Location-aware Network Monitoring using IPFIX/NetFlow

Abdelkader Lahmadi Julien Vaubourg Olivier Festor
Université de Lorraine
Rick Hofstede Aiko Pras
University of Twente

NMRG meeting

July 30, 2013
(compiled on: July 26, 2013)

Outline

- Context and motivation
- Information Elements
- Flowoid and SURFmap
- Conclusion and Future directions

Location-aware network monitoring

Flow-based monitoring provides an aggregate view on the network traffic

- Data is usually exported from fixed locations
- If mobile devices become flow exporter, exporter location can be of interest!

Smartphone traffic usage in space: simple questions

- Where often do users interact with their phones?
- How many applications does a user run in a specific location?
- How much network traffic does an application generate in a specific location?

Why we need to know such information?

- Coupling space and time to understand mobile applications network usage: relate service quality parameters to location changes
- Anomaly detection, provider-independent measurements

Associate locations to exported Flows

- *draft-festor-ipfix-metering-process-location-01.txt*
- Geographic coordinates: latitude, longitude, altitude
- Civic location: human readable information, postal address, proximity information

IPFIX Information Elements: geodetic location

Geodetic point record: there is no known uncertainty

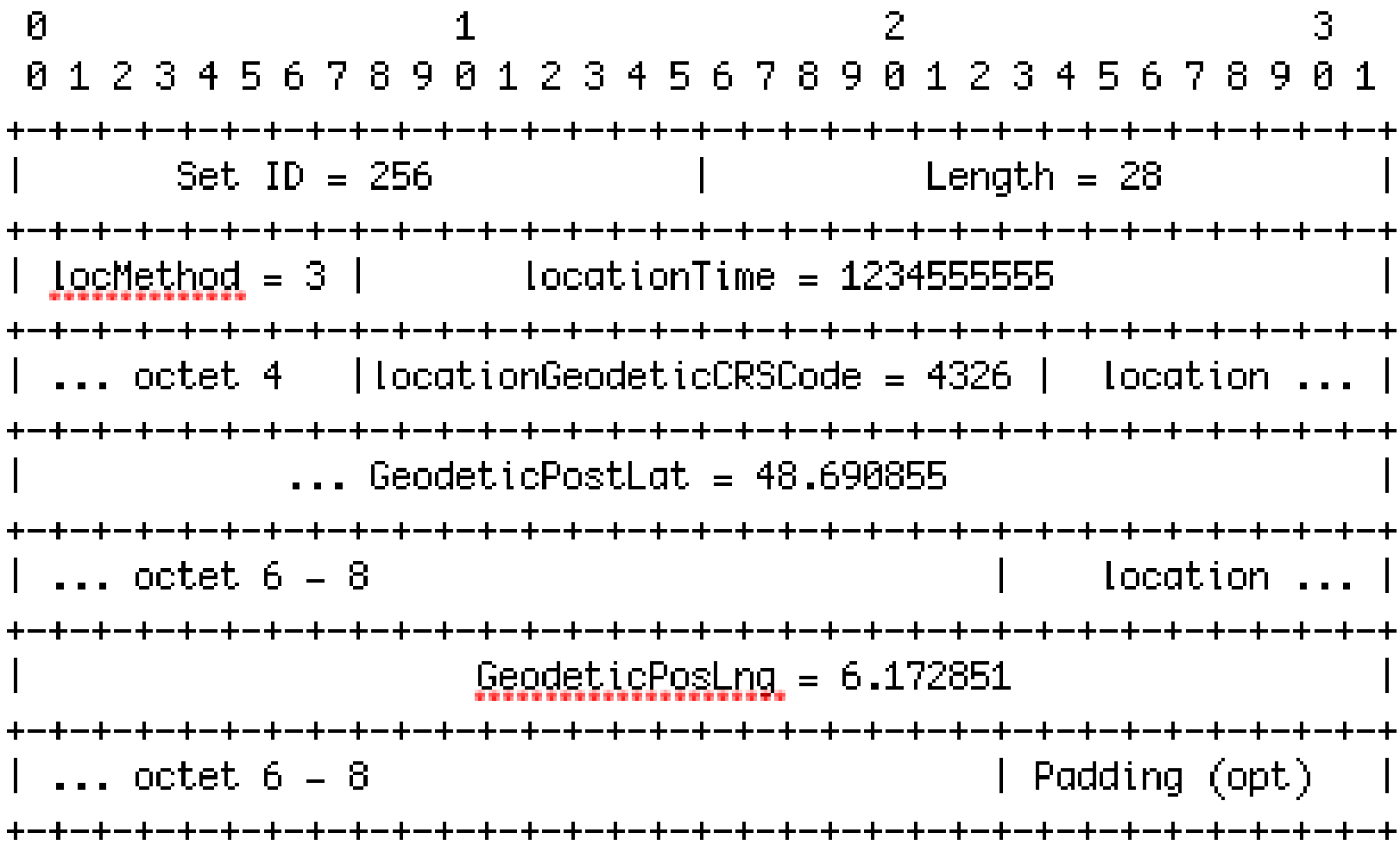


Figure 2: Data record of a geodetic 2D point location

IPFIX Information Elements: geodetic location

Geodetic circle record: there is known uncertainty

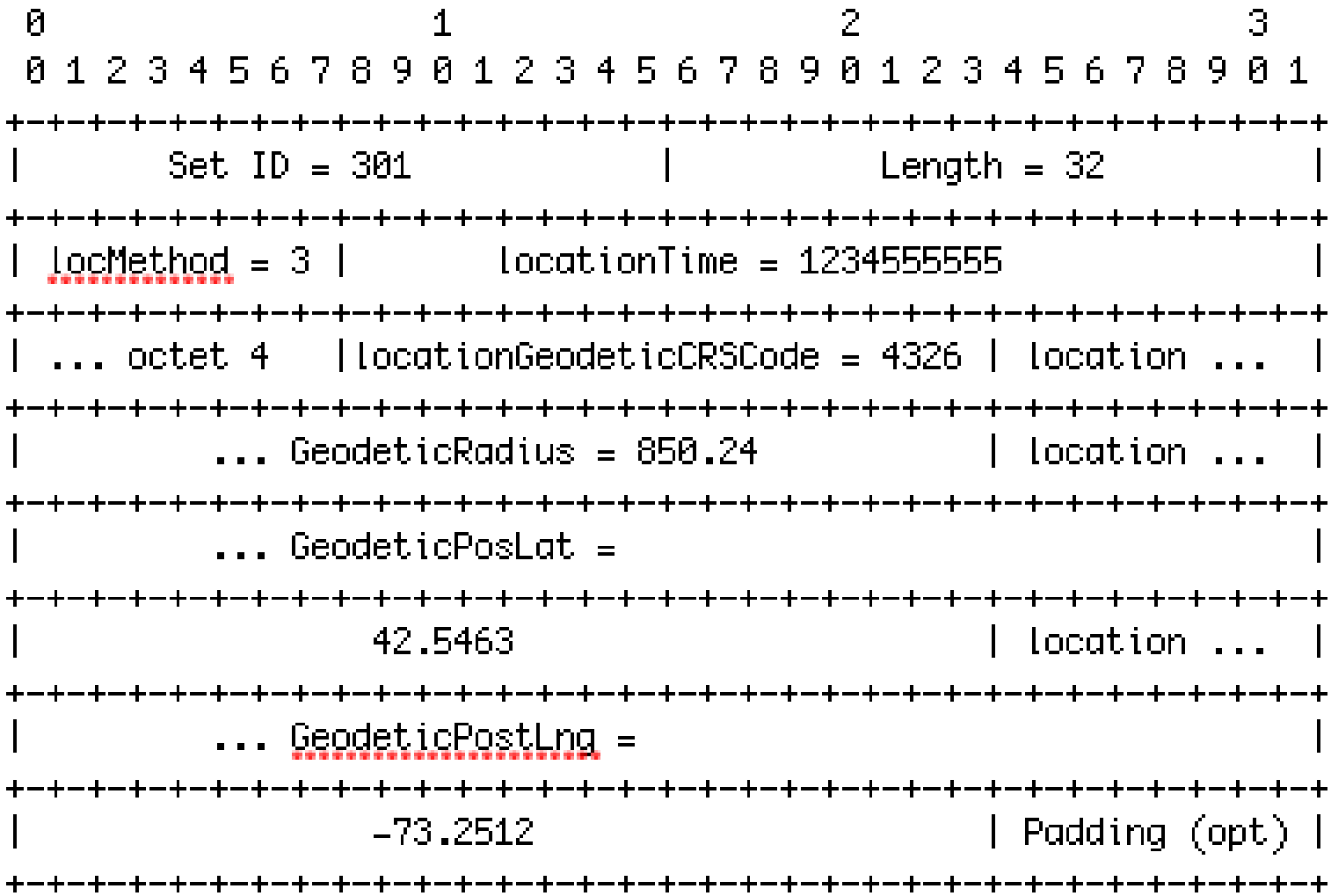
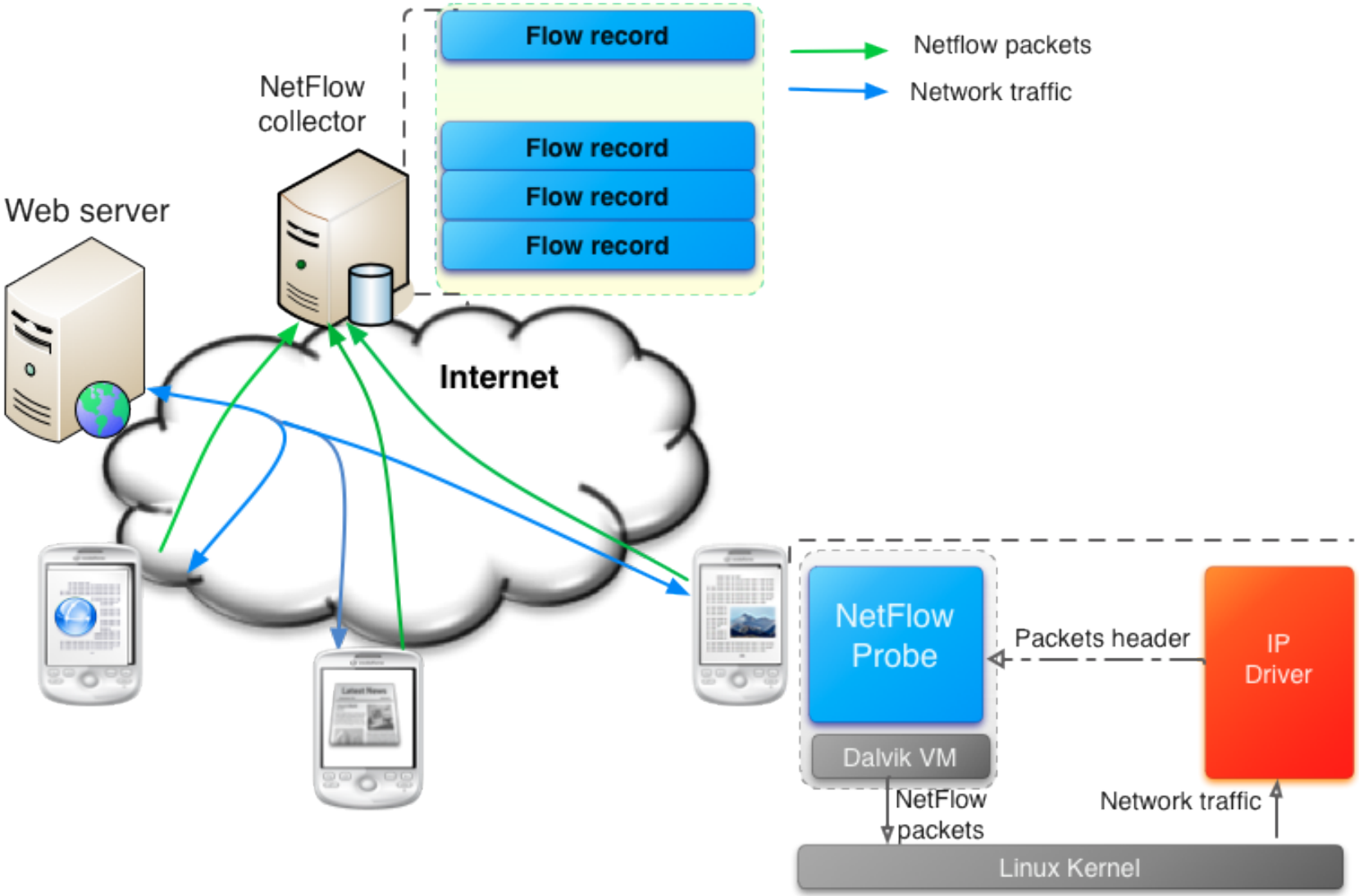


Figure 4: Data record of a circle-based geodetic location

Flowoid

- Flowoid: an Open Source NetFlow exporter for Android devices
- Include location information in NetFlow version 9 records



Geotagged network flows

Support of newly defined information elements is added to existing flow collector software: nfdump

Duration	Dst IP Addr:Port	bps	Lat. (int)	Lat. (dec)	Lng. (int)	Lng. (dec)
318.039	173.194.40.129:443	71	48	6657094	6	1583253
317.787	152.81.144.14:53	1	48	6657094	6	1583253
77.221	173.252.100.27:443	266	48	6657094	6	1583253
317.366	152.81.144.14:53	1	48	6657094	6	1583253
317.187	98.137.200.255:80	13	48	6657094	6	1583253
315.919	152.81.144.14:53	1	48	6657094	6	1583253
75.090	188.125.73.190:80	72	48	6657094	6	1583253
326.120	152.81.144.14:53	1	48	6657451	6	1583478
145.667	173.252.100.29:443	153	48	6657451	6	1583478
312.646	152.81.144.14:53	1	48	6657451	6	1583478
312.546	193.51.224.165:443	57	48	6657451	6	1583478
312.480	152.81.144.14:53	1	48	6657451	6	1583478
953.086	74.125.132.95:443	138	48	6657451	6	1583478
370.779	74.125.132.101:443	35	48	6655431	6	1628925
370.806	172.20.2.10:53	1	48	6655431	6	1628925
368.348	74.125.132.101:443	67	48	6655431	6	1628925
81.586	74.125.195.95:443	240	48	6655431	6	1628925
339.782	152.81.144.14:53	1	48	6657451	6	1583478
79.297	173.252.100.27:443	1153	48	6657451	6	1583478
6671.083	10.103.80.171:47175	1	48	6652353	6	1614169
661.711	74.125.132.147:443	0	48	6652353	6	1614169
5636.372	1.1.1.1:67	1	48	6657451	6	1583478
306.969	193.51.224.148:443	49	48	6657451	6	1583478
306.850	184.73.193.117:443	35	48	6657451	6	1583478
427.759	173.194.34.34:443	1	48	6657451	6	1583478

Network traffic of an Android device: first analysis

Data set

- A single user: Nexus 4 with Android Cyanogen version 4.2.0
- The user interacts with his device without any restrictions
- 24 hours of measurements: 2013-07-21 23:53, 2013-07-22 23:56
- Only 3G network communications
- Installed applications: Chrome, Email, duckduckgo, Google Maps, Facebook, Facebook messenger, Google Plus, Google talk, Google Ears, Twitter, Xabber, adaway

Overview of android network flows

- total bidirectionnel flows: 1789
- total bytes: 27.5 M, total packets: 64801

Protocols

TCP	UDP	ICMP
67%	32%	1%

Destination Ports

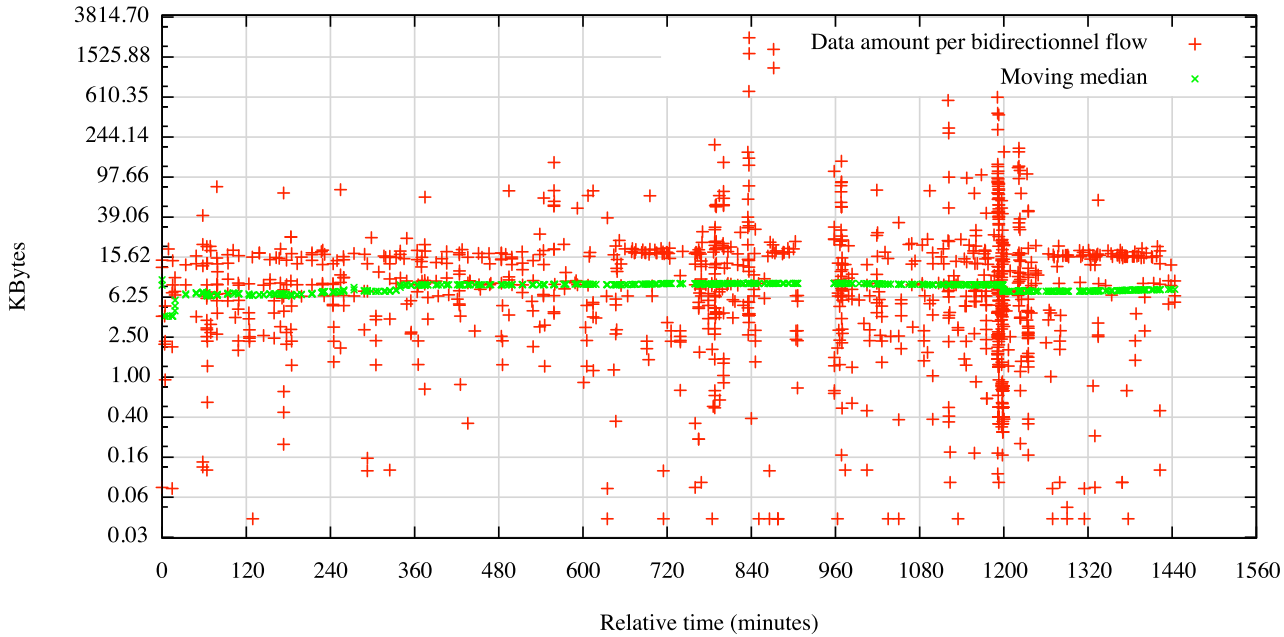
Total ports	80	443	53	993	5222
100	18%	29%	32%	9%	4%

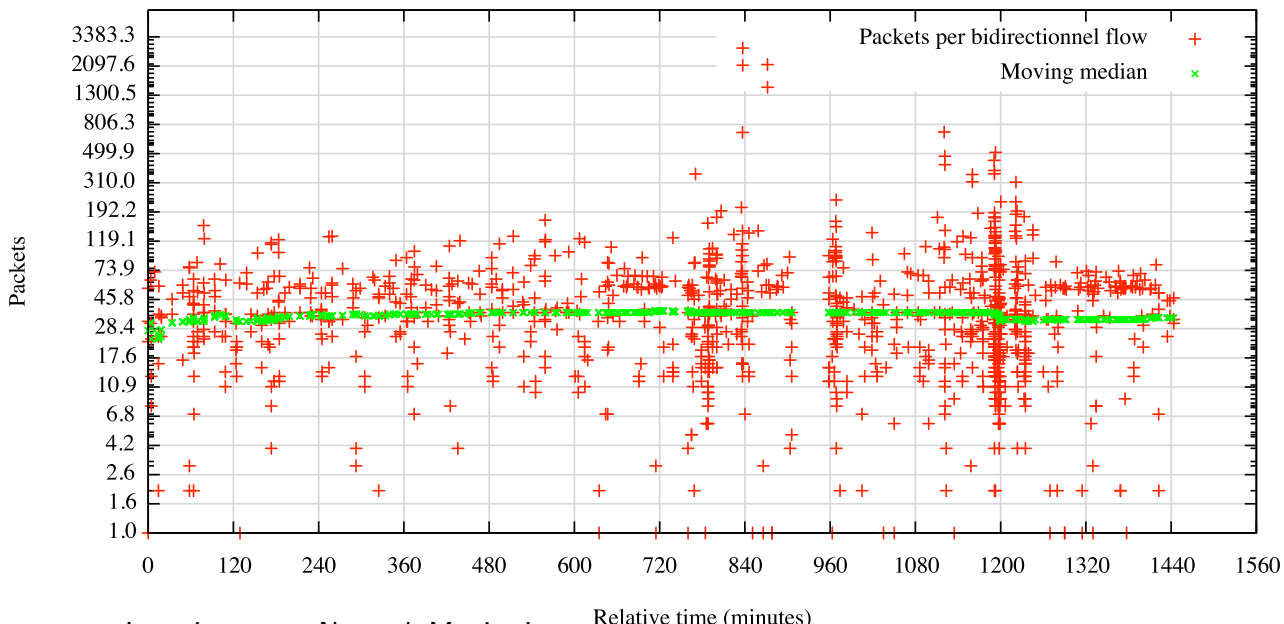
Distinct Contacted servers

TCP	UDP
151	2

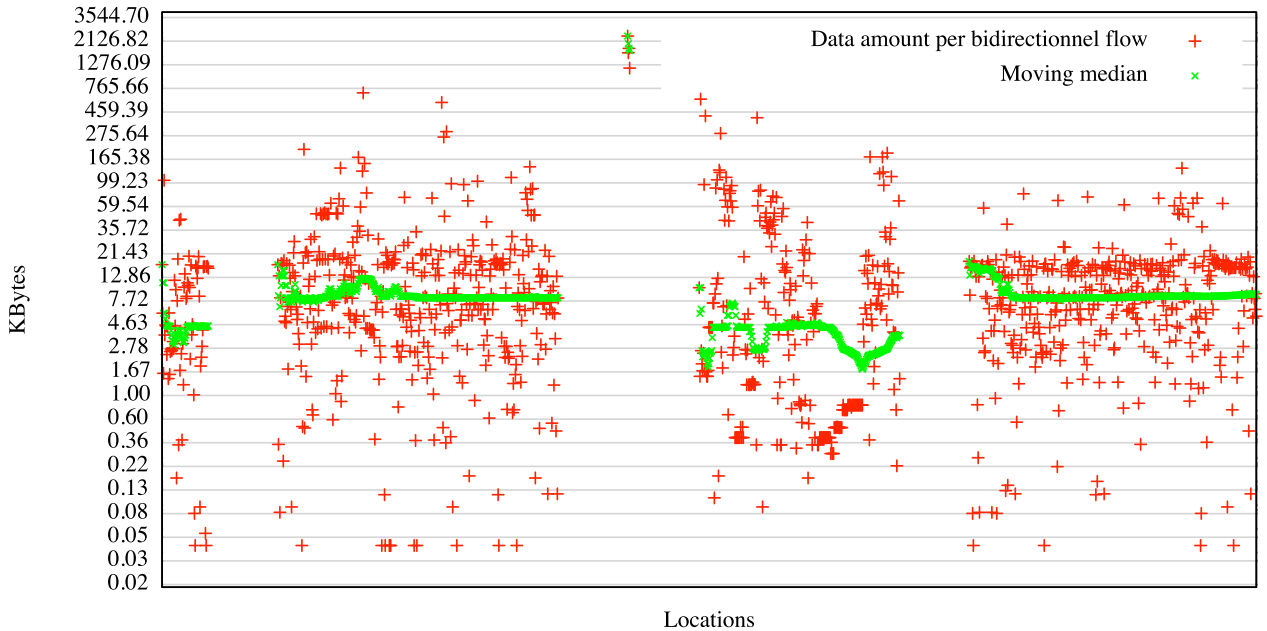
TCP flows=1204			
Destination IP address	ports	Flows	KBytes
173.194.34.8, 173.194.34.33	443	0.46%	7051.24
178.170.95.127	993,5222	13.9%	2143.88
193.51.193.146	993	6.5%	1042.24
31.13.80.49, 31.13.80.1, 31.13.80.33, 31.13.80.6, 69.171.224.45	443	16.5%	1793.83
91.198.174.236	80	1.07%	1215.03
54.230.185.184	443	0.2%	974.17
UDP flows = 582			
192.168.10.110	53	99.82%	128.15

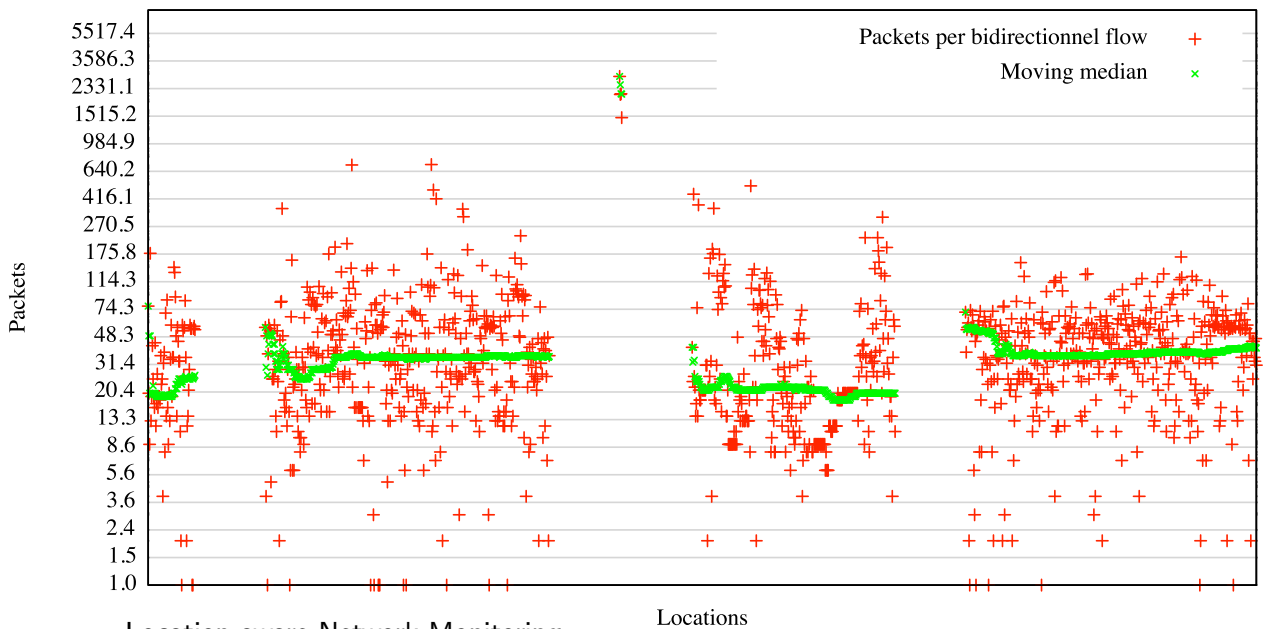
TCP Flows: amount of data over time





TCP Flows: amount of data over locations





Conclusions and Future directions

Understanding mobile network activities

- Networked devices are moving
- NetFlow data extended with exporter location
- Measurements over time and over locations

How to handle location-based expiration ?

- Physical location may change frequently: a mobile in a car
- If we expire flows at each location change, the network will be flooded
- If we accumulate location records as a list, IPFIX messages will be very long

How to analyze and organize measurement data ?

- Existing tools are suitable for time-based measurement
- What about location-based measurements ?

We are developing more informations elements

- Battery usage, device state, application names, ...
- Provide an aggregated view on mobile network traffic and their costs