AGH University of Science and Technology

Trace2Flow

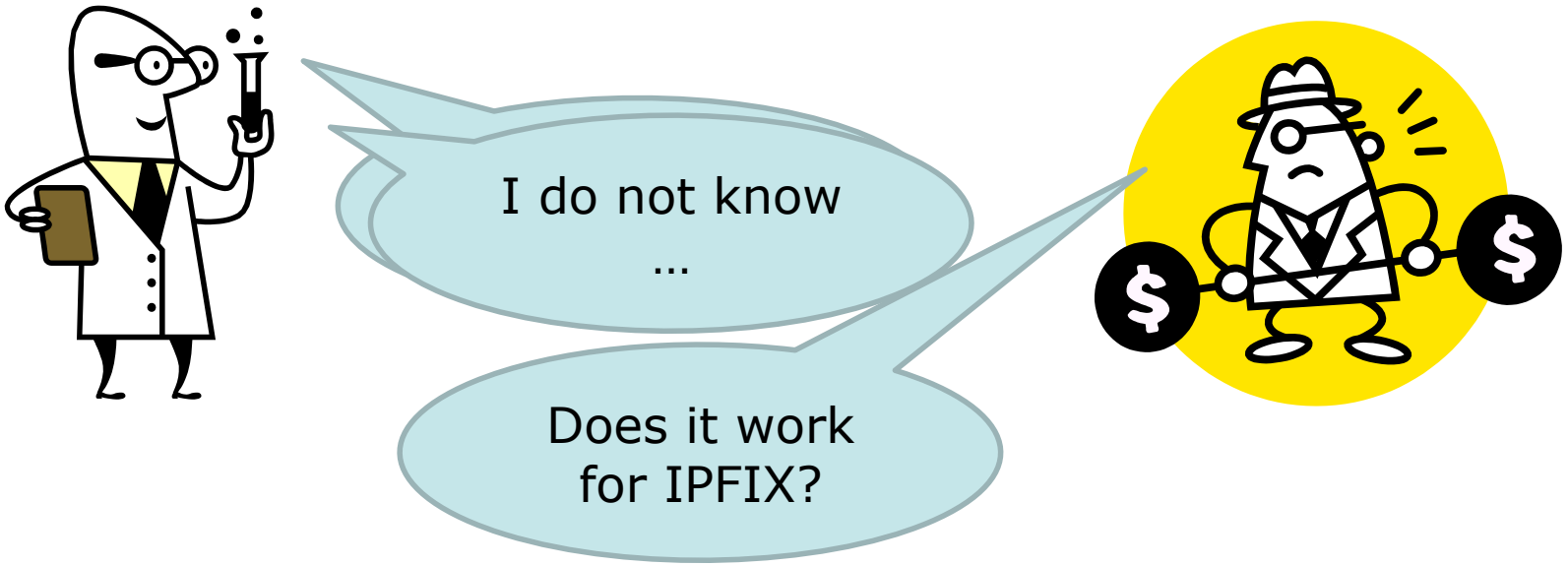
Karol Adamski, Maciej Korczyński, Lucjan Janowski, Krzysztof Rusek

3rd NMRG Workshop on Netflow/IPFIX Usage in Network Management
July 30, 2010, Maastricht

Motivation

I am a member of the COST TMA Action IC0703

(see www.tma-portal.eu)



Solution

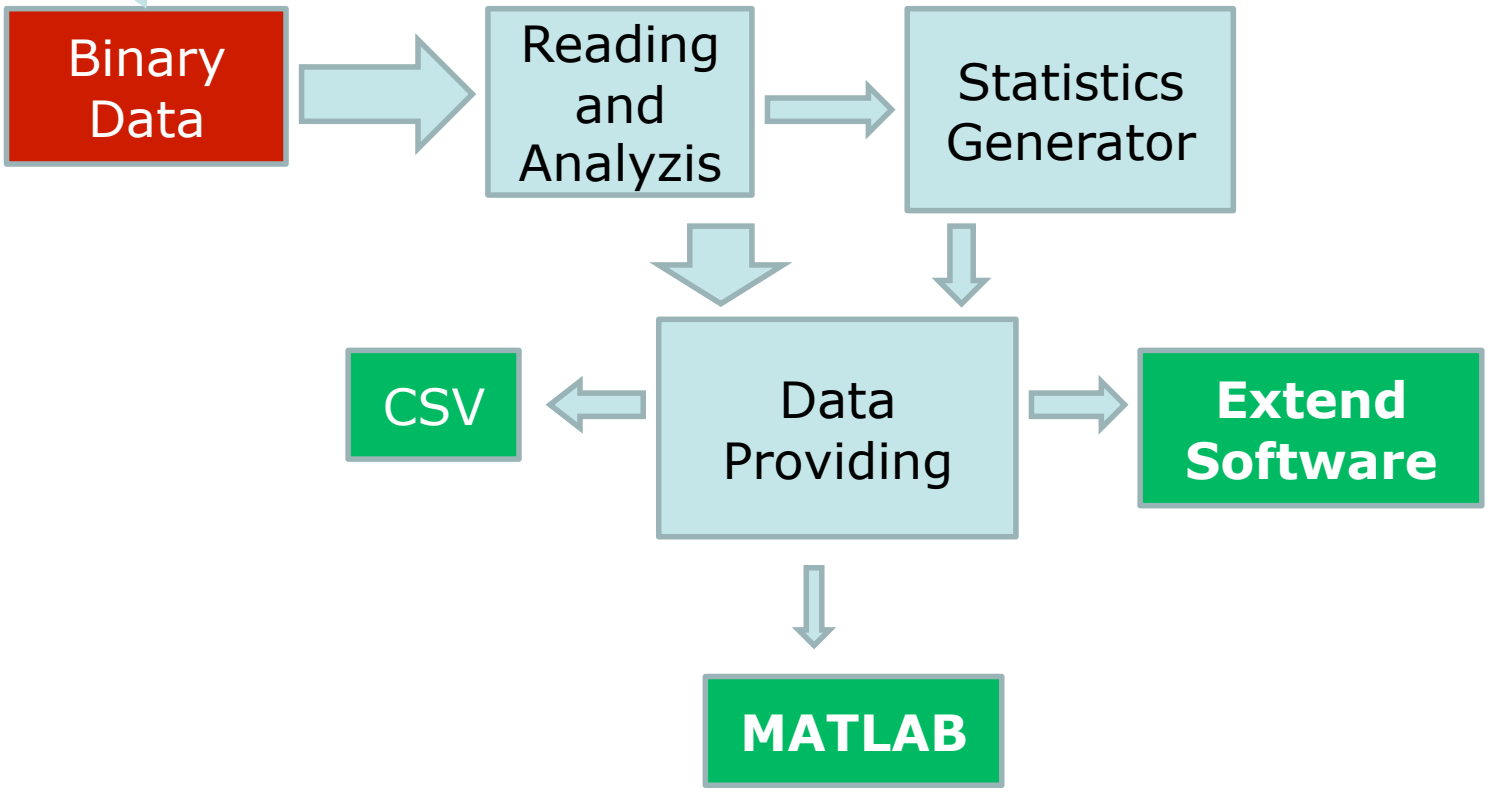
- We should have a tool to generate a IPFIX trace from packet trace and use both of them …
- … so that anyone can compare both packet and IPFIX algorithms
- The conversion should be easy and flexible
- It should work for many operating systems
- We have TracesPlay (http://tracesplay.sourceforge.net/)
  - a tool reading packet traces which work for different operating systems

Whole system

Formats: PCap, ERF, TSH, FR, FR+, SNOOPv2
On-line with lib PCAP
From a buffer

ETH, 802.1q, 802.11, ICMPv4, IPv4, TCP, UDP, RTP, H264, NetFlow v1,5,7,8,9
.....

IPFIX ,
Different samplig methods



Trace2flow Options

- ***-IPFIX <value>*** the flow definition
- ***–c*** the first column of CVS file contains the column name
- ***-e*** show error
- ***–r <file name>*** list of the traces to analyze
- ***–o <fields name>*** list of the IPFIX fields
- ***–s <sampling methods>*** OneToOne, OneToN <value>, RandomFromN <value>, FirstFromTimeIntercal <value>
- ***–w <file name>*** output file, *out.txt by default*

Supported fields

Field Name	Description
IPFIX.inByte	Number of bytes
IPFIX.inPkts	Number of packets
IPFIX.IP.src	Source IP address
IPFIX.IP.dst	Destination IP address
IPFIX.MinTTL	Minimum TTL value
IPFIX.MaxTTL	Maximum TTL value
IPFIX.MinPktLength	Minimum packet length
IPFIX.MaxPktLength	Maximum packet length

Examples

trace2flow.exe -e -s OneToOne –IPFIX 1 -r test.pcap -o IPFIX.inPkts IPFIX.inBytes IPFIX.MinTTL -w out_OneToOne.txt

trace2flow.exe -s OneToN 25 –IPFIX 3 -r test.pcap -o IPFIX.IP.src IPFIX.inBytes IPFIX.MaxTTL –c -w out_OneToN_3.txt

MATLAB:

Data = trace2flow(-s OneToN 100 –IPFIX 1 -r test.pcap -o IPFIX.inPkts);

A Simple Example

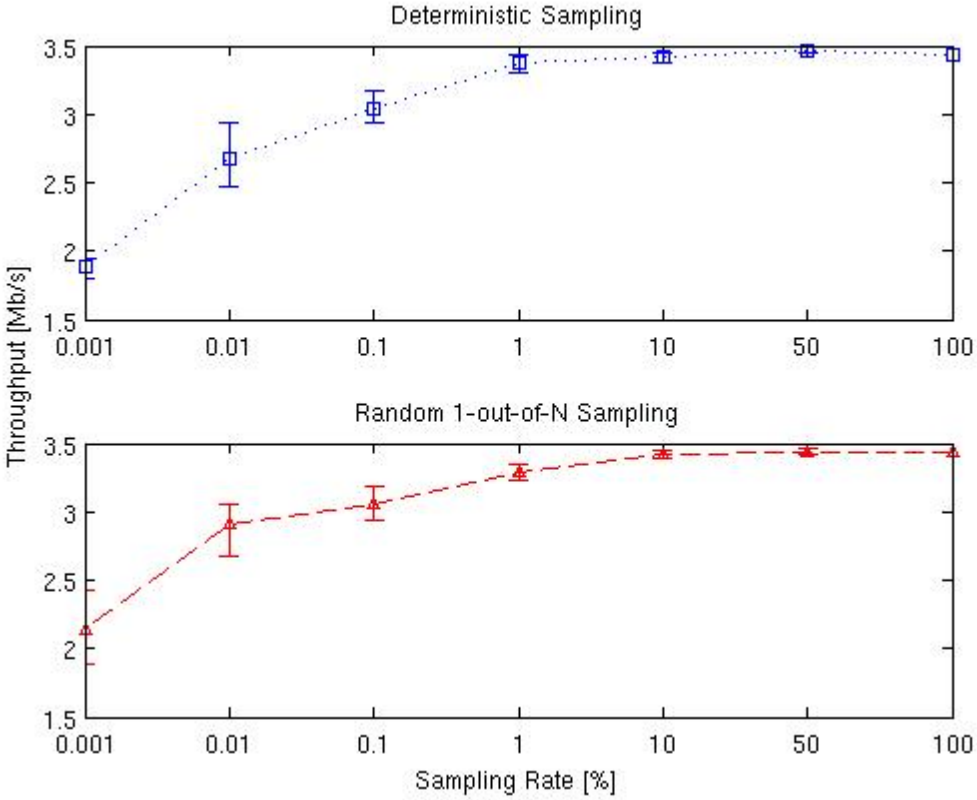
- Packet trace captured within one of subnetworks in campus network in AGH University of Technology in Krakow:
  - amount of packets: 1273722
  - packet duration: 180.8632 s
  - trace size: 100MB
  - average throughput at the time of traffic capturing: 3.45 Mb/s

Throughput Estimation

- Two representative count-based methods were examined (as they are used in Cisco routers):
  - Deteministic Sampling (every n-th packet)
  - Random Sampling (1-out-of-N packet)

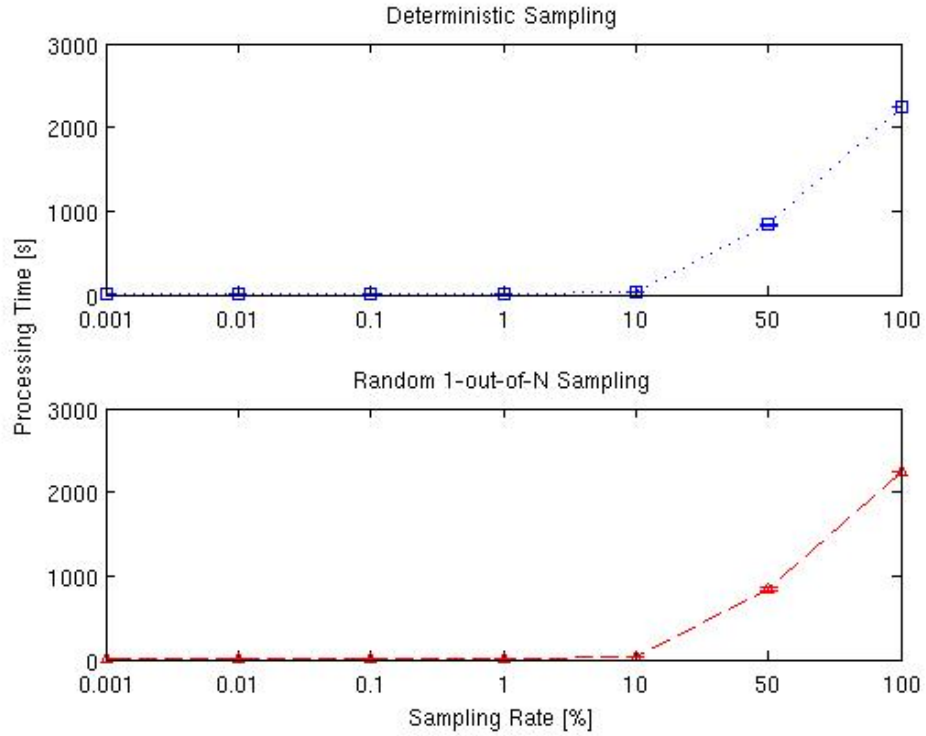
Throughput Estimation - Results

- Underestimation of the throughput for sampling rates lower than 10%



Throughput Estimation - Results

- For sampling rates lower than 10% the time required for processing all packets is lower than 2s in the particular case



Where You Can Find Us

The project web page

http://tracesplay.sourceforge.net/traces2flow/index.html

The Mather project

http://tracesplay.sourceforge.net/