CARACTERIZAÇÃO DE TRÁFEGO UTILIZANDO CLASSIFICAÇÃO DE FLUXOS DE COMUNICAÇÃO

Guilherme Silva Vilela

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Aprovada por:

Prof. Luis Felipe Magalhães de Moraes, Ph. D.

Prof. Aloysio de Castro Pinto Pedroza, Dr.

Prof. Claudio Luis de Amorim, Ph. D.

Prof. Marcio Portes de Albuquerque, Dr.

RIO DE JANEIRO, RJ - BRASIL

MARÇO DE 2006

VILELA, GUILHERME SILVA

Caracterização de Tráfego Utilizando Classificação de Fluxos de Comunicação [Rio de Janeiro] 2006

XIV, 74 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006)

Dissertação - Universidade Federal do Rio de Janeiro, COPPE

1. Caracterização de tráfego
2. Monitoramento de redes
3. Fluxos de comunicação

I. COPPE/UFRJ II. Título (Série)

Dedicatória

A minha família e a Rafaela

Agradecimentos

A toda minha família, por todo amor, apoio e orientação ao longo de minha vida.

Ao meu orientador, Prof. Luis Felipe, pela oportunidade de trabalho, pela confiança que depositou em mim, pela sua orientação, ensinamentos, apoio e amizade.

Aos Profs. Aloysio Pedroza, Claudio Amorim e Marcio Portes por participarem da banca de avaliação do trabalho, contribuindo com correções e sugestões.

À toda equipe do Laboratório RAVEL, pelas intensas discussões, pelo apoio, convivência e amizade.

Ao PESC/COPPE, pelo suporte operacional e equipamentos utilizados.

Ao meu primo Serginho e sua esposa Luciana, que ajudaram muito na melhora do texto da dissertação.

A minha namorada Rafaela, por todo apoio e companheirismo em todos momentos. Sem ela a realização deste trabalho teria sido muito mais difícil.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

CARACTERIZAÇÃO DE TRÁFEGO UTILIZANDO CLASSIFICAÇÃO DE FLUXOS DE COMUNICAÇÃO

Guilherme Silva Vilela

Março/2006

Orientador: Luis Felipe Magalhães de Moraes
Programa: Engenharia de Sistemas e Computação

A caracterização de tráfego é hoje um importante instrumento para o planejamento e gerenciamento das redes de computadores. Entretanto, ainda não existe um consenso sobre métricas e metodologias a serem adotadas. O presente trabalho propõe uma nova metodologia para a classificação dos fluxos de comunicação em N classes. Importantes resultados foram obtidos através do estudo de caso feito na Rede Rio de Computadores, a rede acadêmica e de pesquisa do Estado do Rio de Janeiro. Foram identificadas, as distribuições estatísticas dos diversos tipos de tráfego em função dos seus tamanhos, durações e taxas. Apesar de alguns trabalhos da literatura abordarem tais características, existem poucos estudos sobre como essas variáveis estão relacionadas. Nesta tese é feito um estudo sobre a correlação de tais medidas, indicando os impactos e as possíveis causas do comportamento observado. É apresentada também uma análise sobre quais aplicações são responsáveis pela maior parte do tráfego da rede, assim como comparações dos resultados obtidos com aqueles decorrentes de outros trabalhos existentes na literatura.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

TRAFFIC CHARACTERIZATION USING CLASSIFICATION OF COMMUNICATION FLOWS

Guilherme Silva Vilela

March/2006

Advisor: Luis Felipe Magalhães de Moraes
Department: Computer and System Engineering

Traffic characterization is an important tool for the planning and management of computer networks. However, there is still no agreement about what metrics and methodologies should be used. This dissertation article proposes and presents a new classification methodology for the network flows in N possible classes. To validate the methodology, a case study with Rede Rio de Computadores, the research and academic network of the State of Rio de Janeiro, was performed, and important results were obtained. The statistical distributions of the various types of traffic as a function of the size, duration and rate were identified. Although some works in the literature have focused on these characteristics, there is still a lack of research on how these variables are related. This thesis studies the traffic correlation of these measurements, indicating the impacts and possible causes for the observed behavior. An analysis of which applications are responsible for the majority of the network traffic and comparisons of results obtained from other existing works in the literature are also performed.

Glossário

TCP/IP :	*Transmission Control Protocol / Internet Protocol*;
LAN:	*Local Area Network*;
WWW:	*World Wide Web*;
AS:	*Autonomous System*;
IETF	*Internet Engineering Task Force*;
IPPM	*Internet Protocol Performance Metric*;
SNMP	*Simple Network Management Protocol*
BGP	*Border Gateway Protocol*

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 A História da Internet

A origem da Internet remete ao início da década de 60. O primeiro registro de interação social que se tornou possível devido as redes foi uma série de memorandos escritos por J.C.R. Licklider, do MIT [1], em agosto de 1962, discutindo o conceito da "Rede Galáxica". Esta rede foi idealizada como um conjunto de computadores interligados globalmente, através da qual todos poderiam acessar dados e programas de qualquer local rapidamente.

Aproximadamente no mesmo período (julho de 1961), Leonard Kleinrock publicou o primeiro artigo sobre a teoria de comutação por pacotes [2]. Em paralelo, Paul Baran [3, 4] e membros do grupo Rand Corporation estavam desenvolvendo um projeto de comunicação descentralizada para a Força Aérea Americana, um serviço de redes de chaveamento de pacotes para comunicação de voz segura. Também na mesma época, do outro lado do Atlântico, no National Physical Laboratory (NPL), em Middlesex, Inglaterra, Roger Scantlebury e Donald Davies [5] desenvolviam a NPL Data Network. Todos esses trabalhos proprõem que a comunicação entre os computadores deve ser feita utilizando pacotes e não circuitos. Dentro do paradigma da comutação por circuito, que é empregado nas redes de telefone, os usuários estabelecem uma conexão dedicada com uma quantidade fixa de faixa entre origem e

destino durante a comunicação. Este tipo de abordagem é eficiente para comunicações telefônicas de voz, onde os dados são transmitidos a uma taxa constante e o tempo de estabelecimento da conexão é, em geral, menor que o tempo de duração da comunicação. No entanto, o perfil do tráfego de dados é diferente, não sendo mais um tráfego constante, mas sim por rajada. Desta forma, se o canal é alocado de forma dedicada, uma grande perda de eficiência irá ocorrer, uma vez que poderá haver períodos onde os recursos estão alocados mas não utilizados. Outro problema que pode ser abordado é que, muitas vezes, as transmissões são de curta duração. Desta forma, a configuração para alocação de um circuito terá um grande *overhead*. De acordo com o paradigma de comutação de pacotes, a comunicação não é orientada a conexão, e os dados transmitidos na rede são separados em pequenas unidades, que são chamados pacotes. Cada pacote contém o endereço de destino e origem das duas entidades que trocam informações, e é encaminhado de forma independente através da rede até que ele alcance seu destino, sem a necessidade de reservar recursos ao longo de seu trajeto. Experimentos feitos no ano de 1965 confirmaram que computadores que utilizavam sistema de tempo compartilhado (*time-sharing*) podiam funcionar bem, executando programas e enviando dados, conforme a necessidade, para máquinas remotas. No entanto, a comutação de circuitos da rede telefônica era totalmente inadequado para este tipo de tarefa [6]. Desta forma, o paradigma da comutação por pacotes mostrou-se uma tecnologia adequada para a comunicação entre computadores.

Em 1966, o primeiro conceito do que viria a se tornar a primeira rede de computadores foi desenvolvido [7]. Vários pesquisadores trabalharam na otimização da topologia de rede, e no desenvolvimento do primeiro protocolo ponto-a-ponto, chamando *Network Control Protocol* (NCP). A primeira rede de comunicação de computadores surgiu em 1972 e foi chamada de *Advanced Research Projects Agency Network* (ARPANET). Sua primeira aplicação foi o correio eletrônico (*e-mail*), desenvolvido no mesmo ano, seguido de várias outras aplicações com o objetivo de facilitar a coordenação entre os pesquisadores.

1.2 Da ARPANET até a Internet

A ARPPANET original cresceu e se transformou na Internet, baseando-se na idéia de que haveria diversas redes independentes e de topologias diferentes. A chave por trás do conceito técnico foi a rede de arquitetura aberta (*open-architecture networking*), introduzida por Kahn em 1972. Esta arquitetura tinha quatro regras básicas:

- Cada rede deveria ser independente e nenhuma mudança interna seria necessária para que as redes se conectassem à Internet.
- As comunicações seriam baseadas no melhor esforço (*best-effort*). Se um pacote não conseguisse chegar ao seu destino final, ele seria rapidamente retransmitido pela máquina de origem.
- Caixas pretas (posteriormente chamadas de roteadores) seriam utilizados para interconectar as redes. Nenhuma informação sobre fluxos individuais ou pacotes que passassem nos roteadores seria retida. Isso os manteria simples, evitando que as adaptações e recuperações de falhas fossem complicadas.
- Não haveria controle global em níveis operacionais.

Esses princípios guiaram o desenvolvimento do primeiro protocolo de comunicação da Internet, chamado de *Transmission Control Protocol/Internet Protocol* (TCP/IP). O TCP/IP continha todas as funcionalidades necessárias para as "redes de arquitetura aberta". O protocolo inicial foi posteriormente reorganizado em dois protocolos distintos: *Internet Protocol* (IP), que provê somente o endereçamento e encaminhamento de pacotes individuais, e separadamente o *Transmission Control Protocol* (TCP), que provê alguns serviços como o controle de fluxo e a recuperação de pacotes perdidos. Para aplicações que não precisam da confiabilidade provida pelo TCP, um protocolo alternativo foi elaborado para proporcionar acesso direto aos serviços básicos do protocolo IP. Este protocolo foi chamado *User Datagram Protocol* (UDP). No final de 1985, a Internet estava estabelecida como

uma tecnologia que oferecia suporte a uma larga comunidade de pesquisadores e desenvolvedores, e começava a ser usada por outras comunidades para comunicações diárias entre computadores.

1.3 Provedores de Acesso e a Internet nos Dias de Hoje

Na metade da década de 70, novas redes de computadores surgiam sempre que algum financiamento era encontrado. Em 1984-1985, o programa britânico JANET e o americano NSFNET anunciaram a intenção de patrocinar pesquisadores da área de redes de computadores. Neste mesmo ano, a NSFNET (National Science Foundation Network) reconheceu a necessidade de uma infra-estrutura para redes metropolitanas para dar suporte a comunidade acadêmica e de pesquisadores. Nesta época, começava a ficar evidente que era essencial desenvolver uma estratégia para estabelecer uma infra-estrutura que fosse independente de financiamento federal direto.

A NSF (Nation Science Foundation) encorajou que se buscasse consumidores comerciais e não acadêmicos. Agências federais americanas se comprometeram a dividir os custos de infra-estrutura comum, como por exemplo circuitos transatlânticos. A política de uso da NFS era que nenhum usuário comercial poderia utilizar os recursos do "Backbone", a não ser se estivesse relacionado a algum projeto de pesquisa. Tal política levou ao surgimento e crescimento de redes privadas, como a PSI, UUNet e outros. Neste momento, começavam a surgir os provedores de acesso à Internet.

O Backbone da NSFNET foi oficialmente terminado em abril de 1995. Nessa época, os financiamentos foram voltados para a contratação de acesso à Internet junto a diversas redes privadas de longa distância. O Backbone agora não era constituído de roteadores desenvolvidos por pesquisadores, e sim equipamentos comerciais. Em menos de dez anos, o Backbone cresceu de seis nós com enlaces de

56Kbps para vinte e um nós com múltiplos enlaces de 45Mbps. A Internet havia crescido para mais de 50.000 redes em todos os continentes. No dia 24 de outubro de 1995, a FNC (Federal Networking Council) definiu o termo Internet. A definição segue abaixo:

O Federal Networking Council (FNC) concorda que a seguinte linguagem reflete a nossa definição do termo "Internet". "Internet" refere-se ao sistema global de informação que - (i) está ligado logicamente por um sistema único de endereçamento baseado no Protocolo Internet (IP) ou as suas futuras extensões/continuações; (ii) é capaz de suportar comunicações usando o Protocolo de Controlo e Transmissão/Protocolo Internet (TCP/IP) ou as suas futuras extensões/continuações, e/ou outros protocolos compatíveis com o IP; e (iii) providenciar, usar ou tornar acessível, de forma pública ou privada, serviços de alto nível baseados nas comunicações e infra-estruturas descritas aqui [8].

A Internet mudou muito desde o seu surgimento. Apesar de ter sido concebida em uma era de sistema de tempo compartilhado, ela conseguiu sobreviver na era dos computadores pessoais, de aplicações cliente-servidor e *peer-to-peer*. Ela foi desenvolvida antes do surgimento das redes locais (LANs), mas no entanto acomodou diferentes tecnologias como LAN, ATM, frame-relay e, mais recentemente, redes sem fio. Ela foi prevista para suportar diferentes funções, desde compartilhamento de arquivos e *logins* remotos até compartilhamento de recursos, e acabou absorvendo diversas outras funcionalidades tais como: o correio eletrônico, a *web* e, mais recentemente, o tráfego de voz e vídeo. A Internet começou com a criação de uma pequena equipe de pesquisadores e acabou se tornando um sucesso comercial com bilhões de dólares anuais de investimento.

A Internet de hoje consiste em milhares de redes, interligadas por múltiplas redes de "Backbone", pertencentes a grandes empresas de telecomunicação. O fornecimento de serviços na Internet é um novo e desafiante mercado. No entanto, o acesso básico se tornou uma mercadoria sem diferenciações óbvias, surgindo uma grande pressão nos preços. O mercado da Internet é um dos mais agressivos que existe. Este ambiente de competição fez com que os preços caíssem de tal forma que

em março de 1998 o *Finantial Times* relatou que das vinte e cinco maiores empresas de acesso à Internet, que juntas valiam cerca de 37 bilhões de dólares, vinte ainda estavam com déficit operacional.

1.4 Desafios

Em um mercado de competição tão feroz, um provedor tem diversos desafios para vencer. Esses desafios não estão relacionados somente ao plano de negócios e investimentos financeiros, mas também a avanços tecnológicos. A Internet não atende mais somente a uma pequena comunidade científica, mas também a aplicações comerciais críticas, que dependem constantemente dela para suas atividade. Confiabilidade e desempenho são dois diferenciais importantes entre provedores de acesso.

No entanto, o desempenho experimentado por um usuário não depende somente da rede que ele se conecta, mas também das redes que necessitam ser acessadas até que o destino seja alcançado. Por esta razão, os provedores expandem suas redes com intuito de aumentar sua conectividade para diversos destinos.

Os atuais contratos feitos pelos provedores possuem métricas para medir o desempenho do circuito contratado. As principais são o retardo fim-a-fim e a perda de pacotes. Essas métricas fazem parte do Acordo de Nível de Serviço (*Service Level Agreement (SLA)*). A alta competição existente vem fazendo com que esses valores se tornem cada vez menores, causando um aumento do investimento necessário para atender tais demandas.

Um Backbone IP consiste de centenas de nós e milhares de enlaces. Interações complicadas são realizadas para fazer o roteamento de pacotes entre os domínios internos e externos, tornando o gerenciamento de um Backbone uma tarefa difícil. A permanente necessidade de se melhorar o SLA, juntamente com o complexo ambiente de um Backbone, torna necessário uma melhor compreensão do tráfego que o atravessa, assim como do comportamento da rede.

1.5 Contribuições e Objetivos Deste Trabalho

Atualmente, um operador de rede dispõe de pouca informação a respeito do tráfego que atravessa sua rede e, na maioria das vezes, estas informações se resumem a contadores de pacotes e bytes e ao estado dos enlaces. Muitas vezes, a solução de problemas de uma rede pode ser uma tarefa difícil, dada a pequena quantidade de informação disponível e o fato de que os protocolos de roteamento foram projetados para automaticamente se ajustar às condições existentes.

Para se projetar uma rede de forma eficiente e aplicar melhores práticas de gerenciamento, medições adicionais do tráfego são imprescindíveis. A teoria tradicional de redes de comunicação assume a existência do que é denominada "matriz de tráfego", que denota a quantidade de tráfego fluindo de qualquer origem para qualquer destino. Uma rede IP não foi projetada para prover tal nível de detalhe de informação, e dado o atual tamanho dos backbones, mesmo uma estimativa deste tipo é algo desafiador.

Uma importante técnica utilizada para a caracterização do tráfego é a medição dos fluxos de comunicação (conjunto de pacotes que possuem características semelhantes, tais como número da porta e endereço IP de origem e destino). Ao estudá-los, três variáveis devem ser analisadas: tamanho, duração e taxa. Além disso, é importante poder separá-los em classes que diferenciem os fluxos grandes, pequenos e intermediários.

Estudos recentes mostram que uma porção muito pequena dos fluxos é responsável pela grande maioria do tráfego total (em bytes) nas redes. É importante compreender as propriedades deste tráfego para propósitos de modelagem e monitoração. Estudando esses fluxos, pode-se compreender uma grande porção do tráfego total, possibilitando a tarifação baseada no uso, detecção de ataques e outras ações de interesse. Apesar de ser uma preocupação recente, o estudo da caracterização dos fluxos vem crescendo em importância. No entanto, de uma forma geral, não é claro como as diferentes variáveis dos fluxos estão relacionadas, assim como não existe uma metodologia eficaz, capaz de separá-los em diferentes classes. Por exemplo,

qual é a relação entre fluxos de grande tamanho e os de longa duração? Ou ainda, como se pode dizer se um fluxo é de longa ou pequena duração? As correlações envolvendo características deste tipo de fluxo não são ainda bem conhecidas, e as aplicações deste conhecimento podem ser diversas.

Esta dissertação propõe uma metodologia que permite uma melhor compreensão do tráfego de rede em grandes backbones, compostos de centenas de nós e enlaces. O trabalho mostra como informações adicionais podem aperfeiçoar as atuais técnicas de planejamento e gerenciamento. Utilizando-se das distribuições cumulativas e das freqüências relativas dos tamanhos, durações e taxas, o método proposto divide os fluxos em N classes, indicando seus comportamentos e impactos no tráfego de rede. No intuito de se melhor compreender como os diferentes tipos de tráfegos estão relacionados e as causas de seu comportamento, a metodologia proposta também faz um estudo da correlação das diferentes classes e variáveis.

Diversos métodos de classificação e caracterização de tráfego já foram propostas na literatura. A forma mais comum de se classificar os fluxos é dividí-los em duas classes em função de seus tamanhos. A classe formada por fluxos de tamanho muito grande é chamada elefante, e aquela formada por fluxos pequenos é chamada rato. [9] propos um valor fixo como sendo o limite entre as duas classes, ou seja, se o fluxo for maior que xKB, ele é considerado elefante. Caso contrário, é considerado rato. Uma forma alternativa para classificação [10] estabelece uma fração l de toda capacidade do enlace, sendo que os fluxos grandes serão os maiores responsáveis pela fração l da utilização do enlace. Outra forma simples de classificação estabelece que os fluxos pesados serão os N maiores. Ambas as formas possuem o problema de estabelecer os valores de l e de N, pois não há um método para se obter estes valores. Os valores escolhidos foram arbitrários, ou seja, foram escolhidos sem utilizar algum método, o que pode levar ao questionamento dos valores escolhidos. Em uma tentativa de resolver os problemas citados os trabalhos [11, 12] propuseram uma classificação baseada na média e no desvio padrão, e propõe uma classificação para as taxas dos fluxos, além das variáveis tamanho e duração, sendo os fluxos de alta taxa chamados de chitá. Esta classificação no entanto, ainda classifica os fluxos em apenas duas classes, ou seja, os fluxos intermediários não podem ser identificados

adequadamente. Em uma tentativa de resolver todos os problemas citados [13] propõe uma classificação baseada em fundamentos estatísticos, utilizando testes de hipóteses, mas a necessidade de analisar cada fluxo ao longo de toda sua duração fez com que o processamento e o espaço de armazenamento das informações requeridos sejam proibitivos.

Apesar das diversas propostas apresentadas, de acordo com o nosso conhecimento, não existe uma metodologia que possa ser aplicada em backbones IP, e que ainda possibilite a classificação dos fluxos de comunicação em N classes e indique como eles estão relacionados. A diferenciação em mais de duas classes é importante para que não se perca o comportamento dos fluxos intermediários.

No intuito de validar a metodologia proposta, medições do tráfego de rede foram feitas na Rede Rio, que é uma rede integrada por universidades e centros de pesquisa localizados no Estado do Rio de Janeiro. Os resultados obtidos estão baseados na medição de centenas de milhões de fluxos de comunicação coletados ao longo de dois meses, o que permitiu fazer uma análise acurada do comportamento dos fluxos. Os resultados obtidos neste trabalho envolvem, entre outras coisas, comparações com outros modelos propostos e o estudo de possíveis causas para os fluxos de longa duração. Eles mostram que as variáveis tamanho e taxa possuem alto coeficiente de correlação, além de indicar que o comportamento dos fluxos considerados grandes sugere a necessidade de modificações nas atuais infra-estruturas de redes.

1.6 Organização do Trabalho

Esta tese está organizada da seguinte forma: o capítulo 2 apresenta os conhecimentos básicos necessários para o entendimento do trabalho, enquanto o capítulo 3 faz uma detalhada descrição dos trabalhos relacionados. No capítulo 4, uma metodologia para classificação de tráfego é proposta, e um estudo de caso envolvendo a Rede Rio é feito no capítulo 5. Finalmente, no capítulo 6, a conclusão é apresentada e trabalhos futuros são propostos.

Capítulo 2

Fundamentos Básicos

NESTA seção serão abordados os fundamentos básicos necessários para a compreensão do trabalho. Inicialmente, será feita uma breve descrição dos aspectos de estatística utilizados e, posteriormente, alguns conceitos importantes sobre caracterização de tráfego.

2.1 Roteamento Hierárquico da Internet

A Internet é uma coleção de redes que trocam tráfego usando o protocolo IP [14]. Cada uma destas redes possui um conjunto de endereços IP, representados pelo par endereço e máscara de rede. Este par é chamado prefixo de rede, e é geralmente representado como prefixo/tamanho, onde "prefixo" representa o endereço de rede e o "tamanho" indica o número de bits que corresponde à máscara de rede associada àquela rede.

Grandes corporações ou provedores de acesso à Internet comumente possuem mais de um prefixo de rede, formando um Sistema Autônomo (*Autonomous System* - AS). De uma maneira mais formal, um sistema autônomo é definido como um conjunto de roteadores que possuem uma única política de roteamento, e operam sob uma única administração. Desta forma, grandes redes IP são normalmente vistas na Internet como uma única entidade denotada por um identificador único,

chamado de número do AS.

A Internet global é formada por uma inter-conexão de diferentes sistemas autônomos, trocando informações confiáveis usando protocolos de roteamento entre domínios (ex. BGP). A hierarquia de roteamento da Internet é formada pela relação comercial entre diferentes ASs, onde cada nível de interconexão é geralmente descrita como um *Tier*. De acordo com esta hierarquia, entidades de níveis mais altos (n-1) provêem serviços para as entidades abaixo (n) conectadas diretamente a eles [15]. O que consiste uma rede *Tier-1* (nível mais alto) é algo mais complicado, mas a definição mais popular é que as redes de um provedor *Tier-1* são aquelas que têm acesso a tabela de roteamento global da Internet. O segundo *tier* geralmente possui uma presença nacional menor e pode alugar parte ou toda sua rede de um *Tier-1*.

Nesta tese, o interesse é voltado para redes de provedores *Tier-1*, também chamadas de redes "Backbone".

2.2 Medição de Tráfego

O tráfego de rede tem sido analisado desde o desenvolvimento da ARPANET. Medições feitas em redes operacionais proporcionam informações úteis sobre desempenho e características do tráfego que passa por elas. Os sistemas de medição podem ser classificados em duas categorias: ativa e passiva. Sistemas de medição passiva observam o tráfego passando pelos pontos selecionados dentro da rede. Análises dos dados coletados possibilitam saber a utilização e características do tráfego do enlace. Este método é não-intrusivo, ou seja, a coleta de dados não afeta de forma significativa o tráfego que passa pela rede. Medições ativas, por outro lado, injetam tráfego na rede e medem o seu desempenho baseado no que foi injetado. Tais tipos de medição são consideradas intrusivos, uma vez que o tráfego gerado influencia a operação da rede e, consequentemente, as próprias medições. Sendo assim, se uma medição ativa quiser medir o comportamento de filas no roteador, os próprios pacotes gerados pela medição irão alterar o comportamento da fila. Desta forma, medições ativas devem ser feitas com cuidado, e os resultados analisados devem levar

em consideração os efeitos do tráfego gerado.

2.2.1 Medição Ativa

Alguns exemplos de ferramentas de medição ativa são o *Ping*, *Traceroute* e *Pathchar* [16]. O *Ping* fornece o tempo de ida e volta de um pacote entre a origem e o destino, o *Traceroute* indica quais são os nós que um pacote passa até atingir seu destino, assim como o tempo de ida e volta, e o *Pathchar* a mede utilização da banda, retardo, tamanho médio da fila e taxa de perda para cada nó intermediário. Outras ferramentas que podem ser utilizadas para medições ativas são: *pchar* [17], *bprobe* [18], *nettmer* [19] e *pathrate* [20].

Uma grande desvantagem das medições ativas é o fato de que somente um número limitado de estatísticas podem ser observadas em um determinado momento. Outro fator importante é a impossibilidade de analisar tráfegos de um período no passado. Em outras palavras, não é possível analisar dados anteriores e identificar a razão pela qual certas métricas apresentam determinado tipo de comportamento. Finalmente, a impossibilidade de se controlar o caminho seguido pelos pacotes IP torna a interpretação dos dados coletados uma tarefa difícil.

Alguns esforços no intuito de se criar padrões para métricas de desempenho e técnicas de medições ativas estão sendo feitos pelo grupo de trabalho IPPM (Internet Protocol Performance Metrics) do IETF (Internet Engineering Task Force). Alguns padrões já propostos incluem métricas para conectividade [21], retardo *one-way* [22], perda de pacotes [23] e tempo de ida e volta [24].

2.2.2 Medição Passiva

As medições passivas são aquelas que não utilizam nenhum recurso da rede e não introduzem nenhuma perturbação no funcionamento normal da rede. Estas medições geralmente dependem da existência de equipamentos de monitoração em partes específicas da rede. No entanto, medições passivas podem ser coletadas por

elementos pertencentes a infra-estrutura da rede, que suportem as funções necessárias. O SNMP é um protocolo que permite medições passivas de algumas métricas específicas coletadas nas interfaces de roteadores/switches (estas métricas são geralmente bytes enviados/recebidos, perda de pacotes e erros). Seguindo a mesma linha, existem alguns produtos que possibilitam outras informações do tráfego de rede. Um exemplo é o Netflow, ferramenta de medição passiva desenvolvida pela Cisco. Ele coleta informações sobre todos os fluxos TCP e UDP dos enlaces de um roteador. Uma explicação mais detalhada desta ferramenta é feita na seção 2.4.1.

2.3 Tráfego Auto-Similar

As análises de tráfego utilizando a teoria de filas foi de grande importância para os projetistas de redes e analistas de sistemas, pois através dela é possível fazer planejamento de capacidade e de desempenho. No entanto, ao se analisar o tráfego real da rede, muitos dos resultados previstos diferem dos observados. A principal causa desta diferença se deve ao fato dos modelos assumirem que o tráfego tem características da distribuição de Poisson. No entanto, estudos feitos nos últimos anos [25, 26, 27, 28] vêm indicando que o tráfego de rede em determinados tipos de ambientes tem características de tráfego auto-similar.

A principal característica de um fenômeno auto-similar é que seu comportamento parece o mesmo para diferentes graus de magnitude ou diferentes escalas em uma dimensão. A dimensão pode ser espaço (tamanho, comprimento) ou tempo. Um exemplo de tal característica para o tráfego de rede seria um comportamento de rajada para qualquer escala de tempo utilizada, enquanto o comportamento de um tráfego não auto-similar tende a se estabilizar e não apresentar rajadas após um longo período de tempo. A Figura 2.1 mostra a diferença entre o comportamento de um tráfego auto-similar (a esquerda) em diferentes escalas de tempo e um tráfego Poisson (a direita).

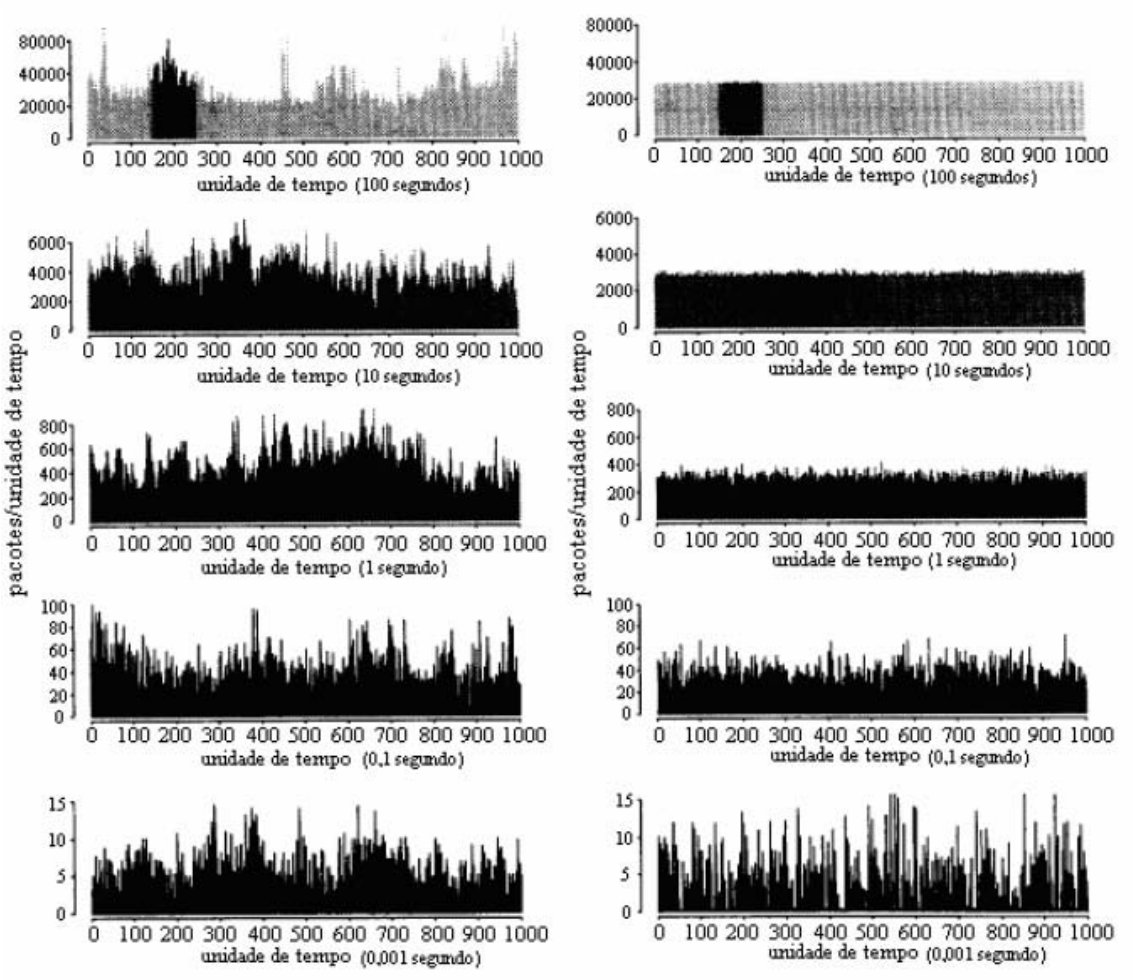


Figura 2.1: Comparação entre um tráfego Auto-Similar e um tráfego Poissoniano (retirado de [25]).

2.4 Fluxos de Comunicação

Um fluxo pode ser definido como um tráfego unidirecional identificado por pacotes que contenham a mesma porta de origem e destinho, mesmo IP de origem e destinho e mesmo protocolo. Qualquer fluxo não contendo pacotes em um período em segundos pré-configurado (o parâmentro *timeout* tem como configuração padrão 64 segundos) é considerado terminado. Um fluxo no qual um pacote foi examinado no último segundo é considerado um fluxo conhecido.

2.4.1 Netflow

Muitos roteadores e switches suportam serviços NetFlow que provêem uma fonte detalhada de dados sobre o tráfego de rede. Os logs são utilizados para planejamento da rede, monitoração de performance, cobrança a partir do uso, e muitos outros temas relacionados a segurança (incluindo detecção de intrusão).

Um registro no NetFlow é criado quando o tráfego é visto primeiramente por um roteador Cisco ou *switch* que é configurado para utilizar os serviços do NetFlow. Os Fluxos são identificados unicamente pelas características do tráfego que eles representam.

As principais vantagens da utilização do Netflow são as seguintes:

- Sua utilização funciona como cache para acelerar os *lookups* nas tabelas de roteamento.
- Com o NetFlow não é necessário verificar as tabelas de *access-list* (apenas de entrada) toda vez que um pacote chega, tornando mais eficiente o processo de roteamento.
- É possível a exportação das informações de fluxo utilizadas pelo cache do NetFlow. Isto facilita a coleta de dados para futuras análises sem a necessidade de colocar um analisador em cada enlace.

Para que o NetFlow funcione em um roteador, é necessário que sua versão do sistema operacional (chamada de IOS) seja compatível [29]. Nos roteadores Cisco, não existe um comando geral que habilite a ferramenta para todas as interfaces, tornando necessária a habilitação individual por interface através do comando `route-cache flow`.

Para o NetFlow o fluxo é definido como sendo um conjunto de 5 variáveis: O campo `Protocol Type`, IP origem, IP destino, Porta origem e Porta destino. Além destas 5 variáveis, as tabelas do NetFlow guardam a interface destino e a interface origem relativa ao trânsito do pacote IP.

Para cada pacote IP que entra na interface, o NetFlow identifica o seu fluxo e verifica se já existe uma entrada do mesmo na tabela de cache. Se existir, ele comuta diretamente para a interface destino especificada. Caso contrário, ele então realiza um *lookup* nas tabelas de roteamento e nas tabelas de *access-list*. Se este pacote possuir alguma restrição nas tabelas de *access-list* ou se o seu IP destino não for achado nas tabelas de roteamento, o pacote então será enviado para a interface `NULL` (um pacote com o destino para interface `NULL` identifica que ele foi descartado). O Netflow também cria uma entrada na sua tabela de cache para o destino `NULL`.

Outra característica importante do NetFlow é o processo de exportação dos dados, conhecido como *flow-export*. O *flow-export* é feito através do envio de dados encapsulados em pacotes UDP. Seu destino é o IP do coletor configurado previamente no roteador. O conteúdo do pacote UDP dependerá da versão em que o NetFlow estiver funcionando. Atualmente, o roteador pode exportar os fluxos criados pelo NetFlow nas versões de 1 a 8. O momento no qual o roteador começa a exportar os dados de fluxo dependerá da configuração, mas geralmente coincide com o instante em que a informação é expirada. Isso acontece assim que sua entrada na tabela do NetFlow é removida. A remoção da tabela do NetFlow pode ocorrer por vários fatores:

- O tamanho da tabela do NetFlow chegou ao limite previamente configurado.
- Não existe mais nenhum tráfego de pacotes no fluxo criado na tabela do Netflow por um certo período de tempo, conhecido como *flowtime-out*.
- Conexões TCP que tenham enviado uma mensagem de finalização (FIN) ou tenham enviado uma mensagem de *reset* (RST).

Através da medida do fluxo de comunicação dos pacotes IP é possível obter uma série de informações úteis, tais como:

- Uma vez de posse do fluxo de dados, é possível escolher um melhor ponto de conexão. Por exemplo, no caso da maioria dos pacotes estarem vindo de uma

rede ASx, e a conexão existente estar em ASy, é mais adequado trocar o ponto de conexão para ASx.

- Através da quantidade de dados e de pacotes dos fluxo é possível ter uma estimativa da aplicação utilizada.
- Ataques que utilizam IPs de origem diferentes do original (IP Spoofing) podem ser detectados através da análise dos fluxos medidos.
- Atualizando as flags do cabeçalho do protocolo TCP é possível detectar ataques do tipo DDoS (Distributed Denial of Services).
- É possível detectar falhas nos filtros de roteamento.

Os seguintes campos podem ser utilizados para identificar um fluxo: TOS, IP flags, TCP flags, AS origem, AS destino, IP origem, IP destino, Porta origem, Porta destino, Rede IP origem (com a máscara), Rede IP destino (com a máscara), Protocolo de transporte e Protocolo de rede. Esses campos podem ser relacionados de forma a definir um fluxo de dados, e inúmeras combinações podem ser feitas. A Figura 2.2 mostra os principais tipos de fluxos utilizados em Backbones Internet.

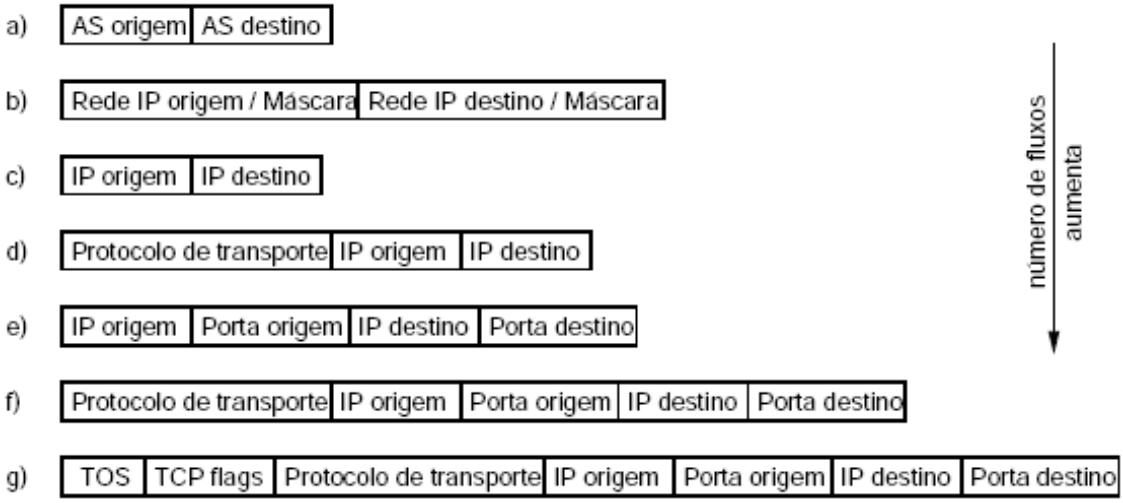


Figura 2.2: Fluxos de comunicação mais comuns

2.4.2 Classificação dos Fluxos

No intuito de tornar o gerenciamento de um grande volume de fluxos relativamente simples, é interessante classificá-los em um pequeno número de classes. A classificação dos fluxos ocorre geralmente em relação ao tamanho, duração e taxa. Estas variáveis são então divididas em classes que representam intervalos de valores que elas podem receber. Por exemplo, se fossem utilizadas apenas duas classes, fluxos de tamanho muito pequeno seriam classificados como pertencentes à classe 1, enquanto os fluxos de grande tamanho pertenceriam à classe 2. Desta forma, pode-se analisar melhor o perfil do tráfego de rede, conhecendo o comportamento de cada classe.

Capítulo 3

Estado da Arte

NESTE capítulo serão apresentados diversos trabalhos sobre medição e caracterização de tráfego. A análise desses trabalhos nos permite entender o estado da arte das pesquisas sobre engenharia de tráfego.

3.1 Caracterização de Tráfego

O grande crescimento das redes de computadores, em particular da Internet, tornou de grande importância o melhor conhecimento das características do tráfego de rede. Em [30] é chamada a atenção para necessidade de uma melhor compreensão das redes de computadores. O trabalho mostra que o crescimento do tráfego ocorreu de forma muito mais rápida do que as pesquisas sobre seu comportamento. Muitas vezes, a necessidade de atendimento às requisições de clientes levava os provedores a aumentarem a vazão de seus enlaces, sem o devido monitoramento do tráfego que passava pelos Backbones. Neste contexto, o trabalho propôs metodologias e formas de monitoração e caracterização de tráfego que possibilitassem uma maior refinação dos dados coletados e, desta forma, a obteção de um maior nível de detalhamento das características do tráfego. O trabalho utilizou medições no Backbone da NSFNET para analisar o comportamento de algumas métricas, como o crescimento do tráfego no Backbone ao longo do tempo, as aplicações que eram responsáveis pela maior

porção do tráfego, número de endereços IP utilizados ao longo do tempo, assim como os usuários responsáveis pela maior utilização dos enlaces.

No intuito de ampliar a visão sobre métricas de desempenho que um Backbone deve possuir, [31] propõe uma metodologia para caracterização de tráfego em backbones IP. O trabalho descreve variáveis importantes que devem ser levadas em consideração ao se medir o desempenho, tais como o retardo fim-a-fim, vazão e perdas de pacotes. Com a utilização de ferramentas desenvolvidas e de código aberto, o trabalho mostra resultados de medições feitas na Rede Rio e na Embratel sobre o comportamento da tabela BGP, crescimento do número de prefixos de rede ao longo do tempo, comportamento da vazão, retardo, retransmissão e fragmentação de pacotes.

O artigo [25] faz um estudo sobre a natureza do tráfego Ethernet. Apesar de alguns outros artigos anteriores discutirem o comportamento do tráfego de rede, este trabalho foi o primeiro a introduzir a noção do tráfego auto-similar. O artigo mostra que a utilização do modelo de Poisson para fazer análises de filas não era adequado para o tráfego da rede Ethernet. O trabalho, através de medições feitas entre 1989 e 1992 nos enlaces da Bellcore, sugere que um novo modelo de análise de tráfego deve ser feito para redes Ethernet. Uma das principais conclusões obtidas diz respeito às implicações na análise de desempenho de tráfegos com característica auto-similar. O artigo mostra que quanto maior a utilização de uma rede Ethernet maior o grau de auto-similaridade. Tal resultado é importante uma vez que é justamente em alta utilização que questões de desempenho se tornam mais relevantes.

Diversos outros trabalhos foram e vêm sendo realizados no intuito de conhecer melhor as características do tráfego que passa pela rede e estudar questões específicas como roteamento [32], comportamento dos pacotes [33] e tipos de tráfego da Internet [34].

É possível notar que a caracterização de tráfego é uma questão ampla e complexa, que envolve diferentes variáveis e métricas, dependendo do que se deseja estudar. Este trabalho tem como objetivo contribuir para o melhor entendimento de como os fluxos de comunicação se comportam no tráfego de backbones. Nas seções seguintes,

será feito um detalhamento sobre o estado da arte dos estudos que vêm sendo feitos sobre os fluxos de comunicação.

3.2 Classificação dos Fluxos

A Internet permite que informações sejam compartilhadas entre milhões de computadores ao redor do mundo. Os usuários enviam pacotes de informação de uma máquina para outra usando diferentes protocolos. Pode-se citar como exemplo o TCP e o UDP como sendo os protocolos dominantes, responsáveis por mais de 95% do tráfego, apesar de novos protocolos estarem começando a surgir.

Qualquer enlace da Internet sempre possui fluxos pertencentes a diversos tipos de aplicações, transportados por diferentes tipos de protocolos. O protocolo UDP não é confiável, isto é, uma aplicação que envia pacotes UDP não recebe uma confirmação se o pacote chegou ao seu destino corretamente. O UDP, desta forma, não está preocupado se a rede está congestionada e continua enviando os pacotes, muitas vezes em altas taxas. O protocolo TCP, por outro lado, não só provê uma conexão confiável, como utiliza as respostas recebidas das máquinas de destino para controlar sua taxa de envio, através de seu algoritmo de controle de congestionamento.

Análises e simulações feitas do protocolo TCP focam em seu comportamento no estado estacionário, utilizando "fontes infinitas" (ex. transferências de grandes arquivos), e assumem que um grande volume de fluxos grandes TCP (fluxos elefantes) não seria afetado de forma significativa pela presença de fluxos pequenos (fluxos ratos). A principal diferença entre estes dois tipos de fluxos é que, no caso dos fluxos elefantes, o algoritmo do TCP consegue, através de seu controle de congestionamento, ajustar as taxas de transmissão. No entanto, fluxos muito pequenos não sofrem controle, uma vez que eles são enviados por inteiro, antes que o algoritmo de congestionamento possa ser acionado. Em virtude deste problema, [35] propôs a utilização de roteadores "sensitivos a carga" que utilizariam rotas diferentes para fluxos elefantes e ratos, melhorando assim o desempenho dos enlaces.

Alguns estudos vêm sendo feitos para se conhecer melhor o comportamento dos

fluxos. Joo *et al* [36] fez uma análise dos fluxos TCP e constatou que, apesar dos fluxos elefantes serem responsáveis pelo maior volume de bytes na rede, o número de fluxos muito pequenos (ratos) é muito maior, podendo causar perdas de pacotes no enlace.

Ao se falar em fluxo muito grande ou muito pequeno, uma pergunta importante deve ser respondida: o que deve ser considerado para se classificar um fluxo como muito grande ou muito pequeno? [9] propõe um valor fixo como sendo o limite entre as duas classes. Ou seja, se o fluxo for maior que x KB, ele é considerado elefante; caso contrário, ele é considerado rato. No trabalho em questão, fluxos menores que 20KB foram considerados como rato. O artigo também propõe uma classificação para fluxos de longa duração (tartaruga), pequena duração (libélula) e uma categoria intermediária, estabelecendo um limiar de 2s para fluxos libélula, até 15 minutos para fluxos de duração intermediária, e maior que 15 minutos para fluxos tartaruga.

Uma forma alternativa para classificação [10] estabelece uma fração l de toda capacidade do enlace, sendo que os fluxos grandes serão os maiores responsáveis pela fração l da utilização do enlace. Outra forma simples de classificação estabelece que os fluxos pesados serão os N maiores. Ambas as formas possuem o problema de estabelecer os valores de l e de N, pois não há um método para se obter estes valores.

A forma de classificação proposta em [9] possui algumas limitações. Os valores foram escolhidos arbitrariamente sem o auxílio de algum método, o que pode levar ao questionamento dos mesmos (por que 15 minutos e não 14?, por exemplo). Outra colocação importante é o fato do tráfego de rede poder apresentar comportamentos diferentes de uma rede para outra, ou seja, o parâmetro escolhido como limiar em uma determinada rede pode não ser adequado em outra. Além disso, a classificação dos fluxos em apenas 2 conjuntos também deve ser evitada, uma vez que as informações sobre fluxos de tamanhos intermediários são perdidas.

Uma tentativa de resolver dois dos problemas citados acima foi proposta nos trabalhos [11, 12], que se baseiam na média e no desvio padrão para classificar as

taxas dos fluxos, seus tamanhos e suas durações. Desta forma os fluxos seriam classificados da seguinte forma:

Tamanho: Fluxos de grande tamanho ("elephant" ou elefante) contêm mais que x KB, enquanto fluxos de tamanho pequeno ("mouse" ou rato) contêm menos que x KB. A variável x é definida como $x = \mu + 3\sigma$, onde μ é a média da variável a ser medida (no caso o tamanho) e σ é a variância de todos os fluxos medidos.

Duração: Fluxos de longa duração ("tortoise" ou tartaruga) são aqueles que duram mais que y minutos, e de curta duração ("dragonfly" ou libélula) aqueles que duram menos que y minutos. A variável y é definida como $y = \mu + 3\sigma$.

Taxa: Fluxos de alta taxa ("cheetahs" ou chitá) são aqueles com taxa maior que z KB/s, e fluxos de baixa taxa ("snails" ou lesma) aqueles com taxa menor que z KB/s. A variável s é definida como $z = \mu + 3\sigma$.

Esta classificação resolve o problema da arbitrariedade e da diversidade das redes. No entanto, ela ainda classifica os fluxos em apenas duas classes. Outro problema importante se deve ao fato de que o tráfego de rede muitas vezes apresenta grandes disparidades (ver seção 3.3), resultando em um comportamento de cauda pesada [34, 37]. Nestes casos, o uso da média e desvio padrão não é adequado, pois os valores destas quantidades podem tender para o infinito (ver seção A.9).

Em uma tentativa de resolver todos os problemas citados acima, [13] propõe uma classificação baseada em fundamentos estatísticos, utilizando testes de hipóteses. A metodologia utilizada analisa o comportamento de um fluxo ao longo do tempo e realiza testes para verificar em qual classe (de um total de n possíveis) a sua distribuição melhor se encaixa. Apesar do método resolver os problemas mencionados anteriormente, ele possui uma grave limitação, pois não consegue analisar grandes quantidades de fluxos (ex. todos os fluxos de um Backbone). A necessidade de analisar cada fluxo ao longo de toda sua duração faz com que o processamento e o espaço de armazenamento das informações sejam proibitivos.

3.3 Diversidade e Disparidade dos Fluxos

Trabalhos recentes de análise de fluxos vêm chamando a atenção para comportamentos de diversidade e disparidade, ou seja, o fato de que a relação entre o número de fluxos e seus tamanhos não é trivial e muitas vezes apresenta uma distribuição de cauda pesada. Pode-se citar como exemplo o fato da arquitetura da Internet ser bastante diversa e dificilmente apresentar pontos com falha. No entanto, cerca de 80-90% das rotas dos pacotes que nela trafegam utilizam cerca de apenas 20 provedores. De forma similar, [38] observou que apenas cerca de 80 ASs (*Autonomous Systems*), entre milhares observados, contribuíam para 95% do tráfego nos enlaces.

Trabalhos analisando o comportamento do tamanho, duração e taxa dos fluxos também mostram que há uma grande diversidade e disparidade entre diferentes classes de fluxos. Essa diversidade pode ser definida como a presença de um grande número de fluxos distintos, enquanto a disparidade é a concentração de tamanho (volume) em um pequeno número de fluxos.

Em [9], foi observado que cerca de 98% dos fluxos possuem duração igual ou inferior a 15 minutos. No entanto, os 2% restantes são responsáveis por cerca de 60% dos bytes trafegados. Zhang *et al* [39] mostra que o tráfego medido é dominado por fluxos de pequeno tamanho, enquanto os fluxos grandes são os maiores responsáveis pelo tráfego em bytes. [12] mostra que 36% dos fluxos de alta taxa correspondem a 2% do tráfego em bytes. Resultados semelhantes foram encontrados em [11], onde os fluxos considerados elefantes representavam 0,071% e seu volume em bytes 62%. O trabalho mostra também que os fluxos tartaruga (0,35%) foram responsáveis por 63% do tráfego em bytes. Nem a diversidade quanto a disparidade devem ser consideradas boas ou ruins. Por outro lado, o impacto imposto por estes tipos de comportamento deve ser analisado.

3.4 Volatilidade dos Fluxos

Alguns trabalhos recentes vêm analisando o comportamento dos fluxos ao longo do tempo. Estes trabalhos verificaram que os fluxos podem mudar de taxa no decorrer de sua existência e assim apresentar grande volume durante certo intervalo de tempo e pequeno volume em outro intervalo. O trabalho [40] mostra que após 25 minutos, 40% do tráfego de grande volume (elefante) deixa de apresentar este comportamento.

O artigo [10] faz um estudo sobre o impacto da volatilidade nos métodos de classificação existentes e propõe uma nova metodologia. Esse estudo mostra que a volatilidade existiu em todas as medições feitas e somente alguns "heavy-flows" e "light-flows" não apresentaram esse comportamento (permaneceram "pesados" ou "leves" por muito tempo). Os fluxos que ocupavam um tamanho intermediário da banda foram os que mais variaram de classes. Foi verificado que muitos fluxos apresentaram aspectos transientes de rajada. No entanto, não foram apresentadas possíveis causas para este comportamento. Baseado nas volatilidades verificadas, [10] propõe uma metodologia que analisa os fluxos ao longo do tempo e os divide em duas classes. A cada m minutos, o fluxo é reclassificado, e verifica-se se ele ultrapassou um determinado limiar. Esse limiar é calculado utilizando a metodologia *aest* [41], que indica a porção de um conjunto de dados que exibe o comportamento de uma lei de potência.

A análise da volatilidade dos fluxos pode ser de grande importância para propostas de novos protocolos de roteamento que diferenciem tráfego formado por "elefantes" e "ratos".

3.5 Correlação

Apesar de alguns estudos focarem nas características dos fluxos, poucos esforços estão sendo feitos para se conhecer como estas características interagem, ou seja, como os fluxos estão relacionados entre si. Por exemplo, os fluxos elefantes são em

sua maioria também tartaruga? A resposta para esta questão depende dos enlaces utilizados para transferência de grandes arquivos. Existem várias aplicações para a diferenciação dos tipos de fluxos, como por exemplo, métodos de cobrança que podem se basear no tamanho ou na duração dos fluxos trafegados. O conhecimento destas relações também pode oferecer dados importantes para se diferenciar os tráfegos maliciosos dos benignos.

Entender a natureza das taxas dos fluxos na Internet também é importante por diversas razões. Para compreender o quanto o desempenho de uma aplicação irá melhorar aumentando as taxas de transmissão, deve-se primeiramente saber o que está limitando a taxa de transmissão. Fluxos que são limitados por congestionamento da rede devem ter uma atenção diferente daqueles que são limitados pelo tamanho dos *buffers* das máquinas. Muitos algoritmos de roteamento para controlar a utilização do enlace pelos fluxos foram propostos, e o desempenho e a escabilidade destes algoritmos dependem da natureza das taxas dos fluxos [42, 43]. Desta forma, saber mais sobre as taxas pode auxiliar no desenvolvimento destes algoritmos. Além disso, o conhecimento da natureza das taxas dos fluxos pode ajudar na criação de melhores modelos do tráfego da Internet. Tais modelos podem ser úteis na geração de simulação e no estudo de problemas na rede.

Zhang *et al* [44] mostrou que existe uma forte correlação entre o tamanho dos fluxos e suas taxas. A hipótese formulada para justificar este comportamento refere-se ao fato de que os usuários escolhem o tamanho dos arquivos que vão ser transferidos baseado no tamanho do enlace disponível, isto é, quanto maior o enlace, maior os arquivos transferidos. No entanto, o artigo [12] propõe que este comportamento pode ser melhor explicado pelo algoritmo dos protocolos para fluxos pequenos/médios. Tal informação é importante para indicar que algumas mudanças devem ser feitas nos protocolos, como por exemplo, aumentar o tamanho da janela inicial do TCP no intuito de melhorar seu desempenho.

Resultados encontrados em [12] indicam que o tráfego *web* é responsável pela grande parte dos fluxos elefantes, e que o DNS é o principal responsável pelos tráfegos de longa duração. O artigo mostra também que há uma correlação entre tamanho

e duração.

3.6 Desafios

Requisitos como a alta disponibilidade e adequação a níveis de serviço rigorosos, assim como uma informação limitada sobre monitoração da rede, fazem do gerenciamento de redes uma tarefa difícil. Nesta seção, serão abordados alguns desafios atuais para o gerenciamente de redes IP de grande escala.

3.6.1 Monitoração de Rede

Todos os dias, operações de monitoração do estado da rede são realizadas e, muitas vezes, ações corretivas são necessárias em caso de congestionamento. O protocolo SNMP possibilita uma forma simples de monitoramento de redes, através de checagem periódica de todas entidades da rede para verificar o estado das mesmas. No entando, a informação disponibilizada pelo SNMP é geralmente limitada a quantidade de bytes trafegados e erros ocorridos em uma interface, apresentados geralmente em intervalos de 5 minutos. Desta forma, pequenas rajadas ou quedas na utilização do enlace são difíceis de serem captadas. O SNMP não pode prover informação sobre as razões que levaram a tal comportamento. Neste caso, o operador de rede necessita de dados sobre todos os fluxos que passaram pela rede e informações sobre possíveis interações dos protocolos de roteamento que poderiam resultar no estado atual do enlace.

Como uma conseqüência, diagnósticos obtidos apenas a partir de informações do SNMP são geralmente baseados na intuição que os administradores ganharam no decorrer dos anos no gerenciamento de redes. Esta tarefa é ainda mais difícil com protocolos IP que foram projetados para automaticamente responder ao congestionamento (ex. TCP) e falhas nos enlaces (ex. protocolos de roteamento dinâmicos).

A falta de informações sobre as causas dos eventos que ocorrem na rede faz com que a engenharia de tráfego seja muitas vezes baseada na tentativa e erro. Não

é incomum para os operadores de rede, no evento de um congestionamento nos enlaces, tentarem escoar o tráfego para áreas menos congestionadas, aumentando a prioridade de algumas rotas dentro da rede.

3.6.2 Projeto de Novas Redes

Devido a problemas similares aos apresentados no tópico anterior, o planejamento para redes de grande escala é um processo que, muitas vezes, é baseado na intuição. O projeto de redes tradicionais de telecomunicações é uma área que requer extensa pesquisa e requer o uso de diversas técnicas para o seu planejamento [45, 46]. No entanto, no campo das redes de telecomunicações, existe uma presunção da habilidade de se medir o tráfego entre qualquer origem e destino da rede. A representação da demanda de tráfego é geralmente chamada de matriz de tráfego. O conhecimento da matriz de tráfego e as políticas de roteamento de uma rede podem fornecer dados para um planejamento ótimo para a alocação de recursos da rede.

Técnicas analíticas para o projeto de uma rede são geralmente específicas para o caso de comutação de circuito, onde o tráfego entre dois nós segue um caminho bem definido, e os nós terminais possuem estatísticas necessárias para a geração da matriz de tráfego. Em redes de comutação de pacotes, o tráfego entre dois nós pode seguir diferentes caminhos, e cada pacote no fluxo é roteado de forma independente. Conseqüentemente, o planejamento para redes de comutação de pacotes é geralmente feito através de simulação, e requer uma modelagem acurada e conhecimento da matriz de tráfego. As redes IP não foram projetadas para reter informações detalhadas dos fluxos, o que torna a obtenção dos dados necessários uma tarefa difícil.

A incapacidade de se gerar matrizes de tráfego para redes IP de grande tamanho dificulta a aplicação de técnicas tradicionais de planejamento. Esta é principal razão pela qual as práticas correntes de gerenciamento e planejamento de redes dependem da intuição humana.

3.6.3 Acordo de Nível de Serviço

Os consumidores estão, cada vez mais, requisitando mais garantias de desempenho, confiabilidade, segurança e conectividade de suas redes. Essas garantias são geralmente dadas na forma de Acordo de Nível de Serviço (ANS), onde um provedor assegura ao consumidor o desempenho que ele espera receber. Devido à grande competição no mercado, os atuais níveis de serviço garantem retardos ponto-a-ponto, que se comparam à transmissão de pacotes na rede na velocidade próxima da luz, tempos mínimos de interrupção do serviço e perdas muito próximas de zero.

No entanto, as métricas contratadas são normalmente médias mensais do desempenho total da rede. Em outras palavras, o provedor mede o retardo e perda na rede inteira, e então faz a média de todas medidas coletadas para toda a rede durante o mês. Desta forma, um desempenho pior em alguns enlaces pode ser compensado por desempenhos melhores em outros. Deve-se chamar a atenção para o fato de que o uso de médias diárias não revela o desempenho nos momentos de maior utilização da rede, como no horário de pico. Conseqüentemente, a computação de valores medidos durante a noite e nos finais de semana pode mascarar a performance realmente obtida durante as horas de maior uso.

3.6.4 Novos serviços Sobre as Redes de Dados

A transmissão de voz e vídeo na Internet fez com que novas métricas de desempenho fossem praticadas. Estudos realizados mostram que a voz sobre IP pode ser acomodada em alguns backbones. No entanto, esta afirmação não é verdade para toda Internet [47]. Além disso, no caso de falhas nos enlaces ou roteadores, os serviços de VoIP podem cair a níveis não aceitáveis.

Estes dois fatos impõem que novos projetos de redes sejam pensados. A convergência de protocolos de roteamento e a interrupção de serviços levantam questões que devem ser resolvidas antes que estes tipos de serviço sejam amplamente oferecidos na Internet. Para melhor responder estas questões, medições adicionais do comportamento dos protocolos de roteamento devem ser realizadas.

3.6.5 Variação do Tráfego

O tráfego da Internet é complexo. Estudos realizados mostram que o volume de tráfego da Internet varia muito ao longo do tempo [25]. Somado a este fato, falhas de equipamento ou nos enlaces são eventos inesperados que podem levar a repentinos aumentos no tráfego e congestionamento em certas partes da rede. Dados os rígidos níveis de serviço, um operador deve gerenciar sua rede de tal forma que estes tipos de rajadas sejam acomodados sem nenhum impacto notável no desempenho das redes dos consumidores.

Práticas atuais adotam o uso moderado da utilização do enlace. Esta técnica é geralmente chamada de "*overprovisioning*". Isto significa que o provedor sempre se assegura que existe uma capacidade excessiva disponível na rede, e que os enlaces nunca excedem certos níveis de utilização. Somente sob estas condições um tráfego afetado por uma falha em um enlace pode ser roteado para outras partes da rede, que então pode carregá-lo sem afetar o desempenho recebido pelos usuários. Além disso, somente nestes casos, um enlace pode sustentar aumentos transientes de tráfego, que pode levar a utilização do enlace a 100% em breves períodos de tempo.

Esta técnica de super dimensionamento resolve com sucesso os problemas descritos, mas é uma solução muito custosa. Ela requer um grande investimento em infra-estrutura de rede, que somente é justificável em algumas ocasiões, quando eventos inesperados ocorrem. No entanto, a falta de entendimento sobre o comportamento de rajada e as dificuldades de evitá-lo faz com que o super dimensionamento seja a única solução que pode oferecer um bom desempenho. Sem nenhum conhecimento sobre o que está por trás das falhas que ocorrem nos enlaces, a freqüência, e os efeitos causados nos protocolos de roteamento, os operadores de rede terão que continuar utilizando uma capacidade de redes maior do que a necessária. Evidentemente, medições de rede podem ajudar a responder essa pergunta, identificando se há possibilidades de se resolver os problemas de desempenho de uma forma mais eficiente e menos custosa.

3.6.6 Crescimento da Rede

Outro importante desafio para os provedores é o fato de que as redes dos backbones estão crescendo rapidamente em tamanho, velocidade e escopo. Um importante movimento que está acontecendo é a transformação de diversas redes dispersas em único sistema integrado. Como resultado, as funções de gerenciamento que podiam ser manuseadas por um pequeno grupo de pessoas, baseado na intuição e experimentação, devem ser agora suportadas por um conjunto de ferramentas de engenharia de tráfego que unem informações de configuração e uso de várias redes.

Um Backbone IP consiste de centenas de elementos de rede e milhares de enlaces ativos, alguns carregando tráfegos de Gigabits todo segundo. Interações entre os protocolos de roteamento e os fluxos destas grandes redes são muito difíceis de se conceber. Raramente um operador de rede pode prever de forma acurada os efeitos de uma mudança na configuração do protocolo de roteamento.

3.6.7 Tarifação

As diversas aplicações que as medições do tráfego de rede possuem também podem ser usadas a serviço do usuário. As informações contidas nas medições feitas podem servir como base para a tarifação de serviços. Por exemplo, pode-se tarifar o cliente pela quantidade de bytes trafegados na rede em determinado tempo.

Capítulo 4

Metodologia Proposta para Caracterização de Tráfego

NESSE capítulo será apresentada a metodologia proposta para a classificação dos fluxos. Diversas classificações foram propostas, mas ainda não há um consenso na literatura sobre qual é o melhor procedimento. O intuito da metodologia proposta é utilizar um método que não apresente os problemas apresentados no capítulo 3 e seja funcional, ou seja, aplicável em enlaces de grande porte como em um Backbone IP.

4.1 Classificação dos Fluxos

A metodologia proposta classifica os fluxos em relação a três variáveis: tamanho, duração e taxa. O procedimento utilizado é o mesmo para cada uma das variáveis e possibilita a classificação dos fluxos em N classes, onde N deve ser escolhido de forma que melhor atenda as necessidades de cada rede. É importante ressaltar que não faz parte do escopo deste trabalho indicar qual deve ser o número de classes escolhido para cada rede. A resposta para esta questão não é simplesmente "quanto maior o número melhor". O nível de precisão necessário dependerá do uso que se pretende fazer com a classificação.

Para a aplicação do algoritmo de classificação e caracterização, é necessário que os fluxos sejam coletados e armazenados em um banco de dados contendo as informações para cada fluxo. As informações são: tamanho em bytes, duração em segundos, taxa em bytes/s, porta de origem e porta de destino.

O banco de dados é utilizado para gerar as distribuições dos fluxos e suas freqüências relativas segundo seus tamanhos, durações e taxas. A função de distribuição de uma variável pode ser definida como:

$$F_X(x) = P\{X \leq x\}. \tag{4.1}$$

A função densidade é definida como:

$$f_X(x) = \frac{dF_X(x)}{dx}. \tag{4.2}$$

Baseado nestas duas funções, é possível iniciar o algoritmo de classificação dos fluxos em N classes. Uma vez escolhido o valor de N, deve-se determinar o valor do fator de corte, que será chamado de C. O fator de corte é definido como:

$$C = \frac{1}{N} \sum_{i=1}^{i=X_f} x_i * p_x, \tag{4.3}$$

onde p_x indica a probabilidade da variável aleatória X possuir o valor x, lembrando que neste caso existem três variáveis aleatórias: tamanho, duração e taxa e X_f é o número de amostras. Portanto, todos estes passos devem ser seguidos para cada uma das variáveis.

O fator de corte C tem como objetivo conhecer a contribuição que cada classe tem na média, desta forma, cada classe será responsável por uma porção (de mesmo valor) da mesma. A separação entre as classes utilizando percentis não foi utilizada pois não levava em conta o valor do fluxo, apenas a quantidade de ocorrencias. O processo de separação das diferentes classes deve levar em consideração o valor do fluxo, pois este fator causa impacto na rede. Por exemplo, um fluxo para ser considerado de grande tamanho deve ter seu valor em bytes analisado antes de classificá-lo como elefante, e não apenas a quantidade de vezes que o fluxo aparece.

Um vez descoberto o valor do fator de corte C, é possível efetuar a divisão das classes. Um fluxo que pertence a primeira classe é aquele que está contido entre

$x_0 \leq X \leq x_{n_1}$, onde x_0 é o menor valor encontrado para aquela variável aleatória, e x_{n_1} será o último valor de X que ainda satisfaz a inequação (4.4),

$$\sum_{i=0}^{i=n_1} x_i * p_x \leq C. \tag{4.4}$$

As demais classes seguirão o mesmo raciocínio, ou seja, a segunda classe será composta por aqueles fluxos onde $x_{n_1} < X \leq x_{n_2}$, onde x_{n_2} será o último valor de X que ainda satisfaz a inequação 4.4 (substituindo-se $i = 0$ por $i = n_1$ e $i = n_1$ por $i = n_2$). O algoritmo se repete até que as N classes sejam obtidas.

Desta forma, a primeira classe será composta por fluxos pequenos mas que em geral ocorrem com freqüência alta, as classes intermediárias serão compostas por fluxos intermediários e ocorrência também intermediária, e finalmente os fluxos grandes serão aqueles que possuem altos valores, mas em geral de pequena freqüência. A seguir será feito um exemplo mostrando o funcionamento da metodologia.

A tabela 4.1 mostra um exemplo do banco de dados, onde 8 fluxos foram coletados.

Tabela 4.1: Exemplo do banco de dados

Fluxo	Tamanho	Duração	Taxa	Porta Origem	Porta Destino
1	96	2.82	33.95	4351	139
2	351	0.64	548.44	53	53
3	1775	0.57	3081.60	57200	80
4	2419	0.89	2699.77	80 2	365
5	2922	71.23	41.02	25	50512
6	3205	49.72	64.45	80	45582
7	5320	71.61	74.28	21	4026
8	5448	71.80	75.86	4232	4662

Para descobrir o fator de corte C para o tamanho deve-se aplicar a equação 4.3. Para $N = 2$, o fator seria calculado da seguinte forma:

$$\begin{aligned} C = \frac{1}{2}[(96 * 1/8) + (351 * 1/8) + (1775 * 1/8) + (2419 * 1/8) \\ +(2922 * 1/8) + (3205 * 1/8) + (5320 * 1/8) + (5448 * 1/8)] = 1346 \end{aligned} \tag{4.5}$$

Desta forma a classe 1 seria obtida utilizando a inequação 4.4, como mostrado a seguir.

$$[(96*1/8)+(351*1/8)+(1775*1/8)+(2419*1/8)+(2922*1/8)+(3205*1/8)] =\leq 1346. \quad (4.6)$$

A classe 1 (rato) seria portanto formada pelos fluxos numerados de 1 a 6, e a classe 2 (elefante) seria formada pelos fluxos 7 e 8.

4.2 Correlação

Um importante fator a ser estudado é a correlação entre as variáveis dos fluxos. Podem-se estudar mecanismos de tarifação de redes, distinguir um tráfego padrão de um malicioso e obter importantes informações para os projetistas de rede e de equipamentos [12].

Através dos dados armazenados no banco de dados, é possível calcular o coeficiente de correlação das variáveis tamanho, taxa e duração e, desta forma, identificar como estas variáveis estão inter-relacionadas.

Para relacionar as diferentes categorias de fluxo (elefante, tartaruga e chitá), duas análises devem ser feitas: análise da percentagem dos fluxos que pertencem a duas categorias diferentes (ex: percentagem de fluxos elefante e tartaruga) e análise da percentagem dos fluxos que pertencem a uma determinada categoria, dado que já pertencem a outra. A seguir é descrito o algoritmo utilizado para estas análises.

Para realizar o cálculo da percentagem dos fluxos que pertencem a duas categorias, todos os fluxos contidos no banco de dados devem ser consultados. É verificado, então, se um determinado fluxo apresenta valores compatíveis com as classes que se deseja comparar. Caso apresente, é adicionada uma unidade ao contador dos fluxos. Ao final do processo, o valor do contador é dividido pelo número total de fluxos. De forma semelhante, na análise da percentagem dos fluxos que pertencem a uma categoria (dado que já pertencem a outra), o banco de dados deve ser consultado. Deve-se verificar se a condição desejada foi respeitada. Caso positivo, deve-se verifi-

car, então, se a outra variável também atendeu a condição. Se estas duas condições forem satisfeitas, é somado 1 ao contador de fluxos. Ao final do processo, o contador é dividido pelo número total de fluxos que respeitaram a primeira condição. Abaixo o algoritmo é descrito.

```
Enquanto há registro de fluxo no banco {
        Se tamanho do fluxo >= tamanho elefante {
                Se duração do fluxo >= duração tartaruga {
                        contador_elefante_tartaruga <- contador_elefante_tartaruga + 1
                }
                Se taxa do fluxo >= taxa chitá {
                        contador_elefante_chita <- contador_elefante_chita + 1
                }
                contador_elefante <- contador_elefante + 1
        }
        Se duração do fluxo >= duração tartaruga {
                Se taxa do fluxo >= taxa chitá {
                        contador_tartaruga_chita <- contador_tartaruga_chita + 1
                }
                contador_tartaruga <- contador_tartaruga + 1
        }
        Se taxa do fluxo >= taxa chitá {
                contador_chita <- contador_chita + 1
        }
        fluxos_total <- fluxos_total + 1
}
Percentagem_elefante_tartaruga <- contador_elefante_tartaruga / fluxos_total
Percentagem_elefante_chita <- contador_elefante_chita / fluxos_total
Percentagem_tartaruga_chita <- contador_tartaruga_chita / fluxos_total
Percentagem_elefante_dado_tartaruga <- contador_elefante_tartaruga / contador_tartaruga
Percentagem_elefante_dado_chita <- contador_elefante_chita / contador_chita
Percentagem_tartaruga_dado_elefante <- contador_elefante_tartaruga / contador_elefante
Percentagem_tartaruga_dado_chita <- contador_tartaruga_chita / contador_chita
Percentagem_chita_dado_elefante <- contador_elefante_chita / contador_elefante
Percentagem_chita_dado_tartaruga <- contador_tartaruga_chita / contador_tartaruga
```

4.3 Comportamento das Aplicações

Para a análise dos serviços mais utilizados, foi criada uma tabela com três campos: número da porta, número de bytes e número de fluxos. A tabela foi construída analisando o número da porta de origem e destino de cada fluxo medido. Após a verificação da porta, é somado ao campo “número de bytes"da tabela o valor do tamanho do fluxo, e somado ao campo “número de fluxos” uma unidade. Após a análise de todos os fluxos medidos, a tabela é ordenada pelo campo “número de bytes”. Abaixo o algoritmo é descrito.

```
Enquanto há registro de fluxo no banco {
Lê valor portaDestino
Lê valor portaOrigem
        numeroBytes[portaDestino] += tamanho
        numeroFluxos[portaDestino] += 1
        numeroBytes[portaOrigem] += tamanho
        numeroFluxos[portaOrigem] += 1

}
```

4.4 Comparações

A metodologia proposta possui algumas vantagens em relação às já existentes na literatura. A primeira grande vantagem é a possibilidade de se analisar grandes volumes de dados. Alguns modelos propostos, como por exemplo [13], apesar de eficazes, são muito complexos e apenas conseguem analisar algumas dezenas de fluxos. Outra importante vantagem da metodologia é a utilização de amostras para fazer a classificação, diferentemente de alguns outros modelos, como [9] e [10], que propõem valores arbitrários para diferenciar as classes. O modelo proposto possibilita o uso de N classes de fluxos, ao contrário da grande maioria dos trabalhos já propostos, permitindo não só uma maior granularidade na classificação, mas também a análise do comportamento de fluxos de valores intermediários. A Tabela 4.2 mostra as principais diferenças entre os modelos de classificação propostos na literatura.

Tabela 4.2: Comparação entre os diferentes métodos

	Método [9]	Método [10]	Método[11]	Método [13]	Médoto Proposto
Número máximo de classes	2	2	2	N	N
Divisão Arbitrária / Estatísitca	Arbitrária	Arbitrária	Estatísitca	Estatísitca	Estatísitca
Análise ao longo do tempo	Não	Não	Não	Não	Sim
Análise de backbones	Sim	Sim	Sim	Sim	Não

Capítulo 5

Aplicação da Metodologia no Estudo de um Caso Real

NESTA seção, é feito um estudo de caso na Rede Rio [48] utilizando a metodologia descrita. Serão feitas diversas análises dos fluxos medidos, mostrando qual é a correlação entre as diferentes categorias de fluxos e como é a distribuição cumulativa das diferentes classes dos fluxos. Serão feitas também comparações com um outro modelo proposto.

A Tabela 4.2 mostrou as principais diferenças entre os modelos de classificação da literatura e o método proposto. É possível notar que o método proposto por possibilitar a classificação dos fluxos em N classes terá resultados melhores que os métodos [9], [10] e [11], pois possibilita a análise do comportamento de fluxos intermediários. Outro fator importante é que diferentemente dos métodos [9] e [10] que fazem as divisões entre as classes de forma arbitrária, de acordo com o sentimento do administrador da rede, o método proposto utiliza métodos estátisticos para dividir as classes, o que torna a divisão mais confiável. Apesar do modelo apresentado em [13] também apresentar as vantagens citadas, ele possui um grande limitador que é a possibilidade de se analisar grandes quantidades de fluxos, impossibilitando assim de se analisar o tráfego de um backbone. Por estes motivos, para o caso estudado (backbone IP) os resultados obtidos representam uma melhora em relação ao que já havia sido apresentado pela literatura.

Tabela 5.1: Descrição dos dados coletados

	Rede Rio
Data de início	26/09/2005
Data de término	11/11/2005
Número de fluxos	1.860.549.382
Número de bytes	22.004.957.909.714

5.1 Dados Medidos

Os dados foram obtidos das interfaces ligadas à Embratel[49] e à RNP [50] do roteador de borda da Rede Rio[48]. O tráfego coletado foi aquele que entrava e saía do roteador, ou seja, todo tráfego com destino à Rede Rio e todo o tráfego com origem na Rede Rio. Os dados correspondem a sete semanas de coletas (o maior período de coleta em relação as referências consultadas), realizadas no horário de maior utilização da rede, das 10h às 16h, excluindo-se os finais de semana e feriados. Na Tabela 5.1, são mostrados quais dados foram obtidos e o período de obtenção dos mesmos.

É interessante enfatizar o tempo de medição bem como o volume de tráfego medido. Em relação a estes aspectos, os dados obtidos apresentam pelo menos duas vantagens em relação a trabalhos anteriores. A primeira vantagem é o grande volume de tráfego coletado, que permite uma maior confiabilidade nos resultados, uma vez que quanto maior o tamanho da amostra, maior a probabilidade dos resultados obtidos representarem o comportamento real da rede. Enquanto medições feitas em [44] foram da ordem de 30 milhões de pacotes, neste trabalho foram analisados mais de 30 bilhões. O trabalho [12] realiza suas medições com cerca de 3 milhões de fluxos. Já no presente trabalho, são analisados cerca de 1.8 bilhão. Os artigos [44, 12] fizeram apenas 2 horas de medição e em [9] o tráfego é medido em um período de 10 horas.

5.2 Tráfego

As Figuras de 5.1 a 5.3 mostram as distribuições cumulativas dos fluxos de acordo com o tamanho, duração e taxa, respectivamente. É importante conhecer tais distribuições para fins de modelagem de tráfego e planejamento de novas redes. A Figura 5.1 mostra que cerca de 91% dos fluxos possuem tamanho de até 10KBytes. A partir deste resultado é possível concluir que o tráfego é predominantemente composto por fluxos de tamanhos pequenos. As implicações deste fato podem ser diversas. Pode-se citar, por exemplo, que as análises e simulações do protocolo TCP são focadas em seu comportamento em regime permanente, com saturação da rede (ex: a transmissão de longos arquivos), assumindo que o grande volume de fluxos elefante não seria afetado pela presença de pequenos fluxos (ratos). No entanto, enquanto os fluxos elefante sofrem o controle de congestionamento do protocolo TCP, os fluxos de pequeno tamanho não são controlados pelo algoritmo do protocolo, uma vez que eles são enviados e recebidos antes que o TCP tenha a oportunidade de aplicar o controle. Desta forma, um grande volume de pequenos fluxos pode gerar perdas de pacotes, aumentando o congestionamento da rede. A distribuição encontrada teve comportamento similar em [12] e [44]. É interessante notar que que a distribuição do tamanho dos fluxos se aproxima muito de uma distribuição de cauda pesada [41] com $\alpha = 0.64$.

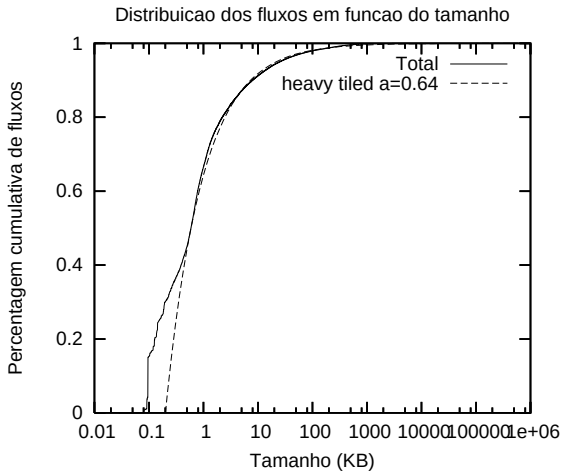


Figura 5.1: Distribuição do tamanho dos fluxos

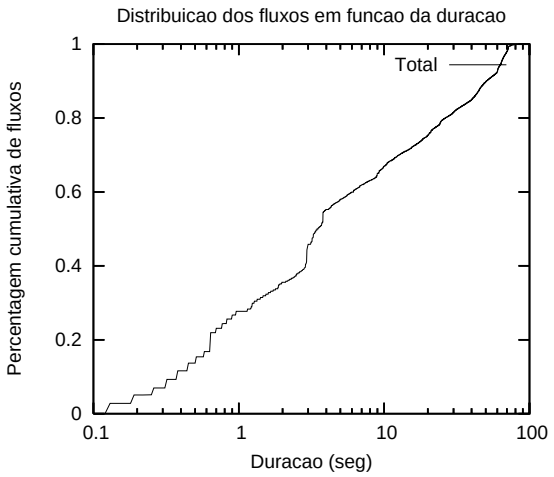


Figura 5.2: Distribuição da duração dos fluxos

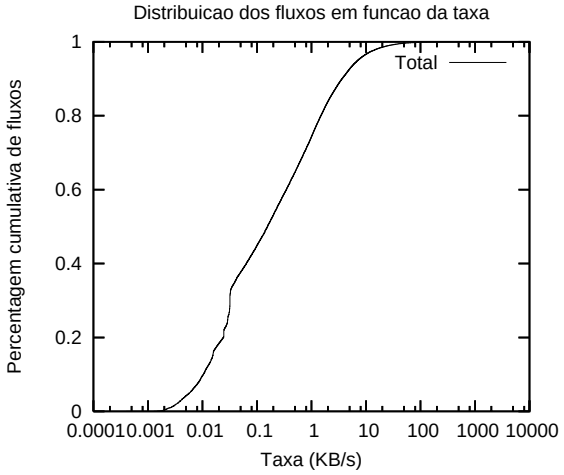


Figura 5.3: Distribuição da taxa dos fluxos

A Figura 5.2 mostra que mais de 85% dos fluxos duram até 25 segundos e cerca de 50% duram até 3 segundos. Pode-se verificar que, em sua maioria, os fluxos são de pequena duração, assim como observado em [9, 12, 44].

Na Figura 5.3, observa-se que mais de 85% dos fluxos possuem taxa igual ou inferior a 2 Kbytes/s, indicando que a grande maioria dos fluxos possuem taxas de transmissão relativamente pequenas. Em [12] a distribuição da taxa se mostrou superior. Cerca de 85% das taxas eram iguais ou inferiores a 10Kbytes/s. Zhang *et al* [44] verificou uma distribuição semelhante, com a grande maioria dos fluxos

apresentando taxas inferiores a 10Kbits/s.

Na Tabela 5.2, é possível verificar os serviços responsáveis pela maior fração do tráfego. O tráfego Web representa cerca de 44% do tráfego da Rede Rio, compreendendo 43% dos fluxos. Pode-se observar também uma grande percentagem de tráfego *Peer to Peer* que representa cerca de 15% do tráfego total em bytes, confirmando o crescimento que as aplicações P2P vêm tendo na Internet. É interessante ressaltar que este valor é certamente inferior ao valor real, uma vez que, nas medições feitas, foram consideradas apenas as portas definidas por cada tipo de aplicação, enquanto as aplicações P2P permitem que o usuário modifique as portas utilizadas no intuito de burlar os *firewalls*.

Tabela 5.2: Serviços utilizados

	Percentagem de bytes	Percentagem de Fluxos
Web	44.93	43.02
E-Donkey	11.51	11.94
SMTP	4.86	3.20
BitTorrent	3.18	1.07
HTTPS	2.31	3.81
FTP	0.57	0.04
SSH	0.50	0.94
DNS	0.24	4.35
Outros	31.90	31.63

5.2.1 Classificação com Duas Classes

Nesta seção serão apresentados os resultados utilizando a metodologia proposta para duas classes. Os fluxos foram considerados de pequeno tamanho (ratos ou classe 1) se tivessem tamanho igual ou inferior a 370 KBytes, e de grande tamanho (elefantes) se tivessem tamanho maior que 370 KBytes. Os fluxos foram considerados de longa duração (tartaruga) se tivessem duração superior a 46.6 segundos. Em relação a taxa, foram classificados como alta taxa (chitá) aqueles com taxa superior

a 12.3 KBps.

É possível perceber um comportamento semelhante nas Figuras 5.4, 5.5 e 5.6, onde a classe 1 tem uma distribuição quase idêntica a distribuição total (classe 1 + classe 2). Devido a utilização de apenas duas classes, não é possível conhecer o comportamento dos fluxos intermediários.

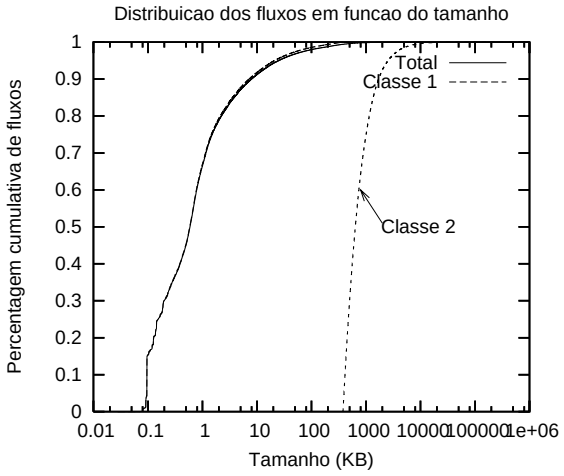


Figura 5.4: Distribuição do tamanho dos fluxos

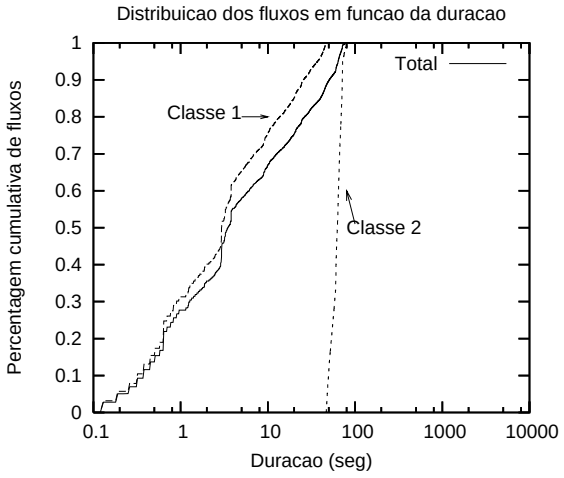


Figura 5.5: Distribuição da duração dos fluxos

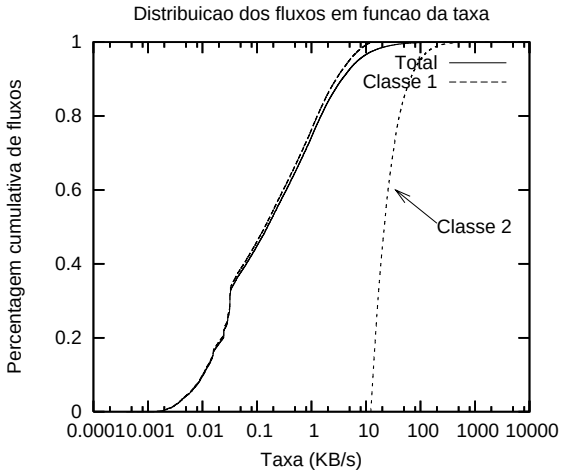


Figura 5.6: Distribuição da taxa dos fluxos

5.2.2 Classificação com Quatro Classes

Nesta seção, os fluxos serão classificados utilizando quatro classes. O principal motivo de se utilizar mais classes se deve ao fato de que a utilização de um número pequeno de classes pode fazer com que haja fluxos de comportamentos substancialmente diferentes pertencentes a uma mesma classe. Um número maior de classes permite realizar distinções importantes. Executando a metodologia para quatro classes, algumas diferenças foram identificadas.

A Figura 5.7 mostra a distribuição do tamanho das diferentes classes. Nota-se que, devido ao comportamento de cauda pesada, a classe 1 ainda tem uma distribuição muito semelhante à total. No entanto, já é possível analisar o comportamento de classes intermediárias (2 e 3) que antes estavam mascaradas. As classes 1 e 2 foram divididas em duas. Utilizando quatro classes, os fluxos elefantes foram aqueles com tamanho superior a 1.1MB. A classe 3 foi estipulada entre 370KB e 1.1MB, enquanto os fluxos de tamanho entre 93KB e 370KB foram classificados como pertencentes à classe 2.

A Figura 5.8 mostra a distribuição da duração das quatro classes. Os fluxos da classe 1 foram estipulados como sendo aqueles de duração entre 0.10s e 24.19s. Pode-se perceber que a classe 1 não possui uma curva tão similar em relação a distribuição

total. Os fluxos com durações entre 24.19s e 46.80s foram considerados pertencentes a classe 2. A classe 3 foi considerada como sendo de fluxos com durações entre 46.80s e 63.87. Finalmente, os fluxos de longa duração (tartaruga) foram aqueles que levaram mais que 63.87s.

A Figura 5.9 mostra o comportamento da distribuição da taxa dos fluxos. Os fluxos da classe 1 (taxas entre 0.41Bytes/s e 3.86KBytes/s) apresentaram uma distribuição muito similar da distribuição total. Os fluxos da classe 2 foram aqueles com taxa entre 3.86KBps e 12.29KBps. A classe 3 foi composta de fluxos com taxas entre 12.29KBps e 42.80KBps. Os fluxos chitá foram aqueles com taxas superiores a 42.80KBps.

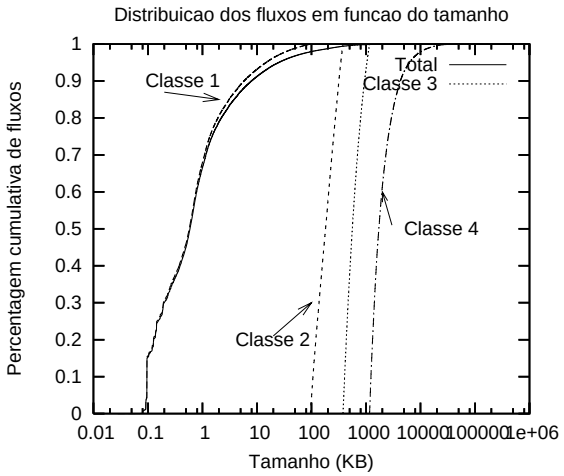


Figura 5.7: Distribuição do tamanho dos fluxos

5.2.3 Comparações Entre a Medotologia Proposta e o Método Proposto em [11]

Nesta seção serão realizadas comparações entre os resultados obtidos na classificação dos fluxos entre a metodologia proposta e o método que utiliza a média e o desvio padrão como forma de classificação. A tabela 5.3 mostra os valores encontrados.

Nas Figuras 5.10 a 5.12, é possível observar algumas importantes diferenças entre os dois métodos. Pode-se observar, por exemplo, que o modelo proposto com

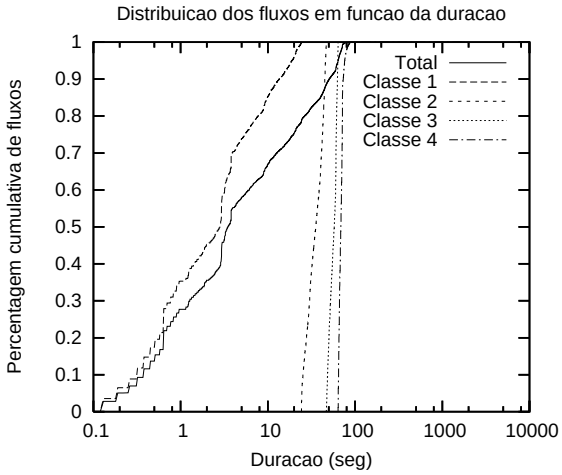


Figura 5.8: Distribuição da duração dos fluxos

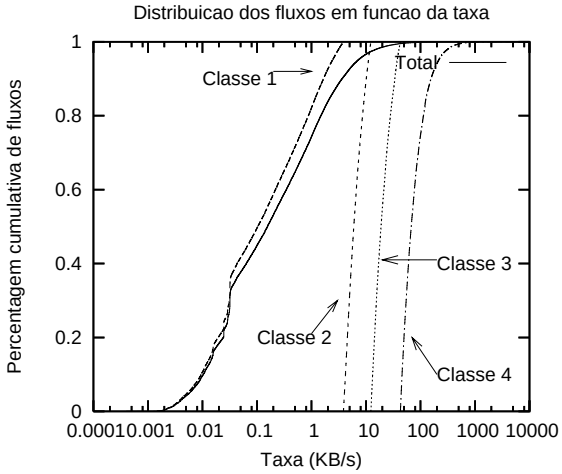


Figura 5.9: Distribuicao da taxa dos fluxos

$N = 4$ foi o que classificou os fluxos elefantes e chitá com os maiores valores para o tamanho e taxa, respectivamente. Como a variável duração foi a que apresentou menor coeficiente de variação, o modelo proposto com $N = 4$ classificou os fluxos tartaruga com um limiar menor que o método que utiliza a média e o desvio padrão. É possível notar também que o método proposto com $N = 2$ foi o que classificou os fluxos como pesados com os menores valores.

Tabela 5.3: Média e desvio padrão dos Fluxos

	Média	Desvio Padrão	Média + 3*desvio padrão
Tamanho (KBytes)	11.54	145.03	446.65
Duração (seg)	14.23	20.51	75.74
Taxa (KBps)	1.86	9.75	30.36

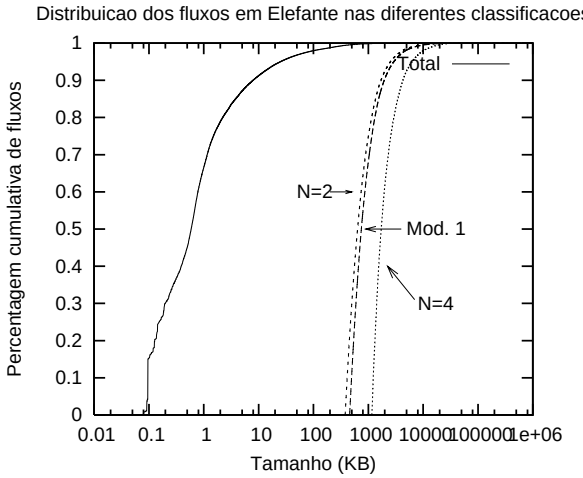


Figura 5.10: Distribuição do tamanho dos fluxos

5.3 Correlação

Nesta seção, serão apresentados diversos resultados obtidos utilizando o modelo proposto para $N = 4$.

A Tabela 5.4 mostra como os fluxos estão relacionados. Verifica-se que apenas 0.09% dos fluxos são elefante e tartaruga, e apenas 0.03% são elefante e chitá. Observa-se também uma pequena relação entre os fluxos de alta taxa e alta duração. Ao analisar a coluna de bytes, percebe-se que, apesar de uma pequena relação entre os fluxos elefante e tartaruga, eles representam 19.51% do tráfego em bytes. Isto mostra que um quinto do tráfego da rede é composto por fluxos de longa duração e grande tamanho, o que indica um perfil de tráfego contínuo.

A Tabela 5.5 apresenta a probabilidade de um fluxo pertencer a uma categoria, dado que já pertence a outra. É verificado que existe uma grande relação entre

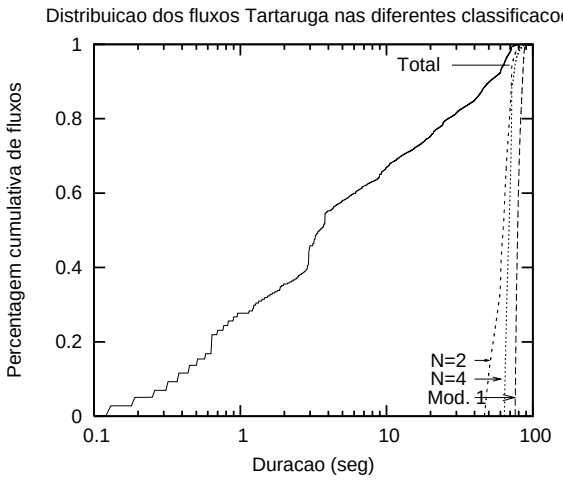


Figura 5.11: Distribuição da duração dos fluxos

Tabela 5.4: Percentagem de fluxos pertencentes a duas categorias

	Elefante		Chitá	
	% Bytes	% Fluxos	% Bytes	% Fluxos
Tartaruga	19.51	0.09	8.82	0.02
Chitá	13.05	0.03	-	-

os fluxos elefante e tartaruga. Um fluxo elefante tem probabilidade 77.75% de ser tartaruga. Pode-se observar que apenas 0.32% dos fluxos de longa duração possuem altas taxas de transmissão, confirmando o fato da maioria dos fluxos tartaruga não serem de grande tamanho. Em relação aos fluxos com alta taxa, 6.66% são elefantes e 3.32% são tartaruga.

Ao se analisar a percentagem de bytes da Tabela 5.5, é possível visualizar uma grande variação. Apesar de apenas 6.66% dos fluxos chitá serem elefante, eles representam cerca de 82% dos bytes, mostrando que uma pequena porção do tráfego chitá é responsável pela maior percentagem de bytes. O mesmo pode ser verificado em relação aos fluxos de longa duração. A única comparação que não apresenta uma grande diferença entre a percentagem de fluxos e bytes é entre os fluxos elefante e tartaruga.

Os estudos [12, 39] mostram que há uma alta correlação entre o tamanho do fluxo

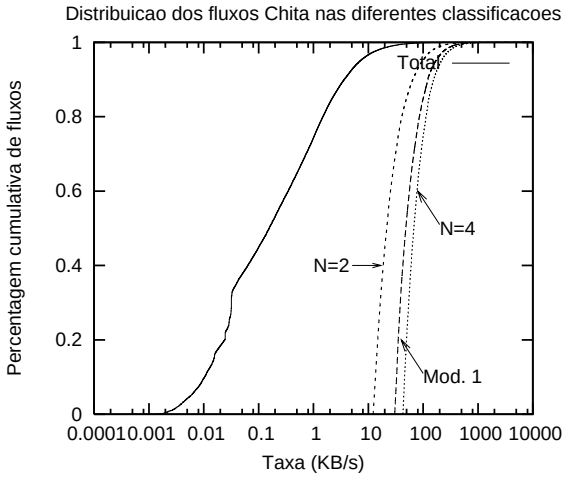


Figura 5.12: Distribuição da taxa dos fluxos

Tabela 5.5: Percentagem de fluxos pertencentes a uma categoria dado que pertence a outra

	Dado					
	Elefante		Tartaruga		chitá	
Valor Esperado	% Fluxos	% Bytes	% Fluxos	% Bytes	% Fluxos	% Bytes
Elefante	-	-	1.77	33.47	6.66	82.96
Tartaruga	77.75	78.05	-	-	3.32	56.05
Chitá	28.11	52.19	0.32	15.12	-	-

e sua taxa. A maioria dos fluxos de alta taxa (93,34%) não é de grande tamanho, o que nos mostra uma característica de tráfego por rajada. No entanto, uma pequena porção de fluxos de alta taxa (fluxos chitá e elefante) responde pela grande maioria dos bytes trafegados. Isto ocorre provavelmente devido a transmissões de grandes arquivos em enlaces de alta velocidade.

Na Tabela 5.6, pode-se verificar uma ausência de relação entre o número de fluxos e volume de tráfego que cada categoria é responsável. Resultados semelhantes foram verificados em [9] e [38]. A tabela indica que, apesar de somente 0.12% dos fluxos serem elefantes, eles representam 25% do tráfego da rede. O mesmo é observado em relação a duração e a taxa, havendo uma grande variação entre a percentagem de fluxos e de bytes. Tal comportamento deve ser analisado, uma

vez que as infra-estruturas de rede e os protocolos atuais são desenvolvidos para um tráfego de rajada. A maior utilização do enlace de rede por um longo período de tempo, devido ao aumento da duração e do tamanho dos fluxos, modifica o perfil do tráfego. Em função deste comportamento, [35] propõe a utilização de roteadores "sensíveis a carga", que utilizariam rotas especiais para tais tipos de fluxos. Em relação aos fluxos chitá, é observado que os percentuais de fluxos e bytes são próximos, mostrando que os mesmos têm pouco impacto no tráfego de rede.

A Tabela 5.7 mostra a correlação dos fluxos. O coeficiente de correlação encontrado entre duração e o tamanho dos fluxos indica que há uma pequena correlação entre estas duas variáveis. Este comportamento pode ser explicado pelo fato de que um aumento no tamanho do fluxo, considerando-se um taxa de transmissão constante, causará um aumento da duração. O coeficiente de correlação entre taxa e tamanho dos fluxos foi o que apresentou maior valor. Este resultado indica que, para uma grande parte do tráfego, o aumento de tamanho implica um aumento de taxa. Isto ocorre provavelmente devido a transferências de grandes arquivos com altas taxas. O coeficiente de correlação entre taxa e duração foi ligeiramente negativo, mostrando que são poucos os fluxos em que o aumento da taxa é seguido pela diminuição da duração.

Tabela 5.6: Percentagem do tráfego de cada categoria

	Elefante	Tartaruga	Chitá
Fluxos	0.12%	5.10%	0.49%
Bytes	25.00%	58.29%	15.72%

Tabela 5.7: Correlação dos fluxos

	Coeficiente de Correlação
Tamanho e Duração	0.15
Tamanho e Taxa	0.29
Taxa e Duração	-0.07

As Tabelas 5.8 e 5.9 mostram as correlações das categorias dos fluxos. A Tabela

5.8 indica que não há correlação entre os fluxos de grande tamanho e longa duração e que há uma pequena correlação negativa entre os fluxos de alta taxa e longa duração, indicando que tais tipos de categorias não possuem relação. O coeficiente de correlação chitá e elefante apresenta o maior valor, mostrando que, em geral, quando os fluxos são elefantes e chitá, o aumento do tamanho do fluxo é acompanhado pelo aumento da taxa.

Tabela 5.8: Correlação entre as categorias

	Coef. de Correlação
Elefante e Tartaruga	0.00
Tartaruga e Chitá	-0.01
Chitá e Elefante	0.39

Tabela 5.9: Correlação entre os fluxos

	Coeficiente de Correlação Dado		
	Elefante	Tartaruga	chitá
Tamanho e Taxa	0.50	0.99	0.21
Tamanho e Duração	0.02	0.04	0.68
Duração e Taxa	-0.27	0.03	-0.01

A Tabela 5.9 fornece informações sobre a correlação dos fluxos dado que eles pertencem a uma determinada categoria. Algumas correlações chamam atenção. O tamanho e a duração dos fluxos de alta taxa apresentam alta correlação, indicando que, nos fluxos chitá, o aumento de tamanho implica um aumento de duração. Este fato também explica a pequena correlação entre duração e taxa nos fluxos chitá. Quando o tamanho cresce, a duração também aumenta, e a taxa conseqüentemente sofre pouca alteração. Os fluxos de longa duração apresentam um coeficiente de correlação próximo de 1, indicando que, nos fluxos tartaruga, o aumento de tamanho levará a um aumento da taxa. Pode-se também observar uma correlação negativa entre duração e taxa nos fluxos de grande tamanho.

A Figura 5.13 mostra a distribuição dos fluxos de cada categoria em função do tamanho. Na literatura, ainda não existe um consenso sobre o que causa fluxos de longa duração. Não se sabe se eles são causados devido ao comportamento dos protocolos/usuário ou devido à transferência de grandes arquivos em enlaces com baixas taxas [12]. Na análise feita, é possível observar que cerca de 30% dos fluxos de longa duração têm tamanho de até 2KB, 60% até 14KB e 90% até 345KB, o que mostra que a grande maioria dos fluxos de longa duração são fluxos de pequeno tamanho. Este fato indica que fluxos de longa duração são causados devido à enlaces de baixa capacidade ou ao comportamento de protocolos utilizados. O gráfico mostra também que apenas 6% dos fluxos de alta taxa possuem tamanho superior a 1.1MB.

Na Figura 5.14, observa-se que cerca de 22% dos fluxos elefante duram até 63 segundos. Mais de 95% dos fluxos de alta taxa duram menos de 26 segundos.

Finalmente, na Figura 5.15, observa-se que cerca de 71% dos fluxos de grande tamanho têm taxa de até 42KB/s, indicando que a maioria dos fluxos elefantes possuem baixas taxas de transmissão. Os fluxos tartaruga apresentaram as menores taxas, com cerca de 90% dos fluxos possuindo taxas até 4.8KB/s.

A partir dos gráficos analisados, conclui-se que os fluxos elefantes têm grande tamanho, grande duração e pequenas taxas. Os fluxos tartaruga têm pequeno tamanho, grande duração e pequenas taxas. Os fluxos chitá, por outro lado, têm pequeno tamanho, pequena duração e alta taxa.

A Tabela 5.10 mostra os principais serviços responsáveis por cada categoria de fluxo. Em todas as categorias, a aplicação responsável pela maior parte dos fluxos é a Web. É interessante notar que as aplicações *peer-to-peer* (E-Donkey e BitTorrent) são responsáveis por 7.12% dos fluxos de grande tamanho e por 17.05% dos fluxos de longa duração, mostrando o importante papel destes tipos de aplicação no tráfego de rede.

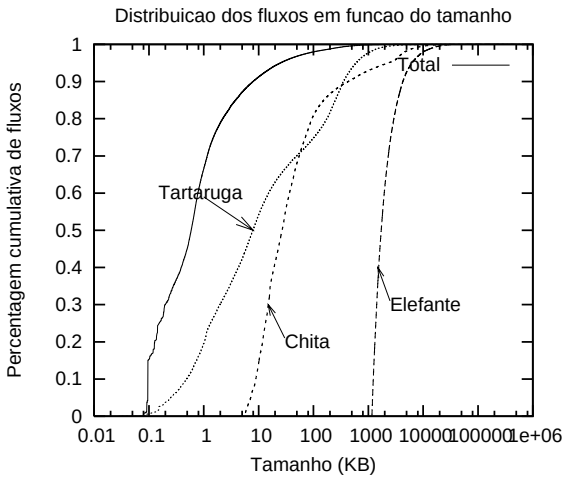


Figura 5.13: Distribuição do tamanho dos fluxos

5.4 Comportamento das Aplicações mais Utilizadas

Nesta seção serão analisados as funções de probabilidade de massas e cumulativas das principais aplicações.

5.4.1 Função Probabilidade de Massas para o Tamanho

A Figura 5.16 mostra as funções probabilidade de massas para o tamanho das principais aplicações medidas na Rede Rio. É possível observar que nenhuma delas tem uma distribuição uni-modal, indicando que existem tamanhos típicos para cada aplicação.

A Figura 5.16(a) mostra que aplicações tipo SSH têm tipicamente fluxos com cerca de 0.2KB. Isso era de se esperar, uma vez que em conexões SSH, poucos dados são trafegados. A Figura 5.16(b) mostra que aplicações SMTP têm tipicamente tamanhos menores que 1KB. As aplicações HTTP e HTTPS mostradas nas Figuras 5.16(c) e 5.16(g) apresentaram um comportamento similar à distribuição normal. O tamaho mais comum é cerca de 1KB, o que indica que estas páginas WEB tem um tamanho pequeno, classificado como classe 1. As aplicações *peer-to-peer* E-Donkey e BitTorrent, apresentadas nas Figuras 5.16(d) e 5.16(f), respectivamente, apresen-

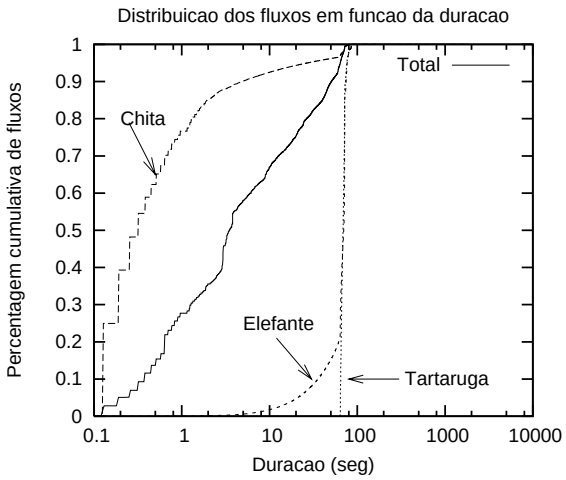


Figura 5.14: Distribuição da duração dos fluxos

taram comportamento ligeiramente diferente, tendo como tamanho mais comum fluxos próximos a 1KB. O comportamento do DNS mostrado na Figura 5.16(e) é composto tipicamente de fluxos pertencentes à classe 1.

5.4.2 Função Probabilidade de Massas para a Duração

A Figura 5.17 mostra as funções probabilidade de massas para a duração das principais aplicações medidas na Rede Rio.

A Figura 5.17(a) mostra que as aplicações SSH tiveram duração típica entre 3 a 6 segundos. Uma possível explicação para este fato pode ser a utilização do protocolo para transferência de arquivos. Aplicações SMTP mostraram que a duração mais comum dos fluxos é de cerca de 10s. As aplicações HTTPS e HTTP, mostradas nas Figuras 5.17(c) e 5.17(g), foram as que apresentaram a menor duração típica. Como esperado, as aplicações *peer-to-peer* foram as que apresentaram maior duração típica. O DNS, provavelmente devido as transações de troca de zona, teve uma duração típica de 50s.

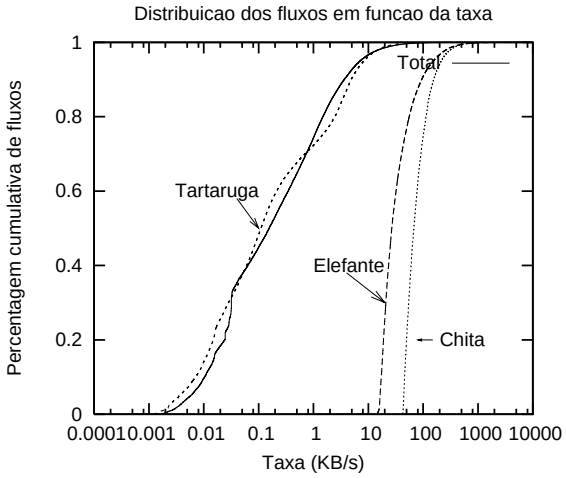


Figura 5.15: Distribuicao da taxa dos fluxos

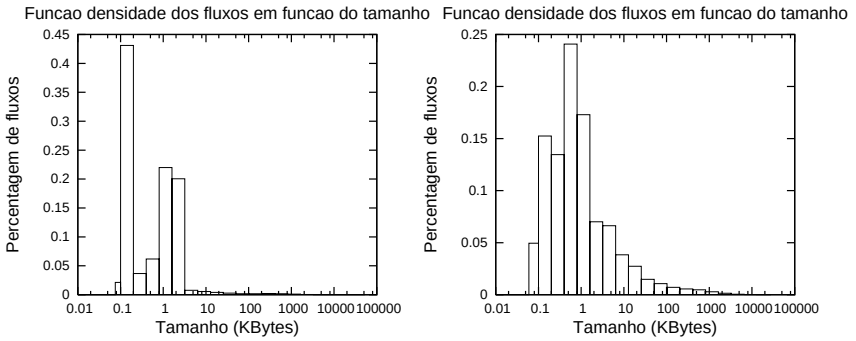
5.4.3 Função Probabilidade de Massas para a Taxa

A Figura 5.18 mostra as funções probabilidade de massas para a taxa das principais aplicações medidas na Rede Rio.

A Figura 5.18(a) mostra que a taxa mais comum do protocolo SSH é de cerca de 0.03KBps, indicando que a aplicação é formada tipicamente por pequenos tamanhos, durações e taxas. O SMTP mostrou uma curva próxima à normal, com uma taxa típica de cerca de 0.1KBps. As aplicações HTTPS e HTTP, mostradas nas Figuras 5.18(c) e 5.18(g), respectivamente, também apresentaram distribuição próxima à normal, com uma taxa típica de 1KBps. As aplicações *peer-to-peer* apresentaram as taxas tipicamente da classe 1, assim como o DNS.

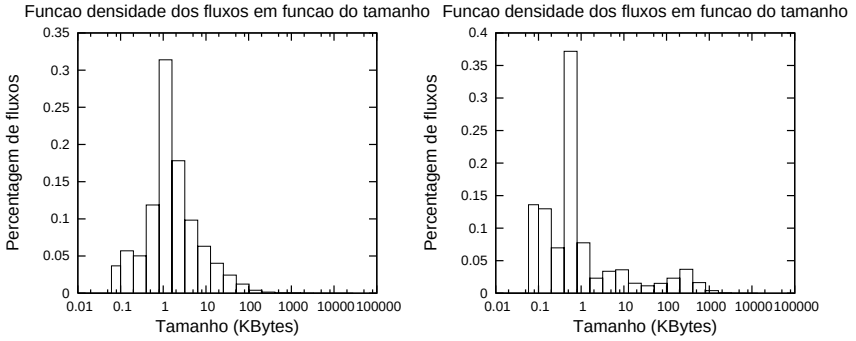
Tabela 5.10: Percentagem das aplicações mais utilizadas de acordos com as categorias dos fluxos

Posição	Elefante (% bytes, % fluxos)	Tartaruga (% bytes, % fluxos)	Chitá (% bytes, % fluxos)
1	Web (47.44%, 43.56%)	Web (26.94%, 18.56%)	Web (58.25%, 87.61%)
2	SMTP (8.34%, 8.50%)	Edonkey (16.36%, 12.90%)	SMTP (11.69%, 4.45%)
3	Edonkey (4.61%, 7.12%)	BitTorrent (4.66%, 4.15%)	LDM (3.47%, 0.16%)
4	FTP (1.61%, 1.29%)	SMTP (2.75%, 1.90%)	FTP (1.71%, 0.24%)
5	HTTPS (1.58%, 1.70%)	LDM (1.41%, 0.43%)	HTTPS (1.67%, 4.07%)



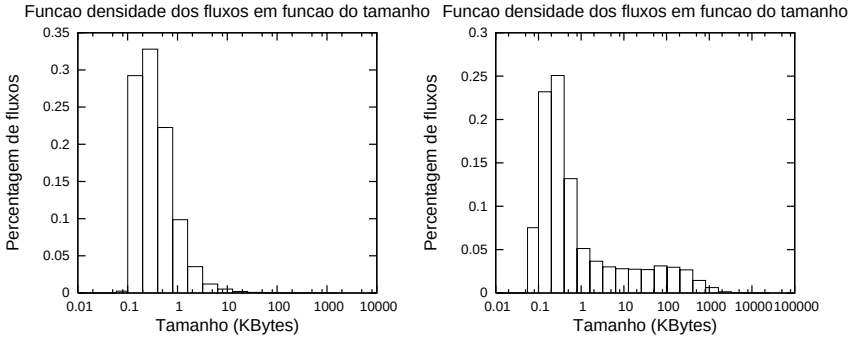
(a) SSH

(b) SMTP



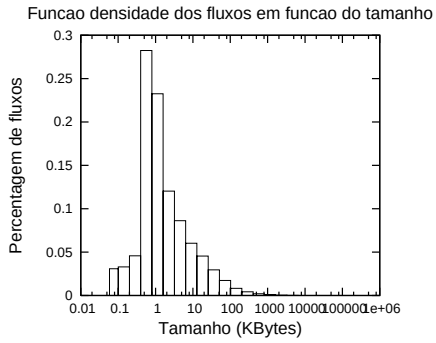
(c) HTTPS

(d) EDONKEY



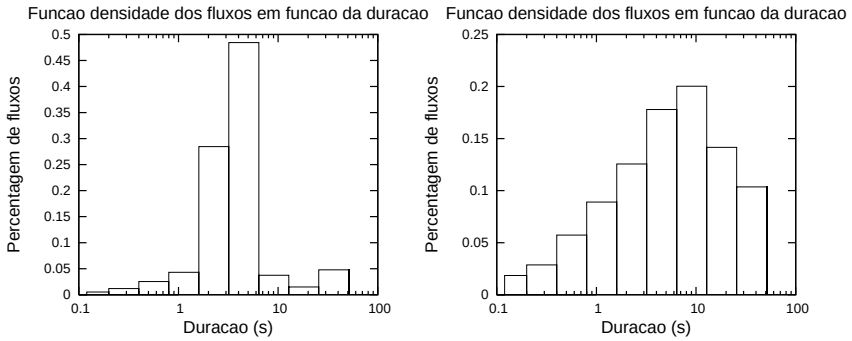
(e) DNS

(f) BIT-TORRENT



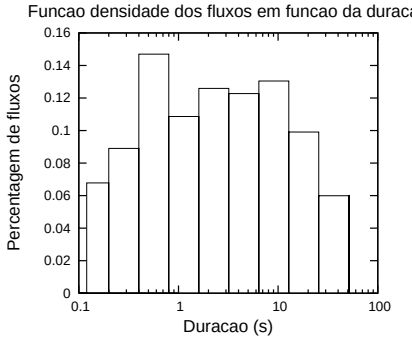
(g) HTTP

Figura 5.16: Função probabilidade de massas para o tamanho dos fluxos das aplicações

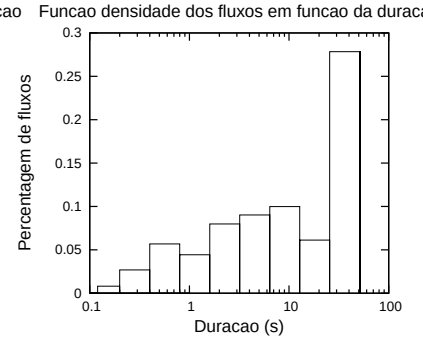


(a) SSH

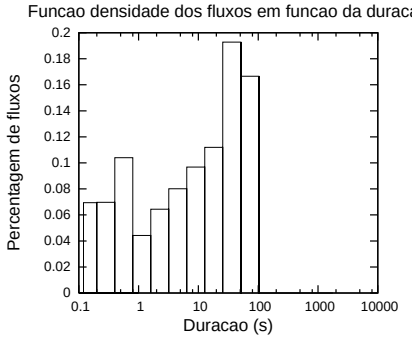
(b) SMTP



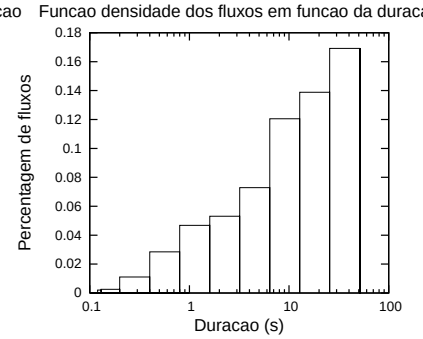
(c) HTTPS



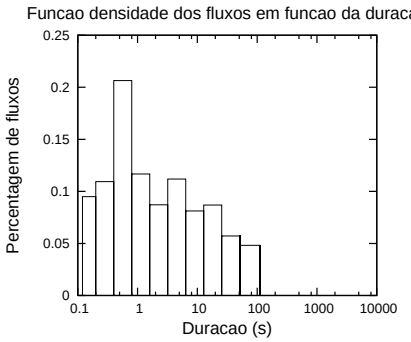
(d) EDONKEY



(e) DNS

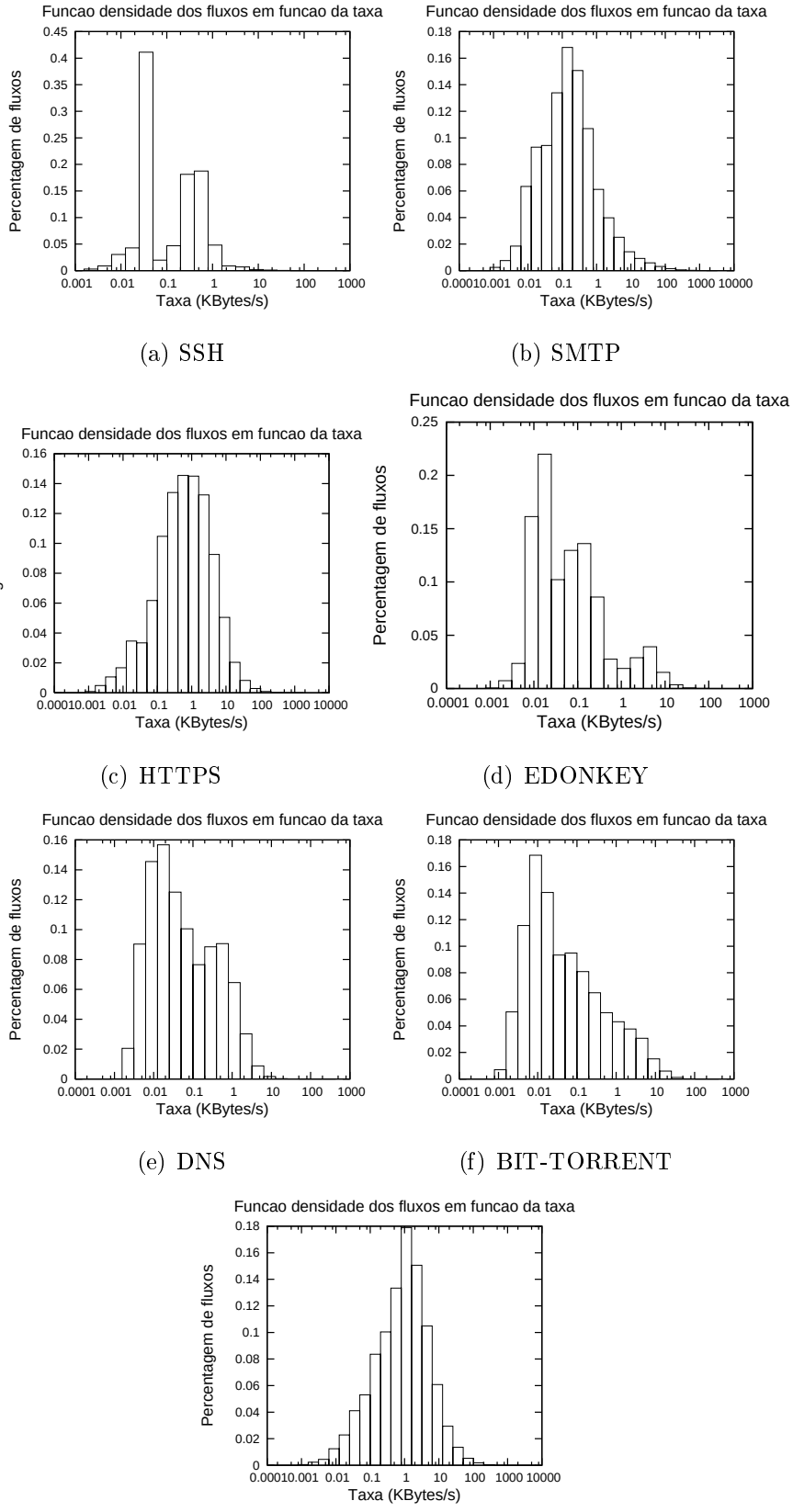


(f) BIT-TORRENT



(g) HTTP

Figura 5.17: Função probabilidade de massas para a duração dos fluxos das aplicações



(a) SSH

(b) SMTP

(c) HTTPS

(d) EDONKEY

(e) DNS

(f) BIT-TORRENT

(g) HTTP

Figura 5.18: Função probabilidade de massas para a taxa dos fluxos das aplicações

Capítulo 6

Conclusões e Trabalhos Futuros

ATUALMENTE , o projeto e a manutenção de um backbone IP são altamente dependentes da intuição dos administradores de rede. A grande variedade do tráfego, a falta de informações de monitoramento, e as complexas interações entre os protocolos de roteamento resultam em técnicas de gerenciamento da rede que muitas vezes se baseiam simplesmente na tentativa e erro. O principal objetivo deste trabalho foi propor uma metodologia de análise que proporcionasse aos operadores um melhor entendimento do tráfego de rede, possibilitando assim, ações não mais baseadas na intuição, mas em análises estatísticas do tráfego de rede.

Um dos grandes problemas existentes para se fazer a caracterização de tráfego é obter os dados necessários. A monitoração de rede é, na maioria das vezes, feita utilizando o protocolo SNMP, que possui um conjunto limitado de informações, que são muitas vezes insuficientes. Uma informação mais detalhada do tráfego de rede pode ser obtida utilizando fluxos de comunicação. Este trabalho procurou utilizar estas medidas como dados de entrada nas análises feitas.

Uma das contribuições deste trabalho foi a proposta de uma nova metodologia de classificação dos fluxos, que resolve diversos problemas apresentados no capítulo 3. O método divide os fluxos em N possíveis classes, segundo seus tamanhos, taxas e durações. Através desta divisão, é possível conhecer melhor as características do tráfego de rede. Pode-se, por exemplo, verificar que o comportamento do tráfego

se aproxima da distribuição de Pareto. Uma das principais características desta distribuição é a existência de uma grande quantidade de fluxos de pequenos que é responsável por uma grande percentagem do tráfego total em bytes. Tal comportamento pode sugerir uma necessidade de adaptação das atuais infra-estruturas de rede, uma vez que uma grande quantidade do tráfego em bytes tem apresentado comportamento não de rajada, mas constante.

Outra importante contribuição feita pelo trabalho foi mostrar como as diferentes classes e tipos de fluxos estão relacionados. O cálculo do coeficiente de correlação possibilitou apresentar algumas possíveis razões para comportamentos encontrados, como por exemplo, a alta correlação entre taxa e tamanho, confirmando o fato de que os enlaces de grande capacidade possuem uma grande quantidade de transmissões de arquivos de grande tamanho. O trabalho também traçou um perfil dos grandes fluxos, mostrando que os fluxos elefantes têm grande tamanho, grande duração e pequenas taxas. Já fluxos tartarugas são de pequeno tamanho, grande duração e grande taxa. Finalmente, os fluxos chitá são de pequeno tamanho, pequena duração e alta taxa.

O trabalho também mostrou o comportamento das aplicações responsáveis pela grande maioria do tráfego total da rede, indicando, por exemplo, que a distribuição da taxa do protocolo HTTP se aproxima da normal. Foram identificados também quais são os protocolos mais utilizados nas diferentes classes de fluxos. As análises feitas sobre os serviços mais utilizados mostram que aplicações *peer-to-peer* são responsáveis por um grande volume de tráfego, além de apresentarem fluxos de longa duração e grande tamanho. O crescimento de aplicações P2P tem diversas implicações, a mais importante talvez sendo a mudança no perfil do tráfego de rede [51].

Os métodos e resultados descritos nesta dissertação possibilitam um melhor entendimento de diversas questões relacionadas a caracterização de tráfego.

Como trabalhos futuros, comparações mais abrangentes com os outros métodos propostos devem ser estudadas, e o comportamento dos fluxos ao longo do tempo deve ser analisado.

Referências Bibliográficas

[1] J. Licklider, "On-Line Man-Computer Communication," in *Spring Joint Computer Conference National Press*, vol. 21, (Palo Alto, California, EUA), pp. 113–128, National Press, maio 1962.

[2] L. Kleinrock, "Information Flow in Large Communication Nets," *RLE Quarterly Progress Report*, julho 1961.

[3] P. Baran, "On Distributed Communications," in *IEEE Transactions on Communication Systems*, vol. 1, pp. 1–9, março 1964.

[4] P. Baran, "Founding Father," *Wired Magazine*, pp. 144–153, Março 2001.

[5] D. Davies and R. Scantlebury, "A Digital Communications Network for Computers Giving Rapid Response at Remote Terminals," in *Proceedings of the first ACM symposium on Operating System Principles*, (New York, NY, EUA), pp. 2.1–2.17, ACM Press, outubro 1967.

[6] B. Leiner, L. Kleinrock, L. Roberts, and S. Wolff, "The Past and Future History of the Internet," in *Communications of the ACM*, vol. 40, pp. 102–108, fevereiro 1997.

[7] L. Roberts, "Multiple Computer Networks and Intercomputer Communication," in *ACM Gatlinburg Conference*, (New York, NY, EUA), pp. 3.1–3.6, ACM Press, outubro 1967.

[8] "Federal Networking Council Resolution: Definition of Internet." http://www.itrd.gov/fnc/Internet_res.html, Último acesso em 31/10/2005.

[9] N.Brownlee and K. C. Claffy, "Understanding Internet Traffic Streams: Dragonflies and Tortoises," in *IEEE Communications*, vol. 40, pp. 110–117, outubro 2002.

[10] K. Papagiannaki, N. Taft, and C. Diot, "Impact of Flow Dynamics on Traffic Engineering Design Principles," in *IEEE INFOCOMM 2004*, vol. 23, pp. 2295–2306, março 2004.

[11] L. F. M. de Moraes and G. Vilela, "Classificação de Tráfego Utilizando Fluxos de Comunicação," in *Anais do 23o Simpósio Brasileiro de Redes de Computadores*, (Fortaleza, CE, Brasil), maio 2005.

[12] K. Lan and J. Heidemann, "On the Correlation of Internet Flow Characteristics." http://www.isi.edu/trpublic/pubs/au-kclan.html, Último acesso em 25/03/2005, 2003.

[13] K. Papagiannaki, A. Soule, K. Salamatian, N. Taft, and R. Emilion, "Flow Classification by Histograms or How to Go on Safari in the Internet," in *ACM SIGMETRICS/Performance*, (New York, NY, EUA), pp. 49–60, junho 2004.

[14] J. Postel, "DoD Standard Internet Protocol," *Defense Advanced Research Projects Agency, Information Processing Techniques Office, RFC 760, IEN128*, janeiro 1980.

[15] L. Subramanian, S. Agarwal, J. Rexford, and R. Katz, "Characterizing the Internet Hierarchy from Multiple Vantage Points," in *IEEE INFOCOM'2002*, (New York, NY, EUA), junho 2002.

[16] V. Jacobson, "Pathchar Home Page." ftp://ftp.ee.lbl.gov/pathchar/, Último acesso em 3/11/2005.

[17] B. Mah, "Pchar: a Tool for Measuring Internet Path Characteristics." http://www.kitchenlab.org/www/bmah/Software/pchar/, Último acesso em 3/11/2005.

[18] R. Carter and M. Crovella, "Measuring Bottleneck Link Speed in Packet-Switched Networks," *Performance Evaluation*, vol. 27 e 28, pp. 297–318, outubro 1996.

[19] K. Lai and M. Baker, "Measuring Bandwidth," in *IEEE INFOCOM'99*, pp. 235–245, abril 1999.

[20] C. Dovrolis, P. Ramanathan, and D. Moore, "What do Packet Dispersion Techniques Measure?," *IEEE INFOCOM*, pp. 905–914, abril 2001.

[21] J. Mahdavi and V. Paxson, "IPPM Metrics for Measuring Connectivity," *Network Working Group, RFC 2678*, setembro 1999.

[22] G. Almes, S. Kalidindi, and M. Zekauskas, "A One-way Delay Metric for IPPM," *RFC 2679*, setembro 1999.

[23] G. Almes, S. Kalidindi, and M. Zekauskas, "A One-way Packet Loss Metric for IPPM," *IETF, RFC 2680*, setembro 1999.

[24] G. Almes, S. Kalidindi, and M. Zekauskas, "A Round-trip Delay Metric for IPPM," *IETF, RFC 2681*, setembro 1999.

[25] W. Leland, M. Taqqu, W. Willinger, and D. Wiolson, "On the Self-Similar Nature of Ethernet Traffic (Extended Version)," in *IEEE/ACM Transactions on Networking*, vol. 2, pp. 1–15, fevereiro 1994.

[26] W. Willinger, M. S. Taqqu, R. Sherman, and D. V. Wilson, "Self-similarity Through High-variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level," *IEEE/ACM Transactions on Networking*, vol. 5, pp. 71–86, fevereiro 1997.

[27] M. Crovella and A. Bestavros, "Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes," in *IEEE/ACM Transactions on Networking*, vol. 5, pp. 835–846, dezembro 1997.

[28] V. Paxson and S. Floyd, "Wide Area Traffic: the Failure of Poisson Modeling," *IEEE/ACM Transactions on Networking*, vol. 3, pp. 226–244, junho 1995.

[29] CISCO, "Netflow Services Solutions Guide." http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm Último acesso em 3/11/2005.

[30] K. C. Claffy, *Internet Traffic Characterization*. PhD thesis, University of California, San Diego, CA, EUA, 1994.

[31] C. R. Töpke, "Uma Metodologia para Caracterização de Tráfego e Medidas de Desempenho em Backbones IP," Master's thesis, Universidade Federal do Rio de Janeiro, COPPE/PESC, Rio de Janeiro, RJ, Brasil, 2001.

[32] M. Davis, "Analysis and Optimization of Computer Networking Routing," Master's thesis, Universidade de Delaware, 1988.

[33] S. Heimlich, "Traffic Characterization of the NSFNET National Backbone," in *Proceedings of the 1990 Winter USENIX Conference*, (Washington, D.C, EUA), pp. 257–258, janeiro 1990.

[34] R. Cáceres, P. B. Danzing, S. Jamin, and D. Mitzel, "Characteristics of Wide-Area TCP/IP Conversation," in *Proceedings of ACM SIGCOMM*, pp. 101–112, setembro 1991.

[35] A. Shaikh, J. Rexford, and K. Shin, "Load-Sensitive Routing of Long-lived IP Flows," in *Proceedings of the ACM SIGCOMM. ACM*, pp. 215–226, setembro 1999.

[36] Y. J. Vinay, J. Ribeiro, and A. Feldmann, "On the Impact of Variability on the Buffer Dynamics in IP Networks," in *Proceedings of 37th Annual Allerton Conf. Commun.*, setembro 1999.

[37] W. E. Leland and D. V. Wilson, "High Time-resolution Measurement and Analysis of LAN Traffic: Implications for LAN Interconnection," in *Proceedings of IEEE INFOCOM'91*, (Bal Harbour, FL, EUA), pp. 1360–1366, abril 1991.

[38] A. Broido, Y. Hyun, and K. C. Claffy, "Their Share: Diversity and Disparity in IP Traffic," in *PAM 2004*, (Juan-les-Pins, França), pp. 113–125, abril 2004.

[39] Y. Zhang and Q. Lili, "Understanding the end-to-end Performance Impact of RED in a Heterogeneous Environment," *Cornell CS Technical Report TR*, 2000.

[40] K. Papagiannaki, *Provisioning IP Backbone Networks Based on Measurements*. PhD thesis, Department of Computer Science, University College London, Londres, Inglaterra, 2003.

[41] M. E. Crovella and M. S. Taqqu, "Estimating the Heavy Tail Index from Scaling Properties," *Methodology and Computing in Applied Probability*, vol. 1, pp. 55–79, julho 1999.

[42] R. Mahajan, S. Floyd, and D. Wetherall, "Controlling High-Bandwidth Flows at the Congested Router," in *Proceedings of 9th International Conference on Network Protocols*, novembro 2001.

[43] H. Martin, A. McGregor, and J. Cleary, "Analysis of Internet Delay Times," in *Proceedings of Passive and Active Measurements workshop*, (Hamilton, Nova Zelândia), pp. 141–148, abril 2000.

[44] V. P. Yin Zhang, Lee Breslau and S. Shenker, "On the Characteristics and Origins of Internet Flow Rates," *Proceedings of ACM SIGCOMM*, pp. 309–322, agosto 2002.

[45] R. S. Cahn, *Wide Area Network Design*. Morgan Kaufmann Publishers, 1998.

[46] M. Schwartz, *Computer Communication Network Design and Analysis*. Prentice Hall, 1 ed., 1977.

[47] A. Markopoulou, F. Tobagi, and M. Karam, "Assessment of VoIP Quality Over Internet Backbones," in *IEEE INFOCOM 2002*, (New York, NY, EUA), pp. 150–159, junho 2002.

[48] "Rede Rio." http://www.rederio.br/, último acesso em 25/03/2005.

[49] Embratel, "Embratel." http://www.embratel.net.br, Último acesso em 25/03/2005.

[50] RNP, "Rede Nacional de Ensino e Pesquisa." http://www.rnp.br/, Último acesso em 5/2/2006.

[51] S. Sen and J. Wang, "Analyzing Peer-To-Peer Traffic Across Large Networks," in *IEEE/ACM Transactions on Networking*, vol. 12, pp. 219–232, abril 2004.

[52] N. M. Markovich, "High Quantile Estimation for Heavy-tailed Distributions," *Performance Evaluation*, vol. 62, pp. 178–192, agosto 2005.

Apêndice A

Probabilidade - Alguns Conceitos e Definições Utilizados no Texto

As teorias científicas lidam com conceitos que tentam expressar a realidade da melhor forma possível. Todos os resultados teóricos são derivados de certos axiomas feitos por deduções lógicas. As pessoas muitas vezes são céticas em relação a validade de um resultado probabilístico. Acredita-se que que as leis físicas descrevem os fatos de forma determinística e a interpretação probabilística é necessária somente devido a nossa ignorância em alguns assuntos. No entanto, a diferença deveria ser vista não na natureza de um ou outro fenômeno, mas nas quantidades que o observador está interessado. Caso ele esteja interessado no resultado de um experimento, então o relato é determinístico; no entanto, se ele está interessado em médias de um grande número de experimentos, então o relato será probabilístico. Em ambos os casos, nenhum acerto categórico é possível. No primeiro caso, as conclusões serão feitas com alguma margem de erro e em alguns intervalos específicos de um parâmetro. Já no segundo caso, a conclusão terá um alto grau de certeza, desde que o número de experimentos seja grande o suficiente.

Neste trabalho, o intuito é propor uma metodologia que utilize mecanismos probabilísticos para se poder caracterizar o tráfego de rede de uma forma acurada. A seguir será feito uma breve descrição dos conceitos utilizados.

A.1 Média

A média representa o valor da tendência central do conjunto de dados amostrados. Essa representação não reflete claramente as características do conjunto de dados, mas apenas indica sua tendência central. A média de um conjunto de dados amostrado é definida como:

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i, \tag{A.1}$$

onde n é o número de experimentos e x a variável que se deseja saber a média.

A.2 Mediana

A mediana M, é uma medida de localização do centro da distribuição dos dados. Ordenados os elementos da amostra, a mediana é o valor (pertencente ou não à amostra) que a divide ao meio, isto é, 50% dos elementos da amostra são menores ou iguais à mediana e os outros 50% são maiores ou iguais à mediana

Para a sua determinação utiliza-se a seguinte regra, depois de ordenada a amostra de n elementos, se n é ímpar, a mediana é o elemento médio (exatamente no meio das duas metades), caso n seja par, a mediana é a média dos dois elementos médios.

A.3 Moda

A moda m representa o valor que surge com mais freqüência dentro da amostra. Esta medida é especialmente útil para reduzir a informação de um conjunto de dados qualitativos, apresentados sob a forma de nomes ou categorias, para os quais não se pode calcular a média e por vezes a mediana.

A.4 Variância

A variância s^2 é utilizada para representar a dipersão dos valores da amostra em relação ao valor médio $\overline{x}$. A equação A.2 mostra como se calcular o valor da variância:

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2, \tag{A.2}$$

onde x_i é a variável que está sendo medida, $\overline{x}$ é a média e n é o número total de experimentos.

A dimensão obtida pelo cálculo de s^2 não tem interpretação direta, uma vez que representa o quadrado da dimensão da variável x. Para se obter uma melhor interpretação do índice de dispersão utiliza-se o desvio padrão s, que é a raiz quadrada da variância, como mostrado abaixo:

$$s = \sqrt{s^2}. \tag{A.3}$$

A.5 Coeficiente de Variação

Muitas vezes, dependendo da ordem de grandeza da variável medida, é necessário saber se o desvio padrão calculado é grande ou pequeno. Esta questão é relevante, por exemplo, na avaliação da precisão de métodos.

Eliminando a influência da ordem de grandeza da variável, a variabilidade dos dados pode ser expressa através do coeficiente de variação, definido por:

$$C.V. = \frac{s}{\overline{x}}. \tag{A.4}$$

Desta forma, quanto menor o $C.V.$, mais homogênio é o conjunto de dados.

A.6 Simetria

É possível avaliar o histograma de freqüências de uma amostra em relação a sua simetria, podendo o histograma ser assimétrico para esquerda, simétrico ou

assimétrico para direita. Um gráfigo assimétrico possui os valores da média ($\overline{x}$), mediana e moda diferentes. Quando o gráfico for assimétrico para direita, a seguinte propriedade pode ser observada: $\overline{x} < M < m$. E quando assimétrico para esquerda, $m < M < \overline{x}$.

Matematicamente, a assimetria pode ser definada como:

$$a = \frac{\sum_{i=1}^{n} (x_i - \overline{x})^3 / n}{s^3} \tag{A.5}$$

Quando $a > 0$, o gráfigo será assimétrico para direita, e quando $a < 0$, será assimétrico para esquerda. Finalmente, se $a = 0$, o gráfico será simétrico.

A.7 Coeficiente de Correlação

O coeficiente de correlação é definido como o valor normalizado da covariância, e indica o grau de associação entre duas variáveis. Duas variáveis são ditas correlacionadas se mudanças em uma variável estão associadas em mudanças na outra variável. O sinal (+ ou -) indica a direção do relacionamento. Seu valor pode variar entre -1 e +1, onde +1 indica um relacionamento positivo perfeito, 0 indica nenhum relacionamento, e -1 indica um relacionamento negativo perfeito (ou uma relação reversa). O coeficiente de correlação é definido como:

$$R_{x,y} = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{s^2(x)}\sqrt{s^2(y)}}, \tag{A.6}$$

onde x_i e y_i são as variáveis cujas correlações se deseja calcular, $\sqrt{s^2}$ é o desvio padrão e n é o número total de amostras.

A.8 Distribuição Cumulativa

A distribuição cumulativa é definida como a probabilidade da variável aleatória X ser menor ou igual que x:

$$F_X(x) = P\{X \leq x\}. \tag{A.7}$$

A.9 Distribuição de Cauda Pesada

Nos últimos anos, uma nova e importante direção foi desenvolvida para a avaliação de desempenho na computação: o estudo de distribuições de cauda pesada (*heavy-tailed*). De uma forma geral, sua "cauda" descreve uma lei de potência com expoente pequeno, em contraste com distribuições tradicionais (ex. gaussiana, exponencial, Poisson) em que a cauda decai exponencialmente. No final dos anos 80 e início dos anos 90, experimentos mostraram evidências que o tráfego de rede, em alguns casos, possuía distribuições de cauda pesada [34, 37, 52].

A definição de distribuições de cauda pesada pode ser feita da seguinte forma: seja X uma variável aleatória com distribuição cumulativa $F(x) = P\{X \leq x\}$. É dito que $F(x)$ possui cauda pesada se:

$$F(x) = 1 - cx^{-\alpha}, \quad 0 < \alpha < 2, \tag{A.8}$$

onde c é uma constante.

Na prática, variáveis aleatórias que seguem distribuições de cauda pesada são caracterizadas por possuírem muitos valores pequenos e alguns poucos valores grandes. Neste tipo de distribuição, a maioria das observações é de pequenos valores, mas a maior contribuição para a média e variância é causada pelos raros (porém grandes) valores observados. Uma maneira de visualizar este tipo de distribuição é imaginar um copo onde foram colocadas diversas bolas de gude e onde, logo em seguida, os espaços vazios foram preenchidos com areia. Neste exemplo, o espaço ocupado por um único grão de areia é bem menor do que o espaço ocupado por uma bola de gude, mas o volume total ocupado por cada um dos dois constituintes é aproximadamente o mesmo. Portanto, neste tipo de comportamento deve-se tomar cuidado ao se "otimizar o caso comum".

A distribuição de Pareto é um exemplo de uma distribuição cuja característica de cauda pesada depende de seus parâmetros. Ela é definida pela integral da função $f(x)$ com relação a x,

$$F(x) = \int_b^x f(x)dx = 1 - (b/x)^a, \tag{A.9}$$

onde

$$f(x) = \frac{ab^a}{x^{a+1}}. \tag{A.10}$$

É fácil mostrar que a média dessa distribuição é

$$\overline{x} = \int_b^\infty f(x)xdx = \frac{ab^a}{(-a+1)} * x^{-a+1}\Big|_b^\infty, \tag{A.11}$$

enquanto a variância σ^2 é dada por

$$\sigma^2 = \overline{x^2} - \overline{x}^2, \tag{A.12}$$

onde

$$\overline{x^2} = \int_b^\infty f(x)x^2dx = \frac{ab^a}{(-a+2)} * x^{-a+2}\Big|_b^\infty. \tag{A.13}$$

É fácil notar que, se $a < 1$, a média tende para o infinito e, no caso de $a < 2$, a variância também tende para o infinito.