Caracterização do Impacto de Incidentes de Aplicações em Redes e Usuários

Leandro A. de Sá Vieira[1], Ítalo Cunha[1], Alex Borges Vieira[2], Idílio Drago[3]

[1]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

[2]Departamento de Ciência da Computação
Universidade Federal de Juiz de Fora

[3]Politecnico di Torino, Itália

{lvieira,cunha}@dcc.ufmg.br, alex.borges@ufjf.edu.br, idilio.drago@polito.it

Abstract. *Characterization studies focused on network incidents provide a foundation for improving user experience, particularly in face of increasingly complex networks and the rise of technologies ever more dependent on the Internet. The causes for network incidents are diverse, including scheduled maintenance, routing issues, optical fiber cuts, and device failures. In this paper we seek to advance our understanding of the impact of network incidents. We study network incidents on large content providers from multiple perspectives, and characterize the impact of incidents on user and application behaviors. Our results indicate changes in the traffic profile of applications, such as an increase in the number of flows concurrent with a decrease in the overall traffic volume, as well as changes in user behavior, like the migration of demand from applications impacted by the incident to applications that were not.*

Resumo. *Estudos focados na caracterização de incidentes com impacto na rede são primordiais para a melhoria da experiência do usuário, principalmente diante de redes com complexidade crescente e do surgimento de novas tecnologias cada vez mais dependentes de Internet. As causas destes incidentes são diversas, podendo ser manutenções programadas, falhas de roteamento, rompimento de cabos ópticos ou falhas de configuração em dispositivos como roteadores e comutadores. Em nosso estudo buscamos aumentar a nossa compreensão analisando de diferentes perspectivas o impacto de incidentes ocorridos em grandes provedores de conteúdo. Caracterizamos o impacto de incidentes no comportamento de usuários e aplicações. Nossos resultados apontam para mudanças no perfil de tráfego durante incidentes em aplicações, como o aumento do número de fluxos acompanhado de redução do volume de tráfego, e mudanças no comportamento de usuários, incluindo a migração de demanda de aplicações afetadas pelo incidente para outras não afetadas.*

1. Introdução

Estudos focados na caracterização de incidentes com impacto na rede são primordiais para a melhoria da experiência do usuário, principalmente diante do crescimento das redes e do

surgimento de novas tecnologias cada vez mais dependentes de Internet. As causas destes incidentes são diversas, podendo ser manutenções programadas, falhas de roteamento, rompimento de cabos ópticos ou falhas de configuração em dispositivos como roteadores e comutadores [Govindan et al. 2016, Turner et al. 2010]. O impacto de um incidente de rede é altamente variável, podendo ir de imperceptível à indisponibilidade. Além disso, a percepção do usuário pode variar de acordo com o incidente e a aplicação utilizada. Por exemplo, aplicações como jogos on-line e de comunicação por voz são mais impactadas quando o incidente causa aumento ou variação de latência. Por outro lado, aplicações como *streaming* de vídeo conseguem ser mais resilientes a um aumento de latência por utilizarem *buffer*, mas são mais afetadas pela diminuição da banda disponível.

Com o objetivo de aumentar a agilidade na resolução de incidentes e no atendimento a demandas de seus clientes, as operadoras de rede mantêm centros de operação de rede (*network operation center*, NOC). Os NOCs funcionam em tempo integral e contam com equipes formadas por técnicos e analistas que trabalham em escalas de revezamento. A operação da rede envolve investimento significativo em capital intelectual. Conforme um relatório da Cisco, recursos humanos correspondem a 50% do custo de operação de uma rede [Cisco 2011]. Além disso, é necessário a utilização de metodologias de análise assertivas e de ferramentas que auxiliem a detecção e mitigação de incidentes, sendo primordial para isso o entendimento dos incidentes que afetam a rede.

Uma forma de entender o impacto de incidentes de rede é através da realização de caracterização do tráfego durante a ocorrência de um incidente. A caracterização do tráfego de rede é importante para elaboração de procedimentos a serem executados na identificação e tratativa de um incidente, além de auxiliar na estimativa do tempo de resolução e mitigação do seus efeitos. Por exemplo, a caracterização do tráfego pode identificar que uma falha em uma aplicação A leva a um aumento de demanda e do tráfego de uma aplicação B. Se a operadora de rede não estiver preparada para esse aumento de tráfego na aplicação B, os usuários da rede poderão ser impactados não apenas pela falha na aplicação A mas também pelo congestionamento no acesso à aplicação B. Neste cenário, o conhecimento prévio do comportamento dos usuários indicaria engenharia de tráfego para alocação de mais recursos para a aplicação B durante falhas da aplicação A objetivando absorver alterações no tráfego da rede. Este estudo visa aprimorar nosso entendimento do comportamento de aplicações e usuários durante a ocorrência de um incidente de rede. Mais especificamente, focamos na caracterização do impacto no comportamento de aplicações e usuários de três redes durante incidentes ocorridos no Google e Facebook, dois dos maiores provedores de conteúdo da atualidade (seção 2). Realizamos a análise de metadados referentes ao tráfego de rede, como duração de fluxos, vazão e latência durante a ocorrência de incidentes em grandes provedores de conteúdo.

Nossos resultados apontam para mudanças no comportamento de aplicações e de usuários. Em particular, identificamos que a falha do Facebook levou a um aumento do número de fluxos gerados pelas aplicações, concomitante com uma redução do número de bytes por fluxo. Também identificamos um aumento de carga após a resolução de uma falha no Google. O entendimento do comportamento de aplicações pode ser útil para operadores de rede detectarem anomalias e se prepararem para possíveis impactos na rede. Também identificamos mudanças no comportamento de usuários, que migram de aplicações afetadas por incidentes para aplicações não afetadas.

Acreditamos que um melhor entendimento do impacto de incidentes será útil para operadores de rede, que podem aplicar nossa metodologia em suas redes para, por exemplo, ajustar políticas de engenharia de tráfego ou contratos de nível de serviço (*service level agreements*, SLA). Nossos resultados também são úteis para pesquisadores, que podem utilizá-los para informar modelos, simulações, experimentos e análises.

2. Conjunto de dados

Nesta seção apresentamos as três bases de dados utilizadas neste trabalho.

2.1. Politecnico di Torino (PoliTo)

Utilizamos sumários de tráfego coletados da rede do Politecnico di Torino (PoliTo) entre 01/01/2019 e 31/12/2019. A infraestrutura de rede do PoliTo abrange 3 campi e possui um roteador principal responsável pela conexão de todo o PoliTo com a Internet. O tráfego de Internet do roteador principal foi espelhado para um servidor e sumarizado executando a ferramenta TStat [Mellia et al. 2003].

A ferramenta TStat computa mais de 100 métricas para cada fluxo de rede dependendo do protocolo, aplicação, e encriptação do fluxo. As métricas podem ser classificadas nos seguintes grupos:

Informações de fluxos TCP: 44 métricas de fluxos TCP, como endereços e portas, número de bytes e pacotes, *timestamps* de início e fim, retransmissões e *flags* observados.

Inferências sobre fluxos TCP: 23 métricas contendo estatísticas indiretas (inferidas) de fluxos TCP, como número de retransmissões desnecessárias, quantidade de reordenação de pacotes e quantidade de retransmissões disparadas por *timeout*.

Informações de fluxos UDP: 9 métricas relacionadas a informações de fluxos UDP como número de bytes, pacotes, endereços IP e porta.

Informações sobre a rota: 7 métricas relacionadas à rota, como a latência fim-a-fim (mínimo, máximo, média) e número de *hops*.

Informações p2p: 6 atributos relacionados a tráfego P2P como número de mensagens de dados e sinalização.

Informações relacionadas à camada de aplicação: 20 métricas relacionadas à camada de aplicação como FQDN, tempo de resposta do DNS, e quantidade de requisições e respostas HTTP.

Identificação de origem do tráfego: O TStat permite a obtenção da origem o tráfego pelo FQDN ou pelo SNI (*Server Name Indicator*) quando o cliente envia o nome do servidor em mensagens *handshake* TLS.

2.2. Operadora X

Utilizamos indicadores de volume de tráfego em várias interfaces de roteadores de uma operadora brasileira de médio porte, que anonimizamos e denotamos como "Operadora X". A Operadora X hospeda caches de três grandes provedores de conteúdo; possui presença em pontos de troca de tráfego (PTT) de 4 estados do Brasil, 1 PTT na Europa, e 2 PTTs nos Estados Unidos, conexões diretas com 6 provedores de conteúdo de grande porte além de conexão com 3 provedores de trânsito escala global. Os dados obtidos são contadores de bytes e pacotes em interfaces de roteadores conectadas a clientes, caches, provedores de conteúdo e provedores de trânsito exportados a cada 5 minutos. Os dados da Operadora X cobrem o período entre 25/06/2019 e 14/07/2019.

2.3. Rede Nacional de Ensino e Pesquisa (RNP)

O conjunto de dados da RNP contém informações sobre fluxos coletados de roteadores concentradores que atendem diversas universidades e instituições de pesquisa do Brasil. Os dados são coletados em formato compatível com o NetFlow. Cada fluxo é sumarizado no conjunto de dados através dos seguintes campos: *timestamp* de início, duração, protocolo, endereço de origem e destino, porta de origem e destino, sistema autônomo (AS) de origem e destino, interface de entrada e saída, flags TCP e tipo de serviço (TOS). Além disso, para cada fluxo é calculado as seguintes informações quantitativas: número de bytes e pacotes de dados. Obtivemos os dados de roteadores de PoPs situados em São Paulo. O período de coleta destes fluxos contempla os meses de dezembro de 2020, fevereiro de 2021 e março de 2021.

3. Descrição dos Incidentes

Utilizamos falhas em grandes provedores de conteúdo para estudar o impacto de incidentes no comportamento de usuários e aplicações. As falhas tiveram impacto confirmado, por exemplo via notícias, reportagens, postagens em redes sociais[1] ou declarações públicas dos provedores de conteúdo.

Analisamos um total de 4 falhas neste trabalho. Porém, devido à pandemia, ensino remoto, e o perfil educacional das redes monitoradas, algumas falhas não tiveram impacto significativo no tráfego. A seguir apresentamos as falhas estudadas. Nas seções seguintes discutiremos apenas as duas primeiras, que tiveram impacto mais expressivo.

1. Falha ocorrida no Facebook dia 03/07/2019 entre 11:05 e 22:00 (GMT -3). Este incidente impactou de forma global os usuários das redes sociais Facebook, Instagram e WhatsApp, que ficaram impossibilitados de realizar o envio de arquivos como fotos, áudios e vídeos durante o período.[2] Este incidente está coberto nos conjuntos de dados do PoliTo e Operadora X.
2. Falha ocorrida no Google dia 14/12/2020 entre 08:40 e 09:35 (GMT -3). O serviço de autenticação de usuários ficou inoperante durante a duração do incidente; vários outros serviços que dependem de autenticação foram afetados.[3] Este incidente está coberto no conjunto de dados da RNP.
3. Falha ocorrida na Microsoft dia 15/03/2021 entre 16:51 e 19:00 (GMT -3). O incidente afetou diversos serviços como Teams e Office 365. A indisponibilidade dos serviços foi devido a uma falha no sistema de autenticação.[4]
4. Falha ocorrida no Facebook no dia 15/03/2021 entre 14:00 e 16:00 (GMT -3). Esta falha foi parcial e comprometeu o envio e recebimento de fotos e vídeos.[5]

4. Metodologia

Nesta seção descrevemos pré-processamento específico para adequar cada base de dado a nossas análises (seção 4.1). Descrevemos também como estabelecemos o comportamento padrão de usuários e aplicações em cada uma das redes analisadas, que comparamos com o comportamento observado durante os incidentes (seção 4.2).

[1] Incluindo o site Down Detector: https://downdetector.com

[2] https://twitter.com/Facebook/status/1146453213777936386

[3] https://status.cloud.google.com/incident/zall/20013

[4] https://twitter.com/MSFT365Status/status/1371554704518352896

[5] https://economia.uol.com.br/noticias/estadao-conteudo/2021/03/19/whatsapp-instagram-e-facebook-enfrentam-instabilidade-nesta-sexta.htm

4.1. Pré-processamento dos Dados

Como pré-processamento comum para todos os conjuntos de dados, removemos ruídos como letras e caracteres especiais, além disso, com intuito de minimizar o impacto da variação do tráfego em curtos intervalos de tempo, agrupamos dados referentes ao tráfego em intervalos de 1 hora. Aplicamos os seguintes passos específicos para cada base de dados:

Polito: Após serem sumarizados pelo TStat os dados do tráfego foram armazenados em um ambiente *Hadoop/Spark* mantido pelo PoliTo denominado BigDataLab. Com acesso para realizar consulta no BigDataLab, os dados de tráfego foram recuperados e classificados utilizando, quando possível, o SNI enviado no *handshake* TLS, caso não fosse possível, utilizamos o FQDN, esse processo foi realizado de forma semelhante ao feito por [Trevisan et al. 2020].

Operadora X: Como o conjunto de dados da Operadora X são simples contadores de volume de bytes e pacotes em interfaces de rede, utilizamos informações da interface para inferir propriedades das aplicações. Em particular, sabemos que enlaces dedicados via PNI *(Private Network Interconnection)* e com caches de CDNs *(Content Distribution Network)* carregam tráfego apenas do respectivo provedor de conteúdo.

RNP: Os dados do NetFlow não possuem informações sobre o FQDN ou URL relacionadas aos endereços IP comunicando em um fluxo. Para contornar esta limitação, inferimos a aplicação relativa a cada fluxo a partir dos ASes responsáveis pelos endereços IP. Classificamos os 263 ASes com maior volume de tráfego (que juntos totalizam 95% do tráfego) como de conteúdo (46), ISP (73) ou educacional (144). A classificação de ASes foi feita manualmente a partir do nome dos ASes cadastrados no whois.

4.2. Comportamento padrão

Neste processo utilizamos dados de uma semana anterior e de uma semana posterior ao dia da ocorrência do incidente. Após isso, buscamos estabelecer um *ground truth* de métricas de rede como duração de fluxos, RTT e vazão.

As series temporais que representam o tráfego possuem variações sazonais. As séries temporais referentes ao PoliTo seguem o fluxo de alunos no *campus* da instituição, com ausência de tráfego nos fins de semana e pouco tráfego no período de férias. A série temporal que representa o tráfego da Operadora X possui um comportamento diferente do PoliTo apresentando um aumento de tráfego no período noturno. Por fim, as séries temporais representam o tráfego da RNP em um momento de isolamento social (devido à pandemia do Coronavírus) em que as atividades das instituições de ensino estão sendo realizadas de forma remota. Diante disso, foram pensadas diferentes formas para se caracterizar a alteração de tráfego causada pelas falhas em provedores de conteúdo mencionadas na seção 2.

Para estimar os valores esperados nas séries temporais, utilizamos o cálculo do desvio padrão do período de 3 semanas excluindo o dia da ocorrência do incidente bem como sábados e domingos. Feito isso, calculamos o valor de 1 desvio padrão para mais e 1 desvio padrão para menos tendo como referência o valor médio de cada hora.

5. Resultados

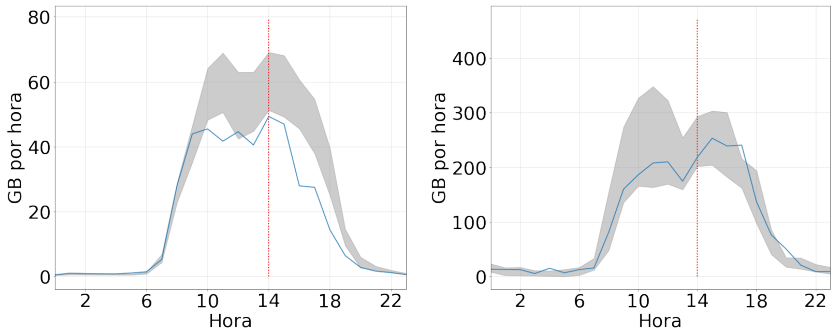
Nesta seção apresentamos a caracterização do impacto na falha do Facebook utilizando dados do PoliTo e Operadora X (seção 5.1), bem como os resultados da caracterização da falha no Google do ponto de vista da RNP (seção 5.2).

5.1. Falha do Facebook 03/07/2019

Os resultados da nossa análise sobre esta falha serão apresentados em três partes. Na primeira analisamos o impacto do incidente no tráfego do PoliTo considerando métricas como vazão, quantidade dos fluxos e duração dos fluxos que foram impactados pelo comportamento da aplicação durante o incidente. Na segunda realizamos análise similar no tráfego de rede da Operadora X, com resultados consistentes. Na terceira focamos no comportamento dos usuários durante o incidente comparando o volume de tráfego para as aplicações do Facebook e outras aplicações não afetadas durante o incidente.

5.1.1. Impacto no Tráfego do PoliTo

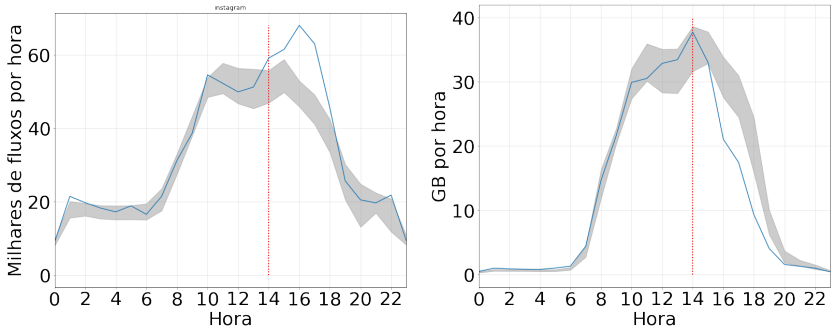
A figura 1 mostra o volume de tráfego durante o incidente (linha azul) e a média $\pm$ desvio padrão do volume de tráfego normal (zona cinza, seção 4.2). O início da falha está demarcado por linhas verticais pontilhadas. A figura 1(a) mostra o volume de tráfego para aplicações do Facebook (Facebook, Instagram e WhatsApp) e a figura 1(b) mostra o complemento do tráfego. Podemos observar na figura 1(a) a queda no volume de tráfego de serviços providos pelo Facebook no horário do incidente, enquanto a figura 1(b) mostra que o volume de tráfego dos demais serviços permaneceu dentro do esperado.



(a) Facebook - Tráfego (b) Outros

Figura 1. Volume de tráfego de aplicações do Facebook (Instagram, WhatApp e Facebook) e demais destinos

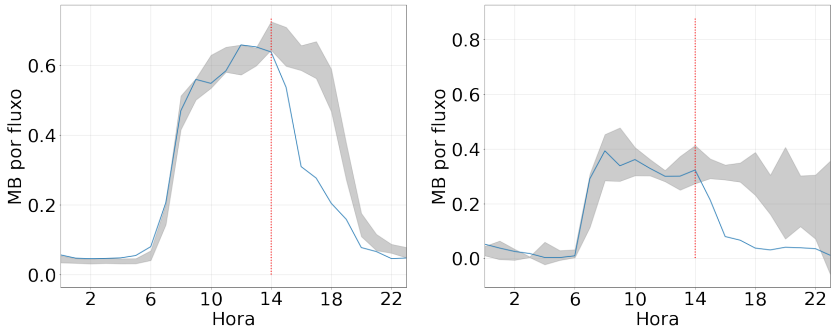
Outra característica observada durante o incidente foi o considerável aumento de conexões estabelecidas com os servidores do Instagram, concomitantemente com uma grande queda nos bytes trafegados. A figura 2 mostra a quantidade de fluxos e de bytes trafegados entre o PoliTo e o Instagram. Observamos um aumento do número de fluxos e uma redução do volume de tráfego, um comportamento inesperado causado por uma redução expressiva ($\approx$50%) da quantidade de bytes por fluxo, como mostrada na figura 3(a). Observamos comportamento similar para o WhatsApp, como evidenciado na figura 3(b). Apesar de não termos observado aumento expressivo na quantidade de fluxos do



(a) Aumento da quantidade de fluxos estabelecidos

(b) Diminuição do tráfego

Figura 2. Volume de tráfego e número de fluxos entre Instagram e PoliTo



(a) Instagram

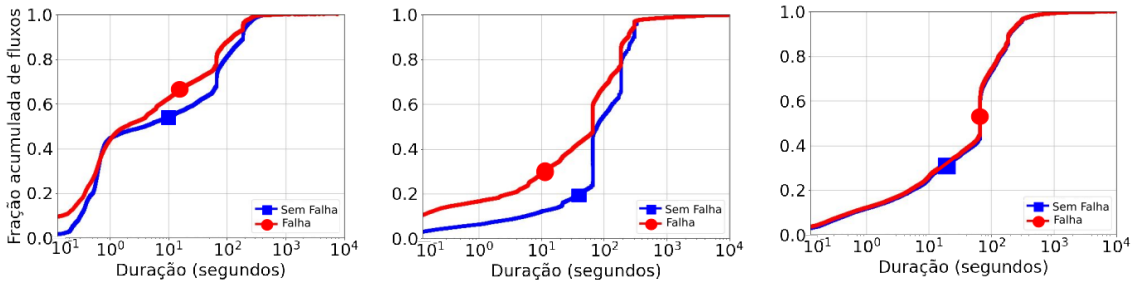
(b) WhatsApp

Figura 3. Número médio de MB trafegados por fluxo

WhatsApp (omitido), a queda de bytes por fluxo foi mais expressiva (≈75%) que para o Instagram.

O incidente no Facebook não causou alteração significativa na distribuição de duração de fluxos quando verificamos o agregado de todo o tráfego do PoliTo (omitido), entretanto, os fluxos relacionados ao Instagram e WhatsApp apresentaram uma redução significativa. A figura 4 mostra a distribuição da duração de fluxos TCP no PoliTo durante o incidente e no mesmo período durante os dias da semana anterior (sem ocorrência de incidente) para as três aplicações do Facebook.

Na figura 4(a) vemos a ocorrência de um aumento de aproximadamente 8% dos fluxos do Instagram terminando com menos de 100ms, e uma redução de aproximadamente 10% nos fluxos de longa duração (maior que 60s). A figura 4(b) mostra comportamento similar para o WhatsApp, mas uma redução ainda maior na duração dos fluxos (menor que 100ms e 60s). Por último, a figura 4(c) mostra que a duração dos fluxos referentes a rede social Facebook não sofreu alterações durante a ocorrência do incidente. Durante a ocorrência da falha, nenhuma alteração significativa foi identificada nos valores de latência ponta a ponta das conexões (omitido), o que indica ausência de mudanças de rotas (p.ex., para pontos de presença ou caches diferentes) ou congestionamento no período no incidente. Também não identificamos variações acentuadas referente a vazão (omitido).



(a) Instagram (b) Whatsapp (c) Facebook

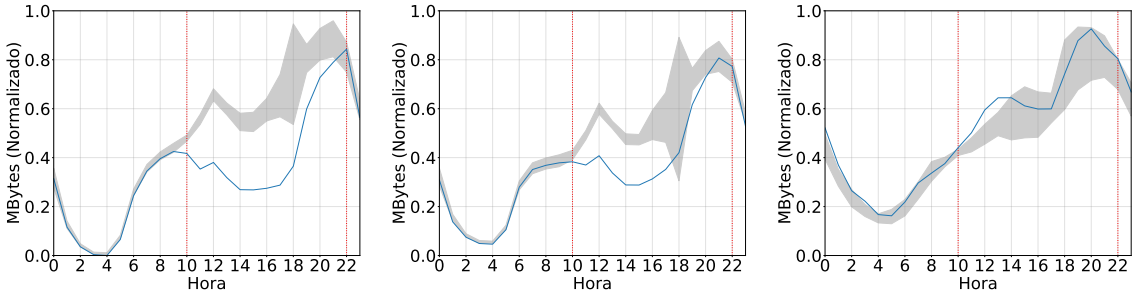
Figura 4. Comparação da duração de todos os fluxos durante a falha no dia 3 de julho e o mesmo dia e período da semana anterior.

Este incidente corresponde a uma falha parcial das aplicações. Durante o incidente era possível realizar algumas operações (como troca de mensagens e postagens), porém o envio e recebimento de fotos, vídeos e mensagens de áudio ficaram indisponíveis. Este comportamento indica uma potencial falha parcial de infra-estrutura que impactou a distribuição de conteúdo, mas não a os canais de controle das aplicações. Observando os dados do PoliTo identificamos que o site da rede social Facebook não foi afetado pelo incidente, o que poderia ser explicado por ele não utilizar, ou utilizar em menor escala, a infra-estrutura de distribuição de conteúdo utilizada pelo Instagram e WhatsApp.

5.1.2. Impacto no Tráfego da Operadora X

Nesta seção iremos apresentar o impacto do incidente no Facebook do ponto de vista da Operadora X. A Operadora X possui conexões diretas com o Facebook (PNI) além de cache CDN. As figuras 5(a) e 5(b) apresentam o tráfego da operadora com o Facebook utilizando PNI e cache CDN respectivamente. Podemos observar uma redução acentuada do volume de tráfego que coincide com o início do incidente e das reclamações dos usuários brasileiros (10 da manhã) conforme identificado pelo site Downdetector. O volume de tráfego utilizando PNI se aproximou a níveis normais por volta das 18h e atingiu um volume dentro da mediana às 22h, demonstrando que o impacto no escoamento do tráfego para o Facebook durou todo o período do incidente (figura 5(a)). O volume de tráfego para cache CDN do Facebook teve comportamento similar, estando dentro do volume esperado por volta das 18h (figura 5(b)). O volume total de tráfego com os provedores de trânsito durante o incidente não foi significativamente alterado (omitido).

Também não foram observadas grandes alterações neste período para outros CDNs ou PNIs (omitidos). A CDN com maior alteração de tráfego foi a Akamai, que teve apenas um leve aumento de tráfego, mostrado na figura 5(c). Concluímos que a variedade de conexões com provedores de Internet e com provedores de conteúdo, juntamente com a ocorrência do incidente em um horário fora do pico de tráfego contribuíram para a mitigação do impacto do incidente na rede da Operadora X.



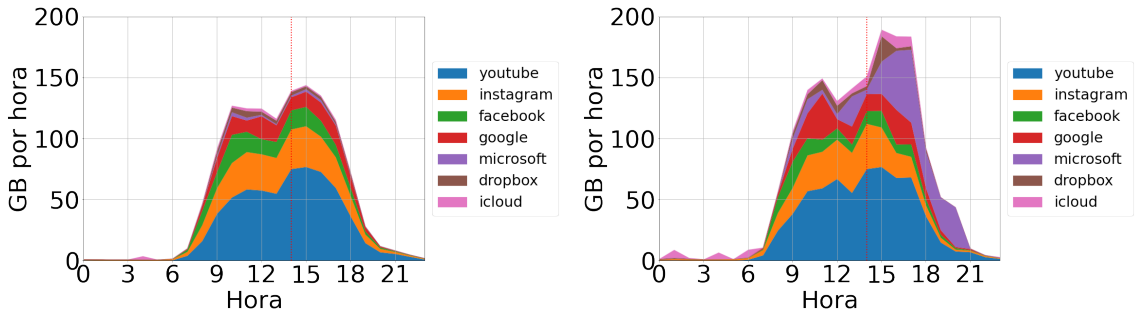
(a) PNI Facebook (b) CDN Facebook (c) CDN Akamai

Figura 5. Alterações no tráfego no dia do incidente

5.1.3. Comportamento do Usuário

Nesta seção iremos analisar como o incidente afetou o comportamento dos usuários, mais precisamente as aplicações e serviços utilizados. Em nossas análises não observamos alterações nos volumes relativos de tráfego de *upload* das aplicações, sendo assim focamos nossas análises no tráfego de *download*.

As figuras 6(a) e (b) apresentam o volume do tráfego de *download* dos serviços com maior tráfego no PoliTo durante o período observado. O Instagram possui o segundo maior tráfego de dados considerando a mediana de cada hora do dia e a rede social Facebook o terceiro maior volume. O somatório dos serviços fornecidos pelo Facebook corresponde a cerca de 15% do tráfego durante o período analisado, sendo o Instagram responsável por cerca de 10% deste tráfego. No momento do incidente no Facebook (após as 14h00 horário no fuso horário Italiano) iniciou-se um aumento de tráfego proveniente de serviços fornecidos pela Microsoft como Office 365, OneDrive, Outlook e Teams (tráfego relacionado a atualização de sistemas operacionais da Microsoft não estão incluídos). A Microsoft foi o provedor de conteúdos com o maior aumento de tráfego no momento do incidente no Facebook. Seguido a este aumento do tráfego para a Microsoft, observamos um aumento de tráfego para os serviços de nuvem como Dropbox e iCloud, como pode ser verificado nas figuras 6(a) e (b).



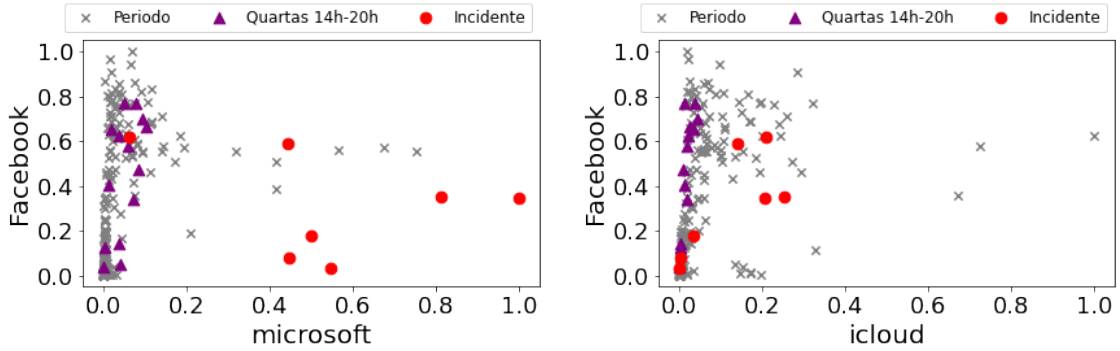
(a) Médiana do tráfego de *download* em dias normais (b) Tráfego de *download* no dia do incidente

Figura 6. Volume de tráfego agregado dos serviços com maior tráfego no período analisado.

As figuras 7(a) e (b) mostram a correlação entre o volume de tráfego de *download* entre diferentes aplicações. As coordenadas de cada ponto são o volume de tráfego das

duas aplicações por um período de uma hora. As coordenadas estão normalizadas pelo maior volume de tráfego observado no período. Os círculos vermelhos indicam o volume de tráfego em cada hora durante o incidente (3 de julho entre 14h e 20h), os triângulos roxos indicam os volumes de tráfego durante o mesmo período (14–20h) nas quartas-feiras das semanas anterior e posterior do incidente (período de 3 semanas). Indicamos de forma especial apenas o período entre 14h e 20h pois o tráfego do PoliTo cai significativamente (em dias normais e no dia do incidente) após as 20h. Os pontos cinzas indicam os volumes de tráfegos em outros dias úteis durante as três semanas.

No período observado não há forte correlação entre o tráfego para aplicações do Facebook e da Microsoft. Entretanto podemos observar no eixo x da figura 7(a) que o volume de tráfego de *download* para a Microsoft no momento do incidente é próximo ao volume máximo registrado no período e cerca de 8 vezes maior que a mediana do horário. Também observamos um aumento do tráfego de *download* de plataformas de hospedagem em nuvem como Dropbox e iCloud. Na figura 7(b) podemos observar comportamento similar: o tráfego do iCloud foi maior do que a média normal do período. Excluindo os 3 pontos cinzas mais à direita da figura 7(b) que ocorreram no período da tarde do dia anterior, temos um aumento de tráfego do iCloud próximo aos valores máximos observados em todo o período de 3 semanas.



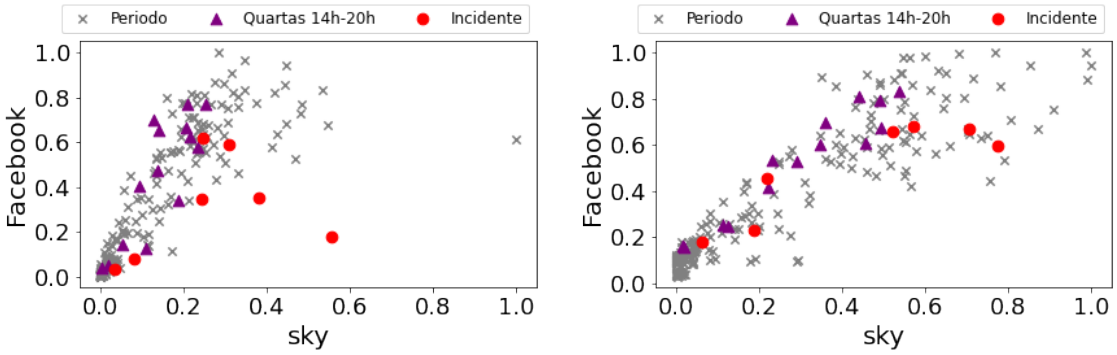
(a) Tráfego de entrada Microsoft

(b) Tráfego de entrada iCloud

Figura 7. Distribuição normalizada e comparativa de tráfego de entrada entre o Facebook e Microsoft e Facebook e iCloud

As figuras 8(a) e (b) são semelhantes às figuras 7(a) e (b). A figura 8(a) mostra o tráfego em cada hora para o Facebook e para a plataforma de TV Sky. Observamos uma correlação positiva entre as plataformas de entretenimento (pontos roxos e cinzas), porém durante o incidente a correlação é majoritariamente negativa (pontos vermelhos) e o volume de tráfego para a Sky fica acima da média do período, indicando uma possível migração de usuários. A figura 8(b) é complementar e mostra a quantidade de fluxos para a plataforma Sky, que aumentou em aproximadamente 40% relativo à média dos períodos sem incidente.

Estes resultados são similares aos de [Duarte et al. 2015], que também detectou migração de usuários de aplicações afetadas por incidentes para aplicações que não foram afetadas. Nossos resultados corroboram esta tendência e fortalecem a recomendação que operadores de rede preparem suas redes para mudanças no perfil de tráfego em caso de incidentes.



(a) Tráfego de entrada Sky

(b) Fluxos Sky

Figura 8. Distribuição normalizada e comparativa de tráfego de entrada (a) e fluxos (b) entre o Facebook e a plataforma Sky

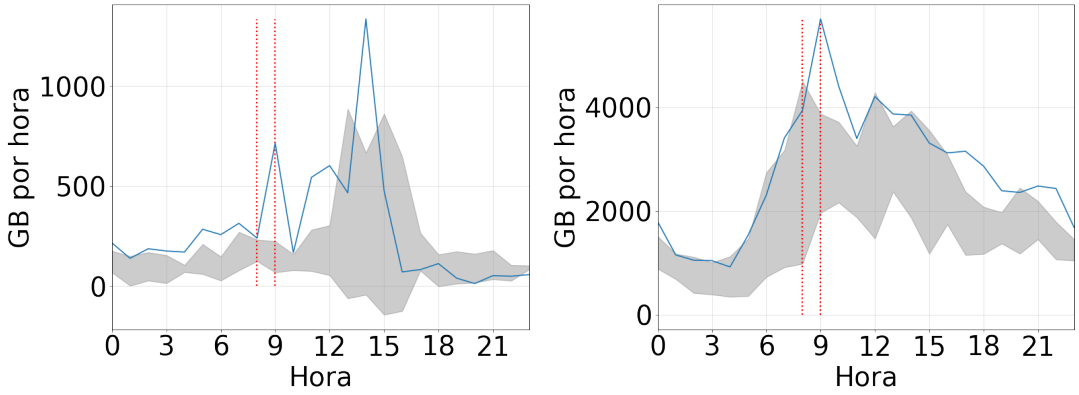
5.2. Falha no Google 14/12/2020

Nesta seção iremos discutir a falha do Google, que é coberta apenas pelos dados da RNP. O isolamento social alterou consideravelmente o comportamento do tráfego da rede da RNP: o trabalho e ensino remotos reduziram o número de usuários em instituições conectadas à RNP e levou a uma significativa redução no volume de tráfego, em particular para provedores de conteúdo como Google e Facebook. Sendo assim, consideramos a hipótese de que a ocorrência de incidentes em grandes provedores de conteúdo exerçam impacto indireto no tráfego da RNP.

O incidente ocorrido no Google teve duração de 1 hora e afetou o serviço de autenticação de usuários, que é utilizado por diversas aplicações, incluindo Gmail, Google Drive e Youtube. A diminuição da presença de pessoas nos *campus* e prédios de institutos de pesquisa devido às restrições impostas pela pandemia não nos permitiu observar o impacto do incidente de forma direta no tráfego da RNP. A figura 9(a) mostra o volume de tráfego entre RNP e Google; vemos que o volume de tráfego durante a pandemia é baixo no período da manhã (em torno de 600 GB/h) e aumentou em aproximadamente 800GB sobre o nível normal na hora seguinte ao incidente. Este aumento é espelhado na figura 9(b), que mostra o volume de tráfego na RNP para instituições de ensino e pesquisa.

Como explicações para estas observações, consideramos que o incidente pode ter levado a um represamento de demanda, que foi atendida após a resolução do incidente. Em particular, instituições que utilizam os serviços do Google Suite, como Google Drive, podem ter levado a um aumento de demanda subsequente à resolução do incidente, p.ex., para sincronização de arquivos. Por último, o aumento do tráfego pode ter sido induzido pelas próprias aplicações do Google após resolução do incidente.

Picos similares de demanda após resolução de incidentes foram observados em trabalhos anteriores [Duarte et al. 2015], e indicam que operadores de rede podem esperar aumento de carga após incidentes. Na falha do Facebook (seção 5.1) não observamos pico de demanda após a resolução do incidente, possivelmente por que o incidente acabou às 02h na Itália e 22h no Brasil, quando a carga está em processo de queda. Outra possível explicação para a ausência de pico de demanda após a resolução do incidente do Facebook é o fato das aplicações do Facebook serem primariamente interativas, de forma que o



(a) Tráfego para o Google (b) Tráfego para Instituições de Ensino e Pesquisa

Figura 9. Tráfego referente a provedores de Internet e instituições de ensino e pesquisa - As sombras correspondem a um desvio padrão.

represamento de demanda é condicionado à atividade dos usuários (que às 22h está em queda).

6. Trabalhos relacionados

A literatura relacionada a caracterização e compreensão de incidentes com impacto na rede é extensa e engloba diferentes abordagens como análises ativas, passivas, caracterização de mensagens, comportamento do usuário e utilização de aprendizado de máquina. Entretanto, os trabalhos com foco na caracterização de incidentes de rede são mais raros de serem encontrados. A seguir iremos apresentar alguns estudos que buscaram de alguma forma aumentar o entendimento relacionado a incidentes de rede.

6.1. Medições e Dados de Rede

A caracterização de incidentes de rede é objeto de estudo de diversos trabalhos envolvendo medições ativas de rede através de ferramentas como *ping* e *traceroute*, medições passiva de dados como atualizações de roteamento e processamento de informações não estruturadas.

Medições ativas com utilização de pontos de medição atuam no plano de dados e plano de controle possibilitando aos pesquisadores uma visão da Internet mesmo sem acesso a informações privilegiadas de rede, medições ativas também são utilizadas na detecção de incidentes de conectividade de redes [Kompella et al. 2007, Katz-Bassett et al. 2012].

Medições passivas da rede possuem a vantagem de não sobrecarregar a rede com envio de sondas para realização de medições. Estes dados podem ser públicos como anúncios BGP ou privados como *syslogs* de equipamentos e atualizações SNMP e IS-IS. A grande maioria dos trabalhos que utilizam de dados privados realizam caracterizações de incidentes ocorridos em redes educacionais ou de pesquisa. Como exemplo, os trabalhos [Markopoulou et al. 2008, Turner et al. 2010] utilizam dados extraídos de logs de dispositivos de rede, atualizações IS-IS e troca de e-mails da equipe responsável pela operação da rede.

Metadados e informações textuais não estruturadas como e-mails e registros de incidentes, são formas típicas de se documentar e acompanhar incidentes de rede. [Markopoulou et al. 2008, Turner et al. 2010] utilizaram destes dados de forma complementar a mensagens IS-IS. [Govindan et al. 2016] realizaram um estudo de mais de 100 registros de incidentes com grande impacto na rede do Google, os incidentes foram documentados em registros conhecidos como *post-mortem*, estes registros geralmente contêm informação detalhada de incidentes que causaram grande impacto no funcionamento da rede, o objetivo principal é que sirvam de aprendizado na elaboração de procedimentos com intuito de impedir a reincidência destes incidentes.

6.2. Comportamento do Usuário em Relação a Incidentes de Rede

Alguns incidentes não são possíveis de serem contornados pela resiliência da rede, p. ex., usando rotas alternativas e podem demandar horas para serem resolvidos. [Duarte et al. 2015] caracterizam incidentes ocorridos na rede da RNP e o seu impacto na rede de uma universidade. O trabalho traz uma perspectiva mais próxima do usuário, relatando as mudanças no perfil do tráfego, como a migração de usuários para o Facebook diante da ocorrência de degradação de conexão com o Youtube. Trabalhos como [Parwez et al. 2017, Qiao et al. 2018] utilizam de processamento de grandes quantidades de dados referentes a fluxos de rede para identificar comportamentos de usuários de redes móveis. O *framework* apresentado por [Qiao et al. 2018] caracteriza a utilização de diferentes tipos de serviços pelos usuários conforme horário do dia, este conhecimento pode ser útil na mitigação de incidentes e na engenharia de tráfego. O entendimento do comportamento do usuário diante de alterações da qualidade da uma aplicação pode ser útil para melhorias de serviços fornecidos pela Internet. Com objetivo de ampliar o conhecimento neste tema o estudo apresentado em [Guarnieri et al. 2017] busca identificar o comportamento do usuário diante de alterações de qualidade em transmissões de partidas de futebol da copa do mundo de 2014, o dataset utilizado pelos pesquisadores contém dados de um grande portal de *streaming*.

7. Conclusão

Neste artigo caracterizamos incidentes em grandes provedores de conteúdo. Comparamos propriedades do tráfego durante o período de incidentes com propriedades do tráfego em períodos normais de operação. Analisando uma falha do Facebook e identificamos mudanças em características do tráfego das aplicações afetadas durante o incidente, mais especificamente uma redução significativa do tamanho e duração dos fluxos de rede. Identificamos também mudanças no volume relativo de tráfego gerado por diferentes aplicações durante o incidente, indicando mudanças de comportamento dos usuários. A pandemia do coronavírus e isolamento social levaram à implantação de teletrabalho e ensino remoto, alterando significativamente o tráfego das instituições analisadas e reduzindo o impacto observável de incidentes de rede no tráfego durante 2020. Apesar disso conseguimos identificar um aumento significativo no volume de tráfego após a restauração de um incidente afetando vários serviços do Google.

Nossos resultados indicam possíveis medidas que operadores de rede podem tomar para mitigar o impacto de incidentes e melhorar a experiência dos usuários. Porém, consideramos que a maior contribuição é a adição de mais resultados sobre o impacto de incidentes de rede em aplicações e usuários, um campo com poucos resultados devido à dificuldade de obtenção de dados, o que foi exacerbado em 2020.

7.1. Trabalhos Futuros

A caracterização de incidentes de rede de acordo com a causa raiz (*root cause*) pode prover informações para construção de modelos para identificação, classificação e mitigação de incidentes em redes de operadoras ou em provedores de conteúdo. Exemplos incluem a priorização de atendimentos e alocação de esforços segundo a classificação de incidentes, melhorando o processo de tomada de decisões quando recursos disponíveis são insuficientes para o atendimento de todas as demandas existentes. De forma complementar a este trabalho, planejamos analisar registros de incidentes juntamente com os dados sobre o tráfego da rede.

Referências

Cisco (2011). The Economics of Networking. In *Technical Report*.

Duarte, R., Vieira, A. B., Cunha, I., and Almeida, J. M. (2015). Impact of Provider Failures on the Traffic at a University Campus. In *Proc. IFIP Networking*.

Govindan, R., Minei, I., Kallahalla, M., Koley, B., and Vahdat, A. (2016). Evolve or die: High-availability design principles drawn from googles network infrastructure. In *Proceedings of the 2016 ACM SIGCOMM Conference*, page 58–72, New York, NY, USA. ACM.

Guarnieri, T., Drago, I., Vieira, A. B., Cunha, I., and Almeida, J. (2017). Characterizing qoe in large-scale live streaming. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pages 1–7.

Katz-Bassett, E., Scott, C., Choffnes, D. R., Cunha, I., Valancius, V., Feamster, N., Madhyastha, H. V., Anderson, T., and Krishnamurthy, A. (2012). LIFEGUARD: Practical Repair of Persistent Route Failures. In *Proc. ACM SIGCOMM*.

Kompella, R., Yates, J., Greenberg, A., and Snoeren, A. (2007). Detection and Localization of Network Blackholes. In *Proc. IEEE INFOCOM*.

Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah, C. N., Ganjali, Y., and Diot, C. (2008). Characterization of Failures in an Operational IP Backbone Network. *IEEE/ACM Trans. Netw.*, 16(4):749–762.

Mellia, M., Carpani, A., and Cigno, R. L. (2003). Tstat: Tcp statistic and analysis tool. In *Proceedings of the Second International Workshop on Quality of Service in Multiservice IP Networks*, QoS-IP 2003, page 145–157, Berlin, Heidelberg. Springer-Verlag.

Parwez, M. S., Rawat, D. B., and Garuba, M. (2017). Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network. *IEEE Transactions on Industrial Informatics*, 13(4):2058–2065.

Qiao, Y., Xing, Z., Fadlullah, Z. M., Yang, J., and Kato, N. (2018). Characterizing flow, application, and user behavior in mobile networks: A framework for mobile big data. *IEEE Wireless Communications*, 25(1):40–49.

Trevisan, M., Giordano, D., Drago, I., Munafò, M. M., and Mellia, M. (2020). Five years at the edge: Watching internet from the isp network. *IEEE/ACM Transactions on Networking*, 28(2):561–574.

Turner, D., Levchenko, K., Snoeren, A., and Savage, S. (2010). California Fault Lines: Understanding the Causes and Impact of Network Failures. In *Proc. ACM SIGCOMM*.