Information Elements for IPFIX Metering Process Location

draft-festor-ipfix-metering-process-location-01

Olivier Festor Abdelkader Lahmadi Rick Hofstede Aiko Pras

Université de Lorraine - Inria University of Twente

IPFIX meeting

July 29, 2013

(compiled on: July 25, 2013)

Motivation

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

- Geographic coordinates: latitude, longitude, altitude
- Geodetic location shapes: point, circle, polygon, ellipse, etc
- Civic location: human readable information, postal address, proximity information

IPFIX Information Elements: geodetic location

Geodetic point record: there is no known uncertainty

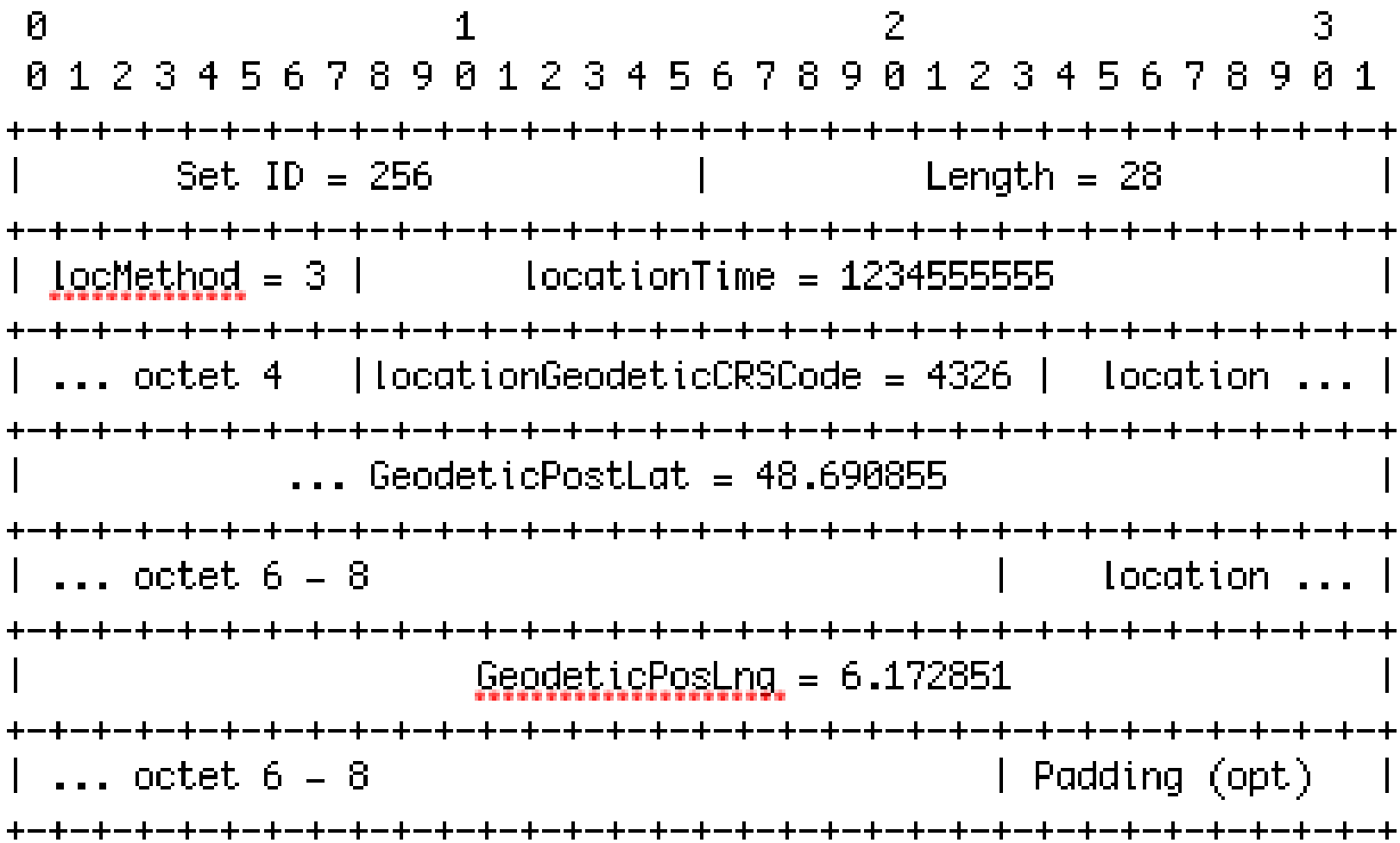

Figure 2: Data record of a geodetic 2D point location

IPFIX Information Elements: geodetic location

Geodetic circle record: there is known uncertainty

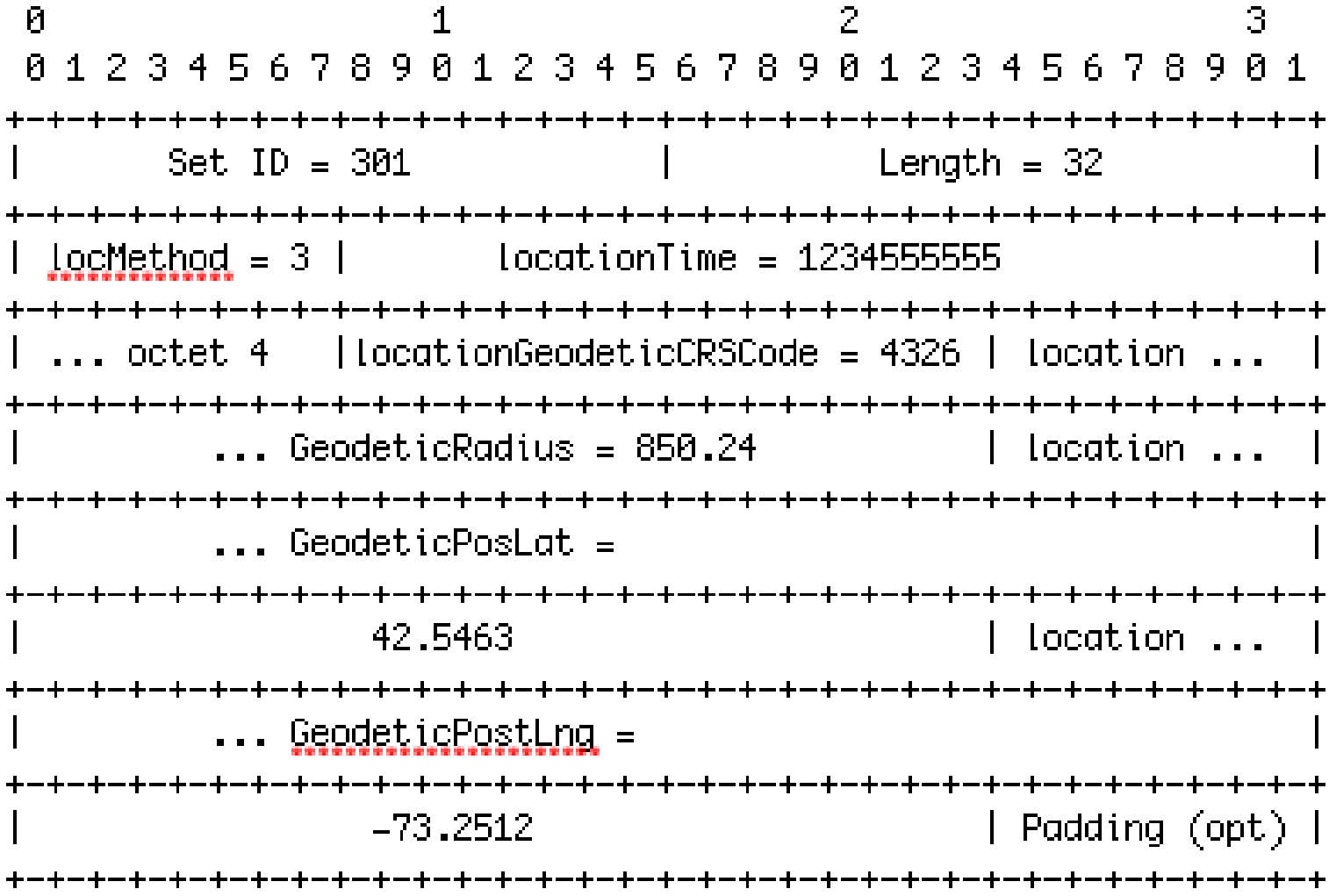

Figure 4: Data record of a circle-based geodetic location

Implementation

- Flowoid: NetFlow version 9 exporter for Android devices
- SURFmap/Nfsen/nfdump: location-aware analysis application

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

Discussion

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

Collected location-based measurement data

- How to analyze and represent them ?
- Existing tools and visualizations are suitable for purely time-based measurements