

# **Massive Data Analysis: What is under the hood?**

S. (Muthu) Muthukrishnan

Google

`mysliceofpizza`

# Talk Overview

- Data Analysis in Different Communities
  - Algorithms, Databases and Networking
- Infrastructure View of Data Analysis
  - Example 1: Cellphone Call Traffic
  - Example 2: IP Packet Traffic Streams
  - Example 3: Web Traffic
- Perspectives

# Data Analysis in Different Communities

- Networking:
  - Mining anomalies using traffic feature distributions  
A. Lakhina, M. Crovella, C. Diot. SIGCOMM 05.
- Algorithms:
  - Streaming and sublinear approximation of entropy and information distances.  
S. Guha, A. McGregor, S. Venkatasubramanian. SODA 2006.
- Databases:
  - Holistic UDAFs at streaming speeds.  
G. Cormode, T. Johnson, F. Korn, S. Muthukrishnan, O. Spatscheck, D. Srivastava. SIGMOD 2004.

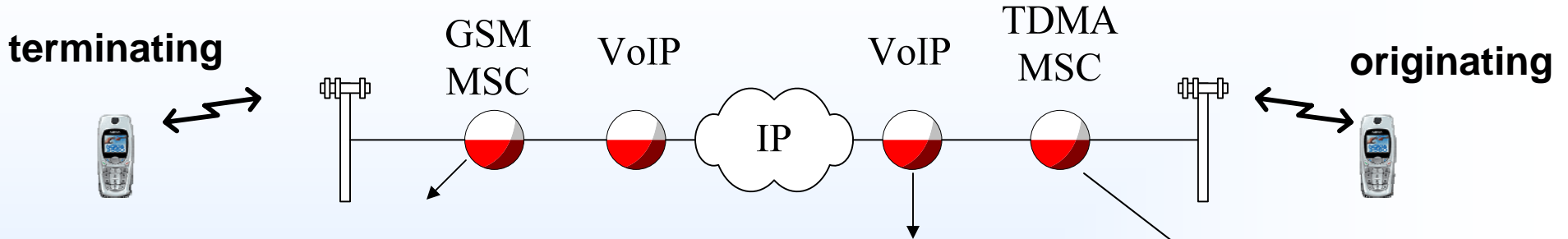
entropy

User defined aggregate function (UDAF), eg., entropy.

# **Infrastructure View, Example 1:**

## **Cellphone Calls Analysis**

# A mobile call: Detailed view of CDRs



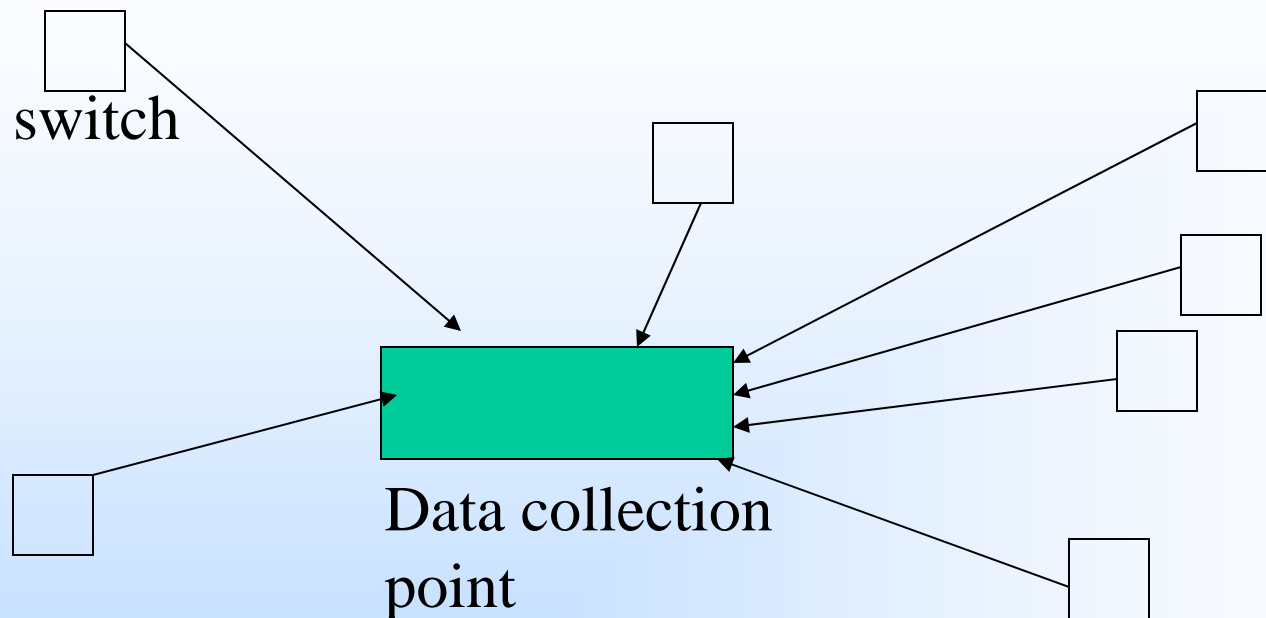
rel	gsm17
scode	3
IMSI	310380049259999
Calling Number	2136109999
Called Number	19493009999
Dialed Digits	
IMEI	352968001799999
Channel Alloc Time	6/26/05 7:28:00
Answer Time	6/26/05 7:28:02
Disconnect Time	6/26/05 7:28:10
Rls Time	6/26/05 7:28:10
Half Rate	0
termcause	004
diag	04127
in adnum	00204
in memkey	00330
out adnum	
out memkey	
in trk seize	6/26/05 7:27:57
out trk seize	
calldur	0000009
BSC in adnum	00520
BSC in memkey	00740
LAC	31038005221
CellID	59165
ChanType	11140
LRN	

Gateway	ANHG2SO
StartTime	6/26/05 7:28:16
Disc_Time	6/26/05 7:28:29
Duration	789
Diag	127
Service	VoIP
ASubNum	2136109999
BSubNum	9516425189 (msrn)
BillNum	9493009999
RouteLabel	RVSDCALBCM5_IM
RouteSelected (Gateway:CLLI)	RVSG5SO:RVSDCALBCM50IMB
LocSIPAddr	155.172.0.9
RemSIPAddr	155.172.0.216
InPSTN_TrkNm	ANHMCACLCM30IMB
InPSTN_CircEnd	1:14:12:7:1079:0x00E37D01:0x00E3C6F2
EgrIP_CircEnd	155.172.0.11:8050/155.172.0.218:8728
PktsOut	620
PktsIn	617
GSX Call Handle	GSX2GSX,0x380D6441
DialedNum	9494661933 (lrn)
GenAddr	9493009999
InCodec	C:1:1
OutCodec	P:1:1
OrigEchCanc	1

Record_type	04
Call_status	2
Call_ID_number	01586580
A_subscriber_number	2136109999
B_subscriber_number	9493009999
Date_for_start_of_charging	6/26/05 7:29:00
Chargeable_duration	7
Time regsz	5
Abnormal_call_release	1
Internal_Cause_and_Location	027B
Outgoing_route	AN2AMGO
Incoming_route	C736CKI

"Transmission fault, incoming" (dropped call)

# Analyzing CDRs: Data

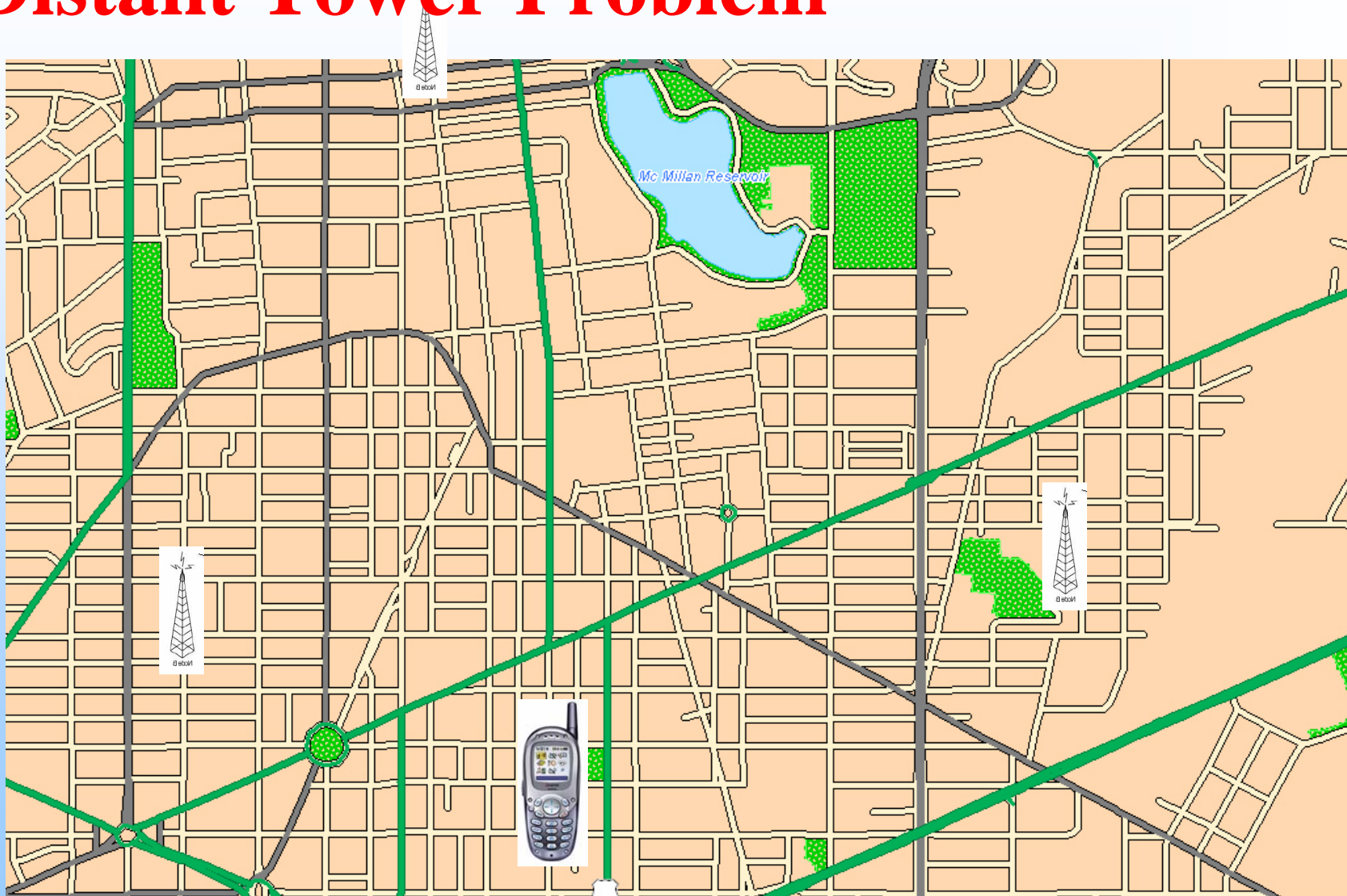


- Data:
  - **TDMA**: Ericsson, Lucent, and Nortel MSCs; **GSM and UMTS**: Nortel MSCs; **VoIP**: Sonus Media Gateways; **GPRS**: Nortel SGSNs, GGSNs, and MMSCs; **SMS logs**.
  - 20 - 30 different data formats.
  - Side tables: LERG. Handset info. Trunk info.
  - About 1 Tbyte/month.

# Analyzing CDRs: Analyses

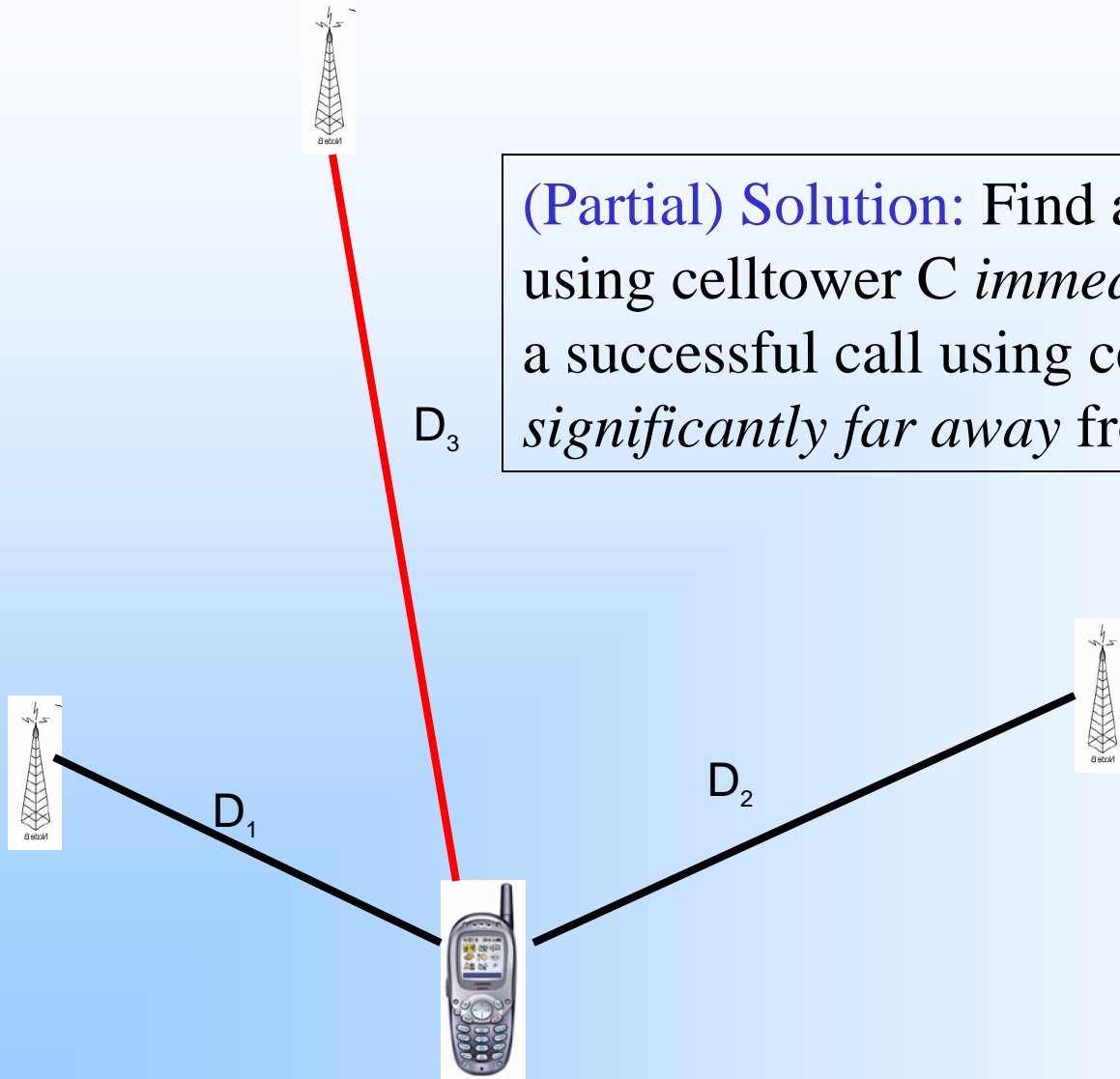
- Analyses:
  - 100's of reports a month.
- Example Analyses:
  - Dropped calls per handset type
  - Glare detection
  - 2A or 2B connections.
  - Fraudulent transit calls
  - Cell adjacency graph

# Example Analysis: Distant Tower Problem





# Distant Tower Problem



(Partial) Solution: Find a dropped call using celltower C *immediately preceding* a successful call using celltower D *significantly far away* from C.

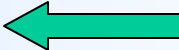
# Analyzing CDRs: Infrastructure

- Challenge is not the size of the data.
  - understanding the data, translating a business problem down to CDR analysis.
- Turnaround time: Days or weeks.
- Small team of analysts responsible.

## Infrastructure:

- Large disks.
- Multiple CPU machines.
- Scripting languages, standard file system.

# Talk Overview

- Data Analysis in Different Communities
  - Algorithms, Databases and Networking
- Infrastructure View of Data Analysis
  - Example 1: Cellphone Call Traffic
  - Example 2: IP Packet Traffic Streams 
  - Example 3: Web Traffic
- Perspectives

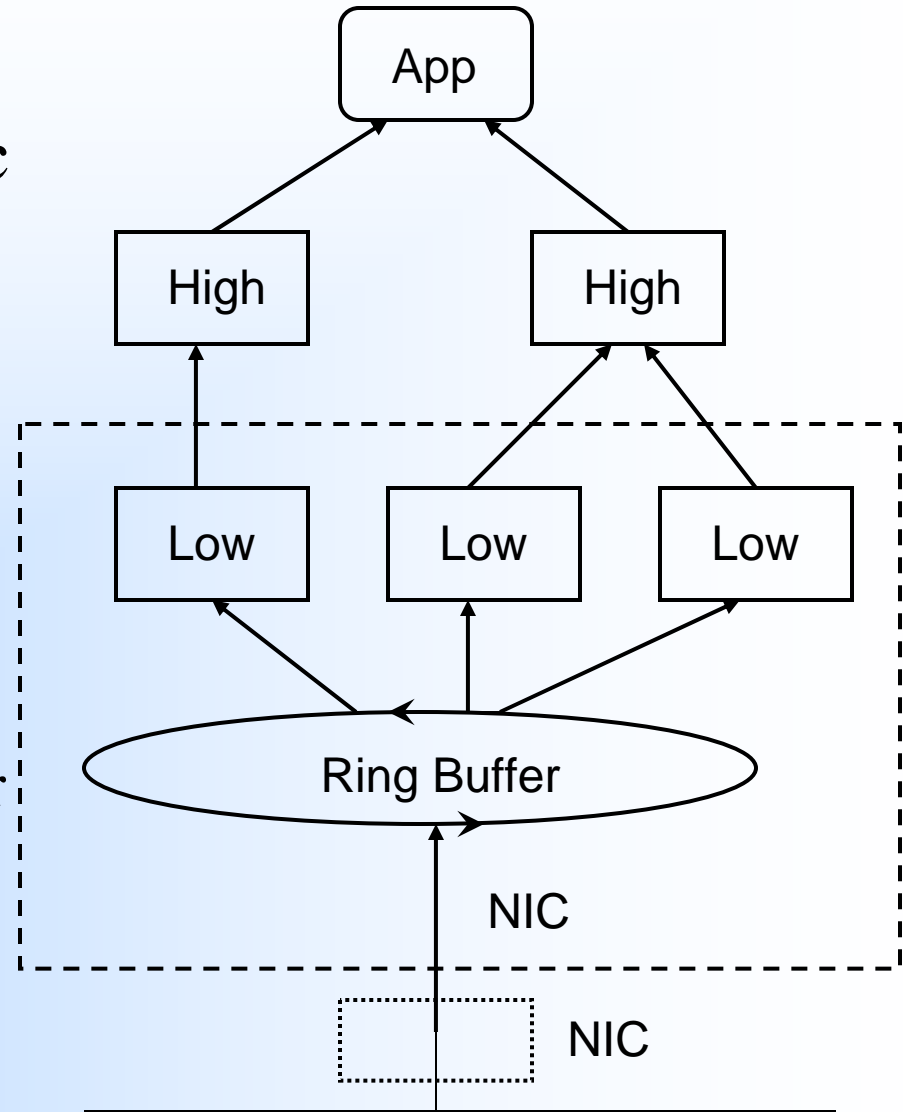
# **Infrastructure View:** **IP Traffic Analysis**

# Analyzing IP Traffic (ISP View): Data

- SNMP, IP flows, **packet header logs**, packet contents, routing tables, BGP updates, fault alarms.
- OC48, 192, 768: xTbytes/hour. 6M -- 96M pkts/sec.
- Real time, router speed analysis.
- Example:
  - Reporting, SLA mediation.
  - Anomaly/Attack detection.
  - Lawful intercept
  - Monitoring failures.
  - Traffic classification.

# Gigascoppe Architecture

- Gigascoppe is an SQL-based operational IP traffic analysis tool at AT&T.
- Has two level arch.
  - Low-level queries perform initial fast selection and aggregation on high speed stream.
  - Complex aggregation on high level, at monitor server
- Depending on the capabilities of the NIC, can push operators and low-level queries into it.



# GSQL Query Splitting

```
Select tb, SrcIP, count(*)  
From UDP  
Group By  
time/60 as tb, SrcIP
```

High  
level

```
Select tb, SrcIP, sum(Cnt)  
From Subq  
Group By tb, SrcIP
```

Subq:

Low  
level

```
Select tb, SrcIP,  
count(*) as Cnt  
From UDP  
Group By  
time/60 as tb, SrcIP
```

# Gigascoppe, Status

Currently supports:

- GSQL, UDAFs.
  - stream aggregate queries.
- Sampling.
  - **Operator** can be specialized to most stream sampling methods.
  - Most complex queries can be executed with **semantic sampling** to provide correct output.
- Regex matcher for flows.
  - Match contents across packets in presence of duplicates, out-of-order or overlapping packets.
- Heartbeats.
  - Prelim distributed implementation.
- Query-aware query partitioning.
- Deployed

Ted Johnson S. Muthukrishnan  
Irina Rozenbaum Vlad Shkapenyuk  
Oliver Spatscheck.



# Sampling Operator

- Many sampling algorithms known for IP traffic streams.
  - Uniform random sampling
  - Priority sampling
  - Value sampling
  - Distinct, inverse, minwise sampling.
- Observation:
  - Most sampling algorithms have a overall common execution structure.
- Our approach:
  - Define and optimize a **single** sampling operator.

# Stream Sampling Operator

- Operator:

```
Select <select expression list>.  
From <stream>.  
Where <predicate>.  
Group by <group-by variables definition list>.  
Cleaning when <predicate>.  
Cleaning by <predicate>.  
[Having <predicate>].
```

- **Cleaning when** – condition for triggering a cleaning phase.
- **Cleaning by** – condition for sample reduction.

- Can be specialized for wide variety of stream sampling algorithms.
- Encourages experimentation and development of new sampling algorithms.

T. Johnson, S. Muthukrishnan and I. Rozenbaum, SIGMOD 2002.

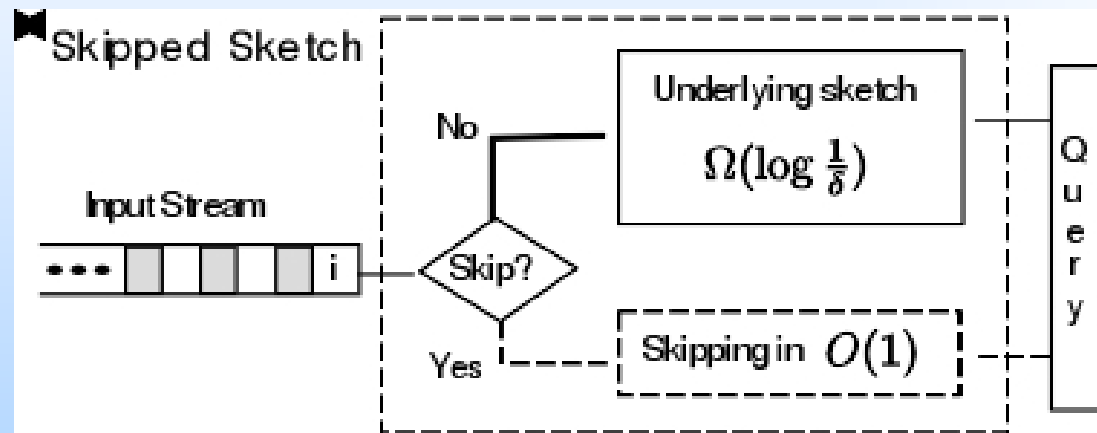
# Sampling Operator

## War story:

- During SYN flooding and DDOS attacks, Cisco Netflow generator is overwhelmed and produces useless output.
- Packet sampling does not provide accurate flow samples.
- By combining flow sampling and flow generation logic using the sampling operator, **Gigascop**e produces meaningful, valuable flow samples even at peak rates of flows such as in attacks.

# Example Analysis

- Heavy hitter q-gram in packet contents.
- Design sampling+sketching method to skip over vast number of packets.



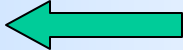
- Orders of magnitude improvement over prior work in networking, skipping fraction of packets.

S. Bhattacharyya, A. Maderia, S. Muthukrishnan and T. Ye.  
Sprint ATL Technical Report, 2006.

# IP Traffic Analysis: Infrastructure

- Challenge:
  - Size, rate of data. Analyses: Simple.
  - Turnaround time: Minutes, days.
  - Moderate sized team of analysts.
- Special infrastructure:
  - Optical splitters, NIC
  - Multiple CPU machines
  - Data stream management systems (DSMSs): different architectures.

# Talk Overview

- Data Analysis in Different Communities
  - Algorithms, Databases and Networking
- Infrastructure View of Data Analysis
  - Example 1: Cellphone Call Traffic
  - Example 2: IP Packet Traffic Streams
  - Example 3: Web Traffic 
- Perspectives

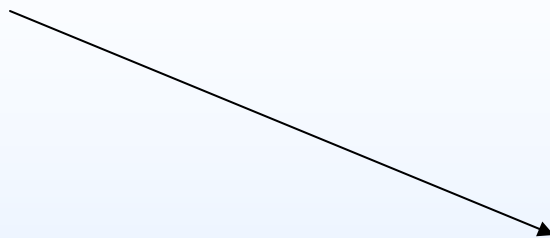
**Infrastructure**

**View:**

**Web Traffic**

**Analysis**

# Google



Search

Web

Image

Video

News

Usenet Groups

Blogs



# Google: Calculator Co.

2\* pi^2 sq ft = ? sq m - Google Search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.google.com/search?hl=en&lr=&q=2\*+pi%5E2+sq+ft+%3D+%3F+sq+m&btnG=Search


Getting Started Latest Headlines

Sign in

Google Web Images Video <sup>New!</sup> News Maps more »

2\* pi^2 sq ft = ? sq m Search [Advanced Search](#) [Preferences](#)

**Web**

 **2 \* (pi^2) (sq ft) = 1.8338325 sq m**

[More about calculator.](#)

Search for documents containing the terms [2\\* pi^2 sq ft = ? sq m](#).

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2006 Google

Done

start Wireless Net... Minenet06 muthu@drag... 2\* pi^2 sq ft ... aramis.rutger... Microsoft Pow... 10:22 AM

# Google: Advertising

The screenshot shows a Mozilla Firefox browser window with the title "fly fishing - Google Search - Mozilla Firefox". The address bar contains the URL "http://www.google.com/search?hl=en&q=fly+fishing&btnG=Google+Search". The search bar contains the text "fly fishing" and the search button is labeled "Search". The search results are displayed under the heading "Web" and show "Results 1 - 10 of about 26,200,000 for fly fishing [definition]. (0.27 seconds)".

The search results are organized into two columns of sponsored links:

- Left Column:**
  - The Fly Tying Station** (Sponsored Links): [www.FlyTyingStation.com](http://www.FlyTyingStation.com) Your own fly tying station. Tie your own flies.
  - Fly Fishing Superstore** (Sponsored Links): [www.sportfish.co.uk](http://www.sportfish.co.uk) World's Top Fly Fishing Tackle Shop Worldwide Shipping & 7000 Products
  - Fly fishing equipment - fly-fishing tackle, fly fishing rods, fly ...**: Fly fishing equipment, discount fly-fishing tackle Flyrods - Fly fishing equipment fly tying supplies and accessories. [www.flyshop.com/](http://www.flyshop.com/) - 14k - [Cached](#) - [Similar pages](#)
  - FlyFish.com | The Online FlyFishing Resource Guide**: FlyFish.com is the online resource guide for fly fishing resources, fishing reports, fly tying instructions, news, hot product reviews, forums, and events. [www.flyfish.com/](http://www.flyfish.com/) - 15k - [Cached](#) - [Similar pages](#)
  - Fishing.com - Leading the world to the water - Your online fishing ...**: Fly Fishing ... Fishing continues to be a favorite pastime in the United States, in 2001, 16% of the US population 16 years old and older (34 million ... [www.fishing.com/](http://www.fishing.com/) - 28k - [Cached](#) - [Similar pages](#)
  - The Orvis Company, Since 1856, quality. Men's Clothing, Women's ...**: Quality fly fishing gear, womens clothing, mens clothing, travel clothing, dog beds, Barbour, men's leather jackets and outerwear, BUZZ OFF and gifts. [www.orvis.com/](http://www.orvis.com/) - 29k - [Cached](#) - [Similar pages](#)
  - Fly Fisherman**: Fly Fisherman magazine is the authoritative source for fly fishing destinations and
- Right Column:**
  - The Flyshop-Online** (Sponsored Links): Hardy-Sage-Greys-Loop-Vision Online Discounts Help and Advice [www.flyshop-online.co.uk](http://www.flyshop-online.co.uk)
  - Online Fly Fishing Gear**: Your complete online Fly Fishing retailer. Low Prices/ Free Shipping [jfisheronline.com](http://jfisheronline.com)
  - Trout Flies Online UK**: Quality flies - Subscribe to free newsletter for year round discount [www.fliesonline.co.uk](http://www.fliesonline.co.uk)
  - Fisheyesoup.com**: current fishing reports from professionals around the world [www.fisheyesoup.com](http://www.fisheyesoup.com)
  - Fly fishing**: Taimen fishing in Mongolia Guided fly-fishing & float trips [FishMongolia.com](http://FishMongolia.com)
  - Flies Buy The Dozen**

The taskbar at the bottom shows the Windows Start button, several open applications including "Wireless Network ...", "muthu@dragon.rut...", "Capture a Screen ...", "fly fishing - Google ...", and "aramis.rutgers.edu...", and the system clock showing "10:18 AM".

# Google

↓  
Search

Web  
Image  
Video  
News  
Usenet Groups  
Blogs

↘  
Calculator  
Co.

Convert units,  
Calculate.

↘  
Advertising

AdWords  
AdSense  
Partner sites  
Coupons

↘  
Earth  
Map  
Finance  
Trends  
Writely  
Personalize  
Froogle  
....

# Example: Sponsored Search

- Advertisers want to place ads in response to user queries.
- Search companies place ads by running an **auction** in response to user queries.
- Have to figure out what queries are interesting, how much to bid on each query, what is the budget,...

# Google Sponsored Search Auction



Campaign Management

Reports

Analytics

My Account

Campaign Summary | Tools | Conversion Tracking

Tools > Traffic Estimator

## Traffic Estimator

Get quick traffic estimates for new keywords without adding them to an account or using the AdWords sign-up wizard.

### 1. Enter keywords, one per line:

fishing  
fly fishing  
fly ties  
big game fishing  
whale hunting

keyword = broad match  
[keyword] = exact match  
"keyword" = phrase match  
-keyword = negative match

Set optional individual CPCs using this format:  
keyword\*\*0.25

### 2. Choose a currency. Enter a specific Max CPC for your estimates, or leave the field blank and we'll provide estimates based on our suggested Max CPC.\*

US Dollars (USD \$) .15

\*Suggested value should deliver ads in the top position 85% of the time.

### 3. Choose daily budget (optional). See estimates for the amount you want to spend each day, or leave field blank to see all available clicks.

### 4. Select targeting.

#### a. Language

All Languages  
-----  
English  
Chinese (simplified)  
Chinese (traditional)  
Danish  
Dutch

#### b. Location Targeting

Countries and territories - choose countries  
 Regions and cities - choose states and regions and/or enter cities  
 Customized - enter a radius and address or coordinates

#### c. Countries

##### Available Countries and Territories

All Countries and Territories  
-----  
Australia  
Austria  
Belgium  
Brazil  
Canada

##### Selected Countries and/or Territories

All Countries and Territories

Add »

« Remove

Continue »

# Traffic Estimation for Sponsored Search

The screenshot shows the Google AdWords Traffic Estimator interface. The browser window title is "Google AdWords: Traffic Estimator - Mozilla Firefox". The address bar shows the URL "https://adwords.google.com/select/mair". The page header includes the Google AdWords logo, the user's email "feldman.jon@gmail.com", and links for Help, Contact Us, and Sign Out. The navigation menu includes Campaign Management, Reports, Analytics, and My Account. The main content area is titled "Traffic Estimator" and includes a "Tools > Traffic Estimator" breadcrumb. Below this, there is a summary of estimates: Average CPC: \$0.10 (at a maximum CPC of \$0.15) and Estimated clicks per day: 1,618 - 2,426 (at a daily budget of \$350.00). A table below shows the estimated traffic for various keywords, including Search Total, big game fishing, fishing, fly fishing, fly ties, and whale hunting. The table columns are Keywords, Search Volume, Estimated Avg. CPC, Estimated Ad Positions, Estimated Clicks / Day, and Estimated Cost / Day. The footer of the page includes the copyright notice "©2006 Google" and links to AdWords Home, Editorial Guidelines, Privacy Policy, and Contact Us.

Google AdWords: Traffic Estimator - Mozilla Firefox  
https://adwords.google.com/select/mair  
Getting Started Latest Headlines Google Engineering: ...  
Google AdWords: Traffic Es... snapshot4.png (PNG Image, 384...  
Google AdWords feldman.jon@gmail.com | Help | Contact Us | Sign Out  
Customer ID: 353-603-9641  
Campaign Management Reports Analytics My Account Advanced Search  
Campaign Summary | Tools | Conversion Tracking Search my campaigns: Search  
Tools > Traffic Estimator  
Traffic Estimator  
Revise settings | Download as .csv  
All estimates are provided as a guideline, and are based on system-wide averages; your actual costs and ad positions may vary. To view estimates based on your keywords' performance history, use the Traffic Estimator within the appropriate Ad Group. Learn more  
Average CPC: \$0.10 (at a maximum CPC of \$0.15) Estimated clicks per day: 1,618 - 2,426 (at a daily budget of \$350.00) Estimates are based on your bid amount and geographical targeting selections. Because the Traffic Estimator does not consider your daily budget, your ad may receive fewer clicks than estimated.  
Maximum CPC: .15 Daily budget: Get New Estimates  
Keywords Search Volume Estimated Avg. CPC Estimated Ad Positions Estimated Clicks / Day Estimated Cost / Day  
Search Total \$0.06 - \$0.14 1 - 3 1,618 - 2,426 \$100 - \$350  
big game fishing \$0.05 - \$0.13 1 - 3 1 - 3 \$1  
fishing \$0.06 - \$0.14 1 - 3 1,513 - 2,263 \$100 - \$330  
fly fishing \$0.06 - \$0.15 1 - 3 103 - 157 \$7 - \$30  
fly ties \$0.00 - \$0.15 4 - 6 0 - 1 \$0 - \$1  
whale hunting \$0.05 - \$0.08 1 - 3 1 - 2 \$1  
Estimates for these keywords are based on clickthrough rates for current advertisers. Some of the keywords above are subject to review by Google and may not trigger your ads until they are approved. Please note that your traffic estimates assume your keywords are approved.  
©2006 Google - AdWords Home - Editorial Guidelines - Privacy Policy - Contact Us  
Done adwords.google.com

# Example Analysis: Traffic Estimation

- **Problem:** Given a set of queries and a potential bid, output the distribution of
  - Number of clicks expected
  - Expected position on the ad list
  - Expected price.
- **Input:** queries, ads shown, bids, price, etc. Terabytes of data on 1000's of commodity machines.

# MapReduce [Dean, Ghemawat OSDI04]

- Parallel programming infrastructure at Google.
- Users specify map and reduce functions.
- **Input:** set of records.
  - Each record is **mapped** to a set of (key, value) pairs.
  - All pairs with same key are considered together and a **reduce** function is applied to the values.
- System automatically takes care of
  - Parallelizing on 100's++ commodity machines.
  - Fault tolerance
  - Scheduling, load balance, locality, inter-machine communication, etc.



# Traffic Estimation Using MapReduce

- Logs consist of  $(q, b_1, p_1, b_2, p_2, \dots, c)$ .
  - $q$  is the query.
  - $b_i$  is the bid of advertiser in  $i$ th place and  $p_i$  the price.
  - $c$  is the ad clicked on.
- **Map** to  $(q, b_i, p_i, i, 1 \text{ if } c=i)$  for all  $i$ ;  $q$  is the key.
- **Reduce** will have all records with same  $q$ . Calculate.
  - number of clicks,
  - average position,
  - average cost per click, etc.
- Run this periodically and index for each  $q$ . Lookup when needed.

# Web Traffic Analysis: Infrastructure

- Terabytes of data on 1000's of commodity machines.
- 100's of engineers running many analyses simultaneously any day.
- Enormously successful at Google for machine learning, graph computing to index generation.

MapReduce was used for 29k jobs, dealt with 3k TB, 300+ programs, 79k machine days, in Aug 04, [OSDI04]

# MapReduce

$\log(n)$   
bits per  
record

$n/M$  records

$n/M$  records

$n/M$  records

$M$  machines

MAP

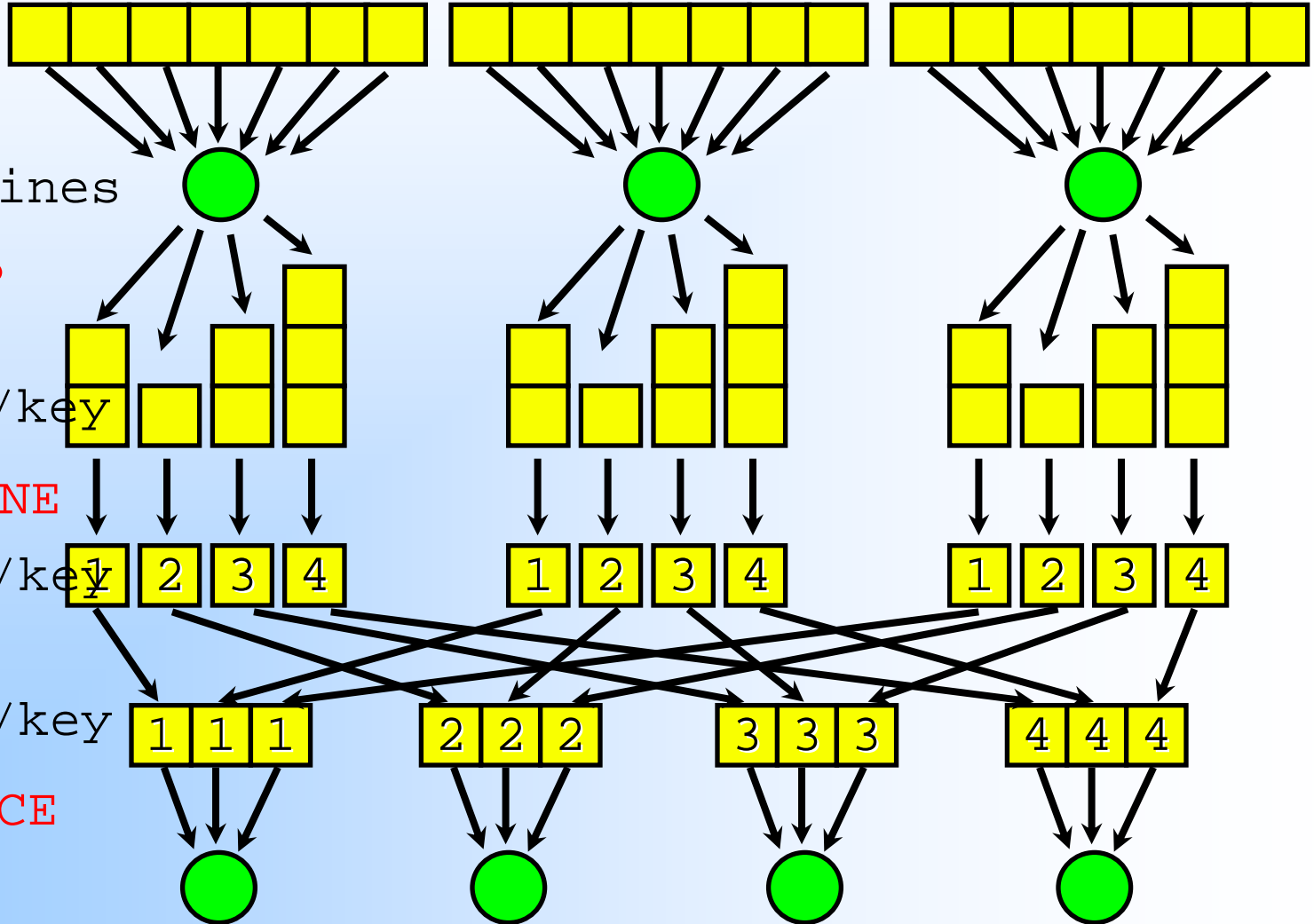
1 list/key

COMBINE

1 record/key

1 stream/key

REDUCE

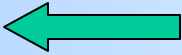


# MapReduce: Theoretical Model

- **MUD Model:** Assume each mapper is a stream, each reducer is a stream, and there is a single key.
  - Looks like **distributed** streaming.
- How is MUD related to streaming?
- For symmetric, total exact functions: **MUD = SS**.
- For promise problems and approximate functions, **MUD  $\neq$  SS**.
- With multiple keys, we can simulate PRAM.
- **Open Problem:** Given **k** keys and **l** rounds, can you solve various problems.

J. Feldman, S. Muthukrishnan, T. Sidiropoulos, Z. Svitkina, C. Stein.

# Talk Overview

- Data Analysis in Different Communities
  - Algorithms, Databases and Networking
- Infrastructure View of Data Analysis
  - Example 1: Cellphone Call Traffic
  - Example 2: IP Packet Traffic Streams
  - Example 3: Web Traffic
- Perspectives 

# Summary

Cellphone traffic (cellco)	IP Traffic (ISP)	Web Traffic (Search Engine)
TB/month weekly/monthly Reports.	TB/hour min/hours/days Detect attacks, appl.	PB/month hours/days Nearly all services.
Small team of analysts.	Small/Moderate # of researchers	Large number of engineers/analysts
File system, script language, parallel CPUs.	Optical splitters, NICs, stream mgmt engines.	1000's of m/c's, GFS, MapReduce, Bigtable, ...
No publications	Alg/DB since 96. Mainly publ.	Mainly systems.

# Acknowledgements

- Thanks to Nathan Hamilton for 5+ years of cellular data analysis.
- Thanks to colleagues at Sprint, AT&T, Narus, Google.
- Thanks to students at Rutgers.

