Detection and Mitigation methodology for Fake Base Stations Detection on 3G / 2G Cellular Networks.

Dare Solomon Abodunrin

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 27.7.2015

Thesis supervisor:

Prof. Jyri Hämäläinen

Thesis advisor:

D.Sc. (Tech.) Yoan Miche

Aalto University
School of Electrical
Engineering

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Dare Solomon Abodunrin

Title: Detection and Mitigation methodology for Fake Base Stations Detection on 3G / 2G Cellular Networks.

Date: 27.7.2015 Language: English Number of pages: 10+60

Department of Communication and Networking

Professorship: Radio Communications

Supervisor: Prof. Jyri Hämäläinen

Advisor: D.Sc. (Tech.) Yoan Miche

Development in technology is rapid, and same can be said particularly in the telecommunication industry, which has experienced an explosive growth both in the massive adoption rate of smart mobile devices and in the huge volume of data traffic generated daily in the recent time. Mobile devices have become extremely smart and used for purposes other than making calls and text messages, making it become an integral part of everyday human life. But while we celebrate this technological achievement, attacks on them have also increasingly become alarming such that our sensitive data transported over the wireless network are not only unsafe, but can easily be illegally requested for by an unauthorized device, also participating invisibly in the network.

We briefly studied the security features available in different generations of mobile communication technologies i.e 2G, 3G, and 4G, with the aim of understanding how fake base station attacks practically occur, and to understand the effect of exposing certain parameters such as IMEI/IMSI, LAC/CID to a third party, usually an intruder.

This work focuses on proposing a detection methodology as a mitigating approach to lessen fake base station attack in a cellular network. A fake base station is an attacking equipment solely used to duplicate a legitimate base station. While we acknowledge that the strategy of attack depends on the type of network, our approach is based on finding dissimilarities in parameters such as the received signal strengths, and existence of base stations participating in a network, from two different database systems. With this set of information, it is possible to arrive at a conclusion to state if a transmitting device is suspicious or legitimate. We present our detecting and mitigating algorithm which is the objective of this work.

Keywords: Fake base station, Signal Strength, LAC/CID, IMEI/IMSI, Base station (BS).

Acknowledgement

Dr. Yoan Miche, how do I even begin? Many thanks, first for accepting to supervise and instruct my work, and for the tireless effort and time you dedicated to reading and re-reading on several occasions as my writing demand. I sometime wonder how you are able to spot those little mistakes that I subconsciously ignore, amid your own busy schedule. Secondly, for the motivation and professional push to learn and do more. There are countless examples of this to cite, but I will just keep it simple:

Thanks Yoan for bringing a balance to my work; professionalism and social wise.

My sincere gratitude goes to **Professor Jyri Hämäläinen**, the Dean of Aalto University School of Electrical Engineering, for his overall guidance and supervision of this thesis work. This also extend to the lessons you have directly taught, and not just within the school walls, but through various exemplary acts, particularly your attentiveness and availability when needed.

I say a very big thank you for making this dream materialize.

This work was done in Nokia Solutions and Network, in the Technology and Innovation Unit, hence, my gratitude to every member of the team, particularly **Gabriel Waller** for everything. It really helps to have a friendly and supportive working environment.

I am glad and honored to have worked with you all.

And finally to **Finland**, for giving me a first rate University education without asking for a penny!

Otaniemi, 01.7.2015

Abodunrin Dare S.

Dedication

To Emma Viitanen,

For the love and support in countless ways, and motivation through it all: especially my disappearances into studies, writing, meditation, and many other unprintable things. Thanks for staying reliable and matured.

My jewel.

To Adetutu and Kemi Abodunrin,

For the sacrifices and unrelenting effort. For the genuine love and care right from my formative years, and till now. I am so honored to have you as my family. Thanks for shaping me up and putting me in the right direction.

We win!

To friends

For putting up with me, and for the encouragement during these years.

Contents

List of Abbreviations

1G	1st Generation
2G	2nd Generation
3G	3rd Generation
4G	4th Generation
3GPP	3rd Generation Partnership Project
AIMSICD	Android IMSI-Catcher Detector
AK	Anonymity Key
AS	Access Stratum
AuC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vector
BCCH	Broadcast Control Channel
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CID	Cell Identity
CK	Confidentiality Key
DL	DownLink
EPS-AKA	Evolved Packet System-Authentication and Key Agreement
eNodeB	Evolved NodeB
GSM	Global Systems for Mobile
GPS	Global Positioning System
GPRS	General Packet Radio Service
HLR	Home Location Register
HE	Home Equipment
ID	Identity
IK	Integrity Key
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
KASME	Key for Access Security Management Entity
KC	Cipher Key
LAC	Local Area Code
LTE	Long Term Evolution
MAC	Message Access Code
MAC-I	Message Authentication Code for Integrity
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
MOB-SCN-REQ	Mobile-Scanning interval-Request

MOB-SCN-REQ	Mobile-Scanning interval-Response
MS	Mobile Station
MSC	Mobile Station Controller
MT	Mobile Terminal
NAS	Non-Access Stratum
NAS-MAC	Non-Access Stratum-Message Authentication Code
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAND	Random Challenge
RES	User Response
RRC	Radio Resource Control
RNC	Radio Network Controller
RSS	Received Signal Strength
SD-CARD	Secure Digital-CARD
SMS	Short Message Service
SN	Serving Network
SNid	Serving Network Identity
SIM	Subscriber Identity Module
SQLite	Relational database management system
SQNms	Sequence Number for mobile station
SS7	Signaling System 7
SRES	Signed Response
TE	Terminal Equipment
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UL	UpLink
UMTS	Universal Mobile Telecommunications System
USIM	User Services Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VLR	Visitor Location Register
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WIMAX	Worldwide Inter-Operability for Microwave Access
XMAC	Expected MAC
XMAC-I	Expected MAC used for data integrity of signaling messages
XNAS-MAC	Message authentication code calculated by MME
XRES	Expected user Response

List of Figures

1 Introduction

1.1 Overview and Motivation

A large number of publications in recent times have increasingly sensitized us to the dangers surrounding wireless communication channels and how data transported over them have constantly been spied on [27] and used for some purposes unknown to the rightful owners: A term referred to as unilateral surveillance [48]. As this form of surveillance is rapidly becoming a norm and almost unstoppable [13], it has rendered the constant effort and energy of security inclined organizations i.e. Information and Infrastructure security companies and engineers, put into trying to curb them or streamline into positive [1] use only almost unrecognizable and, or under-acknowledged.

In relation to the mobile telecommunication industry, network vulnerabilities have always been a major concern for the mobile operators [50], but have also increasingly become an important issue to the end users especially since the intervention of those termed as "security whistle blowers" in attempts to create awareness on privacy intrusion of data; a reference to the Snowden case [68]. This as a result, has influenced two different levels of curiosity among the mobile technology users: the majority that are concerned about the exposure of their sensitive data during communication, and the others, attackers who are also concerned but also want to gain access to unauthorized data for exploitation. However these two categories are interpreted, both revolve around data, and while there are ongoing research work for its protection, series of methods are also being devised [9] for its capture.

The use of fake base station is one of such. A fairly new and growing method that is set up to monitor and gain access to network data traffic between two end points, the user and the mobile operator. This specifically is what this work centers around, to propose a methodology that can identify them when present in a network. My proposition in terms of work done in this project is to mitigate the effect of such entity. From a less technical perspective, communication can be defined basically as an interaction between the Base Stations (henceforth, BS) and the Mobile Stations (henceforth, MS). A Fake BS according to [57] is an equipment located in restricted area to act as a real BS by broadcasting signals over air in attempts to lure mobile devices around to connect to it. Since fake base stations are dynamic in nature, meaning that their precise location in the network is difficult to determine or track, it empowers them to outsmart target devices by obtaining all possible IMSIs (International Mobile Subscriber Identity) within range, after forcing a downgrade (illustrated in figure 1) on user equipment to a communication network where weaker security mechanisms and encryption are used.

[1] for monitoring possible attacks or business growth predictions e.t.c

1.2 State of the art

Recent study has shown an increasing attack rate [11] against our mobile devices and has triggered many security responses over the years. The 3GPP standardization team [2] is one body that has constantly been involved in the creation of standardization documents which help to adequately define needs, fixes, monitor implementations and development, and the maintenance of these standards. Many other security enthusiasts have also contributed tremendously but with more focus on either stretching discussion on the existence of fake BS and how it works, or through practical implementation of a similar form of attack simply to showcase the weaknesses of the GSM security architecture, all of which serves as a good foundation on which this work is built. This is evident in the summary of selected list of publications (see chapter 3) chosen for review as we will later discuss.

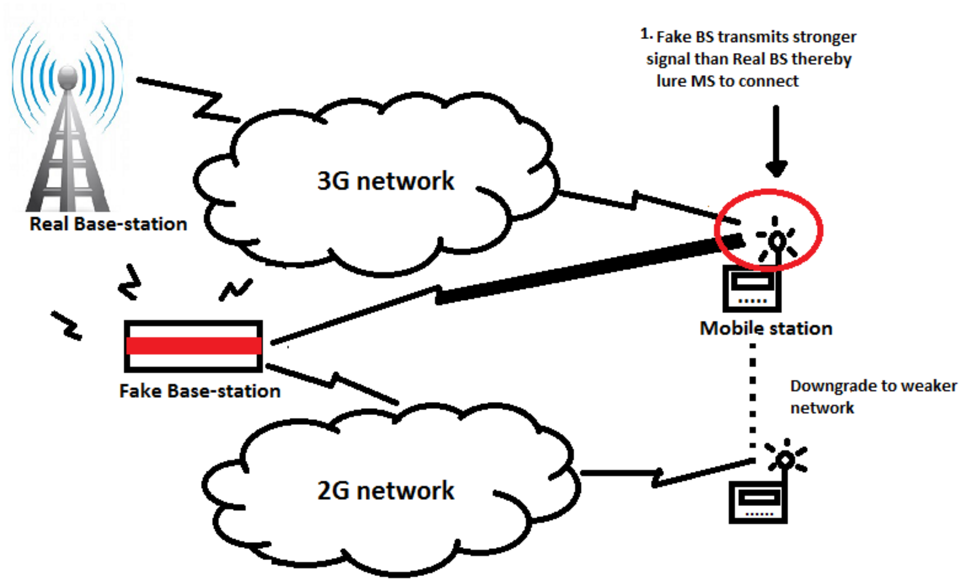
1. Fake BS transmits stronger signal than Real BS thereby lure MS to connect
Real Base-station
3G network
Mobile station
Fake Base-station
Downgrade to weaker network
2G network

Figure 1: Fake base station forcing a downgrade on mobile device: initial communication was via 3G but was tricked into communicating through 2G where it is easier to penetrate.

1.3 Research methodology

Unlike most of the previous research works, the methodology embraced here is built on the reasoning that it is only after the mobile operator is able to detect an attacker (impersonating real base station) that a complete defense mechanism can be implemented. What this translates into is that a potential fake base station should be detectable by the operator, and then probably send an alert message to the user's mobile device, while an immediate counter response is instantaneously launched

[2] http://www.3gpp.org/

together with the already available security protocols implemented to render such attacks useless, known, and predictable in future occurrence.

To achieve this, some useful captured network parameters, that is constituted by all participating devices, should be made available for an extensive study before subjecting them to a comparative analysis to solidify the above approach. However, different cases are considered in this work to ensure detailed coverage of relevant and possible scenarios, all of which depend on how the attacking equipment is set up as would later be discussed.

1.4 Thesis outline

- Chapter 2 centers on the security implementations and how protocols are established between mobile device and the operator network during communication, in these selected mobile technologies. However, the omission of certain technologies, especially before 2G is intentional, and this is because security implementation in them is not accessible to the public, or there is no security implementation at all except in their core networks.

- Chapter 3 summarizes selected work done till date relating to fake base station and wireless security issues in general. The section begins by first establishing distinctions between genuine and fake base stations, before delving into the main discussion of what has been done.

- Chapter 4 introduces the practical measurement approach we gave this work which is carried out in an attempt to be able to detect abnormalities through comparison of two data set; one achieved from our measurement, and the other from operator. The chapter ends with a summary of our observations from the gathered data analysis and manual inspection.

- Chapter 5 presents the main work of this project, which is the detection and mitigation of false base station as the title reads. A detailed discussion on the cases considered, possible scenarios, short comings and assumptions made leading to the proposed methodology are presented in this chapter.

It is however good to note ahead that some words are used synonymously in this work, such as; false BTS, fake BTS, rogue BTS, to mean same. This should not be mis-interpreted or cause confusion to mean something different, other than an attacking device.

2 Security Evolution in Mobile Communication Technologies

Wireless communication is defined as the transfer of information from one location to another regardless of the distance between, without the use of cables[3] [28]. Unlike in wired communication where data transportation relies on cables, making it less difficult to trace attacks done through wiretapping since this requires physical intervention. In wireless communication the story is different, and this is because the transmission medium for data is air, through radio frequency propagation. This means that an attacker does not need to be physically involved with or be around its target before carrying out for instance a passive probing [42] attack on the radio path, or perform some other form of attacks as described in [40].

The cellular network implementation did not start with the 2G technology [26, 66], it only started gaining popularity as the technology became cheaper and accessible to users [45] by bringing features that aid communication. Although other peculiar reasons such as unavailability of a unified standardization body and proper documentation, specifically in 1G, can be attributed to some of its undermined nature such as: poor sound quality, frequent ongoing call drop, and issues with security [46]. Before 2G, existing telephony technologies[4] offered almost entirely voice communication services [39] but with some limitations as already mentioned. Those limitations got more attention and were improved in subsequent technologies, starting with the 2G [29], where the switch from analog to digital system became a reality. With digital communication [64], more advanced techniques became available such as source coding which helps to efficiently use the scarce radio spectrum [18], while interference and fading can also be reduced by using error correction coding techniques [16], eventually translating into low power transmission.

Figure 2 shows the success of 2G and subsequent releases[5] as it became widely adopted and still in use. Some of the many reasons attributed to this success come with the improvement in sound quality where talking became clearer, provision of better data service (comparison to 1G), and most importantly the introduction of standardization bodies to govern its development [45]. But even with all these, protection over the communication path between mobile devices and their serving network was still an issue. According to [46], lack of cryptographic protection in 2G systems exposed the vulnerability of sensitive control data i.e. the key used for radio interface ciphering becomes vulnerable when subjected to brute force attacks[6]. In other words, while 2G overcame certain limitations of the previous technologies, its radio link connection to an external device in the mobile equipment module, and

[3] Twisted-pair, co-axial, fibre-optics [67]

[4] 1G

[5] 2.5G, 2.75G.

[6] systematically checking all possible keys or passwords until the correct one is found [37].

a few other factors[7] needed to be improved. This motivated the move for better security and mobility implementation in the next generation.

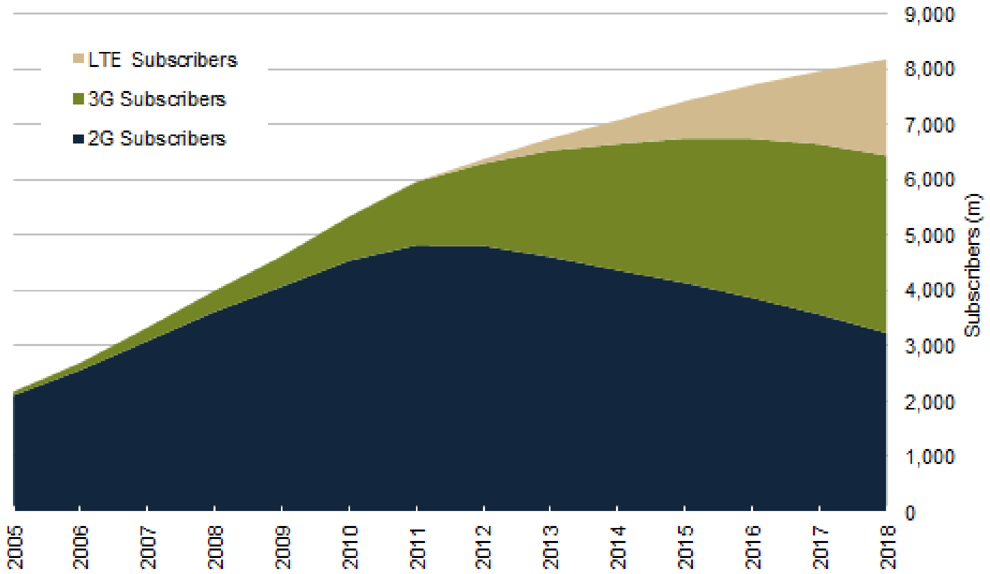

Figure 2: 2G's success and adoption over the years (From [63]): figure illustrates both its rise before the introduction of newer technologies and decline from year 2013.

According to [6], the third generation of mobile networks is designed to fix inherited weaknesses from earlier technologies and to offer stronger security features over the entire network. It is the standard that revolutionized the mobile industry, enabling network operators to offer subscribers better and newer services. These services [35] include the long planned smooth mobility, multimedia services [19], possibility to access e-mail, perform online bank transactions, and unlimited network connection on mobile devices irrespective of the device mode[8] or location. However, with this new set of features, daily network traffic management became the new problem, while attacks on 3G networks decreases because of the strong 2-way authentication security protocol (see section 2.2 for details) implemented to establish trust between serving network and mobile device [28, 46]. The success of this technology as shown in figure 3 is measured by its increasing global adoption rate over the years.

The latest of these standards of mobile communication technologies is the 4G. Its objective [21, 36] is to meet the exhaustive bandwidth usage that is rapidly increasing due to the enormous use of smart mobile devices, generating massive traffic as devices have become smarter and highly feature equipped. Logically, this implies that 4G inherited all the security properties implemented in earlier mobile

[7] active attack on the network, secrecy [46] in some part of the network architecture

[8] active or idle mode

technologies[9], mostly 3G, and even got improved[10] as a way of complementing initial set objectives [20].

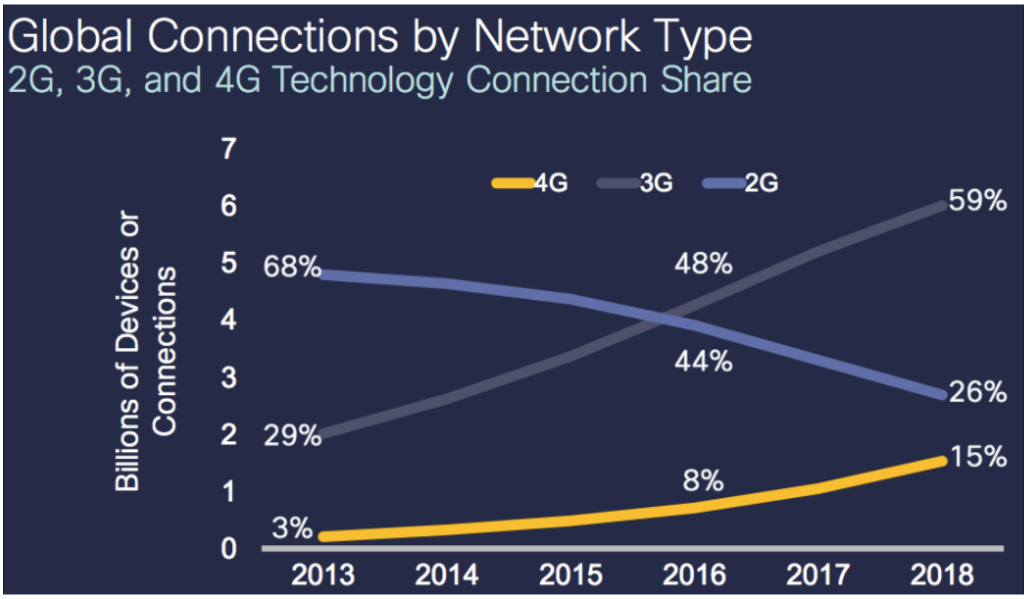

Figure 3: 3G network global acceptance over the years (From [61]): a rise in 3G devices and connections measured in billions, causes decline in 2G while 4G slowly rise.

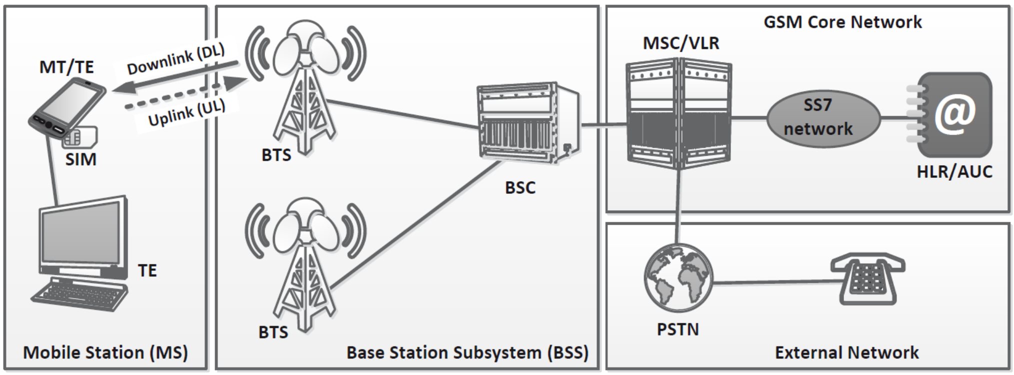

Figure 4: 2G Network Architecture.

2.1 2G Authentication and Encryption

Like every other wireless technologies, 2G (popularly referred to as GSM) suffers the risks of being susceptible to attackers either: during transmission session done

[9] 3.5G, 3.75G.

[10] Long Term Evolution

through the radio link between mobile devices and serving network, or in idle state [43]. While 2G is rapidly becoming less significant in the current mobile technological trend [12], it is still the most suitable network to launch fake base station attacks since it possess weak and hackable [47] security architecture. An overview of the GSM system architecture is given in figure 4 to show how components are inter-connected.

However, the two major security features [4, 62] introduced to mitigate risks in 2G are:

1. User authentication
2. Encryption of user traffic.

The system depicted in figure 4 comprises many network elements but is technically separated into three functional units [32]: the Mobile Station, the Base Station Subsystem, and the GSM Core Network.

- Mobile Station (MS):
  This unit represents a collection of various equipments [11] used by the subscriber for communication purposes through the network. One very important but small-sized physical component present in the mobile station is the SIM card: **S**ubscriber **I**dentity **M**odule. It holds vital information [12] about the user, and also participates in the user authentication process by providing some useful parameters (see section 2.1.1) as we shall see in the discussion relating to confidentiality [45] in the next subsection.

- Base Station Subsystem:
  Mobile Station is not designed to talk directly with the core network, for this reason it needs an intermediary which is the BSS. BSS consists of group of infrastructure machines [13] that are responsible for the cellular aspect of GSM. One of its functionality includes transmission and reception on the radio path and its management after.

  A reference to figure 4 indicates that this module contains two main elements and they are;

  - BTS (Base Transceiver Station): This is the element in the BSS module that interacts directly with the mobile devices through the available radio interface, and its primary functionality revolves around transmission between mobile device and the network [45].
  - BSC (Base Station Controller) is responsible for handling the traffic and signaling between mobile station and network switching subsystem. In functionality terms, this is the managing equipment which work includes:

[11] vehicle-mounted, portable devices and hand held mobile devices [45]

[12] such as: IMSI (International Mobile Subscriber Identity), subscriber's telephone directory, encryption codes [3]

[13] Base transceiver station, base station controller

allocation of radio channels, measurements received from mobile devices, and handover control between BTSs [45].

- GSM Core Network:
  This is the backbone of the whole network where functionalities such as mobility management, switching of roaming calls, and the data hub of the network is situated. Its main role is to manage communication between users in its own network and other networks. It comprises of network elements such as;
  - **MSC** (Mobile services Switching Centers): This controls several BSCs connected to it, and performs the switching of calls between the mobile and other mobile network users, as well as the management of mobile services[14]. MSC also performs functions such as network interfacing, toll ticketing, and common channel signaling.
  - **VLR** (Visitors Location Register): This is a temporary database that holds roaming user information that MSC uses to service them.
  - **HLR** (Home Location Register): This is the container for the permanent storage of subscriber specific parameters, location area code, and many more.
  - **AuC** (Authentication Center): This is also a form of database which contains a copy of secret keys used for user authentication to the network.

Breaking the network into three distinct units gives the opportunity to clearly identify each segment of the network during the authentication process analysis, and also note their contributions. This way, the authentication procedure explanation between the mobile device and the network as described in the following algorithm can be better understood using this sequence diagram of figure 5.

2.1.1 User Authentication in 2G

Authentication in GSM systems is one-way [59], and it is performed by the serving network to strengthen the network security both by identifying the device trying to connect to it and generating an encryption key [62] that is used to protect user data during transfer. However, pre-authentication condition [34, 44] necessitate that both the mobile device and the authentication center must already have a secret permanent key, denoted as Ki, created and stored in them (refer to fgure 4 to see where these two are located). This key is stored in the SIM card (see section 2.1) and must be kept safe and secret to just the device.

User authentication algorithm:

1. User starts by sending its unique identity, IMSI[15], to VLR.

[14] registration, authentication, location updating, handovers, and call routing to a roaming subscriber.

[15] Every mobile device in a network has this

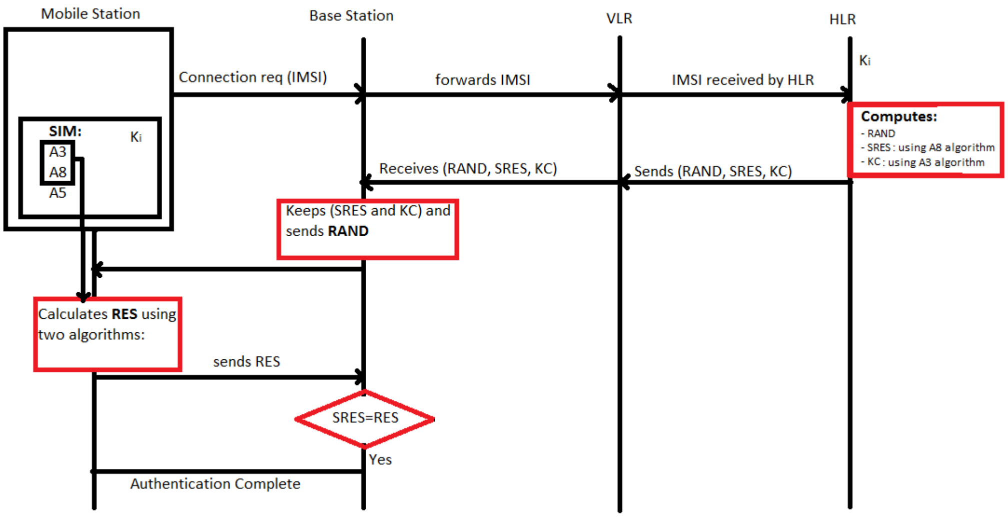

Figure 5: GSM Authentication sequence diagram showing how the process unfolds between these entities.

2. Since VLR can not decide to authenticate user on its own, it passes this information to the HLR to notify the network of 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. 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. 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.

2.1.2 2G data traffic encryption

In figure 4, we observe the need to secure the radio path between the base station and the mobile station. It is not just enough to be able to identify the connecting device, but also to secure the transmission path so that the data in transit is protected from a malicious attacker. As we shall present and discuss in chapter 4, some attacks pass through the weak authentication [15] challenge-response protocol in GSM or act as a form of man in the middle attack thereby intercepting communication in order to gain access to unauthorized data.

According to [62], and figure 7, every SIM card has a secret key Ki, when used with the A8 algorithm [34] generates a cipher key, Kc. The combination of both A5 algorithm and Kc as depicted in figure 6, becomes the tool to encrypt and decrypt data over the radio path between mobile device and base station. Generally, A5 is the known algorithm used in 2G to protect the radio path and it comes in two variants: A5/1 and A5/2. The first variant of the A5 algorithm is the european version which is known to be stronger than the second [34].

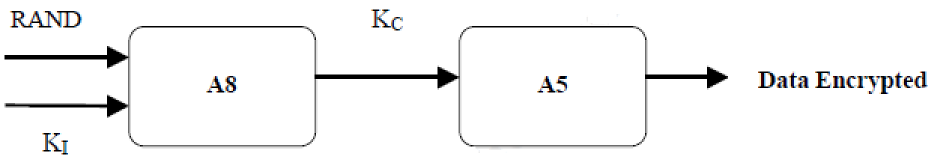

Figure 6: Encrypting data using a ciphering key.

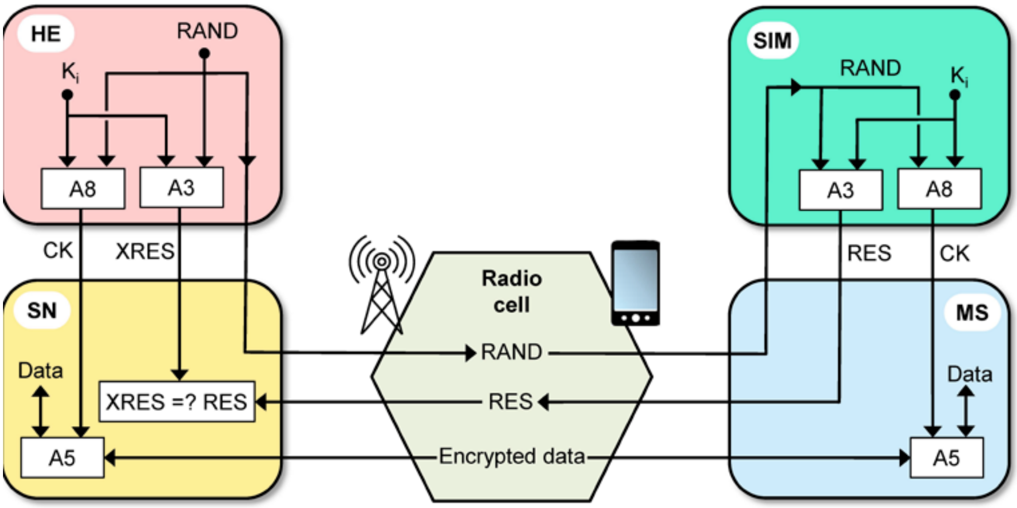

Figure 7: GSM Security Architecture (From [34]): colour indicates different sections of the GSM network element division and algorithms each implement during authentication and encryption processes.

2.2 3G Authentication and Encryption

While 2G already offered voice communication and some messaging features[16], 3G technology which is popularly known as UMTS, focused on provision of stronger

[16] SMS, GPRS, WAP [53]

security implementation than in earlier technologies while also offering both mobility in the true sense and better multimedia services [35, 46].

UMTS architecture, as depicted in figure 8, is similar to the GSM but with several modifications. The access network is referred to as Universal Terrestrial Radio Access Network (UTRAN) and comprises of two entities; several base stations known as NodeBs and Radio Network Controller (RNC). The Core Network however supports both packet and circuit switched connections, which are used for carrying other data [17] and voice services respectively [51].

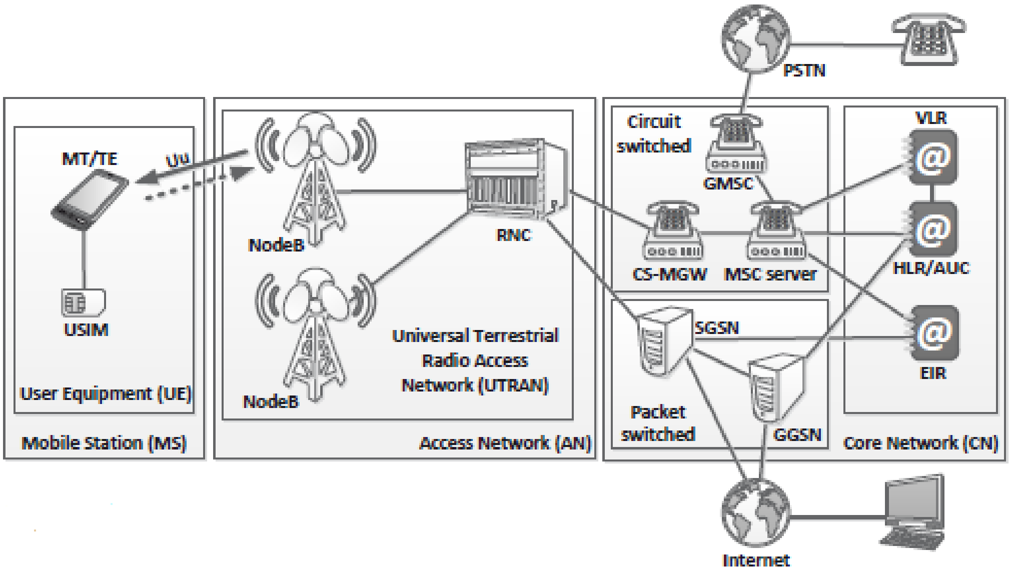

Figure 8: UMTS network architecture.

Since 3G is the modified version of previous technology, its security architecture retained the structure of 2G but with additional new set of cryptographic functions [18] to address inherited problems such as;

- unsecured radio path between mobile device and network
- unsecured sensitive data
- one sided network authentication

which means that the network security architecture, shown in figure 10 became more complex than in the previous technology. Similar to 2G, the whole system is divided into three units comprising the User equipment, serving network, and the home network.

[17] web browsing through HTTP, and file download / upload through FTP.

[18] cryptographic functions: f0, f1, f2, f3, f4, f5, f8, f9 [5]

2.2.1 User Authentication in 3G

Unlike in 2G where only the network gets permission to ask for authentication, mobile devices are also empowered to challenge the network to authenticate itself. Meaning that the inherited one-way authentication method is dropped, and a new two-way authentication method is implemented in 3G as the following algorithm describes. However, initial condition is that USIM[19] must contain a secret key, Ki [34]. Refer to figure 9 to view user authentication sequence diagram.

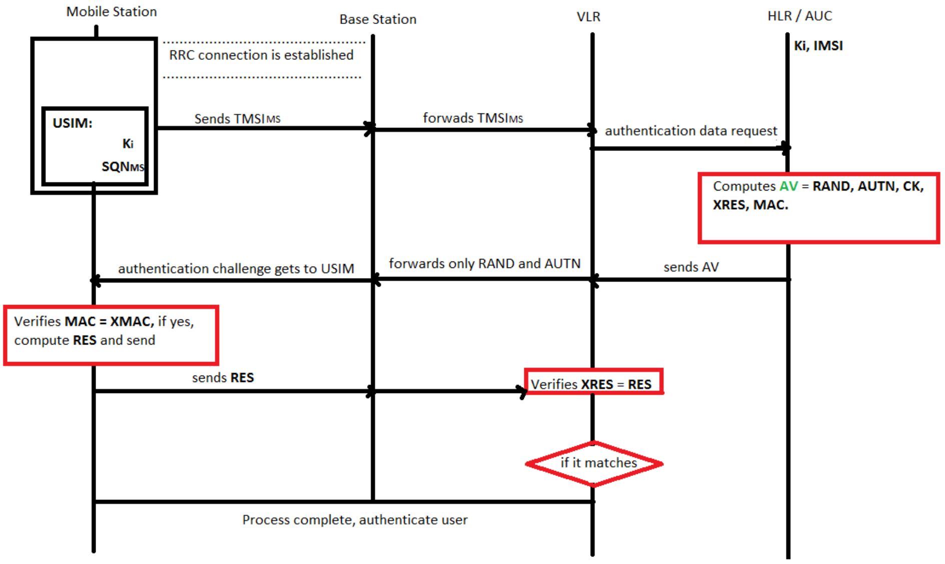
Mobile Station
Base Station
VLR
HLR / AUC
Ki, IMSI
RRC connection is established
USIM:
Ki
SQNMS
Sends TMSIMS
forwads TMSIMS
authentication data request
Computes AV = RAND, AUTN, CK, XRES, MAC.
authentication challenge gets to USIM
forwards only RAND and AUTN
sends AV
Verifies MAC = XMAC, if yes, compute RES and send
sends RES
Verifies XRES = RES
if it matches
Process complete, authenticate user

Figure 9: UMTS authentication sequence diagram indicating how the process is established and the interactions between network entities.

The following describes user authentication procedure as it is done in 3G:

1. Firstly, an RRC connection (Radio resource Control) [52] is established between the Mobile device and network. This signals the beginning of a session, while MS uses it as an opportunity to send its security capabilities to the base station.

2. User's device send its TMSI[20] through the base station to the network.

3. Serving network then sends a request for authentication data from the home network.

4. Mobile's home network as a response generates a set of authentication vectors which includes random challenge: denoted as RAND, expected response: denoted as XRES, an authentication token: denoted as AUTN, encryption and integrity keys: CK and IK respectively.

[19] A smart card inserted into the mobile device

[20] will be requested to send its IMSI only if the network is unable to resolve its TMSI

5. Serving network keeps both generated keys and expected response from the network, sending only RAND and AUTN to the mobile device.

6. Mobile device's USIM verifies the received AUTN to check its genuity[21].

7. If valid, mobile device sends back its authentication response, denoted as RES, to the serving network.

8. As a security measure, serving base station also compares received response, RES, with XRES to check the correctness. If there is a match, then the authentication phase is successful.

An important step to note in the above process is the part where mobile device also verifies the AUTN in order to confirm its genuity. If for instance after verification the token was confirmed faulty, mobile device will discard the message giving it the power to also verify if the serving network is genuine or not from the home network.

2.2.2 Encryption of user traffic in 3G

Mutual authentication is a fraction of the needed security measure for protecting the whole mobile communication networks. While this mechanism is successful at verifying authentication conformity of participating network elements, it is not designed to cover the radio path security, which is a very crucial aspect of any wireless communication network. The encryption mechanism implementation in 3G serves this purpose.

Traffic encryption revolves around CK and IK [46]. In reality, radio link itself can not be fully protected from external attacks, meaning that attackers can tamper with the path but transferred data can be protected from getting hijacked by an eavesdropper. According to [55], the cryptographic function responsible for user data confidentiality is f8, while f9 is responsible for the protection of user data integrity in UMTS, both based on the KASUMI [38] algorithm. With the aid of figure 10, UMTS confidentiality encryption algorithm is described as follows:

1. f8 algorithm in the user's device computes an output bit stream using CK transferred to it by USIM.

2. This output bit stream is XORed[22] bit by bit with the data stream, also known as plaintext to obtain ciphertext.

3. Ciphertext is sent to the network through radio link.

4. The f8 algorithm in RNC [23] uses the same inputs as the user equipment, including the shared cipher key CK, to generate the same output bit stream that was computed in the user equipment.

[21] MAC must be equal to XMAC otherwise, it is not accepted

[22] mathematical approach

[23] Radio Network Controller [41]

5. The output bit stream is XORed with the ciphertext received to recover the initial information.

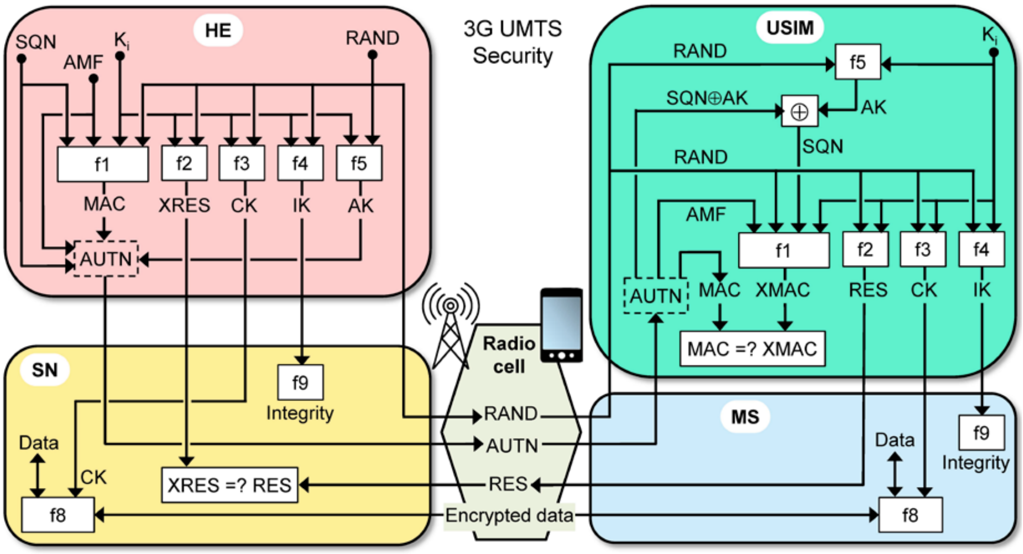

Figure 10: UMTS Security Architecture (From [34]): different colours to indicate different sections of the UMTS network element and algorithm implementation during authentication and encryption processes.

2.3 4G Authentication and Encryption

4G is the current state of mobile communication technology with two standards: WIMAX and the more popular LTE, developed to meet defined requirements for the present and future needs of mobile communication. Although the earlier discussed generations i.e. 2G and 3G are still the global dominating technologies in use, LTE was developed by 3GPP with strong consideration for security to mitigate observed limitations in earlier generations [8].

LTE major difference from others lie in the way its cryptographic protection is provided on many different layers and as such deviates from applying the usual fixed set of standardized module, as used in 2G and 3G, to having quite a number of choices of security functionalities to decide from [34]. Figure 11 and 12 below gives a glimpse of the LTE network and security architecture respectively.

2.3.1 Authentication procedure in 4G

Authentication is done between user equipment and the network using a procedure known as EPS-AKA. This procedure is built on the concept of mutual authentication, otherwise referred to as two-way authentication (see section 2.2.1) but with a slight difference in method. Aside the difference in cryptographic procedure and key hierarchy used, network is more involved [7] in handling the authentication procedure,

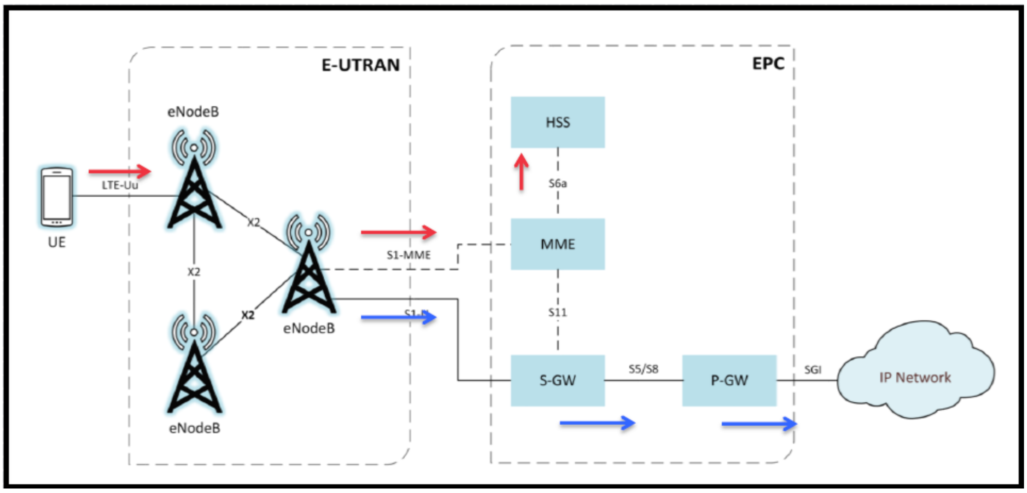

Figure 11: LTE network architecture.

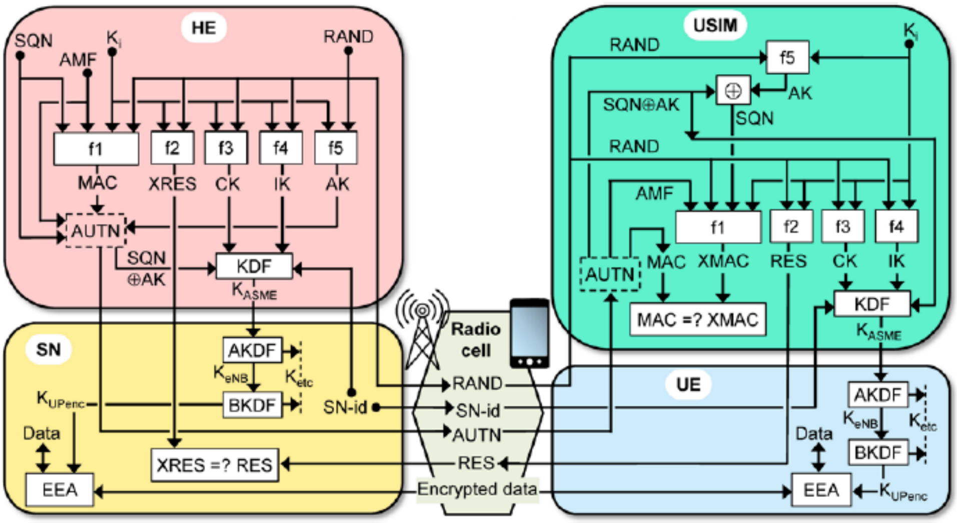

Figure 12: 4G Security Architecture (From [34]): colour code indicates different entities and the security functions they possess.

and 4G mobile station module uses USIM with more complexity than its predecessor. This is evident in the sequence diagram depicted in figure 13 and a narrative algorithm that follows:

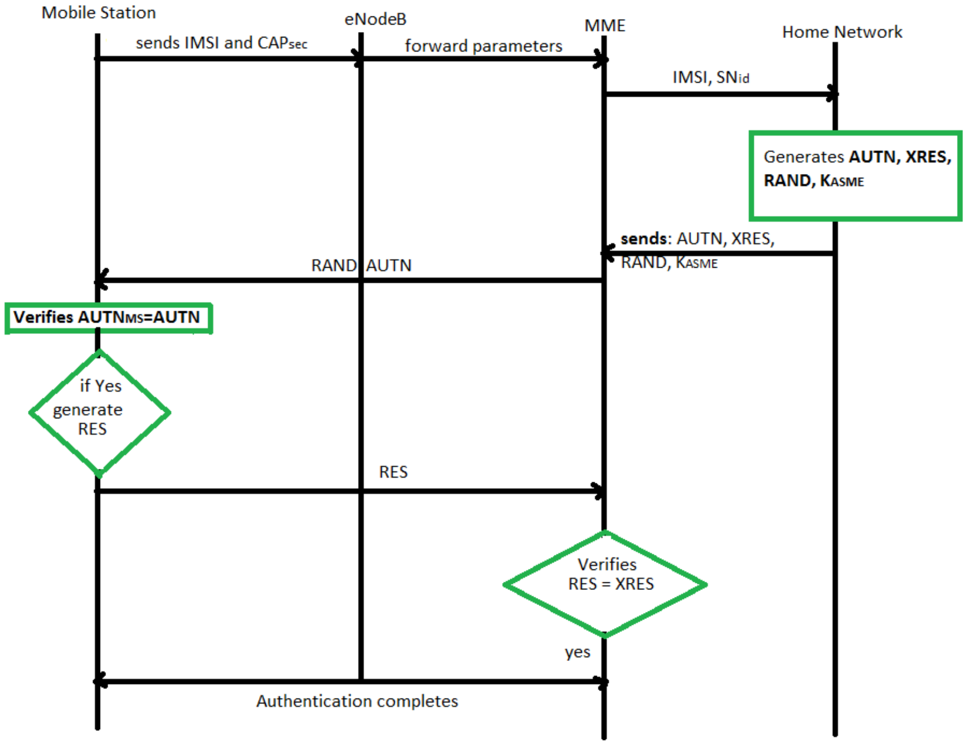

Figure 13: 4G Authenticaton sequence diagram showing entities interaction with one another and the order.

1. User device triggers connection request sending its TMSI and security capabilities to the serving network.

2. This attempt triggers the EPS-AKA authentication procedure. Serving network, starting with eNode forwards received parameters, i.e. IMSI, security capabilities, to MME.

3. MME attaches it own identity, SNid, and forwards both the user's device identifier, IMSI, and its own identity, SNid, to the home network.

4. Home network generates RAND, AUTN, XRES, and Kasme (access security management entity key) using EPS-AKA algorithm which it then sends back to MME.

5. MME stores received parameters from home network before selecting one of them for mutual authentication purpose and sends both RAND and AUTN to user's mobile.

6. Mobile device's USIM verifies the received AUTN to check its genuity. If this is genuine, then mobile device authenticates network and generates response which is sent to the MME through eNode.

7. MME compares to verify the correctness of received RES response from mobile with its own XRES i.e. XRES=RES. If it matches, it sends to the device KEYS which are used to protect NAS [24], while base station also derives and send key to protect AS as well as user data.

Through this procedure, both user device and network are authenticated. For clarity, MME is verified, or authenticated, by the home network when its SNid [25] was sent along with the user IMSI in the third step of the EPS-AKA procedure above.

2.3.2 Encryption of user data in 4G

Since mutual authentication is already established between device and network, it means that they both share same Kasme as an authentication key which is useful to encrypt user data during communication [24]. LTE uses two approaches to set up maximum data protection, and these are;

- **NAS Security:**
  This security deals with making sure that the signaling messages between user equipment and the MME over radio path is secured. It is mandatory in this procedure that the integrity check is performed, while ciphering is not [25].

  The procedure is as follows:

  1. MME selects ciphering and integrity algorithm to be used based on user device's security capabilities earlier sent during authentication. Also generates NAS-MAC (Message Access Code) for integrity. It sends this to user's device using Security Mode Command.
  2. User's device verifies parameters received through Security Mode Command for genuity. Meaning that it generates XNAS-MAC and compares it with NAS-MAC. User's equipment then encrypts response message: Security Mode Complete, using agreed encryption algorithm and then send to MME.
  3. MME decrypts and verifies the integrity of the Security Mode Complete message received from user. Once that is confirmed to be genuine, then the NAS set up is complete, meaning that messages sent after this can be encrypted and integrity protected.

- **AS Security:**
  Unlike in NAS, both integrity and cipher checks of RRC signaling messages

[24] Non-Access Stratum [33]

[25] Serving Network identity

and ciphering of IP packets are mandatory here. AS security ensures the secure delivery of data between user's device and MME [25].

The procedure is as follows:

1. eNodeB selects security algorithm i.e. ciphering and integrity algorithms, to use. It generates MAC-I and attaches this to Security Mode Command message which is forwards to user's device.
2. User's device verifies that the received MAC-I matches its own XMAC-I. If this matches, it then sends Security Mode Complete message to eNodeB.
3. eNodeB verifies the integrity of this message, and if it matches, all the RRC messages between user's device and eNodeB are integrity protected and encrypted, and all the IP packets are also encrypted before being sent.

While we already have established an understanding of the authentication and encryption methods used in 2G, 3G, and 4G respectively, the next chapter discusses limitations still present in these mobile networks and what has been proposed by researchers to mitigate against a specific type of attack, fake base station.

3 Fake Base Station: Summary till date

3.1 Describing Fake Base Station

To define what a fake base station is, one would also need to raise discussion on the non-fake, a legitimate base station, and the services it renders. This way, distinction between these two can therefore be identified as a way of establishing fake base station abnormalities which serves as the foundation for further work. According to [1], a base station is a network entity [26] responsible for serving one cell and ensuring connectivity between the subscribers in that cell and the core network. This means that a mobile device wishing to use the resources provided by a serving network must do so through a serving base station for that cell, and therefore exposes its sensitive data to the environment.

On the other hand, a fake base station [23] is a malicious station that acts as a legitimate one. For several reasons (see section 3.1.1), network subscribers are tricked into thinking the established connection and interaction is with a legitimate base station while unknowingly being exploited. Unlike a legitimate base station that has a fixed tower structure for broadcast [22], fake base stations are usually smaller and mobile [49] thereby making it possible to constantly change location in order to get closer to targets. This mobility characteristics makes it difficult to detect a fake base station when present in the network. Figure 14 shows three equipment [27] interacting while the fake base station transmits close to the mobile station.

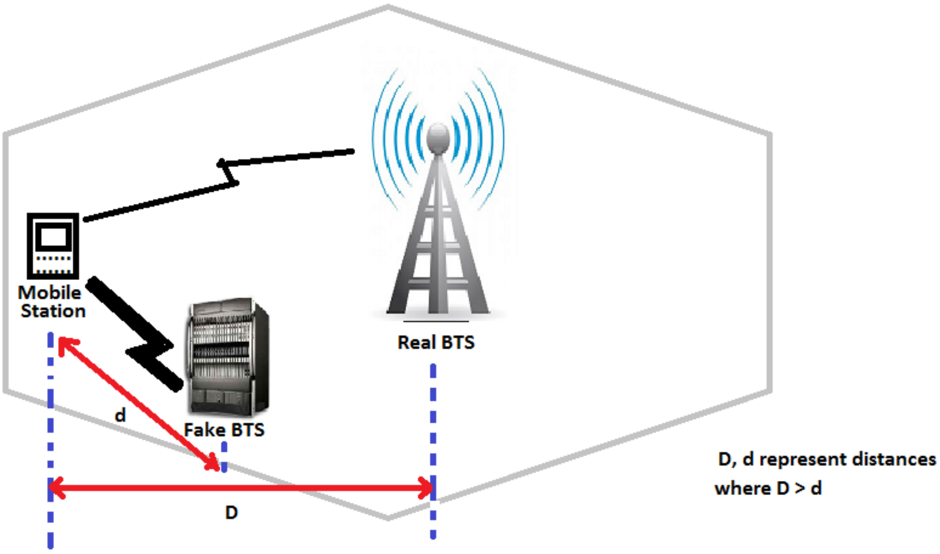

Figure 14: Fake base station transmitting to a mobile station at a close range.

[26] All the equipment that makes up a wireless/cellular network
[27] mobile device, legitimate base station, and fake base station

3.1.1 Possible attack scenarios

There are several types of attacks [2] a base station can possibly launch. While majority of these attacks are directed toward the mobile devices, some few are also launched at the core networks. Security implementations in the core network of standards like UMTS and LTE, i.e. 3G and 4G respectively (refer to section 2), are strongly designed to withstand the maneuvering tactics of a fake base station. But in 2G, the security design is weak against such attack making it the most ”friendly” network environment for fake base stations to operate. The type of attacks are classified as shown in figure 15 below followed by the description of each of these.

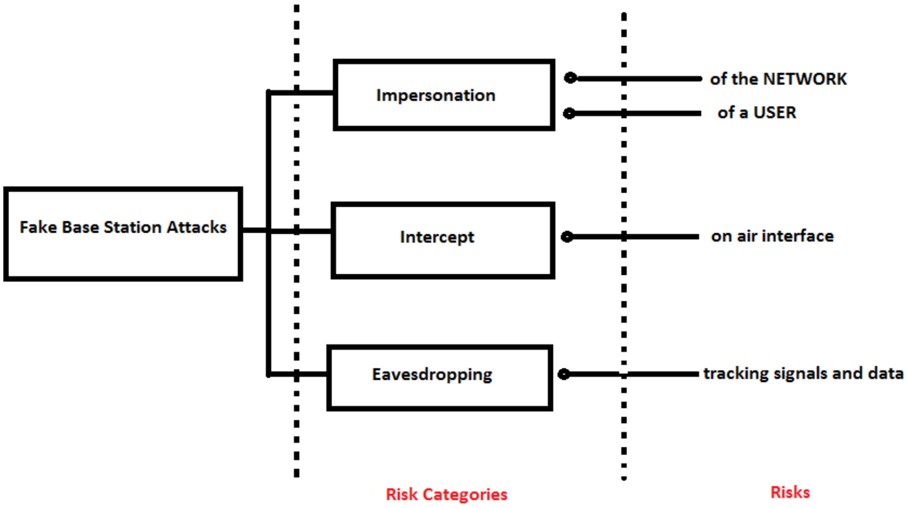

Figure 15: Classification of fake base station attack types.

- Impersonation:
  An intruder poses to be some other. It is the case of identity theft, and can be done in two ways. One is to hijack the mobile user’s identity through the use of complex attack phones and then starts communicating with the network, presenting itself like the rightful user [2]. This is called: **Impersonation of user**.

  The second technique deals with the intruder presenting itself as a legitimate network equipment authorized to communicate with the mobile users [2]. This is refered to as: **Impersonation of the Network**.

- Intercept:
  Interception is a form of a man in the middle attack where the attacker blocks the communication from the mobile device to the legitimate base station.

- Eavesdropping:
  This occurs when an intruder secretly listens to the conversation of others without having the right to do so. Although there are two types of eavesdropping:

Active and Passive, but when discussing fake base station attacks, attention is then more on the active. Reason being that a passive eavesdropper is not necessarily affecting the communication between sender and receiver [17], it monitors and listens, although could also be useful in carrying out attack [40]. The attacker in active may partially or fully know the texts being transported, however, it actively injects own message to translate the texts in session if partially unknown, or create decryption on the packages if text is known.

3.2 Proposed solutions and methodologies

Many research papers treating the fake base stations as a topic have been published over the years. Some of these publications not only identified the risks on mobile network securities, but also proposed some rectifications or solutions that deem fit to curb this growing fake base station attacks. We have chosen a few of these publications for summary as this would help identify the next direction and what could be done as a contribution to the fight against wireless network attacks.

3.2.1 Work on risks and detection of Fake base station

Mazroa and Arozullah [10] proposed a rogue base station identification protocol to protect the privacy of user equipment in the network. Their work is based on utilizing mobile properties captured during measurement in different locations, to estimate location and power of the base stations. The proposed protocol acts as a verifier that distinguishes genuine base station from fake. If the base station is confirmed or verified to be genuine, then user's equipment is allowed to connect to it.

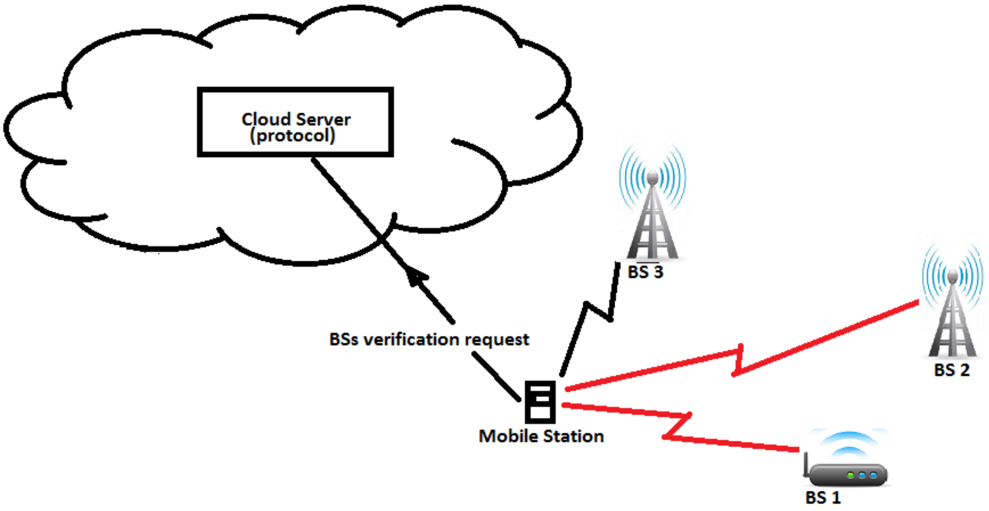

Figure 16: Proposed protocol for detecting false base station in [10].

Their solution relies on the decision of a cloud server which contains the list of real base stations for comparison purpose. So after the mobile station has measured surrounding base stations received signals, it sends these parameters to the cloud server for verification and waits for response. The logic behind these is the fact that a real base station transmission coverage area should be large while a fake one only covers small area [10]. Based on this, a fake base station can be identified. Figure 16 captures the verification procedure summarized above.

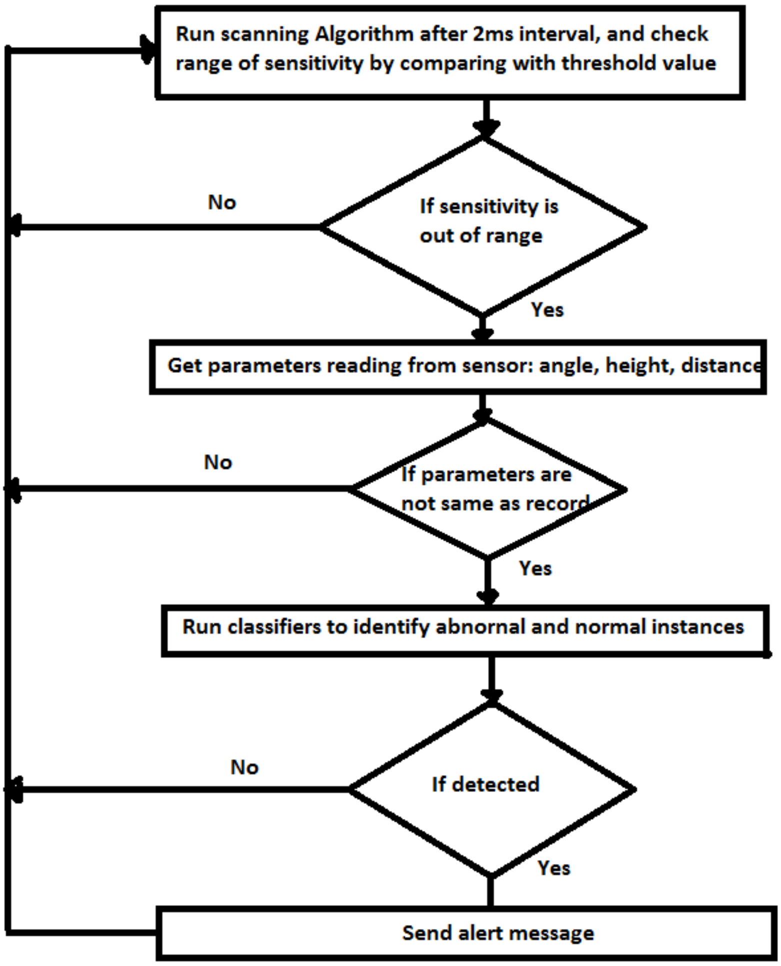
Run scanning Algorithm after 2ms interval, and check range of sensitivity by comparing with threshold value
No
If sensitivity is out of range
Yes
Get parameters reading from sensor: angle, height, distance
No
If parameters are not same as record
Yes
Run classifiers to identify abnornal and normal instances
No
If detected
Yes
Send alert message

Figure 17: Flowchart for rogue base station detection from [22].

Deepti and Khokhar [22] also worked on resolving the fake base station attack issues proposing a method built on the concept of dynamic threshold for calculating the sensitivity of base station and specific values to derive some attributes which aids in the decision making for detecting fake base stations. These attributes include; height, angle, and acceptable distance. Their proposed solution is a scanning algorithm which by the use of sensors check through the spectrum completely at every 2ms (time) for the sensitivity of base station. In order word, there must already be a defined threshold, calculated as the mean of collected sensitivity values in the last twenty-four hours, to represent the standard value by which newly measured values are compared. The sensors reading these values were given allowable error threshold of 0.1% to make decision accuracy flexible afterwards so that legitimate base stations are not mistakenly classified as fake. A work flow-chart, in figure 17, describes how the protocol procedure is performed.

In the work of **Song Y et al** [57], a software radio platform was developed and made to run a Base Transceiver Station protocol stack. This way it was possible to launch two types of attack: first one is an IMSI/IMEI catcher, while the second is a selective jamming attack. Main idea is that the developed system was able to transmit alongside other base stations, and user was able to connect to this fake base station under the condition that it appears to be in the BCCH allocation list of the AM3517 experiment kit [28] used for its design. Meaning that without the use of a jamming device, it is possible to trick mobile devices to connect to this fake Base station and then provide parameters such as IMSI/IMEI to the attacker.

The second proposed attack, a selective jamming protocol, implements a two way [29] decision approach to either block targeted mobile device or not. The first approach deals with manipulation of signal transmission power, making fake base station power higher than the legitimate therefore luring the mobile device, while second approach is a display of power on connected mobile devices. Their work basically is to expose the vulnerability of network technologies, particularly in 2G.

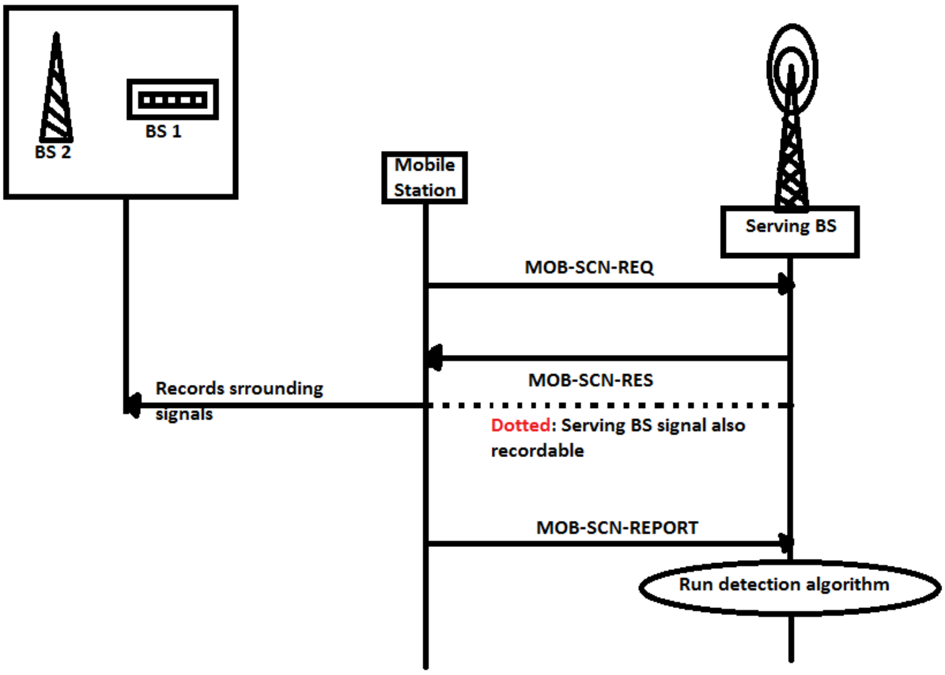

Figure 18: The scanning-interval algorithm procedure from [14].

[28] A high-performance electronic board device that can be configured to create software radio.
[29] Cell selection and re-selection, and blocking method

Barbeau and Robert [14] published a scanning interval algorithm to detect rogue base. This technique is based on the received signal strength (henceforth, RSS). When the RSS of the serving base station falls below a defined threshold, mobile device can initiate handover in search for better service from neighboring cells in order to maintain quality of service. To do this, MS demands from current serving network the permission to scan and assess surrounding base stations. Figure 18 depict procedure flow.

The procedure begins with mobile device sending to its serving network a scanning interval allocation request (MOB-SCN-REQ) message. Serving base station sends a scanning interval allocation response (MOB-SCN-RES) message back to the mobile device. This response contains MAC addresses of recommended base stations. The mobile device can decide to perform association tests with these recommended base stations during the allocated scanning interval. However, mobile device sends a scanning result report (MOB-SCN-REPORT) message back to the serving BS. Algorithm is then run on received report, known to consist of a list of pairs of recommended base stations parameters i.e. a base station ID and corresponding RSS value. The RSS parameter is what the algorithm mainly uses to detect malicious stations. Two limitations observed in this algorithm are: it only works when mobile device is performing the scanning interval routine, and has a level of uncertainty in accuracy.

Ramanpreet and Sukhwinder [56] proposed a rogue base station detection protocol that centers on Wimax/802.16 network, based on observed inconsistencies both in sensitivity and received signal strength measurement reported by mobile station. Their work rely basically on the use of parameters such as; signal-to-noise ratio, path loss, and receiver sensitivity, to detect fake base stations.

Proposed method works as a sensitivity algorithm applying the fundamental understanding that a Wimax device can measure the variations in the received signal strength coming from a transmitting base station. And in a similar approach as those presented in the work of Barbeau et al (already described above), algorithm scans, for all frequencies at every interval of 2msc in order to detect a rogue base station. Since received signal strength is the base for this algorithm, their work also considered factors such as unusual or abnormal noise, and interference, as those can affect the received value. In a summary, their proposed algorithm calculates the received signal power as well as path loss based on optimal sampling frequencies, before comparing them with the threshold. Depending on the outcome of this comparison, for instance if checksum error is too great, then an alarm signal beeps on the mobile.

These few selected publications is a way of demonstrating that research work in the security field, particularly communication sector, is non-stop. Either by showing that fake BTS exists, or by proposing a detection methodology, all work still points in one direction. The next chapter presents our data collection procedure, useful for practical analysis to detect one, in later work.

4 Practical network activity measurement

In this section, we describe in detail the procedures and factors taken into consideration for data collection with the objective of seeing several types of on going events, and to possibly identify abnormalities 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. However, full details about the hardware, software, and protocol used can be found in the next section. Section ends with the presentation of covered areas and observations in them.

4.1 Experimental protocol

4.1.1 Protocol

To conduct this study, we selected three busy areas in the Helsinki neighborhood namely: Eira, Kulosaari, and Kuusisaari. This areas are of particular interest because of the concentration of Embassies (see 6) situated in those locations making it attractive enough to motivate attackers and spies. The measurements are based on the use of both software applications and physical equipment to capture possible network activities happening around target locations, while the interest for doing this is to be able to extract useful parameters such as: LAC/CID [30] changes, the network type i.e. 2G or 3G, and power received from the BTS, all to aid analysis.

Three mobile phones (see section 4.1.3 for specification) were used as the physical equipment for capturing, with each having one of the three networks (refer to section 4.1.5) SIM cards inserted. The same experiments (see protocol below), are run on all three phones (and therefore, networks) at the same time. For the 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.

[30] Location Area Code / Cell IDentity

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".

4.1.2 Software used

- **Snoopsnitch** According to the website[31] description: "SnoopSnitch is an Android app that collects and analyzes mobile radio data to make you aware of your mobile network security and to warn you about threats like fake base stations (IMSI catchers), user tracking and over the-air updates. With SnoopSnitch you can use the data collected in the GSM Security Map at gsmmap.org and contribute your own data to GSM Map." The application logs all activity in a SQLite database on the phone memory, including GPS position, recorded cell data, and results of the active tests it performs.

  In order to run this application to capture mobile network and access data thereafter, root privileges are required [60]. Several versions have been released but the latest version is 0.9.7 (as at 4th of May, 2015).

- **Android IMSI Catcher** From the website[32] description: "Android-based project to detect and avoid fake base stations (IMSI-Catchers) in GSM/UMTS Networks. The application logs similar data as the Snoopsnitch one, also in a SQLite database but there is no active testing for this one. So regardless of whoever [33] is attempting to sniff or catch our data, this application is aimed at detecting them and giving users safer experience through an alert on their devices on possible tracking or interception [54].

  There has been several versions of the application released till date, and the latest version is Version 0.1.28-alpha-b00 (as at 4th of May, 2015)

4.1.3 Hardware used

- Sony Xperia Z2
  1. Model Number: D6503
  2. Processor: Qualcomm MSM8974PRO-AB

[31] https://opensource.srlabs.de/projects/snoopsnitch
[32] https://secupwn.github.io/Android-IMSI-Catcher-Detector/
[33] The authorities or hackers

3. Android: 4.4.2
4. Baseband: 8974-AAAAANPZQ-00015-10
5. Build Number: 17.1.2.A.0.314
6. IMEI: 355609063515414
7. Serial: BH916MF116
8. Network: DNA

- Sony Xperia Z2

1. Model Number: D6503
2. Processor: Qualcomm MSM8974PRO-AB
3. Android: 4.4.2
4. Baseband: 8974-AAAAANPZQ-00015-10
5. Build Number: 17.1.2.A.0.314
6. IMEI: 355609064637514
7. Serial: BH91A4YA16
8. Network: Sonera

- Galaxy Note 2

1. Model Number: GT-N7105
2. Processor: Qualcomm MSM8974PRO-AB
3. Android: 4.4.2
4. Baseband: N7105XXUFND3
5. Build Number: KOT49H.N7105XXUFNE3
6. IMEI:
7. Serial: Exynos 4 Quad4412
8. Network: Elisa

4.1.4 Software installed

- Snoopsnitch, version 0.9.3
- AIMSI Catcher, version 0.1.25-alpha-b6
- Xposed Framework, version 2.6.1
- Xprivacy module, version 3.6
- Root, SuperSU, version 2.01

4.1.5 SIM Cards used

- 2.5.1 Saunalahti Prepaid
    1. Number: 0456 xxx xxx
- 2.5.2 Sonera Prepaid
    1. Number: 0402 xxx xxx
- 2.5.3 DNA Prepaid
    1. Number: 0449 xxx xxx

4.2 Data extraction and observation

Measured data from experiments are stored in the core [34] of the mobile phones, not on the detachable SD-Card or temporary storage unit on the phone, and therefore requires root access to get these files. In this case, data folder path to each of the three phones are similar and given below for both Snoopsnitch and AIMSICD application:

- Snoopsnitch: /data/data/Android/de.srlabs.snoopsnitch/
- AIMSICD: /data/data/Android/COM.SecUpwN.AIMSICD/

The main file that holds data is saved as a .db extension in SQLite format, this suggest the use of a database editor to read file. In this case, preferred option to use is the SQLiteBrowser with which the file was opened and studied.

4.2.1 Observation on Eira

Data was captured in Eira on two different days, 2015-02-05 and 2015-03-03, as both Figure 19 and Figure 20 depicts, following different routes as a way of spreading search coverage area. The duration to complete the first Measurement took almost three hours: starting from 11:31:57 till 14:14:27, while the second took 1:20:26 to complete.

4.2.1.1 Elisa

- 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

4.2.1.2 Sonera

- Nothing to remark

[34] in-built memory

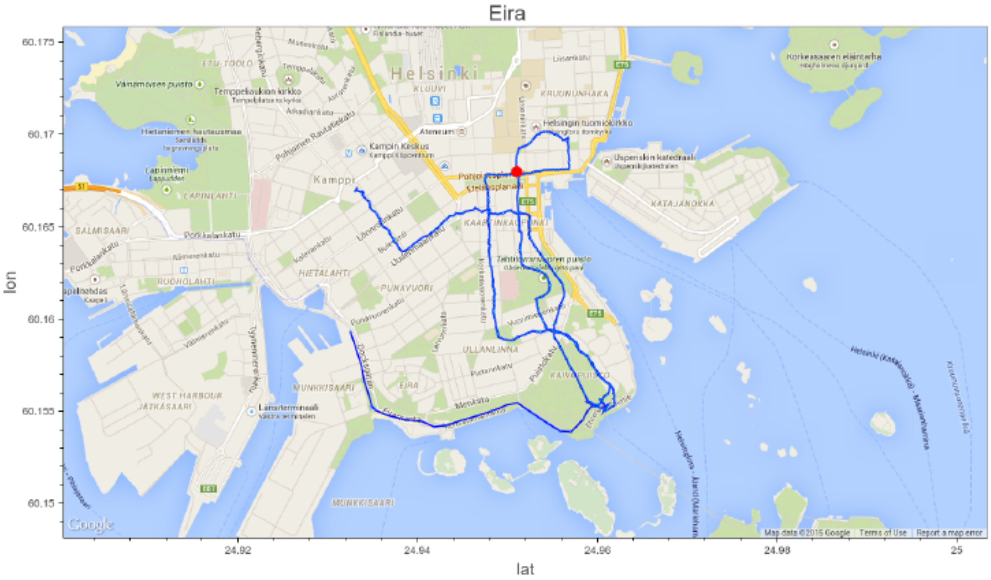

Figure 19: Itinerary in Eira on 2015-02-05. Red dots indicate approximate location of major events.

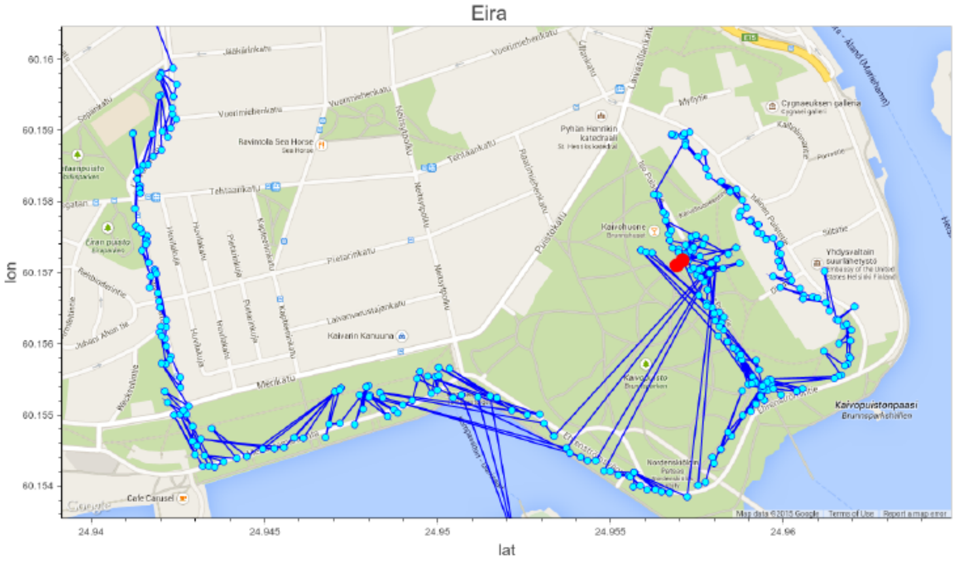

Figure 20: Itinerary in Eira on 2015-03-03. Red dots indicate approximate location of major events .

4.2.1.3 DNA

- Downgrade 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)

4.2.2 Observation on Kulosaari

Similarly, data capturing was done on two different days, 2015-02-13 and 2015-03-03, and in two different routes as depicted in Figure 21 and Figure 22 respectively.

4.2.2.1 Elisa

- Multiple cuts from 3G network over UMTS, no CID or 29006/422217
- Up to 3 minutes cuts, sometimes connected to 29006/422217
- Lost network while switching from 3G to 2G, for 1 minute

4.2.2.2 Sonera

- Lost network for 1 minute 13 seconds while switching from 2G to 3G (connected to one BTS, varying power)
- Connected to unknown BTS (LAC/CID reported 2147483647, which means unknown for Android) for 20 seconds, varying power. This could be normal

4.2.2.3 DNA

- Downgrade to 2G for 40 seconds
- Multiple network cuts on 3G for up to 4 minutes 13 seconds

4.2.3 Observation on Kuusisaari

As shown in Figure 23 and Figure 24, is a representation of two different routes covered on two different days, 2015-02-20 and 2015-03-03, for data capturing in Kuusisaari part of Helsinki.

4.2.3.1 Elisa

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

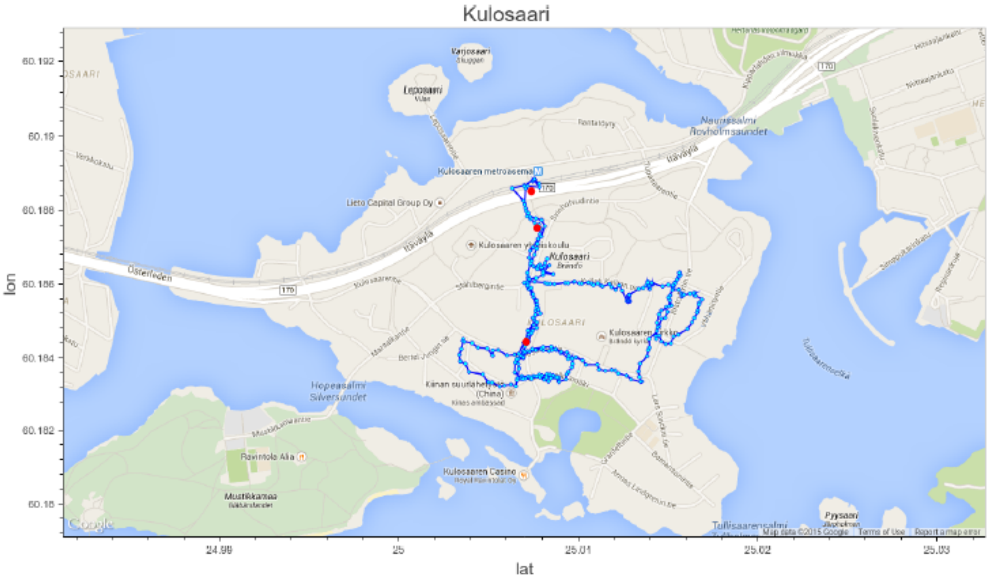

Figure 21: Itinerary in Kulosaari on 2015-02-13. Red dots indicate approximate location of major events.

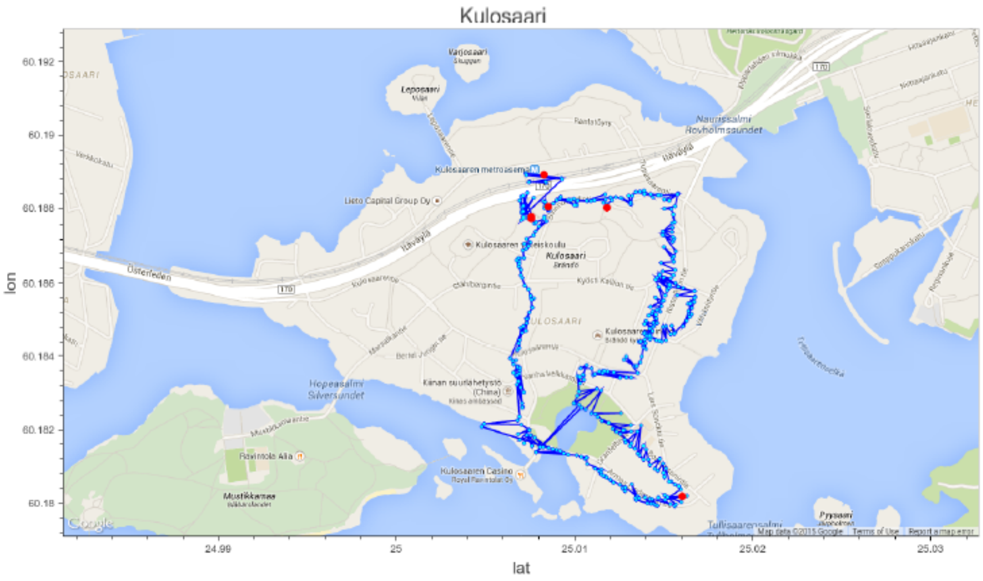

Figure 22: Itinerary in Kulosaari on 2015-03-03. Red dots indicate approximate location of major events.

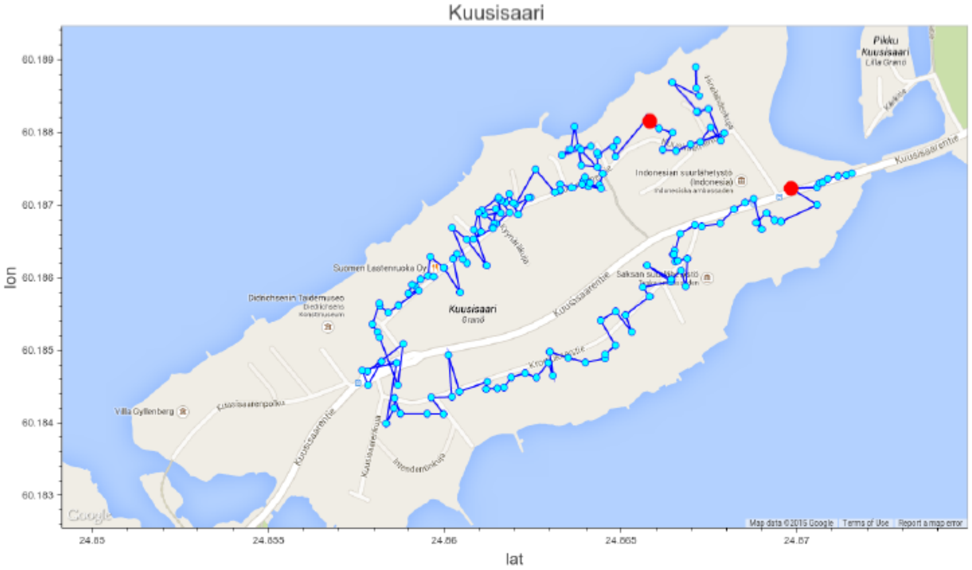

Figure 23: Itinerary in Kusisaari on 2015-02-20. Red dots indicate approximate location of major events.

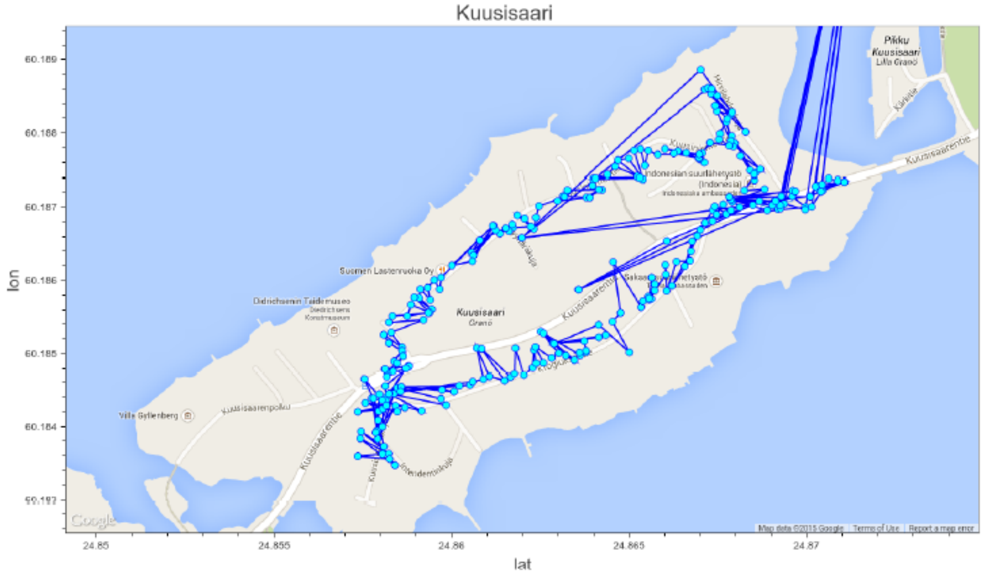

Figure 24: Itinerary in Kusisaari on 2015-03-03.

4.2.3.2 Sonera

- Nothing to remark

4.2.3.3 DNA

- Nothing to remark

4.3 Summary

The gathered events and findings presented above in the concluded experimental study can be argued not to be solid enough to claim that these network activities are abnormal, but certain suspicious occurrences such as: downgrades from 3G to 2G in areas that are not densely populated, at times where little activity is present, are unusual. Especially regarding the coverage claims from the operators. In addition, and while these details are not fully disclosed here, several of the major events noted correspond to moments when incoming calls and SMS were never reaching the devices (using Snoopsnitch active testing mode).

A proposed solution to solidify these results would be to directly collaborate with the network operators, presenting the possibility to be able to cross-check the events we encountered with the state of the network on their side at the same time. To achieve this goal, we have made attempts to reach out to some of the operators but did not get any response from them. Future work on this topic would consider deeper analysis at other sites of base-band log parsing on the UE, which contains more information. In addition, verification and analysis done in this work was performed by a human. To achieve better result and accuracy, we are proposing to use machine learning techniques to analyze the logs at the Android OS level, and possibly at the baseband log level.

Finally, a detection and mitigation solution enabling the user equipment to verify the authenticity of the BTS it is attempting to connect to, as well as predefined scenarios for the cases where the UE is believed to be in a hostile environment[35] is presented as the main work of this project in the following Chapter.

[35] IMSI Catcher, and fake BTS.

5 Proposed Detection and Mitigation methods

5.1 Introduction and work background

While much has already been discussed on the existence and presence of fake base stations and their intentions in a network (section 3), the focus therefore in this section is to propose a methodology that can be implemented in the user's mobile equipment for its detection and mitigation. This methodology should be implemented as a software or an application that relies on the real operator's database information of all existing and genuine base transceiver station. Meaning that the user's mobile device plays an active and fragile role, as the actual detector which after spotting an abnormal activity then alerts or reports to the operator of a suspicious fake base station present in the network.

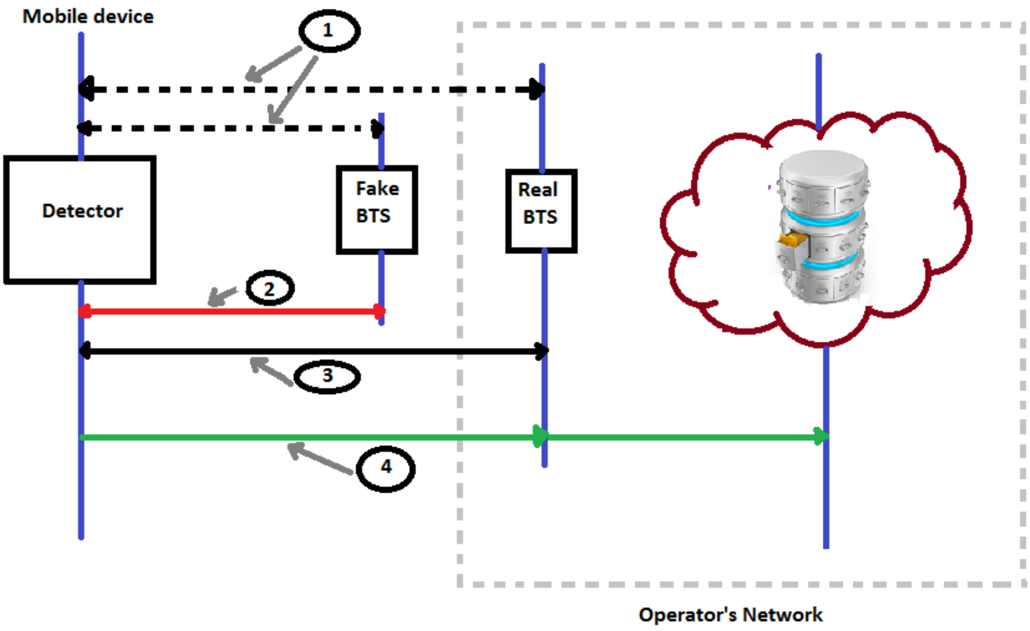

Figure 25: General overview of proposed methodology indicating process flow.

A detailed description of figure 25 is as follows. Logically, there are four entities and these are; mobile device (which we are proposing to be the real detector), fake BTS (not initially known as fake), real BTS (we are also initially uncertain of), and the operator's database (implemented in the network). These four are represented using candle stick notation of different box sizes, and different colors to denote different considered interaction states (this will be properly explained hereafter). There are two types of line notations used, dotted and straight.

We start with the general assumption that both the mobile device and operator's network have already passed through an authentication process and confirmed to be genuine, and therefore are certain that the mobile device is connected and have access to the real database. For several reasons, one of such is mobility [64, 26], mobile device interacts with one or many base stations, for instance during mobility where the mobile device is in motion, and moving from one location to another. During this stage, 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 best transmission signal power [31].

The pair of black dotted lines as we see in figure 25, 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, mobile device uses our proposed methodology (described in section 5.2.1) 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, represent an alert initiated by mobile device and sent to the network of a suspicious activity and the presence of an unregistered BTS in the network. One might then ask how certain are we that the alert gets to the network, for instance, what if it is sent via a new fake BTS that just joined shortly after the verification process was done? **Answer:** is that after the verification process, we have two separate sets of BTSs, fake and real. Since we know the real (through authentication), we choose to send through this, while we ignore the uncertain BTS.

On a precise note, 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 (future), in these two considered cases:

1. A base transceiver station with wrong LAC/CID but on the operator network. Such fake BTS in this case have correct MNC and MCC.

2. A base transceiver station with correct LAC/CID but existing on the operator network, trying to pass for a real BTS.

- What precisely are: LAC, CID, MNC, MCC?

With billions of devices interacting in the present mobile networks, it is expected for every of these participating devices to have some form of identification which makes it possible for operators to identify them. It is of course not sufficient enough to have just each device's number but to also be able to locate them. That is the fundamental idea behind the creation of LAC and CID. As shown in figure 26, each cell of a network has its own unique identification number and this is referred to as Cell ID. LAC on the other hand is used to denote a collection of several cells in a mapped location, which is controlled by an operator controlling that specific area.

Mobile Country Code (MCC) and Mobile Network Code (MNC) are assigned codes to represent the country and the service rendering operator respectively [30]. A glimpse of what these two acronyms represent and are used for in detail can be found in [65].

In a relative term, CID would represent a building on a street, while LAC would represent the collection of several buildings to make up a street. So when a paper mail is to be delivered to a specific resident in that area, the carrier (post man) first find the street, locate the building on that street, and finally check through the list of residents in the building to deliver the mail to rightful recipient.

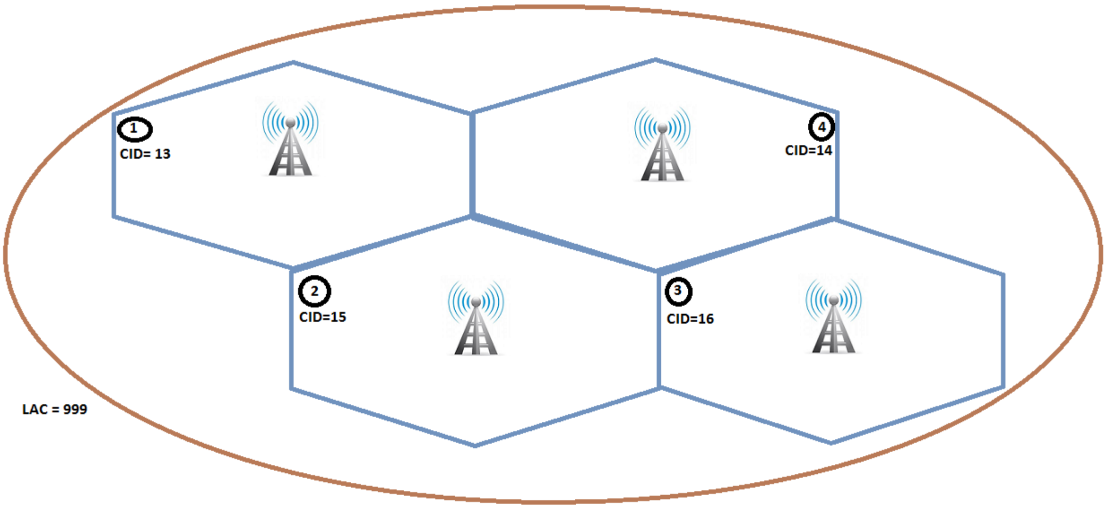

Figure 26: Clarification between Location Area Code (**LAC**) and Cell Identity (**CID**).

Building on this knowledge, the first case mentioned above therefore arises when a false 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, false base station impersonates a real base station within the attack region and thus pretend to be part of the operator's network. It is also possible in this case to have the false base station connected as a proxy to the operator network, or not connected to it at all.

5.1.1 Considered scenarios

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 25 is given and explained in figure 27. By an ideal situation, we refer to a genuine case that comprises of real BTS, and real DB, which is what our first scenario case describes (as we shall later see). Meanwhile, the interaction flow in figure 27 between active entities is briefly described as follows;

1. Mobile Station initiates interaction by sending an encrypted data request message for core network's copy of genuine list of database to the Base Transceiver Station. This encryption is secured with the core network's public key, which is denoted as OpKEY, to ensure that only core network can access this message.

2. Base Transceiver Station forward this encrypted data to the core network.

3. Core network decrypt received mobile station encrypted data. Then makes a copy of genuine lists of BTS, as requested by MS i.e. Req BTS. Finally, Core Network responds with an encrypted message, denoted as Res BTS, ensuring that only the right MS can decrypt this message by using MS public key i.e. MS_{KEY}, and then forward to BTS.

4. Base Transceiver Station forward this message from Core network to mobile station.

5. Mobile Station decrypt received encrypted message from Core network, and then compare the received Database list denoted as DB_{core}, to its own Database [36] denoted as DB_{MS}.

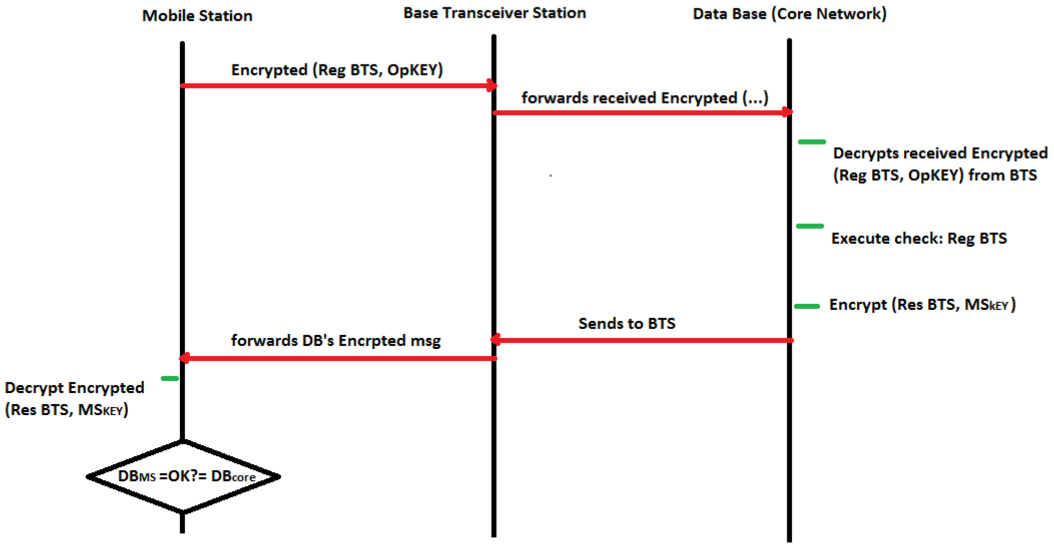
Mobile Station
Base Transceiver Station
Data Base (Core Network)
Encrypted (Reg BTS, OpKEY)
forwards received Encrypted (...)
Decrypts received Encrypted (Reg BTS, OpKEY) from BTS
Execute check: Reg BTS
Encrypt (Res BTS, MSKEY)
Sends to BTS
forwards DB's Encrpted msg
Decrypt Encrypted (Res BTS, MSKEY)
DBMS =OK?= DBcore

Figure 27: Description of the process flow and transferred data between the three participating entities in the network.

[36] Using Figure 25: Mobile Station listens to all received nearby transmitting BTSs, and stores them

The procedure above is intended to clarify misconceptions and should help to better understand discussion that arises in the next three considered scenarios, which are denoted as case 1, case 2, and case 3 as presented below;

Case 1:

As depicted in figure 28, mobile station 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 MS is able to access it. This means that the mobile station, through listening, is able to acquire necessary parameters such as; LAC, CID, and $\text{Power}_{\text{phone}}$ from nearby cells. While through already explained interactive process between MS and Core Network in figure 27, mobile device gets access to several genuine data set useful for comparison.

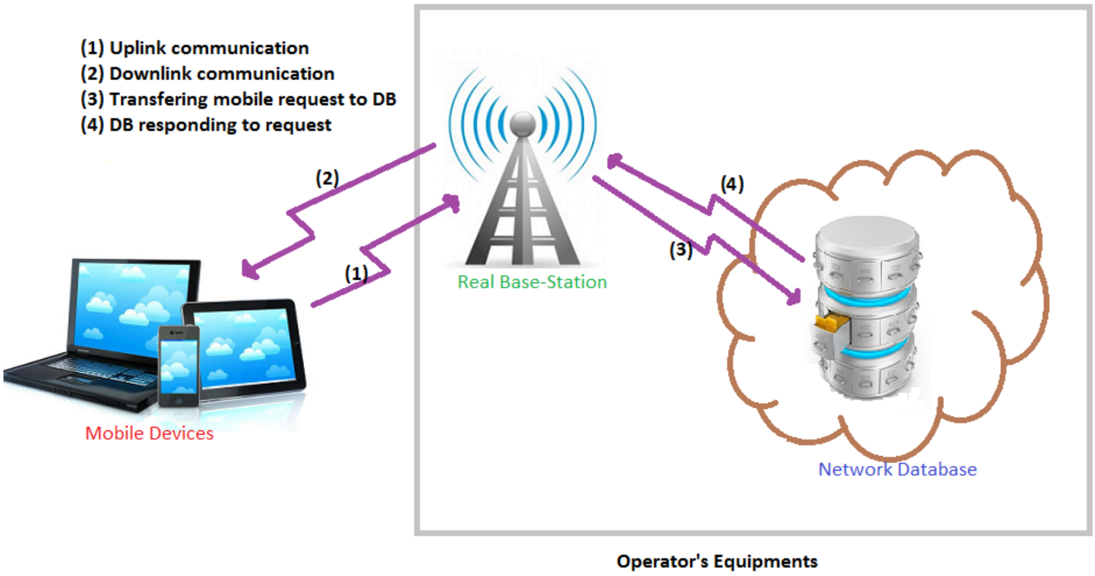

Figure 28: Scenario considers mobile device communicating with a real base station and the real network's database. These equipments on the network sides are genuine.

Each data set include parameters such as LAC, CID, $\text{Power}_{\text{now}}$ (measured transmit power from base station), and GPS_{real} (since base station is static). With these parameters, we can compute;

- GPS_{EST} through $\text{Power}_{\text{phone}}$ and other Radio data.
- $\text{Power}_{\text{EST}}$ through $\text{Power}_{\text{phone}}$, GPS_{real}, $\text{GPS}_{\text{phone}}$, and $\text{Power}_{\text{now}}$.

After computing these two parameters, a comparison process between them and other important and useful parameters is expected to be performed in order to reach a possible conclusion to detecting a rogue base station. The comparison procedure is explained below:

1. Mobile Station checks if $\mathrm{GPS}_{\mathrm{EST}}$ is not equal to $\mathrm{GPS}_{\mathrm{real}}$: variations in GPS coordinates can help to make conclusions. For instance, if actual BTS location realized is far too greater than the expected transmitting BTS location.

2. It is also possible to check if $\mathrm{Power}_{\mathrm{EST}}$ is not equal to $\mathrm{Power}_{\mathrm{now}}$: This also is similar to the above explanation, although it might not be an appropriate method to base conclusion on because different factors can influence the received transmission power, which can sum up to cause huge variation i.e. interference generated around the cell. (See section 5.2.3 for detailed power estimation)

Case 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 centers around the existence and interference of fake BTS on mobile device accessibility to the database. We split this scenarios into two as; access to DB via genuine BTS, and access to DB only through fake BTS.

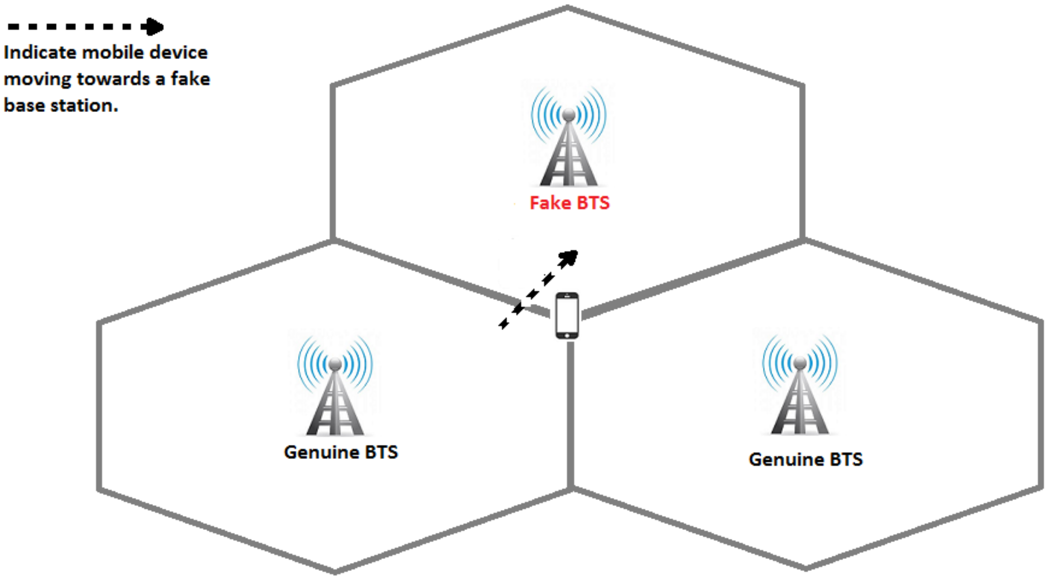

Figure 29: A wandering mobile device receiving signal both from genuine and fake base stations as it approaches the fake one.

- Access to Database via genuine BTS

Using figure 29, it is possible to consider two scenarios. The first one being a situation where mobile phone is at the mid-point of the three cells, meaning that it is getting signals from both genuine and fake BTSs, but moving more toward a fake base station. In this situation, mobile station try to connect to DB through fake BTS, 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 high transmitting fake base station around, and then successfully connects to the network's database as described in case 1.

- Access to Database only through fake BTS

In a situation as this, where the mobile station can only locate or is surrounded by only fake base stations, it is definitely obvious that it cannot gain access to the network's database. As depicted in figure 30, mobile station moves closer to the fake base station, and therefore senses only that base station which it then attempt to connect through to get to database. Since the fake base station is not legally registered to the network, its does not exist to the core network, and therefore can not establish any interaction in that network i.e. connect to the real database.

The only remaining possibility therefore is for the mobile station to compare and check for genuity of existing BTSs with the local copy of the real network's database previously stored on its internal SD-CARD.

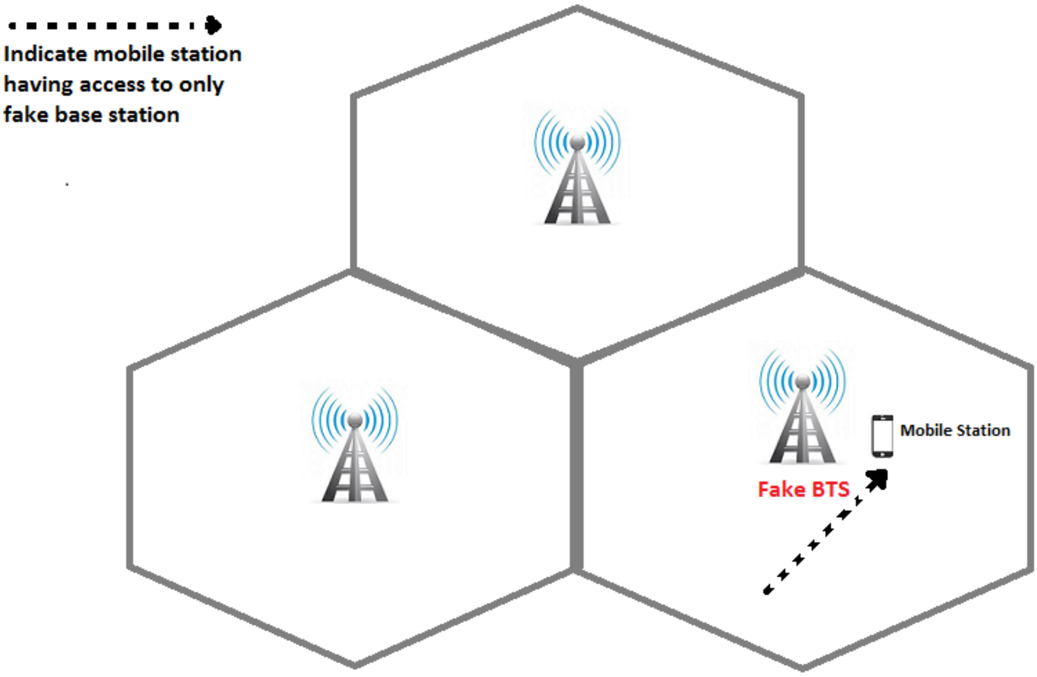
Indicate mobile station having access to only fake base station
Mobile Station
Fake BTS

Figure 30: A situation where mobile device can only receive signal from a fake base station.

Case 3:

Figure 31 illustrate another possible scenario where 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 (see [58]).

In this type of scenario, where the mobile device has no connection to the real operator's network, it can only rely on the data already stored in itself. Meaning for instance, the use of SD-CARD or internal storage holding a copy of the legal data previously collected as the only option to revert.

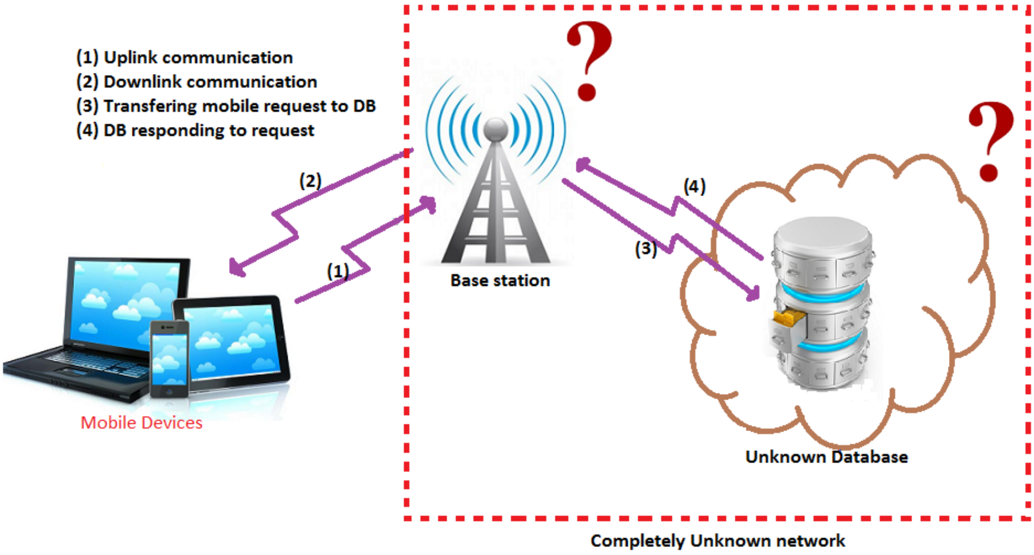
(1) Uplink communication
(2) Downlink communication
(3) Transfering mobile request to DB
(4) DB responding to request
?
?
(2)
(1)
(4)
(3)
Base station
Mobile Devices
Unknown Database
Completely Unknown network

Figure 31: The interaction between Mobile station and the network can not be trusted because the network is completely unknown.

5.2 Fake BTS Detection Methodology

The methodology proposed in this section is modeled under certain assumptions, and works without the need of having to design a new physical hardware. Assuming that the assumptions discussed in section 5.3.1 are met, the whole methodology can be implemented and installed as a software on existing mobile device.

5.2.1 Detection methodology

The proposed methodology relies on two main assumptions (see section 5.3.1): The availability of a database, in the operator's network, that the mobile device can query through a genuine BTS, and which holds a recently updated list of LAC/CID, GPS coordinates (and eventually power emitted) for all the BTS deployed by the operator. The second assumption is that the mobile device is able to receive vital information

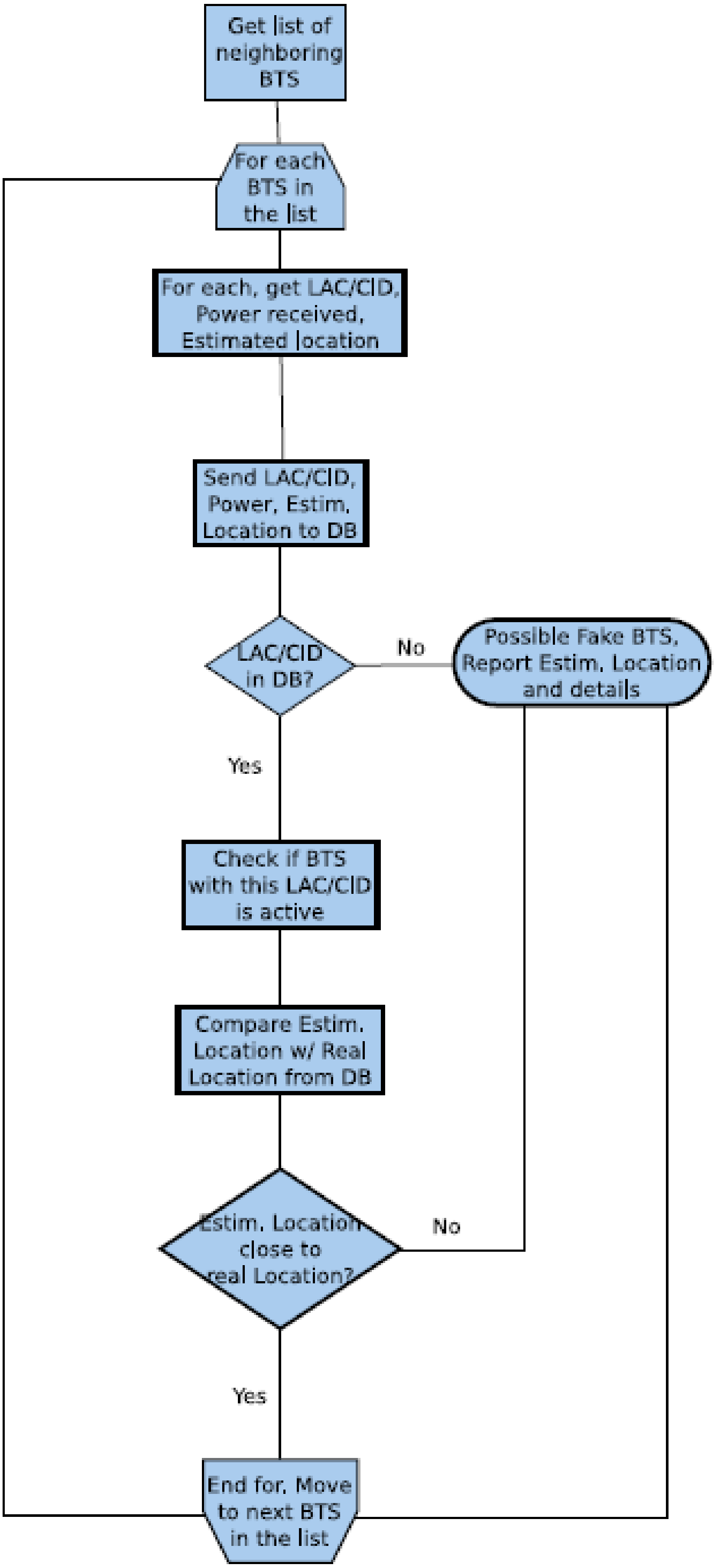
Get list of neighboring BTS
For each BTS in the list
For each, get LAC/CID, Power received, Estimated location
Send LAC/CID, Power, Estim. Location to DB
LAC/CID in DB?
No
Possible Fake BTS, Report Estim. Location and details
Yes
Check if BTS with this LAC/CID is active
Compare Estim. Location w/ Real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

Figure 32: Overall schematic of the proposed methodology.

such as; LAC/CID and transmitting power from neighboring BTSs within range.

When all these conditions are met, the mobile station which is already equipped through the installation of the proposed methodology as a software, should be able to run the following sequence of steps depicted in Figure 32 at regular intervals:

1. Collect the list of BTS that are within range (possible since MS keep 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 location (see section 5.2.2);

   (b) Compare received parameters [37] from the network's DB to own internal database i.e. SD-CARD (see figure 33);

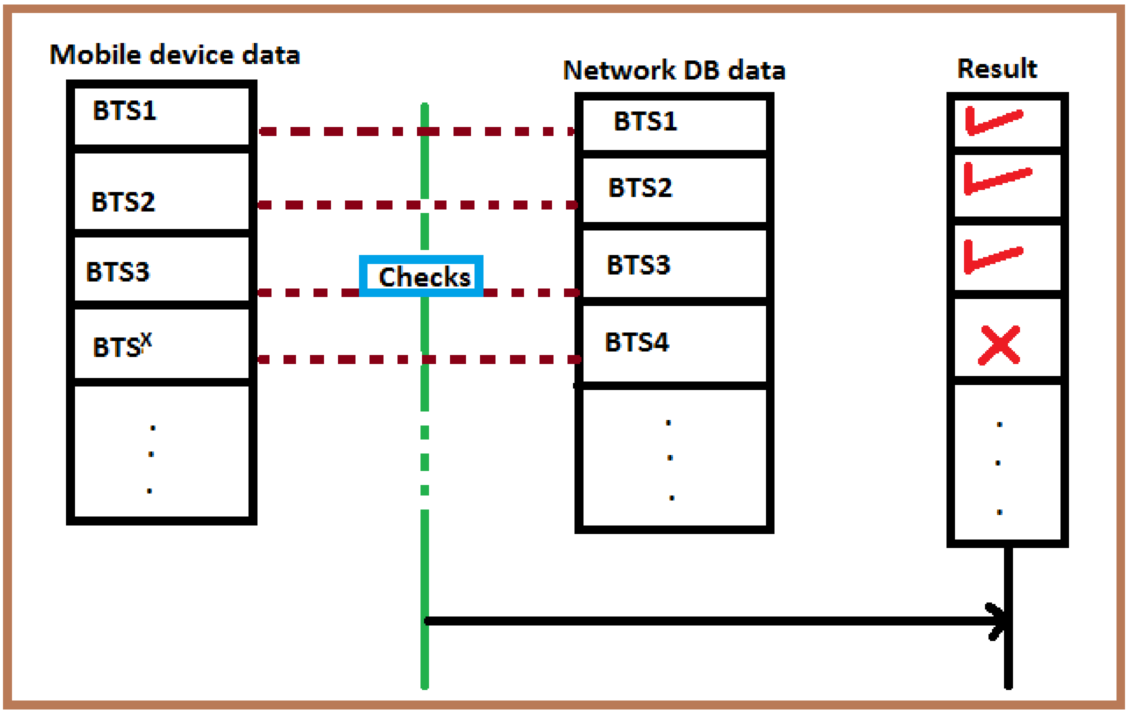

Figure 33: Proposed methodology implemented as a sofware on mobile device to verify data.

   (c) If the LAC/CID is not in the DB: The BTS with this LAC/CID could be a fake (figure 33). 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);

[37] LAC/CID, received signal strength, e.t.c

(e) Compare the estimated location with the one obtained from the database;

(f) If the distance between estimated and the real location are too different, send an alert or report to the operator;

(g) Else, move to the next BTS in the list.

Both power and location estimation can be derived using the received signal strength as described in the following subsections. The reason for discussing how this estimates can be achieved is because of cases where the mobile device also need to estimate transmitting device's location, as we have seen in cases where there is no access or connectivity to the core network. For instance, in case 3 discussed above.

5.2.2 Location Estimation

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 under suspicion. Triangulation is relatively simple to perform as described, for both mobile device and network BTS, in the following given illustration for clarity purpose, and to better understand its application to our case, while one can also refer to this webpage [38] for more description of the method.

- Network Location estimation

A network's BTS is able to apply the triangulating method this way: Since the antennas on a BTS are arranged in a triangle (this explains the mid-center triangle in the figures), and by dividing the surroundings of a BTS into three sectors, as depicted in figure 34, it is then possible for BTS to tell from which side (sector) the interacting device is stationed. The number marking one to five, usually extend more than this in reality, in the same figure is used to denote the distances away from the base station.

Using just one BTS, which is the BTS interested in estimating the location of an intruder, it first must be able to determine where the signal is coming from, and we have chosen the beta sector of figure 34 for this. It is not difficult to estimate intruder's location through the received signal strength which to support this example is chosen to be five miles away. Meaning that the suspect can be in any point along the marked region and this is not sufficient enough.

Since signal is radiated in all directions from the source, a second nearby BTS also in that vicinity, can can also play a part in estimating the location of the suspect whose signal is also received by this second BTS. Figure 35 depict a case where the second BTS also estimates the location of these suspicious device, and then follow a similar approach as described in BTS 1. Judging by the diagram, BTS 2 senses the

[38] http://www.neilson.co.za/mobile-network-geolocation-obtaining-the-cell-ids-the-signal-strength-of-surrounding-towers-from-a-gsm-modem/

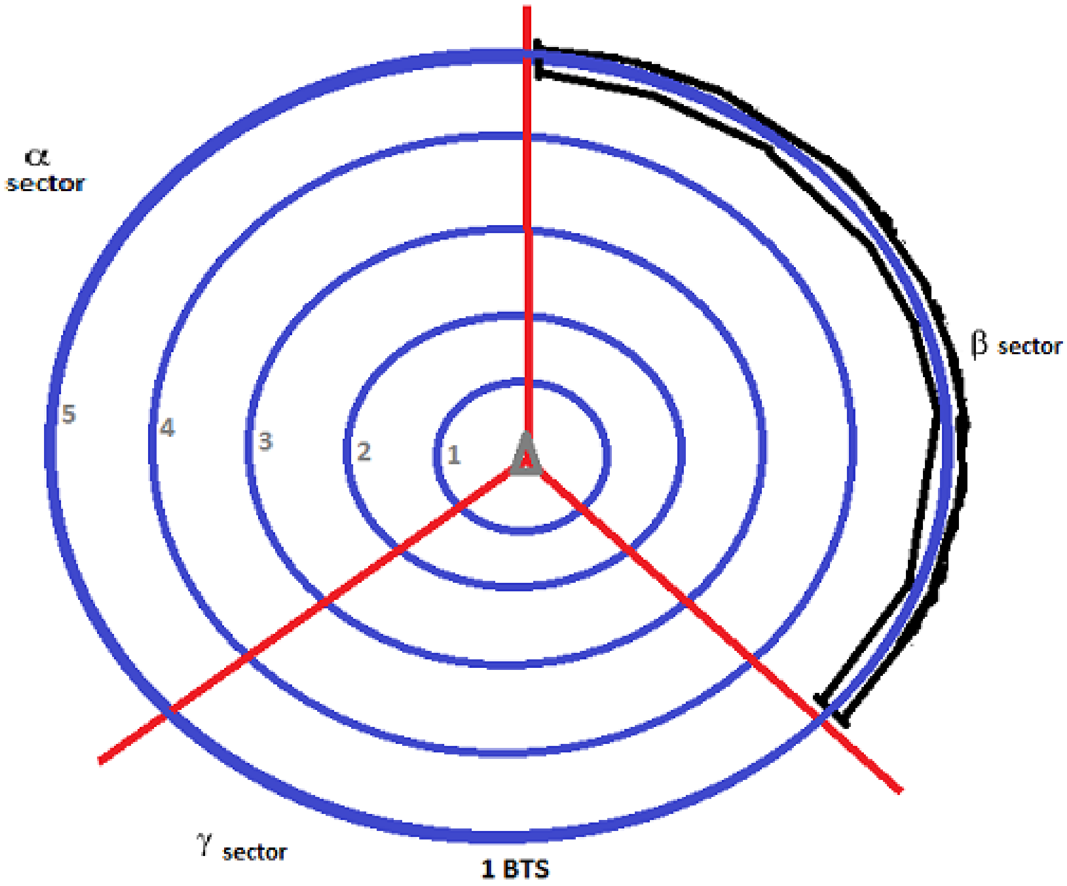

Figure 34: Application of the triangulation method to aid in estimating fake transmitting device location using one Base Transceiver Station only.

signal in the alpha sector, and using the strength of the received transmission signal from device, it estimate device to be four miles away. One can see that the location is getting more narrowed and exact that in using just one BTS.

For a better and more precise location estimation, this method is applied to a third BTS, depicted in figure 36, which also senses the transmitting signal of the mobile device five miles away.

- Location estimation for Mobile device

Mobile devices can also apply the triangulating method to locate devices but in a slightly different way than used in 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 [39].

Mobile device, acting as a detector, measures and saves the received signal (device

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

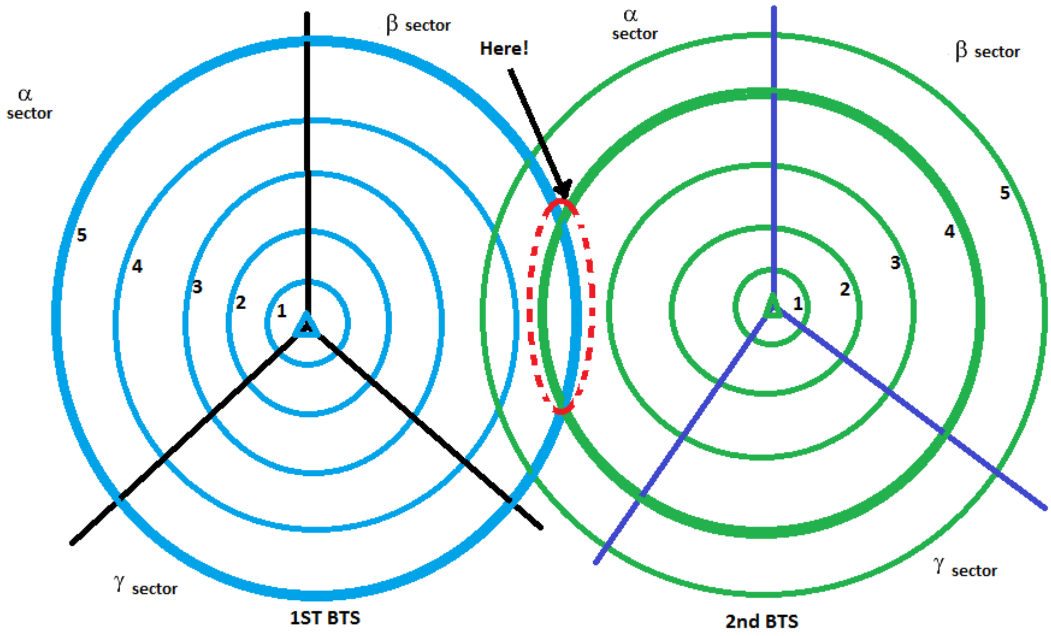

Figure 35: Application of the triangulation method to achieve a better location estimation for suspicious transmitting device using two Base Transceiver Stations.

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 37, from different locations, mobile device was able to collect different signal power from the suspicious transmitting device, which then applies same triangulating method as used in BTS estimation to estimate location.

5.2.3 Power Estimation

Finally, if the power emitted and received by the BTS are available, it is also possible to estimate what power should be received from the analyzed BTS. Using statistical modeling approach such as the Okumura-Hata model [26] and others [40], 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 (real BTS as assumed 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 38

[40] Shadow fading, Multipath fading, exponential distribution

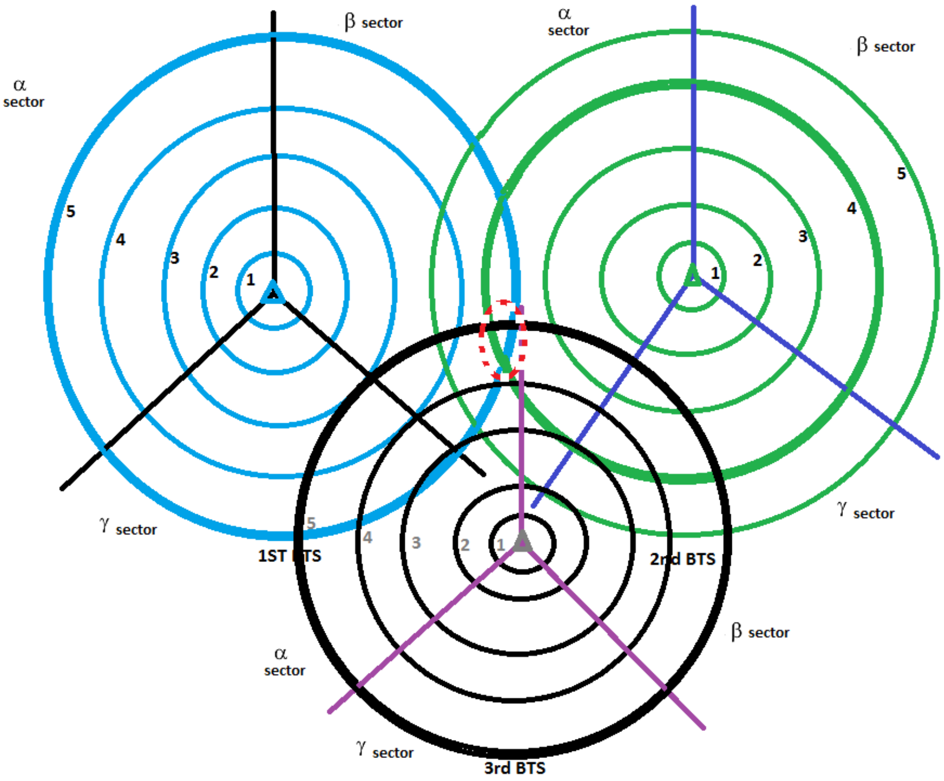

Figure 36: Using three Base Transceiver Stations to help in estimating the location of a suspicious transmitting device.

helps to solidify the description already explained.

The following describes how Okumura-Hata model is applied mathematically to obtain the received power at 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 are denoted as i = 1, 2, 3, and 4 respectively. While the Antenna type for Okumura-Hata is Isotropic.

Okumura-Hata Average path loss is given as L_{50} (dB) = L_{F} + A_{mu} (f, d) - G (h_{te}) - G (h_{re}) - $\mathrm{G}_{\mathrm{AREA}}$.

where,

L_{50} = 50 percent value of propagation path loss (median).

L_{F} = free space propagation loss.

A_{mu} (f, d) = median attenuation relative to free space.

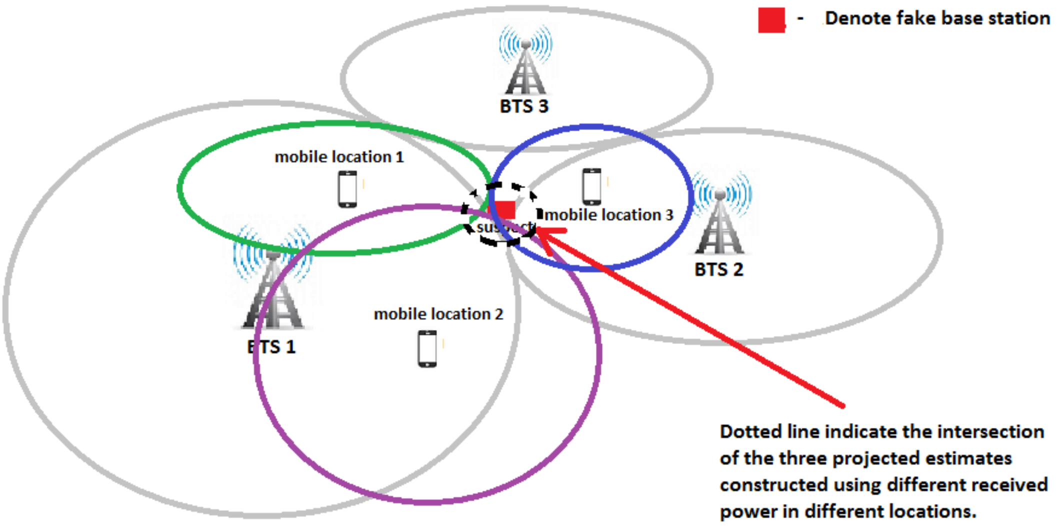
🟥 - Denote fake base station
BTS 3
mobile location 1
mobile location 3
BTS 2
suspect
BTS 1
mobile location 2
Dotted line indicate the intersection of the three projected estimates constructed using different received power in different locations.

Figure 37: Mobile device applying the triangulation method from three different locations in order to estimate a fake base station.

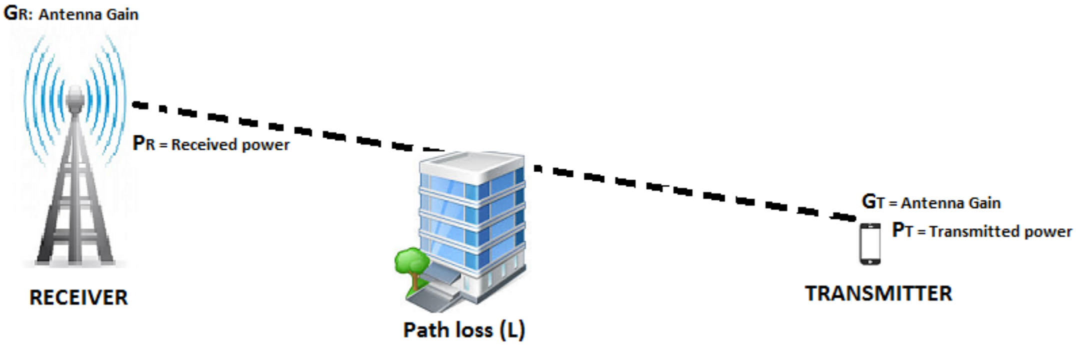

Figure 38: Showing path loss between the transmitter and the receiver: it is the difference (in dB) between the transmitted power and the received power.

G $(\mathrm{h_{te}})$ = base station antenna height gain factor.

G $(\mathrm{h_{re}})$ = mobile antenna height gain factor.

$\mathrm{G_{AREA}}$ = gain due to environment.

f and d = 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 respectively.

Further computation done by substituting the value of $\mathrm{L_{50}}$ into $\mathrm{P_R}$, denoting the received power at the base station is given below.

$P_R = P_T - L_{50}$.

where,

P_T = transmitted power from source.

As one should expect, each of these parameters used briefly to calculate the received signal strength (power) in the above illustration can further be studied to understand their derivation in order to understand better their impact when used in modeling real life situations (kindly refer to [26]).

5.3 Fake Base Station Mitigation algorithm

Mobile device is the main detector in this work, but like every other end user's mobile device, it has no power to decide on device allowed to participate or use the network resources. The core network does this. Therefore, mitigation, the other part of this work, is carried out in the core network, as shown in figure 39.

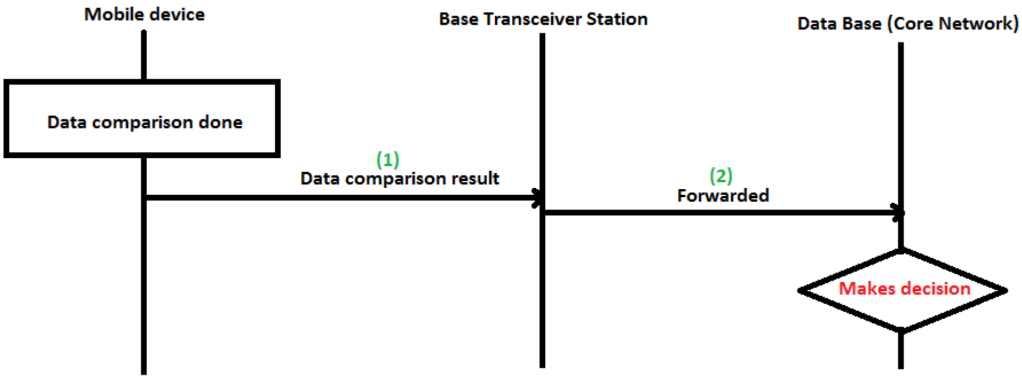

Figure 39: Mobile device sends an alert message to the core network about the existence of a suspicious transmitter.

By mitigation, we try to lessen the effect of a suspicious transmitting device, a fake base station in this case, by proposing a methodology relying on the fact that being able to identify its existence or presence in the network, is the beginning of curbing its disturbance in the network. It is usually or almost impossible for the network operators to even notice them when they exist. Therefore, we present as given in figure 39 the simple alert algorithm to mitigating the effect of fake BTS as follows;

1. Mobile device already compare several parameters (see section 5.2.1). If a suspicious device is found transmitting, MS sends an alert message to the core network through BTS.

2. Network's BTS forwards the message to the core network.

3. Core network verifies received message and takes some mitigating decision on what next to do.

5.3.1 Discussion on the Assumptions made

Assumption that MS can Triangulate and estimate Power

It is assumed in this work, that the mobile station, which is the analyzing device, is able to triangulate in order to locate the position of the suspicious transmitting mobile device as previously explained in section 5.2.2, and estimate power "well enough" which is useful during comparative analysis for detection purpose.

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 operator's 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. (Optional) The power at which the BTS is emitting right now.

The proposed methodology requires that each BTS can query this database, to search for a list of LAC/CID combinations, and obtain the associated GPS location and power for all the records that are found in the database. This information is sent back to the BTS that queried it, for verifying if the neighboring BTS are legitimate.

Assumption on the Connection BTS-DB

It is finally assumed that the connection between the BTS carrying the analysis and the DB holding all BTS information for the operator, is secure and not compromised.

5.4 Alternative approach: Problems encountered

Time and resources are two important factors that must be well planned and managed in any research work, especially such as this one. In an ideal situation, expectation is to have access to a genuine data set for comparison purpose with the data captured from the practical measurement described in section 4. By a genuine data set, we refer to the data that contains network interaction activity with other transmitting devices, stored in the core network's database, from the network operator. This would serve as the standard data set, with the understanding that these have not been compromised as explained in section 5.3.1.

- Initial approach: Network operator (data)
We intended to compare these two different set of data i.e. data from the network, and data from practical network measurement, using either manual or automated software. After this, further work would be to apply some statistical and graphical approach to analyze our findings in order to identify abnormal activities in the network. The major drawback or problem encountered from using this approach was that after submitting a request to several network operators within the vicinity of interest, the response was not favorable and this is due to the security measures on sensitive data involved. Such data contains real life and real people's data and activities, therefore its not an easy data to give out to a third party. It requires a long process and documentations submission, which stretches the time limit we have to carry out this project work.

- Network Simulator
Following the choice of approach eventually used, which is to propose a methodology for detection. We also thought of using a network simulator to develop a system level simulator to demonstrate the scenarios considered in this work. This would require simulating in different cellular networks i.e. 2G, 3G, and 4G. The first option was to simulate our methodology using the new NS-3 (Network Simulator 3). Which means more time is needed to study and use this simulator in order to write reasonable and simple but functional codes. Considering the time frame we have left to finish the project, it was unrealistic and impossible to accomplish the task of writing completely a new simulation code. NS-3 only have an existing 4G (LTE) module, which can be edited to suit our case. Alternatively, to use NS-2 (Network Simulator 2), that also would require having some reasonable time to study the programming environment and to write functional codes to suit our purpose.

6 Conclusion

Years back, the arguments was that although several types of man in the middle form of attack do exist, and have been in existence for many years, yet there is no physical evidence of such attacking equipment as the described fake base station. In response, many scientific articles have been published, see section 3, to support the claim that they certainly do exist, and some have even gone to the extent of building software version of such attack to support their claims, while a few others have designed equipment that can catch IMSI-catcher (as it is sometimes referred to). We acknowledge their existence and that is why we have chosen to work in this direction, and to propose a solution to help mitigate such attacks.

As a starting point, we studied the security implementations in different generations of mobile technologies, this enabled us to understand why fake base station attack occurs mainly on the 2G network. This is not just because 2G is still the most widely adopted technology, but because its security implementation is very vulnerable, as we did show in section 2, making it a suitable choice to carry out such attack. So this means that if a target mobile device is on a 3G or 4G network, a fake base station will manipulatively deceive and force a downgrade on this mobile device, before fully exploiting it.

One of the main objectives we set to achieve in this work, as a way of contributing to the fight against such attack, is to be able to identify a fake base station when present in a network from user's end point. This has two positive effects from both business and technical point of view; first, network subscribers feel their importance to the network topology, as they evidently see improvement in the security features implemented, and to know that their data is getting better protection. This consolidates the trust already existing between subscribers and the network operators. Secondly, network operators feel better in charge and control of their networks. We are of the opinion that it is just not enough to render communication services to subscribers, or to build general security mechanisms as we have, but to completely understand who is causing the damage. After then can a solid mitigating step be developed.

To help in mitigating fake base station attacks, and since mobile devices are not designed to carry out any core network duties, we proposed a simple but functional algorithm to alert the core network of the existence of a suspicious transmitting device, otherwise referred to as a Fake BTS. In most cases, fake BTS only target mobile devices, and not directly the core network, therefore it is possible for such device to be in a network and not noticed. By this algorithm, the opinion is that sensitizing the network is the first step to properly curb such an attack.

However, our proposed detection and mitigation methodology needs to be implemented as a real software (application) on the mobile device. As one might have observed, this work considers mobile device as the detector, to find dis-similarities through comparison between data stored on mobile device and that received from core network database. We would encourage future work to focus more on the network side (core network), where an algorithm can be designed for the network to directly spot this attacker and act against its participation in the network, particularly transmission to mobile devices. Reason for this is related to the third case considered in section 5.1.1, where there is possibility for the mobile station to be in the attacker's set up network, where the genuine network can not locate mobile device.

References

[1] ETSI GSM Technical Specification (1996). Digital cellular telecommunications system; base station controller - base transceiver station (bsc - bts) interface; interface principles (gsm 08.52); version 5.0.

[2] 3GPP TR 33.900 V1.3.0 (2000-02). 3rd generation partnership project; technical specification group sa wg3; a guide to 3rd generation security (3gpp tr 33.900 version 1.3.0).

[3] ETSI TS 100 929 V8.0.0 (2000-10). Digital cellular telecommunications system (phase 2+); security related network functions (gsm 03.20 version 8.0.0 release 1999).

[4] ETSI TS 100 940 V7.8.0 (2000-10). Digital cellular telecommunications system (phase 2+); mobile radio interface layer 3 specification (gsm 04.08 version 7.8.0 release 1998).

[5] ETSI TS 133 105 V3.5.0 (2000-10). Universal mobile telecommunications system (umts); 3g security; cryptographic algorithm requirements.

[6] ETSI TS 133 120 V4.0.0 (2001-03). Universal mobile telecommunications system (umts); 3g security; security principles and objectives (3gpp ts 33.120 version 4.0.0 release 4).

[7] ETSI TS 133 105 V8.0.0 (2009-02). Universal mobile telecommunications system (umts); lte; cryptographic algorithm requirements (3gpp ts 33.105 version 8.0.0 release 8).

[8] 3GPP TS 33.401 V8.6.0 (2009-12). 3rd generation partnership project; technical specification group services and system aspects; 3gpp system architecture evolution (sae): Security architecture; (release 8). 2009.

[9] Mustaque Ahamad, Dave Amster, Michael Barrett, Tom Cross, George Heron, Don Jackson, Jeff King, Wenke Lee, Ryan Naraine, Gunter Ollmann, et al. Emerging cyber threats report for 2009. 2008.

[10] Alanoud Al Mazroa and Mohammed Arozullah. Detection and remediation of attack by fake base stations in lte networks.

[11] ALCATEL-LUCENT. Motive security labs malware report - h2 2014. Technical report, 2014.

[12] M Junaid Arshad, Amjad Farooq, and Abad Shah. Evolution and development towards 4th generation (4g) mobile communication systems. *Journal of American Science*, 6(12):63–68, 2010.

[13] David Banisar and Simon G Davies. Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *John Marshall Journal of Computer & Information Law*, 18(1), 1999.

[14] Michel Barbeau and Jean-Marc Robert. Rogue-base station detection in wimax/802.16 wireless access networks. In *Annales des télécommunications*, volume 61, pages 1300–1313. Springer, 2006.

[15] Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of gsm encrypted communication. In *Advances in Cryptology-CRYPTO 2003*, pages 600–616. Springer, 2003.

[16] Christian R Berger, Shengli Zhou, Yonggang Wen, Peter Willett, and Krishna Pattipati. Optimizing joint erasure-and error-correction coding for wireless packet transmissions. *Wireless Communications, IEEE Transactions on*, 7(11):4586–4595, 2008.

[17] Zhengjun Cao. Eavesdropping or disrupting a communication-on the weakness of quantum communications. *IACR Cryptology ePrint Archive*, 2013:474, 2013.

[18] John Chapin and William Lehr. Mobile broadband growth, spectrum scarcity, and sustainable competition. TPRC, 2011.

[19] Luis M Correia. *Mobile broadband multimedia networks: techniques, models and tools for 4G*. Academic Press, 2010.

[20] Christopher Cox. *An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications*. John Wiley & Sons, 2012.

[21] Erik Dahlman, Stefan Parkvall, Johan Skold, and Per Beming. *3G evolution: HSPA and LTE for mobile broadband*. Academic press, 2010.

[22] Deepti and Deepika Khokhar. Detection of rogue base stations in wimax/ieee802.16 using sensors. *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN*, 3(4), 2012.

[23] Deepika Khokhar Deepti and Satinder Pal Ahuja. “a survey of rogue base station attacks in wimax/ieee802. 16. *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN*, 2277, 2012.

[24] Netmanias LTE Technical Documents. Lte security i: Concept and authentication.

[25] Netmanias LTE Technical Documents. Lte security ii: Nas and as security.

[26] Alexis Dowhuszko and Jyri 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.

[27] Alan W Ezekiel. Hackers, spies, and stolen secrets: Protecting law firms from data theft. *Harv. JL & Tech.*, 26:649, 2012.

[28] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[29] Christoph Hanser, Simon Moritz, Farjola Zaloshnja, and Qin Zhang. Security in mobile telephony: The security levels in the different handy generations.

[30] Henry Haverinen, Jouni Mikkonen, and Timo Takamäki. Cellular access control and charging for mobile operator wireless local area networks. *Wireless Communications, IEEE*, 9(6):52–60, 2002.

[31] Jyri 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.

[32] Abbas Jamalipour. The wireless mobile internet. *John Wiley & Sons Ltd*, pages 368–384, 2003.

[33] Chris Johnson. Non-access stratum. *Radio Access Networks for UMTS: Principles and Practice*, pages 231–247.

[34] Audun Jøsang, Laurent Miralabé, and Léonard Dallot. It's not a bug, it's a feature: 25 years of mobile network insecurity.

[35] Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siamk Naghian, and Valtteri Niemi. Umts networks. *Architecture, Mobility and Services. Wiley*, 2001.

[36] Farooq Khan. *LTE for 4G mobile broadband: air interface technologies and performance*. Cambridge University Press, 2009.

[37] Lars R Knudsen and Matthew JB Robshaw. Brute force attacks. In *The Block Cipher Companion*, pages 95–108. Springer, 2011.

[38] GM Køien. Overview of umts security for release 99. *Feature: Broadband Radio Access*, page 102, 2000.

[39] Juha Korhonen. *Introduction to 3G mobile communications*. Artech House, 2003.

[40] Umesh Kumar and Sapna Gambhir. A literature review of security threats to wireless networks. *International Journal of Future Generation Communication and Networking*, 7(4):25–34, 2014.

[41] Jaana Laiho, Achim Wacker, and Tomáš Novosad. *Radio network planning and optimisation for UMTS*. John Wiley & Sons, 2006.

[42] Christopher Low. Understanding wireless attacks & detection. *GIAC Security Essentials Certification (GSEC) Practical Assignment Version*, 1, 2005.

[43] Merritt Maxim and David Pollino. *Wireless security*. McGraw-Hill/Osborne, 2002.

[44] Ulrike Meyer. *Secure roaming and handover procedures in wireless access networks*. PhD thesis, TU Darmstadt, 2006.

[45] Michel Mouly, Marie-Bernadette Pautet, and Thomas Foreword By-Haug. *The GSM system for mobile communications*. Telecom Publishing, 1992.

[46] Valtteri Niemi and Kaisa Nyberg. *UMTS security*. John Wiley & Sons, 2003.

[47] Karsten Nohl. Attacking phone privacy. *Black Hat USA*, 2010. BlackHat 2010 Lecture Notes , https://srlabs.de/blog/wp-content/uploads/2010/07/Attacking.Phone_.Privacy_Karsten.Nohl_1.pdf.

[48] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. Long-term effects of ubiquitous surveillance in the home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 41–50. ACM, 2012.

[49] Matthew Phelan. Rogue "interceptor" cell phone towers discovered near u.s. army bases, March 2014. http://blackbag.gawker.com/rogue-interceptor-cell-phone-towers-discovered-near-u-1630079351, Retrieved 9/06/2015.

[50] Fabio Ricciato, Angelo Coluccia, and Alessandro D'Alconzo. A review of dos attack models for 3g cellular networks from a system-design perspective. *Computer Communications*, 33(5):551–558, 2010.

[51] KW Richardson. Umts overview. *Electronics & Communication Engineering Journal*, 12(3):93–100, 2000.

[52] Kari Rikkinen, Kalle Ahmavaara, Mikko Rinne, and Mika Rinne. Method for radio resource control, February 29 2000. US Patent 6,031,827.

[53] John Scourias. *Overview of GSM: The global system for mobile communications*. University of Waterloo, Computer Science Department, 1996.

[54] SecUpwN. Android imsi catcher, December 2014. http://secupwn.github.io/Android-IMSI-Catcher-Detector/, Retrieved 18/05/2015.

[55] Technical Specification Group Services and System Aspects (TSG SA WG3). 3rd generation partnership project; technical specification group services and system aspects; 3g security; cryptographic algorithm requirements (3g ts 33.105 version 1.0.0). Technical report, June 1999. 3G TS 33.105 V1.0.0.

[56] Ramanpreet Singh and Sukhwinder Singh. Detection of rogue base station using matlab. *International Journal of Soft Computing and Engineering, ISSN*, pages 2231–2307, 2011.

[57] Yubo Song, Kan Zhou, and Xi Chen. Fake bts attacks of gsm system on software radio platform. *Journal of Networks*, 7(2):275–281, 2012.

[58] Yubo Song, Kan Zhou, and Xi Chen. Fake bts attacks of gsm system on software radio platform. *Journal of Networks*, 7(2):275–281, 2012.

[59] Eric Southern, Abdelkader Ouda, and Abdallah Shami. Wireless security: securing mobile umts communications from interoperation of gsm. *Security and Communication Networks*, 6(4):498–508, 2013.

[60] SRLabs. Snoopsnitch, December 2014. https://opensource.srlabs.de/projects/snoopsnitch, Retrieved 21/05/2015.

[61] CISCO SYSTEMS. Visual networking index: Global mobile traffic patterns, 2013-2017.

[62] Chunyu Tang, David A Naumann, and Susanne Wetzel. Analysis of authentication and key establishment in inter-generational mobile telephony.

[63] TeleGeography:authoritative telecom data. Globalcomms forecast service, 2015.

[64] Olav 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.

[65] TSB. Mobile network codes (mnc) for the international identification plan for public networks and subscriptions (according to recommendation itu-t e.212 (05/2008)) (position on 1st january 2013). http://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.212B-2013-PDF-E.pdf, Retrieved 18/06/2015.

[66] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[67] Toby Velte and Anthony Velte. *Cisco: a beginner's guide*. McGraw-Hill, Inc., 2006.

[68] Joseph Verble. The nsa and edward snowden: surveillance in the 21st century. *ACM SIGCAS Computers and Society*, 44(3):14–20, 2014.

A Eira: Data collection site

Here are the Lists of observed Embassies in the Eira part of Helsinki, Finland. One of the three locations visited during the practical measurement phase.

- Embassy of Italy (Itäinen Puistotie 4, 00140 Helsinki (60.1588545, 24.9577421))
- Embassy of USA (Itäinen Puistotie 14 A, 00140 Helsinki (60.1571107, 24.9606093))
- Embassy of France (Itäinen Puistotie 13, 00140 Helsinki (60.1568308, 24.9602479))
- Embassy of Japan (Unioninkatu 20-22, 00130 Helsinki (60.1660545, 24.950773))
- Embassy of Brazil (Itäinen Puistotie 4 B 1, 00140 Helsinki (60.1589244, 24.9574973))
- Embassy of Belgium (Kalliolinnantie 5, 00140 Helsinki (60.158505, 24.9596014))
- Embassy of Estonia (Itäinen Puistotie 10, 00140 Helsinki (60.1578404, 24.9594198))
- Embassy of Kazakhstan (Unioninkatu 24, 00130 Helsinki (60.1663084, 24.9506673))
- Embassy of South Africa (Pohjoinen Makasiinikatu 4, 00130 Helsinki (60.16552, 24.9510308))
- Embassy of Turkey (Puistokatu 1 B A 3, 00140 Helsinki (60.1585628, 24.9538638))

B Kulosaari: Data collection site

This were the observed Embassies in the Kulosaari part of Helsinki, Finland. The second location visited during the practical data capturing phase.

- Embassy of China (Vanha Kelkkamäki 9-11, 00570 Helsinki (60.18303, 25.005794))
- Embassy of Iran (Kulosaarentie 9, 00570 Helsinki (60.1840489, 25.0052605))
- Embassy of Vietnam (Kulosaarentie 12, 00570 Helsinki (60.1844906, 25.0041641))
- Embassy of India (Kulosaarentie 32, 00160 Helsinki (60.1842178, 25.0091695))
- Embassy of Ukraine (Vahaniityntie 9, 00570 Helsinki (60.185278, 25.0176697))
- Embassy of Serbia (Kulosaarentie 36, 00570 Helsinki (60.184102, 25.0096631))
- Embassy of Iraq (Lars Sonckin tie 2, 00570 Helsinki (60.1835136, 25.0138013))

C Kuusisaari: Data collection site

This are the lists of Embassies observed in the third and final location where practical measurement was carried out. It is called Kuusisaari, in the western part of Helsinki, Finland.

- Embassy of Indonesia (Kuusisaarentie 3, 00340 Helsinki, (60.187327, 24.868043))
- Embassy of Germany (Krogiuksentie 4, 00340 Helsinki, (60.185989, 24.867097))
- Embassy of Bulgaria (Kuusisaarentie 2B, 00340 Helsinki, (60.186925, 24.870268))
- Embassy of Japan (Kuusisaarentie 6, 00340 Helsinki, (60.186501, 24.868699))
- Residence of the Ambassador of Iran (Kuusisaarentie 4, 00340 Helsinki, (60.186640, 24.869764))
- Residence of the Ambassador of Korea (Hirvilahdenkuja 5, 00340 Helsinki, (60.189031, 24.867320))