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

Centre for Resilient Networks and Applications
Simula Research Laboratory

Publication date 01. July 2015

Contents

1. Introduction

This report is produced by the Center for Resilient Networks and Applications (CRNA), a part of Simula Research Laboratory. CRNA conducts basic research to improve the resiliency and security of communication infrastructures. The report was prepared at the request of the Norwegian Police Security Service (PST). The conclusions of this report are independent and represent the views of CRNA.

In December 2014 Aftenposten, the largest daily newspaper in Norway, reported on an inquiry it carried into the use of fake base stations in Oslo. The publication of these reports triggered a debate about whether fake base stations were in use in Oslo and whether Aftenposten measurements data bears enough evidence to support that. CRNA among others was also interested in investigating these claims. We conducted a small scale investigation earlier this year which was not conclusive. We were later tasked by PST to give an expert opinion on whether the data collected by Aftenposten presents a compelling evidence of fake base stations use in Oslo late last year. We were provided with additional data set that PST obtained from the companies that performed Aftenposten's study and telecom operators.

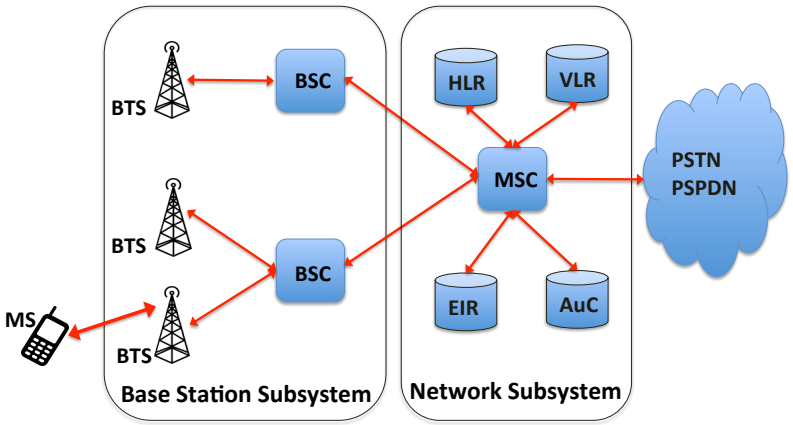
In this report, we examine all suspicious anomalies in Aftenposten measurements and check whether these anomalies indicate the presence of fake base stations. This report specifically investigates whether the data from the Aftenposten investigation indicates the presence of fake base stations. Independent of the results of this report, we can never rule out that fake base stations have been in use. Our conclusions are valid only for this particular set of data.

The rest of this report is organized as follows. We provide a brief technical overview of GSM networks in Chapter. 2. Chapter. 3 describes the data set we investigate. Chapter. 4 and 5 check whether the measurement data gives a compelling evidence of the use of fake basestations. We summarize our findings in Chapter. 6

2. Technical Background

This section gives a brief technical overview that is necessary for understanding the analysis in the upcoming sections. We describe the architecture of a typical GSM network and how mobile devices move between cells in such a network. Note that we limit ourselves to GSM networks, because the measurements we analyze in this report were mostly performed on 2G networks. For more details about GSM networks we refer the reader to [2].

2.1 GSM network architecture



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

Figure 2.1: GSM network architecture.

Figure. 2.1 depicts the high level architecture of a typical GSM network which consists of three parts: Mobile Station (MS), Base Station Subsystem

(BSS) and Network Subsystem (NSS). The MS is basically the end user equipment that is responsible for connecting users to the GSM network. It hosts a Subscriber Identity Module (SIM), which includes all necessary information for identifying and authenticating a user. The BSS includes Base Transceiver Stations (BTSs) and Base Station Controllers (BSCs). BTSs are the radio cells that facilitate communication between MSs and the GSM network. A BTS coverage range can vary from a 100 meters to tens of kilometers. BSCs are devices that control BTSs, connect BTSs to the NSS, and manage mobility as users move between BTSs. BTSs in a certain region are controlled by the same BSC. BTSs in a GSM network are typically grouped into regions. Each such region is identified by a unique Location Area Code (LAC). A BSC is responsible for serving at least one LAC. The NSS manages communication between mobile users and other fixed or mobile users. It also manages users registration, authentication, and mobility as users move between BSCs.

2.2 Cell Selection and Reselection

Cell Selection refers to the attachment procedure performed by a MS when it initially joins the network. When a MS is powered up, it starts measuring the signal strength of Broadcast Channels (BCCH) from all nearby cells. Using a few samples, it estimates the signal strength, which is referred to as RXLEV in GSM, of each cell. RXLEV decreases as the distance between the MS and the cell increases, but it can also decrease because of natural obstacles (terrain) or high buildings. After estimating RXLEV for each neighboring cell the MS calculates the cell selection parameter (i.e. Path Loss Criterion) C1 to determine the strongest available cell using the following equation.

$$C1 = (RXLV - RLAM) - Max(B, 0) \tag{2.1}$$

Where:

- $RLAM$ is a cell specific parameter that decides the minimum allowed signal strength for a MS to accessing that cell.
- B is the difference between the transmission power that a MS needs for communicating with the cell and the MS maximum power output.

The MS ranks all cells according to their C1 values. It then chooses the cell with the highest positive C1 value to camp on. This cell is known as serving cell. Further, the MS sends a location update to the network informing of its current LAC.

Cell Reselection refers to the process through which a MS chooses a new cell to camp on after the initial registration. Once a MS has camped on a cell, it keeps monitoring received signal strength from the current camp on cell and the six best neighboring (adjacent) channels. Note that, a MS receives the list of adjacent channels from the current camp on cell. These channels are expressed as numbers known as Absolute Radio Frequency Channel Number (ARFCN). The MS calculates the C1 parameter for all monitored cells and use it to compute the cell reselection parameter C2 using the following equation.

$$C2 = C1 + CRO - TO * H(PT - T) \tag{2.2}$$

Where:

- *CRO* is the cell reselection offset which is a value from 0 to 63 that corresponds to a range from 0 to 126 dB with a step of 2. CRO value is set to modulate MS's preference for reselecting a cell; the higher the CRO the more attractive the cell.
- *PT* is the penalty time, which denotes the time that a MS needs to spend in a cell before it can camp on it. It is used to discourage fast moving MSs from connecting to pico or micro cells and encourage them to connect to macro cells to reduce the number of cell reselections. PT varies in the range between 20 and 620 seconds with a step of 20 seconds.
- *T* is the time that has passed since the MS started measuring the cell. This timer is reset whenever the cell is removed from the adjacency list. H(PT-T) is 1 if the MS has spent time in the cell shorter than PT and 0 otherwise. H(PT-T) is also 0 for the current camp on cell.
- *TO* is the cell reselect temporary offset which is used to temporarily modify C2 (i.e. decrease it) for cases where the MS has spent time in the cell shorter than PT.

After calculating C2, a MS ranks the cells accordingly, the higher C2 the better the cell. What happens next depends on the MS current mode of operation. A MS can either be in an idle or a dedicated mode. When a MS is in idle mode it compares C2 values and changes the camp on cell if a neighboring cell has higher C2 than the current cell. It only signals this to the network if the new cell belongs to a different LAC. A MS is in a dedicated mode whenever it is engaged in a call or data transmission which means that it has been allocated a dedicated control channel (SDCCH) or a dedicated traffic channel (TCH). MSs in dedicated mode send their C1 and C2 measurements to the network which decides on reselection on behalf of MSs.

2.3 Handovers

Network controlled cell reselection is referred to as handover. This network side coordination is needed to ensure the seamless continuation of ongoing sessions as MSs change serving cells. There are different types of handovers in GSM.

1. **Intra-BTS.** This happens when a MS is instructed by the BTS to change used frequency or slot. In this type of handover, the MS does not change cells.
2. **Inter-BTS Intra-BSC.** This type of handover happens when a MS moves from one cell to another cell that are both controlled by the same BSC. Handover decision and management is performed by the BSC.
3. **Inter-BSC.** This type of handover happens when a MS moves from one cell to another cell that is controlled by a different BSC. Handover decision and management is controlled by the MSC involving both the old BSC and the new BSC.

4. **Inter-MSC.** This type of handover happens when a MS moves between GSM networks. The handover process involves signaling and coordination between the old and new network MSCs.

3. Data set

Aftenposten with the help of Cepia Technologies and Delma MSS conducted a set of surveys in Oslo to check for the presence of IMSI catchers. The surveys were carried out during November and December 2014 as well as April 2015. These surveys were performed using two different technologies: a Cryptophone and a specialized measurement hardware and software from Delma. The Cryptophone is a secure mobile phone that runs a firewall software to detect abnormal phone activity as well as suspicious network activity. Delma's specialized measurement hardware and software passively monitor mobile connection metadata to check for presence of surveillance or IMSI catchers by examining irregularities in signal strength, attachment information (LAC,CELL ID), and cell selection and reselection parameters. For more information about Cryptophone and Delma's system please refer to [3].

The data set investigated in this report consists of the following:

- All reports that Aftenposten has shared with PST which include all measurements performed using Cryptophone and measurements performed by Cepia. It also includes four reports from Cepia.
- The data set and report published by Aftenposten publicly in January.
- The information that Delma MSS shared with PST. This includes four reports and the same measurements data as the one shared by Aftenposten but with more details and extra data points.
- The recent report from Delma, which was published publicly on the 24th of June [4]. Besides the measurements carried in December, this report also refers to new measurements that were performed in April. We do not investigate the new measurements since we do not have the corresponding data set
- A set of private correspondence and exchanges that PST had with Telenor, Netcom, and Network Norway. In these exchanges, the operators answered questions about their network configurations and whether some base stations are part of their infrastructure.

The data provided by Delma to PST differs from the data published by Aftenposten in two aspects:

1. Delma's data set include measurements with no-GPS data. These measurements were removed from Aftenposten's data set.

2. The measurement records in the Aftenposten's data set do not specify whether a measured base station is a serving or a neighboring cell.

4. Analysis of Delma's measurements

This section examines all measurement alarms and alleged IMSI catcher presence cases that were reported by Delma and Aftenposten. We start by identifying the measurement data related to each case and check whether these measurements include anomalies that substantiate the conclusions drawn by Delma and Aftenposten. Delma's equipment monitors a set of GSM connection metadata, and generates alarms with different severity levels depending on observed changes in these metadata.

4.1 Recorded alarms

Delma's alarms are not necessarily mutually exclusive, which means that the same case can be reported multiple times. We therefore group alarms into the following categories to ensure that each case is counted only once.

1. **Radio channel duplication.** In these cases, Delma recorded the use of the same channel (ARFCN) by two different cells in a small time window. Alarms of this type are marked with a medium severity level. According to Delma, this severity level means that the case is less likely to be explained by network conditions, thus warranting further investigation.

2. **Cell ID duplication.** The same Cell ID is observed in two different networks (e.g. Telenor and Netcom) in the same area. Alarms of this type are marked with a medium or low severity level. According to Delma, low severity alarms can be explained by network conditions.

3. **Unexpected variations in C1/C2.** In these cases, Delma measured non-trivial variations in C1/C2. Alarms of this type are marked with a medium or low severity level.

4. **Short-lived cells.** This involves cases where cells with strong signal appear for a very short time period. Alarms of this type are marked with a medium severity level.

5. **LAC anomalies.** This category can be divided into three subcategories. The first includes cases when Delma recorded measurements that involve a LAC from a different operator. The second includes cases when the same channel appears to be associated with two different LACs in the same area. The last includes cases with absent (zero) LAC values. Cases in the first subcategory are marked with a high severity level, while cases in the second and third subcategories are marked with a medium severity level.

Category	Unique cases	Total cases
Radio channel duplication	25	31
Cell ID duplication	2	10
Unexpected variations in C1/C2	7	8
Short-lived cells	1	1
LAC anomalies	6	8
Provider anomaly	1	1
Fake cell/LAC	1	1

Table 4.1: The number of cases in each category

According to Delma, high severity alarms indicates with a high probability the presence of IMSI-catchers and warrant immediate investigation.

6. **Provider anomaly.** This involves cases when cells from a different operator appear on the neighbor list. Alarms of this type are marked with a high severity level.

7. **Fake cell/LAC.** This category includes cases where a fake cell/LAC was observed. Alarms of this type are marked with a high severity level.

Table. 4.1 presents the count of cases measured by Delma in each category. We limit ourselves to cases where suspicious CELL ID, LAC, or ARFCN is mentioned explicitly. Delma tends to report alarms repeatedly. For instance, channel 982 (Network Norway) was observed as used by two cells 61051 and 40041 in three different surveys (event,mob5,static1b) and yet reported each time without referring to the previous occurrences. Thus, we show two different counts in the table: the number of unique cases and the total number of cases. Radio channel duplication stands out as the category with the highest number of unique cases followed by C1/C2 variations.

4.2 Analysis of Alarms

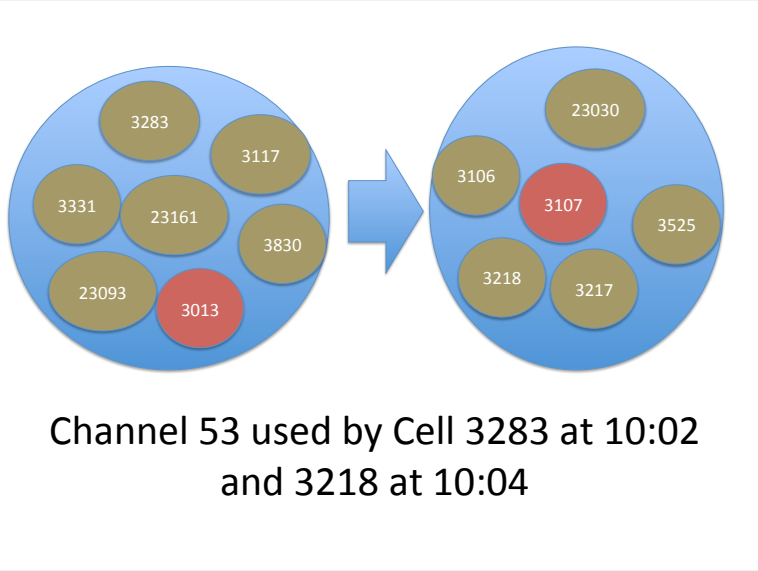
In this section we dissect different alarm categories.

Radio channel duplication This category corresponds to cases where Delma observed that same ARFCN was used by two different cells very close in time. The number of unique cases is 13 for Network Norway, 8 Netcom, and 4 Telenor. By reviewing all cases, we note that cells sharing the same frequency channel are usually present as adjacent (neighbor) to the serving cell. Further, their appearance always coincides with a change in the serving cell. We demonstrate one of these cases in the box below.

We agree that such measurement results do warrant further investigation to clarify if the operators use radio channels in the way experienced by the measurement equipment. After looking into correspondence between PST and the operators, we find that all cases in this category are consistent with expected network conditions Operators confirmed in their correspondence with PST the fact that they reuse frequencies in the same area. Further, two cells that use the same frequency channel may share a subset of their neighbors. This means that if the equipment was close to one of these shared neighbors would be

expected to generate an alarm that belongs to this category. We also note that Delma mentioned that the change always happened within a few meters. In fact, what matters here is not the number of meters but rather the location of the equipment relative to the two cells sharing the same channel.

Sample channel duplication case



The figure above shows the composition of Delma's equipment cellular neighborhood. Serving and adjacent cells are depicted in red and green respectively. At 10:02 the serving cell was 3013 and channel 53 was in use by cell 3283. At 10:04 the serving cell became 3107 and channel 53 became occupied by cell 3218. Note that the total cellular neighborhood changed significantly between 10:02 and 10:04

Cell ID duplication Delma recorded that the Cell ID 3629 was present in both Telenor and Netcom in the same area. The same was also recorded for Cell ID 3013.

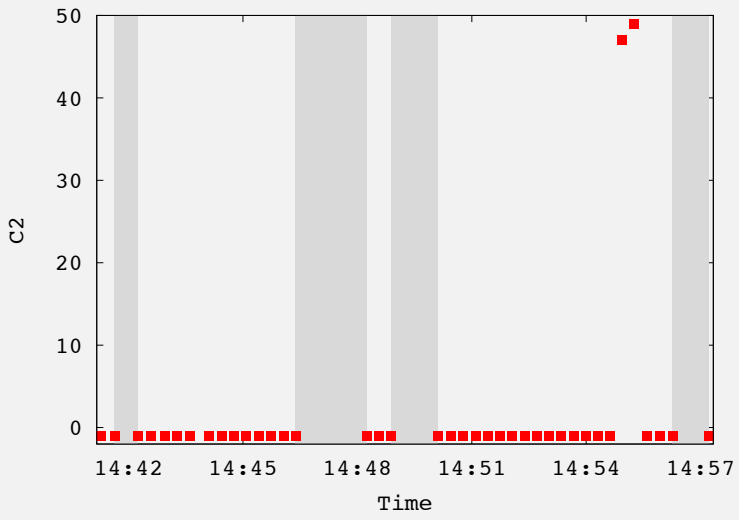
When such measurement results are found to be suspicious, they have to be compared to information on how the operators use Cell IDs. Telenor and Netcom confirmed in their correspondence with PST that they have cells with the two IDs above in the same area where Delma conducted its measurements. Hence, the cases above are consistent with the expected network conditions.

Unexpected variations in C1/C2. This category includes cases where Delma measured fluctuations in C1 or C2 values. Variations in C1 values are caused by fluctuations in the received signal strength. Such fluctuation are expected when the equipment moves, and can e.g. be caused by getting a building between the equipment and the cell. For instance, Delma measured a variation of 39 dBm in the received signal strength from cell 3257 in survey par-1214 and

marked it as an alarm with a medium severity. The GPS coordinates around the fluctuation time, however, indicate that the equipment was moving. Such cases do therefore not warrant further investigation.

We also investigate all reported abnormal variations in C2. Some of these cases did warrant further investigation, as they were hard to explain without having information on how the operators have parameterized their equipment. Knowing the penalty timer set by the operator, however, we do find them consistent with the standard cell reselection process (see Ch. 2). We analyze one of these cases in the box below.

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



The figure above shows the time series of C2 values measured by Delma for Netcom cell 24079.The grey areas mark periods where 24079 was not one of the adjacent cells. This cell always appeared as an adjacent cell except for the period from 14:54:57 to 14:55:16 where it was a serving cell. The correspondence between Netcom and PST indicated that Netcom uses a penalty timer of 300 seconds in some of its sites. Note that this timer is reset whenever the cell is removed and re-added to the adjacency list. In other words, for this timer to expire a MS must have the cell in its neighbor list for 300 seconds. The time series shows that Delma's equipment always had 24079 on its neighbor list for less than five minutes except for the period between 14:49:49 and 14:54:57. This means that timer was always reset except for the specified period, which explains why C2 always stayed at -1 and suddenly jumped to 47 at 14:54:57 making 24079 attractive to be picked as a serving cell. Hence, the observed behavior is consistent with the standard cell reselection procedure and does not warrant further investigation.

Short-lived cells. In the *event* survey Delma flagged the appearance of Netcom cell 34371 for 11 minutes with RxL values around -77dBm as an alarm with a medium severity level. Serving cells in urban areas would typically announce a set of adjacent ARFCNs, but the MS monitors only six of them. Therefore, cells that go into and out of the set of monitored adjacent cells is to be expected. In the measurements collected by Delma, there are 227 such instances. The appearance and disappearance of cell 34371 is only one of these. Hence we do not see any departure from expected networks conditions in this case.

LAC anomalies LAC anomalies identified by Delma can be divided into three subcategories: observing LACs that do not belong to the measured network, absent LAC, and channel LAC switches that happen close in time. As for the latter, it is similar to the radio channel duplication cases above. The likelihood for experiencing such a switch depends on the location of the measurement device and network planning by the operators and has no dependency on time difference or distance in meters. Observations of channel LAC switches that happen close in time do therefore not warrant further investigation.

In the following, we present and analyze three cases from subcategories one and two.

Time	ARFCN	LAC	CELLID	BSIC	RxL	C1	C2	type
09:50:44	5	3804	51171	19	-78	32	32	A Cell
09:50:56	5	0	51171	19	-80	31	31	S Cell
09:51:20	0	0	0	0	-200	0	0	No GSM
09:51:33	5	3804	51171	19	-77	34	34	S Cell

Table 4.2: LAC anomaly - sample one (Netcom - 03/12/2014)

Time	ARFCN	LAC	CELLID	BSIC	RxL	C1	C2	type
13:44:50	43	3801	13422	18	-73	38	38	S Cell
13:45:07	43	11901	13422	18	-73	38	38	S Cell
13:45:42	43	3801	13422	18	-73	38	38	S Cell

Table 4.3: LAC anomaly - sample two (Netcom - 03/12/2014)

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

Table 4.4: LAC anomaly - sample three (Netcom – 22/12/2014)

Table. 4.2 shows a case where the LAC was temporarily zero followed by a loss of coverage and then restoration. Apart of the LAC all other meta-data remained either exactly the same (ARFCN, BSIC) or stayed within range (RxL,C1,C2). According to 3GPP standards LAC values 0000 and FFFE are reserved values that are used in some special cases when no valid location area identity (LAI) exists in the MS. Hence, the absence of LAC here could be related to the loss of connectivity that happened next.

Table. 4.3 shows a case where the serving cell switched its LAC temporarily (second row) to a LAC that belongs to Telenor. Again, apart of LAC all other fields were exactly the same in all three rows.

Table. 4.4 shows a case similar to the previous one with a caveat though; Telenor LAC appeared when the coverage was lost (second row). Basically, the second row says that there was no service and yet the LAC was known. This is not consistent with the way a MS learns about the current LAC in GSM networks. The current LAC is periodically broadcasted by each cell on its broadcast channel. Hence, to know the LAC a MS needs to have service and to be able to listen and decode messages sent on at least one broadcast channel. This means that the LAC can not be known when there is no service.

The explanation for the case of table. 4.4 has to be found within the measurement equipment itself. Further, the case of table. 4.2 also shows a LAC value that is set by the MS when it has no valid LAI. While the cases in tables 4.2 and 4.3 display measurements that could be explained by external factors like fake base stations, the case in table 4.4 cannot. This gives rise to detailed questions as how the measurement equipment register LAC. It is therefore not advisable to conclude on these cases without a thorough investigation of the measurement equipment.

Provider anomaly. Delma recorded that a Mobile Norway cell had two Telenor cells (59403,58135) in its neighbor list and marked it as an alarm with a high severity. Until early this year Network Norway had a national roaming agreement with Telenor to use Telenor's radio access network in places where Mobile Norway [1] had poor or no coverage. Hence, it is absolutely expected that Network Norway cells would have Telenor cells in their neighbor list. Such observations do therefore not warrant further investigations.

Fake cell/LAC. Delma reported the presence of a cell and LAC that do not belong to Telenor (CELL ID 32478 and LAC 12901) during the MC survey conducted on the 22/12/2014. Their equipment reportedly lost network connectivity and halted after picking the strange cell as a serving cell. Such observations do require further investigations. Our analysis is given below.

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	43	A Cell
14:16:03	679	12901	32478	0	-83	32	83	S Cell
14:16:21	0	0	0	0	-200	0	0	No GSM

Table 4.5: Fake LAC and cell anomaly (Telenor – 22/12/2014)

Table. 4.5 shows the measurement records captured between the appearance of the strange cell and until the loss of service. We make the following observations based on these records.

Strange cell ARFCN. The strange cell was broadcasting on ARFCN 679. This ARFCN was observed during the same survey about 17 minutes earlier and it was used by cell 23161 from LAC 11901.

[1] Mobile Norway was the name of the shared radio access network owned by Tele2 and Network Norway.

C1/C2 values. C2 and C1 are related via equation. 2.2. There are two measurements from the strange cell at 14:15:44 as an adjacent cell and at 14:16:03 as a serving cell. Now, let's substitute the measured C1 and C2 values into equation. 2.2 and check whether we get a consistent solution i.e. the same CRO. Note that we ignore the last term in equation. 2.2, since IMSI catchers are not expected to set a penalty timer to discourage MSs from connecting to them.

$$43 = 8 + CRO \tag{4.1}$$

$$83 = 32 + CRO \tag{4.2}$$

Solving the two equations yields the following results. Equation. 4.1 gives $CRO = 35$ while equation. 4.2 gives $CRO = 51$. These values are inconsistent with GSM standards in two respects:

1. *The CRO values are not equal.* Since the strange cell had a different LAC, we may assume that the CRO value computed before it became a serving cell can be $(CRO - CRH)$ instead of CRO. CRH is a parameter called cell reselection hysteresis that is used to discourage MSs present in areas covered by two LACs from switching LACs frequently. The maximum value CRH can take is 14dB, meaning that the maximum CRO in case CRH was used is 49, which still differs from the value calculated by Eq.4.2

2. *The CRO values are odd numbers.* According to the standards CRO value in dB is supposed to be an even number. CRO is a 6-bit field broadcasted by cells over their BCCH channel as part of the system information block [1]. Hence, the CRO value received from a cell can be between 0 and 63. The MS converts this value to dB by multiplying it by 2. Hence, the odd numbers above can not be explained by external factors e.g. fake base station.

The second point above and the lack of more measurement points suggest that it is not advisable to conclude on this case without a thorough investigation of the measurement equipment.

5. Analysis of Cryptophone measurements

The CryptoPhone monitors connection metadata as well as the activity of the base band processor (BP) and application processor (AP). The former is the part of the phone that is responsible for radio communication, while the latter is the phone CPU.

We have investigated the 122 CryptoPhone measurements that Aftenposten deemed very suspicious. All 122 events have a cause BB data activity detected without OS data activity(Norwegian: "Observasjon: Data sendes inn og ut av mobiltelefonen uten at den er i bruk.") CryptoPhone describes these events as situations when "a data context has been established without AP intention". It is explained further that when there is BP data activity, there also should be OS data activity". CryptoPhone provides rationale for such situations: "if the BP would have been exploited, then the attacker would likely try to exfiltrate data to the outside world" If any of those 122 events signals the presence of suspicious base stations, it must mean that the baseband processor of the CryptoPhone device Aftenposten used was exploited by the attacker and it happened on the first day of their measurements or the device was infected from the very beginning If this was the case, i.e. on the first day an attacker got exploit code running on the BP with an aim "to exfiltrate data, or to cause the BP to work as a room bug, Aftenposten should have stopped all further measurements as the BP was affected. CryptoPhone clearly states that the analysis of BP behavior in correlation to the AP is a statistical function and that individual warnings of suspicious events do not necessarily indicate a successful BP exploit, or the presence of an IMSI-catcher". We believe that the observed BP data activity is a normal operation and part of standard 3G PDP context management.

Aftenposten did not consider any of the non BP-related events detectable by CryptoPhone, such as active connections without ciphering or the absence of neighboring cells, as their goal was to detect IMSI-catchers. This is also strongly recommended by CryptoPhone: "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".

6. Discussion and conclusions

We have conducted a thorough investigation into whether the measurement data collected by Aftenposten and Delma can indicate that fake basestation were in use in Oslo late last year. Next, we summarize our findings.

Delma's measurements. We have found that Delma's alarms can be classified into two groups. The first includes alarms that were raised over changes that are consistent with the normal operation of the Norwegian GSM networks. This involves duplicate radio channel cases, CELL ID duplication, C1/C2 variations, short-lived cells, and provider anomaly. In many of these cases, reaching out to mobile operators and having an adequate understanding of the way mobile networks are configured in Norway could have reduced the number of false alarms. The second group includes alarms that were raised over LAC anomalies and a reportedly fake base station. The measurement data for this group include irregularities that could be induced by external equipment like fake base stations. However, these incidents are paired with observations that can only be explained by irregular behavior of the measurement equipment itself. Drawing conclusions on the second group of alarms is therefore not advisable.
Cryptophone measurements. We have investigated all Cryptophone measurements that were classified as suspicious by Aftenposten. All of them were raising alarms over the presence of radio activity without accompanied data activity. We believe that such radio activity is part of the normal operation of user equipment.

Finally we would like to emphasize that measurements like these are inadequate to exclude the possibility of fake base stations. It is, however, our view that they do not constitute a compelling case that fake base stations were in use.

Bibliography

[1] 3rd Generation Partnership Project. *3GPP TS 44.018 V8.10.0*, 2010.

[2] Timo Halonen, Javier Romero, and Juan Melero. *GSM, GPRS and EDGE Performance Evolution Towards 3G/UMTS*. John Wiley & Sons Ltd., 2nd edition, 2003.

[3] Per Anders Johansen, Andreas Bakke Foss, and Fredrik Hager-Thoresen. *Teknisk beskrivelse av Aftenpostens kartlegging av mobilovervåking i Oslo*, Jan 2015.

[4] Gordon McKay. *Mobile network forensic analysis*, May 2015.