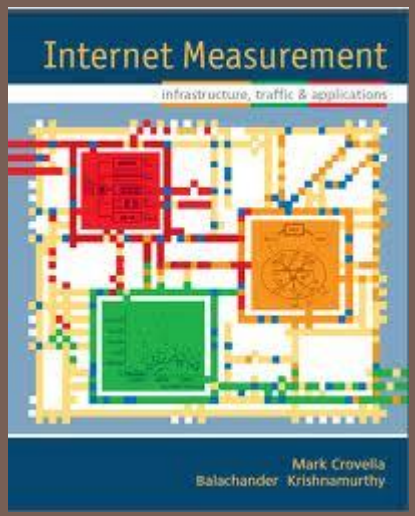


TRÁFEGO

Capítulo 6

Crovella, M, Krishnamurthy, B. Internet Measurement: infrastructure, traffic & applications. John Wiley & Sons, 2006.

Introdução

- Neste capítulo descreveremos:
  - As propriedades do tráfego que são importantes entender e medir
  - Os desafios encontrados na medição do tráfego
  - As ferramentas disponíveis para as medições de tráfego
  - Os resultados mais importantes em relação às propriedades do tráfego da Internet

Introdução

- A medição e a modelagem de tráfego são importantes para a:
  - Análise de desempenho: requer medições de tráfego acuradas de modo a construir modelos úteis para responder questões relacionadas a vazão, perda de pacotes e atraso de pacotes induzida por elementos de rede.
    - Escala de tempo de microssegundos a dezenas de minutos
  - Engenharia de tráfego: configuração de rede, planejamento de capacidades, previsão de demanda, melhoria na operação da rede.
    - Escala de tempo de minutos a anos.

Roteiro

- Propriedades
- Desafios
- Ferramentas
- Estado da Arte

Propriedades

Propriedades

- Nesta seção são examinadas as propriedades do tráfego da Internet que pode ser importante para as medições.
- Todo o tráfego da Internet pode ser visto ao nível do IP simplesmente como uma coleção de *pacotes*.

O Básico: Pacotes e Bytes

- Como podemos resumir o tráfego observado em um determinado ponto (ex. uma das extremidades de um link)?
  - Podemos considerar apenas aqueles instantes de tempo em que os pacotes chegam ao nosso ponto de observação: $\{A_n, n = 0,1, \dots\}$
    - Este conjunto de instantes de tempo pode ser modelado como um processo de chegada.
    - Uma sumarização simples de um processo de chegada consiste da caracterização da distribuição e talvez as propriedades de mais alta ordem dos intervalos entre chegadas:
      - $\{I_n, n = 0,1, \dots\}$ onde $I_n \equiv A_n - A_{n-1}$.

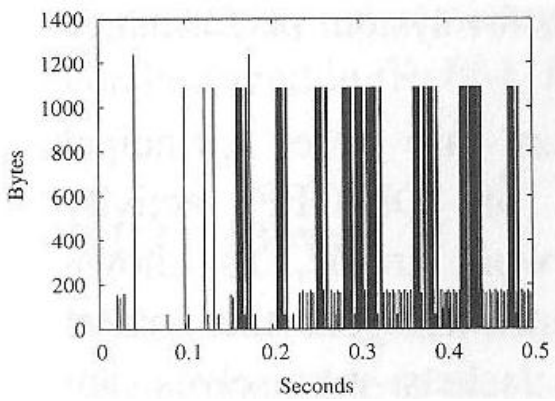
O Básico: Pacotes e Bytes

- Em alguns casos o esforço para coletar os detalhes dos instantes de chegada podem não valer a pena.
  - Nestes casos pode ser usada a série temporal da contagem do tráfego em alguma escala de tempo T.
  - Para um intervalo de tempo fixo T, isto leva a:
    - $\{C_n, n = 0,1, \ldots\}$ onde $C_n \equiv \#\{A_m | nT < A_m \leq (n+1)T\}$
    - Novamente, este série temporal de contagens pode ser resumida aproximadamente através da sua distribuição e propriedades de mais alta ordem.

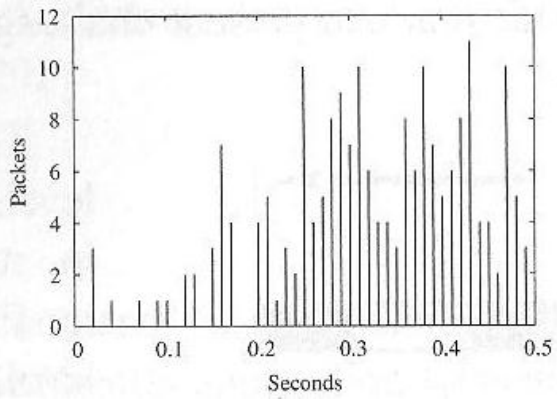
O Básico: Pacotes e Bytes

- Número de bytes:
  - É diferente da contagem de pacotes pois estes têm tamanhos variáveis.
  - Contagem do número de bytes por intervalo de tempo fixo T:
    - $\{B_n, n = 0,1, \ldots\}$ onde $B_n \equiv \sum_{nT<A_m\leq(n+1)T} \text{size}(A_m)$
      - Onde $\text{size}(t)$ é o tamanho do pacote que chega no instante t
        - Inclui também os bytes dos cabeçalhos relevantes.

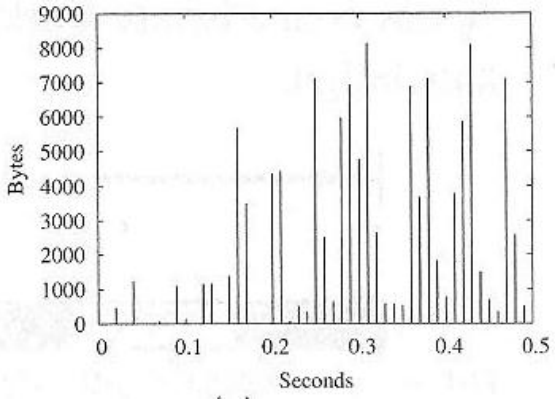
Três Visões do Tráfego



Instantes de chegada (A_n) e o comprimento associado de cada pacote correspondente (size(A_n)).



Série temporal da contagem de pacotes (C_n), para um intervalo $T = 0{,}01$ seg.



Série temporal da contagem de bytes (B_n), para o mesmo intervalo $T = 0{,}01$ seg.

O Básico: Pacotes e Bytes

- A série temporal da contagem de bytes é a medida mais comumente usada da carga representada pelo tráfego
  - Dado que captura a quantidade de largura de banda consumida à medida que os pacotes passam através dos roteadores e dos links.
- A série temporal da contagem de pacotes é útil para entender a carga gerada pelo tráfego a cada pacote, tais como as consultas a endereços realizadas pelos roteadores.

O Básico: Pacotes e Bytes

- Como os pacotes têm tamanhos variáveis, pode ser interessante a distribuição dos tamanhos dos pacotes encontrados, que é útil para o projeto de roteadores.
- Caso sejam feitas medições de tráfego e todos os links da rede simultaneamente, as séries temporais de contagem B_n e C_n se tornariam séries temporais com múltiplas variáveis $\vec{B}_n$ e $\vec{C}_n$ com dimensão igual ao número de pontos de observação.

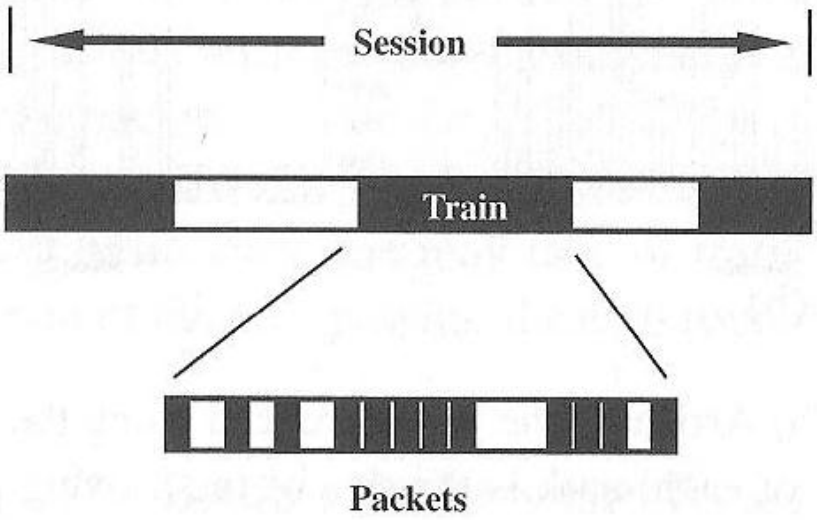
Estrutura de Nível mais Alto

- Há uma estrutura considerável no tráfego que é imposta pelos *protocolos de transporte* e em última análise pelos geradores do tráfego de rede, ou seja, as *aplicações*.
- A compreensão desta estrutura pode ajudar-nos a interpretar as propriedades observadas do tráfego da rede
- E também, podemos aprender sobre os protocolos de alto nível e as aplicações que geram o tráfego de rede examinando esta estrutura.

Processos ON/OFF

- Podemos descrever a estrutura do tráfego como o resultado de uma coleção de processos ON/OFF
- Um processo ON/OFF é um processo que alterna entre um estado ‘on’ no qual gera atividade de tráfego e um estado ‘off’ no qual permanece em silêncio.
- Os processos ON/OFF geram cargas de trabalho explosivas que apresentam desafios à análise e projeto de sistemas.

Níveis de Atividade



- Os próprios pacotes formam um processo ON/OFF: transmissão de pacotes ou silêncio no link de comunicação.
- Trens de pacotes: coleção de pacotes com baixos intervalos entre pacotes.
  - Pode ser estabelecido um limiar para determinar se o pacote pertence ou não a um mesmo trem de pacotes.
- Uma sessão corresponde a uma mesma execução de uma aplicação, que normalmente possui um início e um fim.

Fluxos

- Um fluxo é compreendido aqui como a coleção de todos os pacotes associados com a troca de dados entre dois pontos terminais
  - Com a finalidade de tarifação, modelagem e sumarização do tráfego.
- A RFC 3917 (IPFIX – *IP Flow Information Export*) define um fluxo como um conjunto de pacotes que passam por um ponto de observação durante um certo intervalo de tempo, com todos os pacotes tendo um conjunto comum de propriedades.
  - Estas propriedades podem ser baseadas nos conteúdos dos campos do cabeçalho do pacote, características do próprio pacote (tal como rótulo de camada 2), ou como o pacote é processado (o endereço IP da próxima etapa ou a interface de saída).

Fluxos IP

- Um conjunto de pacotes identificados pelos seus endereços de origem e destino ou qualquer outra função dos campos dos seus cabeçalhos IP ou de transporte.
- Existem estruturas de trem de pacotes dentro de fluxos IP entre sistemas finais individuais definidos por seus endereços IP.
- Os fluxos IP podem ser definidos em uma variedade de níveis de agregação.
  - Podem ser agregados por porta, protocolo, endereço ou combinações destes.
  - A agregação de endereços pode ser feita em diversos níveis por prefixo, no qual todos os endereços IP que pertencem a um dado prefixo são alocados ao mesmo fluxo.

Fluxos Definidos pela Rede

- Fluxos são frequentemente definidos em relação a uma carga de rede particular.
- Para uma rede na qual o roteamento não esteja sendo mudado, uma definição importante de fluxo corresponde aos pontos de entrada e saída:
  - Fluxo origem-destino ou fluxo entrada-saída (*ingress-egress*)
  - Se mudar o roteamento este fluxo também muda.

Fluxos Definidos pela Rede

- Dadas as contagens de bytes (ou pacotes) de fluxos origem destino $\vec{B}_{(f)}$ e uma matriz de roteamento $A = G^T$, a contagem correspondente nos links é dada por $\vec{B}_{(l)} = A\vec{B}_{(f)}$.
- O conjunto completo de fluxos origem-destino na rede é chamado de *matriz de tráfego*
- E o mapeamento de fluxos a caminhos na rede é chamado de *matriz de caminhos*
- Dado que podem haver múltiplas rotas para um prefixo de destino, um conjunto de pacotes destinados a um ponto terminal comum pode ter múltiplos pontos de saída de uma rede.
  - O conjunto de fluxos origem-destino a qualquer instante são a realização de demandas ponto a multiponto determinadas pelas políticas de roteamento

Tipos de Tráfegos Distintos Semanticamente

- Tráfego de Dados
- Tráfego de Controle
  - Formado por pacotes que implementam os protocolos de roteamento (BGP, OSPF, IS-IS), pacotes de medição (SNMP) e pacotes de controle genéricos (ICMP).
  - A medição deste tráfego pode ser de interesse para reproduzi-lo em simulações ou porque refletem o desempenho do sistema de roteamento.
- Tráfego Malicioso:
  - Será estudado no Capítulo 9.

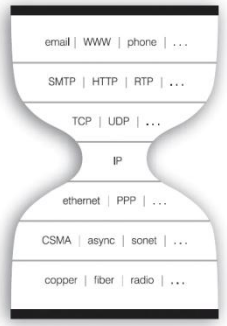
Desafios

Questões Práticas

- Observabilidade:
  - Simplicidade do núcleo: a ênfase na simplicidade das funções do roteador levou a um falta de observabilidade em muitos pontos da rede.
    - Fluxos: como os roteadores não precisam manter informações de estado por fluxo e
      - As capacitações de monitoração de fluxos levaram tempo e outras questões levaram a uma dificuldade na intepretação das medições.
    - Pacotes: normalmente não está disponível a captura de pacotes na rede.
      - A captura de pacotes é geralmente implementada em sistemas finais ou por um hardware adicionado à rede.

Questões Práticas

- Observabilidade:
  - Interconexão Distribuída:
    - Não há mais um único *backbone* e não há uma rede que proveja um ponto de medição conveniente para a maioria do tráfego da rede.
    - Cada ponto de medição apresenta uma visão local da rede e das propriedades de tráfego que podem não ser representativas de outros pontos de medição.
  - A Ampulheta IP:
    - A corrupção de pacotes, atrasos e perdas na camada física podem ser mascaradas por retransmissões na camada de enlace ou FEC.
    - Estas propriedades de tráfego em geral não são visíveis quando as medições são realizadas na camada IP ou acima.



Questões Práticas

- Volume de Dados:
  - Com o crescimento da largura de banda dos links, a captura completa de um pacote se torna um desafio para processar, armazenar e gerenciar.
  - O processamento dos dados deve ser realizado por algoritmos eficientes.
  - O armazenamento deve ser realizado num meio local ao link que está sendo monitorado (normalmente em um disco dedicado).
  - Se os dados tiverem que ser deslocados para um outro local para processamento, o momento e a taxa de transferência devem ser escolhidos cuidadosamente.

Questões Práticas

- Volume de Dados (cont.):
  - A captura completa de pacotes em links de alta velocidade é apropriada apenas em pequenas escalas de tempo (um minuto ou menos).
    - Com amostragem ou sumarização pode ser viável escalar a dias, especialmente se forem calculados resumos dos fluxos.
  - Outros problemas:
    - Para estender o período de armazenagem, frequentemente são armazenados apenas os cabeçalhos dos pacotes. O que frustra análises que dependeriam do conteúdo dos pacotes.
    - Podemos perder dados por conta de *overflow* de buffers.
    - O conjunto resultante de dados é armazenado e processado em formatos não padronizados.

Questões Práticas

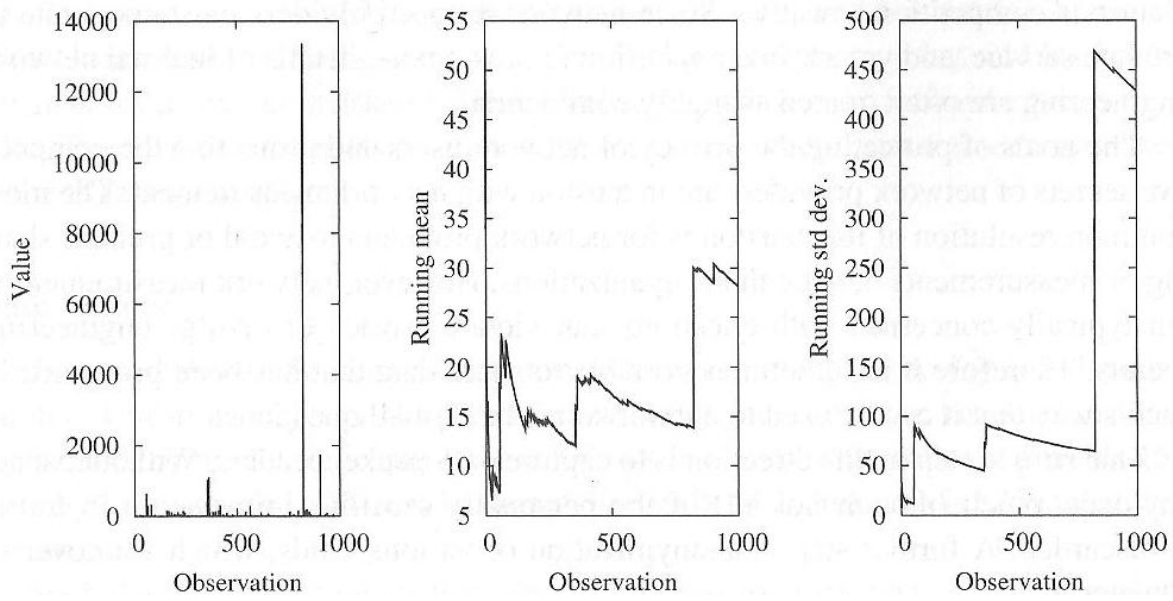
- Compartilhamento dos Dados:
  - As medições contêm dados altamente sensíveis:
    - A captura completa de pacotes registra a atividade dos usuários da rede.
      - Estes registros podem ser usados para extrair informações tais como sites Web visitados, senhas, e conteúdos de mensagens trocadas.
    - Mesmo quando as medições não forem muito detalhadas, mesmo assim podem fornecer informações sobre a configuração e o funcionamento da rede que está sendo monitorada.
      - Identidade ou natureza dos parceiros do provedor, usuários, pontos de interconexão e políticas de roteamento de tráfego.
      - Algumas destas informações são sensíveis à competição.

Questões Práticas

- Compartilhamento dos Dados (cont.):
  - Tensão entre manter a privacidade dos usuários e as medições da rede.
  - A solução mais comum é a proibição por parte dos provedores de rede do compartilhamento de medições fora de suas organizações.
  - Às vezes é possível compartilhar dados que tenham sido processados de uma tal forma que possam ser usadas para responder algumas embora nem todas as questões.
    - Por exemplo, podem ser capturados apenas os cabeçalhos dos pacotes.
    - Há também diversas formas de anonimização que serão cobertas no Capítulo 8.

Dificuldades Estatísticas

- Caudas Longas e Alta Variabilidade:
  - Instabilidade das métricas:
    - Instabilidade de resumos tradicionais estatísticos, particularmente a média e a variância da amostra.



Dificuldades Estatísticas

- Caudas Longas e Alta Variabilidade:
  - Dificuldade de Modelagem:
    - Pode ser difícil escolher o melhor modelo probabilístico para descrever dados altamente variáveis.
    - Alguns conjuntos de dados mostram uma faixa de apenas três ou quatro ordens de magnitude. Ou seja, a cauda é medida apenas numa pequena faixa de valores.
    - As diferenças entre as distribuições de Pareto e lognormal podem ser muito pequenas quando a nossa atenção está restrita a um faixa limitada de valores.
      - Como resultado, pesquisadores olhando para conjuntos de dados ligeiramente diferentes e usando métodos ligeiramente diferentes podem chegar a resultados bem diferentes sobre a presença da lei de potência na cauda do conjunto de dados.

Dificuldades Estatísticas

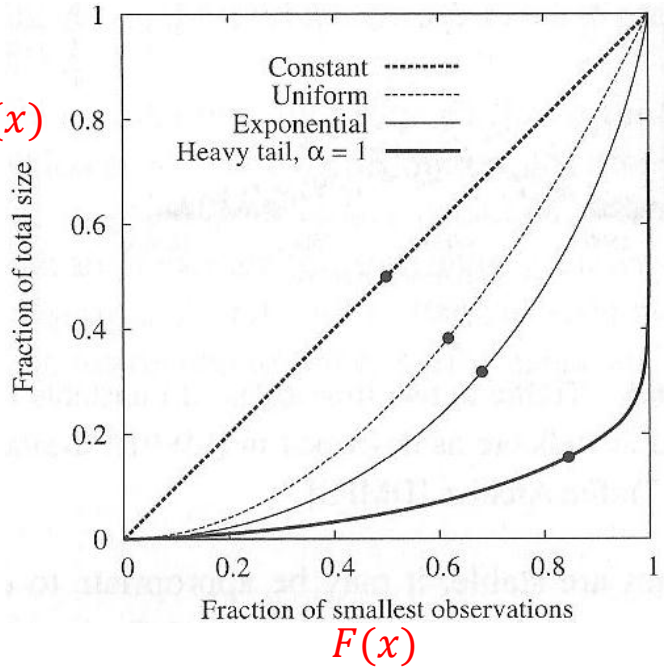
- Caudas Longas e Alta Variabilidade:
  - Intuição Confusa:
    - Ao trabalhar com modelos de cauda pesada é importante ter presente certas propriedades estatísticas que diferem do que é normalmente esperado:
      - Taxa de falhas declinante: $E[X|X > k] \sim k$ quando X é uma v.a. com cauda pesada e k é grande o suficiente para estar na cauda.
        - Quanto mais tivermos esperado por um evento, mais tempo deveremos esperar.
        - O normal seria quanto mais tempo tivéssemos esperado, menos tempo fôssemos esperar.

Dificuldades Estatísticas

- Caudas Longas e Alta Variabilidade:
  - Intuição Confusa:
    - Disparidade entre a contagem e o tamanho dos objetos em uma amostra:
      - A maioria dos comprimentos medidos em um conjunto de observações está concentrada em um pequeno subconjunto das observações.
      - A forma da cauda superior da distribuição de uma soma de v.a.s é determinada apenas pelo valor máximo da soma:
        - $\lim_{x\to\infty} \frac{P[X_1+\cdots+X_n>x]}{P[\max(X_1,\ldots,X_n)>x]} = 1$ para todo $n \geq 2$

Dificuldades Estatísticas

- Caudas Longas e Alta Variabilidade:
  - Intuição Confusa:
    - Disparidade entre a contagem e o tamanho dos objetos em uma amostra:
      - Função distribuição do tamanho ponderado:
        - $F_w(x) = \frac{\int_{-\infty}^{x} u dF(u)}{\int_{-\infty}^{\infty} v dF(v)}$
      - Que pode ser comparada com $F(x)$
        - Vide figura ao lado.
      - Fenômenos dos “elefantes” e dos “ratos” que será discutido na Seção 6.4.

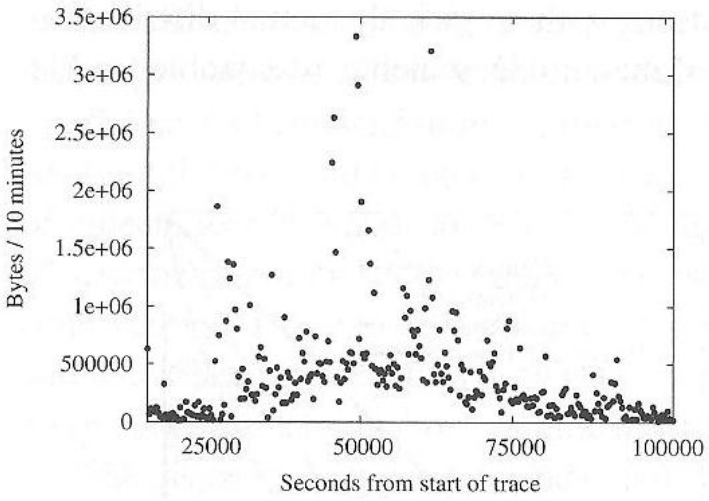


Dificuldades Estatísticas

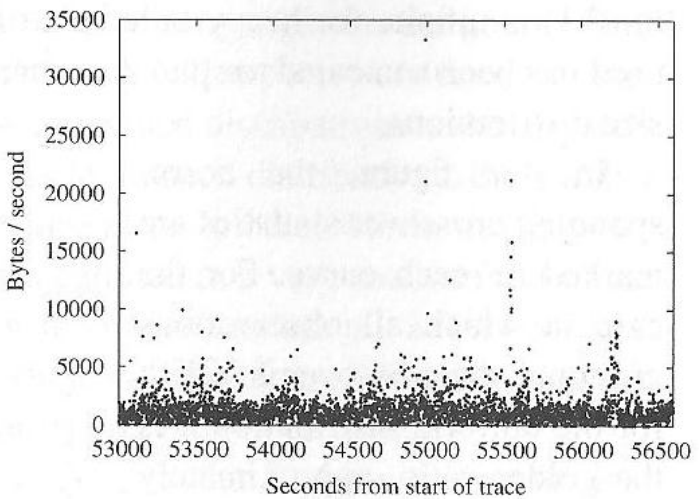
- Estacionariedade e Estabilidade:
  - Estabilidade refere à consistência das propriedades do tráfego ao longo do tempo.
  - Estacionariedade é uma propriedade formal de um processo estocástico.
  - Quando as propriedades de medição são estáveis, pode ser apropriado descrever as medições usando um modelo estacionário.
  - Muitas propriedades de tráfego podem ser instáveis em algumas escalas de tempo e estáveis em outras escalas de tempo.

Dificuldades Estatísticas

- Estacionariedade e Estabilidade:
  - Tráfego em duas escalas de tempo:



Instável (24 horas)



Estável (1 hora)

Dificuldades Estatísticas

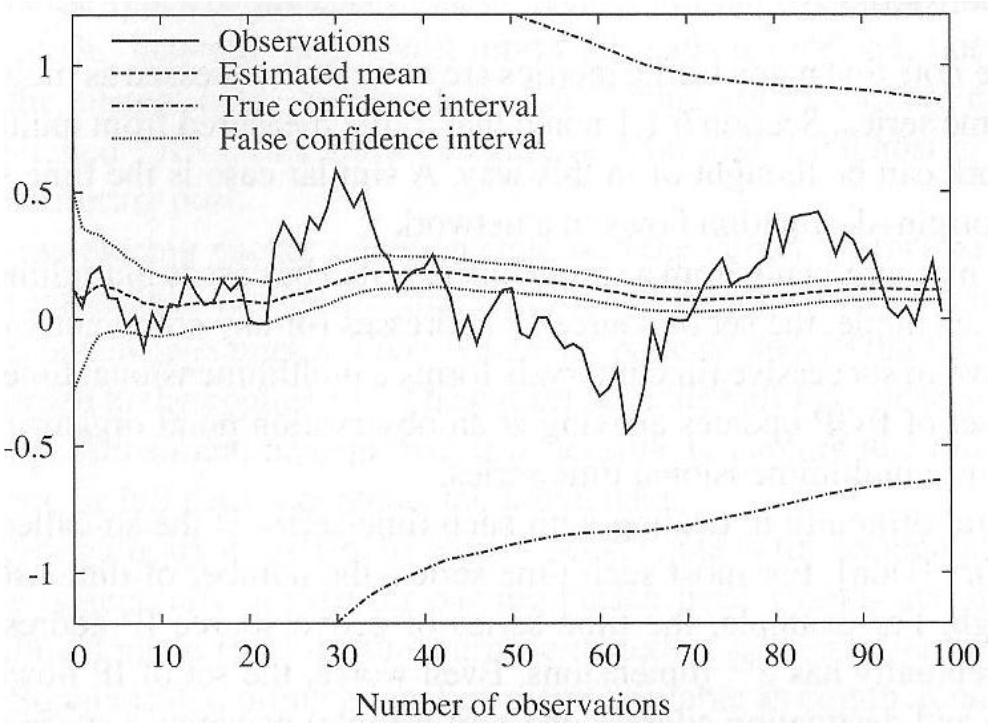
- Estacionariedade e Estabilidade:
  - Medições de tráfego em escalas de tempo mais grosseiras (ex. contagens SNMP a cada 5 minutos) tendem a obscurecer as explosões de tráfego que são importantes par a análise de desempenho.
  - Escalas de tempo mais finas exigirão técnicas mais difíceis tais como captura de pacotes mas podem dar uma melhor compreensão sobre questões relacionadas com o desempenho de roteadores e perda de pacotes.

Dificuldades Estatísticas

- Autocorrelação e Memória no Comportamento do Sistema:
  - As redes e sistemas finais exibem memória pois contêm buffers e algoritmos de controle que mantêm a história passada de um modo que afeta o comportamento atual.
  - A memória do sistema torna o futuro próximo mais previsível. No entanto, ela também reduz a quantidade de informação que é obtida pela medição.
    - Por isto os intervalos de confiança deverão ser mais largos do que se não houvesse memória.
    - E se os calcularmos usando as fórmulas que assumem independência entre as observações, os ICs serão incorretamente menores, levando a uma falsa sensação de precisão dos resultados.

Dificuldades Estatísticas

- Autocorrelação e Memória no Comportamento do Sistema:
  - Efeitos da autocorrelação nos intervalos de confiança:



Dificuldades Estatísticas

- Autocorrelação e Memória no Comportamento do Sistema:
  - Memória devida a atrasos de enfileiramento:
    - Para uma fila M/M/1 a variância assintótica é dada por:
      - $s^2 \approx \frac{4\rho^2}{(1-\rho)^4}$
      - Onde ρ é a utilização da fila (taxa de chegadas vezes o tempo médio de serviço).
      - Podemos perceber que a variância cresce com o crescimento da carga e é bastante sensível à mesma como pode ser visto pela potência de 4 no denominador.

Dificuldades Estatísticas

- Alta dimensionalidade:
  - Muitas métricas de tráfego são expressas naturalmente como séries temporais multidimensionais.
  - Exemplos:
    - Tráfego medido em diversos pontos da rede (já apresentado)
    - Conjunto dos endereços IP de origem (ou qualquer combinação de campos do cabeçalho IP)
  - Dificuldade principal: o número de dimensões envolvidas é muito alto:
    - Os endereços IP têm 2^{32} dimensões
    - O conjunto de fluxos IP possui $2^{32} \times 2^{32} \times 2^{16} \times 2^{16}$

Dificuldades Estatísticas

- Alta dimensionalidade:
  - Tende a prevenir uma fácil visualização dos dados e complica a modelagem e análise dos dados.
    - A visualização é difícil após três dimensões
    - Extrair resumos úteis de dados altamente dimensionais é difícil porque a caracterização acurada dos relacionamentos entre as D dimensões pode requerer no caso geral um número de medições exponencial em D.

Ferramentas

Roteiro

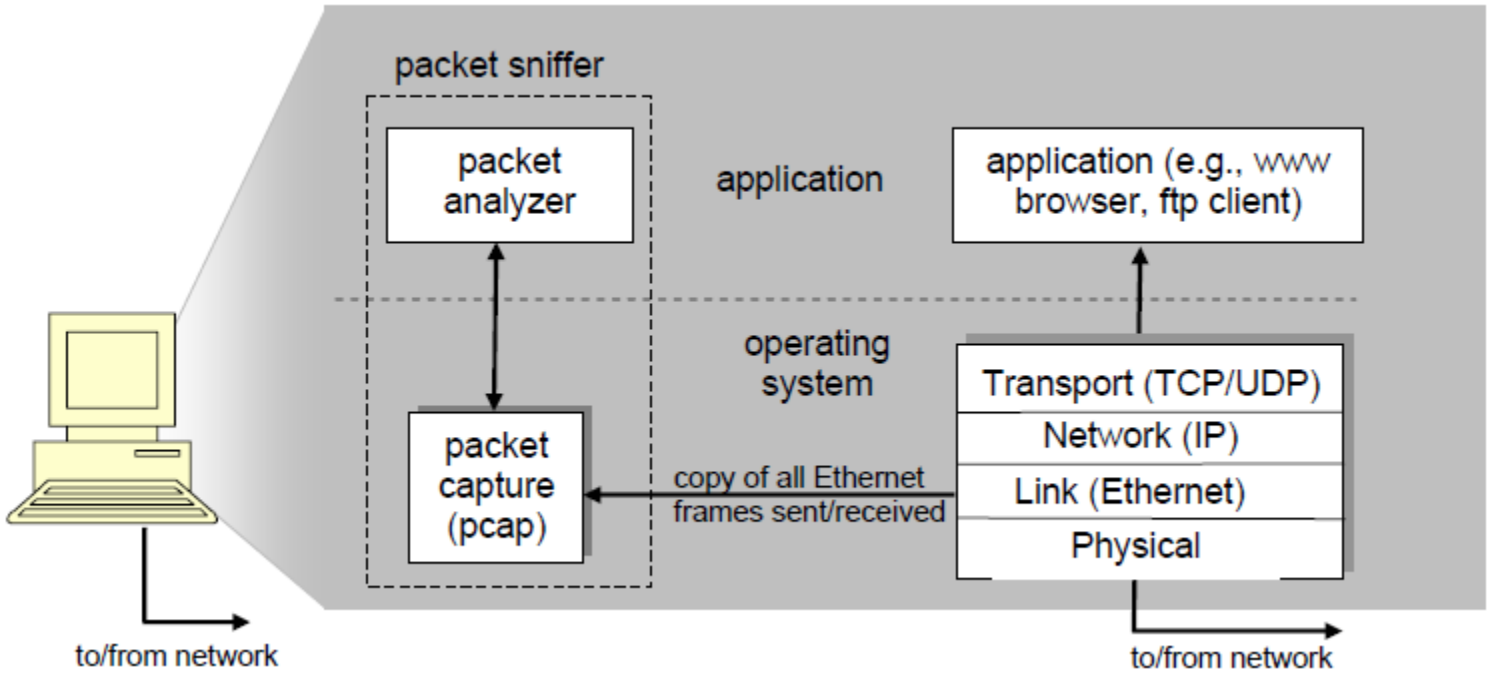
- Captura de Pacotes
- Gerenciamento dos Dados
- Redução dos Dados
- Inferência

Captura de Pacotes

- Medição de tráfego *passiva*.
- Captura de Pacotes em Sistemas de Propósito Geral:
  - API mais comum: `libpcap`
    - Uma interface pode ser colocada em modo *promíscuo* capturando todos os pacotes recebidos (mesmo que não sejam destinados a esta interface).
    - Em LANs de difusão são capturados todos os pacotes transmitidos.
    - Em LANs comutadas podem ser capturados todo o tráfego se este *host* estiver conectado a uma porta de monitoração do *switch*.

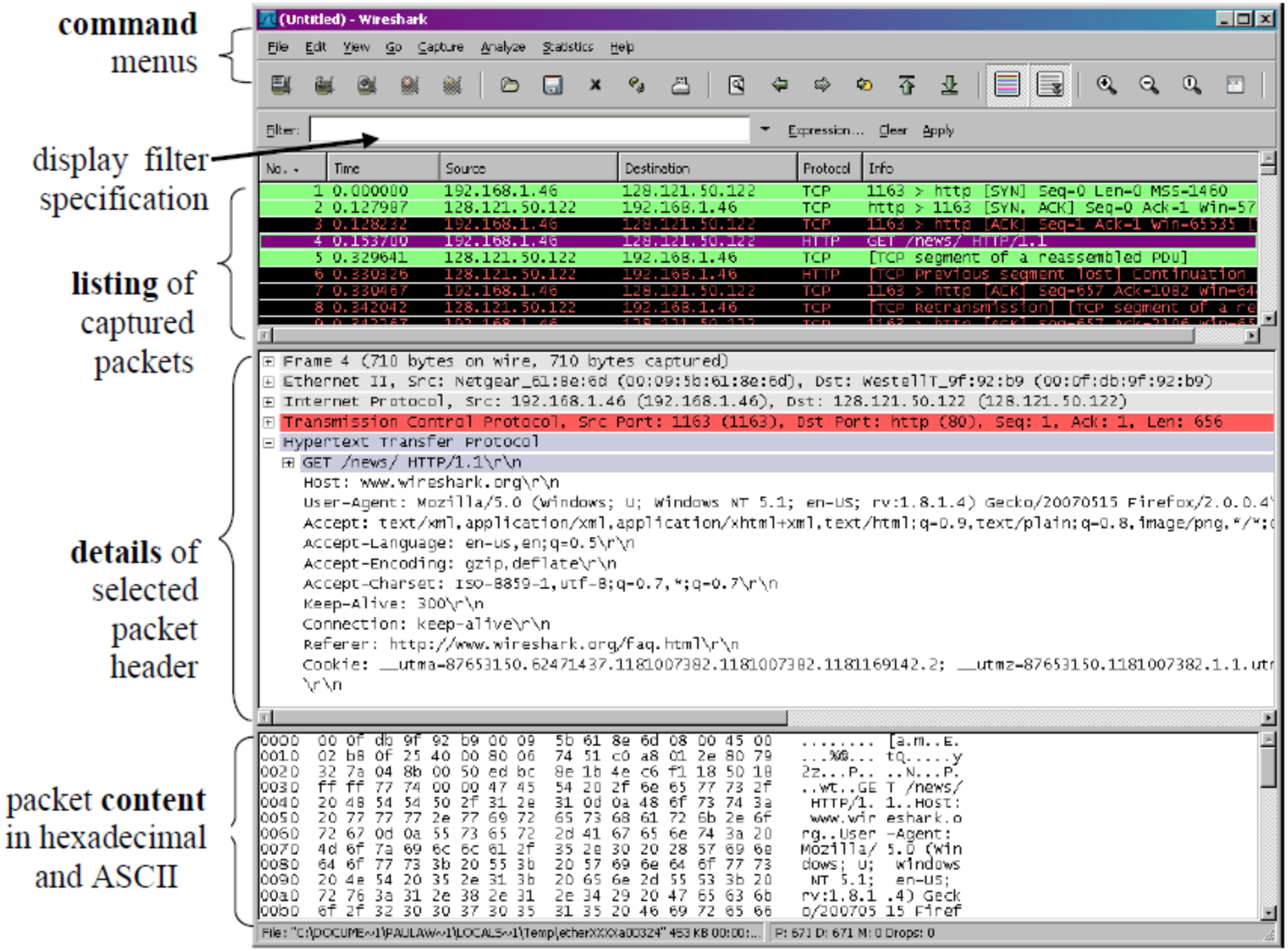
Captura de Pacotes

- Captura de Pacotes em Sistemas de Propósito Geral:
  - API mais comum: `libpcap`



Captura de Pacotes

- Captura de Pacotes em Sistemas de Propósito Geral:
  - Softwares de interpretação dos pacotes capturados por protocolos:
    - Tcpdump: http://www.tcpdump.org/
    - Wireshark: http://www.wireshark.org/
  - Ferramentas que permitem que usuários não privilegiados possam capturar e injetar pacotes:
    - Pktd (http://www.icir.org/vern/papers/pktd-pam03.pdf)
    - Scriptroute (http://www.cs.umd.edu/~nspring/scriptroute.html)


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.1.46 128.121.50.122 TCP 1163 > http [SYN] Seq=0 Len=0 MSS=1460
2 0.127987 128.121.50.122 192.168.1.46 TCP http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
3 0.128232 192.168.1.46 128.121.50.122 TCP 1163 > http [ACK] Seq=1 Ack=1 Win=65535
4 0.153700 192.168.1.46 128.121.50.122 HTTP GET /news/ HTTP/1.1
5 0.329641 128.121.50.122 192.168.1.46 TCP [TCP segment of a reassembled PDU]
6 0.330326 128.121.50.122 192.168.1.46 HTTP [TCP Previous segment lost] Continuation
7 0.330467 192.168.1.46 128.121.50.122 TCP 1163 > http [ACK] Seq=657 Ack=1082 Win=64
8 0.342042 128.121.50.122 192.168.1.46 TCP [TCP Retransmission] [TCP segment of a re
Frame 4 (710 bytes on wire, 710 bytes captured)
Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
Hypertext Transfer Protocol
GET /news/ HTTP/1.1\r\n
Host: www.wireshark.org\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
Referer: http://www.wireshark.org/faq.html\r\n
Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
\r\n
0000 00 0f db 9f 92 b9 00 09 5b 61 8e 6d 08 00 45 00 .... [a.m..E.
0010 02 b8 0f 25 40 00 80 06 74 51 c0 a8 01 2e 80 79 ...%@... tQ.....y
0020 32 7a 04 8b 00 50 ed bc 8e 1b 4e c6 f1 18 50 18 2z...P.. ..N...P.
0030 ff ff 77 74 00 00 47 45 54 20 2f 6e 65 77 73 2f ..wt..GE T /news/
0040 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host:
0050 20 77 77 77 2e 77 69 72 65 73 68 61 72 6b 2e 6f www.wir eshark.o
0060 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 rg..User -Agent:
0070 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win
0080 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 dows; U; Windows
0090 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b 20 NT 5.1; en-US;
00a0 72 76 3a 31 2e 38 2e 31 2e 34 29 20 47 65 63 6b rv:1.8.1 .4) Geck
00b0 6f 2f 32 30 30 37 30 35 31 35 20 46 69 72 65 66 o/200705 15 Firef
File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXa00324" 453 KB 00:00:...
P: 671 D: 671 M: 0 Drops: 0

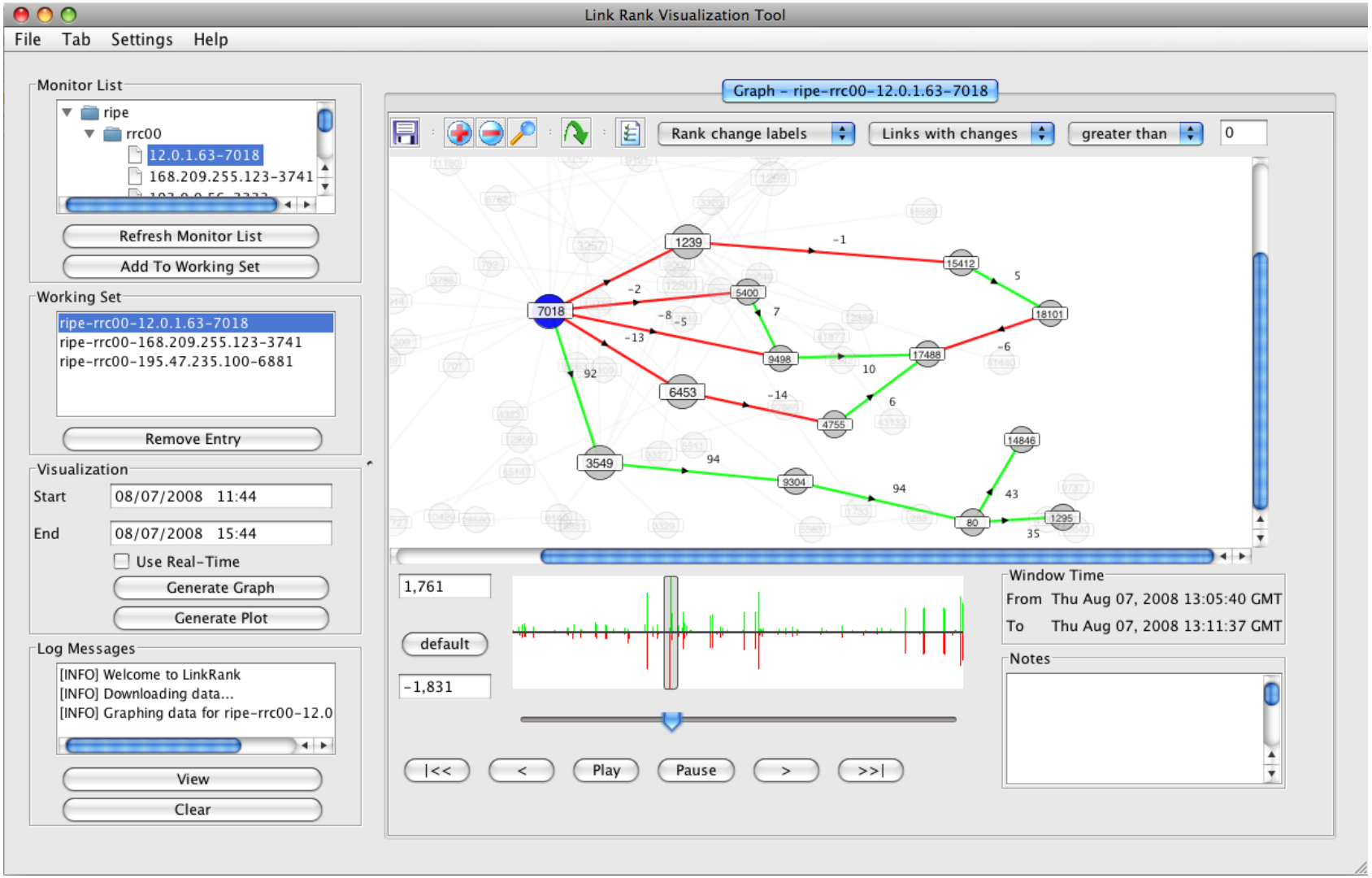
Captura de Pacotes

- Captura de Pacotes por Sistemas Específicos:
  - Placas e Servidores especializados para a captura de pacotes em links de alta velocidade (10 Gbps e brevemente 100 Gbps sem perdas).
    - Endace: www.endace.com
    - CoralReef: http://www.caida.org/tools/measurement/coralreef/hardware.xml

Captura de Pacotes

- Tráfego do Plano de Controle:
  - Pode ser capturado participando diretamente na comunicação do plano de controle.
    - Ex.: troca de mensagens de roteamento.
  - Obtenção de visão local do sistema BGP (ou OSPF):
    - Registrar para receber atualizações BGP estabelecendo uma sessão com um roteador que fale BGP.
    - Um PC padrão pode ser configurado com software para falar BGP:
      - Quagga software: http://www.nongnu.org/quagga/
    - Coleção de tráfego BGP:
      - http://www.routeviews.org/

Ferramenta de Visualização



Gerenciamento dos Dados

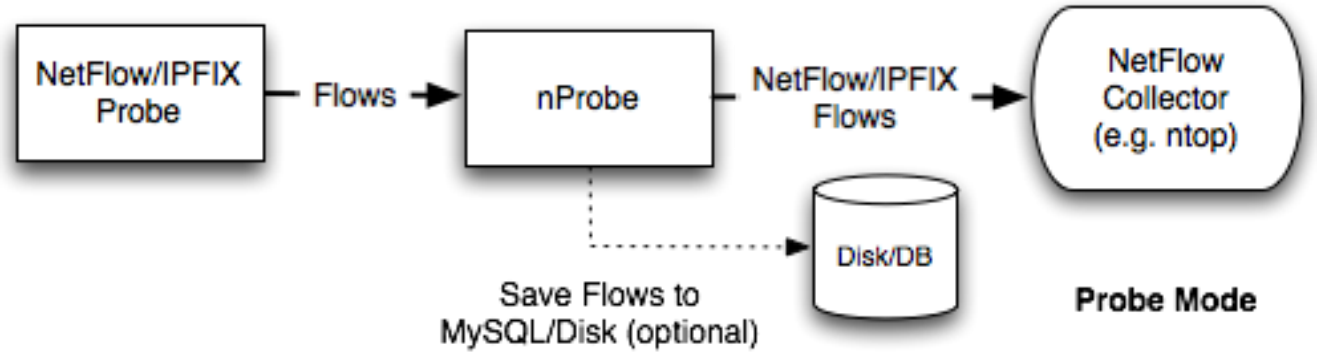
- A captura e armazenamento de pacotes completos pode ser bem desafiadora.
  - E a dificuldade cresce com o aumento da velocidade dos links
- Estes desafios são criados pela largura de banda limitada dos barramentos assim como a velocidade de acesso à memória dos PCs de uso geral, além de limites nas velocidades e capacidades dos discos.
- Mesmo quando conseguimos capturá-los, o seu tamanho imenso pode tornar difícil a análise subsequente e o seu gerenciamento.
- Uma forma de enfrentar estes desafios é através da construção e uso de ferramentas especializadas.
  - Com uso de algoritmos sofisticados para operar com grandes *streams* de dados.

Ferramentas

- SMACQ – *System for Modular Analysis and Continuous Queries* [http://smacq.sourceforge.net/]. Última atualização 06/10/2009.
- Windmill:
  - Sistema focado na medição de desempenho de protocolo.
  - Está organizado em torno de:
    - Um filtro de pacotes para a captura de tráfego
    - Um conjunto de módulos incorporando protocolos Internet para o processamento de pacotes
    - Uma máquina extensível de experimentos.

Ferramentas

- Nprobe [http://www.ntop.org/products/nprobe/]: semelhante à Windmill mas incorporando explicitamente a redução de dados on-line para melhorar a escalabilidade.



Ferramentas

- O sistema FLAME – *An Open Packet Monitoring Architecture* (última atualização: 15/12/02) [http://www.cis.upenn.edu/~dsl/FLAME/index.html]
  - Focado em prover um processamento in-kernel mais extenso.
- Coral Reef:
  - Sistema organizado como um conjunto de ferramentas para ler e processar dados de tráfego em uma variedade de formatos.
  - [http://www.caida.org/tools/measurement/coralreef/]

Ferramentas

- S-net: conjunto de ferramentas que facilitam a análise dos dados dos cabeçalhos de pacotes num pacote estatístico de alto-nível.

Ferramentas

- *Data Stream Management Systems* (DSMS):
  - Tribeca
  - Borealis
    http://www.cs.brown.edu/research/borealis/public/
  - Projetos:
    - STREAMS
    - TelegraphCQ
      - http://telegraph.cs.berkeley.edu/telegraphcq/v0.2/
    - Gigascope (AT&T Labs)
    - GT-BackstreamDB
    - "OML"

Gigascope

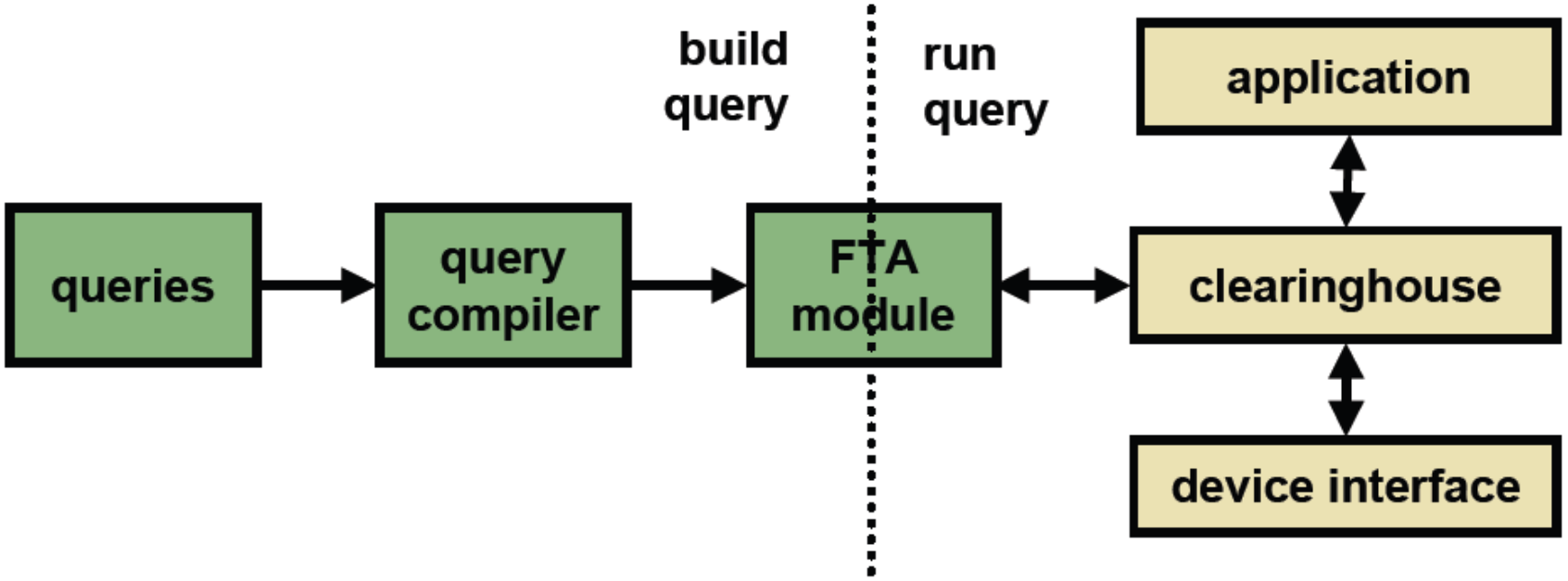
- Sistema de gerenciamento de streams de dados especializado para a análise do tráfego de redes
  - Usado em conjunto com uma captura de pacotes de alto desempenho.
- As consultas são expressas em GSQL que usa uma sintaxe similar à do SQL com algumas extensões e restrições.
  - Uma das restrições é que as operações de blocos devem operar numa janela de tempo de tamanho fixo.

Gigascope: Exemplo de Consulta


```
Select tb, srcIP,  sum(len)
From IPv4
Where protocol=6
Group by time/60 as tb, srcIP
Having count(*)>5
```

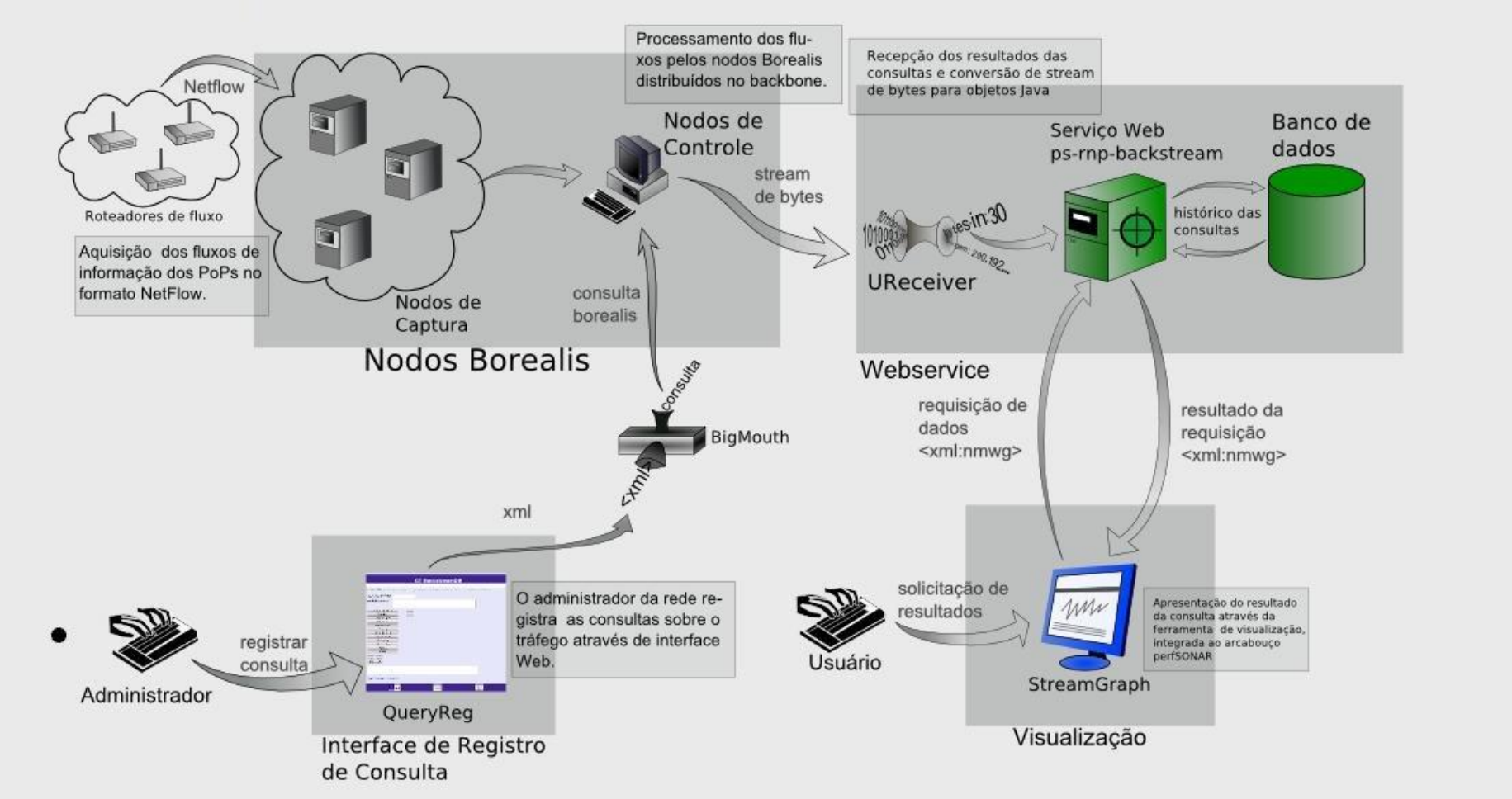
- Esta consulta examina um fluxo de pacotes IPv4 e encontra todos os casos nos quais uma única fonte envia mais do que cinco pacotes numa janela de 60 segundos.

Gigascope



- Compilador de consultas: traduz consultas GSQL para múltiplos módulos FTA (C ou C++)
- Módulo FTA: filtra, transforma e agrega dados de redes.

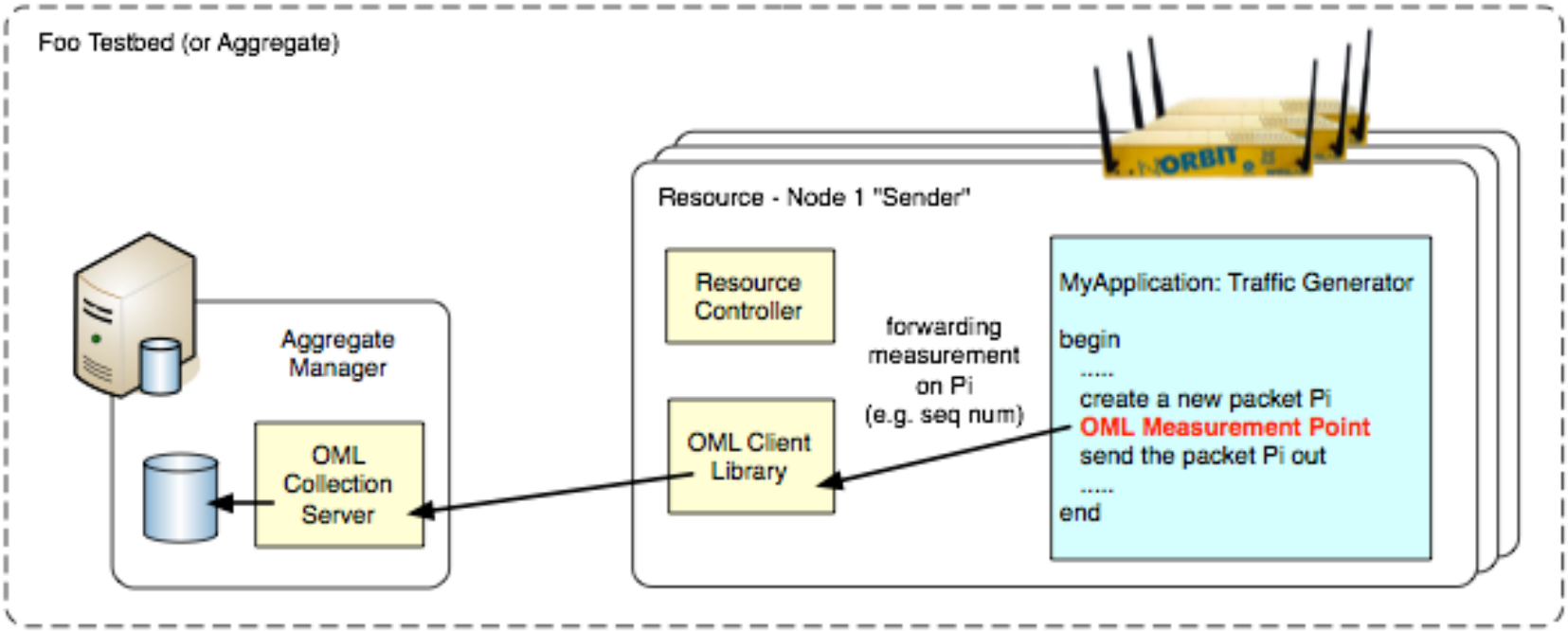
GT BackStreamDB



Fonte: http://backstreamdb.arauc.br/

OML

- *Orbit Measurement Library*



Redução dos Dados

- Redução do volume de dados
- Métodos:
  - Contadores
  - Captura de fluxos
  - Amostragem
  - Sumarização
  - Redução da Dimensionalidade
  - Modelos Probabilísticos

Contadores

- A forma mais comum de resumo dos dados é a agregação para formar séries temporais de estatísticas de tráfego.
  - Ex.: bytes ou pacotes por unidade de tempo.
- Isto é suportado em todos os roteadores atuais através da MIB-II (*Management Information Base*) acessada através do protocolo SNMP.
- Em redes Ethernet estatísticas equivalentes podem ser obtidas através da Base de Informações de Gerenciamento do RMON.

Contadores

- Estas MIBs dão acesso a contagens e, portanto, podem ser criadas séries temporais através da consulta periódica (*polling*) aos mesmos.
  - Estas estatísticas são chamadas genericamente de *contagens SNMP*

Campos na `ifEntry` da MIB-II

- Informações relativas a cada interface (if).

Field Name	Meaning
`ifIndex`	A unique value for each interface
`ifDescr`	A text string including the name of the manufacturer, the product name and the version of the hardware interface
`ifType`	An indication of the link layer technology of the interface
`ifMtu`	The size of the largest datagram which can be sent/received on the interface
`ifSpeed`	An estimate of the interface's current or nominal bandwidth in bits per second
`ifPhysAddress`	The interface's address at the next lower protocol layer, if such a value exists
`ifAdminStatus`	Desired state: "up," "down," or "testing"
`ifOperStatus`	Operational state: "up," "down," or "testing"
`ifLastChange`	The time the interface entered its current operational state
`ifInOctets`	The total number of octets received on the interface, including framing characters
`ifInUcastPkts`	The number of subnetwork-unicast packets delivered to a higher-layer protocol
`ifInNUcastPkts`	The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol

Campos na `ifEntry` da MIB-II

Field Name	Meaning
`ifInDiscards`	The number of non-corrupted inbound packets which were chosen to be discarded (e.g., for lack of buffer space)
`ifInErrors`	The number of corrupted inbound packets
`ifInUnknownProtos`	The number of packets discarded because of an unknown or unsupported protocol
`ifOutOctets`	The total number of octets transmitted out of the interface, including framing characters
`ifOutUcastPkts`	The total number of packets to be transmitted to a unicast address, including those that were discarded or not sent
`ifOutNUcastPkts`	The total number of packets to be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent
`ifOutDiscards`	The number of outbound packets that were chosen to be discarded (e.g., for lack of buffer space)
`ifOutErrors`	The number of outbound packets that could not be transmitted because of errors
`ifOutQLen`	The length of the output packet queue (in packets)
`ifSpecific`	MIB definitions specific to the particular media used on the interface

Contadores SNMP

- Vantagens:
  - Podem ser facilmente capturados sem grandes impactos no desempenho do roteador.
  - Extremamente compacto em relação ao traço de tráfego.
- Desvantagens:
  - Pacotes de medição podem ser perdidos (usa UDP)
  - Difícil realizar medições sincronizadas em múltiplas interfaces na rede
  - Resolução muito baixa para alguns usos.

Captura de Fluxos

- Os contadores apesar de representar a informação básica de atividade da rede, perdem quase toda a semântica do tráfego.
- Alternativa: captura de *trens de pacotes* ou *fluxos*.

Conteúdo de Um Registro de Trem de Pacotes

- 5-tupla do Cabeçalho do Pacote:
  - Endereço IP da origem
  - Porta TCP ou UDP de origem
  - Endereço IP do destino
  - Porta de destino
  - Identificação do protocolo
- Instante de início
- Instante de fim
- Número de pacotes
- Número de bytes

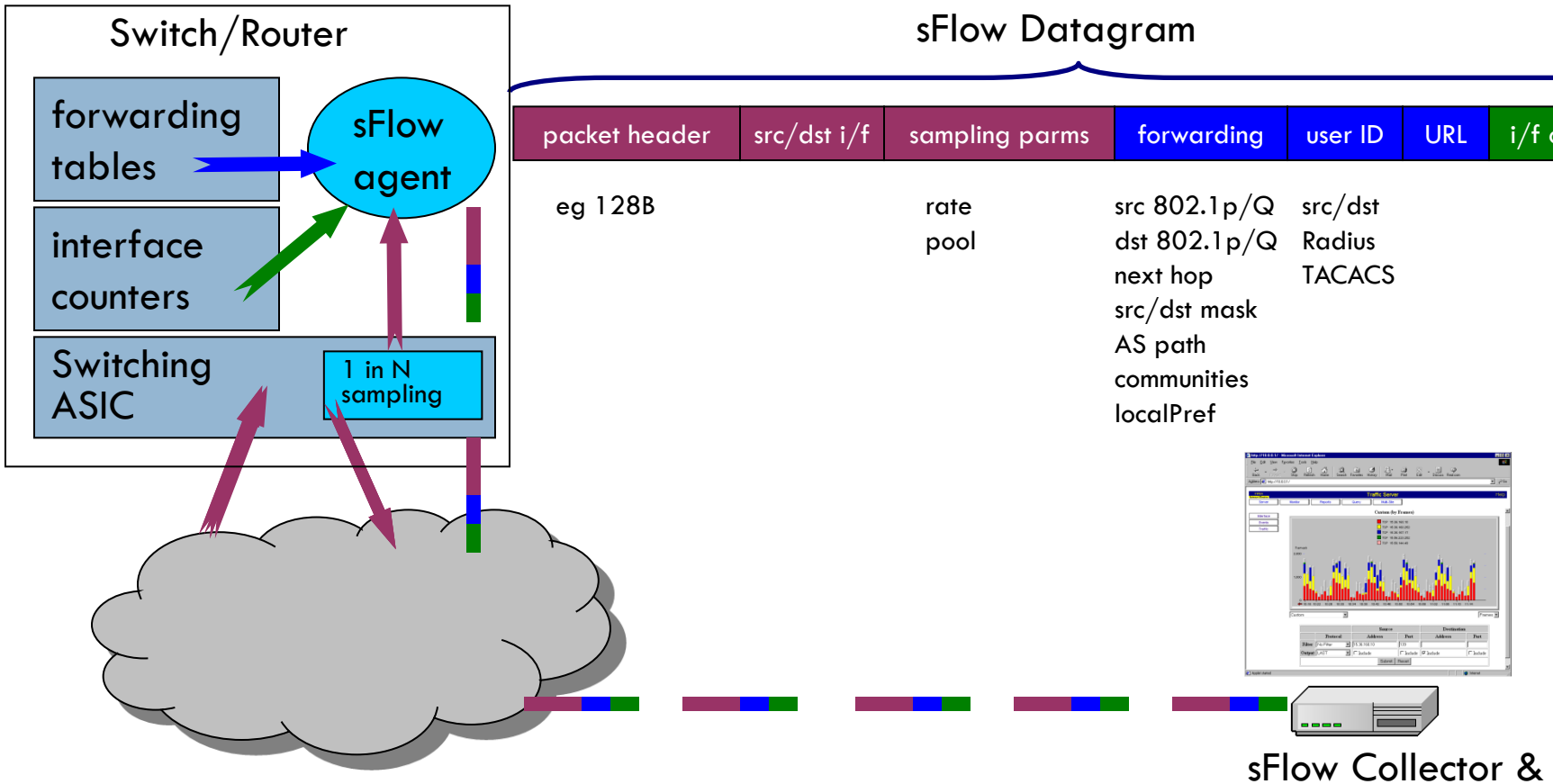
Trem de Pacotes

- Vantagem:
  - Redução drástica no tamanho do traço (1,5% para o Netflow)
- Desvantagem:
  - Definição do fim de um trem de pacotes
  - Critérios variados:
    - Limiar do intervalo de tempo entre pacotes
    - Limiar aplicado a todo o comprimento do fluxo
    - Observação de um segmento de FIN ou RST
    - Decisão de retomar a memória no roteador
  - Esta diversidade pode resultar na identificação incorreta de conexões TCP.

Fluxos de Pacotes

- Em alguns casos não é necessário conhecer os instantes de início e de fim dos trens de pacotes.
  - Basta o número de bytes ou pacotes que contém um determinado valor para a 5-tupla em um dado intervalo de tempo.
  - Isto corresponde a capturar fluxos de pacotes ao invés de trens de pacotes
- Embora muitos roteadores e switches possam exportar algum tipo de registro de fluxos, normalmente são necessários software de alto-nível para processar e interpretar os dados brutos.

sFlow em operação



http://www.sflow.org

Fluxos de Pacotes

- Flowtools:
  - Conjunto de ferramentas que podem coletar, enviar, processar e gerar relatórios a partir de dados do Netflow (Cisco) ou cflowd (Juniper)
  - http://code.google.com/p/flow-tools/
- IPFIX (Próximo slide)

- Lista de ferramentas de processamento de fluxos:
  - http://www.switch.ch/network/projects/completed/TF-NGN/floma/software.html

IPFIX: IP *Flow Information Export*

- Definido na RFC 3917
- Um fluxo consiste de todos os pacotes que satisfazem todas as propriedades definidas para o fluxo:
  - Um ou mais campos do cabeçalho do pacote (endereço IP destino), do protocolo de transporte (número da porta de destino) ou da aplicação;
  - Uma ou mais características do próprio pacote;
  - Um ou mais campos derivados do tratamento do pacote (próxima etapa, interface de saída, etc.)
- A arquitetura especifica padrões para os *exportadores* e para os coletores.
- Implementado nos pacotes `ntop` e `flowtools`

RTFM – *Real Time Flow Metering*

- Conjunto antigo de padrões (1999) para o relato de fluxos.
- A arquitetura RTFM define:
  - Uma MIB para o medidor que pode ser acessada via SNMP
  - Leitores (*meter readers*) que coletam fluxos de dados e
  - Gerentes que coordenam os medidores e os leitores.
- Foi implementada na ferramenta NeTraMet
  - http://www.caida.org/tools/measurement/netramet/

Amostragem

- É escolhido um subconjunto dos pacotes para a captura (ex.: 1%).
- Questões importantes:
  - Como os pacotes devem ser escolhidos?
  - Como deve-se compensar ou corrigir os dados ao se efetuar as análises para levar em consideração o efeito das amostragens?

Amostragem Básica de Pacotes

- O processo de amostragem é executado de forma independente em cada link que está sendo monitorado.
- Taxa constante ou variável de amostragem.
- Taxa Constante:
  - Amostragem aleatória: os pacotes são escolhidos para amostragem de acordo com alguma probabilidade fixa $0 < p < 1$.
  - Amostragem determinística: os pacotes são escolhidos periodicamente, i.e, é escolhido sempre o N-ésimo pacote.
  - Amostragem estratificada: o processo de amostragem é dividido em múltiplos passos. Os pacotes são primeiro divididos em subconjuntos e depois a amostragem é aplicada dentro de cada subconjunto.

Amostragens aleatória e determinística

- Em muitos casos as diferenças entre amostragem aleatória e determinística pode ser irrelevante.
- A diferença entre os dois métodos tende a diminuir para links com alto nível de multiplexação, no qual estão entremeados pacotes de muitos fluxos.

Efeito da Amostragem

- Quando os pacotes são amostrados a uma taxa constante, é possível estimar com uma razoável acurácia o número real de pacotes ou bytes, multiplicando a contagem correspondente pela taxa de amostragem.
- No entanto, outras estatísticas não são tão facilmente obtidas.
  - Por exemplo, é mais fácil aparecer trens de pacotes mais longos do que os mais curtos. Portanto, estimativas acuradas do número total de trens e seus comprimentos não são obtidos simplesmente pela ampliação das estatísticas correspondentes!

Métodos para Atacar estes Problemas

- Explorar os detalhes a nível dos protocolos reportados nos registros de fluxo
  - Por exemplo a observação de um “pacote” SYN
- Amostragem estratificada ao nível dos trens de pacotes.

Métodos para Atacar estes Problemas

- *Sample and hold*: explora a disparidade da contagem do tamanho dos trens de pacotes.
  - Os pacotes são amostrados com uma probabilidade fixa.
  - Cada pacote de um fluxo que não tinha sido visto antes dispara a criação de uma nova entrada.
  - Em seguida, *todos* os pacotes daquele fluxo são amostrados e para cada um destes pacotes é atualizada a entrada correspondente na tabela de fluxos.
  - Isto resulta numa contagem precisa do número de pacotes para aqueles fluxos que são amostrados.
    - Certamente os fluxos com um grande volume de dados serão amostrados
    - Faz utilização de uma quantidade menor de espaço, contabilizando a maior parte deles.

Precisão

- Em geral, a acurácia das estatísticas obtidas através da amostragem de tráfego depende da taxa de amostragem e, portanto, da quantidade de memória e recursos de processamento alocados à amostragem.
- Taxas variáveis de amostragem foram desenvolvidas para enfrentar as limitações em acurácia, desempenho e consumo de recursos.

Amostragem da Trajetória

- Se fizermos amostragens em diferentes pontos da rede, muito provavelmente selecionaremos pacotes distintos.
  - Impedindo a medição de atrasos por pacote e a medição de fluxo através da rede.
- Neste método um pacote que for escolhido por amostragem em qualquer ponto da rede, será escolhido em todos os pontos da rede.

Amostragem da Trajetória

- Implementação:
  - Os dispositivos de medição de tráfego (ex. roteadores) calculam uma função de *hash* para cada pacote em função dos valores de alguns campos do cabeçalho.
    - Os campos usados são apenas aqueles que não se alteram quando o pacote se move na rede e que sejam suficientes para identificar o pacote.
  - O dispositivo de medição seleciona um pacote para reportar se o valor do *hash* estiver numa determinada faixa.
    - Variando o tamanho desta faixa pode-se variar a taxa de amostragem dos pacotes.

Amostragem da Trajetória

- Implementação:
  - É possível preparar pacotes de modo que eles sejam amostrados e injetá-los na rede, permitindo uma forma combinada de monitoração ativa/passiva.
- Dificuldades:
  - Uso do UDP para relatar as medidas, devido à possível perda dos datagramas.
    - Podem ser usados filtros Bloom.

IETF: PSAMP WG

- PSAMP – *Packet Sampling*
  - Grupo de trabalho do IETF que encerrou seus trabalhos em 2009
  - Produziu 4 RFCs:
    - RFC 5474: *A Framework for Packet Selection and Reporting*
    - RFC 5475: *Sampling and Filtering Techniques for IP Packet Selection*
    - RFC 5476: *Packet Sampling (PSAMP) Protocol Specifications*
    - RFC 5477: *Information Model for Packet Sampling Exports*
  - Incluem tanto a amostragem básica como a de trajetórias.

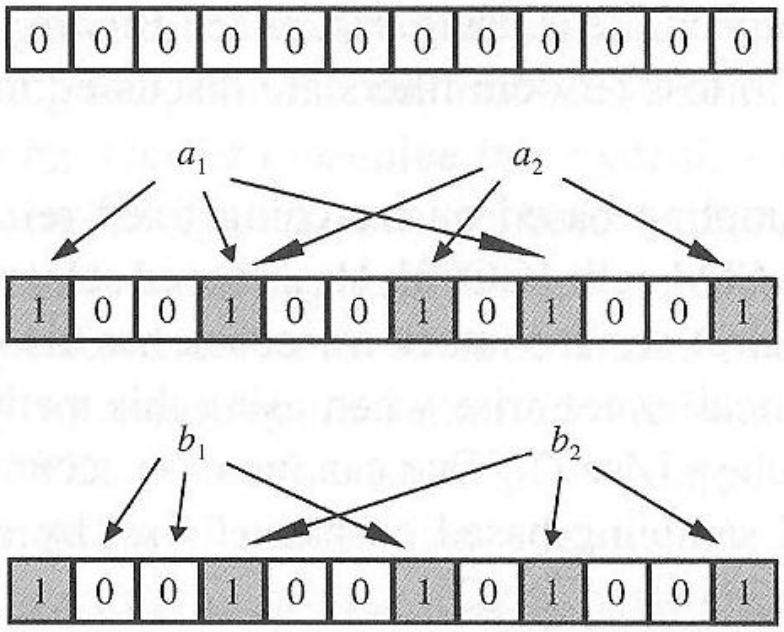
Sumarização

- Outra abordagem para lidar com o grande volume de dados obtidos na medição de tráfego da Internet é através da formação de resumos compactos que sejam úteis para responder questões específicas:
  - Filtros de Bloom
  - *Sketches*
  - Estruturas de dados especializadas

Filtros de Bloom

- É o resumo de um conjunto que suporta consultas de pertencimento.
- Ideia:
  - permitir uma pequena probabilidade de falsos positivos em troca de uma grande redução no espaço de armazenamento necessário.

Filtro de Bloom



- O vetor de bits é inicializado com zeros.

- Cada item do conjunto a_i é *hasheado* k vezes e os bits correspondentes são setados para um.
- Para verificar se um elemento b_i pertence ao conjunto, ele deve ser *hasheado* k vezes e ser verificado se os bits correspondentes estão setados:
  - O elemento b_1 não pertence ao conjunto dado que alguns dos seus bits são zero.
  - Já o elemento b_2 ou pertence ao conjunto ou produziu um falso positivo.

Filtro de Bloom

- Dado um conjunto de chaves $A = \{a_1, a_2, \ldots, a_n\}$
- Um filtro de Bloom fornece uma estrutura de dados e um algoritmo que nos permite perguntar se uma chave a_n está presente no conjunto A.
  - A estrutura de dados é um vetor de m bits
  - O algoritmo está baseado em um conjunto de k funções de *hash* independentes $h_1, h_2, \ldots, h_k$ cada uma com uma faixa de $\{1, \ldots, m\}$.
    - Estas funções são escolhidas de modo a mapear cada item em A a um número aleatório uniforme na faixa $\{1, \ldots, m\}$.

Filtro de Bloom

- Algoritmo:
  - Todos os bits do vetor são inicializados com zeros.
  - Para cada chave $a \in A$, os bits $h_i(a)$ são setados para 1 para $1 \leq i \leq k$.
  - Para verificar se um item b está em A, deve se verificar se todos os bits especificados por $h_i(b)$ estão setados.
    - Se não estiverem então b não é pertence a A
    - Se estiverem assume-se que b pertença a A, embora haja uma possibilidade de que esta conclusão esteja incorreta.
      - O filtro de Bloom produz um *falso positivo* com uma probabilidade que depende dos valores de k, m e n.

Filtro de Bloom: Probabilidade de *falso positivo*

- Depois que todos os elementos de A tiverem registrado no filtro de Bloom, a probabilidade de que um bit escolhido aleatoriamente ainda seja 0 é dada por:
  - $\left(1 - \frac{1}{m}\right)^{kn}$
- Portanto, a probabilidade de que k bits escolhidos aleatoriamente sejam 1 é dada por:
  - $\left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^{k}$ (probabilidade de *falso positivo*)

Filtro de Bloom: Escolha dos parâmetros

- Para minimizar a probabilidade de falsos positivos dados alguns valores de m e n, procuramos o número de função de *hash* que equalizam o número de 1's e 0's no vetor de bits.
  - O número ótimo de funções de *hash* seria então $k = \ln 2 \cdot \left(\frac{m}{n}\right)$
  - Neste caso a taxa de falsos positivos seria
    - $\left(\frac{1}{2}\right)^k \approx (0{,}6185)^{\frac{m}{n}}$
    - No entanto, na prática o k deve ser inteiro, então este desempenho pode não ser alcançado.

Filtros de Bloom

- Permitem uma probabilidade de falso positivos constante usando apenas um número constante de bits por conjunto de elementos.
- Eles não são adequados para armazenar conjuntos cujos membros deixem de pertencer ao conjunto com o tempo, pois o bit pode ser necessário para outro membro.
  - Poderia ser usado um contador no lugar de cada bit. Deste modo a inserção de um membro incrementaria os contadores dos *hashes* correspondentes, e a saída provocaria um decremento dos contadores correspondentes.

Filtros de Bloom: Aplicações

- Resumo do conteúdo de caches Web para facilitar o compartilhamento do conteúdo das mesmas.
- Sistemas p2p
- Roteamento
- Gerenciamento ativo de filas
- Descoberta de topologia

Filtros de Bloom: Filtros Multiestágios

- Existem k vetores de bits de comprimento ℓ,
- E k funções de *hash* que retornam valores em $\{1, \ldots, \ell\}$.
- Cada identificador de fluxo de pacote é *hasheado* k vezes e os contadores correspondentes em cada vetor são incrementados pelo número de bytes no pacote.
- Para a identificação de fluxos intensos, note que se um fluxo que contenha M bytes tiver sido processado, então os contadores correspondentes terão um valor pelo menos igual a M.
  - Portanto, dado algum limiar T escolhido adequadamente, os maiores fluxos são aqueles cujo valor mínimo do contador seja T.

Sketches

- Um filtro multiestágios pode ser visto como um conjunto de projeções aleatórias, no seguinte sentido:
  - Seja x o histograma das contagens de fluxos observados em algum traço.
    - Então x_i é o número de pacotes ou bytes observados por fluxo i, com $1 \leq i \leq n$. Este é um vetor em um espaço de alta dimensões.
  - Podemos então construir uma projeção aleatória de baixa dimensão do seguinte modo:
    - Para $m \ll n$, construa a matriz $m \times n$ P de 0-1, de modo que cada coluna de P tenha um único 1 em uma linha escolhida aleatoriamente.
    - O produto Px será então equivalente a construir um conjunto de contadores do filtro multiestágios.

Sketches

- Projeções aleatórias têm muitas qualidades úteis como resumos de tráfego.
  - Quando usados para responder questões aproximadas sobre grandes conjuntos de dados, as projeções aleatórias para redução de dimensões são chamadas de *sketches*.
- Uma propriedade importante dos *sketches* é que eles são lineares:
  - A soma aritmética de dois *sketches* é o mesmo que o *sketch* da superposição dos dois conjuntos de dados correspondentes.
  - Esta linearidade torna-os particularmente adequados para o processamento através de *wavelets* (ondaletas).

Sketches

- Eles foram propostos como uma ferramenta genérica para abordar uma variedade de problemas incluindo:
  - Compressão de tráfego
  - Detecção de similaridade de tráfego
  - Estimativa dos maiores fluxos (*heavy-hitter*)

Sketches

- Podem ser usados também para detectar mudanças significativas na distribuição de endereços em um fluxo de tráfego.
  - A ideia consiste em usar métodos de séries temporais para prever o valor do *sketch* no próximo intervalo de tempo baseado nos valores passados.
  - A diferença entre a previsão obtida do modelo de série temporal e o valor realmente observado pode ser usado como uma métrica para detectar tráfego anômalo.

Outras Abordagens

- Foram propostas uma variedade de outras estruturas de dados e algoritmos para dar suporte a perguntas específicas sobre fluxos de tráfegos resumidos.

Redução da Dimensionalidade

- Como mencionado anteriormente, os identificadores de fluxo ocupam um espaço com dimensionalidade alta o que complica a análise.
  - No entanto, esta alta dimensionalidade é um artefato da representação do tráfego e não uma propriedade fundamental do mesmo.
  - Deve-se, portanto, buscar uma representação que exponha a verdadeira estrutura (de baixa dimensionalidade) dos dados.
  - Após esta redução a análise fica muito mais simples.
- Abordagens:
  - Clusterização
  - Análise do Componente Principal

Clusterização

- Baseia-se numa *métrica de similaridade* definida no conjunto de características de tráfego.
- Dentro de cada *cluster* as características de tráfego são bem semelhantes, e bem diferentes entre clusters distintos.
  - Dado este conjunto de definições do *cluster*, o tráfego pode ser resumido baseado em seus *clusters* e não em suas características originais.

Clusterização

- Para os cinco campos de cabeçalho geralmente usados para as análises de fluxos:
  - Endereços: a similaridade entre os endereços pode ser expressa pelo agrupamento hierárquico natural de endereços em prefixos.
  - Portas: consideradas similares se forem:
    - Idênticas
    - Alocadas estaticamente ou alocadas dinamicamente
  - Protocolos: se forem idênticos.

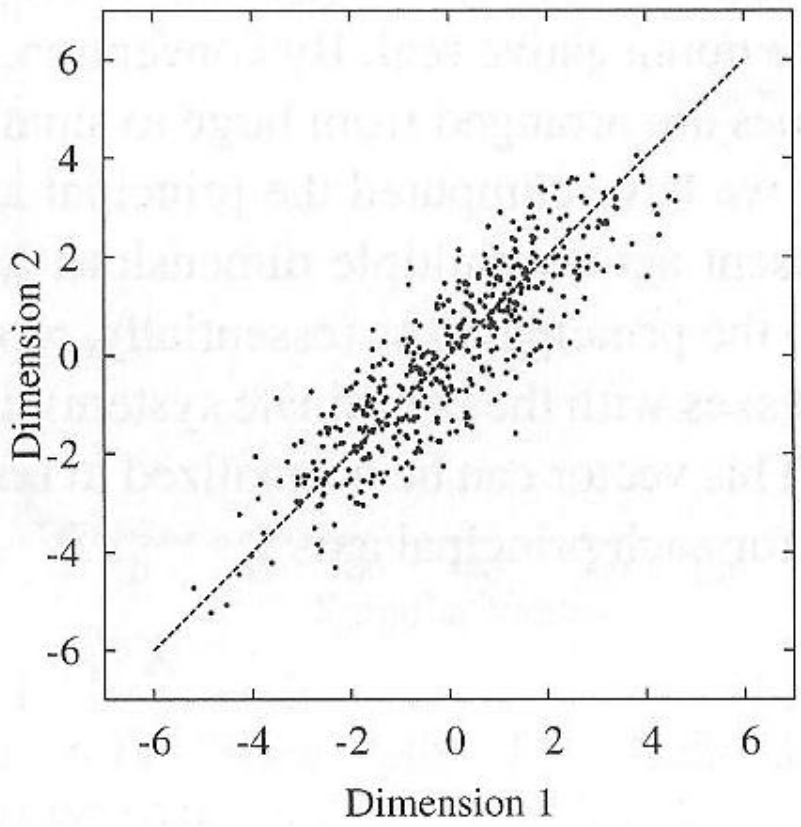
Clusterização

- Pode ser usada, por exemplo, para descobrir como os fluxos estão associados às aplicações.
  - A abordagem óbvia de usar o protocolo IP e o número da porta pode não ser efetivo pois:
    - O HTTP pode ser usado para transportar uma grande variedade de objetos.
    - O mesmo tipo de objeto pode ser transportado por diferentes protocolos (FTP, HTTP)
    - Quando o tráfego está criptografado, o protocolo e os números das portas podem não estar disponíveis.

Análise do Componente Principal

- PCA – *Principal Component Analysis*
- É um método de transformação de coordenadas que mapeia os dados medidos em um novo conjunto de eixos.
  - Estes eixos são chamados de eixos ou componentes principais.
  - Cada componente principal tem a propriedade de apontar na direção da variação máxima restante dos dados, levando em conta a *variação* já considerada nos componentes anteriores.

Análise do Componente Principal



- Ilustração do PCA em um conjunto de dados 2D correlacionado.

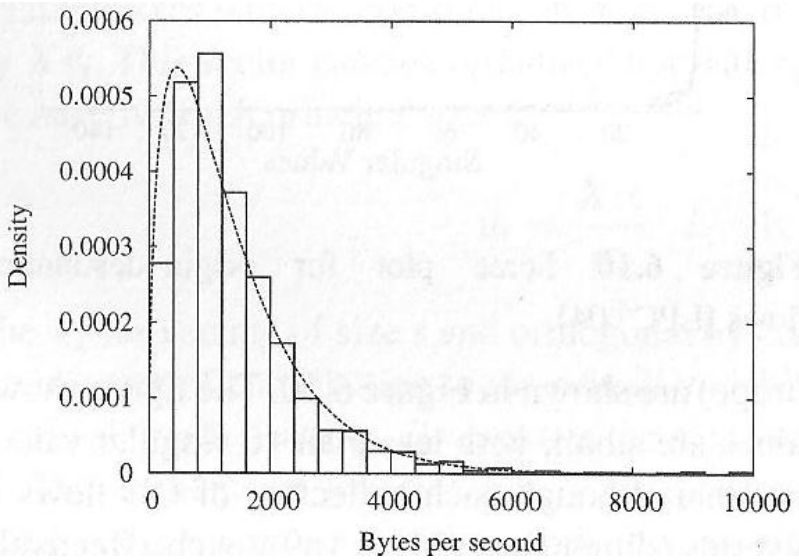
Modelos Probabilísticos

- Resumir os resultados na forma de modelos probabilísticos:
  - Trata as observações como se elas tivessem sido geradas por um processo aleatório.
- Modelos:
  - De Distribuição
  - Estrutura de Dependência

Modelos de Distribuição

- As características de um traço de tráfego pode ser resumido fornecendo a distribuição de probabilidades que casa com a distribuição empírica encontrada.
- São chamados normalmente de modelos analíticos.
- Benefícios do seu uso:
  - Estes modelos podem ser manipulados matematicamente, por exemplo, para cálculo da média, variância, etc.
  - São concisos e facilmente comunicados. Em alguns casos, apenas o tipo da distribuição e dois ou três parâmetros bastam para uma especificação completa.
  - Os valores particulares dos parâmetros do modelo podem dar uma compreensão da natureza dos dados subjacentes.

Modelos de Distribuição

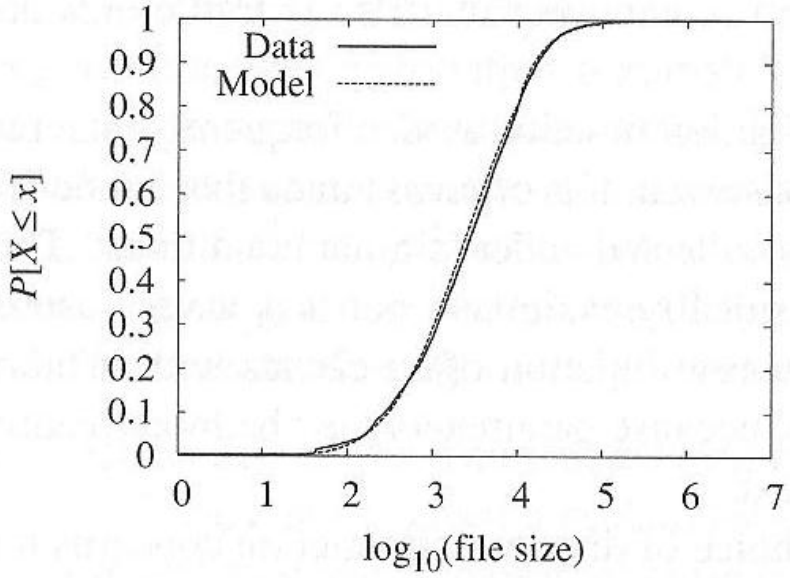


- As barras compõem um histograma da contagem de bytes por segundo, para um traço anterior.
- A curva suave corresponde à distribuição Gama, escolhida por melhor casar com os dados observados.
- A massa de informação presente no traço de tráfego foi reduzido a um pequeno conjunto de parâmetros necessários para especificar uma instância particular da distribuição gama.

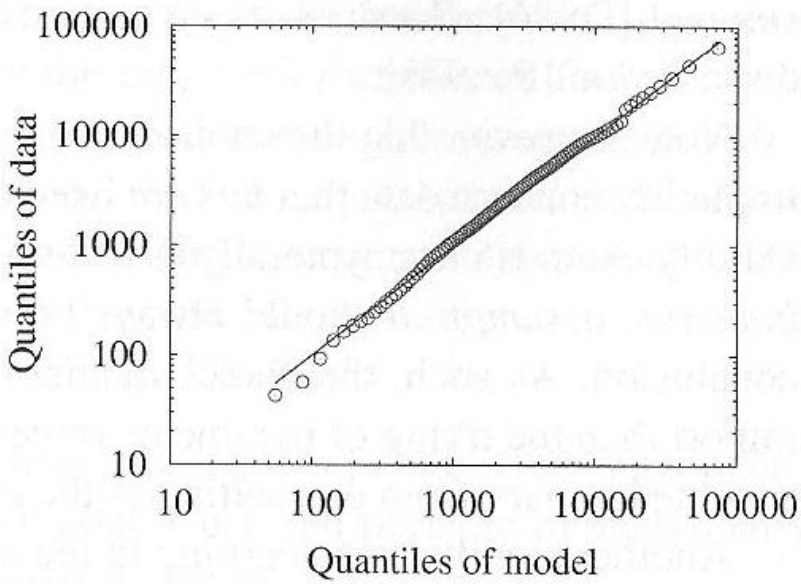
Modelagem Probabilística

- Envolve dois passos:
  - A escolha da função distribuição
  - Estimativa dos valores dos parâmetros relevantes

Verificações Visuais

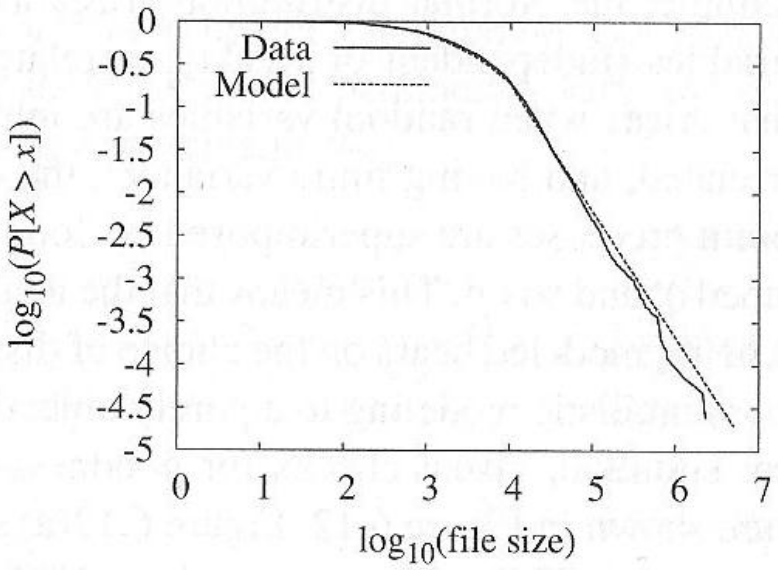


- Comparação entre a CDF analítica (modelo) e a empírica (dados)



- Gráfico quantil-quantil.
- Se os dados corresponderem à distribuição utilizada, o resultado deveria ser uma linha reta.

Verificações Visuais



- Log-log da distribuição complementar

- Para dados altamente variáveis.
- Para verificar o casamento da cauda superior, usa-se um gráfico log-log da distribuição complementar:
  - Comparação entre $\log\big(1 - F(x)\big)$ e $\log x$

Estrutura de Dependência

- Modelar uma série temporal de tráfego tal como $\{C_n, n = 0,1, \ldots\}$ apenas em termos da sua distribuição pode não capturar todas as suas propriedades importantes.
- Como notado anteriormente, muitas medidas de tráfego de rede apresentam dependência entre valores sucessivos no tempo, que pode ter uma forte influência no comportamento do sistema.

Estrutura de Dependência

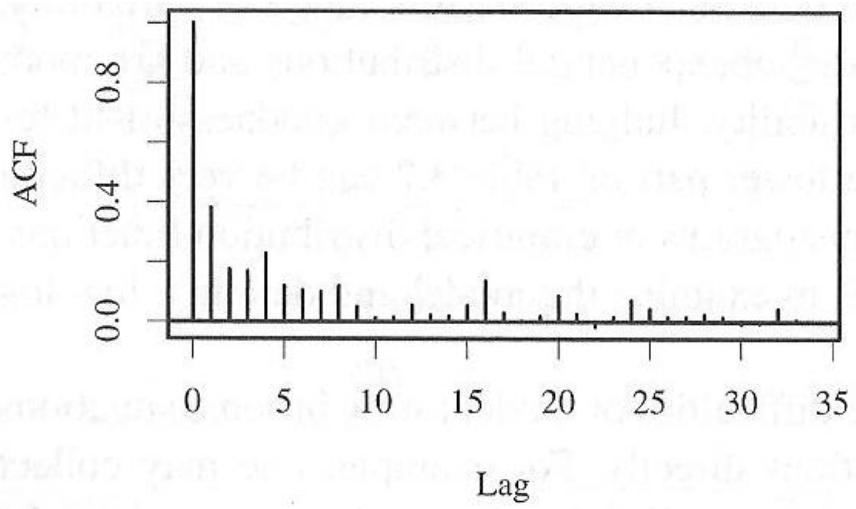
- O grau de dependência pode ser aferido usando a *função autocorrelação* empírica (ACF).
- A autocorrelação é a correlação de uma série com uma cópia dela própria deslocada no tempo.
- A autocorrelação $r(k)$ de uma série temporal $\{X_n, n = 1,2, \dots\}$ é definida como a sua autocorrelação normalizada com distância (*lag*) k:
  - $r(k) = \frac{\mathrm{Cov}(X_n, X_{n+k})}{\mathrm{Var}(X)} = \frac{E[X_n X_{n+k}] - E^2[X]}{\mathrm{Var}(X)}$

Estrutura de Dependência

- A autocorrelação pode ser estimada para uma amostragem finita $\{x_n, n = 1, \dots, T\}$ pela ACF empírica:
  - $\hat{r}(k) = \frac{\frac{1}{T-k}\sum_{i=1}^{T-k}(x_i - \bar{x})(x_{i+k} - \bar{x})}{\frac{1}{T-1}\sum_{i=1}^{T}(x_i - \bar{x})^2}$
- Note que, como muitos estimadores baseados em momentos, a ACF empírica pode ser não confiável quando aplicada a dados altamente variáveis e as estimativas da autocorrelação empírica para grandes k podem estar baseadas num pequeno número de amostras.

Estrutura de Dependência

- A autocorrelação dá uma medida da dependência entre v.a.s em função da distância (ou tempo) k.
  - Valores próximos a 1 ou -1 indicam uma forte dependência
  - Enquanto v.a.s independentes têm autocorrelação 0.



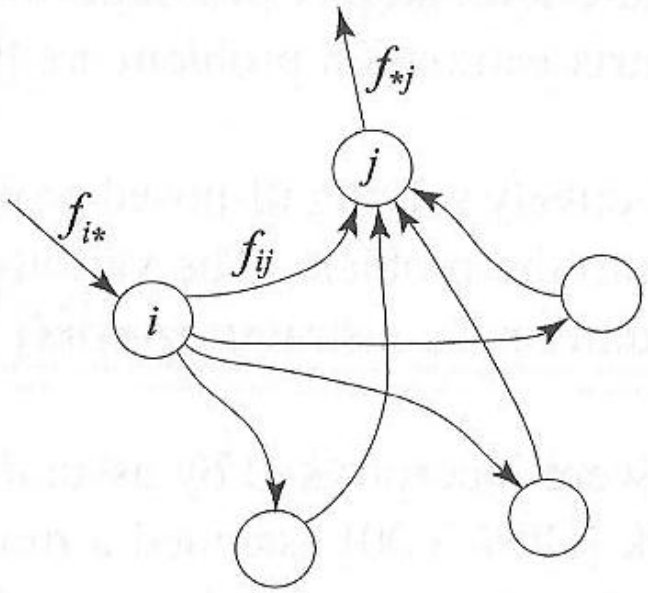
Inferência

- Estimativa da Matriz de Tráfego:
  - Problema de minimização:
    - $\min_{\vec{x}} \|\vec{y} - A\vec{x}\|_2^2 + \lambda J(\vec{x})$
    - Onde
      - $\|\cdot\|_2$ denota a norma l_2
      - $\lambda > 0$ é um parâmetro de regularização e
      - $J(\vec{x})$ é uma função de penalização.
    - A escolha particular de $J(\cdot)$ captura a natureza das restrições particulares anteriores.
    - Neste arcabouço, a regularização mais apropriada é começar a partir de um modelo *independente* (algumas vezes chamado de modelo de *gravidade*).

Inferência: Fluxos numa Rede

- Os relacionamentos entre o volume de tráfego em cada rede e o tráfego que entra e sai da rede pode ser expresso como segue:
- f_{ij} é o tráfego total que flui durante um certo intervalo de tempo entre o ponto de entrada i e o ponto de saída j.

Inferência: Fluxos numa Rede



- O tráfego total que entra na rede no nó i é:
  - $f_{i*} = \sum_{k \in S} f_{ik}$

- O tráfego total que sai da rede no nó j é:
  - $f_{*j} = \sum_{k \in S} f_{kj}$
- Usamos f_{**} para denotar todo o tráfego que flui na rede:
  - $f_{**} = \sum_{i \in S} \sum_{j \in S} f_{ij}$

Inferência: Fluxos numa Rede

- Estas frequências podem ser usadas para formar estimativas de probabilidades empíricas.
- A probabilidade conjunta de que um pacote tenha entrado na origem i e saído no destino j é dada por:
  - $p_{O,D}(i,j) = \frac{f_{ij}}{f_{**}}$
- A probabilidade marginal de entrar na origem i é:
  - $p_O(i) = \frac{f_{i*}}{f_{**}}$
- E a probabilidade de sair no destino j é dada por:
  - $p_D(j) = \frac{f_{*j}}{f_{**}}$

Inferência: Fluxos numa Rede

- O modelo de independência assume independência da origem e do destino, i.e.,
  - $p_{O,D}(i,j) = p_O(i) \cdot p_D(j)$
- Ou seja, a probabilidade de que um pacote entre no nó i e saía em um outro nó j é a mesma probabilidade de que qualquer pacote escolhido aleatoriamente, saía no nó j.
- Este modelo raramente é uma previsão perfeita do comportamento atual do tráfego.
  - Ou seja, é improvável que obtenhamos exatamente
    - $f_{ij} = \frac{f_{i*} f_{*j}}{f_{**}}$ para todo $i \in S, j \in S$.
  - Mas, serve como uma primeira aproximação!

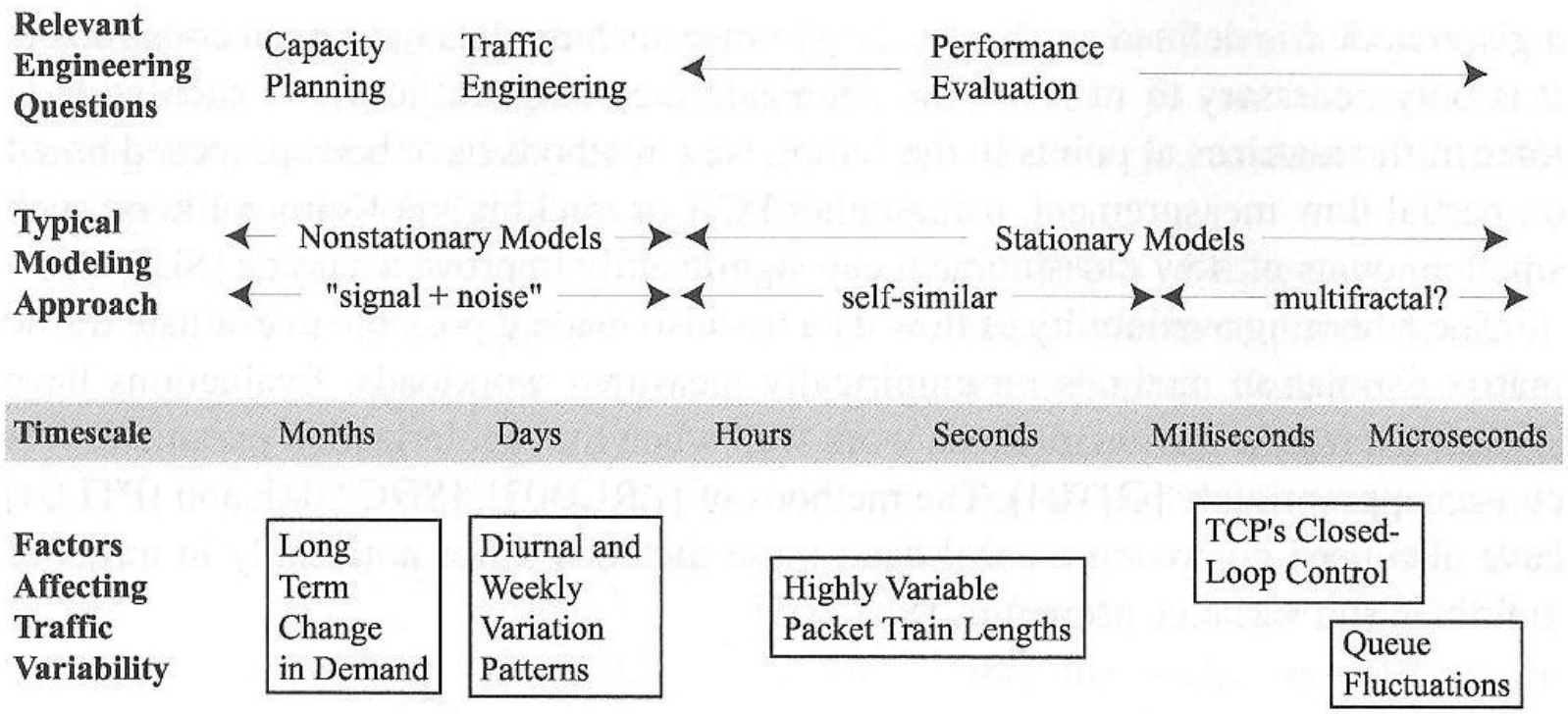
Estado da Arte

Roteiro

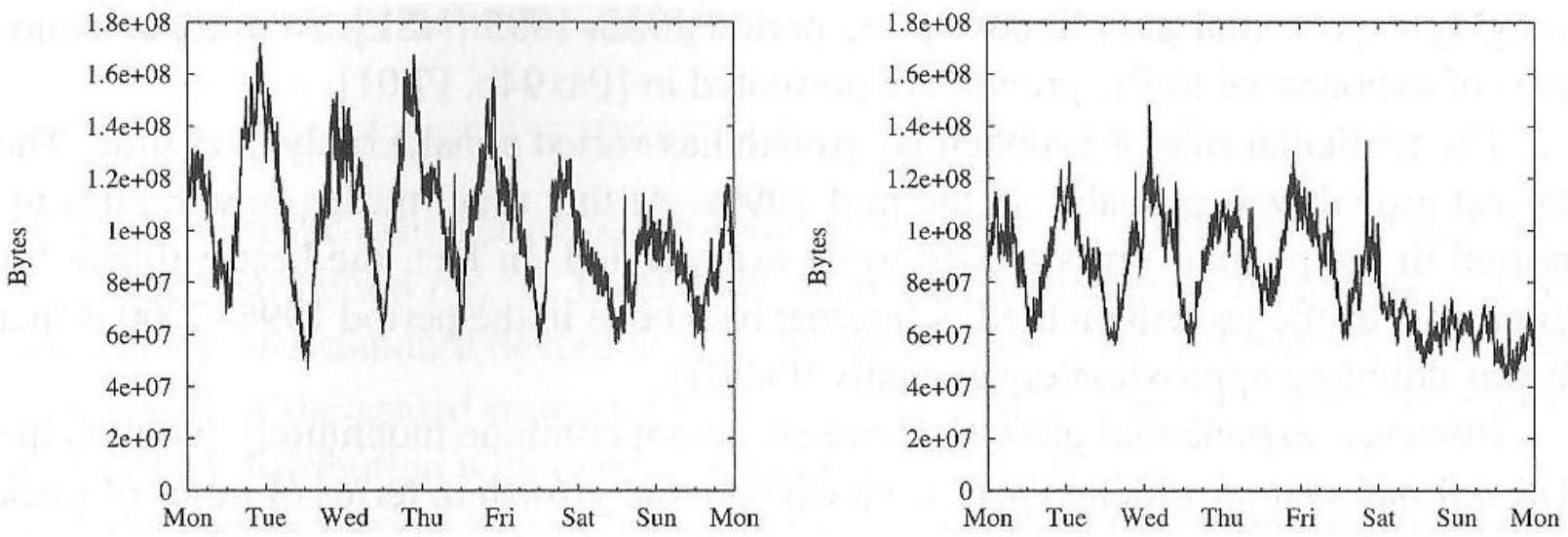
- Pacotes e Bytes
- Estruturas de Mais Alto Nível
- Fluxos
- Tráfego de Controle
- Sem Fio

Pacotes e Bytes

- Panorama da análise de tráfego:



Escalas de Tempo Longas: Tendências



- Uma semana de tráfego em dois links da rede Abilene.
- A variação diária é o componente dominante na variabilidade do tráfego total em escalas de tempo maiores do que uma hora.
- Superposta com a variação diária há um *ruído* considerável – variação aleatória.
  - Este ruído normalmente apresenta uma variabilidade do tipo Gaussiana, exceto por picos ocasionais nos quais o tráfego se afasta bastante da média.

Escalas de Tempo Longas: Tendências

- Podemos então pensar no tráfego de rede em escalas de tempo longas como tendo dois componentes:
  - Previsível (sinal)
    - Pode ser modelado como uma média variante com o tempo
  - Estocástico (ruído)
    - Suas propriedades serão discutidas na próxima seção.
- Esta separação foi realizada usando diversas abordagens:
  - Séries temporais
  - Análise de ondaletas (*wavelets*)
  - Análise do componente principal

Escalas de Tempo Curtas: Escalas

- Em escalas de tempo mais curtas, podemos usar modelos estacionários para descrever o tráfego da rede.
- Não há variações previsíveis e os modelos estocásticos são apropriados.
  - Mas, encontramos que a variação estocástica no tráfego da Internet geralmente apresenta características pouco usuais.
  - Estas propriedades podem ser descritas em termos de *comportamento de escala*, ou seja, a maneira na qual as propriedades estatísticas variam ao observarmos o tráfego em diferentes escalas de tempo.

Escalas de Tempo Curtas: Escalas

- Dada algumas séries temporais de contagem de tráfego $\{B_n, n = 0,1, \ldots\}$ em uma escala de tempo particular T,
  - Podemos formar uma visão em uma nova escala do tráfego $\left\{B_n^{(m)}, n = 0,1, \ldots\right\}$ definindo
    - $B_n^{(m)} = \sum_{i=nm}^{nm+m+1} B_i$ para algum inteiro positivo m
  - Portanto, $\left\{B_n^{(m)}\right\}$ é apenas $\{B_n\}$ somado em blocos não superpostos de tamanho m.
    - E, portanto, re-escalar a série temporal de tráfego por m é equivalente a observar o tráfego original na escala de tempo Tm.
    - O *comportamento de escala* refere-se a como as propriedades estatísticas de $\left\{B_n^{(m)}\right\}$ variam com m.

Independência

- Se não houvesse correlações, o tráfego seria independente.
- Considerando o modelo de contagem de tráfego como um processo estocástico $\{X_n, n = 0,1, \dots\}$, se os $\{X_n\}$ forem independentes então muitas propriedades do processo são simples de calcular e de entender:
  - Todas as distribuições conjuntas podem ser expressas na forma de produto:
    - $p_{X_0,X_1}(x_0, x_1) = p_{X_0}(x_0) \cdot p_{X_1}(x_1) = p_{X_0}(x_0) \cdot p_{X_0}(x_1)$
    - Então, para descrever a distribuição de todo o processo $\{X_n\}$ basta caracterizar uma única distribuição $p_{X_0}(\cdot)$.

Independência

- A independência afeta também as propriedades de escala:
  - Se X_0 tem uma média μ e um desvio padrão $\sigma < \infty$ então, pelo Teorema do Limite Central qualquer elemento do processo escalado $(X_0^{(m)} - \mu)/\sqrt{m}$ convergirá a sua distribuição para a distribuição Normal com média 0 e desvio padrão σ.
- Modelos independentes foram usados largamente em análise de desempenho sobretudo dos sistemas telefônicos:
  - Trabalho de Erlang (1909) usando processos de Poisson.

Podemos usar modelos independentes como uma aproximação?

- ... Apesar de termos visto que o tráfego da Internet exibe correlações?
- Considere a situação na qual $p_{X_0,X_n}(x_0, x_n) = p_{X_0}(x_0) \cdot p_{X_n}(x_n)$ sempre que n for maior do que algum limiar θ.
  - Isto significa que observações de tráfego distantes o suficiente são independentes.
  - Isto afeta a função de autocorrelação: $r(k) = 0$ quando $k > \theta$.

Podemos usar modelos independentes como uma aproximação?

- Consideremos agora o processo escalonado $\left\{X_n^{(m)}\right\}$ onde $m \gg \theta$. Neste processo, as v.a.s $\left\{X_n^{(m)}\right\}$ serão aproximadamente independentes.
  - Para ver isto, tome $X_0^{(m)}$ e $X_1^{(m)}$. Muitas das v.a.s no bloco de somas que formou $X_0^{(m)}$ são independentes de muitas das v.a.s que formaram $X_1^{(m)}$, e portanto, devemos esperar que as somas $X_0^{(m)}$ e $X_1^{(m)}$, sejam elas mesmas aproximadamente independentes.

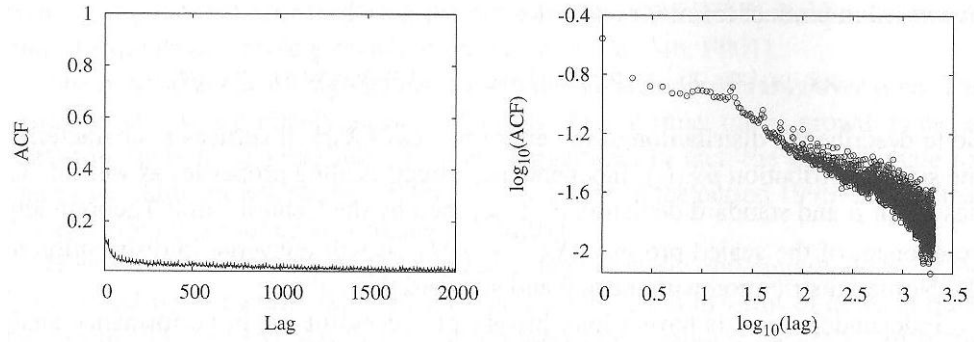
Dependência de Curto Alcance

- Definição formal do conceito anterior.
- Um processo estocástico estacionário com função de autocorrelação $r(k)$ exibe dependência de curto alcance se e só se:
  - $\sum_{k=1}^{\infty} r(k) < \infty$
- Casos importantes de dependência de curto alcance:
  - $r(k) = 0$ sempre que $k > \theta$, para algum $\theta > 0$ e
  - $r(k) \sim a^{-k}$ sempre que $k > \theta$, para algum $\theta > 0$ e $a > 1$.

Dependência de Curto Alcance

- A dependência de curto alcance permite-nos efetuar algumas análises úteis baseadas em modelos independentes
  - Aplicando estes modelos em escalas de tempo longas o suficiente para que a independência aproximada seja obtida.

Correlações no Tráfego de Rede



- A figura acima mostra uma hora de tráfego TCP capturado num link de acesso de uma grande organização à Internet.
- A função autocorrelação (ACF) foi calculada sobre a contagem de bytes $\{B_n\}$ numa escala de tempo $T = 10$ ms.
- Podemos observar que a autocorrelação não chega a zero mesmo com grandes saltos (*lag*), e que ela não é exponencial
- O gráfico log-log mostra que a ACF se comporta mais como uma lei de potência, i.e.,
  - $r(k) \sim k^{-\beta}$, com um valor de β menor do que um. (6.8)

Dependência de Longo Alcance

- Um processo estocástico estacionário com função de autocorrelação $r(k)$ exibe dependência de longo alcance (LRD – *Long Range Dependence*) se e só se:
  - $\sum_{k=1}^{\infty} r(k) = \infty$
- Na prática isto implica que para grandes valores de k, $r(k)$ tem uma forma aproximadamente de lei de potência $k^{-\beta}$ com $0 < \beta < 1$.
- Processos com dependência de longo alcance possuem propriedades bem diferentes dos processos tradicionais.
- Intuitivamente, observações que estão arbitrariamente distantes uma das outras no tempo possuem uma correlação não desprezível.

Dependência de Longo Alcance

- Tráfego com dependência de longo alcance apresenta flutuações num grande espectro de escalas de tempo.
- Não há nenhuma escala de tempo na qual a hipótese de independência se verifique nem mesmo aproximadamente.
- "*Uma interpretação intuitiva ... é que 'picos'* (spikes) *de tráfego... estão montados em 'ondulações'* (ripples) *de longo prazo, que por sua vez estão montadas em 'expansões'* (swells) *de prazos ainda mais longos.*

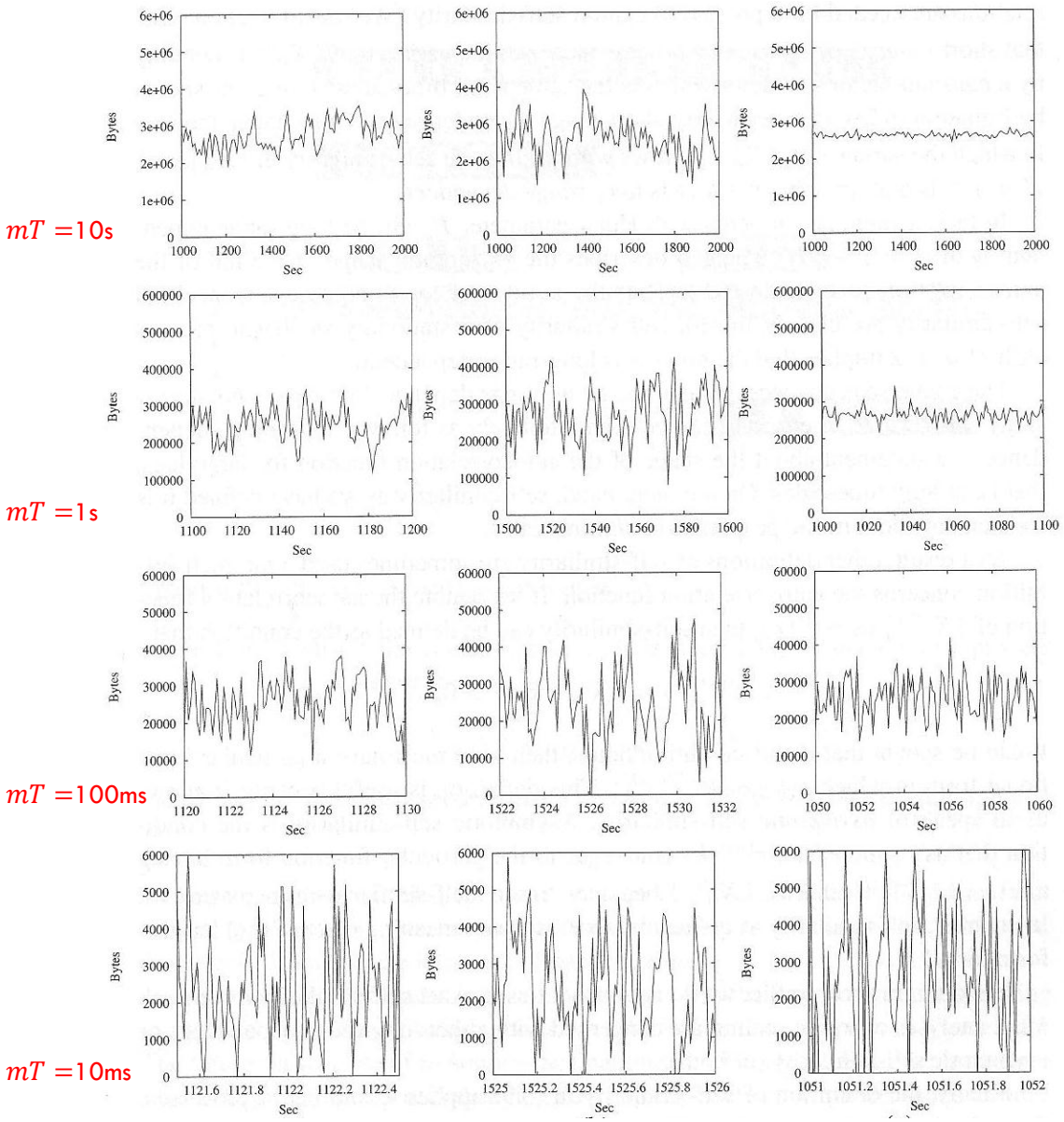
Autossimilaridade

- A ocorrência de flutuações de tráfego em uma grande faixa de escalas de tempo significa que o tráfego não parece 'suave' em nenhuma escala de tempo.
- Esta propriedade é capturada pela noção de *autossimilaridade*.
- Mais especificamente, o fenômeno da autossimilaridade diz respeito a como as flutuações em $\left\{X_n^{(m)}\right\}$ variam com a escala de tempo m.

Definição de Autossimilaridade

- Um processo estacionário de tempo discreto com média zero $\{X_n\}$ é chamado *autossimilar* com *parâmetro de Hurst* H se, para todo m, o processo agregado $\{X^{(m)}\}$ tiver as mesmas distribuições que $\{m^H X_n\}$.
- Mais precisamente,
  - $\{m^H X_n\} \approx \{X^{(m)}\} \;\; m > 0, \frac{1}{2} \leq H < 1$ (6.9)
  - Onde $\approx$ está significando que os processos em cada lado têm a mesma distribuição.
  - Ou seja, o processo agregado estatisticamente parece com o processo original ampliado por um fator m^H.

Séries Temporais em diferentes escalas de tempo



- Nas escalas de tempo menores, as flutuações de tráfego típicas aparentam ser semelhantes às dos tráfegos sintéticos.
- No entanto, com o crescimento das escalas de tempo, a variabilidade do tráfego não suaviza rapidamente como no caso dos processos independentes ($H = 0{,}5$)

Traço real (H =0,83)

Tráf. sintético (H = 0,83)

Tráf. sintético (H = 0,5)

Autossimilaridade e LRD

- Autossimilaridade surge devido a correlações no tráfego.
- Mas que tipo de correlações são necessárias para que o processo exiba autossimilaridade?
  - Vimos que a dependência de curto alcance em um processo faz crescer a variância de $\left\{X_n^{(m)}\right\}$, mas apenas por um fator constante.
  - Em outras palavras, a dependência de curto alcance não muda a forma na qual a variância de $\left\{X_n^{(m)}\right\}$ cresce com m.
    - De fato, a autossimilaridade em $\{X_n\}$ com $H \neq \frac{1}{2}$ é possível apenas se $\{X_n\}$ for *dependente de longo alcance*.

Autossimilaridade e LRD

- Um processo estacionário com parâmetro de Hurst H é dependente de longo alcance com $\beta = 2 - 2H$, onde β descreve a forma assintótica da cauda da função autocorrelação.
- Portanto, as noções de dependência de longo alcance e autossimilaridade estão fortemente ligadas:
  - A autossimilaridade de um processo estocástico estacionário com $H \neq \frac{1}{2}$ implica que o processo seja dependente de longo alcance.

Autossimilaridade e LRD

- O inverso não é necessariamente verdadeiro: um processo LRD não é necessariamente autossimilar.
  - Razão:
    - A dependência de longo alcance é uma afirmação sobre a forma da ACF para grandes saltos, i.e., em escalas de tempo longas.
    - Por outro lado, a autossimilaridade como nós a definimos é uma afirmação sobre propriedades de tráfego em *todas* as escalas de tempo.

Outras definições de Autossimilaridade

- Usando a função autocorrelação:
  - Se denotarmos a função autocorrelação de $\left\{X_n^{(m)}\right\}$ por $r^{(m)}(k)$, então a autossimilaridade pode ser definida como a condição
    - $r^{(m)}(k) = r(k), \quad k, m > 0,$
    - Podemos mostrar que se esta condição se verifica então $r(k)$ deve ter uma forma funcional particular na qual $r(k) \sim k^{-(2-2H)}$.
  - Esta definição é útil porque nos permite falar em autossimilaridade *assintótica*.
    - O processo se torna 'mais' autossimilar com o crescimento de m.

Outras definições de Autossimilaridade

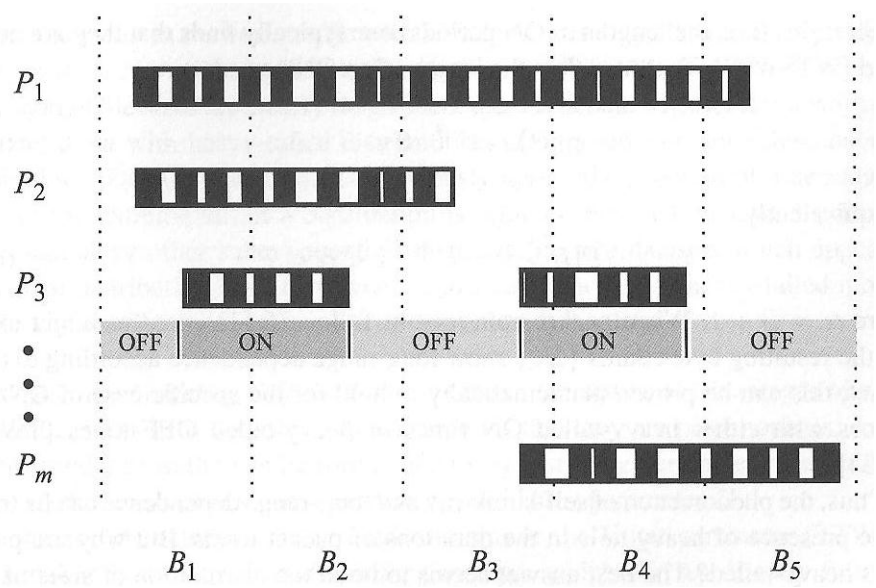
- Autossimilaridade no tempo:
  - A nossa definição original de autossimilaridade se aplica a processos estacionários.
    - A propriedade de autossimilaridade relaciona diferentes versões do processo (em diferentes níveis de agregação m)
  - A autossimilaridade é também frequentemente definida em relação a processos estocásticos de tempo contínuo não-estacionários $\{Y_t, t \geq 0\}$ com incrementos estacionários como:
    - $Y_{at} \approx a^H Y_t, \ \ a > 0.$ (6.10)
    - Esta forma de autossimilaridade relaciona um único processo a ele mesmo em diferentes instantes.

Outras definições de Autossimilaridade

- Autossimilaridade no tempo (cont.):
  - A conexão com a autossimilaridade definida anteriormente é que se $\{X_n\}$ for um processo incremental de $\{Y_t\}$ em qualquer escala de tempo $T > 0$, ou seja,
    - $X_n = Y_{(n+1)T} - Y_{nT},\ n \geq 0,$
  - Então, $\{X_n\}$ será um processo estacionário que é autossimilar de acordo com a nossa definição anterior, com o mesmo valor de H.

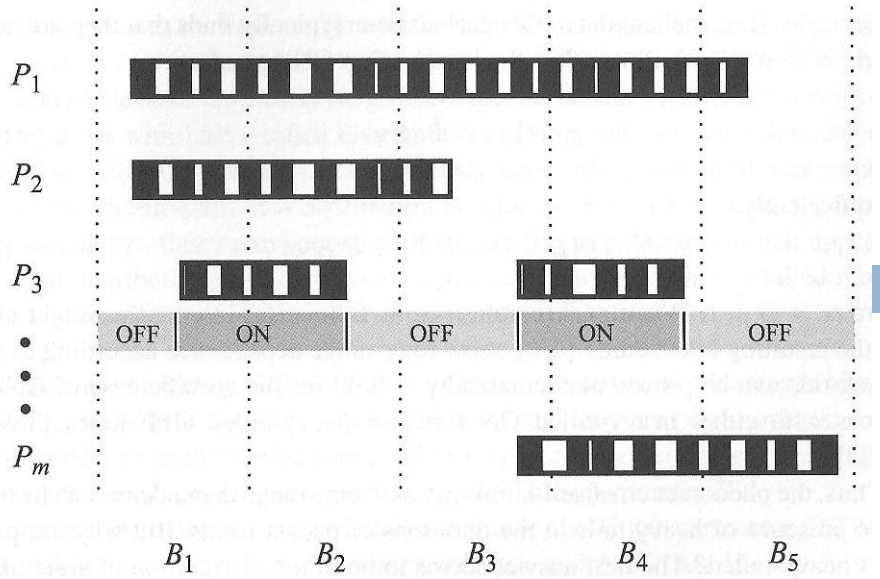
Conexão com Caudas Pesadas

- A principal causa da presença de LRD e autossimilaridade assintótica no tráfego de rede é a influência dos trens de pacotes.



- Um trem de pacotes que se estende por diversas observações contribui com pacotes para cada observação.

Conexão com Caudas Pesadas



- Vemos aqui um conjunto de m pares origem-destino $P_1, P_2, \ldots, P_m$.
- Cada par tem uma sessão em progresso e estão transmitindo objetos de dados que se tornam trens de pacotes.
  - Cada par exibe um comportamento ON/OFF distinto.

- Ao construirmos uma série temporal de contagens de bytes por unidade de tempo $\{B_1, B_2, \ldots\}$ vemos que muitos trens de pacotes (períodos ON) contribuem para mais de um intervalo de contagem.
- Quando um trem de pacotes contribui para uma faixa de contagens $\{B_i, B_{i+1}, \ldots, B_{i+n}\}$ então os valores na faixa se tornam correlacionados.

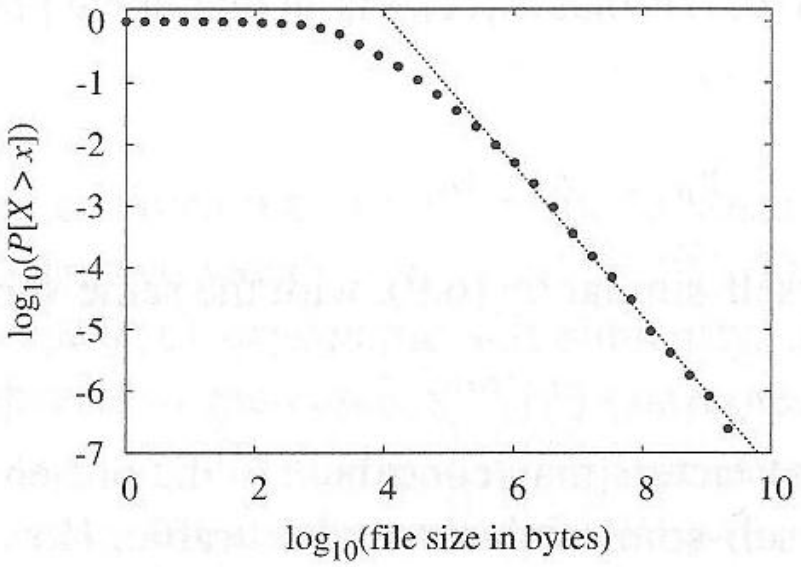
Conexão com Caudas Pesadas

- Para entender de onde vem a dependência de longo alcance, a observação chave é que *os comprimentos do trens de pacotes possuem geralmente caudas pesadas*.
- Se observarmos as durações dos trens de pacotes (i.e., os comprimentos dos períodos ON) encontraremos que eles têm normalmente caudas pesadas.
- Ou seja, se L for o comprimento de um período ON:
  - $p_L(t) \sim t^{-\beta} \quad 0 < \beta < 1$ (6.11)
- Ou de forma equivalente
  - $P[L > t] \sim t^{-\alpha} \quad 1 < \alpha < 2$ (6.12)
  - Onde $\alpha = \beta + 1$.
- Quando os comprimentos dos trens de pacotes seguem (6.11) podemos esperar que a contagem de bytes resultante $\{B_n\}$ apresente dependência de longo alcance de acordo com (6.8).

Por que os trens de pacotes exibem Cauda Pesada?

- A melhor resposta parece estar na distribuição dos comprimentos dos próprios objetos de dados.
  - A quantidade de bytes contida em longos trens de pacotes exibe frequentemente cauda pesada.
  - Este fenômeno tem sido observado nas distribuições dos comprimentos dos arquivos.

Distribuições dos comprimentos dos arquivos



- LLCD de comprimentos de arquivos em sistemas UNIX:
  - Mais do que 12 milhões de comprimentos obtidos de 1000 diferentes sistemas de arquivos UNIX em 1993.

- O gráfico mostra que a cauda da distribuição exibe uma forma aproximadamente de lei de potência com $\alpha \approx 1{,}2$.
- Valores particulares para α encontrados para objetos de dados estão normalmente entre 1 e 2.
- Bytes de dados em rajadas FTP casa bem com uma distribuição de Pareto com α entre 0,9 e 1,4.
- Objetos Web: α entre 1,1 e 1,3.

Medindo e Modelando a Autossimilaridade

- Uma das principais vantagens de usar modelos autossimilares para descrever o tráfego da rede é que eles são parcimoniosos.
  - Um modelo razoável de tráfego pode ser formulado usando apenas três parâmetros:
    - Taxa média de tráfego, μ
    - Variância do tráfego em alguma escala de tempo, σ_0^2
    - Parâmetro de Hurst, H

Métodos para Estimar o Parâmetro de Hurst

- Método da variância agregada:
  - Derivado diretamente da definição de autossimilaridade em (6.9).
  - Dada uma série de contagens B_n, a variância de $\frac{1}{m}B^{(m)}$ é plotada em relação a m em um gráfico log-log.
  - Se os dados originais for bem modelado por um processo estacionário autossimilar, a variância de $\frac{1}{m}B^{(m)}$ seguirá m^{2H-2} e o gráfico mostrará uma linha reta com declividade $(-\beta)$ maior do que -1.
    - O parâmetro de Hurst poderá então ser estimado por $H = 1 - \beta/2$.

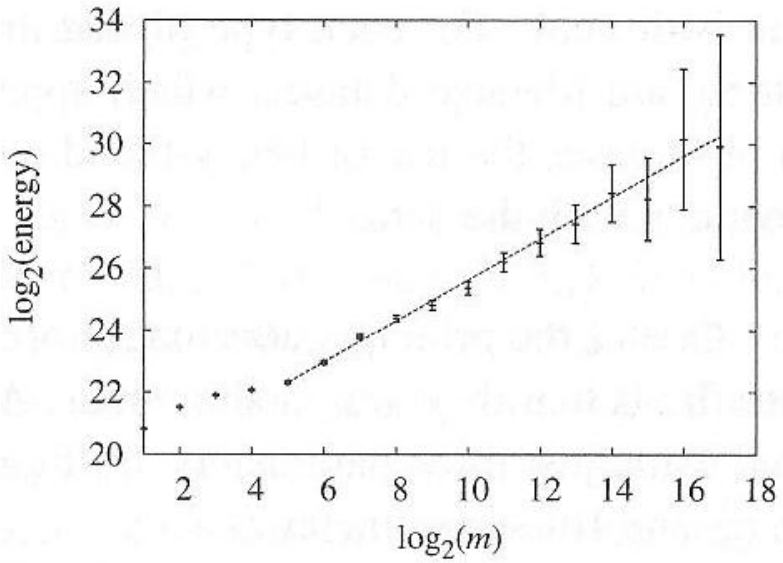
Métodos para Estimar o Parâmetro de Hurst

- Método da variância agregada:
  - Apesar de simples, este método é muito sensível a violações das hipóteses de estacionariedade e autossimilaridade exata.
  - Por exemplo, uma mudança na média verdadeira do processo de tráfego pode aparecer nas estatísticas da amostra como uma variância mais alta em longas escalas de tempo,
    - Levando a uma estimativa errônea das propriedades de escala.
    - O método apresentado a seguir seria melhor.

Métodos para Estimar o Parâmetro de Hurst

- Método do diagrama em escala logarítmica:
  - A ideia deste método é a de analisar o tráfego usando ondaletas (*wavelets*).
    - O uso de ondaletas como uma ferramenta de sumarização do tráfego permite que as estimativas resultantes sejam robustas na presença de tendências determinísticas.
    - A análise mede a *energia* em diversas faixas de escalas de tempo, que é diretamente relacionada com a variância.
  - O método permite que sejam construídos intervalos de confiança para o H, ao invés de apenas a estimativa de um ponto.

Método do diagrama em escala logarítmica



- Diagrama de escala logarítmica para os mesmos dados apresentados anteriormente.

- Comportamento linear neste gráfico é uma evidência de um relacionamento de escala entre a variância e a escala de tempo.
- Um comportamento linear iniciando em alguma escala θ e se estendendo para todo $m > \theta$ é consistente com LRD ou autossimilaridade assintótica.
- A linha obtida produz uma estimativa de $H \approx 0{,}83$; enquanto que o intervalo de confiança em H é de (0,82; 0,84).

Síntese de Tráfego

- O processo de análise inicia com o tráfego e estima os seus parâmetros.
- Síntese de tráfego é também importante: frequentemente é útil começar com valores particulares dos parâmetros e gerar um tráfego sintético que case com estas propriedades.
- Um método direto seria começar com um processo estocástico (i.e., um modelo) que incorpore autossimilaridade ou LRD.
  - Exemplos:
    - ARIMA fracionário e
    - Ruído Gaussiano fracionário (usado no tráfego sintético apresentado anteriormente).

Síntese de Tráfego

- Estes métodos podem facilmente produzir um traço precalculado de tráfego sintético com certas propriedades de escala.
- No entanto, para a simulação de tráfego, o uso de traço de tráfego precalculado pode não ser apropriado.
  - O tráfego da rede reflete efeitos combinados da atividade do usuário, aplicações e protocolos de controle.
  - A interação do tráfego com a rede (ex., perda de pacotes e atrasos de enfileiramento) realimenta os usuários, aplicações e protocolos causando modificação no tráfego que chega em seguida.
  - Um traço precalculado não refletirá estes efeitos de laço fechado.

Síntese de Tráfego

- Uma boa solução para este caso seria gerar um tráfego autossimilar de um modo que reflita a compreensão de como a autossimilaridade surge nas redes.
  - Em particular, uma simulação envolvendo muitas transferências concorrentes de objetos de dados (“arquivos”) cujos tamanhos tenham sido extraídos de uma distribuição com cauda pesada, gerará tráfego autossimilar de uma forma natural.
  - Uma simulação usando TCP para transferir objetos de dados cuja distribuição tenha cauda pesada com expoente α tenderá a gerar tráfego autossimilar com $H \approx \frac{3-\alpha}{2}$.
  - Esta abordagem permite realizar experimentos de simulação com tráfego de rede realista exibindo um dado parâmetro de Hurst.

Impactos da Autossimilaridade

- Efeito no comportamento das filas de tráfego:
  - De um ponto de vista analítico foi mostrado que diversos modelos de tráfego LRD resultam em comportamento das filas com cauda longa.
    - Estes resultados são normalmente assintóticos, aplicáveis apenas a filas infinitas.
    - No entanto, como são muito diferentes dos casos onde o tráfego exibe dependência de curto alcance, sugerem que o comportamento da fila provavelmente será bem diferente mesmo para os casos realistas de filas finitas.

Impactos da Autossimilaridade

- Efeito no comportamento das filas de tráfego:
  - Mais precisamente, se denotarmos o comprimento da fila como Q, resultados típicos mostram que para certos processos de tráfego LRD:
    - $p_Q(x) \sim \exp(-\kappa x^{2-2H})$
    - Onde $\kappa > 0$ é uma constante que depende do processo de tráfego específico.
    - Quando $H > 0{,}5$ esta é uma distribuição subexponencial (uma distribuição Weibull).
    - Enquanto que no caso de tráfego com dependência de curto alcance, as distribuições do comprimento da fila decairiam exponencialmente.

Impactos da Autossimilaridade

- Efeito no comportamento das filas de tráfego:
  - Resultados obtidos por simulação mostram que o comportamento das filas para tráfego autossimilar é muito diferente daquele para tráfego com dependência de curto alcance:
    - Comprimentos de fila, atrasos de pacote e perdas de pacotes são maiores.
    - A ocupação dos buffers cresce dramaticamente com o aumento do comprimento dos buffers.
      - Consequências importantes para o tamanho dos buffers nos roteadores.
      - A adição de buffer para diminuir as perdas pode resultar em atrasos inaceitáveis.
    - Por outro lado, se os buffers forem mantidos pequenos, a LRD pode não ter nenhum impacto significativo no desempenho.

Tráfegos que exibem LRD

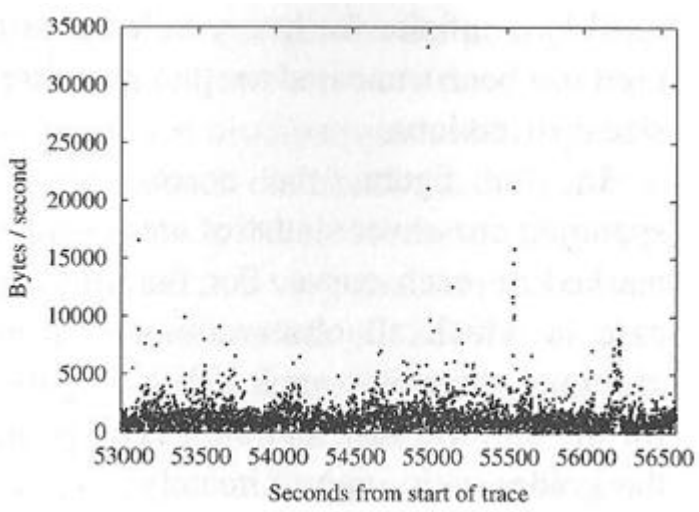
- Modelos que incorporam LRD ou autossimilaridade assintótica foram propostos como apropriados para o tráfego de muitos tipos e localidades diferentes na Internet:
  - Tráfego Ethernet
  - Tráfego WAN
  - Tráfego de células ATM
  - Tráfego Web
  - Tráfego de vídeo
  - Tráfego GPRS

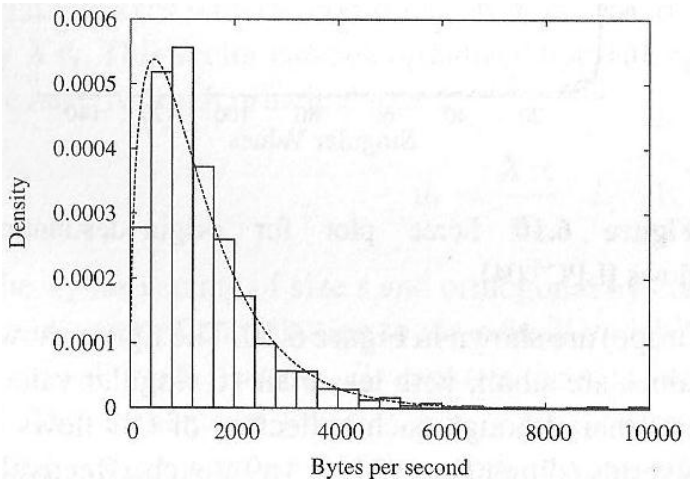
Distribuição Marginal do Tráfego

- Além da estrutura de correlação do tráfego é também importante entender a distribuição marginal do tráfego.
- O modelo mais comumente usado para descrever o tráfego de bytes é a distribuição Gaussiana (Normal).
  - Ela é atraente por ser parcimoniosa (requer apenas a média e a variância) e por causa do Teorema do Limite Central que sugere que se o tráfego for suficientemente agregado, a sua distribuição tende a ser Gaussiana.
    - No entanto, isto ocorre em altos níveis de agregação seja em termos do número de fluxos concorrentes que na duração.
    - Esta convergência pode não ocorrer na prática se as fontes de tráfego que estão sendo agregadas apresentarem alta variabilidade em termos de suas taxas de transmissão.

Variabilidade do Tráfego

- Em muitos casos poucas conexões de alto volume e de alta taxa podem causar 'picos' intensos de tráfego,
  - Onde a distribuição de B_n se distancia bastante da Gaussiana.
  - Isto pode ser observado no traço de tráfego abaixo que mostra um pequeno número de valores altos incomuns, e a sua distribuição marginal que mostra uma cauda superior longa.





Tráfegos alfa e beta

- *Tráfego alfa*: tráfego de conexões com altas taxas e volumes.
  - Podem representar uma fração muito pequena de todas as conexões (menos do que 0,1%) mas têm um grande impacto nas propriedades do tráfego.
  - Apresenta marginais altamente variáveis
- *Tráfego beta*: composto pelas conexões mais comuns que apresentam baixo volume, baixas taxas, ou ambos.
  - Apresenta uma distribuição marginal Gaussiana.

Separação entre as Componentes Alfa e Beta do Tráfego

- Para cada conexão pode se separar as componentes alfa e beta do tráfego.
- Podemos identificar conexões alfa procurando intervalos n em que B_n exceda um limiar e, escolhendo então, a conexão com a maior taxa que transmitiu naquele intervalo de tempo.
- Após remover todas estas conexões, o que resta é o tráfego beta.

O que causa o tráfego Alfa?

- O tráfego alfa surge naqueles relativamente casos raros que o transmissor possui um grande volume de dados para transmitir num caminho de rede com grande largura de banda.
  - Portanto, a causa principal da alta variabilidade nas taxas dos tráfegos é a heterogeneidade nas larguras de banda dos gargalos.
    - Há evidências de que esta heterogeneidade seja influenciada pelo atraso de ida e volta (RTT): caminhos de rede com menores RTTs têm mais chances de apresentar altas larguras de banda do gargalo.

Distinção entre Alfa e Beta

- Adiciona uma nova dimensão aos modelos de tráfego além do fenômeno da LRD.
  - A LRD é entendida em termos do modelo ON/OFF como oriunda de conexões com cauda pesada cujas transferências estão espalhadas no tempo.
  - Por outro lado, se algumas conexões puderem transmitir em altas taxas, o seu tráfego pode *não* se espalhar muito no tempo.
    - Neste caso, conexões com caudas longas resultam em marginais de tráfego de cauda longa ao invés de autocorrelações de cauda longa.
- Isto resulta numa visão mais genérica do tráfego que é o resultado natural da interação de demandas de cauda pesada com a estrutura da rede.

Escalas de Tempo Muito Curtas

- A LRD está mais claramente presente em tráfego de rede em escalas de centenas de milissegundos até aproximadamente uma hora.
  - Além de uma hora o tráfego não é modelado bem como sendo estacionário.
  - Por outro lado, o limite inferior (centenas de milissegundos) é aproximadamente a faixa dos RTTs em muitas partes da Internet.
- Em escalas de tempo sub-RTT os padrões de chegada de pacotes são afetados por diversos fatores:
  - Dinâmica dos protocolos de transporte (principalmente TCP)
  - Variação do comprimento das filas nos roteadores (que afeta o espaçamento entre pacotes)
  - Mistura particular de fluxos de alta e baixa taxas.

Processos Multifractais

- Estes efeitos combinados fazem com que o tráfego seja muito explosivo em escalas de tempo mais finas, mas não de uma forma que possa ser caracterizado pela autossimilaridade.
  - Esta explosividade tem sido caracterizada como sendo *multifractal*.
- Um processo multifractal apresenta diferentes comportamentos de escala em diferentes instantes de tempo.

Processos Multifractais

- Considere um processo de chegada de tráfego $\{Y_t, t \geq 0\}$, onde Y_t denota a quantidade total de tráfego que chega do instante 0 até o instante t.
- A série temporal de contagens correspondente numa escala de tempo particular Δ é o processo incremental,
  - $X_t^{(\Delta)} = Y_{t+\Delta} - Y_t, \qquad t \geq 0.$
- O processo $\{Y_t\}$ possui expoente de escala local (ou expoente de Hölder local) $\alpha(t_0)$ no instante $t_0 \geq 0$ se
  - $X_{t_0}^{(\Delta)} \sim \Delta^{\alpha(t_0)}$ à medida que $\Delta \to 0$.

Escala Local

- Há diversas distinções entre a escala local e as propriedades de escala associadas à autossimilaridade:
  - A escala local diz respeito ao comportamento do tráfego no limite de pequenas escalas de tempo ($\Delta \to 0$).
    - Enquanto que a autossimilaridade assintótica diz repeito ao tráfego em escalas de tempo longas ($\Delta \to \infty$).
  - A escala local permite que um processo tenha comportamentos de escala *diferentes* em diferentes instantes de tempo.
  - A escala local pode ser aplicada a um processo $\{Y_t\}$ que possua média zero
    - Para um processo autossimilar exato com incrementos estacionários isto seria verdade apenas para $H = 1$.

Estruturas de Mais Alto Nível: Trens de Pacotes

- Em alternância a períodos de silêncio (Modelo ON/OFF)
- Os tempos ON exibem um comportamento de cauda pesada
- Também o volume do trem de pacotes (número de bytes ou pacotes contidos em um trem de pacotes) apresenta caudas pesadas.
  - Os valores típicos de α estão na faixa de 1,0 a 1,5.
  - O tráfego analisado em [PF95] mostrou que 50-80% dos bytes em transferências FTP foram devidas a 2% de todas as transferências.
  - Foi encontrado [TMW97] no *backbone* comercial da MCI que 50% dos pacotes estavam contidos em 20% dos trens de pacotes.
  - Fenômeno dos “elefantes e ratos”.

Estruturas de Mais Alto Nível: Trens de Pacotes (cont.)

- Os tempos OFF também apresentam durações com cauda pesada
  - Os valores típicos de α estão na faixa de 1,0 a 1,5.
  - Estes valores também foram observados para o conjunto de pacotes transmitidos por uma única estação de trabalho.
  - Implicações para a identificação de um trem de pacotes:
    - Conjunto de pacotes com intervalos entre chegadas inferiores a um dado limiar.
    - Devido às caudas pesadas, os resultados são relativamente insensíveis a pequenas mudanças neste limiar.

Estruturas de Mais Alto Nível: Trens de Pacotes (cont.)

- Em níveis mais altos de agregação a estrutura de dependência no processo de chegada de trens de pacotes se enfraquece, mas geralmente não é bem descrita como sendo Poisson.
- Conexões TCP:
  - Tempos entre chegadas exibem autossimilaridade assintótica [Fel99].
  - No entanto, a autossimilaridade no nível de pacote para não depender significativamente do processo de chegada TCP [HVA02].
  - Os intervalos entre chegadas de conexões TCP são altamente variáveis e foram modelados usando distribuições de Weibull [Fel99, OB01].

Estruturas de Mais Alto Nível: Taxas dos trens de pacotes

- Velocidade na qual os bytes fluem.
- A taxa de transferência de um trem de pacotes individual é diretamente influenciada pelo protocolo de transporte utilizado
  - RTP e UDP não impões nenhum limite superior nesta taxa.
  - Mas esta pode ser limitada por algum controle ao nível da aplicação
  - No caso do TCP, foi mostrado que para baixas perdas de pacotes ($p < 2\%$) a vazão do TCP pode ser aproximada por
    - $R = \frac{MSS}{RTT \cdot \sqrt{p}}$

Estruturas de Mais Alto Nível: Taxas dos trens de pacotes

- Vazão do TCP: $R = \frac{MSS}{RTT \cdot \sqrt{p}}$
- A taxa da conexão é dependente da condição da rede: perda de pacotes (p) e caminho da rede (RTT).
- A taxa de transferência das conexões é altamente variável [ZBPS02]
  - Numa janela de 5 seg, 1% das conexões podem transmitir cerca de 50% dos bytes que passam por um roteador [MFW01].
- Distinção de tráfego alfa/beta:
  - Um pequeno número de conexões têm taxas muito altas [SRB01]
- As taxas observadas para conexões em um servidor Web podem apresentar grandes variabilidades e são bem modeladas pela distribuição lognormal [BSSK97].

Estruturas de Mais Alto Nível: Taxas dos trens de pacotes

- Esta taxa apresenta correlação com o tamanho da transferência para grandes transferências [ZBPS02]
  - Sugere que o comportamento do usuário possa mudar em resposta ao desempenho da rede
- Esta taxa também depende da duração [Bkc02]:
  - Trens de longa duração (mais do que 15 minutos) tendem a transportar tráfego multimídia ou interativo podendo ter taxas altas ou baixas.
  - Trens de duração média (entre 2 seg e 15 min) tendem a ser transferências de arquivos em altas taxas.
  - Trens de curta duração ocorrem em taxas variadas.

Estruturas de Mais Alto Nível: Sessões

- Acima das conexões individuais.
- Parece haver pouca dependência entre as sessões.
- Em geral o processo de chegadas de sessões é bem descrito como sendo Poisson [PF95].
- A hipótese de independência parece bem válida.
- Dentro de uma sessão:
  - O número de conexões TCP apresentam alta variabilidade [FGWK98]
  - O número de páginas Web referenciadas numa página Web típica apresenta uma distribuição de cauda pesada [BC98].

Fluxos

- Fluxos podem ser definidos em diversos níveis de agregação:
  - Fluxos IP
  - Fluxos de rede
  - Fluxos a nível dos ASs
- Em cada caso encontramos exemplos de alta variabilidade.
  - O número de bytes transmitidos por um fluxo IP em intervalos de tempo foram descritos como seguindo a lei de Zipf [WDF+05]
    - E também em fluxos a nível dos ASes [FP99]
  - Observa-se uma maior disparidade a nível do IP com valores de cruzamento *(crossover)* frequentemente maiores que 80/20, podendo ser tão alto como 95/5 [BHGkc04]

Fluxos: Matrizes de Tráfego

- Como o tráfego está dividido entre diversos caminhos fim-a-fim em uma rede?
  - As matrizes de tráfego apresentam alta variabilidade no volume que passa por diversos caminhos.
    - Ao nível IP a matriz é bem esparsa.
      - [WTSW97] encontraram que apenas 6,8% de todos os pares de hosts em uma rede Ethernet com 121 hosts trocaram dados em uma hora.
      - Encontraram ainda que 1,6% de todos os pares de hosts foram responsáveis por 98% de todos os bytes em uma hora.

Fluxos: Matrizes de Tráfego

- Propriedade de "localidade" [JR86]:
  - As taxas dos diversos fluxos f_{ij} variam muito.
  - Esta tem sido uma propriedade consistente desde o início da ARPANET [KN74]
  - Foi notada também:
    - Na NSFNET [Hei90]
    - Em *backbones* de redes comerciais modernas [BDJT01]
    - Fluxos ponto a multiponto [FGL+00]
  - Este desbalanceamento no volume de fluxos tende a induzir também um grande desbalanceamento nos níveis de tráfego nos enlaces das redes [BDJT01]

Fluxos: Matrizes de Tráfego

- Tráfego total entrante ou "sainte" de um PoP (f_{i*} ou f_{*j}):
  - A distribuição deste tráfego também apresenta alta variabilidade [BDJT01]
    - Estes pontos servem populações de diferentes tamanhos
      - Há evidências de relacionamento deste tráfego com a população local [FCE05]
    - Alguns destes pontos estão ligados a fontes ou destinos de grande volume de tráfego.

Fluxos: Matrizes de Tráfego

- O modelo de independência (entre origem e destino) é, frequentemente, uma boa aproximação:
  - $f_{ij} \approx \frac{f_{i*} f_{*j}}{f_{**}}$ para todo $i \in S, j \in S$.
    - Esta relação sugere que a alta variabilidade nos fluxos origem-destino podem ser fortemente influenciada pela alta variabilidade no tráfego que entra e sai de cada PoP.
- Por outro lado, medições mostram que o modelo de independência é frequentemente violado de forma consistente:
  - Influência da distância: caminhos curtos tendem a transportar mais tráfego do que caminhos mais longos.

Tráfego de Controle

- Troca de mensagens de roteamento
- Pode ser medido de duas formas:
  - O volume é importante para a avaliação do desempenho de roteadores.
  - O conteúdo é importante para entender o comportamento do sistema de roteamento.
- A ocorrência de mudanças frequentes nas informações de alcançabilidade ou de topologia da rede trocadas através de protocolos de roteamento é chamada de instabilidade de roteamento.
  - Pode ser causada por erros de configuração ou falhas de links ou equipamento.
  - Pode levar à perda de pacotes, aumento na variabilidade das medidas de desempenho e consumo adicional dos recursos (links e roteadores).

Tráfego de Controle: BGP

- A falha de um roteador BGP pode causar uma "tempestade" de instabilidade:
  - Um roteador sobrecarregado pode deixar de responder a mensagens BGP de Keep-Alive.
  - Os parceiros deste roteador irão então marcá-lo como inalcançável e gerarão atualizações para refletir esta mudança na topologia que serão enviadas a seus parceiros.
  - O roteador sobrecarregado poderá voltar a responder, o que exigirá a recepção de tabelas BGP completas de cada um dos seus parceiros.
  - Este aumento de carga poderá provocar que mais roteadores falhem ou fiquem indisponíveis temporariamente.

Tráfego de Controle: BGP

- Muitas mudanças foram realizadas no BGP e no software dos roteadores para mitigar o efeito destas tempestades.
  - No entanto, medições ainda mostram uma instabilidade considerável na Internet.
  - O roteamento Internet pode apresentar laços de roteamento, mudanças de conectividade de pequenas escalas de tempo, roteamento com oscilações rápidas, entre outras patologias [Pax97a, ZDPS01]

Tráfego de Controle: BGP

- As primeiras medições detalhadas do BGP [LMJ98] mostraram algumas surpresas:
  - Volume de atualizações de roteamento cerca de 10 vezes superior ao esperado
  - A maioria das atualizações de roteamento trocadas via BGP eram redundantes ou patológicas.
  - Mudanças posteriores no software dos roteadores diminuíram mas não eliminaram a geração de mensagens BGP redundantes [LMJ99]

Tráfego de Controle: BGP

- Chegada de mensagens BGP:
  - Extremamente explosivas
  - Periodicidades: 7 dias e 24 horas.
    - Efeito do congestionamento na Internet
  - Demora na convergência
- A instabilidade do BGP apresenta alta variabilidade entre prefixos e destinos.
  - Provém de um conjunto relativamente pequeno de prefixos
    - No entanto, a maioria da instabilidade corresponde a redes com baixas cargas de tráfego [RWXZ02]
  - Interações entre os IGPs e o BGP.

Tráfego de Controle: IGP

- Ao contrário do BGP, o tráfego dos IGPs tendem a ser muito mais estáveis.
- A principal causa de instabilidade no roteamento interno aparenta ser devido a mudanças de rota externas (i.e., BGP) [WJL03]

Sem Fio

- Tráfego que flui em alguma parte do seu caminho através de um link sem fio.
- São mantidas:
  - A estrutura básica imposta por sessões, fluxos e pacotes.
  - Tráfego em rajadas e com variação diária.

Sem Fio: Padrões de Acesso do Usuário

- Larguras de banda média e de pico por usuário são em geral menores que nas redes cabeadas.
  - Pode ser devida ao seu menor desempenho
    - Mas, com a melhoria da tecnologia esta diferença deve diminuir.
- Medidas de atividade dos usuários apresentam alta variabilidade:
  - Duração das sessões
  - Taxa de transferência média por usuário

Sem Fio: Distribuição Espacial

- Diferentemente das redes cabeadas, a localização física dos usuários afeta os padrões de tráfego.
- Os usuários tendem a exibir uma distribuição irregular no espaço.
  - As cargas nos pontos de acesso tendem a ser muito diferente
- Apesar da distribuição irregular dos usuários, as taxas altamente variáveis em que os usuários individuais transferem dados, aparentam ser a causa principal da demanda não equilibrada colocada nos pontos de acesso [BVR02, BC03].

Sem Fio: Mobilidade

- Habilidade do usuário em mudar de posição durante e entre acessos à rede.
- A mobilidade do usuário varia entre diferentes ambientes:
  - Num ambiente de conferência os usuários se movem em bloco (por exemplo, ao final de uma sessão).
  - Em geral apenas uma pequena fração dos usuários é móvel (ativo em dois ou mais pontos de acesso) em um dia.
  - Entre os móveis, muitos se movem pouco, mas pouco são altamente móveis.
- Será que estes mesmos padrões ainda são válidos?!?