Detecting IMSI-catcher using Soft Computing

Thanh van Do[1,2] , Hai Thanh Nguyen[1], Nikolov Momchil[1], Van Thuan Do[3]

[1] Telenor ASA. Snarøyveien 30 1331 Fornebu, Norway
[2] Norwegian University of Science and Technology, O.S. Bragstadsplass 2B 7031 Trondheim, Norway
[3] Linus AS, Martin Linges vei 15, 1364 Fornebu, Norway

{thanh-van.do, haithanh.nguyen}@telenor.com
Mnikolov@telenor.bg
t.do@linus.no

Abstract. Lately, from a secure system providing adequate user's protection of confidentiality and privacy, the mobile communication has been degraded to be a less trustful one due to the revelation of IMSI catchers that enable mobile phone tapping. To fight against these illegal infringements there are a lot of activities aiming at detecting these IMSI catchers. However, so far the existing solutions are only device-based and intended for the users in their self-protection. This paper presents an innovative network-based IMSI catcher solution that makes use of machine learning techniques. After giving a brief description of the IMSI catcher the paper identifies the attributes of the IMSI catcher anomaly. The challenges that the proposed system has to surmount are also explained. Last but least, the overall architecture of the proposed Machine Learning based IMSI catcher Detection system is described thoroughly.

Keywords: IMSI catcher detection, mobile phone tapping, phone eavesdropping, machine learning, anomaly detection.

1 Introduction

Until recently, mobile communication has been perceived by the majority of users as quite secure regarding both confidentiality and privacy thanks to the strong encryption combined with use of temporary identities. In fact, users quite often consider mobile telephony as more secure than fixed telephony. Recently, a series of scandalous phone tapping incidents in the United States, United Kingdom, Germany, China, etc. revealed by Snowden, a former American National Security Agency (NSA) agent had eroded this conviction. It is really shocking that not only very important people at high position like the German chancellor, prime ministers, members of parliament, etc. but also regular people may be victims of phone eavesdropping. But most frightening lies perhaps in the fact that the monitoring may be done by anybody from the police, governmental intelligence agencies, security institutions, etc. to private companies or organisations. With advances in

microelectronics and the availability of mobile open source software, equipment used in phone tapping are getting both smaller, easier to handle, more available and also quite affordable in the range of US $1500-2000.

Since the last couple of months, Aftenposten [1], one of the biggest newspapers in Norway has published several articles telling that they have detected the presence of many IMSI catchers aka fake base stations in the region of Oslo that could be used in the surveillance of mobile users.

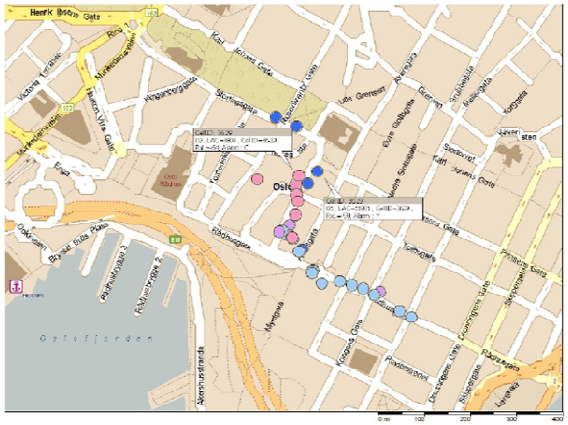

Figure 1 IMSI catchers detected around the Parliament in Oslo (courtesy: Aftenposten)

The detection has been done using mobile devices such as GSMK Cryptophone [2] that the reporters carried with them when moving around in Oslo. In fact, the existing IMSI detection solutions are based on portable devices that monitor the radio access network to detect possible presence of IMSI catchers. There is today no network based solution to detect IMSI catchers and the reasons are twofold. First, the need for IMSI detection is so far non-existent because there are only a few IMSI catchers used by governmental agencies in the fight against crimes and terrorism. Secondly, mobile operators do not consider IMSI catchers as threats because they just monitor the users' conversation and do not do any harm to their mobile networks. However, with the increasing number of mobile phone tapping incidents, the users start to lose confident in mobile communication and mobile operators begin to realise that something must be done. This paper introduces a Machine Learning based IMSI catcher Detection system that was initiated by the Telenor ImobSec project in collaboration with Norwegian universities and security experts. The paper begins with a review of related works. Next, a comprehensive explanation of the IMSI catcher is given. For the detection of IMSI catcher the attributes of the anomaly input data set are then identified and clarified. The challenges to the proposed system are also analysed. The central part of the paper is the proposed Machine Learning based IMSI catcher Detection system which is described thoroughly. Further works are proposed in the conclusion.

2 Related works

There are currently several initiatives aiming at developing IMSI detection solutions and as the review in this section will show they are all mobile device based solutions.

2.1 Security Research Labs (SRLabs)

The SRLabs [3] in Berlin directed by the famous German Cryptographer and security scientist Karsten Nohl has conducted a few activities focused on the detection of mobile phone tapping. For the assessment of mobile network security SRLabs offers a set of tools.

CatcherCatcher
One of these tools is the CatcherCatcher tool which has the ability to detect mobile network irregularities suggestin a fake base station activity. The CatcherCatcher consists of:

- Osmocom[1] phone [4]
- Osmocom cable
- Linux computer

Figure 2 SnoopSnitch main Views

SnoopSnitch
SnoopSnitch is an Android application which by collecting and analysing wireless radio data, makes users aware of their mobile network security and warns them about possible threats such as fake base stations (IMSI catchers), user tracking and Over The Air updates as shown in Figure 2. With SnoopSnitch users can both make use and contribute data to the GSM Security Map at gsmmap.org.

---

1 The Osmocom project is a family of projects that are related Open source mobile communications. Its provides software and tools for a variety of mobile communication standards, including GSM, DECT, TETRA and others.

This application is currently working only on Android phones with a Qualcomm chipset and a stock Android ROM (or a suitable custom ROM with Qualcomm DIAG driver). Root privilege is required to capture mobile network data.

2.2 Android IMSI-Catcher Detector (#AIMSICD)

#AIMSICD [5] is an Android-based project originated from XDA forum[2] with the goal of detecting and avoiding fake base stations (IMSI-Catchers) in GSM/UMTS networks which receives contributions from a large amount of anonymous and public Android developers, baseband hackers. All the developments are fully open source under GPL v3+ and located in an official GitHub repository.

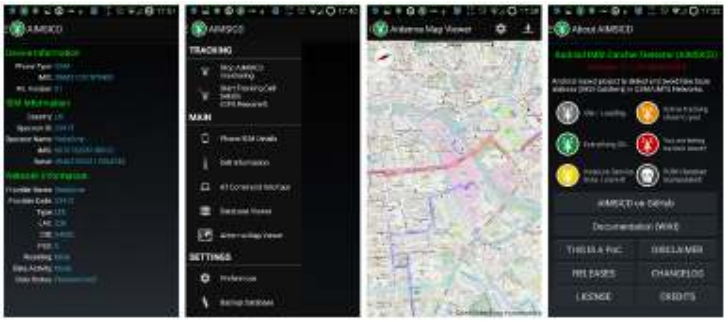

Figure 3 #AIMSICD main views: Main Screen, Cell Information, Database Viewer, Map Viewer (Courtesy: #AIMSICD)

The project has achieved the following:

- Main Views as shown in Figure 3:
  - **Main Screen:** Information about Device, Network and SIM-Card
  - **Cell Information:** Relevant variables using public AOS API calls (LAC, CID, Signal Strength)
  - **Database Viewer:** Data collected by the phone and from public DB of Cell Towers
  - **Map Viewer:** Shows Cell-Towers from the public database that are in your area
- Functions:
  - **Cell-Monitoring:** Collects information about the cell towers you are/were connected to and saves it in the local database
  - **Cell Tracking:** Tracks your position while you are connected to the cell-tower and saves it with cell data in the local database
  - **Download data** from public cell-tower database (right now only from OpenCell_ID)

2 XDA Developer (also known simply as XDA; often denoted as xda-developers) is a mobile software development community of over 5 million members worldwide, started in January 2003

    - **Position Tracking:** Using the GPS-Sensor and Google Location Service
- Detection:
    - **Check Cell_ID**'s collected by the phone against public Cell-Tower Database.
    - **Check for "Changing LAC"** of each Cell-ID that is collected by the phone.

2.3 SBA Research

SBA Research is an Austrian research center for Information Security funded by the national initiative for COMET Competence Centers for Excellent Technologies. It enables the collaboration of 25 companies, 4 Austrian universities, one university of applied sciences, a non-university research institute, and many international research partners on challenges categorizing from organizational to technical security. SBA Research has two independent implementations of an IMSI Catcher Catcher (ICC). The first one employs a network of stationary (sICC) measurement units installed in a geographical area and constantly scanning all frequency bands for cell announcements and fingerprinting the cell network parameters. These rooftop-mounted devices can cover large areas. The second implementation is an app for standard consumer grade mobile phones (mICC), without the need to root or jailbreak them [6].

3 Brief description of IMSI catcher

An IMSI catcher is a device for intercepting GSM mobile phones. It subjects the phones in its vicinity to a Man-In-The-Middle (MITM) attack by pretending to be the preferred base station in terms of signal strength.

As its name tells, the IMSI catcher logs the IMSI numbers of all the mobile phones in the area, as they attempt to attach to the base station, and can determine the phone number of each individual phone. It also allows forcing the mobile phone connected to it to revert to A5/0 for call encryption (in other words, no encryption at all), making the call data easy to intercept and convert to audio. The phone calls can hence be tapped and recorded by the IMSI Catcher.

This specific MITM attack was patented by Rohde & Schwarz, which presented the first IMSI Catcher GA 090 in Munich in 1996. On 24 January 2012, the Court of Appeal of England and Wales held that the patent is invalid for obviousness, since in reality it is just a modified cell tower with a malicious operator.

The GSM specification requires the handset to authenticate to the network, but does not require the network to authenticate to the handset. This is obviously a weakness but GSM is a 26 years old technology and at its specification time it was almost impossible to have access to a false base station and a mutual authentication would be too heavy for the SIM card. IMSI catchers are employed by law enforcement and intelligence agencies.

To remedy the weakness of GSM, UMTS (3G) and LTE (4G) introduce mutual authentication, which requires also the authentication of base stations towards the mobile handset. Unfortunately, due to backward compatibility and the use of GSM as a fallback network where UMTS is not available, mobile phones can be forced to downgrade to a 2G connection and fully exposed to tapping [6].

Figure 4 Various current IMSI catchers (courtesy: #AIMSICD)

As shown in Figure 4, not like the first generation IMSI catchers which were big, heavy and expensive, the current ones come in uncountable shapes, sizes and prices, and can be as tiny as the portable Septier IMSI-Catcher Mini.

4 Detection of IMSI catcher

To detect the presence of IMSI catcher it is necessary identify the anomalies in the mobile networks and to define the nature of anomaly detection input data set [7]. The outlier (anomaly) detection approach type 3 [8] is chosen since we already have a lot of knowledge about the mobile network. A few cases of IMSI catcher presence are considered to model anomalies and to define the input data set.

4.1 Camping in 2G instead of 3G

In many areas, especially the urban ones, 2G, 3G and 4G networks will quite often coexist to accommodate all kinds of handsets and subscriptions. A 3G enabled handset will normally connect itself to 3G networks since services with higher QoS could be provided. An IMSI catcher would jam the signals of the 3G base stations and force the mobile phone to disconnect from the original network and register to it. The IMSI catcher [9] acts as a base station toward the mobile station and as a mobile station toward the real base station as shown in Figure 5. The IMSI catcher can establish a regular connection with the mobile network using its own SIM or without a SIM. In the latter case, in the authentication process, the IMSI catcher simply forwards the authentication data received from the mobile terminal to the base station and conveys the data from the base station to the mobile phone. The session has to be conducted with disabled encryption in both ways since the IMSI catcher does possess the ciphering key K_c.

Seen from the network anomalies created by the IMSI catcher in an area may have as a contextual attributes the *percentage of mobile phones on 2G* and the *one of mobile phones on 3G*. Indeed, a 2G percentage higher than average or a 3G

percentage lower than average will be considered as contextual anomalies. Another contextual attribute is the *percentage of 3G enabled mobile handset* that together with the two previous ones constitute a collective anomaly. The anomaly model can be improved further by the addition of more attributes such as *signal strength*, *antenna type* (omnidirectional, sectorial), *cell ID*, *cell size*, etc. such that the detection can be improved and false positive reduced.

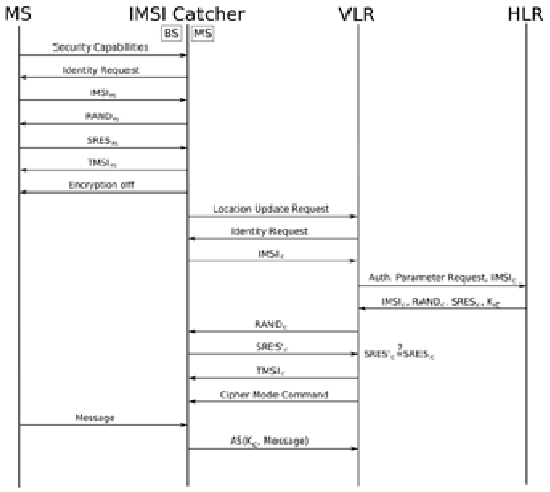

Figure 5 Man-in-the-middle attack with an IMSI Catcher

4.2 Temporary disappearance of mobile phones

Quite often IMSI catchers have to jam all the signals in its vicinity. This will make the mobile stations around lose their connections to the mobile network. They will not be reached by the paging of the base station controller (BSC) at incoming calls addressed to them. The calls can hence not be delivered to the mobile phones as if they have moved to an area without coverage or if there are switched off or ran out of power. Anyway they seem to disappear from the network.

The *number of mobile phones* that disappear for certain period of time from a network area will be used as a condition attribute for the IMSI catcher anomaly because a high value of disappeared mobile phones can indicate the possible presence of an IMSI catcher.

4.3 Disabling of encryption

Although not all the IMSI catchers the ones that do not use their own SIM to establish a connection to the mobile network, must disable encryption to tap the call since they do not have access to the ciphering key K_c. Although they have lower

probability to succeed due the security requirement at many mobile operators these IMSI catchers are still in operation in many countries.

The number of call established with disable encryption can be used a contextual attribute for the IMSI catcher anomaly because a high value of calls with disable encryption can be an indication of the presence of an IMSI catcher.

4.4 Challenges to the IMSI catcher anomaly

Although using anomaly detection in the detection of IMSI catcher there are, however, a few challenges that need to be considered carefully as follows:

Determination of the area for the IMSI catcher anomaly

To determine the area for the collection of the input data set could be a challenging task because 2G (GSM), 3G (UMTS) and 4G (LTE) have different partitioning for location updating of the mobile phone.

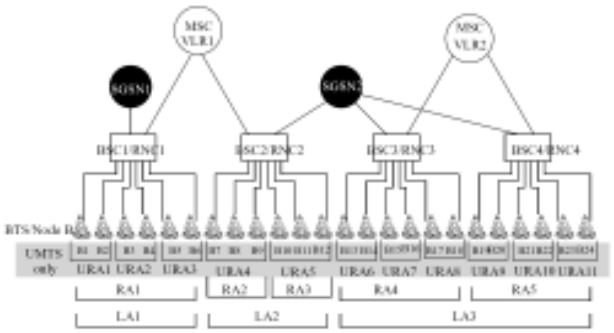

Figure 6 Geographical partitioning in UMTS

A GSM network (2G) is divided into cells, which are grouped into a *location Area (LA)*. A mobile phone in motion keeps the network informed about changes of the location area [10]. When moving from a cell belonging to a location area to another cell belonging to another location area, the mobile terminal has to perform a location area update to inform the network about the new location area in which it is located. A location area is usually managed by a base station controller (BSC) and could be a candidate for the data collection area.

In a UMTS network (3G) a serving GPRS support node (SGSN) manages one or more Radio Network Controllers (RNC) and an RNC manages several Node B (equivalent to base station in GSM) [11].

To track the location of a UE (mobile phone) some geographical groups are defined within the UMTS Radio Access Network (UTRAN) as follows [12]:

- *Location Area (LA):* covers the area of one or more Radio Network Controllers (RNC) managed by the same SGSN.
- *Routing Area (RA)*: is a subset of a LA. It only covers one RNC or even only a subset of an RNC.

- *UTRAN RA (URA):* is a subset of an RA. It only covers multiple NodeBs of one RNC.

LAs are used in the Circuit-Switched-domain and RAs in the Packet-Switched domain. As shown in Figure 6 Geographical partitioning in UMTS, a LA can have one or more RNC and one or more RA. An RA can have one or more URA. All the geographical partition may be considered as data collection area since the mobile station could be tracked in all of them.

In an LTE network (4G) the cells (eNodeB) are grouped in *Tracking Area (TA)* used for paging of the UE (Mobile phone) [13]. Tracking areas can be grouped into lists of Tracking Areas (TA lists), which are administered by the User Equipment (UE). Tracking area updates are performed periodically or when the UE moves to a tracking area that is not included in its TA list. Mobile operators can allocate different TA lists to different UEs. By this way signaling peaks can be avoided in some conditions. For example, User equipment of train passengers may not perform tracking area updates simultaneously. The dimension of the TA compared to the LA depends on many factors like LTE paging capacity, TA update overhead, LA update overhead, etc. and could vary depending on the network. The Tracking Area (TA) may be considered as a data collection area because the mobile phone could be tracked in it.

At the first glance, the Location Area of 2G is most suitable to be the data collection area but considerations have to be done when performing the mapping of Routing Area (RA), UTRAN (URA) and Tracking Area (TA) to LA because full match may not be achieved.

Collection of data

The attributes of the input data set for the IMSI catcher are operational data of the mobile networks. They are collected, used and disposed within a period of time because they are huge in amount. For a more permanent storage of these attributes upgrades on the mobile networks have to done and this could pose financial issues.

The ultimate goal of the IMSI catcher detection system is to identify the fake base stations as quickly as possible. Since those base stations quite often are on the move the collection of data has to be done mostly in real time. This becomes a bigger challenge when the input data are collected from distributed network components. A solution could be a distributed system having a collection and detection function for each data collection area e.g. Location Area.

5 The proposed Machine Learning based IMSI catcher Detection system

To utilize and combine the previously mentioned contextual attributes for the detection of IMSI catcher we propose an innovative detection system based on machine-learning techniques which consists of two main parts as shown in Figure 7 namely the online-detection part and the off-line learning part.

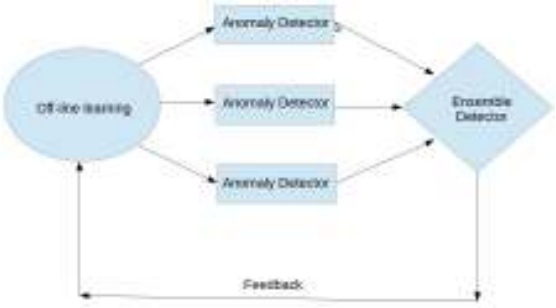

Figure 7 The proposed Machine Learning based IMSI catcher Detection system

As shown in Figure 7, the online-detection part contains different anomaly detectors, each of which uses a contextual attribute to define normal or abnormal behavior. For example, in our case we can have three different anomaly detectors. The first one is based on the change between 2G and 3G modes. The second one takes into account the temporary disappearance of mobile phones. The third one uses the disabling of the encryption. To combine these detectors, an ensemble detector is needed. A simplest form of the ensemble model is the majority voting between the different detectors but a weighted voting may also be considered in later phases. Several machine-learning algorithms, such as one-class Support Vector Machines [14] and Neural Networks, can be used as anomaly detectors.

Following the suggestions from the ensemble detector, security experts would then look at suspicious places to verify if there any true IMSI catchers at a point in time. The feedback from the security experts is then given back to off-line learning part to update the models where the normal behavior was defined.

At the present stage of our project no real data set has been yet collected from the mobile network and for illustration sake we did some experiments on the public available data set related to IMSI catcher detection from Aftenposten [15]. The data came from a handset while interacting with the mobile network and possibly with the IMSI catchers as well, and we cannot show the advantages of machine-learning in correlating different events from many different devices. However, the main objective of this experiment is to show that there is a potential of applying machine learning techniques to facilitate the detection process.

For our simple experiment, from the data set we were interested in the frequency of the mode change between 2G and 3G. Our hypothesis is that the high value of the frequency would indicate abnormality in an area.

We split the data by equal time slots and calculate the ratio between the number of 2G and 3G in each time slot. We applied the anomaly detection algorithm named S-H-ESD from Twitter [16] to detect abnormalities for those obtained ratio values. The result is shown in Figure 8. The three high spikes, which denote the abnormalities, indicate the possible presence of IMSI catcher

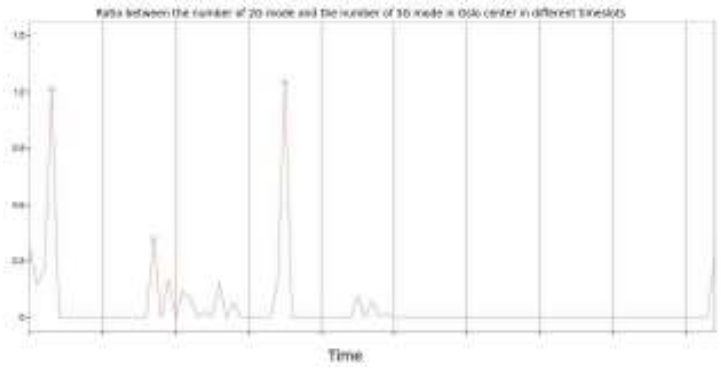

Figure 8 Experiments on 2G/3G modes with Aftenposten data set

6 Conclusion

In this paper an innovative system for the detection of IMSI catcher is presented and described. It has a few advantages compared to the current existing solutions. First, according to our knowledge, most of the current IMSI catcher detectors, are located on the handset side, either as a dedicated device or an application that can be downloaded and installed in a regular mobile phone. They are intended for the users and put the responsibility of protecting confidentiality and privacy on the users' shoulders. This may be both unfair and unmanageable for non-technical users. The proposed Machine Learning based IMSI catcher Detection system is network based and intended for mobile operators in the protection of their users. It is offering a more balanced and fair solution. Second, by being network based the proposed system will be able to carry out the data collection and detection at several areas simultaneously and hence improving the ability to detect an IMSI catcher. Third, the proposed detection system is using machine learning techniques and can hence learn and enhances itself more rapidly than the current IMSI catcher. However, as stated in the paper, there are also a few challenges such as determination of the area for the IMSI catcher anomaly, and collection of data, that have to be surmounted. The ImobSec project is also in very earlier phase and only data set from Aftenposten has been experimented. As future works, the proposed Machine Learning based IMSI catcher Detection system will be installed and deployed in the Telenor Norway mobile test network. Experiments will then be carried out with the introduction of the project's IMSI catcher in the network. The lessons learned will then be applied to optimize and improve the system further.

References

1. A.B. Foss, P.A. Johansen, F. Hager-Thoresen: Secret surveillance of Norway's leaders detected; Aftenposten, 16 Dec 2104; http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html
2. GSMK CRYPTOPHONE: http://www.cryptophone.de/en/
3. Security Research Labs: https://opensource.srlabs.de/
4. The Osmocom (Open Source Mobile Communication) project: http://openbsc.osmocom.org/trac/wiki/OsmocomOverview
5. Android IMSI-Catcher Detector (#AIMSICD); https://secupwn.github.io/Android-IMSI-Catcher-Detector/
6. A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani and E. R. Weippl: IMSI-Catch Me If You Can: IMSI-Catcher-Catchers in Annual Computer Security Applications Conference (ACSAC), 2014, ACM 978-1-4503-3005-3/14/12
7. Chandola, V.; Banerjee, A.; Kumar, V. (2009). "Anomaly detection: A survey". ACM Computing Surveys 41 (3): 1. doi:10.1145/1541880.1541882
8. Hodge, V. J.; Austin, J. (2004). "A Survey of Outlier Detection Methodologies". Artificial Intelligence Review 22 (2): 85. doi:10.1007/s10462-004-4304-y
9. Daehyun Strobel: IMSI Catcher, Chair for Communication Security, Ruhr-Universität Bochum, July 13, 2007
10. 3GPP: Technical Specification TS 23.012 Location management procedures, V12.0.0 (2014-09)
11. 3GPP: Technical Specification TS 23.060 GPRS Service Description describes, V13.2.0 (2015-03)
12. Yuh-Shyan Chen: Chapter 2 Mobility Management for GPRS and UMTS; Department of Computer Science and Information Engineering National Taipei University
13. Ayman ElNashar, Mohamed El-saidny, Mahmoud Sherif: Design, Deployment and Performance of 4G-LTE Networks: A Practical Approach; ISBN 1118703448, 9781118703441- John Wiley & Sons, 2014
14. R. Vert, J.-P. Vert, Consistency and Convergence Rates of One-Class SVMs and Related Algorithms, JMLR 7, 817-854, 2006
15. Aftenposten data set. http://www.aftenposten.no/meninger/kommentarer/Derfor-publiserer-Aftenposten-hele-datagrunnlaget-for-mobilspionasje-sakene-7849555.html
16. Anomaly Detection algorithm from Twitter. https://github.com/twitter/AnomalyDetection