STUDY OF SECURITY IN 5G MOBILE NETWORKS AND ATTACK VECTORS ON SUBSCRIBER IDENTITIES

Gallego Vara, Miguel
ICAI
Ethon Shield
Madrid, Spain

July 2021

***Abstract*— 5G technology promises to be the solution to the great demand for services not only from the industry but also from ordinary users. The speeds that devices connected to these mobile networks will be able to reach will far exceed those provided by its predecessor, the fourth generation, allowing not only Internet access to users with cell phones but also to IoT devices, cars or industrial machinery, communicating in real time. Over the last few years, there has been much speculation about the security of this new technology, questioning its improvement. Therefore, one of the objectives of this paper is to display the overall security of 5G compared to previous technologies. Furthermore, this project has focused on one of the most renowned attacks on mobile technologies: the IMSI Catcher. The purpose of this attack is to steal the subscriber's identity in order to determine its location, in addition to being able to perpetrate numerous other attacks based on obtaining this number. Pre-5G technologies were vulnerable to these attacks because they sent the customer's identity in plane text, so with knowledge of the various network access procedures, it was possible to attack these vulnerabilities. This attack will be tested in the two main deployments that the fifth generation has, both 5G-NSA and 5G-SA.**

Keywords *– 5G, 4G, IMSI, NSA, SA, gNB, eNB, NG, SDR, OAI, 3GPP, USIM, UE, SUPI, SUCI*

I. INTRODUCTION

The fifth generation of mobile networks is expected to be a revolution in telecommunications, allowing all types of equipment to be connected to the Internet or the cloud, and to talk to each other in real time with almost no latency. The standards ensure that browsing speeds will be so high that it will be possible to download a movie in a matter of seconds. However, the big revolution has not been exclusively in the use of high frequencies to increase data transmission speeds; a major innovation is also coming from a term that is becoming more and more familiar in the telecommunications world: virtualization. SDN and NFV are virtualization architectures that move the hardware away from the networks, replacing it with software, favoring greater flexibility and scalability of these, and being able to specify the users' quality of service selectively. This will make it possible to dynamically manage data flows at off-peak and peak times, similar to what is done in the electricity sector, considerably reducing the possibility of network saturation and modifying these flows depending on the geographical mobility of subscribers. Thus, in summer, when the population in Spain generally moves to the coast, it will be possible to transfer capacities to these geographical areas.

The objectives of 5G are multiple, among them we find:

- Enabling the advancement of the Internet of Things (IoT)
- Enable much higher availability, very low latency and very high mobility
- Significantly improve data transmission speeds
- Consolidate new industrial network customers

II. ARQUITECTURE

The structure of 5G networks, like their predecessors, are divided into three main components:

- **UE**: Device that has the SIM card that uniquely identifies the customer. In previous technologies they have always corresponded to cell phones or tablets, but from now on they may range from cars to machinery in the industrial sector.
- **NG-RAN**: The radio access network, the architecture that has been considerably modified to increase upload and download speeds, with the use of high frequencies. The node that is responsible for communicating with the UE is called the gNB, similar to the eNB of 4G-LTE.
- **NG-MC:** This is the core of the network where multiple functionalities are combined, including: providing communication with the Internet, enabling user mobility and billing. All this while ensuring security and QoS.

A. RAN

The RAN is the part of the mobile network that communicates with customers through the radio (air) interface, being the intermediary between them and the network core. The main components of the RAN include base stations and antennas that provide coverage to a region or cell.

Base stations in 5G are known as gNodeB - gNB. In the downstream direction, when the network core wants to communicate with the UE, these base stations generate the necessary fragments and schedule them for respective transmission over the air interface. On the other hand, when the UE wants to access the Internet, they convert the physical layer segments into IP fragments and redirect them to the user plane of the network core.

These base stations communicate via interfaces with the following nodes, as shown in Figure 1:

- Network core (AMF/UPF): NG-C/U interface.

- Other base stations (gNBs): Interface Xn
- Network subscribers (UE): Interface Uu

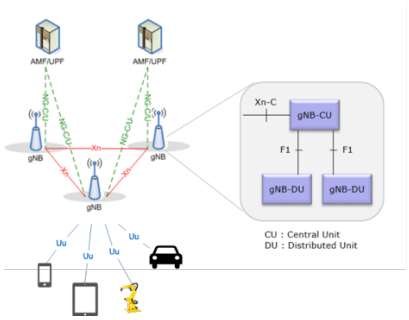

Figure 1: 5G RAN Architecture [1]

B. Mobile Core

The network core is the central part of a network that provides services to users, including traffic routing, authentication and charging. In 4G it was called EPC and in 5G it was renamed NG-Core (Next Generation Core). Virtualization will play a significant role in the development of this infrastructure since many of the network functions can be deployed on dedicated servers via software.

Some of the most important functions performed in the core of a mobile network are as follows:

- Routing of network traffic
- Connection to an external data network such as the Internet
- Pricing policies
- User mobility management
- Telephone calls
- Roaming
- Providing security through mechanisms such as customer identification and authentication or encryption of communications.

Although new functionalities have been added in 5G networks, there are certain nodes that have to exist in any deployment:

- **AMF**: It could be compared to the MME of 4G - LTE, the brain of the network. It is in charge of user authentication, mobility and location services. Unlike the MME, the AMF is not in charge of managing user sessions, forwarding this information to the SMF.
- **SMF:** Handles the session of each UE by assigning IP addresses, roaming functionalities or DHCP functions.
- UPF: Handles packet forwarding between the radio node and the Internet, user plane QoS or reports traffic usage.
- **UDM:** Manages user identity, such as the generation of authentication credentials, thus sharing part of the functions that the HSS node had in 4G-LTE or network permissions.
- **AUSF:** It could be compared to the HSS of 4G-LTE, a database that acts as an authentication server. Processing the credentials generated by the UDM, it authenticates the user who is trying to register.
- **UDR:** Database in charge of storing several types of data, including the user's subscription and pricing policies. This function provides its data to other functions such as the UDM or the PCF.

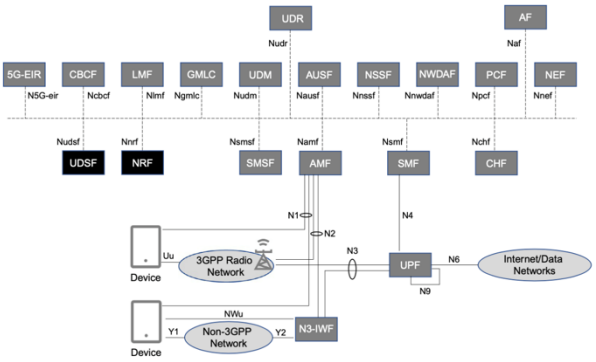

Figure 2: 5G Mobile Core [2]

These functions will communicate with each other using HTTP REST interfaces, standards that define how web pages interact through the use of APIs. The most important requests in this paradigm are the following:

- **GET:** get information from a server without modifying the data.
- **POST:** send information to a server
- **PUT:** modify existing information from a server
- **DELETE:** delete information from a server

C. 5G Deployments

With the existence of 4G infrastructure deployed globally, it is necessary to consider the issue of the transition to 5G. 3GPP proposes multiple 5G network deployment scenarios that fall into two main categories: NSA and SA. Regarding Figure 3, options 1, 2 and 5 belong to SA deployment while options 3, 4 and 7 belong to NSA deployment.

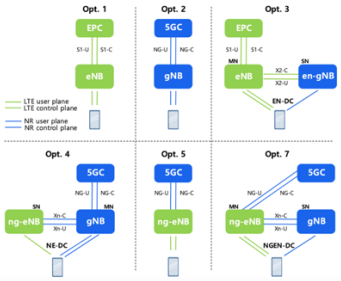

Figure 3: 5G deployment options [3]

1) NSA deployment

This deployment enables 5G by building on the existing 4G-LTE infrastructure. Since it relies on the previous technology, the UE can connect to both the eNB and the gNB radio node. Between these two nodes, one of them acts as the master node, while the other is called the secondary node.

- **Option 3:** As shown in Figure 3, the gNB node is connected to the eNB node, which in this case would be the master, and the latter is connected to the network core, belonging to the 4G infrastructure. This option is preferable for operators that have a very wide deployment of 4G nationwide since it allows an easy

migration to 5G features by installing only the radio nodes. However, on the downside, only the new RAN capabilities provided by the gNB can be leveraged.

- **Option 4:** In this case, unlike Option 3, the master node would be the gNB that is connected to the 5G core. In this option, the eNB node has to be upgraded to ng-eNB to be able to interact with the new radio node.
- **Option 7:** This option is identical to Option 4 except that now, the master node is the ng-eNB since it is the one connected to the network core.

2) SA deployment

Finally, and much more recently, 5G-SA networks have been defined. As the name suggests, this type of network will be completely 5G. Therefore, both the radio infrastructure and the core of the network will have to be implemented. Today it is practically impossible to find any commercial 5G-SA network, since part of the standards are still being defined, although it is true that some pilot networks have been developed. Regarding the types of deployments, we find the following options:

- **Option 2:** This option is completely 5G, since no node belonging to the previous technology appears. As can be seen, there is only the radio node, gNB, which is connected to the new core, the NG-MC.
- **Option 5:** In this option, the enhanced node ng-eNB is the one connected to the NG-MC. However, there is no gNB node. This allows the new network core functions to be used, but the capabilities of the radio node, such as the use of millimeter frequencies, are not implemented.

III. CURRENT STATUS OF 5G NETWORKS

A. Frequency Licensing

There are two main frequency bands:
- FR1 (Frequency Range 1): 410 MHz - 7 125 MHz
- FR2 (Frequency Range 2): 24 250 MHz - 52 600 MHz

In the first range there are frequencies that are already used in other technologies such as GSM 900, DCS or LTE. However, a percentage of this bandwidth is expected to be used by 5G over the next few years. The second group of frequencies, FR2, is known as mmWave due to its millimeter nature. In this frequency range, the coverage is much smaller but the data transmission speed increases considerably.

Based on the Spanish National 5G Plan proposed by the Ministry of Energy, Tourism and Social Agenda, within the two frequency bands three relevant ranges are identified:
- 3.4 GHz - 3.8 GHz band will be considered as the main band to initiate communications throughout Europe.
- 694 MHz - 790 MHz band as the 5G band with superior coverage range and wall penetration, providing higher quality of service.
- 24.25 GHz - 27.5 GHz band as the first range within the millimeter frequencies to be deployed, with a much more limited coverage range, but very high data rates.

The current status of these ranges is as follows:

3.4 GHz - 3.8 GHz band:

- 3.4 GHz - 3.6 GHz band: These were auctioned at the turn of the century to encourage the development of technologies such as LMDS or WiMax. Although they were awarded to operators that no longer exist, the bandwidths became part of today's large operators. There were 40 MHz belonging to the Ministry of Defense, and 20 MHz were auctioned in February 2021 and fell into the hands of Movistar and Orange. In addition, the 3480 MHz to 3500 MHz range will be migrated to the lower part of the spectrum and cannot be used to not interfere with NATO communications that use frequencies just below 3400 MHz. Finally, for efficiency reasons, in the coming years this band will be reorganized to allow operators to use carriers with more bandwidth.
- 3.6 GHz - 3.8 GHz band: This range was awarded in 2018 to carriers. This range was sold in the auction for a total price of €437.65 million and the operators will hold this range for the next 20 years, until 2038.

BAND 3600-3800					
Auction			Reorganization		
Frequencies (MHz)		Operator	Frequencies (MHz)		Operator
3600	3610	Vodafone	3600	3660	Orange
3610	3620	Movistar	3660	3750	Vodafone
3620	3640	Orange	3750	3800	Movistar
3640	3650	Vodafone			
3650	3660	Orange			
3660	3670	Vodafone			
3670	3680	Orange			
3680	3720	Movistar			
3720	3780	Vodafone			
3780	3800	Orange			

BANDA 3400-3600		
Frequencies (MHz)		Operator
3400	3440	Mas movil
3440	3460	Movistar
3460	3480	Orange
3480	3500	Ministerio de Defensa
3500	3540	Mas movil
3540	3560	Movistar
3560	3580	Orange
3580	3590	Movistar
3590	3600	Orange

700 MHz band

It was used for Digital Terrestrial Television (DTT), so it has had to be released over the last few years to avoid interferences. DTT will move from the 700 MHz band to the 600 MHz band. This band will be auctioned in July 2021. This range, since its penetration will be the highest of the main 5G frequencies, is expected to be the most expensive in history. The Spanish government has already launched the auction with a starting price of €995.5 million.

Band 24.25 - 27.5 GHz

This band currently has three blocks available for immediate use. The other part of the spectrum is used for radio links or suffers from limitations.
However, the National Frequency Allocation Table has set a deadline of December 31, 2021 for this range to be released.

B. Current implementation

This project also wanted to check the state of implementation of 5G networks, both NSA and SA. In order to perform this test, a 5G terminal was used, specifically, the Oppo Reno 4z 5G, with its corresponding SIM card. Several applications were installed to track the identifiers of the cells to which the cell phone was connected, its location, technology and transmission speed. Specifically, GNet-Track, Network Signal Info and LTE Signalling were used.

Then, a wardriving was performed in different areas of the Community of Madrid to obtain the information of the different cells and to which technology they belonged, obtaining the heat map shown in Figure 4. This heat map represents the 5G cells found from the Movistar operator, from which only 5G NSA traces were obtained, except in the Telefónica district located in the M-40, where 5G-SA was obtained.

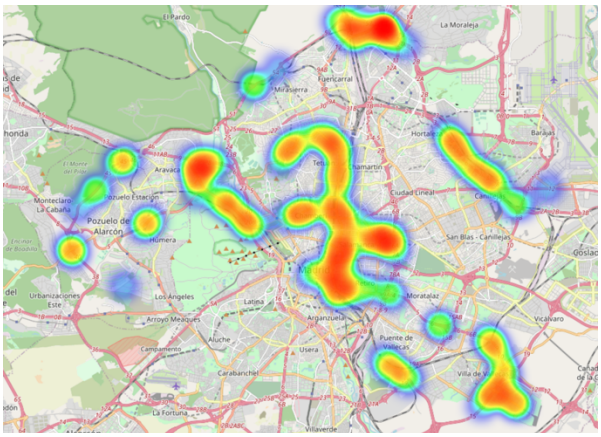

Figure 4: Madrid 5G heatmap

IV. 5G Security

5G will connect thousands of devices in a very complex network, so the attack surface will be much larger. Not only that, but these networks will support critical infrastructure and an attack on this infrastructure could have a much greater impact on society than in other technologies. It is therefore necessary to place special emphasis on research and highlight the security challenges in this type of mobile networks.

The new aspects to be taken into account for securing 5G networks would be the following:

- User privacy
- Security of virtualization: SDN and NFV
- Security of the thousands of new connected devices

A. USER PRIVACY

One of the big problems of pre-5G generations was the aforementioned fake stations, or IMSI Catchers, since the identity of the device was sent in clear text. This is because the identification process occurred without any ciphering. Fortunately, this vulnerability has been addressed in 5G.

The unique identifier in 5G technology is called SUPI, and this should not be sent directly in clear text, as detailed in the 3GPP TS 33.501 specification, "SUPI should not be transferred in clear text over NG-RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC)." [4] The only exception will be emergency calls where authentication would not be necessary, and in this case the IMEI will be sent in clear text.

The SUPI can have two values:

- IMSI: just like the previous technologies. This is composed of the following parameters:
  - MCC - 3-digit number identifying the user's country of domicile.
  - MNC: 2 to 3 digit number that identifies the user's operator.
  - MSIN: User identification number within the network.
- NAI: this value is in the form of username@realm, defined in the RFC-4282 specification [5].

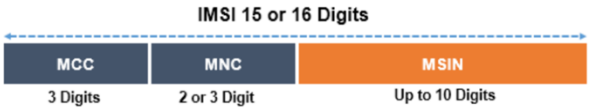

Figure 5: SUPI [6]

In order not to transfer the SUPI in clear text, an encrypted identity known as SUCI is used. If the network is secure, there will be a public/private key pair from the operator and the public key will be stored in the UE's factory SIM card, so that the SUCI can be sent securely for subsequent authentication of the user.

The SUCI consists of the following parameters:

- SUPI Type - Value between 0 and 7, which identifies the type of SUPI stored.
  - 0: IMSI
  - 1: NAI
  - 2 to 7: Values for possible future uses
- Home Network Identifier - Identifies the user's home network.
- Routing Indicator - 1 to 4 decimal places assigned by the operator
- Protection Scheme Identifier
  - Null - No protection exists so the SUPI is transferred in clear text, i.e. in the Scheme Output the MSIN is transferred.
  - Profile A
  - Profile B
- Home Network Public Identifier - Consists of a public key of the operator. If the Protection Scheme Identifier is null, this value is 0.
- Protection Scheme Output - The clear or encrypted value of the SUPI MSIN.

In the Protection Scheme Identifier there are two possible profiles to use. Both are based on the Elliptic Curve Integrated Encryption Scheme (ECIES), an encryption scheme commonly used in cryptography.

- Profile A
  - ECC 256-bit Public Key
  - Encrypted Text
- Profile B:
  - ECC 264-bit Public Key o Encrypted Text Profile B.
  - Encrypted Text

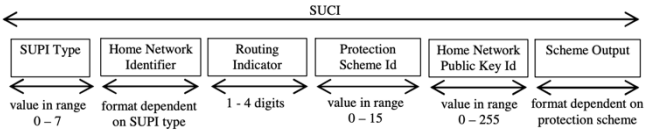

Figure 6: SUCI structure [7]

Therefore, the registration by the subscriber will be done as follows:

1. Registration Request by the UE, in which both the MCC and the MNC and on the other hand the SUCI or the GUTI will be sent in clear text 2.
2. If the SUCI is sent, the network will check which is the SUPI in its database.
3. A temporal identifier is generated and sent to the user.
4. The Registration Request is accepted and the next time the user wants to connect, the temporal identifier will be sent instead of the SUCI.

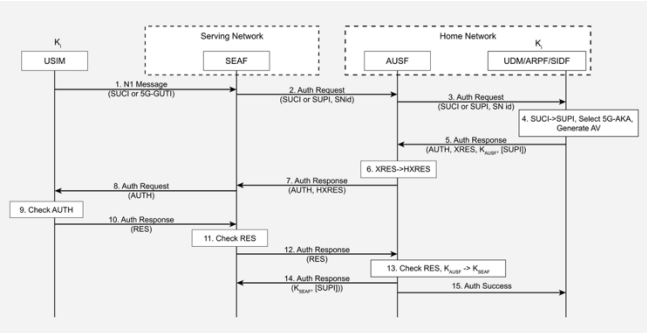

Figure 7: Registration Request procedure [8]

In addition, another feature that prevents SUCI tracking is that the SUCI is not static; in each Identity Response the SUCI sent is modified. This is due to the fact that the SUCI is not only generated using the operator's public key, but also a private key - ephemeral key. The public key of the ephemeral pair is sent through the channel to the home network to use it for the deciphering.

B. VIRTUALIZATION SECUTIRY

One of the great advances and revolution of this new technology is virtualization, which, on the one hand, increases the flexibility and scalability of the network, but on the other, offers a new attack surface.

Although there is a wide range of configuration and deployment possibilities, security standards are being generated that are applicable to all situations, but due to the complexity of these, it is likely that operators will end up protecting their infrastructure in a way that is specific to each deployment. The standards are specified by ETSI, which defines the countermeasures to be applied to virtualization attacks.

The main risks associated with virtualization described by ETSI are as follows:

- Escaping from the virtual machine to the real machine, where control of the network may be obtained.
- Securization and authentication of APIs.
- Isolation of both hardware elements, resources and critical VNFs. If a virtual network element is attacked, this isolation will not allow other devices to remain unaffected.
- In SDN there is generally a controller, so there must be authentication between the controller and the entities under its control since, if the controller is attacked, the entities would be affected.

V. TOOLS

a. *Open Air Interface - OAI*

Open Air Interface Software Alliance is a free software organization focused on the development of Radio Access Network (RAN) and Core Network (CN) projects. Being Open Source, the developer community can collaborate with the projects, accelerating their progress and bringing the industrial community closer to the university and research community. OAI started with the implementation of an LTE network, however, in recent years they have decided to dedicate time to the development of 5G networks, both NSA and SA. The 5G - NSA network is fully developed, as it is supported by a 4G infrastructure. However, as from July 2021, the 5G - SA network is still under development. In this project, the code provided by this organization will be used to build a 5G network and perform different security tests.

b. *SDR*

SDRs are devices that aim to replace hardware with software components. This allows greater flexibility in programming and signal processing and has brought about a revolution in the development and research of mobile networks.

Ettus Research [9] is a company specialized in SDRs and Wireless technology research. The Ettus USRP B200 and B200 mini were used in this project. The USRP B200 has a frequency coverage of 70 MHz to 6 GHz and a bandwidth of 56 MHz. In addition, it has an affordable price for the quality of service. On the other hand, the "light" version of the B200, known as B200 mini, was also used. It has practically the same specifications as the previous one. One of the main differences that the USRP B200 has GPS connector, to stabilize the reference clock, very useful in this kind of experimentations. Many of the projects carried out with Open Air Interface for 5G NSA and SA networks used the USRP B210, in which the main difference is that it is MIMO (Multiple Input Multiple Output) while the aforementioned are SISO (Single Input Single Output).

Figure 9: USRP B200 [9]

Figure 9: USRP B200 mini [9]

c. Sysmocom – SIM Cards

Sysmocom (Systems for Mobile Communications GmbH) is a company that develops telecommunications products and services and free software.

In the case of this project, SIM cards - sysmoISIM-SJA2 - were used. These cards are the evolution of the sysmoUSIM-SJS1, cards used for 2G, 3G and 4G technologies; in which the following aspects relevant to this project have been added and improved:

- Addition of the ISIM application for IMS/VoLTE to part of SIM + USIM.

These SIM cards have the ability to be reprogrammed using an open source program developed by sysmocom, specified in its manual. [10]

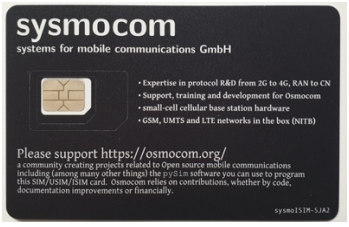

Figure 10: Sysmocom SIM card [11]

VI. IMSI-CATCHERS

An IMSI Catcher is an attack to intercept the IMSI during the network attachment procedure in order to track the user's location, or even intercept text messages, calls or traffic. Obtaining the IMSI is therefore considered a critical vulnerability.

The idea behind this attack is to simulate a mobile network or base station and make the subscriber try to connect to this network. It is not even necessary to connect since only the IMSI will be needed to authenticate the user and the user will not be registered in the database and will be rejected. These devices first appeared in the 1990s but they were large, heavy and expensive. However, over the years, with the arrival of free software and SDRs, IMSI Catchers can now be made for a very modest price.

There are several ways for a user to attempt to connect to the fake base station. First, propagate a radio signal with more power and the UE will try to connect, as long as the operator's data matches the SIM card. Another way would be to inhibit the frequencies of the target technology and thus force the UE to scan all frequencies again.

IMSI Catchers have been around since 2G technology, where security is weak and mobile devices connect to "any" network. Their successors, both 3G and 4G, implement temporary identifiers, but on several occasions the IMSI has to be sent in clear text. Therefore, IMSI Catchers also work on these technologies.

VII. PROPOSED SOLUTION

The standard establishes requirements for laboratory experiments with SDRs and mobile technologies, including the use of a Faraday box. This is because the frequencies used could interfere with other users near the devices and they could be affected. The Faraday box acts as an environment in which no radio frequencies can enter or leave, so the network would be completely isolated.

Figure 11: Faraday cage

A. SOFTWARE AND HARDWARE REQUIREMENTS

OAI required a minimum to be able to install its software and run it without problems. For the hardware it required hosts with Intel processors for DSP functions that make use of SIMD instructions. The supported software was:

- Generations 3/4/5/6 Intel Core i5,i7
- Generations 2/3/4 Intel Xeon
- Intel Atom Rangeley, E38xx, x5-z8300

In addition, a minimum of 4 cores and a minimum Ubuntu version of 16.04 were required for the git branches used.

SDRs supported: USRP B210, USRP X310, BladeRF, LimeSDR and EURECOM EXPRESSMIMO2 RF

The commercial UE's that had been tested were as follows: Oppo Reno 5G, Samsung A90 5G, Samsung A42 5G, Google Pixel 5G (note1), Simcom SIMCOM8200EA and the Quectel RM500Q-GL.

3) NSA

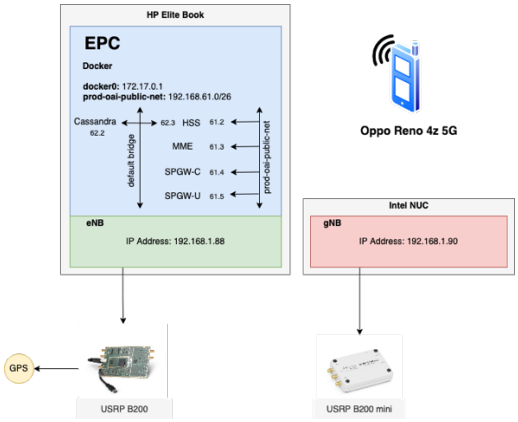

Figure 12: NSA Architecture

First, before installing the software, several hosts with certain requirements were needed. As can be seen in Figure 12, in this project two different hosts were used, one for the EPC and eNB and another for the gNB.

It was decided to have this architecture to save resources, since the documentation provided by OAI used three hosts, one for each node. The following table details the specifications of the computers used for the experimentation.

Node	eNB y docker	gNB
Model	HP EliteBook 2570p	Intel NUC
CPU	Intel® Core™ i5-3340M CPU @ 2.70 GHz	Intel® Core™ i7-10710U CPU @ 1.10GHz
Memory	256 GB	120 GB
OS	Ubuntu 18.04 LT 64 bits	Ubuntu 18.04 LT 64 bits
Kernel	5.4.0-77-generic	4.15.0-147-generic
USB Version	3.0	3.0

Table 1: Hosts specifications for NSA architecture

On the other hand, as for the SDRs, there were several alternatives, but finally a USRP B200 and a USRP B200. For the UE, an Oppo Reno 4z 5G was used.

For the simulation of a 5G NSA laboratory network, the following steps were followed (explained in detail in [12]):

1. First, required for the network core configuration (EPC), docker was installed
2. The source code was downloaded from the corresponding repositories. In this case, two repositories were needed:
   a. One for the EPC [13] in the tag: ***2021.w06***
   b. One for the eNB and gNB nodes [14] in the *develop* branch with a corresponding tag.[1]
3. To configure the EPC it was first necessary to download the images of the following nodes: Cassandra, HSS, MME, SPGWC and SPGWU
4. These images were configured accordingly
5. The eNB and gNB nodes were configured to be able to communicate between them.
6. The SDRs were connected to the corresponding hosts. It is necessary to connect them to a USB 3.0.
7. Run the network core through docker.
8. Run eNB
9. Run the gNB

Once executed, the radio nodes will communicate with each other with a first message in which the gNB makes itself known.

When a UE attempts to connect to the eNB, the following message will be received:

```
[RRC] [FRAME 00218][eNB][MOD 00][RNTI
c63a] Accept new connection from UE
random UE identity (0xf106d192d1000000)
MME code 0 TMSI 0 cause 3.
```

This message corresponds to the RRC Connection Request. As you can see, since this is the first time the UE tries to connect to this network, it will send a random UE identity. Once this connection attempt message has been received, the IMSI sent in the Attach Request is checked in the MME logs.

Whether or not it exists in the database, since it is the first time you are trying to connect to this network, you will have to send the IMSI in clear text.

```
000536 00049:345289 7F5F188FA700 DEBUG
NAS-EM r-
mme/src/nas/emm/emm_data_ctx.c:0197
ue_id=1 set IMSI 901700000013638 (valid)
```

With this message, we now have the user's IMSI and could perpetrate numerous additional attacks.

The project was done in BASH because of its ease in executing operating system commands and coordinating different scripts. It was decided to automate the whole process of starting and stopping the different nodes, both eNB, gNB and the core of the network. Meanwhile, a watchdog was checking if any device had tried to connect to the network. If so, it checked the traces in the EPC to find and determine the client's IMSI.

The IMSIS discovered during the experimentation were stored in a file:

```
2021-07-20 12:44:02 -> Found IMSI:
214075555551043473, MNC: 214, MCC: 07
```

4) SA

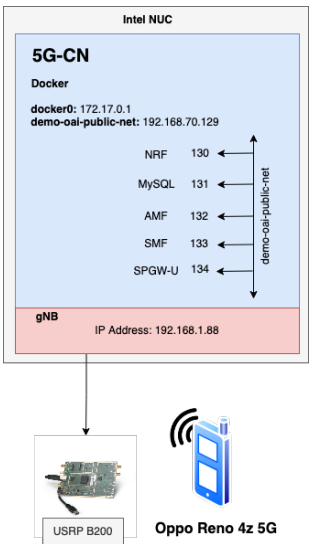

Figure 13: SA Architecture

For the execution of the SA deployment, the following steps were followed (explained in detail in [15]):

1. First of all, docker was installed, which is necessary for the execution of the core nodes of the network.
2. Downloaded the source code of the gNB node.

[1] *f21ac1a84ca7bfa0c19e46b50b02b5078c18c427*

3. The images of the main nodes were downloaded: AMF, SMF, NRF and SPGWU. Unlike EPC, images were configured using the docker-compose.yaml file.
4. Download the source code for the 5G core, using the corresponding sha1[2] and synchronize the components.
5. Once all components were installed, they were run in the corresponding order.
    a. First, the network core
    b. Secondly, the gNB.

For the correct execution of the nodes, it is important that both the gNB configuration file and the amf have the same MCC, MNC and TAC values. In a first instance, the gNB communicates with the AMF by means of the following messages.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
6136	21.094633288	0.000000000	192.168.70.129	192.168.70.132	NGAP	138	NGSetupRequest
6138	21.095831040	0.001197752	192.168.70.132	192.168.70.129	NGAP	574	NGSetupResponse

However, the only communication that existed between the UE and the gNB was the Msg1, the Random Preamble sent by the UE.

Therefore, it was not possible to check the Registration Request with the current version of Open Air Interface.

VIII. CONCLUSIONS

It has been verified that in the 5G-NSA deployment it is possible to perpetrate an IMSI Catcher, concretely in the deployment option where the eNB is the master node and both radio nodes are connected to the 4G core. This is because UE connects with the same procedure as in the previous technology, 4G-LTE. Although in this technology it is true that temporary identifiers such as GUTI are used, if a device connects to a network for the first time, he has to identify itself with the IMSI, sending it in clear text. This makes the interception of this value possible, violating the privacy of users.

However, in 5G-SA it has not been possible to test this because the development by OAI is still very early and the necessary messages, such as the Identity Request/Response in which critical user information is exchanged, have not been reached. Therefore, it will be necessary to wait until an organization such as Open Air Interface finishes implementing the 5G network core and the gNB radio node.

On the other hand, the state of deployment of 5G networks is still at a very early stage. If 5G deployments exist, they are of the NSA type, relying on 4G infrastructure. There is still a lot of investment and development to be done before the new infrastructure is deployed by operators as the specifications are still under development.

Another thought regarding 5G is whether operators will develop their infrastructure with virtualization in mind. Although it is true that this reduces costs considerably, both SDN and NFV are premature and complicated technologies to develop. In addition, there are no standards that operators can follow to implement their infrastructure due to the infinite possibilities in the deployments. Therefore, the implementation of these virtualization technologies is still up in the air.

A. Future studies

Future studies will focus on checking whether the specifications described by 3GPP will be met at a practical level or not, whether the IMSI Catcher can be implemented in the 5G - SA deployment. This can be done in several ways. Wait for OAI or other free software such as srsRAN to develop 5G-SA or use a commercial solution such as Amarisoft's Callbox series, since it includes both the core network and the radio nodes. It will have to be checked which 3GPP Release has been used in the product and see if there are any changes regarding security in subsequent releases.

[2] *51bf03b84327b402afbf2068e1b186a4b12796ec*

REFERENCES

[1] ShareTechnote, «5G/NR - RAN Architecture,» [En línea]. Available: https://www.sharetechnote.com/html/5G/5G_RAN_Architecture.html.

[2] P. H. M. O. L. F. S. S. C. M. Stefan Rommer, 5G Core Network Powering Digitalization, ELSEVIER, 2020.

[3] SAMSUNG, «5G Standalone Architecture».

[4] ENISA, «Security in 5G Specifications,» 2021.

[5] «The Network Access Identifier,» [En línea]. Available: https://datatracker.ietf.org/doc/html/rfc4282.

[6] «5G Identifiers SUPI and SUCI,» 2019. [En línea]. Available: https://www.techplayon.com/5g-identifiers-supi-and-suci/.

[7] ETSI, «Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification».

[8] «A Comparative Introduction to 4G and 5G Authentication,» 2019. [En línea]. Available: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication.

[9] «Ettus Research - A National Instruments Brand,» [En línea]. Available: https://www.ettus.com/.

[10] H. Welte, *sysmoUSIM / sysmoISIM User Manual,* 2021.

[11] [En línea]. Available: http://shop.sysmocom.de/products/sysmoISIM-SJA2.

[12] «OAI NSA SETUP COTS UE TESTING,» [En línea]. Available: https://gitlab.eurecom.fr/oai/openairinterface5g/-/blob/develop/doc/TESTING_GNB_W_COTS_UE.md.

[13] «OPEN AIR INTERFACE / oai-epc,» [En línea]. Available: https://github.com/OPENAIRINTERFACE/openair-epc-fed/blob/2021.w06/docs/DEPLOY_HOME.md.

[14] «OPEN AIR INTERFACE,» [En línea]. Available: https://gitlab.eurecom.fr/oai/openairinterface5g.

[15] «OAI - oai-cn5g-fed,» [En línea]. Available: https://gitlab.eurecom.fr/oai/cn5g/oai-cn5g-fed/-/blob/master/docs/DEPLOY_HOME.md.

[16] «Características técnicas Oppo Reno 4 Z 5G,» [En línea]. Available: https://www.smart-gsm.com/moviles/oppo-reno-4-z-5g.