Some Dangers from 2G Networks Legacy Support and a Possible Mitigation

Conference Paper · September 2015

DOI: 10.1109/CNS.2015.7346872

Abodunrin Dare
Aalto University
1 PUBLICATION **7** CITATIONS
SEE PROFILE

Yoan Miche
Nokia Bell Labs, Espoo, Finland
120 PUBLICATIONS **3,580** CITATIONS
SEE PROFILE

Some Dangers from 2G Networks Legacy Support and a Possible Mitigation

Dare Abodunrin, Yoan Miche and Silke Holtmanns
Nokia Solutions and Networks Group
Espoo, Finland
Email: first.last@nokia.com

***Abstract*—We present in this short study, some of the well-known problems with the current legacy support for 2G cellular networks, and the security and authentication problems this poses, as demonstrated in recent document leaks about spying from US embassies [1]. We have conducted focused radio measurements in the Helsinki Metropolitan area on these security problems and present some of the findings here. Also, we propose some mitigation methods for the most likely scenarios that arise in supporting legacy 2G systems in modern operator networks.**

I. Introduction

The first problem with 2G cellular networks, is that they are inherently insecure, due to lacking network authentication. The second problem with them, is that they are still so well supported (for legacy and technical reasons). These two problems are basically at the root of most of the recent news articles about IMSI catching, cellular phone call interception, SMS interception,... One can see [2], [3], [4] for examples of such matters.

Most of these attacks and interceptions were carried out using Fake Base Stations, and following some of the possibilities already mentioned in 2010 at Defcon [5], for example. A fake base station is a base station that is set up to intercept the communication between a user and the mobile operator network, and while the first fake base stations were created for network measurement purposes [6], it is now relatively easy to purchase the hardware and software needed to run one. To the User Equipment (UE), the fake base station appears to be a legitimate base station and to the operator network, the base station appears as a regular user.

One of the primary reason why fake base stations are possible on 2G networks, is that in 2G, the network does not authenticate itself [7]; this has changed in 3G and 4G. But since many areas in the world only provide 2G coverage and many 2G phones still exist, 2G needs to be supported for both terminals and networks.

In order to "catch" users connected to more recent networks such as 3G or 4G, the typical attack scenario is for the fake BTS to tell the terminal that it currently cannot operate on 3G or 4G, and thus force a downgrade to 2G. From then on, due to the now insecure authentication and encryption mechanisms in the 2G standard, it becomes possible to spy on the user.

The following section II goes into some of the details of why 2G is insecure, and how can it happen on modern networks. Section III summarizes a real case analysis performed in the Helsinki Metropolitan area, to find such unusual behaviours and possible fake base stations, while section IV proposes some basic mechanisms that can be embedded on the user terminal to avoid connecting to fake base stations, thus not requiring massive infrastructure changes on the operator's side.

II. Some Dangers of 2G Legacy Systems

Here we present some of the reasons why 2G based networks are still in active use and supported, even on the most recent networks, and then some details on the inherent insecurity of the 2G architecture.

A. Downgrading to 2G

All current cellular networks support downgrading to the 2G standard (at least the hardware does; the software can be made not to accept it). This is regardless of which standards the base station supports (3G, 4G). And while it is possible for an operator to disable this support (software), this is usually not done, if only for the fact that not all phones in current use support 3G, or that users sometimes don't want to use solely 3G and 4G networks, for battery consumption reasons.

This legacy support has other reasons: many operators switch to the 2G (GSM) standard for their users calls (and SMS), while the 3G is used for the data transfers. This is because the usual costs of a voice call over 3G are higher to the operator than over 2G, for core network design reasons. Thus, while the user might see the 3G logo while surfing internet, the moment he places a call, it is likely that the operator will require the phone to switch back to 2G for the duration of the call. As we usually have the phone on the ear during a phone call, this is never obvious to notice. There are also cases where access to a data connection is provided for free, and unlimited, but on 2G only (with 3G/4G data connections being at quite different pricing) [8].

In case of a very busy network activity in a certain area, it is also likely that some users will get downgraded by the operator (legitimately, here), to 2G, to accommodate for the load. Inhabitants of dense urban areas often see this happening at rush hours: 4G connection not reaching the destination, followed by a downgrade to 3G and eventually to 2G to be able to place the call.

B. 2G is inherently insecure

The 2G system was designed for the time where it was too impractical or even impossible for someone to get their hands on the hardware equipment necessary to set up a base station. Thus, the authentication and verification mechanisms between the user equipment and the base station are very easily circumvented. To be more precise, the user equipment is required to authenticate against the network, in order to use the service. This happens as follows:

1) User starts by sending its unique identity, IMSI, to the Visitors Location Register (MSC/VLR, a temporary database of users);
2) Since MSC/VLR cannot decide to authenticate user on its own, it passes this information to the Home Location Register (HLR) of the user to notify the network of the user's intention to connect to it;
3) In response, HLR generates a random number known as RAND, and a cipher key, KC, for subsequent connection attempt. It also generates the security result, SRES. All these three parameters, refered to as the authentication vectors or GSM triplets, are sent back to the VLR.
4) MSC/VLR only transferred RAND to the user but keeps both the cipher key, KC, and the SRES for authentication purposes.
5) User's mobile device, transfers this to its SIM card to resolve. In SIM is a one-way function, A3, that takes its input:Ki and RAND to calculate RES and sends back to VLR.
6) MSC/VLR checks the received RES from mobile user and compares it with the SRES received from the HLR. If both matches, VLR sends to user's device, Kt and a TMSI for connection. Meaning that user does not need to contact the HLR in subsequent authentication attempts.

One notable thing in this authentication algorithm, is that the user equipment never gets the chance to authenticate the network it is connecting to, nor the base station it communicates with. Therefore, it might send its IMSI to a fake base station, as part of the authentication mechanism. Finally, setting up a device mimicking a BTS (at least for 2G networks) is nowadays rather cheap and quite trivial [9], or can be obtained for research purposes [10].

The second reason for the insecurity of the 2G standard is due to the crypto used in the communication between the user equipment and the base station.

2G security mechanisms and encryption are known to be weak and hack-able, thus enabling the hacker to record/intercept the calls and the messages sent. The fake base station may even claim that it can not offer encryption (i.e. only A5/0 support) and force then the terminal to switch off encryption on the air interface. Alternatively, it may force an old terminal to use A5/2 or depending on how much computational power the attacker has available, A5/1 (for the case that the real operator is using A5/3, which is currently not that widely rolled out yet).

The first theoretical attacks on A5/1 were performed in 1994 by Ross Andersson [11] and through subsequent improvements and research e.g. Barkan, Biham and Keller [12], became "practically feasible" around 2003-2006. Further attack refinements yielded substantial improvement with respect to needed computational effort. That those attacks are taking place was confirmed in [13].

And while this possibility has been documented and investigated for 2G networks extensively since 2010 [5], the existence of fake base stations (or interceptors/stingrays) that can pretend to be legitimate 4G ones was only discovered rather recently, through confidential documents leaks [14]. Even if the mobile operator provides high quality air-security, recent SS7 attacks via the roaming interconnection network may lead to the compromise of the security keys [15] which then in turn can be used to decrypt the communication over the air. One reason not to intercept the communication also over the air interface might be that the interceptor leaves less data traces and is harder to note by network screening tools.

To summarize, the fact that 2G is still so heavily and "blindly" supported (meaning without ensuring that the request to use 2G is legitimate), makes fake base stations, intercepters, and IMSI Catchers possible.

III. Surely, This does not happen on modern networks: Study

One could think that on modern and up to date (i.e. recent 4G hardware and excellent 4G coverage of an European capital area), such events and 2G downgrades should not happen.

We have conducted a short study in the Helsinki Metropolitan area to check if such behavior happens at all, during daytime, in excellent 3G coverage areas according to operator coverage maps ([16], [17], [18]), with very little users. We were looking for obvious signs of possible fake base station activity, such as

- Unusual long cuts in the network, both in 2G and 3G, while still connected to BTS;
- Base stations with unusual power;
- Base stations with unusual LAC/CID/MNC;
- Deactivation of encryption;
- Sudden downgrades from 3G to 2G;
- Inavailability of encryption, especially status changes (A5/3 to A5/1/0);

on three mobile networks in Finland.

A. Experimental protocol

To conduct this study, we selected three busy areas in the Helsinki neighborhood namely: Eira, Kulosaari, and Kuusisaari. These areas are of particular interest because of the concentration of Embassies situated in those locations making it attractive enough to motivate attackers and spies. In addition, embassies can be interesting locations to place network equipment meant for monitoring [19], as they are usually located in busy city locations, and eventually nearby official buildings.

The measurements are based on the use of both software applications and physical equipment to capture possible network activities happening around target locations.

Three 4G capable mobile phones (two Sony Xperia Z2 and a Galaxy Note 2 LTE) were used as the physical equipment for capturing, with each one connected to a different operator network (three major ones in Finland). The same experiments (see protocol below), are run on all three phones (and therefore, networks) at the same time. For a second measurement, we manually downgraded from 3G to 2G on all these phones within a few seconds and at the same time, then run same protocol again as given below.

The overall protocol is:

1) Reach one of the selected areas.
2) Set phone networks to WCDMA / UMTS mode only (3G).
3) Start data recording on both Snoopsnitch and AIMSI catcher
4) Run 5x4 tests in Snoopsnitch, several times.
5) Walk around the area while running active tests.
6) After one tour is done, switch all phone networks to 2G mode only.
7) Restart the same experiments on 2G, with similar tour.

B. *Observations*

While we will not present all of the data from the study here, for technical and space reasons, we can summarize the findings per area as follows:

a) Eira Area:

- Cuts for 2-5 seconds over UMTS (no network)
- One long cut of 27 over UMTS (no network)
- Almost 2 minutes lost network while switching from 3G to 2G, connected to one BTS, but no network
- Downgrade from 3G to 2G for 2 minutes 49 seconds
- Lost network for 8 minutes 51 seconds while switching 3G to 2G (connected to 2 BTS with varying power)

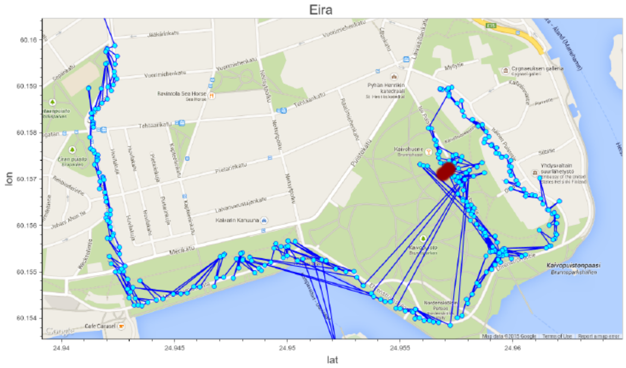

Fig. 1: Itinerary in Eira on 2015-03-03. Dark red dots indicate approximate location of major events .

b) Kulosaari Area:

- Multiple cuts from 3G network over UMTS, no Cell ID or 29006/422217
- Up to 3 minutes cuts, sometimes connected to 29006/422217
- Lost network while switching from 3G to 2G, for 1 minute
- Downgrade to 2G for 40 seconds
- Multiple network cuts on 3G for up to 4 minutes 13 seconds

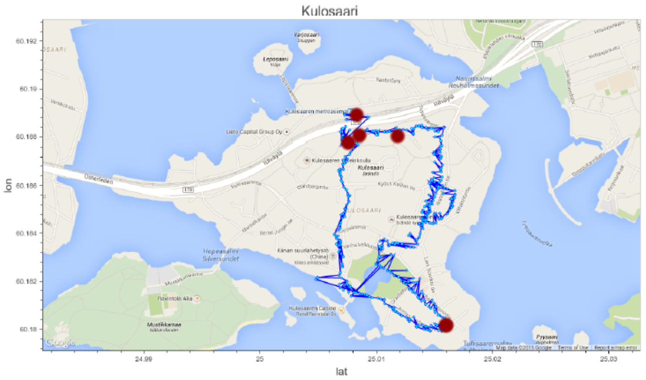

Fig. 2: Itinerary in Kulosaari on 2015-03-03. Dark red dots indicate approximate location of major events.

1) Kuusisaari Area:

- Downgrade from 3G to 2G for 2 minutes 28 seconds
- Multiple LAC changes (might be normal)
- Lost the 2G network for 1 minute 45 seconds

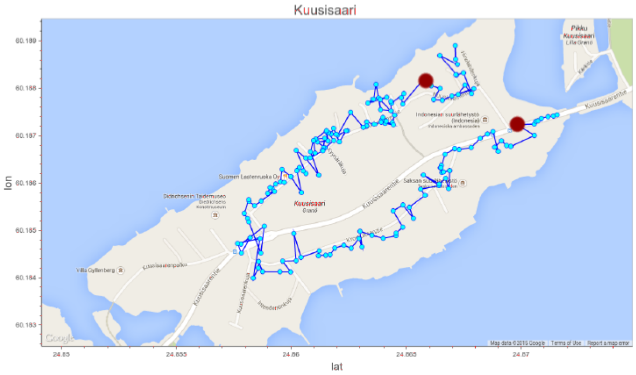

Fig. 3: Itinerary in Kusisaari on 2015-02-20. Dark red dots indicate approximate location of major events.

While we could not get access to operator data in order to validate (or invalidate) these findings, it is worth noting that: if even some of these findings are actual anomalies (IMSI Catchers, fake base stations, e.g.), the situation is worrysome. And if none of them are, this means that all three major operators, downgrade their users from 3G to 2G, for no apparent reason (to remind, this was all conducted during workdays, work hours, with no unusual concentration of users, and in areas that are supposed to be perfectly covered by 3G and 4G). The likelihood of downgrades over more than one operator at a time, in the same place, at the same time, is highly unlikely, as this would imply a configuration error for two or more operators in parallel.

In any case, while it is probably too much of an effort to modify the 2G authentication mechanisms for better security, it is possible to at least warn the user about the possibility of unusual activity and fake base stations. Some applications (discussed in the following) already allow for such information to be provided to the user. We propose in addition a mitigation mechanism to avoid connecting to a fake base station, and thus to avoid revealing IMSI and having calls and SMS being intercepted.

IV. Making sure the fallback to 2G is more secure: Mitigation

A. Current Alerting Applications

Currently, there are three major applications available for the Android platform which can be used as a source of information on the base stations in range: Snoopsnitch [20], AIMSIC [21], and Darshak [22]. These applications each have a different scope and data sources, and therefore perform slightly differently: Snoopsnitch [20] relies on baseband level data, using the Osmocore library, and therefore is limited to a specific type of modem chipsets. Snoopsnitch focuses primarily on listening for possible SS7 abuse and SMS/call interception, by providing active testing (their servers act as a caller/receiver and the phone tries to place and receive calls and SMS to it. AIMSIC [21] is focused specifically on IMSI Catchers, although they support displaying indications of all sorts of unusual activity. As the application remains at the userspace level (no need for root access), it does not use baseband level information, but the data provided by the Android OS layer. Finally, Darshak [22] is a blend of the two applications, currently only for Intel XGold baseband chipsets: it offers warnings and information about the encryption levels used by the base station, the authentication mechanisms used, as well warning for silent SMS and potentially intercepted phone calls and messages.

Overall, the information captured by these applications and displayed back to the user is very valuable. But it is worth noting that almost all of the "anomalies" detected by these applications could be part of normal network operations (albeit not in favor of the user experience...). In addition, these applications merely warn the user of abnormal activity, and not to avoid the connection to a potential fake base station.

In the following subsection IV-B, we propose a mitigation possibility for the problem of the fallback to 2G (or downgrade). In section IV-C, we propose to illustrate the methodology in three different scenarii, each likely to happen in real life cases.

B. Proposed Mitigation

1) Setup for the Mitigation: This methodology can be implemented in the user's mobile equipment and should be implemented as a software or an application that relies on the real operator information of all existing and genuine base stations.

Meaning that the user's mobile device plays an active role, as the actual detector which after spotting an abnormal activity then alerts or reports to the operator of a suspected fake base station present in the network, and avoids connecting to it, or sending it any information.

The methodology relies mostly on the existence of a database on the operator core network, holding the exact location of all the BTS in use, the power with which they emit, and their characteristics (Location Aread Code (LAC), Cell ID (CID)).

As depicted on Figure 4 there are four entities involved in this methodology: the mobile device (which we are proposing to be the detector), fake BTS (not initially known as fake), real BTS (we are also initially uncertain of), and an operator's database (present in the operator core network).

We start with the general assumption that both mobile device and operator's network have already passed through an authentication process and confirmed to be genuine at some point in the past, and therefore are certain that the mobile device is connected and has access to the real database at some point.

For several reasons (one of them being mobility [23], [24]), the mobile device interacts with one or many base stations, for example while the mobile device is in motion, and moving from one location to another. During this stage, the received Quality of Service (QoS) is a priority that must be maintained, therefore the mobile device keeps listening to nearby base stations to select the one offering the best transmission signal power [25].

The pair of black dotted lines as we see in Figure 4, denoted as number one, is used to represent unconfirmed base stations that the mobile device is able to receive transmission signal from i.e. through which the mobile device can communicate with the network if they are genuine.

As a detector, the mobile device uses our proposed methodology (described in detail in the next section IV-B2) to verify all received nearby signals. The red solid line which is numbered as two denotes a suspicious BTS, while the second BTS, denoted by a long black solid line and numbered three is used to represent the real operator's BTS.

The final phase of the proposed methodology, denoted by a green line and numbered as four, represents an alert initiated by the mobile device and sent to the network of a suspicious activity and the presence of an unregistered BTS in the network.

On a precise note, the proposed methodology should enable a mobile device to practically detect false base station and alert the network as a mitigating step on 2G, 3G, 4G, and possibly 5G, in these two considered cases:

1) A base station with wrong LAC/CID but on the operator network. Such fake BTS in this case have correct Mobile Network Code (MNC) and Mobile Country Code (MCC).
2) A base station with correct LAC/CID but existing on the operator network, trying to pass for a real BTS.

Each base station is in fact uniquely identified by these four identifiers (from widest range to smallest): MCC, MNC, LAC,

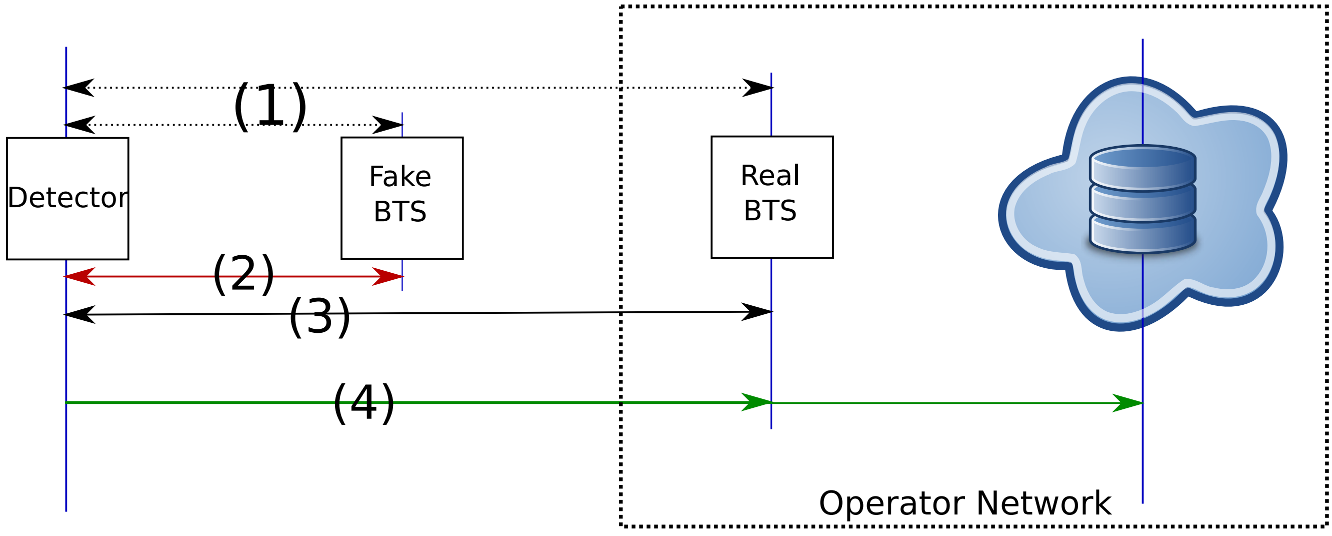

Fig. 4: General overview of proposed methodology indicating process flow.

CID. The MCC and MNC are country and operator specific and this couple uniquely identifies an operator in a country. The LAC allows the operator to divide the territory it covers in large areas, in each of which a set of base stations with a unique CID (for this LAC) are located.

The first case mentioned above therefore arises when a fake base station, which can be operating as a proxy in the operator network or not, does not use an existing LAC/CID combination from the operator it claims to be connected to. While in the second case, the fake base station impersonates a real base station within the attack region and thus pretends to be part of the operator's network. It is also possible in this case to have the fake base station connected as a proxy to the operator network, or not connected to it at all.

2) Methodology: A more detailed technical overview, which shows the type of information passed from one entity to another and the process flow in an ideal situation, as a way of complementing the already described procedure of figure 4 is given and explained in figure 5. By an ideal situation, we refer to a genuine case that comprises of real BTS, and real operator database, which is what our first scenario case describes (as we shall later see). Meanwhile, the interaction flow in Figure 5 between active entities is briefly described as follows.

1) The user equipment initiates the interaction by sending a request to the operator network in order to obtain a copy of the operator database (for the area of interest). This request is encrypted with the core network's public key, which is denoted as OpKEY, to ensure that only the real operator's core network can access this message;
2) Base Transceiver Station forward this encrypted request to the core network;
3) Core network decrypts received mobile station encrypted request. Then makes a copy of genuine lists of BTS, as requested by the user equipment.
4) This portion of the database is encrypted with the user equipment's public key and forwarded to the BTS.
5) BTS forwards this message from to the user equipment.
6) The user equipment decrypts the received message, and compares the received Database list (denoted as DB_{core}), to its own Database [1] denoted as DB_{UE}.

The comparison between the obtained data from the operator database (DB_{core}) and the one the user equipment collects (DB_{UE}) is performed at several different levels: Identifiers (LAC/CID), GPS location, and emitted power. The comparison is performed as follows:

1) Collect the list of BTS that are within range (possible since the UE keeps listening to all available nearby transmitting signals), enabling it access also to their various signal power and also their LAC/CID as well;
2) For each BTS in this list:
   a) Calculate estimated GPS location (see section IV-D1);
   b) Compare received parameters (LAC/CID, received signal strength, etc.) from DB_{core} to own internal database DB_{UE} (see figure 6);
   c) If the LAC/CID is not in the DB_{core}: The BTS with this LAC/CID could be a fake (figure 6). Report the details (LAC/CID, power, estimated location) to the operator and move on to the next BTS in the list;
   d) Else, check if the BTS with this LAC/CID is active (i.e. in a normal state);
   e) Compare the estimated location with the one obtained from the database;
   f) Compare also the estimated emitted power with the real emitted power;
   g) If estimated location and power are too different from the operator values, send an alert or report to the operator;
   h) Else, move to the next BTS in the list.

The basic idea behind this methodology is that it is very

[1] Using Figure 4: Mobile Station listens to all received nearby transmitting BTSs, and stores them

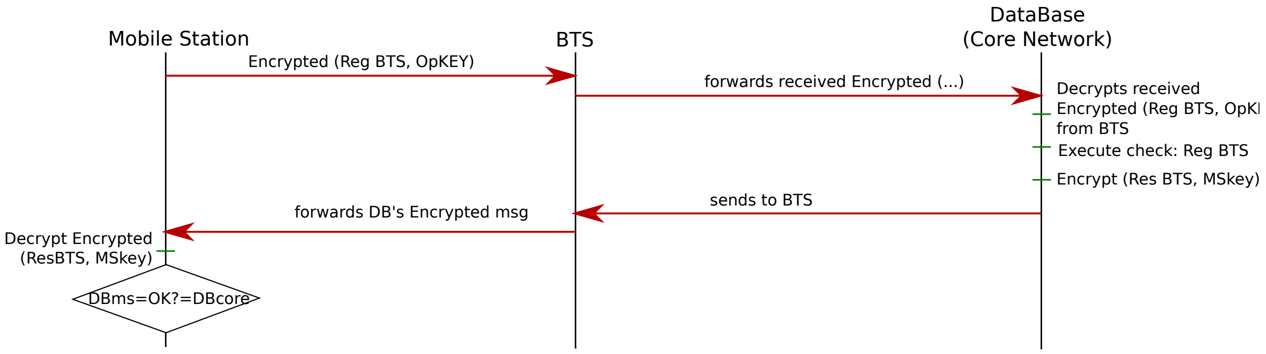

Fig. 5: Description of the process flow and transferred data between the three participating entities in the network.

difficult for a fake base station to have the same LAC/CID as the real one, emit at the same power as the real one, and be in the same location, all at the same time. Faking one or two of each of these verified characteristics is doable, but all at the same time is difficult (not impossible, though).

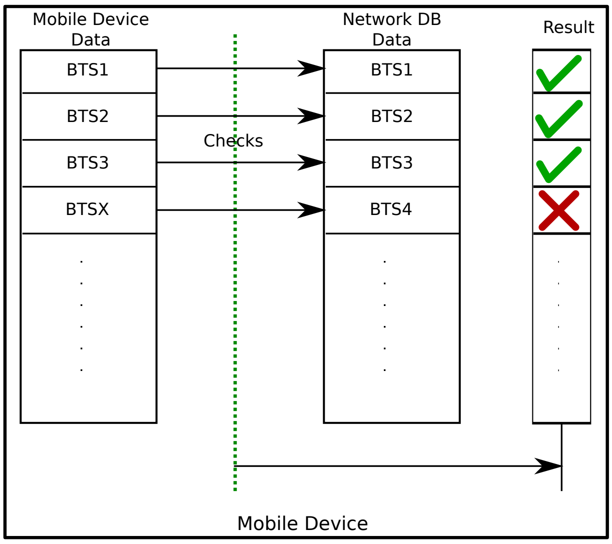

Fig. 6: Proposed methodology implemented as a data verifier on mobile device.

C. Considered Scenarii

We now consider three scenarii that can arise (and which should cover the likeliest situations for a user), and how the proposed methodology handles them.

1) Scenario 1: As depicted in Figure 8, the user equipment interacts with the real operator's database via the operator's base station. In this case, we are certain that the data in the database are genuine simply because it is the real operator's database, and the UE is able to access it. This means that the UE, through listening, is able to acquire the necessary parameters such as LAC, CID, and $\text{Power}_{\text{phone}}$ from nearby cells.

Following the procedure from IV-B2, the UE gets access to the real database and therefore can verify the BTS.

2) Scenario 2: Unlike the first case considered where the network is completely genuine and accessing the database through a real BTS was possible, this second case focuses on the existence of a fake BTS, and its influence on the methodology proposed. We split this scenario into two: access to DB_{core} via a genuine BTS, and access to DB_{core} only through fake BTS.

a) Access to Operator Database via genuine BTS: Using Figure 9, it is possible to consider two scenarios. The first one being a situation where the UE is at the mid-point of the three cells, meaning that it is getting signals from both genuine and fake BTS, but moving more toward a fake base station. In this situation, the UE tries to connect to the operator DB through fake BTS (which has for example, a higher transmission power), which obviously cannot work because a fake base station cannot get access to the real network's database i.e. not authenticated.

The second possible occurrence is when the mobile device connects to a genuine BTS, even with the presence of a fake base station around, and then successfully connects to the network's database as described in the previous Scenario 1.

b) Access to Database only through fake BTS: In a situation as this, where the user equipment can only locate or is surrounded by only fake base stations, it is definitely obvious that it cannot gain access to the operator network's database. As depicted in Figure 10, the UE moves closer to the fake base station, and therefore senses only that base station which it then attempts to connect through to get to the database. The fake base station cannot access the operator core network and even if it creates a fake database to feed the UE, it will not be authenticated with the operator's encryption keys.

3) Scenario 3: Figure 11 illustrates another possible scenario where the mobile device is totally communicating through and with the attacker's set-up network. It has been demonstrated that this is possible in the work of Yubo Song et al. [26].

In this setup, the only safe and possible verification the user equipment can perform, is to use a previously obtained copy of the official database from the operator, and rely on it to verify the nearby base stations. This scenario is relatively unlikely, though, as the user equipment can probably always reach at least one genuine base station, even if this means ramping up the transmission power.

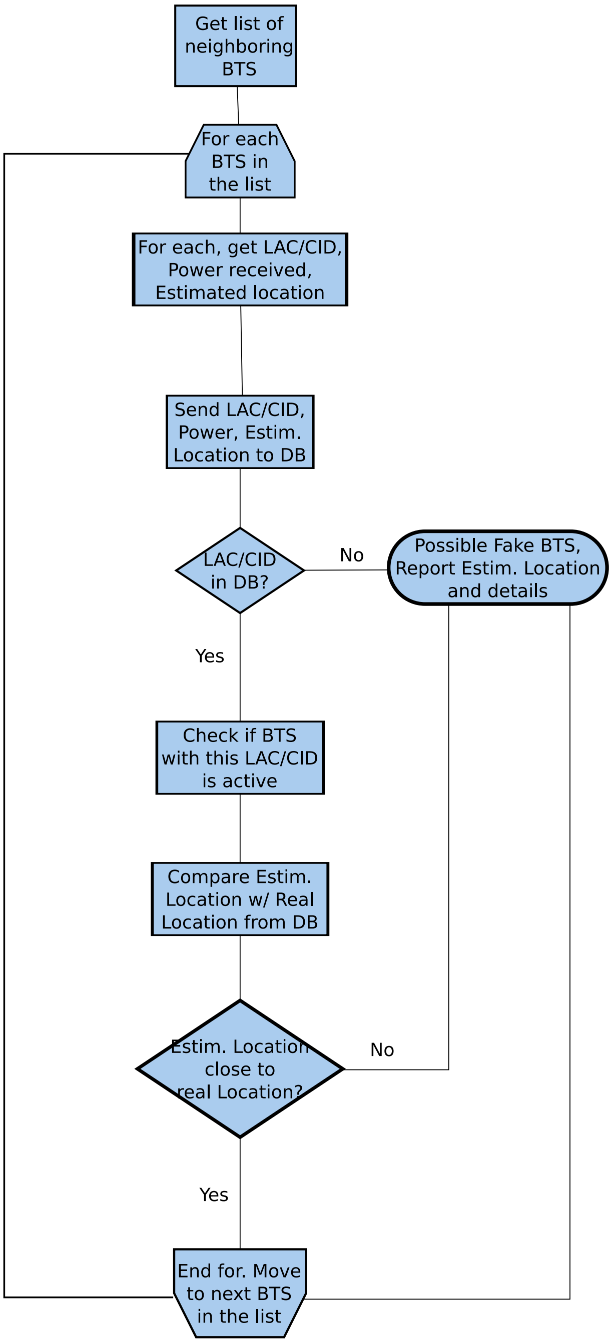
Get list of neighboring BTS
For each BTS in the list
For each, get LAC/CID, Power received, Estimated location
Send LAC/CID, Power, Estim. Location to DB
LAC/CID in DB?
No
Possible Fake BTS, Report Estim. Location and details
Yes
Check if BTS with this LAC/CID is active
Compare Estim. Location w/ Real Location from DB
Estim. Location close to real Location?
No
Yes
End for. Move to next BTS in the list

Fig. 7: Overall schematic of the methodology.

D. Discussion on the Assumptions made

1) Location estimation for Mobile device: It is assumed in this work, that the mobile device, which is the analyzing device, is able to triangulate the position of the BTS it is analyzing.

One benefit of using mobile device as a detector is the dynamic nature it possesses, which gives it the flexibility to move from one location to another. This attribute to move around makes it possible to directly triangulate the origin of the signal coming from the BTS being analyzed.

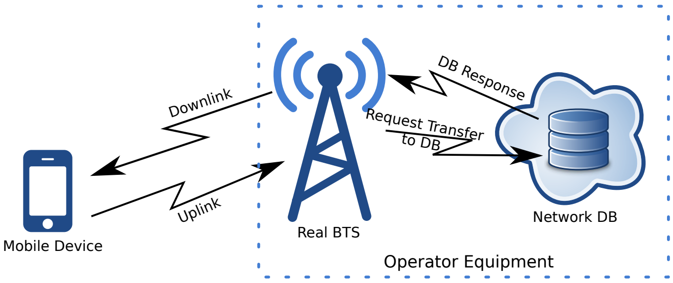

Fig. 8: This scenario considers the user equipment communicating with a real base station and the real network's database. The equipments on the network sides are genuine.

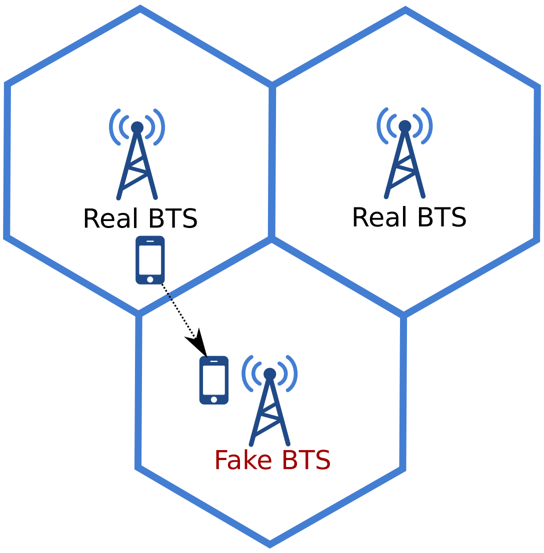

Fig. 9: A wandering mobile device receiving signal both from genuine and fake base stations as it approaches the fake one.

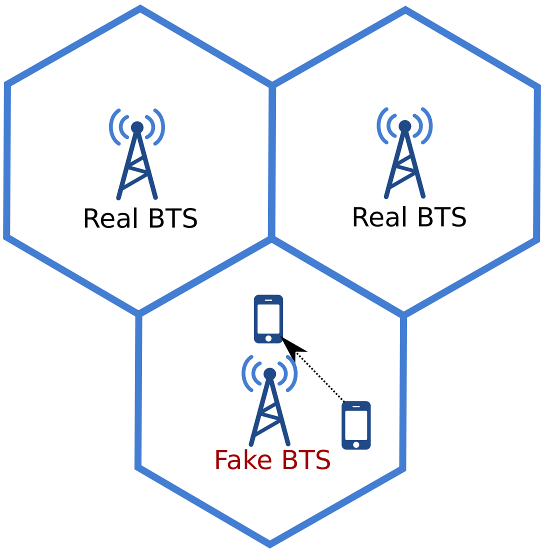

Fig. 10: A situation where mobile device can only receive signal from a fake base station.

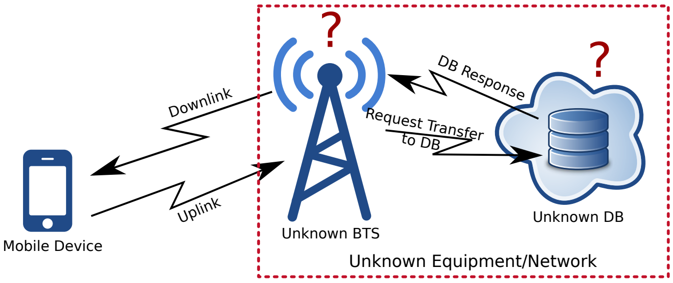

Fig. 11: The interaction between Mobile station and the network can not be trusted because the network is completely unknown.

Mobile devices can apply the triangulating method to locate devices but in a slightly different way than used by the network's BTS. The first requirement is for the mobile device to already have information about the carrier and coordinates of the vicinity, this type of information is available on these web sites [2].

The mobile device, acting as a detector, measures and saves the received signal (device signal strength) from the suspicious device first in location A. The detector moves to another location B and also measures and saves the transmitting device's signal strength received. This procedure can be repeated in several locations for as much as needed, with the knowledge that when more locations are covered, the chances to estimate suspicious device location becomes more accurate. As depicted in Figure 12, from different locations, the mobile device was able to collect different signal power from the suspicious transmitting device, which then applies a triangulation method to estimate location.

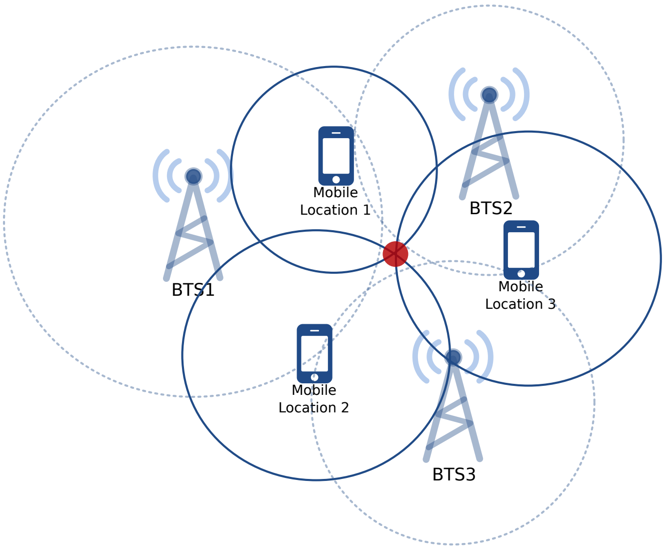

Fig. 12: Mobile device applying the triangulation method from three different locations in order to estimate a base station location, denoted as a red dot.

2) Power Estimation: Using statistical modeling approach such as the Okumura-Hata model [24] and others [3], depending on the building density, BTS height and frequency bands used by the BTS, we can estimate the average path loss between the suspicious transmitting BTS and those receiving its signal (the user equipment in our case), and therefore also compare the received power with the one that should be received.

Path loss measurement becomes very useful during the comparative analysis of the received signal strengths (power) between expected and received values. A translation of this is that by knowing path loss values, one is better equipped in judging what value of received signal power is acceptable or can be considered suspicious. Figure 13 illustrates this idea.

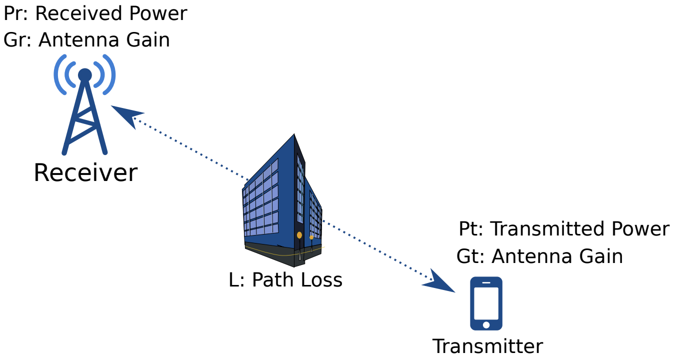

Fig. 13: Showing path loss between the transmitter and the receiver: it is the difference (in dB) between the transmitted power and the received power.

The following describes how the widely used Okumura-Hata model is applied mathematically to obtain the received power from the operator's base station. Certain considerations are taken into account such as; type of environment, and type of antenna used. Environment in this sense translates to the area type, and as such could be large or dense city, medium or small size city, sub-urban, rural or open area, all of which influence the parameters and calculation differently.

The Okumura-Hata Average path loss is given as

$$L_{50}(dB) = L_F + A_{mu}(f,d) - G(h_{te}) - G(h_{re}) - G_{\text{AREA}}, \quad (1)$$

where L_{50} is the 50 percent value of propagation path loss (median), L_F the free space propagation loss, $A_{mu}(f,d)$ the median attenuation relative to free space, $G(h_{te})$ the base station antenna height gain factor, $G(h_{re})$ the mobile antenna height gain factor and G_{AREA} the gain due to environment.

f and d are respectively the operating frequency (150MHz-1500MHz in the original Okumura-Hata model and 1500MHz-2000MHz in the new extension of same model called COST-231) and distance between transmitter and receiver in kilometer.

Further computation is done by substituting the value of L_{50} into P_R, denoting the received power from the base station is done as

$$P_R = P_T - L_{50}, \quad (2)$$

where P_T is the transmitted power from the source.

[2] http://opencellid.org/, and http://location-api.com/

[3] Shadow fading, Multipath fading, exponential distribution

3) Assumption on a Database of BTS from the operator: It is also assumed that the base station can have access (i.e. can query) to a database of all the operators BTS. This database is assumed to have the following information:

1) All the LAC/CID combinations in use for the operator BTS.
2) The associated GPS location (precise) of all the operator's BTS.
3) The power at which the BTS is emitting right now.

V. Conclusions and Future Work

In this study work, we assess some of the weaknesses of the existing 2G legacy systems in telecom operators, and of the dangers of the fallback to 2G from more secure and recent standards such as 3G and 4G. By measuring some unusual activity in Helsinki Metropolitan area, we have also found that such problems can happen, even on modern and "up to date" networks. Finally, in an attempt to mitigate the current issues with downgrading to 2G, we propose a methodology that can be implemented as a software on the user equipment, and requires very little new hardware/software on the operator side. This methodology enables the user equipment to act a detector of fake base stations, to report them to the operator, while having less false positives than the existing applications such as Snoopsnitch.

Future work on this topic is to implement the methodology proposed as an Android application (possibly as part of one of the existing applications mentioned in this article), and propose the solution in collaboration with operators.

Finally, this methodology can still be attacked and circumvented, but we are as of yet unsure whether these attacks are realistic and possible. We are currently investigating these possibilities and further mitigation means.

References

[1] France24, "France summons us ambassador over unacceptable spying," June 2015, http://www.france24.com/en/20150624-france-summons-us-ambassador-wikileaks-unacceptable-spying, Retrieved 02/07/2015.

[2] Y. Uutiset, "Ficora: No evidence of fake mobile phone stations," December 2014, http://yle.fi/uutiset/ficora_no_evidence_of_fake_mobile_phone_stations, Retrieved 23/04/2015.

[3] W. Kim Zetter, "Hacker spoofs cell phone tower to intercept calls," July 2010, http://www.wired.com/2010/07/intercepting-cell-phone-calls/, Retrieved 23/04/2015.

[4] A. B. Foss, P. A. Johansen, and F. Hager-Thoresen, "Secret surveillance of norways leaders detected," December 2014, http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html, Retrieved 23/04/2015.

[5] K. J. Higgins, "Researcher intercepts gsm cell phones during defcon demo," July 2010, http://www.darkreading.com/attacks-breaches/researcher-intercepts-gsm-cell-phones-during-defcon-demo/d/d-id/1134099?, Retrieved 23/04/2015.

[6] F. Joachim and B. R. (Rohde & Schwarz), "Method for identifying a mobile phone user or for eavesdropping on outgoing calls," 2003, patent EP1051053 (A2).

[7] 3GPP, "3gpp ts 55.205: Specification of the gsm-milenage algorithms: An example algorithm set for the gsm authentication and key generation functions a3 and a8," 2014, http://www.3gpp.org/DynaReport/55205.htm.

[8] A. Police, "Testing t-mobile's free roaming data and how $50 gets you so much more," March 2014, http://www.androidcentral.com/testing-t-mobiles-free-roaming-data-and-how-50-gets-you-so-much-more, Retrieved 02/07/2015.

[9] I. Androulidakis, "Using a gsm tester to intercept calls and sms," January 2015, http://www.twelvesec.com/using-gsm-tester-intercept-calls-sms-pt1/, Retrieved 23/04/2015.

[10] "Osmocom openbsc project," http://openbsc.osmocom.org/trac/.

[11] R. Anderson, "A5 (was: Hacking digital phones)," June 17th 1994, newsgroup: uk.telecom. Usenet: 2ts9a0$95r @lyra.csx.cam.ac.uk.

[12] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of gsm encrypted communication," in *Advances in Cryptology - CRYPTO 2003*, ser. Lecture Notes in Computer Science, D. Boneh, Ed. Springer Berlin Heidelberg, 2003, vol. 2729, pp. 600–616.

[13] Slashdot, "Nsa able to crack a5/1 cellphone crypto," December 2013, http://yro.slashdot.org/story/13/12/14/0148251/nsa-able-to-crack-a51-cellphone-crypto, Retrieved 23/04/2015.

[14] D. Storm, "Are your calls being intercepted? 17 fake cell towers discovered in one month," September 2014, http://www.computerworld.com/article/2600348/mobile-security/are-your-calls-being-intercepted-17-fake-cell-towers-discovered-in-one-month.html, Retrieved 23/04/2015.

[15] S. Puzankov and D. K. (Positive Technology), "Cell phone tapping: How it is done and will anybody protect the subscribers," August 2014, http://blog.ptsecurity.com/2014/08/cell-phone-tapping-how-it-is-done-and.html.

[16] "Sonera network coverage (finland)," http://www.sonera.fi/etsi+apua+ja+tukea/verkkokartat/peittoaluekartta/.

[17] "Elisa network coverage (finland)," https://elisa.fi/kuuluvuus/.

[18] "Dna network coverage (finland)," http://opensignal.com/networks/suomi/dna-kattavuus.

[19] D. Campbell, "The embassy spy centre network," 2015, http://www.duncancampbell.org/content/embassy-spy-centre-network, Retrieved 02/07/2015.

[20] SRLabs, "Snoopsnitch," December 2014, https://opensource.srlabs.de/projects/snoopsnitch, Retrieved 23/04/2015.

[21] SecUpwN, "Android imsi catcher," December 2014, http://secupwn.github.io/Android-IMSI-Catcher-Detector/, Retrieved 23/04/2015.

[22] S. Udar and R. Borgaonkar, "Darshak framework and application," 2014, https://github.com/darshakframework/darshak, Retrieved 02/07/2015.

[23] O. Tirkkonen, "S-72.2205 digital transmission methods," 2015, aalto University, Department of Communications and Networking, https://noppa.aalto.fi/noppa/kurssi/s-72.2205/etusivu.

[24] A. Dowhuszko and J. Hämäläinen, "S72.3216 radio communication systems i (5 cr)," 2013, department of Communications and Networking, Aalto University, https://noppa.aalto.fi/noppa/kurssi/s-72.3216/etusivu.

[25] J. Hämäläinen, "S72.3226 radio communication systems 2 (5 cr)," 2014, department of Communications and Networking, Aalto University, https://noppa.aalto.fi/noppa/kurssi/s-72.3226/luennot/S-72_3226_lecture_2_material.pdf.

[26] Y. Song, K. Zhou, and X. Chen, "Fake bts attacks of gsm system on software radio platform," *Journal of Networks*, vol. 7, no. 2, pp. 275–281, 2012.