando uma possível melhora de eficiência, com a alteração das rotas. Neste caso acreditamos que as rotas podem ter sido alternadas para links que apesar de possuir menor capacidade, apresentaram um RTT mais favorável. O percentual de retransmissão foi afetado negativamente pelas falhas, mostrando desta vez poucas exceções a este comportamento.

Na tabela 5.5 temos um período de falha no dia 21 de novembro, onde a RNP reportou falhas nos circuitos entre os POPs RJ-SP e MG-SP. Na mesma tabela mostramos ainda as mesmas métricas para 28 de novembro (sem falhas reportadas), no mesmo período do dia. Durante esta falha observamos a diminuição do RTT médio para todos os estados das regiões norte e nordeste estudados, e aumento para os demais destinos, com destaque para os estados da região sul do Brasil e para o estado de São Paulo, cujas médias de RTT aumentaram pelo menos para o dobro de seu valor padrão, chegando a ser mais de cinco vezes maiores para SP e PR. Já os RTTs médios referentes aos estados de MG e DF foram pouco afetados pela falha.

Consideramos interessante observar que, contrariando as expectativas, em muitos casos temos melhoria das médias de RTT para alguns destinos durante períodos de falha. Esta constatação nos leva a pensar se a alteração na configuração de algumas rotas, poderia trazer um ganhos em termos de desempenho para o backbone da RNP.

Nas tabelas mostradas observamos que as conexões para a *Amazon*, localizada fora do país e para a UOL, ligada a Internet comercial do Brasil sofreram pioras consideráveis (aumento) em seus RTTs médios durante todos os períodos de falhas.

Rota do Tráfego	conexões		volume de tráfego (MB)		% de retransmissão		RTT médio (ms)	
	09/07/13	16/07/13	09/07/13	16/07/13	09/07/13	16/07/13	09/07/13	16/07/13
POP-MG	1235	869	96,7	59,2	1,05	0,60	65,4	17,6
POP-DF	290	499	59,2	63,4	0,11	0,20	22,9	35,3
POP-PA	74	127	51,6	38,1	1,00	0,39	110,1	95,8
POP-PB	120	13	13,5	14,2	0,67	0,74	51,0	72,4
POP-PE	147	72	16,4	14,9	2,37	0,42	107,3	24,9
POP-PR	23957	308	4042,4	125,8	0,14	0,38	30,2	34,3
POP-RJ	3665	3498	263,4	102,7	0,96	2,18	45,6	31,2
POP-RN	74	61	20,9	8,9	0,21	0,43	35,2	38,1
POP-RS	538	402	89,0	55,0	0,65	1,30	48,5	31,7
POP-SC	711	315	79,2	103,3	1,89	0,41	72,2	30,6
POP-SE	14	22	14,9	4,4	0,39	0,11	18,0	20,6
POP-SP	2238	2885	738,2	992,0	0,73	0,35	52,7	34,7
Amazon	18927	18890	241,3	270,6	2,19	1,98	54,8	33,3
UOL	187932	143939	5512,2	4595,8	0,68	0,70	49,2	26,8

Tabela 5.2: Tráfego HTTP por rotas nos dias 9 (falha) e 16 (sem falha) de julho.

Rota do Tráfego	conexões		volume de tráfego (MB)		% de retransmissão		RTT médio (ms)	
	19/08/13	12/08/13	19/08/13	12/08/13	19/08/13	12/08/13	19/08/13	12/08/13
POP-MG	1785	1102	114,9	147,1	0,55	0,60	34,0	16,8
POP-DF	2561	228	33,1	16,9	0,36	0,28	17,2	47,4
POP-PA	160	73	12,4	16,2	0,53	0,42	109,9	52,5
POP-PB	65	188	20,1	23,1	0,47	0,73	41,0	45,6
POP-PE	265	154	52,4	22,1	0,27	0,56	34,0	35,2
POP-PR	7746	293	3987,9	100,5	0,12	0,69	23,6	231,0
POP-RJ	13016	6608	622,9	682,8	0,29	0,50	25,5	31,9
POP-RN	162	92	9,3	33,3	1,65	0,41	41,6	77,5
POP-RS	424	519	50,7	61,8	0,80	0,76	65,6	35,6
POP-SC	942	498	145,3	41,5	0,86	2,27	104,5	66,4
POP-SE	61	38	14,2	4,0	1,64	0,16	26,7	29,9
POP-SP	2986	2057	415,0	272,7	1,11	0,92	82,8	31,9
Amazon	24687	18193	477,7	218,2	1,07	2,81	62,1	36,7
UOL	133681	132501	4099,3	5673,4	0,96	0,59	54,9	25,1

Tabela 5.3: Tráfego HTTP por rotas nos dias 19 (falha) e 12 (sem falha) de agosto.

Rota do Tráfego	conexões		volume de tráfego (MB)		% de retransmissão		RTT médio (ms)	
	28/08/13	21/08/13	28/08/13	21/08/13	28/08/13	21/08/13	28/08/13	21/08/13
POP-MG	668	397	58,5	55,2	0,64	0,72	82,4	48,4
POP-DF	435	228	29,8	19,0	1,30	0,77	109,1	23,4
POP-PA	47	49	6,3	15,1	0,64	0,48	46,0	62,2
POP-PB	98	97	20,3	6,0	0,73	0,43	100,9	45,2
POP-PE	170	33	4,8	5,8	0,85	0,22	27,3	51,7
POP-PR	928	299	809,5	136,4	0,99	0,58	179,2	73,4
POP-RJ	2683	1837	146,2	144,5	1,47	0,69	108,7	70,0
POP-RN	19	27	3,8	20,7	0,74	1,14	38,5	42,1
POP-RS	390	263	40,9	48,0	3,17	0,55	173,4	43,7
POP-SC	451	334	55,5	306,1	2,28	0,57	142,0	55,0
POP-SE	59	25	4,2	3,4	0,59	2,49	26,7	55,7
POP-SP	2959	1850	424,3	731,3	1,35	0,80	166,1	48,8
Amazon	8575	20220	88,5	273,4	2,42	1,05	138,1	40,7
UOL	66575	93492	1704,5	2950,3	1,24	1,01	129,2	47,5

Tabela 5.4: Tráfego HTTP por rotas nos dias 28 (falha) e 21 (sem falha) de agosto.

Rota do Tráfego	conexões		volume de tráfego (MB)		% de retransmissão		RTT médio (ms)	
	21/11/13	28/11/13	21/11/13	28/11/13	21/11/13	28/11/13	21/11/13	28/11/13
POP-MG	411	262	27,2	32,0	0,69	0,47	20,5	17,4
POP-DF	56	42	6,4	16,1	0,08	0,53	24,8	22,9
POP-PA	5	75	5,5	13,4	0,26	0,78	36,2	74,7
POP-PB	90	25	10,0	2,6	1,52	2,28	36,6	38,5
POP-PE	22	16	11,5	1,5	0,29	4,26	34,0	62,9
POP-PR	216	171	17,8	66,2	1,37	0,29	144,1	26,0
POP-RJ	3945	3200	192,0	217,8	1,27	0,85	25,6	22,6
POP-RN	9	43	4,8	4,3	0,45	0,26	30,9	47,2
POP-RS	398	346	36,7	45,1	2,28	1,89	133,6	54,2
POP-SC	253	216	31,0	26,9	1,24	0,87	124,1	55,8
POP-SE	41	60	1,3	13,8	1,16	0,32	21,3	39,9
POP-SP	5767	3429	169,0	1157,9	1,94	0,80	130,6	21,9
Amazon	15556	14345	246,7	244,4	2,30	1,86	133,8	30,2
UOL	86452	95443	1300,0	2458,7	2,38	0,90	120,7	29,0

Tabela 5.5: Tráfego HTTP por rotas nos dias 21 (falha) e 28 (sem falha) de novembro.

6 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou uma caracterização do impacto de falhas no backbone da RNP no tráfego da Universidade Federal de Juiz de Fora. As falhas por nós estudadas são de dois tipos, as falhas parciais e as falhas de desempenho.

Nas falhas parciais de enlaces, os destinos internacionais ficaram inacessíveis durante horas enquanto destinos no Brasil praticamente não foram afetados. Nós focamos no impacto das falhas no comportamento dos usuários e no comportamento de aplicações assíncronas que rodam em plano de fundo. Observamos indicativos de evasão dos usuários da rede da universidade durante falhas. Observamos também que o tráfego de entretenimento migra de aplicações indisponíveis para aplicações disponíveis (em particular, do *Facebook* para o *YouTube*). Por último, discutimos que aplicações assíncronas com servidores fora do Brasil, como Dropbox e SMTP, podem acumular tarefas durante a falha e gerar uma rajada de tráfego imediatamente após restauração da falha.

Um potencial mecanismo para redução da evasão dos usuários da rede durante falhas é o estabelecimento de parcerias de troca de tráfego com redes que hospedam serviços de produtividade. Em particular, conectividade com o Google, *Akamai* e *Amazon Web Services* em pontos de troca de tráfego nacionais tornaria vários serviços disponíveis durante falhas. Infelizmente esta solução depende da criação de centros de processamento de dados no Brasil, o que requer investimentos. Uma alternativa mais imediata é usar outras redes como provedores de acesso a serviços críticos durante falhas; por exemplo, outras redes educacionais da América Latina podem prover conectividade internacional temporariamente durante falhas.

Rajadas de tráfego geradas por aplicações assíncronas após restauração de falhas podem comprometer o desempenho da rede. Apesar das falhas que analisamos terem sido restauradas em período de baixa carga (após as 19:55), rajadas após uma restauração em horário de pico podem levar a congestionamento de enlaces internacionais e comprometer aplicações como voz sobre IP. Este problema pode ser mitigado por modificações no *software*, modeladores de tráfego (*traffic shaping*) ou priorização de tráfego.

Nas falhas de desempenho, uma ou mais ligações entre Pontos de Presença do Backbone da RNP foram interrompidas geralmente por rompimento de fibras de operadoras

parceiras. Apesar da interrupção, os usuários finais conseguiram acessar praticamente todos os serviços de rede, provavelmente graças a rotas alternativas disponíveis para o tráfego.

O maior impacto observado para este tipo de falha foi identificado nas métricas de desempenho da rede, não tendo sido identificadas alterações no comportamento dos usuários. Observamos que falhas em poucos links de conexão nos Pontos de Presença não diretamente ligados à rede final dos usuários geram pouco impacto final para a rede. Por outro lado, as falhas em um número maior de Pontos de Presença diversificados ou apenas em dois ou mais pontos de presença diretamente ligados a rede final pode ocasionar reduções consideráveis do volume trafegado para a rede e perda considerável de desempenho nas conexões.

Também foi identificado que as falhas de desempenho podem fazer com que os usuários, devido à demora em receber alguns dados da rede, em relação a dias normais, iniciem um maior número de conexões, sobrecarregando a rede com solicitações muitas vezes repetidas e desnecessárias. Verificamos isto ao observar que, mesmo quando ocorre considerável queda no volume trafegado durante as falhas, o número de conexões iniciadas no período praticamente não se altera.

Outro fator que chamou a atenção foi que as falhas de pequeno impacto, que provocaram apenas alterações de caminhos de roteamento, algumas vezes proporcionaram melhorias no acesso para alguns pontos na rede. Isto provavelmente ocorreu devido à rota alternativa possuir um desempenho mais favorável para estes destinos. Mecanismo de rotas redundantes são satisfatórios como paliativo para falhas de pequena dimensão, no entanto é necessário um estudo atento das características dos enlaces e do tráfego, para uma escolha eficiente dos caminhos primários do tráfego.

Para falhas que comprometem um maior número de ligações, a diversificação e o aumento de rotas alternativas aparentam ser soluções plausíveis.

Alguns dos resultados observados em nossas análises de falhas parciais são:

- Falhas nos enlaces internacionais da RNP não afetam o desempenho do tráfego nacional, possivelmente devido ao bom provisionamento dos enlaces nacionais.
- Redução gradativa de tráfego interativo durante as falhas parciais, resultante de alterações nas atividades realizadas pelos usuários no período ou até mesmo usuários deixando o campus prematuramente devido aos problemas de conectividade.

- A migração das aplicações utilizadas, particularmente aplicações de redes sociais, de sites indisponíveis (hospedados no exterior) para sites hospedados nacionalmente (e.g., do *Facebook* para o *YouTube*) é outro padrão identificado para falhas parciais.
- Aplicações assíncronas que executam em plano de fundo, e.g., *Dropbox* e SMTP, acumulam tarefas durante a falha e causam rajadas de tráfego após a restauração da falha.

Em relação às análises de falhas de desempenho alguns resultados observados são:

- Durante falhas de desempenho ocorre queda no volume de dados trafegados, porém são mantidas ou até aumentadas as quantidades de conexões observadas durante períodos de falhas.
- Ainda em relação às falhas de desempenho, não foram observados sinais de alterações no comportamento de usuários ou migração entre aplicações.
- Melhoria dos valores de RTT para algumas conexões nos períodos de falhas de desempenho, demonstrando que algumas alterações nas rotas motivadas pela ocorrência de falhas provocaram uma melhora considerável no desempenho de algumas conexões.

6.1 TRABALHOS FUTUROS

Atualmente estamos procurando outras universidades parceiras para obter dados de períodos com falha e estender nossa análise. Queremos também explorar alterações no comportamento de usuários e aplicações para melhorar técnicas de detecção de falhas. Por exemplo, um período com ausência de tráfego *Dropbox* seguido de uma rajada pode ser indicativo de uma falha (potencialmente parcial) de acesso a servidores do *Dropbox*. Em uma possível parceria com a RNP, gostaríamos ainda de analisar dados coletados junto a roteadores dos POPs, permitindo uma ampliação do escopo da análise através da correlação entre a análise das coletas locais e dos dados da RNP.

Agradecimentos

Agradecemos o apoio da UFJF, CNPq, CAPES, FAPEMIG e do projeto EU-IP mPlane (n-318627).

REFERÊNCIAS

ANAGNOSTAKIS, K. G.; IOANNIDIS, S.; MILTCHEV, S.; GREENWALD, M.; SMITH, J. M.; IOANNIDIS, J. Efficient packet monitoring for network management. In: IEEE. **Network Operations and Management Symposium, 2002. NOMS 2002. 2002 IEEE/IFIP**, 2002. p. 423–436.

BARFORD, P.; CROVELLA, M. Measuring web performance in the wide area. **ACM SIGMETRICS Performance Evaluation Review**, ACM, v. 27, n. 2, p. 37–48, 1999.

BERMUDEZ, I. N.; MELLIA, M.; MUNAFÒ, M. M.; KERALAPURA, R.; NUCCI, A. Dns to the rescue: Discerning content and services in a tangled web. In: ACM. **Proceedings of the 2012 ACM conference on Internet measurement conference**, 2012. p. 413–426.

BONFIGLIO, D.; MELLIA, M.; MEO, M.; ROSSI, D. Detailed analysis of skype traffic. **Multimedia, IEEE Transactions on**, IEEE, v. 11, n. 1, p. 117–127, 2009.

CARTER, R. L.; CROVELLA, M. E. Measuring bottleneck link speed in packet-switched networks. **Performance evaluation**, Elsevier, v. 27, p. 297–318, 1996.

CLAFFY, K.; MCCREARY, S. Internet measurement and data analysis: passive and active measurement. **University of California, CAIDA, USA**, 1999.

CLAFFY, K. C.; POLYZOS, G. C.; BRAUN, H.-W. Traffic characteristics of the t1 nsfnet backbone. In: IEEE. **INFOCOM'93. Proceedings. Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies. Networking: Foundation for the Future, IEEE**, 1993. p. 885–892.

DAINOTTI, A.; SQUARCELLA, C.; ABEN, E.; CLAFFY, K. C.; CHIESA, M.; RUSSO, M.; PESCAPÉ, A. Analysis of country-wide internet outages caused by censorship. In: ACM. **Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference**, 2011. p. 1–18.

DRAGO, I.; BOCCHI, E.; MELLIA, M.; SLATMAN, H.; PRAS, A. Benchmarking personal cloud storage. In: ACM. **Proceedings of the 2013 conference on Internet measurement conference**, 2013. p. 205–212.

DRAGO, I.; MELLIA, M.; MUNAFO, M. M.; SPEROTTO, A.; SADRE, R.; PRAS, A. Inside dropbox: understanding personal cloud storage services. In: ACM. **Proceedings of the 2012 ACM conference on Internet measurement conference**, 2012. p. 481–494.

FINAMORE, A.; MELLIA, M.; MEO, M.; MUNAFò, M. M.; ROSSI, D. Experiences of Internet traffic monitoring with tstat. **IEEE Network**, v. 25, n. 3, p. 8–14, 2011.

FRANCESCHINIS, M.; MELLIA, M.; MEO, M.; MUNAFO, M. et al. Measuring tcp over wifi: A real case. In: **1st workshop on Wireless Network Measurements (Winmee), Riva Del Garda, Italy**, 2005.

FRAZER, K. D. **NSFNET: A Partnership for High-speed Networking: Final Report, 1987-1995**, 1996.

FUENTES, F.; KAR, D. C. Ethereal vs. tcpdump: a comparative study on packet sniffing tools for educational purpose. **Journal of Computing Sciences in Colleges**, Consortium for Computing Sciences in Colleges, v. 20, n. 4, p. 169–176, 2005.

GILL, P.; JAIN, N.; NAGAPPAN, N. Understanding network failures in data centers: measurement, analysis, and implications. In: ACM. **ACM SIGCOMM Computer Communication Review**, 2011. v. 41, n. 4, p. 350–361.

HEIMLICH, S. A. Traffic characterization of the nsfnet national backbone. In: **Proceedings of the 1990 ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems**. p. 257–258.

IANNACCONE, G.; CHUAH, C.-n.; MORTIER, R.; BHATTACHARYYA, S.; DIOT, C. Analysis of link failures in an ip backbone. In: ACM. **Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment**, 2002. p. 237–242.

JACOBSON, V. Traceroute software. **Lawrence Berkeley Laboratories**, p. 473480, 1989.

JACOBSON, V. **Pathchar: A tool to infer characteristics of Internet paths**. 1997.

JACOBSON, V.; LERES, C.; MCCANNE, S. The tcpdump manual page. **Lawrence Berkeley Laboratory, Berkeley, CA**, 1989.

KATZ-BASSETT, E.; MADHYASTHA, H.; JOHN, J. P.; KRISHNAMURTHY, A.; WETHERALL, D.; ANDERSON, T. Studying Black Holes in the Internet with Hubble. In: **NSDI'08 Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation**, 2008. p. 247–262.

KOMPELLA, R.; YATES, J.; GREENBERG, A.; SNOEREN, A. Detection and Localization of Network Blackholes. In: **Proceedings of IEEE Infocom**, 2007.

LAI, K.; BAKER, M. Nettimer: A tool for measuring bottleneck link bandwidth. In: **USENIX Symp. Internet Technologies and Systems**, 2001. v. 1, p. 123 –134.

LAKHINA, A.; CROVELLA, M.; DIOT, C. Characterization of network-wide anomalies in traffic flows. In: ACM. **Proceedings of the 4th ACM SIGCOMM conference on Internet measurement**, 2004a. p. 201–206.

LAKHINA, A.; CROVELLA, M.; DIOT, C. Diagnosing Network-wide Traffic Anomalies. In: ACM. **SIGCOMM '04 Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications**, 2004b. p. 219–230.

MARKOPOULOU, A.; IANNACCONE, G.; BHATTACHARYYA, S.; CHUAH, C. N.; GANJALI, Y.; DIOT, C. Characterization of Failures in an Operational IP Backbone Network. In: **IEEE/ACM Transactions on Networking (TON)**, 2008. v. 16, n. 4, p. 749–762.

MATHIS, M.; ALLMAN, M. Empirical bulk transfer capacity. **IP Performance Metrics Working Group report in Proceedings of the Forty Third Internet Engineering Task Force, Orlando, FL**, 1988.

MCROBB, D.; HAWKINSON, J. **cflowd: a Cisco flow- export collector**. 1997.

MELLIA, M.; CARPANI, A.; CIGNO, R. L. Tstat web page. **URL: http://tstat.polito.it/index.shtml**, 2001.

MELLIA, M.; CARPANI, A.; CIGNO, R. L. Tstat: Tcp statistic and analysis tool. In: **Quality of Service in Multiservice IP Networks**, 2003. p. 145–157.

MELLIA, M.; CIGNO, R. L.; NERI, F. Measuring ip and tcp behavior on edge nodes with tstat. **Computer Networks**, Elsevier, v. 47, n. 1, p. 1–21, 2005.

MELLIA, M.; MEO, M. Measurement of iptv traffic from an operative network. **European Transactions on Telecommunications**, Wiley Online Library, v. 21, n. 4, p. 324–336, 2010.

MELLIA, M.; MEO, M.; MUSCARIELLO, L.; ROSSI, D. Passive identification and analysis of tcp anomalies. In: IEEE. **Communications, 2006. ICC'06. IEEE International Conference on**, 2006. v. 2, p. 723–728.

MOHAN, V.; REDDY, Y. J.; KALPANA, K. Active and passive network measurements: a survey. **Int J Comput Sci Inf Technol, ISSN**, p. 0975–9646, 2011.

MOORE, D.; KEYS, K.; KOGA, R.; LAGACHE, E.; CLAFFY, K. C. The coralreef software suite as a tool for system and network administrators. In: USENIX ASSOCIATION. **Proceedings of the 15th USENIX conference on System administration**, 2001. p. 133–144.

MURRAY, M. et al. Measuring the immeasurable: Global internet measurement infrastructure. In: **PAM–A workshop on Passive and Active Measurements**, 2001. p. 159–167.

NGUYEN, H. X.; THIRAN, P. Active measurement for multiple link failures diagnosis in ip networks. In: **Passive and Active Network Measurement**, 2004. p. 185–194.

OREBAUGH, A.; RAMIREZ, G.; BEALE, J. **Wireshark & Ethereal network protocol analyzer toolkit**, 2006.

OSTERMANN, S. Tcptrace: A tcp connection analysis tool. **URL: http://www.tcptrace.org**, 2000.

PAXSON, V. End-to-end internet packet dynamics. **IEEE/ACM Transactions on Networking (TON)**, IEEE Press, v. 7, n. 3, p. 277–292, 1999.

PAXSON, V.; MAHDAVI, J.; MATHIS, M.; ALMES, G. Framework for ip performance metrics. **Framework**, 1998.

POESE, I.; ; UHLIG, S.; KAAFAR, M. A.; DONNET, B.; GUEYE, B. IP Geolocation Databases: Unreliable? **SIGCOMM Comput. Commun. Rev.**, v. 41, n. 2, p. 53–56, 2011.

SANDVINE. **Global Internet Phenomena Report 2H2013**. 2013. Available at: `http://www.sandvine.com/trends/global-internet-phenomena`.

STINE, R. H. Fyi on a network management tool catalog: Tools for monitoring and debugging tcp/ip internets and interconnected devices. **IETF RFC 1147**, 1990.

THOMPSON, K.; MILLER, G. J.; WILDER, R. Wide-area internet traffic patterns and characteristics. **Network, iEEE**, IEEE, v. 11, n. 6, p. 10–23, 1997.

TURNER, D.; LEVCHENKO, K.; SAVAGE, S.; SNOEREN, A. C. A comparison of syslog and is-is for network failure analysis. In: **Proceedings of IMC**, 2013.

TURNER, D.; LEVCHENKO, K.; SNOEREN, A.; SAVAGE, S. California Fault Lines: Understanding the Causes and Impact of Network Failures. In: **Proceedings of the ACM SIGCOMM 2010 conference**, 2010. p. 315–326.

ZHANG, M.; ZHANG, C.; PAI, V. S.; PETERSON, L. L.; WANG, R. Y. Planetseer: Internet path failure monitoring and characterization in wide-area services. In: **OSDI**, 2004. v. 4, p. 12–12.

ZHANG, Z.; ZHANG, Y.; HU, Y. C.; MAO, Z. M.; BUSH, R. iSPY: Detecting IP Prefix Hijacking On My Own. In: **Proceedings of the ACM SIGCOMM 2008 conference on Data communication**, 2008. p. 327–338.