An investigation into the claims of IMSI catchers use in Oslo in late 2014

Ahmed Elmokashfi

[simula . research laboratory]

Outline

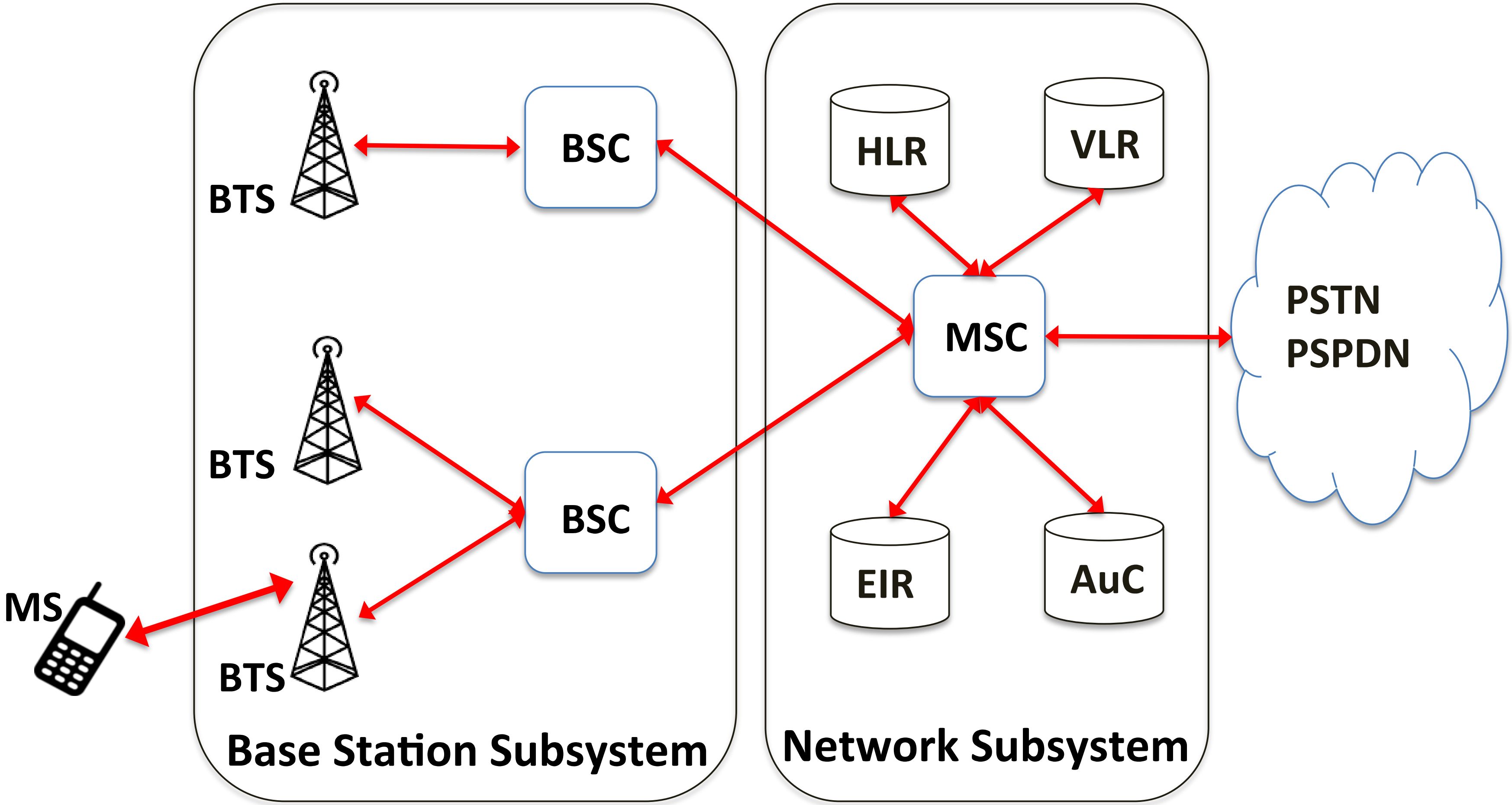
❑ Technical overview

❑ Data set

❑ Analysis of Delma’s measurements

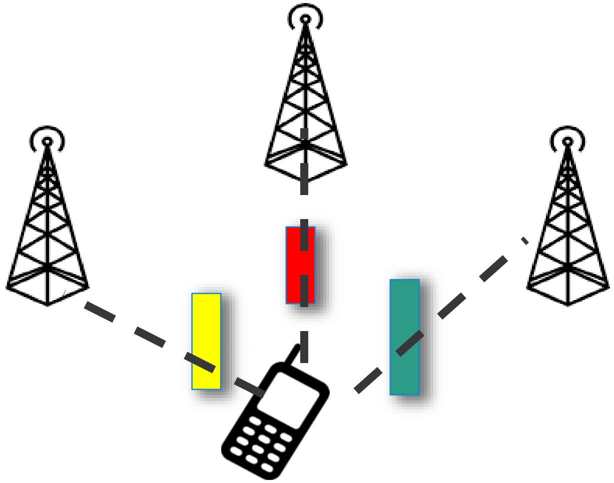
❑ Analysis of Cryptophone measurements

❑ Conclusions



MS	Mobile Station	VLR	Visitor Location Register
BTS	Base Transceiver Station	MSC	Mobile Services Switching Center
BSC	Base Station Controller	EIR	Equipment Identity Register
HLR	Home Location Register	AuC	Authentication Center
PSTN	Public Switched Telephone Network	PSPDN	Packet-Switched Public Data Network

Cell Selection

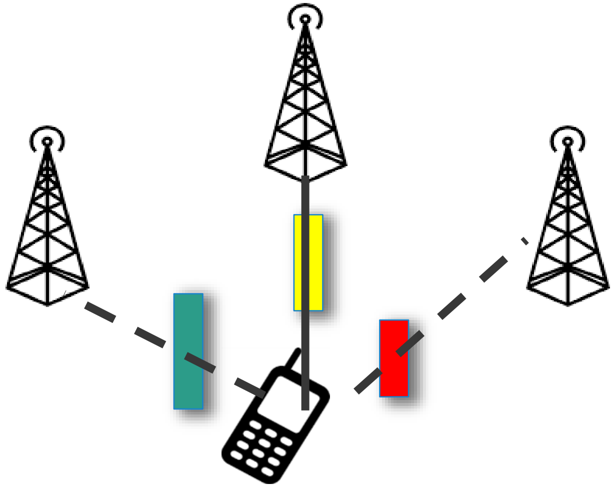


C1

Parameters

- RXLEV
- Cell power req.

Cell Reselection



C2

Parameters

- CRO
- Penalty Timer

Data Set

I. Reports that Aftenposten and Cepia shared with PST

II. Data published by Aftenposten publicly

III. The information that Delma MSS shared with PST

IV. Delma's report published on the 24th of June

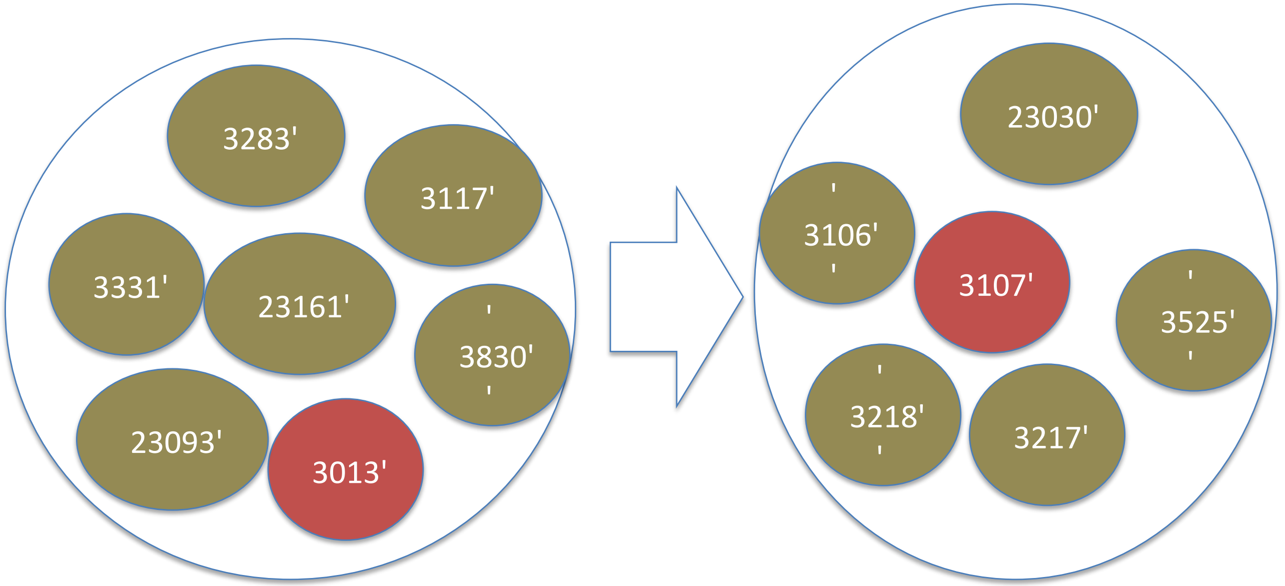
I. Private correspondence between PST and Telecom providers.

Classification of Delma’s alarms

Alarm	Severity	Unique cases
Radio channel duplication	Medium	25
Cell ID duplication	Medium/Low	2
Unexpected C1/C2 variation	Medium/Low	7
Short-lived cells	Medium	1
LAC anomalies	High/Medium	6
Provider anomaly	High	1
Fake cell/LAC	High	1

Radio Channel duplication

The same radio frequency channel is observed in use by two different cells very close in time



Channel'53'used'by'Cell'3283'at'10:02''
and'3218'at'10:04'

Radio Channel duplication

Such measurements warrant further investigation.

Operators correspondence with PST confirmed the reuse of frequencies in the same area.

Cell ID duplication

Cell IDs were observed in both Telenor and Netcom networks in the same area (3629, 3013).

Operators correspondence with PST confirmed the use of the two IDs above in the measured areas.

Unexpected variations in C1/C2

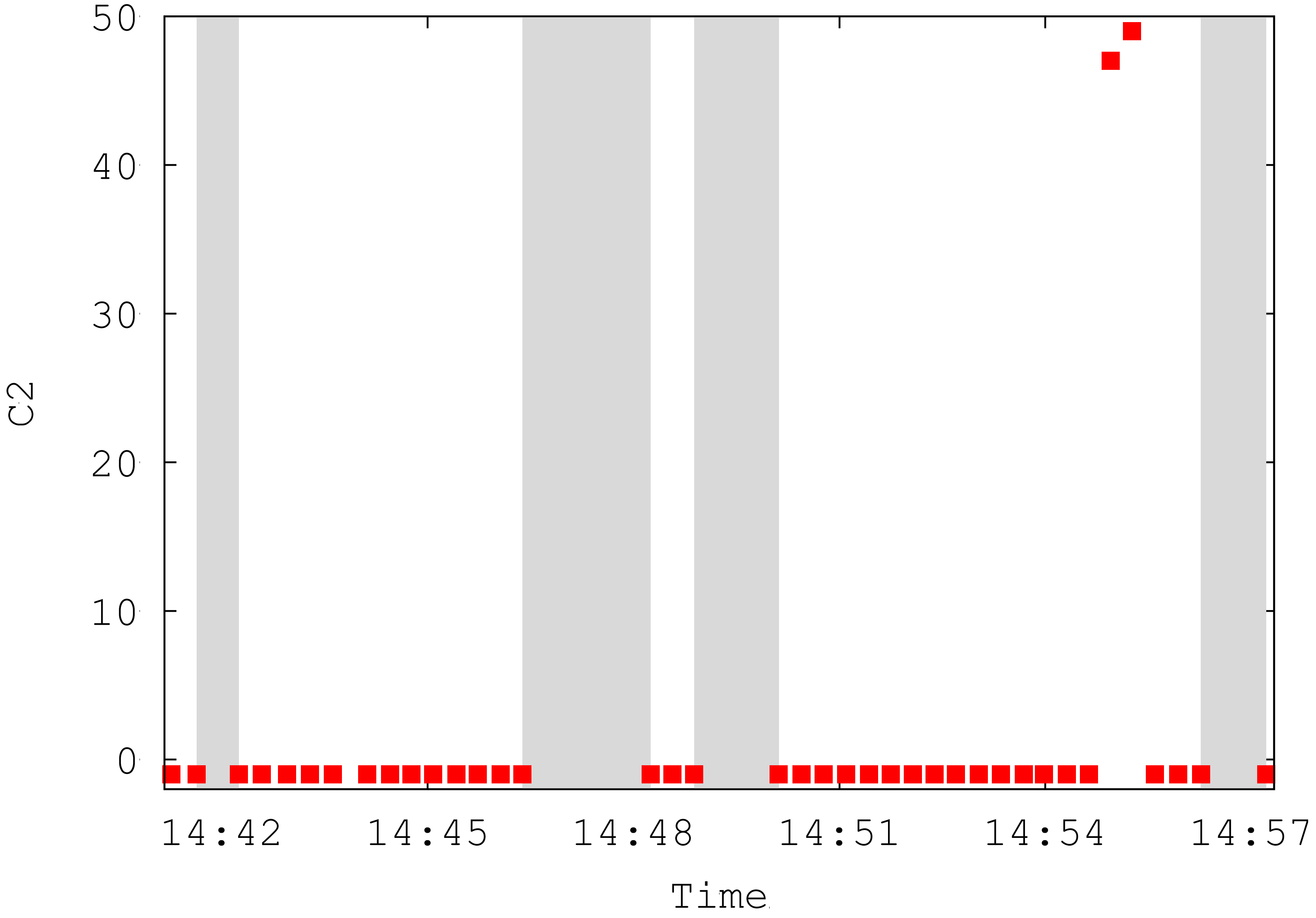
Sudden jumps and drops in C1 and/or C2 values.

C1 variations are caused by fluctuations in RXLEV which are expected as equipment moves.

Variations in C2 warrant further investigation; a knowledge of network configuration is required.

We find C2 variations consistent with the standard cell reselection process.

Sample C2 variation (3/12/2014 "mobile-124" survey)



Short-lived cells

The appearance of Netcom cell 34371 for 11 minutes with RXLEV ~-77 dBm.

This case is one out of 227 cases in the measurement data.

Such behavior is expected since the list of adjacent cells reported by the UE is dynamic.

LAC anomalies

The reported anomalies comprise three categories:

1- LACs that do not belong to the measured network

2- Absent LAC

3- Channel LAC switches that happen close in time.

Channel LAC switches resemble radio channel duplications and do not warrant further investigation.

While some of category 1 and 2 cases could be explained by external factors, the explanation of some has to be found in the measurement equipment.

Time	ARFCN	LAC	CELLID	BSIC	RxL	C1	C2	type
12:08:32	721	3805	51787	43	-92	3	-1	A Cell
12:08:51	0	11901	0	0	-200	0	0	No GSM
12:09:17	12	3805	24063	15	-106	5	5	S Cell

Provider anomaly

A Mobile Norway cell had two Telenor cells in its neighbor list.

This is perfectly fine since Network Norway had until early this year a national roaming agreement with Telenor.

Fake cell/LAC

The presence of a cell and LAC that do not belong to Telenor was observed on the 22nd of December (32478,12901).

Time	ARFCN	LAC	CELLID	BSIC	RxL	C1	C2	type
14:15:44	672	11901	23488	22	-91	15	15	S Cell
14:15:44	61	11901	3783	47	-103	7	7	A Cell
14:15:44	679	12901	32478	0	-94	8	8	A Cell
14:16:03	679	12901	32478	0	-83	32	32	S Cell
14:16:21	0	0	0	0	-200	0	0	No GSM

Fake cell/LAC

$$C2 = C1 + CRO$$

C1	C2	CRO
8	43	35
32	83	51

The estimated CRO values are inconsistent and odd which can not be explained by external factors

- *The cell sends a 6-bit field that the MS multiplies by two giving a CRO between 0 and 126.*

This inconsistency and lack of extra data suggests it is not advisable to conclude on this case without further investigations.

“If you plan to use the BBFW specifically to detect IMSI-Catchers in a specific geographic area, then it is strongly recommended to focus on the “*active connection without ciphering detected*” in combination with “*no neighbor cells detected*” events, especially when a 3G towards 2G network change has happened before them. Other warnings may pop up triggered by specific attack techniques, but not necessarily so.”

Conclusions

A subset of the reported alarms are related to the normal operation of the Norwegian GSM networks.

The remaining subset includes irregularities that can be explained by fake base stations, but also observations that can only be explained by problems in the measurement equipment.

The analyzed measurements do not constitute a compelling case that fake base stations were in use.