UNIVERSIDAD DE VALLADOLID

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN

TRABAJO FIN DE Máster

Máster EN INGENIERÍA DE TELECOMUNICACIÓN

Seguridad en dispositivos móviles

Autor:

D. Adrián Rojo Becerril

Tutor:

D. Rubén Mateo Lorenzo

Valladolid, 21 de septiembre de 2021

TÍTULO:	**Seguridad en aplicaciones móviles**
AUTOR:	**D. Adrián Rojo Becerril**
TUTOR:	**D. Álvaro Castellanos Andrés**
	D. Rubén Mateo Lorenzo
DEPARTAMENTO:	**Departamento de Teoría de la Señal y Comunicaciones e Ingeniería Telemática**

TRIBUNAL

PRESIDENTE:	**Dra. Dª. Patricia Fernández Reguero**
VOCAL:	**Dr. D. Ramón Durán Barroso**
SECRETARIO:	**Dr. D. Ramón de la Rosa Steinz**
SUPLENTE:	**Dr. D. Javier Aguiar Pérez**
SUPLENTE:	**Dr. D. Ignacio de Miguel Jiménez**

FECHA:	**16 de septiembre de 2021**
CALIFICACIÓN:	

En colaboración con Orange España.

"*Per Aspera Ad Astra*"

Séneca

Agradecimientos

Quiero agradecer a mis tutores, Álvaro y Rubén por su supervisión y valiosos consejos. Y al resto de gente de Orange por la oportunidad de realizar este proyecto.

A mi familia, por estar siempre ahí apoyando y más concretamente a mis padres, por su dedicación y ayuda.

A mis compañeras del Máster por su imprescindible aliento a largo de este año.

A Daniel, por su indispensable ayuda para afrontar mis estudios.

Y por último agradecer los buenos momentos y el apoyo a mis amigos, tanto los que ya traía como a los que he conocido durante estos cinco maravillosos años.

Gracias a todos, por todo

Palabras Clave

Ciberseguridad, Redes móviles, GSM, UMTS, LTE, 2G, 3G, 4G, 5G, IoT, IMSI, IMSI-Catcher, FPGA, YateBTS, Osmocom, SDR, Yate

Resumen

En este proyecto se aborda cubrir la necesidad detectada en la mitigación de riesgos de seguridad en los usuarios debido a la existencia de los IMSI-Catchers. Este tipo de ataque se basa en obtener el International Mobile Subscriber Identity (IMSI) del usuario con lo que se pueden realizar ataques de tipo Man in the Middle (MitM) a nivel de radio o escucha remota atacando al núcleo de la red vía el protocolo SS7. Además, permite ubicar al usuario y realizar un seguimiento del mismo.

Para ello se ha recopilado información sobre las distintas generaciones de redes de telefonía, detallando su proceso de autenticación, momento en el que son vulnerables a este tipo de ataques. Después se ha profundizado en el funcionamiento del IMSI-Catcher así como investigado que métodos existen para la detección de estos dispositivos. Una vez conocidos los métodos de detección se han recopilado las herramientas disponibles en el mercado para la detección de IMSI-Catchers analizando su funcionamiento.

Posteriormente se ha realizado la implementación de un IMSI-Catcher funcional mediante software definido por radio (SDR) concretamente las FPGA USRP N210 y BladeRFx40 y software de emulación de redes móviles como Osmocom y YateBTS descartando el primero por su complejidad. La celda creada es totalmente funcional, pudiendo realizarse llamadas, así como el envío y recepción de SMS.

Una vez vistas las herramientas y creado un IMSI-Catcher, se ha procedido a evaluar la eficiencia de estas herramientas al poder probarlas con un caso real. Comparando su rendimiento, debemos destacar Cell Spy Catcher por sus buenos resultados, aunque arroja gran cantidad de falsos positivos, no arrojó falsos negativos.

Índice

Índice de Figuras

Índice de Tablas

Glosario y acrónimos

IoT	Internet de las Cosas
5G	Quinta generación de tecnologías de telefonía móvil
GSMA	Asociación GSM
M2M	Machine to machine
IMSI	International Mobile Subscriber Identity
MitM	Man in the Middle
SS7	Sistema de señalización por canal común n.º 7
SDR	Radio definida por software
GSM	Sistema global para las comunicaciones móviles
SMA	SubMiniature version A
FPGA	Matriz de puertas lógicas programable en campo
RAM	Random Acces Memory
SSD	Solid State Disk
USIM	Universal Subscriber Identity Module
NMT	Nordic Mobile Telephone
AMPS	Advanced Mobile Phone System
RAN	Red de acceso radio
BSS	Subsistema de la estación base
NSS	Subsistema de Conmutación de Red
OSS	Subsistema de la operación de apoyo
MS	Dispositivo del usuario
BS	Estación base
BSC	Controlador de la estación base
BCCH	canal lógico de control de difusión
HLR	Home Location Register
VLR	Visited Location register
MSC	Centro de conmutación móvil
LA	Área de localización
CC	Country Code
MNC	Mobile network code
LAC	Código de localización de área
MSISDN	Mobile Subscriber ISDN Number
IMEI	International Mobile Station Equipment Identity

EIR	Equipment Identity Register
IMSI	International Mobile Subscriber Identity
MCC	Código móvil por país
MSIN	Número de identificación del subscriptor móvil
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecomunications System
RNC	Radio Network Controler
RRC	Radio Resource Control
UICC	Universal Integrated Circuit
SRNC	Serving Radio Network Controller
LTE	Long Term Evolution
MME	Mobile Management Entity
HSS	Home Subscriber Server
GUTI	Globally Unique Temporary Identifier
AMF	Access and Mobility Management
AUSF	Authentication Server Function
EAP	Extensible Authentication Protocol
N3IWF	Non-3GPP Interworking Function
VPN	Red privada virtual
SUPI	Subscription Permanent Identifier
SUCI	Subscription Concealed Identifier
AKA	Authentication and Key Agreement
GPS	Sistema de Posicionamiento Global
EDGE	Enhanced Data rates for GSM Evolution
SIP	Session Initiation Protocol
VoIP	Voz sobre IP
STP	Signal Transfer Point
Yate	Yet Another Telephony Engine

Capítulo 1: Introducción

El espectro electromagnético ha sido explotado de forma muy amplia en el último siglo, desde las primeras comunicaciones por radio hasta las actuales redes de telefonía. Durante los últimos cien años el espectro ha sido empleado de forma imparable, desde las primeras comunicaciones de Marconi a pequeña escala a las comunicaciones interestelares con sondas como la Voyager 2[1]. Las comunicaciones mediante radio han permitido mantener el planeta conectado desde sus puntos más recónditos. Aunque también ha sido empleado para usos menos gratificantes, como la guerra electrónica, con casos documentados a principios del siglo XX. [2]

Durante este tiempo, conforme se han desarrollado y abaratado los dispositivos ha sido necesario mejorar los sistemas de comunicación para dar cabida al creciente número de usuarios que las utilizaban.

En las últimas décadas las comunicaciones por radio se han extendido enormemente, sobre todo con el auge de los dispositivos móviles. Con la llegada de los dispositivos inteligentes el mundo ha cambiado. Tus datos ya no solo están almacenados en tu ordenador en un lugar seguro como tu casa. Ahora siempre llevas contigo información que te identifica, datos personales, financieros en tu bolsillo, allá donde vas. Y esta tendencia va a continuar, favorecida por la introducción del Internet de las Cosas (IoT) así como el 5G con lo que aumentará de forma significativa el número de dispositivos conectados.

Como podemos ver en la Figura 1 y conforme a los estudios de GSMA y Ericsson, arrojan unos resultados muy similares en los cuales entorno a un 65 % de las personas del planeta cuenta con un dispositivo móvil, sin embargo, hay más conexiones móviles que seres humanos en el planeta, esto se debe a que de media cada persona tiene 1.53 conexiones asociadas, ya sea por dispositivos personales, de trabajo etc. [3][4]

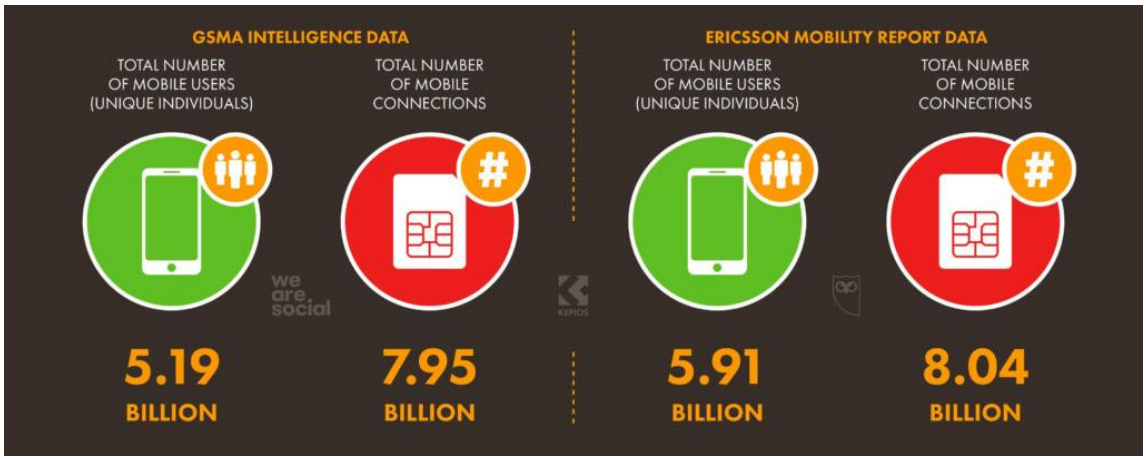


Figura 1: Usuarios de dispositivos y conexiones GSMA vs Ericsson

Y si nos vamos a la Figura 2 podemos ver como las conexiones de dispositivos IoT son de unos 13 billones casi duplicando la cifra de los seres humanos en el planeta. Estas conexiones, denominadas máquina a máquina (M2M) van a seguir creciendo debido al mencionado aumento de los dispositivos IoT. Como podemos ver, dentro de los dispositivos IoT hay dos categorías, en las que podemos ver los dispositivos de rango cercano y de rango lejano. Ambos emplean el espectro electromagnético, pero únicamente los que son definidos como rango lejano son lo que emplean tecnologías celulares. Estos dispositivos IoT en muchas ocasiones por razones

económicas o de ubicación además no usan las últimas tecnologías disponibles, o porque en muchas ocasiones por la naturaleza de sus sensores no precisan de altas capacidades. [3]

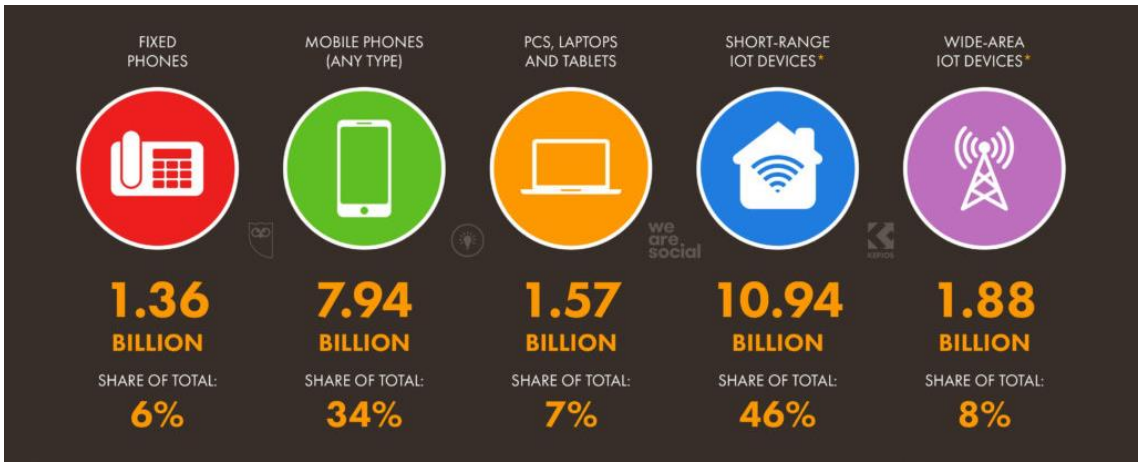


Figura 2: Conexiones de dispositivos a lo largo del planeta por categoría.

Durante los últimos cuarenta años, las generaciones de telefonía se han sucedido, estas generaciones han mejorado las tecnologías empleadas, los dispositivos, y los protocolos. Esto ha permitido una mayor velocidad, mejores servicios, mejor seguridad, etc.

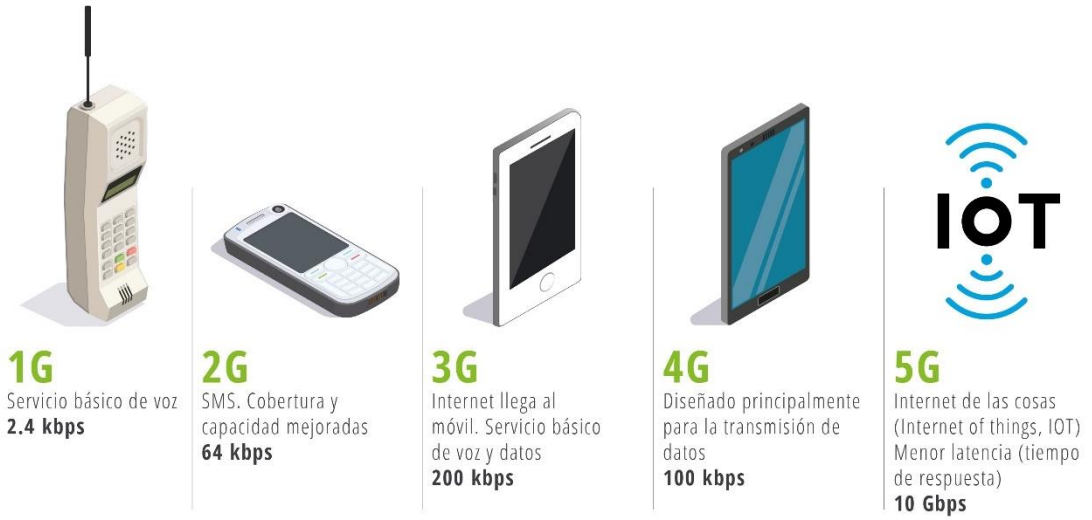


Figura 3: Evolución temporal y de servicios de las redes de telefonía.

Salvo para la primera generación analógica, la compatibilidad hacia atrás con las otras generaciones de ha mantenido, pudiendo recurrir a ellas en caso de congestión o mala cobertura. [5]

Esta retrocompatibilidad es muy beneficiosa, pero entraña problemas ya que el uso de una generación anterior este sujeto al uso de protocolos menos avanzados, los cuales debido a un mayor tiempo de vida pueden presentar vulnerabilidades que ya han sido ampliamente documentadas.

Esto sucede con un fallo en el proceso de autenticación en las redes de 2G, que permite obtener el identificador privado único de cada usuario haciendo uso de una tecnología denominada IMSI-

Catcher. Al obtener el International Mobile Subscriber Identity (IMSI) se pueden realizar ataques Man in the Middle (MitM) a nivel de radio o escucha remota atacando al núcleo de la red vía el protocolo SS7. Además, permite ubicar al usuario y realizar un seguimiento del mismo.[6]

Esta vulnerabilidad es conocida desde principios de los años 2000 por las agencias gubernamentales, las cuales construyeron equipos específicos para explotarla. Pero ha sido durante la década de 2010 con la facilidad de acceso a equipos de radio definida por software (SDR) cuando la explotación de esta vulnerabilidad ha aumentado. [6]

En este proyecto se va a profundizar en algunos aspectos de seguridad de las redes móviles, para sus diferentes generaciones.

Ver más detalladamente en que consiste un IMSI-Catcher, que formas hay de detectarlo y que herramientas hay disponibles en el mercado para su detección.

Además, se va a realizar empleando un SDR un IMSI-Catcher funcional, con el que evaluar las citadas herramientas.

1.1 Estructura del documento

El presente documento consta de diez capítulos los cuales podemos, dividir en varios bloques principales. En el primer bloque se realiza la identificación de la necesidad en el **capítulo primero** y durante cuánto tiempo se plantea y de qué modo se va a realizar el proyecto en los **capítulos segundo** y **tercero** respectivamente.

En el siguiente bloque que está compuesto por el **capítulo cuarto** en el que se muestra el equipamiento usado en el proyecto.

El tercer bloque comprendido por los **capítulos quinto y sexto** aborda desde un aspecto teórico las redes de telefonía, su evolución y la mejora de su seguridad y proceso de autenticación. También profundiza en el concepto de IMSI-Catcher mostrando herramientas en el mercado que sirven para detectarlos.

En el **capítulo séptimo** realizamos la implementación de un IMSI-Catcher. Y realizamos una comparativa entre dos herramientas que viendo el rendimiento de cada una de ellas. Este bloque se extiende por los **capítulos octavo**.

Por último, vemos las conclusiones del proyecto y sus futuras líneas de trabajo en los **capítulos noveno** y **décimo.**

Capítulo 2: Fases del proyecto

De la experiencia obtenida de la realización del Trabajo de Grado, en la que me fue muy útil opté por elaborar una propuesta de tiempos y objetivos que seguir durante la realización del proyecto. Esta práctica es muy habitual, ya que es de vital importancia dejar bien definidos al inicio del proyecto cuales son los objetivos de este, determinar los recursos que van a ser empleados y marcar objetivos de seguimiento.

La realización por mi parte de esta planificación con la supervisión de mis tutores previa a la realización del proyecto ha sido muy útil y me ha permitido ver como se aborda este tipo de proyectos desde el mundo laboral.

Asimismo, durante la realización del proyecto cumplir con los objetivos fijados previamente o adaptarlos según las situaciones del momento ha sido una valiosa lección.

Esto es lo que vamos a ver en este capítulo desgranando las fases del proyecto, declarando su inicio y su final, así como el número de horas destinadas a cada una de estas fases.

- Inicio del proyecto: En esta fase se planteó la necesidad de conocer más sobre técnicas de ataque empleando el acceso radio a la red móvil, más concretamente el IMSI-Catcher.
- Recopilación de conocimientos: En esta etapa se comenzó a estudiar más detenidamente las redes móviles en gran detalle, así como consultando documentación técnica para poder operar la estación de forma adecuada. (100 horas). Cabe destacar que esta fase se puede alargar de forma indefinida, por lo que se estipuló que llegase a ser entorno a un 30% de la extensión del proyecto.
- Estudio de las herramientas y contacto con las empresas: Se buscó herramientas en el mercado las cuales se pudieran emplearse para la detección de IMSI-Catchers y se solicitaron demos técnicas para comprender su funcionamiento. (60 horas).
- Desarrollo de una estación base de telefonía empleando SDR: Obtención de los componentes, instalación, ajuste de parámetros para obtener el funcionamiento deseado. (120 horas).
- Prueba de las herramientas para la detección de IMSI-Catchers en conjunto con el IMSI-Catcher desarrollado. (30 horas)
- Redacción
- Final del proyecto.

Capítulo 3: Metodología

En este proyecto se aborda investigar sobre la seguridad en dispositivos móviles, enfocándonos a las comunicaciones por el acceso radio y ver las posibles amenazas que pueden provocar los denominados IMSI-Catchers. Cubre la necesidad detectada en la mitigación de riesgos de seguridad en los usuarios como es el análisis desde el punto de vista de seguridad de las comunicaciones radio en los teléfonos inteligentes los usuarios.

El proyecto se plantea en fases de manera que se vayan cubriendo hitos:

- Identificación de necesidades
    - Herramientas: Evaluar una serie de herramientas con las que realizar los análisis anteriormente descritos.
    - Documentación: Tener documentación relativa al estudio realizado y los resultados arrojados por las herramientas.
    - Hardware: Realizar un IMSI-Catcher con el que probar la eficiencia de las herramientas basándonos en un dispositivo real.
- Alcance
    - Herramientas usadas: Se recopilaron una serie de herramientas con las que evaluar la presencia de IMSI-Catcher, tanto de proyectos de código abierto como de empresas.
- Objetivos del proyecto
    - Conocer las herramientas de detección de IMSI-Catcher disponibles.
    - Realizar un IMSI-Catcher.
    - Evaluar las mencionadas herramientas.
- Plazos
    - El tiempo dedicado para cada fase lo hemos podido ver en el capítulo 2.
- Hitos
    - Recopilar información para el proyecto.
    - Tener una estación base de telefonía funcional.
    - Probar las herramientas mencionadas con el IMSI-Catcher desarrollado.

- Desarrollo
    - Una vez estudiada la problemática de los IMSI-Catcher se procedió a conocer las herramientas disponibles. Tras obtener información de dichas herramientas a través de internet o en reuniones con sus proveedores se desarrolló un IMSI-Catcher funcional con el que probar la eficiencia de estas.
- Conclusión y futuras líneas de trabajo
    - Comentar los resultados obtenidos tras la realización del proyecto, lo aprendido durante su realización y los próximos pasos a seguir en su mejora.

Capítulo 4: Equipamiento usado en el proyecto

En este capítulo vamos a comentar el equipamiento usado para la realización del proyecto, sus principales características y requisitos necesarios.

El equipamiento usado ha sido el siguiente:

Se ha empleado un SDR, la FPGA *BladeRFx40* que se puede ver en la Figura 4.

Figura 4: FPGA BladeRFx40

Este modelo de *Nuand* nos permite sintonizar cualquier frecuencia desde 300MHz a 3.8GHz por lo que ha sido ideal para la realización del proyecto ya que dentro de esas frecuencias se encuentran las frecuencias empleadas en telefonía.

El código fuente de esta FPGA es proporcionado por el fabricante empleando *Github*, por lo que es de libre acceso y se encuentra en constante actualización para la mejora de su rendimiento. [7]

Aunque esta FPGA se puede alimentar únicamente con la energía proporcionada por el USB que la acompaña, debido al uso como transmisor que va a tener fue necesario cambiar su alimentación añadiendo una fuente de 5V, modificando su conexión y cambiando la configuración de la FPGA mediante los jumpers que esta posee.

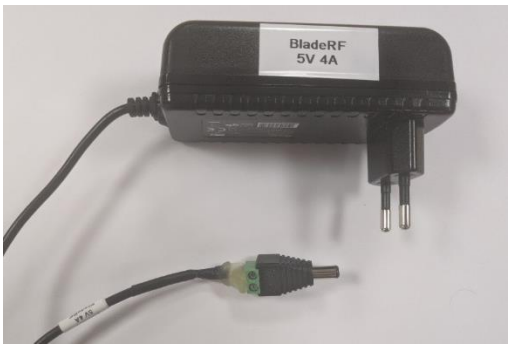


Figura 5: Alimentación modificada de la FPGA BladeRFx40

Además, han sido necesarias dos antenas las cuales son adecuadas para radiar en la banda GSM 900 que es la frecuencia de telefonía GSM. Estas antenas se conectan mediante conectores SMA a la FPGA, y las podemos ver en la Figura 6.

Figura 6: Antenas para la banda GSM 900

El otro SDR empleado fue el *USRP N210* de la empresa *Ettus* el cual podemos ver en la Figura 7. Al igual que la *BladeRFx40* incluye una FPGA, aunque de mayores prestaciones, además de incorporar una interfaz de Gigabit Ethernet. [8]

Figura 7: USRP N210

Otro SDR, en este caso un *HackRF One* que se empleará como sonda pasiva y que podemos ver en la Figura 8. Este SDR puede trabajar en el rango de frecuencias de 1 MHz a 6 GHz. [9]

Figura 8: HackRF One

Un ordenador del siguiente modelo, HP EliteBook 850 G5 con las siguientes características:

- Intel Quad Core i7-10570
- 16 GB RAM
- 1TB SDD con Windows 10 Pro
- 256GB SDD con la distribución Kali Linux.

Podemos verlo en la Figura 9.

Figura 9: Equipo usado para el despliegue de la plataforma del proyecto

La elección de este ordenador no es trivial, ya que se realizaron múltiples pruebas empleando como controlador de la FPGA una *Raspberry Pi Model 3*, sin embargo, los resultados no fueron los esperados, por lo que se descartó. Esto nos lleva a concluir que de cara a la realización de un proyecto como este se debe tener un compromiso con el equipo utilizado. No es necesario que tenga unas prestaciones tan altas como las mostradas, pero si ser más potente que una *Raspberry Pi Model 3*. Hay que hacer notar también que un equipo potente nos va a permitir trabajar de forma más optima.

Por otro lado, se ha usado varios dispositivos móviles del modelo *Samsung Galaxy S7* el cual cuenta con el sistema Android en su versión **6.0.1**. Lo podemos ver en la Figura 6

Figura 10: Ejemplo dispositivo móvil usado durante el proyecto

En estos terminales fueron introducidos además tarjetas USIM tradicionales, así como dos tarjetas USIM modificadas para la detección de IMSI-Catchers.

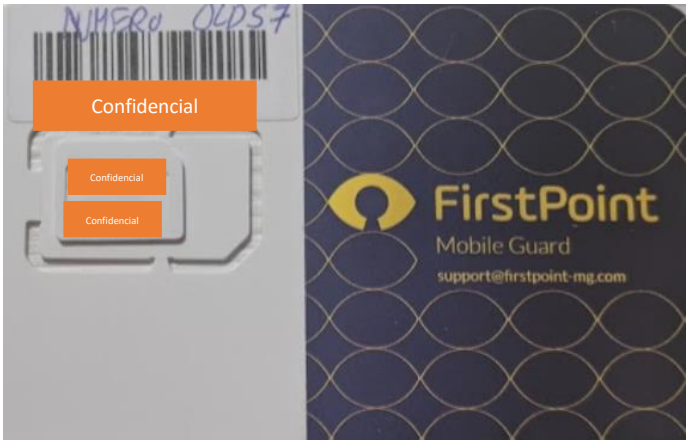


Figura 11: USIM modificada para la detección de IMSI-Catchers

Esto nos vale para probar el funcionamiento tanto con las tarjetas USIM tradicionales como con tarjetas eSIM que son empleadas cada vez más para IoT. [10]

Capítulo 5: Redes Móviles

En este capítulo abordaremos la evolución de las redes móviles, viendo sus arquitecturas y funciones principales, centrándonos en su proceso de autenticación ya que es en el momento más delicado y en el que los IMSI-Catchers actúan.

La primera generación de redes de telefonía era analógica, y no se encontraba tan estandarizada, conviviendo multitud de estándares como Nordic Mobile Telephone (NMT), Advanced Mobile Phone System (AMPS), Radiocom 2000, … Es por esto por lo que no nos vamos a detener en ella y vamos a pasar directamente a la segunda generación. [5]

También hay que destacar que existieron generaciones intermedias, como 2.5 G, 3.75G, LTE – que aportaron mejoras a la generación anterior, aunque no las vamos a comentar.

5.2 Redes de segunda generación, 2G, GSM

La tecnología de segunda generación comenzó a ser desarrollada en los años 80 en los países nórdicos, y fue transferida al "Groupe Special Mobile". Esta tecnología nació siendo ya digital y con el objetivo de aportar una calidad igual a la que se tenía con los sistemas digitales y un uso del espectro más eficiente. Conocida como Global System Mobile (GSM) aportó una serie de servicios a mayores de la voz como serían *roaming* global, SMS, autenticación, cifrado de los datos del usuario y de la señalización y mejoró la privacidad del usuario al cifrar su identificador. [5]

También se introdujo GPRS, el servicio de paquetes radio de GSM que fue desarrollado sobre GSM, esto permitió introducir el protocolo IP en los dispositivos, para ello debieron introducirse dos nuevos nodos a la arquitectura, el nodo de servicio GPRS (SGSN) y la puerta de enlace al nodo de soporte GPRS (GGSN). Esto permitió un aumento de los servicios ofrecidos, así como una mejora del rendimiento. [5]

Su arquitectura básica es la de la Figura 12, en la que se observan 3 subredes principales la red de acceso radio (RAN), la red del núcleo de la red, así como la red de gestión. En el estándar de GSM, se denominan también subsistemas definidos como subsistema de la estación base (BSS), subsistema de conmutación de red (NSS) y subsistema de la operación de apoyo (OSS) respectivamente.

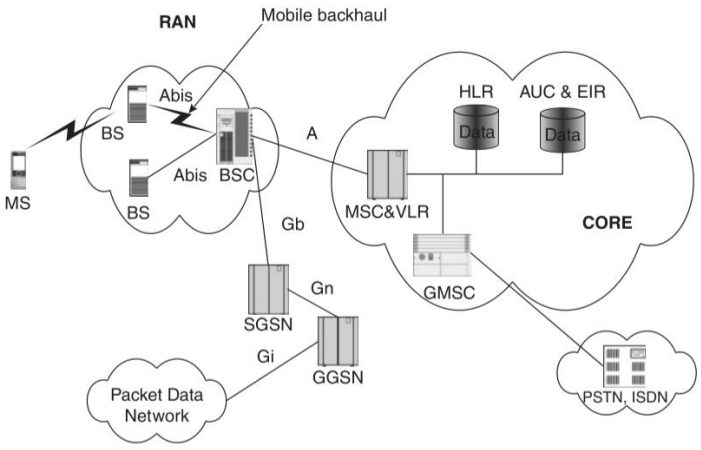


Figura 12: Arquitectura de GSM [5]

Nos centraremos en el subsistema BSS.

En ella podemos distinguir el dispositivo del usuario (MS), la estación base (BS) y el controlador de la estación base (BSC). El dispositivo del usuario se comunica con la estación base mediante un radioenlace, esta estación base puede encontrarse en exteriores o interiores y está compuesta de infraestructura adicional como serían antenas, equipos de alimentación y su pertinente conexión con el controlador de las estaciones base (BSC).

Cada estación base genera una celda de radio, la cual presenta canales de control y de tráfico. Cada celda está definida por la presencia del canal lógico de control de difusión (BCCH). La BSC se encarga de gestionar los recursos radio de las estaciones base, a las cuales se encuentran conectadas por cable o con un radioenlace, el cual se denomina *Mobile Backhaul*.

En la Tabla 1 podemos ver que funciones realiza cada uno de los componentes anteriormente descritos.

Función principal	Estación base (BS)	Controlador de la estación base (BSC)
Gestión de los canales de radio		X
Adaptación de la tasa y codificación del canal	X	
Autenticación		X
Encriptado	X	X
Saltos de frecuencia	X	
Medida de la potencia del canal de subida	X	
Medida del tráfico		X
Alta	X	X
Gestión de cambio de celda		X
Actualización de localización		X

Tabla 1: Funciones de los elementos del BSS en GSM

El BSS se encuentra conectado al núcleo de la red mediante centro de conmutación móvil (MSC). Dentro de la red, el conjunto formado por una MSC y su BSS se denomina área de localización (LA).

En el núcleo de la red se encuentran bases de datos de los usuarios, tanto de su localización como de sus perfiles en el Home Location Register (HLR) y Visited Location register (VLR). La VLR normalmente se encuentra implementada dentro de la MSC, siendo el HLR la base de datos raíz del operador la cual suele estar distribuida.

Cada área de localización (LA) tiene un identificador, que se encuentra estandarizado y está formado por el Country code CC (3 dígitos), el Mobile network code (MNC)C (2 dígitos) y el código de localización de área (LAC) de máximo 5 dígitos. Estos valores son primordiales para identificar la celda y son transmitidos por el BCCH.

Tal y como indicamos antes, GSM incorporaba la autenticación de los usuarios, por lo que vamos a ver cómo se realiza.

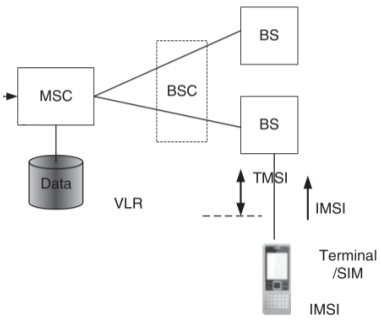
En este caso el número de teléfono asignado es lo que se conoce como Mobile Subscriber ISDN Number (MSISDN), pero además son necesarios el International Mobile Station Equipment Identity (IMEI), un número de serie asociado a dispositivo que los operadores almacenen el

Equipment Identity Register (EIR) para detectar dispositivos robados o extraviados y el International Mobile Subscriber Identity (IMSI). Nos detendremos en él.

El IMSI, formado como máximo de 15 dígitos, es único por cada usuario y este lo almacena en la tarjeta SIM, está formado por código móvil por país (MCC) de 3 dígitos y estandarizado por país, aquí en España es el 214, el código de la red móvil (2 dígitos), que indica al operador al que pertenece la red y también se encuentra registrado y por último el número de identificación del subscriptor móvil (MSIN), con un máximo de 10 dígitos.

Aunque el MSISDN presenta una estructura similar, el IMSI tiene tanta relevancia ya que es un identificador que debe ser privado, estando la relación entre MSISDN e IMSI en los HLR del operador.

Debido al carácter privado del IMSI, se emplea únicamente al registrarse en la red ya que posteriormente se emplea otro identificador el Temporary Mobile Subscriber Identity (TMSI), gestionado por la VLR y con validez para el LA gestionado por la VLR, no se transfiere a la HLR. A partir de ese momento, la comunicación por el radio enlace será usando la tupla del TMSI y el LAI. [5]



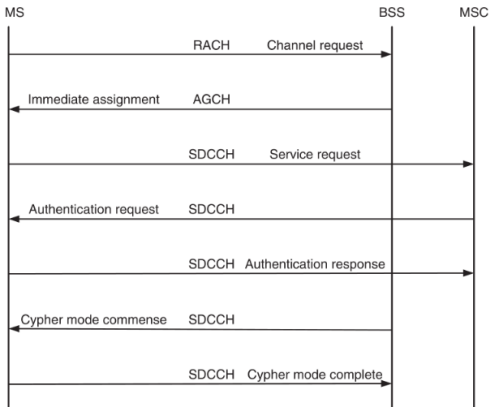


Figura 13: Proceso de autenticación en GSM [5]

En la Figura 13 podemos ver el proceso de autenticación en GSM, los identificadores empleados, así como los canales lógicos empleados. Es importante indicar que GSM incorporó encriptación, aunque varios de esos métodos de encriptación se fueron rompiendo conforme pasó el tiempo.

5.2 Redes de tercera generación,3G, UMTS

Las redes de tercera generación, desarrolladas con el nombre de Universal Mobile Telecomunications System (UMTS) aparecieron en el año 1999 teniendo compatibilidad con GSM. En la Figura 14 podemos ver su arquitectura similar a GSM, aunque ahora las estaciones base y el controlador de las estaciones base evolucionan en sus capacidades tomando el nombre de NodeB y Radio Network Controler (RNC) respectivamente.

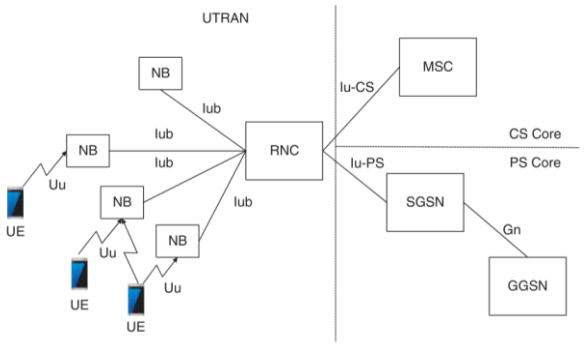


Figura 14: Arquitectura de UMTS [5]

En UMTS se incorporó la separación entre el plano de control y el plano de usuario, así como la separación de la red radio de la red de transporte. El protocolo encargado de la gestión de la conexión es el Radio Resource Control (RRC) que será empleado a partir de UMTS en adelante.

La tarjeta SIM de GSMA pasa a ser USIM implementada en un Universal Integrated Circuit (UICC), permitiendo ahora modificar los datos del usuario a través del radioenlace, ser modificada por la red, o tener aplicaciones Java almacenadas.

Esta mejora de la USIM permite realizar autenticación mutua entre el usuario UMTS y la red, reduciendo los riesgos presentes en GSM.

Esta autenticación mutua se realiza al tener lugar una conexión entre el dispositivo y la VLR/SGSN, los protocolos de seguridad implementados en la USIM son enviados al Serving Radio Network Controller (SRNC) en el que el SRNC elige los algoritmos a usar de la lista que tiene disponible y de los que ha enviado el dispositivo que es capaz de usar. Entonces envía un mensaje, en el que se incluyen las capacidades del dispositivo, con lo que este se asegura de emplear la celda legítima. En la Figura 15 vemos un esquema de este proceso. [11]

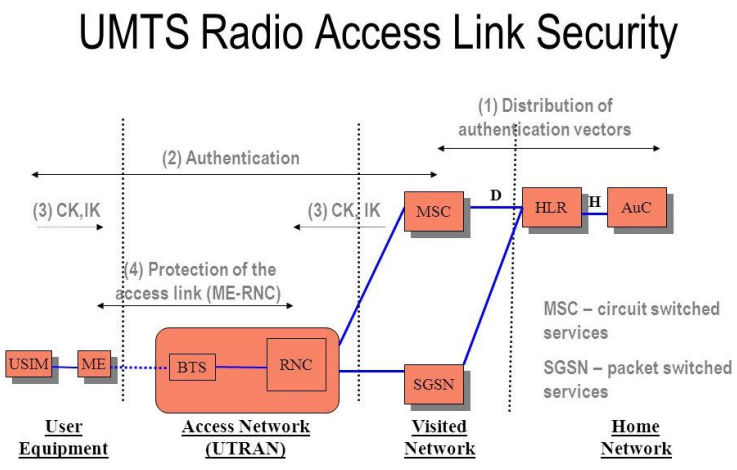


Figura 15: Proceso de autenticación en UMTS [11]

5.3 Redes de cuarta generación, 4G, LTE

Las redes de cuarta generación surgieron como una necesidad debido a la gran demanda generada por los usuarios, así como el bajo precio de los dispositivos. Ofrece mayores velocidades, lo que permite su uso para telefonía IP, televisión en alta definición, para las aplicaciones de los dispositivos inteligentes de los usuarios, …. Es la más extendida ahora mismo, y se sigue empleando hasta su sustitución por la quita generación (5G) En la Figura 16 podemos ver su arquitectura de la que podemos destacar como nuevos elementos el Mobile Management Entity (MME), que se encargará de autenticar, gestionar el contexto del usuario que se encuentra almacenado el Home Subscriber Server (HSS).

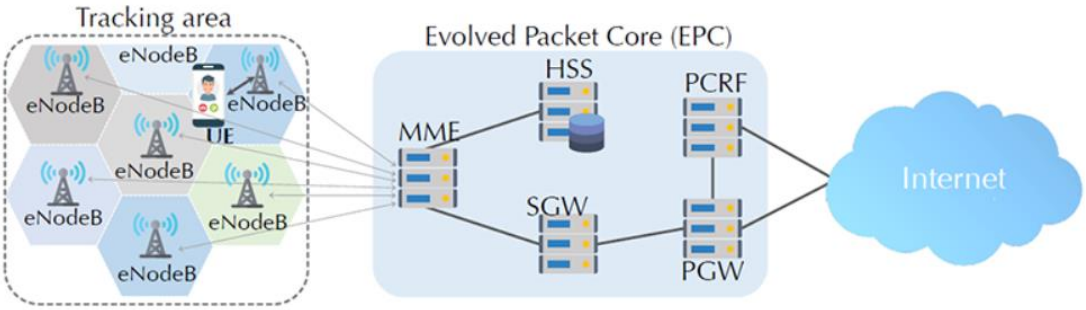


Figura 16: Arquitectura de LTE [5]

Las estaciones base pasan a ser denominadas eNodeB, mejorando sus prestaciones. También se introduce un nuevo identificador el Globally Unique Temporary Identifier (GUTI) tras un primer uso del IMSI, la estructura de este identificador la podemos ver en la Figura 17.

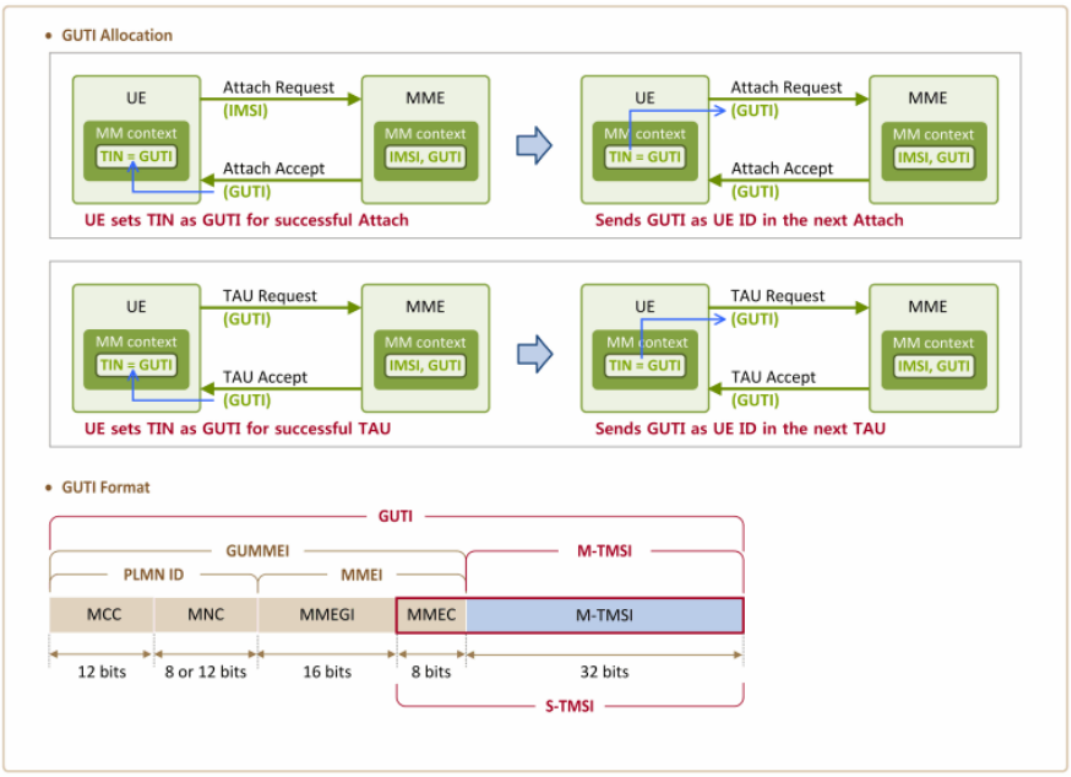


Figura 17: Identificador GUTI en LTE [12]

En la Figura 18 podemos ver cómo es el proceso de autenticación, en el que al igual que en UMTS se produce autenticación mutua. Como podemos ver el proceso de autenticación se ha mejorado, aumentando la seguridad. Se sigue produciendo autenticación mutual, como en 3G además de haber mejorado los protocolos de autenticación. En LTE, se sigue empleando el IMSI, en la primera conexión.

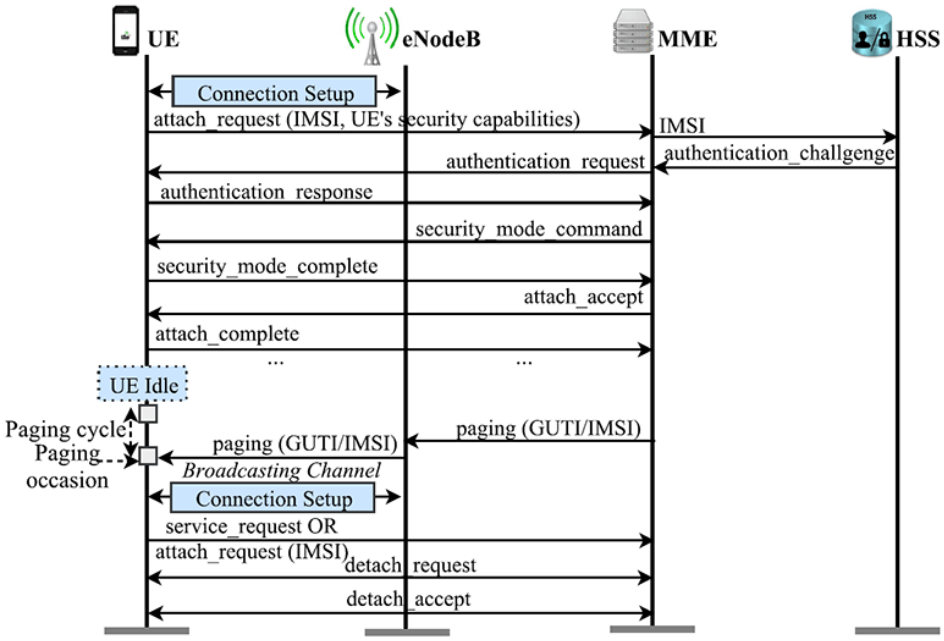


Figura 18: Proceso de autenticación en LTE [5]

Como resumen, en la Figura 19 podemos ver un esquema de cómo ha evolucionado la seguridad en las diferentes generaciones, mejorando la encriptación e incorporando mecanismos de seguridad como la autenticación mutua.

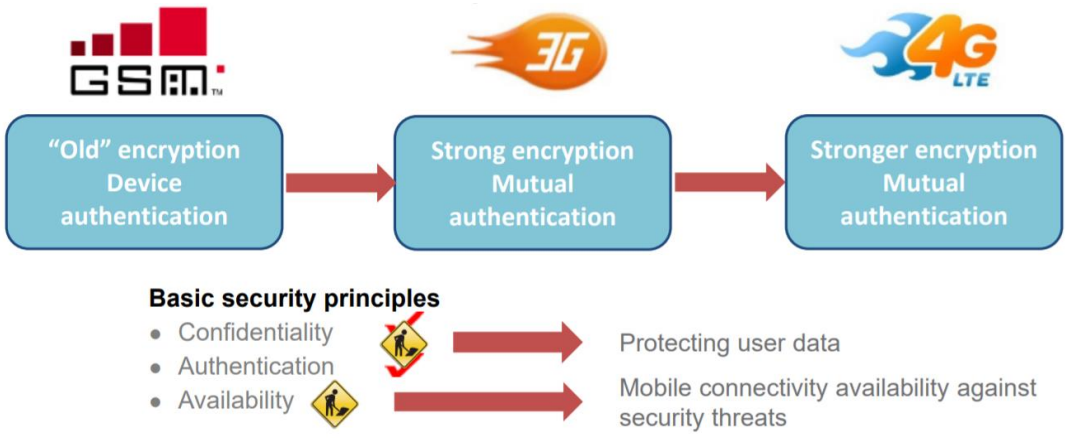


Figura 19: Evolución de la seguridad en las 4 primeras generaciones

Es importante notar tal y como indican informes de GSMA, que sobre todo en Europa no se ha producido un apagado de las redes de telefonía de generaciones anteriores, como se puede ver en la Figura 20. Esto está motivado por el hecho de que multitud de comunicaciones M2M y de IoT se siguen realizando, llegando el extremo de que los operadores europeos plantean apagar primero la red de 3G que la de 2G debido a sus costes. [13]

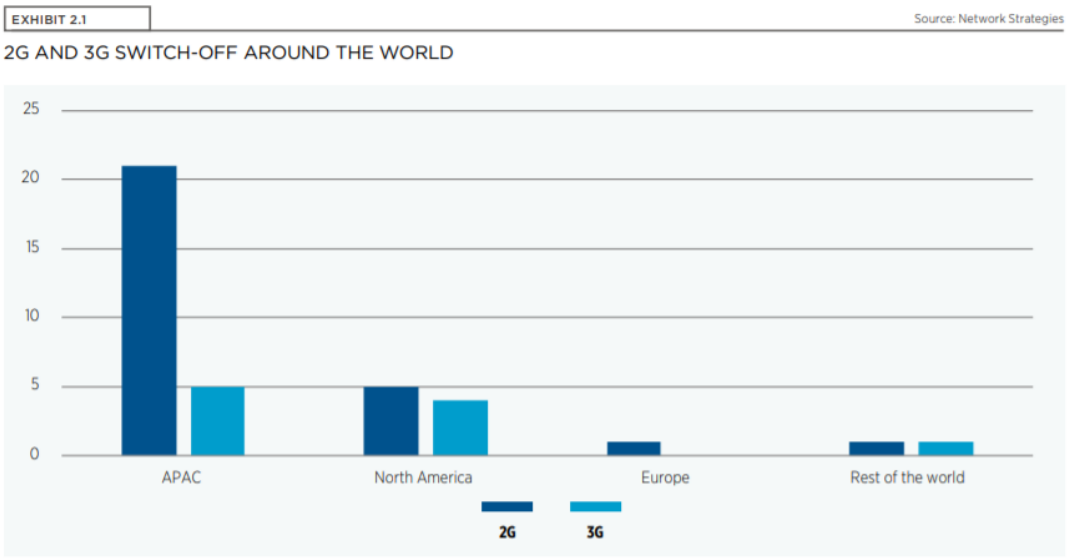


Figura 20: Estado de las redes GSM y UMTS en el planeta [12]

5.4 Redes de quinta generación. 5G

Las redes de quinta generación o 5G se están desplegando en la actualidad, entrando en servicio ya en 2021. Estas redes tienen como característica una gran velocidad asociada a unas latencias de menos de un milisegundo, lo que va a permitir conectividad el tiempo real. Además, está destinado a permitir la interconexión de billones de dispositivos, como los dispositivos IoT además de los tradicionales dispositivos de los usuarios.

En la Figura 21 podemos ver la arquitectura de esta nueva tecnología. Debido a la extensión de esta nueva tecnología únicamente entraremos a comentar la parte de la RAN y el elemento que se encarga de la autenticación que está compuesta por g-NodeB y el Access and Mobility Management (AMF).

El AMF hereda parte de las funciones del MME de LTE, todas las relacionadas con la información de conexión y sesión enviada por el dispositivo de usuario, debiendo encargarse únicamente de la gestión de la conexión y de la gestión de la movilidad entre celdas. Es el punto en el que 5G-RAN se conecta con el núcleo.

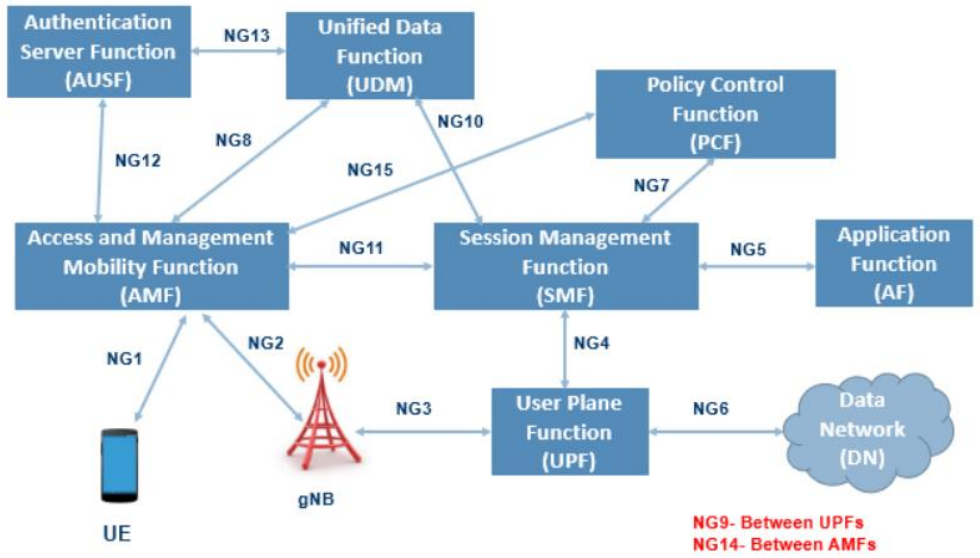


Figura 21: Arquitectura en 5G [14]

En cuanto a la autenticación, cuyo proceso podemos ver en la Figura 22. Para esta nueva tecnología se ha realizado un proceso de autenticación que no depende de la tecnología empleada, empleándose para redes celulares como en las tecnologías previas, pero también para redes Wi-Fi o cableadas.

En el caso de las comunicaciones celulares se produce la autenticación con el Authentication Server Function (AUSF) a través del AMF, empleando el Extensible Authentication Protocol (EAP). Al emplear las otras redes de acceso descritas, surge la figura del Non-3GPP Interworking Function (N3IWF) que actúa como una red privada virtual (VPN) para acceder al núcleo de la red 5G.

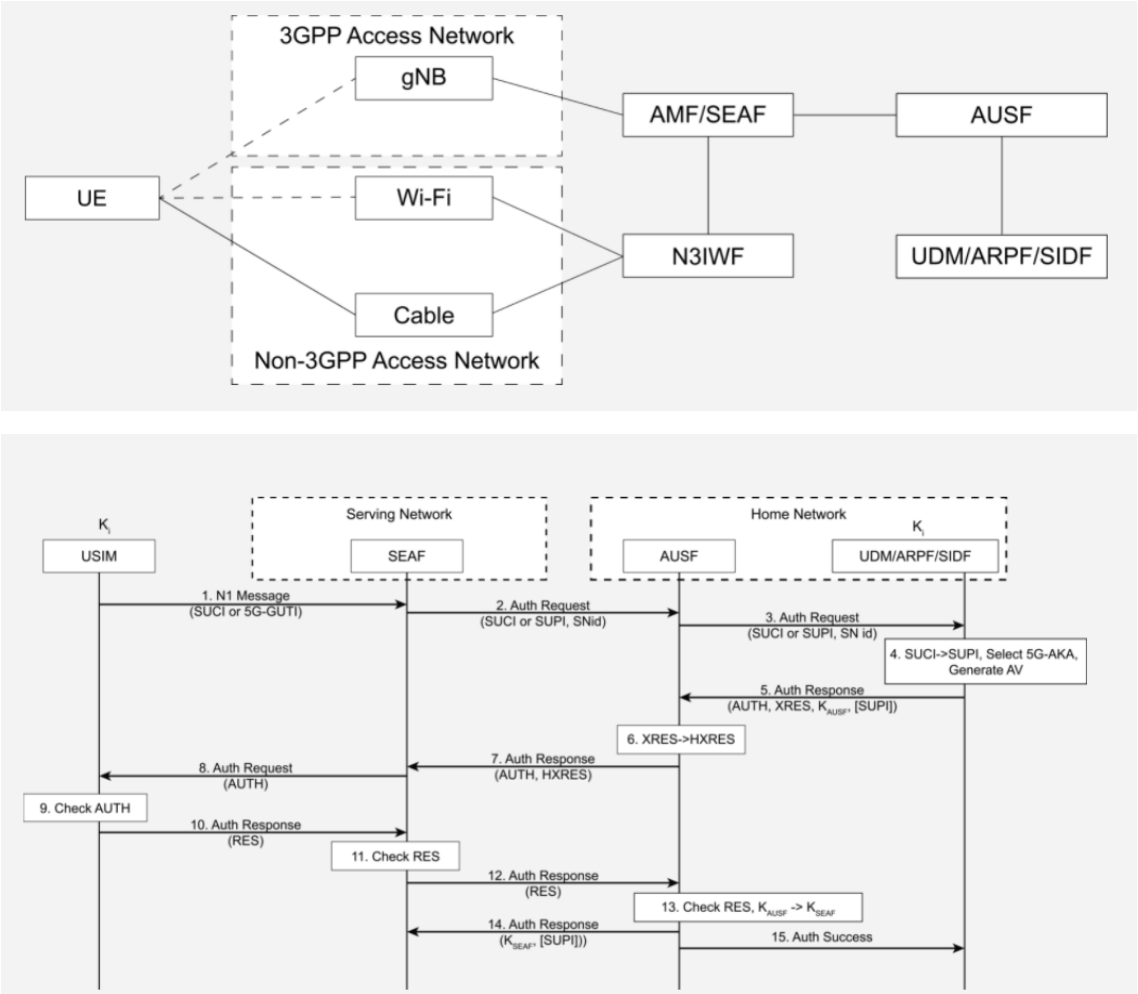


Figura 22: Autenticación en 5G [15]

Tal y como se puede ver en la Figura 22 en el caso de 5G ya no tendremos el IMSI cómo identificador, sino que nos encontramos el Subscription Permanent Identifier (SUPI) y su versión encriptada, el Subscription Concealed Identifier (SUCI). Estos identificadores presentan la estructura de la Figura 23.

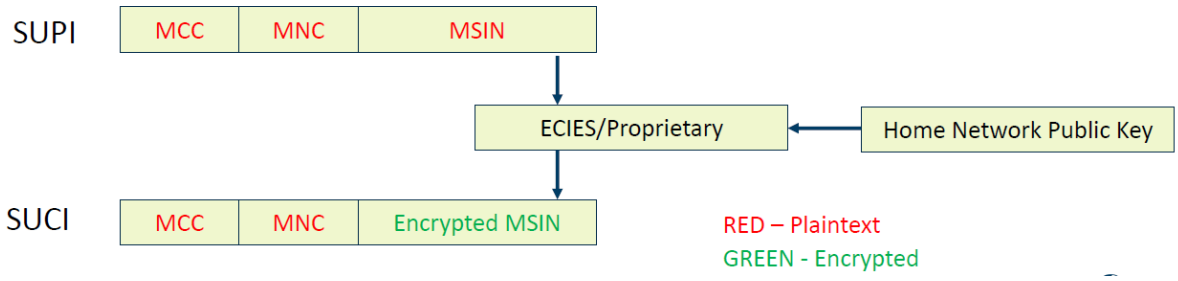


Figura 23: SUPI y SUCI en 5G

Para la transmisión por la red se empleará el SUCI, nunca el SUPI salvo que nos encontremos en células con tecnologías anteriores.

También en las redes de 5G nos encontramos con una mayor seguridad ya que el TMSI va a ser refrescado tras su uso en el sistema de alta.

Capítulo 6: IMSI Catcher

Los IMSI-Catchers, también conocidos como Stingrays son simuladores de una celda de telefonía. Actúan como una estación base celular maliciosa que puede ser usada para determinar la localización de móviles o en ocasiones obtener información durante una comunicación que emplea la mencionada celda. Este tipo de dispositivos han sido usados de forma amplia por los gobiernos de diversos países como podrían ser EE. UU., Ucrania... [6]

Como su nombre indica este tipo de dispositivos buscan obtener el IMSI (International Mobile Subscriber Identity) del dispositivo.

Sin embargo, hay que tener en cuenta si el uso de este tipo de dispositivos se puede extender a un mayor público y ser usado con fines criminales. Con la proliferación de los dispositivos SDR, el acceso a poseer o desarrollar un IMSI-Catcher se ha convertido en una tarea sencilla.

Los ataques que emplean un IMSI-Catcher son ataques del tipo MitM (*Man in the Middle*), por lo que se puede obtener información del usuario a través de sus llamadas, sus SMS, los datos móviles, etc…

Los IMSI-Catcher se dividen en dos categorías fundamentalmente:

Pasivos: Este tipo de IMSI-Catcher es menos eficaz puesto que no interactúa con los dispositivos móviles o con la red. Sin embargo, tienen como contrapunto que son mucho más difíciles de detectar ya que al no interferir con la red o los dispositivos su detección es mucho más complicada.

Activos: Este tipo de IMSI-Catcher es más eficaz, ya que tiene el control de los dispositivos móviles durante su uso. Esta categoría de IMSI-Catcher es detectable, ya que interfiere con la red.

En la Figura 24 podemos ver su arquitectura

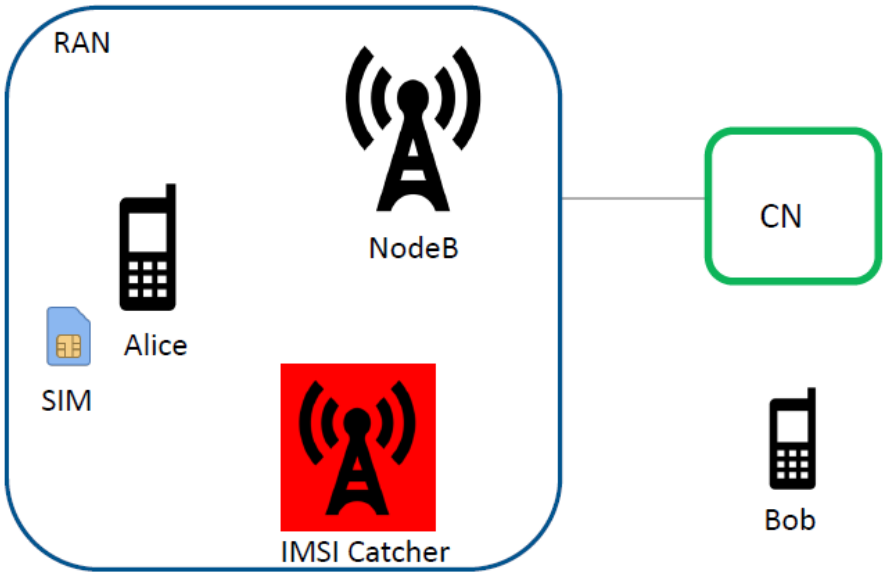


Figura 24: Esquema lógico de un IMSI-Catcher

Como podemos ver el dispositivo de Alice se encuentra en las inmediaciones de un IMSI-Catcher. Dependiendo del tipo del IMSI-Catcher, si es pasivo podría únicamente dedicarse a recopilar información emitida por Alice, tratando de desencriptarla.

Si es activo en cambio, habrá obtenido y replicado las características de una celda legítima, también incorporará un dispositivo que bloquee las frecuencias de tecnologías superiores con el fin de hacer que el dispositivo de Alice se conecte al IMSI-Catcher.

Este tipo de ataques son más sencillos de realizar en redes de generaciones antiguas como 2G, ya que no precisa autenticación mutua entre el dispositivo y la red, tal y como hemos visto en el apartado anterior en el que las redes 3G y 4G emplean este mecanismo de seguridad.

Una de las formas de realizar estos ataques en este tipo de redes avanzadas es empleando como superficie de ataque el periodo del protocolo en el que se produce la autenticación mutua, como hemos podido ver en capítulos anteriores.

También se ha visto que versiones sofisticadas de este tipo de ataques que son capaces de reducir la generación de los servicios empleados a generaciones en las que no se emplea la autenticación mutua.

Esto se hace empleando dispositivos conocidos como *Jammers* cuyo cometido es provocar que el dispositivo abandone las tecnologías superiores (3G,4G…) y vuelva

Aunque hasta ahora hemos hablado de redes de telefonía como 2G, 3G, 4G debemos tener en cuenta que las redes 5G ya están siendo desplegadas y ofrecidas por los operadores.

Pero hay que tener en cuenta que actualmente no va a haber únicamente redes con la tecnología 5G, sino que va a convivir con la red 4G en lo que se conoce como 5G Non-Standalone.

En las redes LTE como se vio está el identificadore Globally Unique Temporary Identifier (GUTI) tras un primer uso del IMSI. por lo que es posible realizar un seguimiento del dispositivo si el GUTI no cambiado de forma aleatoria cada poco tiempo.

En el caso del 5G-GUTI este es obligatorio que sea refrescado de forma inmediata tras el registro de un dispositivo, por lo que se reduce la posibilidad de explotar esa vulnerabilidad.

En 5G los ataques basados en forzar al usuario a emplear tecnologías anteriores serán más complicados, sobre todo para emplear 2G o 3G. [16]

Para las redes de 5G hay que tener en cuenta que, aunque son más seguras, hay aspectos como los protocolos como los Authentication and Key Agreement (AKA) que son usados por esta tecnología y permiten también el seguimiento de los usuarios. Los fabricantes de dispositivos no tienen un estándar por el que seleccionar a la red a la que se conectan, ni tienen forma de indicar si la comunicación que está teniendo lugar se está cifrando de una forma adecuada.

Y aunque se ha mencionado, el código SUCI, aunque esté encriptado va a permitir distinguir a los usuarios que estén en *roaming*.

6.1 Detección IMSI Catcher

No hay una forma clara de detección de estos dispositivos, aunque hay algunos síntomas significativos ya que un IMSI-Catcher introducirá irregularidades en la red que pueden ser estudiadas para determinar si hay un IMSI-Catcher en las inmediaciones.

6.1.1 Uso de frecuencias distintas

Para reducir la interferencia de la seña, y aumentar su calidad, el atacante podría usar frecuencias no utilizadas en la zona (canales de guarda). Sin embargo, esto conlleva que los dispositivos tiendan menos a conectarse al IMSI-Catcher ya que las celdas anuncian las frecuencias a las que operan sus vecinos y por tanto suelen probar a realizar la conexión en primer lugar con ellas. Otra forma de explotar esto es emplear una frecuencia que se anuncia por las estaciones vecinas debido a un error de configuración.
Detectabilidad: Se puede controlar el uso de frecuencias no planeadas estando en contacto con las autoridades ya que los planes de frecuencia son públicos y se encuentran regulados por los países. [6]

6.1.2 Elección de una identificación de celda

Normalmente el IMSI-Catcher tendrá una ID de celda nueva empleando un nuevo LAC no usado en la zona, esto se realiza debido a que el dispositivo no debería recibir los mismos del IMSI-Catcher que de la celda legítima para no provocar desajustes en el protocolo. Este cambio en los valores de identificación de la celda provocará que el dispositivo móvil mande un *Location Update Request* y con ello sea atraído al IMSI-Catcher.
Detectabilidad: Los valores de identificación de la celda son unos valores muy estáticos, que en algunos dispositivos son usado accediendo a bases de datos estaciones de telefonía para estimar de manera aproximada la ubicación del teléfono cuando el GPS no está disponible, la señal del GPS es muy débil o aportar unos datos de sincronismo cuando el GPS se está inicializando.
Mediante el uso de estas bases de datos se podría descubrir una celda en la que sus valores de identificación sean discordantes, tanto por su ID como por la frecuencia que esta emplea.

6.1.3 Capacidades de la estación base anunciada

Las señales baliza de las estaciones base de telefonía envían además de la información de identificación de la celda una lista de las funciones que soporta dicha celda. Esto podría ser los servicios de radio por paquetes, como GPRS o EDGE los cuales podrían no estar implementados dentro de las capacidades del IMSI-Catcher ya que precisan una emulación mucho más compleja. Estos protocolos comparten slots de tiempo con GSM, pero emplean una modulación distinta.

Detectabilidad: El dispositivo móvil debería consultar una base de datos de celda sen las que esta información se encuentre anotada. Empleando la información de las bases de datos se podrían encontrar celdas ilegítimas ya que son parámetros que no se suelen cambiar, y en el caso de cambiarse se produce por actualización a tecnologías superiores, nunca se producirá hacia atrás en la tecnología como podrían ser de GPRS a EDGE.
También se podría detectar una celda ilegítima si esta no transmite ciertos mensajes de broadcast con la información el sistema (SIB), ignorar solicitudes estándar de servicios o que el IMSI-Catcher no emita tráfico de búsqueda en el entorno.

6.1.4 Huella digital de parámetros de red

Otra información transmitida por las señales baliza a los dispositivos son parámetros básicos de la red sobre la organización de la red móvil, valores umbrales y valores de *temporizadore*. Estos valores pueden diferir de una estación base a otra, pero se ha visto que la mayoría de ellos tienden a ser uniformes en un determinado operador de red, pero varían entre diferentes operadores.

Es posible que IMSI-Catcher no siempre copie todos estos parámetros, ya que no son operativamente importantes para un ataque y su recopilación no es fácil.

6.1.5 Obligar a un dispositivo a registrarse

Otra forma del IMSI-Catcher de captar el dispositivo en vez de proporcionar la mejor señal y esperar que llegue una víctima para cambiar de celda, sería forzar a ese dispositivo a realizar el cambio. Una forma sencilla de obligar a la víctima a desconectarse de la red original y registrarse en una nueva estación base, que sería el IMSI-Catcher es un bloqueador de RF, los mencionados *Jammers*. Genera interferencias en la banda que bloquean las señales de las estaciones base legítimas y obligan a que el dispositivo tras un escaneo infructuoso de las frecuencias vecinas anunciadas, el dispositivo eventualmente realiza un escaneo completo, lo que le da al IMSI-Catcher la oportunidad para atraer el dispositivo.
Detectabilidad: Una forma de detectar estos es que esa interferencia puede ser detectada por otra estación móvil mediante ver los niveles de ruido del canal (por ejemplo, de la lista de vecinos).

6.1.6 Manejo de clientes UMTS

Otra forma posible es degradar un usuario UMTS a la red GSM, al usar UMTS canales que serán inutilizados con un bloqueador de RF (como arriba). Esta capa está presente en la mayoría de UMTS implementados ya que utilizan GSM para compatibilidad con versiones anteriores y aumentar la cobertura.
Detectabilidad: La interferencia se puede detectar como se describe encima. Se puede utilizar una base de datos celular para detectar GSM donde UMTS debería estar normalmente disponible.

6.1.7 Cifrado

Los IMSI-Catchers más primitivos pueden deshabilitar el cifrado (A5/0) para facilitar el seguimiento. Sin embargo, debido a los avances técnicos es posible realizar un descifrado de A5 / 1 y A5 / 2 desencriptado en tiempo real.
Sin embargo, el más potente, la variante A5 / 1 también es propensa a ataques ya que este cifrado se encuentra actualmente “roto”. Ordenadores no demasiado sofisticados con un disco duro de 2 TB y 2 GB de RAM para recuperar la clave en unos dos minutos. Mientras esto hace es posible la escucha completamente pasiva de las llamadas telefónicas.
Detectabilidad: La ausencia de un cifrado por sí solo no es un indicador suficiente, ya que el cifrado puede no estar disponible en redes *roaming*. Sin embargo, una vez que un teléfono tenía una sesión con una red particular y una tarjeta SIM particular, debe asumir que una ausencia repentina de cualquier cifrado es una señal alarmante.

6.1.8 Encarcelamiento celular

Una vez que el IMSI Catcher atrapa un dispositivo, intentará bloquear para que no cambie a otra celda activa. Por lo tanto, transmitirá una lista de vecinos vacía al teléfono o una lista con vecinos únicamente no disponibles. La estación base también puede manipular el valor de ganancia de recepción, haciendo que el dispositivo sea incapaz de detectar otras estaciones que serían legítimas. Este valor se añade a los niveles de señal realmente medidos por la MS para
prefiere una celda específica sobre otra (histéresis).
Detectabilidad: Una estación de telefonía que monitoriza a sus vecinos (por ejemplo, junto con una base de datos geográfica) es capaz de encontrar modificaciones tan sospechosas.

6.1.9 Reenvío de tráfico

El atacante para pasar inadvertido necesita reenviar las llamadas, los datos y los SMS al sistema telefónico público. Una forma de lograr esto es utilizar otra SIM y una estación de telefonía legítima para retransmitir llamadas a la red móvil. Sin embargo, desde el punto de vista de las redes, estas llamadas serán hecho bajo otra identidad lo cual podría ser detectado con un identificador de llamadas
Otra forma sería haciendo uso del protocolo Session Initiation Protocol (SIP) y un proveedor de VoIP podría enrutar estas llamadas directamente a una red SS7. Los operadores de telecomunicaciones suelen confiar sus socios mayoristas y de intercambio conexiones para establecer identificaciones de llamadas legítimas. Se podrían lograr llamadas telefónicas y mensajes de texto salientes, no así para las entrantes.
Detectabilidad: La primera configuración es detectable al realizar una prueba
llamadas y comprobar de forma independiente el identificador de llamadas (por ejemplo, utilizando un sistema automático).

6.1.10 Patrón de uso

Los IMSI-Catcher se suelen utilizar durante períodos de tiempo bastante cortos para localizar y verificar un teléfono.
La celda está activa sólo durante la duración de la vigilancia. Los tiempos durante los que esta funciona son mucho más cortos que los de una celda legítima.
Detectabilidad: Celdas que aparecen repentinamente (con buena calidad de la señal) durante un corto período de tiempo y dejan de existir después con un tiempo de vida mucho más corto.

6.2 Herramientas de detección de IMSI-Catchers

Una vez vistos los métodos que pueden ser usados para la identificación de un IMSI-Catcher vamos a ver las soluciones en el mercado para realizar la detección.

6.2.1 BTS-Tracker

Esta herramienta de la empresa italiana SecurCube consta de un hardware dedicado que se puede ver en la Figura 25y una aplicación móvil que lo controla. La aplicación también se puede usar de forma autónoma respecto al hardware ya que es gratuita y te permite obtener los parámetros [17].

Figura 25: Hardware dedicado de SecurCube [17]

Tanto el hardware como la aplicación recolectan datos de las celdas de telefonía cercanas, debiendo analizar posteriormente si los datos obtenidos son sospechosos. En la Figura 26, podemos ver los obtenido desde la aplicación.

Figura 26: Resultados de la aplicación BTS-Tracker

No hay detrás ningún análisis de los datos que nos indique si estamos ante un IMSI-Catcher.

6.2.2 Snoopsnitch

Esta aplicación de código abierto permite a los usuarios probar la seguridad de sus dispositivos mediante la evaluación de las redes móviles a las que se conecta. Sólo es válida para dispositivos Android y precisa tener permisos de *root* para su operación. [18]

Esta aplicación busca detectar ataques generados en la red, como serían los IMSI-Catchers. Está pensada para redes de 2G y 3G, y para LTE solo recopila datos. Para estimar los métodos de detección de IMSI Catcher, emplea algunos de los mecanismos descritos anteriormente, como serian la comprobación de los datos de la celda, uso de frecuencias distintos, celdas sin celdas vecinas anunciadas, uso de protocolos de protocolos de cifrado obsoletos. [19]

En la Figura 27 podemos ver algunas capturas de pantalla.

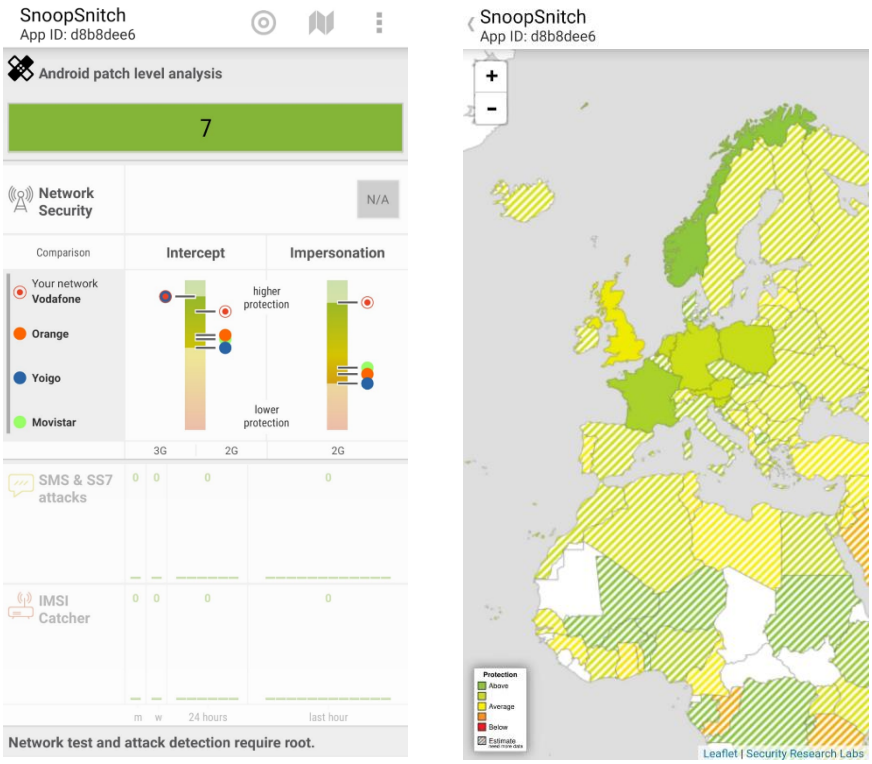


Figura 27: Capturas de pantalla de SnoopSnitch

6.2.3 Android IMSI Catcher Detector (AIMSICD)

Esta aplicación está pensada para la detección de IMSI-Catcher precisa el tener permisos *root* para la detección de celdas. Para la detección de los IMSI-Catcher, realiza una comparación de los datos de posición y de la celda comparándolos que bases de datos de internet. También monitoriza la señal enviada por la celda en busca de comportamientos inusuales como subidas bruscas de potencia. [20] [21]

En la Figura 28 podemos ver la información que recopila esta aplicación, como serían los datos de la celda, los datos de la lista de celdas vecinas, así como una representación sobre un mapa de las estaciones colindantes.

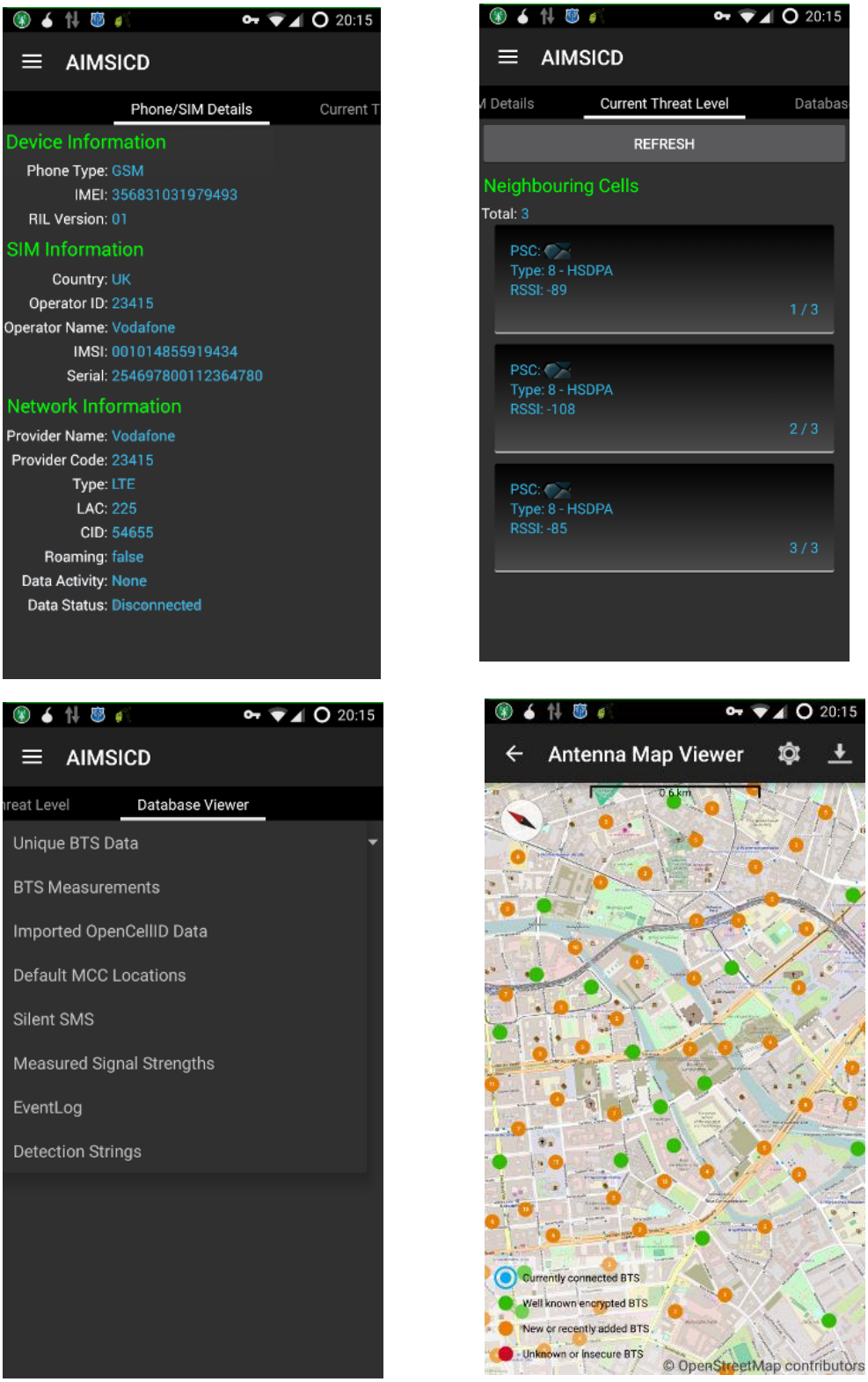


Figura 28: Capturas de Android IMSI-Catcher Detector

6.2.5 Cell Spy Catcher

Esta aplicación no necesita permisos de *root* Una vez instalado necesita un tiempo de aprendizaje en el que recopila datos de la zona, con el finde conocer y recopilar información de las celdas que se encuentran alrededor. Ese tiempo es configurable y con extensión mínima de un día. Una vez finalizado ese proceso comienza a recopilar y analizar las redes móviles a las que se conecta el dispositivo. Recopila y compara los valores de Local Area Code (LAC) el ID de la celda, así como el MNC y MCC que la celda entrega, con varias bases de datos disponibles en Internet. También recopila el tiempo durante el que se ha detectado la red.

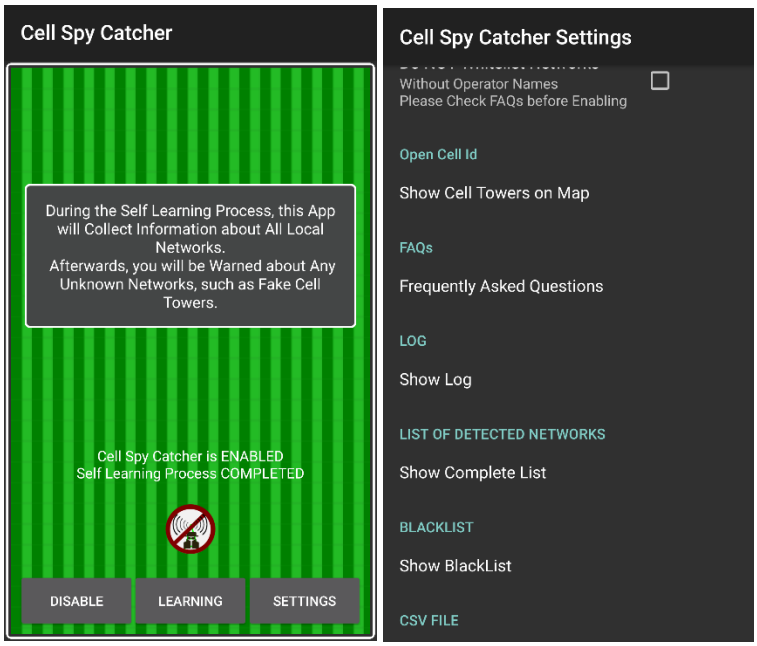


Figura 29: Capturas de Cell Spy Catcher

En la Figura 29 podemos ver la interfaz de la aplicación, así como el menú en el que se ven las opciones disponibles en la herramienta.

6.2.6 First Point

Esta herramienta realiza la detección del IMSI-Catcher mediante el uso de una tarjeta USIM con un applet insertado. La detección de una celda falsa se realiza en unos 400 ms según el fabricante. El método empleado es mandando peticiones a la celda, entre las que se incluyen mensajes falsos (para estudiar la respuesta de la BTS a ellos). También evalúan cambios en la frecuencia. El IMSI-Catcher debe ser de activo para poder realizar la detección.

Cuando un IMSI-Catcher es detectado en el dispositivo aparece una alerta pop up indicando la presencia de un IMISI-Catcher. El producto está asociado al número de teléfono, salvo la detección del IMSI-Catcher, que es usando una SIM proporcionada por ellos. Usa una pila de Elasticsearch, Logstash y Kibana para mostrar el número de incidencias, así como ataques de SS7, Diameter… que recibe el número.

En la Figura 30 podemos ver el esquema de cómo funciona esta herramienta. Se basa en enviar el tráfico a través de un nodo especial de SS7 el Signal Transfer Point (STP) hacia la red del fabricante. Allí el tráfico es analizado, dando lugar a las alertas en el caso de que hubiera un ataque.

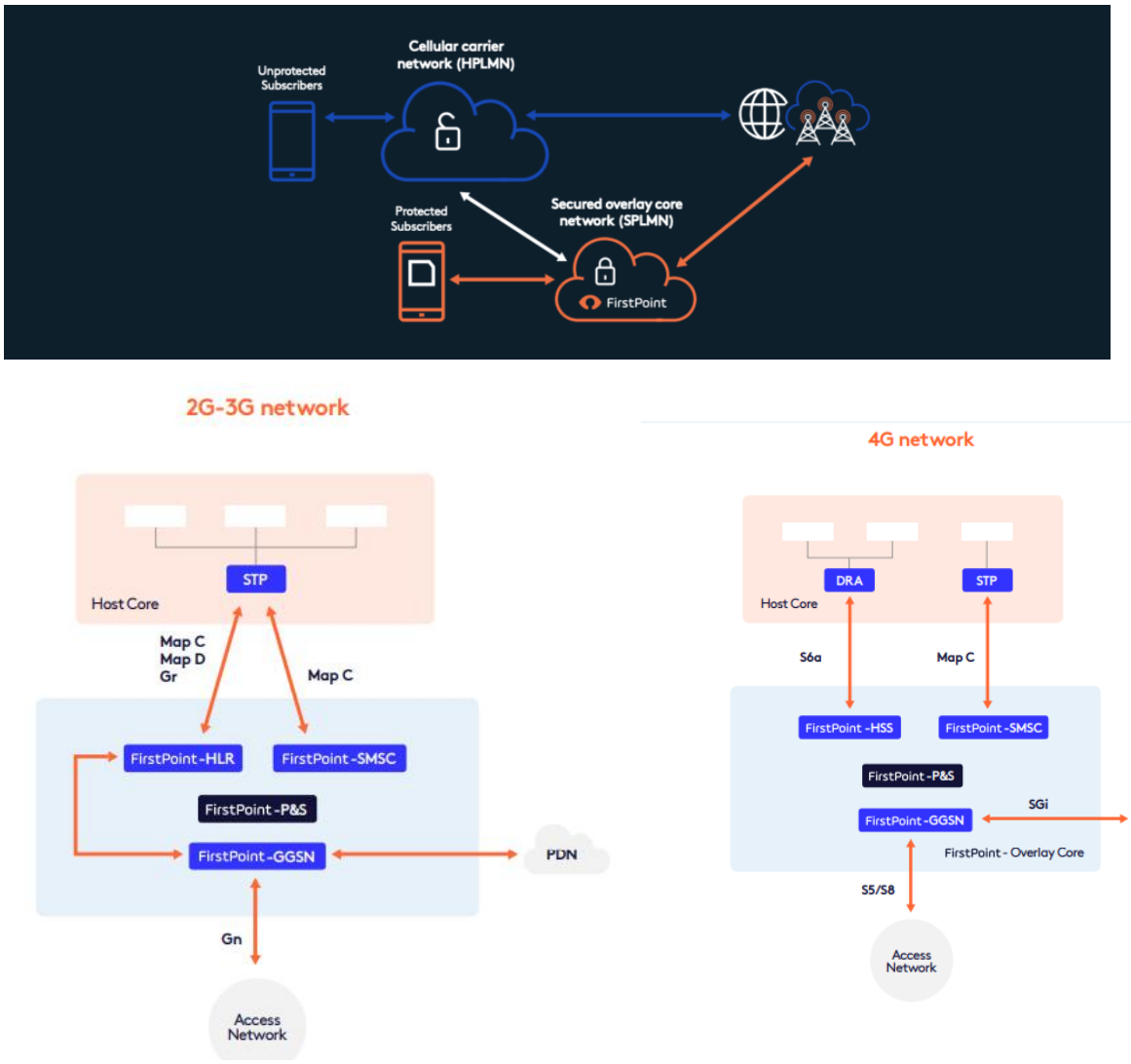


Figura 30: Esquema de la arquitectura

6.2.7 Tabla resumen

En esta tabla podemos ver en resumen las herramientas estudiadas, indicando en verde si utilizan el método de detección arriba explicado o no en rojo.

Método de detección	First Point	SecurCube	SnoopSnitch	AIMSICD	Cell Spy Catcher
Indica si es IMSI-Catcher	Si	No	Si	Si	Si
Frecuencias distintas	Si	Si	Si	Si	Si
Identificación de celdas	No	No	Si	Si	Si
Funcionalidades de la red	Si	No	Si	Si	Si
Valores de la configuración BTS	Si	Si	Si	Si	Si
Obligar a MS a registrarse	Si	No	Si	SI	No
Clientes UMTS	No	No	No	No	No
Cifrado	Si	No	Si	Si	No
Encarcelamiento celular	No	No	No	Si	No
Reenvío de tráfico	Si	No	No	No	No
Apariciones cortas	No	No	Si	No	Si
Precisa permisos *root*	No	No	Si	Si	No

Tabla 2: Tabla comparativa de los métodos de detección empleados por cada herramienta

Capítulo 7: Desarrollo de una BTS

En este capítulo vamos a abordar la realización de una estación de telefonía con el fin de poder comprobar si las soluciones presentadas en el capítulo anterior son capaces de detectar si hay un IMSI-Catcher en las inmediaciones.

En un primer momento, se comenzó a desplegar un IMSI-Catcher haciendo uso del SDR N210 empleando el software de Osmocom. [23]

Para ello se empleó una máquina virtual en la que los distintos elementos de la arquitectura de GSM fueron creados como servicios en el sistema. El software de los distintos servicios se puede encontrar en [23]. En la Figura 31 se puede ver un esquema de estos servicios. Sin embargo, la ejecución de todos ellos lo máximo que se logró fue una celda de telefonía en la que la señalización era correcta sin embargo el usuario no era capaz de obtener el audio al realizar llamadas.

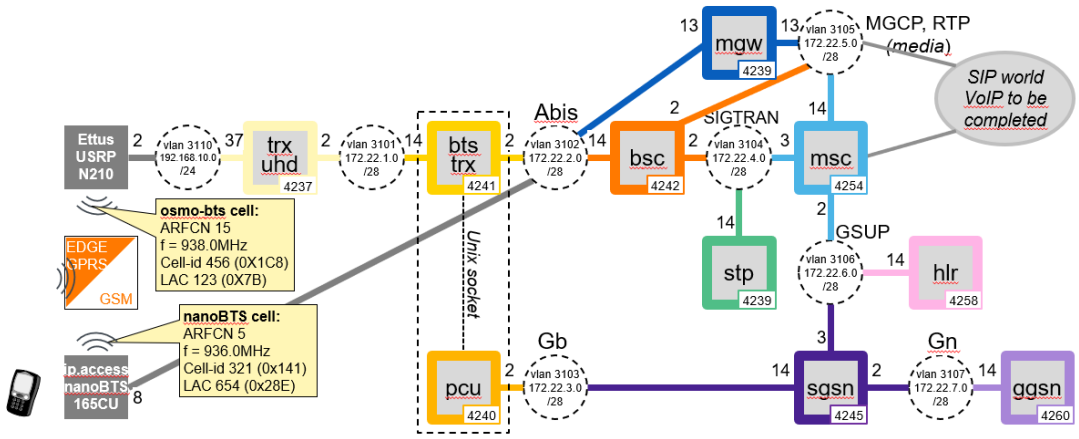


Figura 31: Esquema de los servicios implementados con Osmocom

Tras los infructuosos intentos con Osmocom se pasó a implementar el IMSI-Catcher haciendo uso de la FPGA BladeRFx40 mencionada anteriormente. El software empleado para emular la celda de telefonía es YateBTS. [24]

En la Figura 32 podemos ver es esquema de lo que se va a realizar con YateBTS.

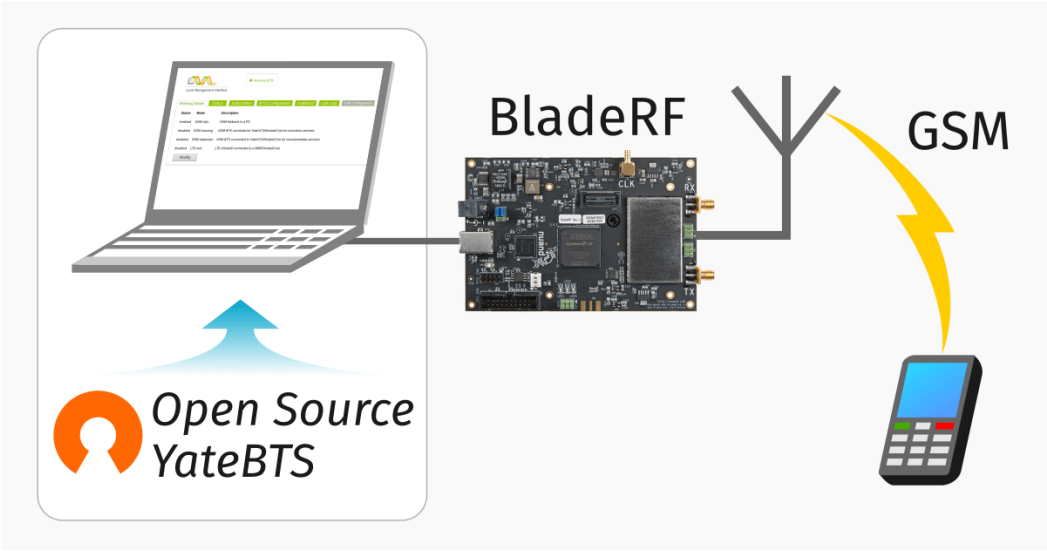


Figura 32: Esquema general de la implementación del IMSI-Catcher

YateBTS es un software que nos permite implementar una estación de telefonía con las capacidades de GSM y GPRS. Esta implementación se puede sincronizar con un núcleo de red de 2G o 4G. Esta implementado sobre un servidor de telefonía IP Yet Another Telephony Engine (Yate) el cual es de código abierto. Es capaz de soportar lenguajes de programación como *Javascript.* La elección de este software sobre otro software como Osmocom radica en su capacidad de personalización y no excesiva complejidad.

En el Anexo 1 nos encontraremos el modo de instalar este software. [7]

Una vez instalado vamos a configurar nuestra estación base. Pare ello necesitamos la información de las torres de telefonía cercanas. Esta información la obtuvimos empleando el analizador de espectro con el que localizamos a la frecuencia que emitían las estaciones cercanas. Obtuvimos el valor de frecuencia central obtenido en las señales y luego empleando [25] obtuvimos el ARFCN de la celda, el cual nos permite elegir el canal físico de la celda, el cual en GSM 900 se define como 890 +0.2 (n-1024) MHz para el canal de subida (siendo n el canal) y debiendo sumar 45 MHz al de subida para obtener la frecuencia del canal de bajada.

Luego empleando el HackRF One junto a GNU Radio siendo conocido el ARFCN de la celda pudimos capturar de forma exitosa con Wireshark los paquetes emitidos por estas antenas legitimas. Inspeccionando ese tráfico obtuvimos sus parámetros de igual forma que podría realizar un atacante.

En la Figura 33 podemos ver tráfico analizado con Wireshark en el que se aprecian los campos que llevan parte de la información configuración de esas celdas.

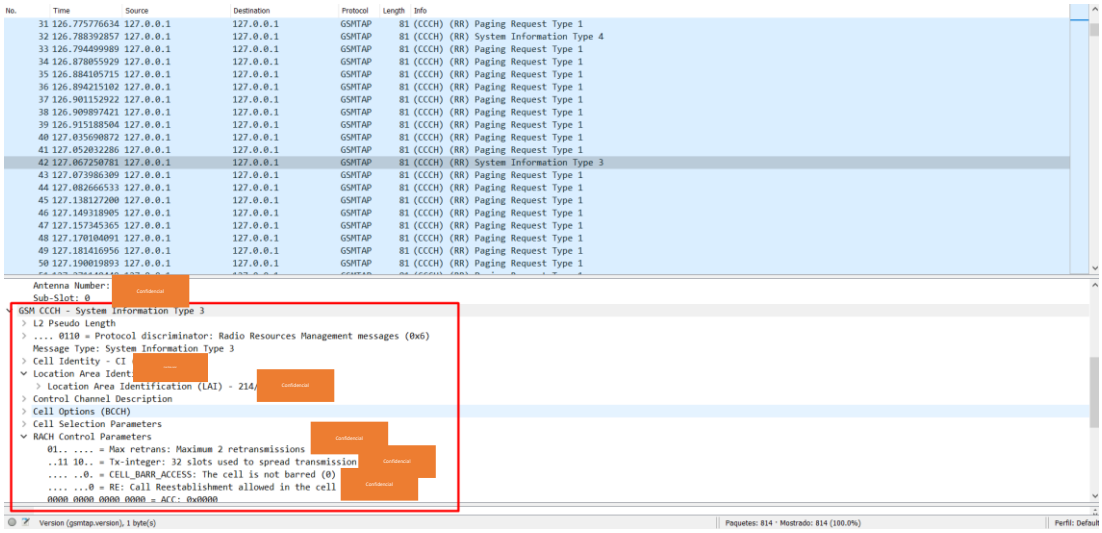


Figura 33: Captura de tráfico generado por una celda obtenido con Wireshark y HackRF One

Una vez obtenida esa información nos dispusimos a configurar nuestro IMSI-Catcher de acuerdo con los datos obtenidos.

Es importante tener en cuenta que en GSM existen los canales lógicos, de los que anteriormente habíamos hablado sólo del BCCH. En la Figura 34 podemos ver que canales lógicos existen en GSM y que deberán ser configurados.

Um Logical Channels		
Traffic Channels	Full rate traffic channel	TCH/F
	Half rate traffic channel	TCH/H
Dedicated control Channels	Standalone Dedicated Control Channel	SDCCH
	Fast Associated Control Channel	FACCH
	Slow Associated Control Channel	SACCH
Common control Channels	Broadcast Control Channel	BCCH
	Synchronization Channel	SCH
	Frequency Correction Channel	FCCH
	Paging Channel	PCH
	Access Grant Channel	AGCH
	Random Access Channel	RACH

Figura 34: Canales lógicos en GSM [5]

YateBTS emula los servicios principales que presenta una red GSM (2G). Además, también se incluye los elementos necesarios para GPRS. Podemos verlo en detalle en la Figura 35 cómo son los componentes que controlan el funcionamiento de YateBTS.

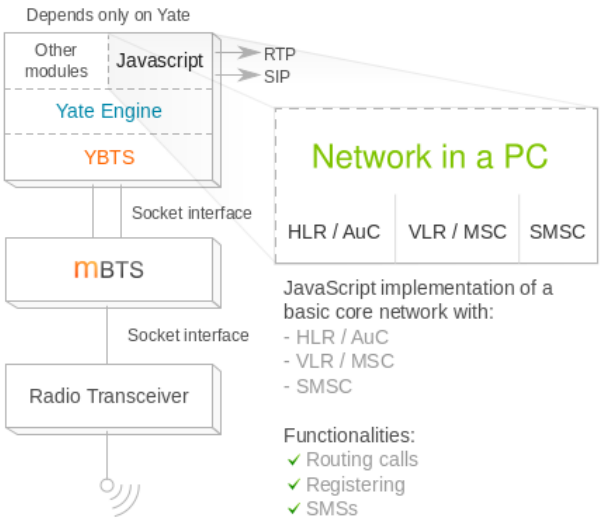


Figura 35: Esquema lógico del IMSI-Catcher empleando YateBTS

Podemos ver como los módulos mBTS y YBTS que controlan respectivamente la parte radio y los parámetros de configuración de GSM. También podemos ver el módulo Network in a PC que se encarga de gestionar la capa de red lo que nos permite por ejemplo ver los dispositivos registrados.

Para ello se cargó en la FPGA el software proporcionado por el fabricante, y se editaron los ficheros de configuración de YateBTS. En las siguientes Figuras comentaremos algunos de sus aspectos más destacados.

```
; Radio.Band: keyword: The GSM operating band.
; For non-multiband units this value must match the hardware.
; Valid values: 850, 900, 1800, 1900.
; THERE IS NO DEFAULT, YOU MUST SET A VALUE HERE!
Radio.Band=900

; Radio.C0: integer: The C0 ARFCN, also base ARFCN for a multi-ARFCN configuration.
; Valid values depend on the selected Radio.Band:
;  850   (GSM850): 128..251
;  900  (EGSM900): 0..124 or 975..1023
;  1800 (DSC1800): 512..885
;  1900 (PCS1900): 512..810
; THERE IS NO DEFAULT, YOU MUST SET A VALUE HERE!
Radio.C0=981

; Identity.MCC: string: Mobile Country Code, must have three digits.
; The value 001 is reserved for for test networks.
; Defaults to 001 (Test Network).
Identity.MCC=278

; Identity.MNC: string: Mobile Network Code, must have two or three digits.
; The value 01 is usual for test networks with a MCC value set on 001.
; Defaults to 01 (Test Network, only in association with Identity.MCC=001).
Identity.MNC=01

; Identity.LAC: integer: Location Area Code, 16 bits, values 0xFFxx are reserved.
; For multi-BTS networks, assign a unique LAC to each BTS unit.
; Interval allowed: 0..65280.
; Defaults to 1000 (arbitrary).
Identity.LAC=[redacted]

; Identity.CI: integer: Cell ID, 16 bits, should be unique.
; Interval allowed: 0..65535.
; Defaults to 10 (arbitrary).
Identity.CI=[redacted]
```

Figura 36: Configuración de la identificación de la celda

En la Figura 36 podemos ver los valores empleados para configurar la identificación de la celda, estos valores han sido recogidos con el tráfico capturado y con información interna.

```
; Identity.BSIC.BCC: integer: GSM Basestation Color Code; lower 3 bits of the BSIC.
; BCC values in a multi-BTS network should be assigned so that BTS units with
;  overlapping coverage do not share a BCC.
; This value will also select the training sequence used for all slots on this unit.
; Interval allowed: 0..7.
; Defaults to 2 (arbitrary).
Identity.BSIC.BCC=[redacted]

; Identity.BSIC.NCC: integer: GSM Network Color Code; upper 3 bits of the BSIC.
; Assigned by your national regulator; must be different from NCCs of other GSM
;  operators in your area.
; Interval allowed: 0..7.
; Defaults to 0.
Identity.BSIC.NCC=[redacted]
Identity.Shortname=AdrianYates

; Radio.PowerManager.MaxAttenDB: integer: Maximum transmitter attenuation level
;  in dB wrt full scale on the D/A output.
; This sets the minimum power output level in the output power control loop.
; Interval allowed: 0..80.
; Defaults to 10 (-10dB).
Radio.PowerManager.MaxAttenDB=10

; Radio.PowerManager.MinAttenDB: integer: Minimum transmitter attenuation level
;  in dB wrt full scale on the D/A output.
; This sets the maximum power output level in the output power control loop.
; Interval allowed: 0..80, must be less or equal to Radio.PowerManager.MaxAttenDB.
; Defaults to 0 (maximum power).
Radio.PowerManager.MinAttenDB=30
```

Figura 37: Configuración de la celda y niveles de potencia

Podemos ver en la Figura 37 más información de la configuración de la celda, así como los niveles de potencia radiada.

```
[gprs]
; This section controls basic GPRS operations.
; You should review all the parameters in this section.

; Enable: boolean: Advertise GPRS in C0T0 beacon and start service on demand.
; See also Channels.* in [gprs_advanced] to find out how many channels are reserved.
; Defaults to yes.
Enable=yes

; RAC: integer: GPRS Routing Area Code, as advertised in the C0T0 beacon.
; Interval allowed: 0..255.
; Defaults to 0 (arbitrary).
RAC=[redacted]

; RA_COLOUR: integer: GPRS Routing Area Color, as advertised in the C0T0 beacon.
; Interval allowed: 0..7.
; Defaults to 0 (arbitrary).
RA_COLOUR=[redacted]
```

Figura 38: Configuración de GPRS

En la Figura 38 podemos ver la configuración de GPRS, de acuerdo con la información interna.

```
; MinimumRxRSSI: integer: Minimum signal strength (in dB) of acceptable bursts.
; Bursts received at the physical layer below this threshold are ignored.
; Do not adjust without proper calibration.
; Interval allowed: -90..90.
; Defaults to -63.
MinimumRxRSSI=-90
```

```
; Radio.RxGain: integer: Receiver gain setting in dB.
; Ideal value is dictated by the hardware
; Interval allowed: 0..75.
; Defaults to 0 (but some radios provide their own calibrated default).
Radio.RxGain=40
```

Figura 39: Configuración de los niveles de potencia aceptado de los dispositivos que se conecten al IMSI-Catcher y la ganancia de recepción

La Figura 39 es muy relevante puesto que una mala configuración no permitirá que el dispositivo se registre en la red.

Estos ficheros se cargan al ejecutar el programa, por lo que no se aceptan cambios mientras el IMSI-Catcher se encuentra activo.

Una vez arrancada la estación, comenzamos a operar en ella, conectando los dispositivos.

Si escaneamos el entorno en busca de redes GSM, nos encontramos la Figura 40 en la que se ve nuestra red, la cual puede estar identificada por el PLMN ID o por la combinación del MNC+MCC. Hemos probado con varios móviles y algunos en vez de mostrar los números muestran el operador al que corresponden. Esta relación la podemos ver en [26]. También parece que hay una caché ya que cambiando el nombre posteriormente el cambio no se ve reflejado.

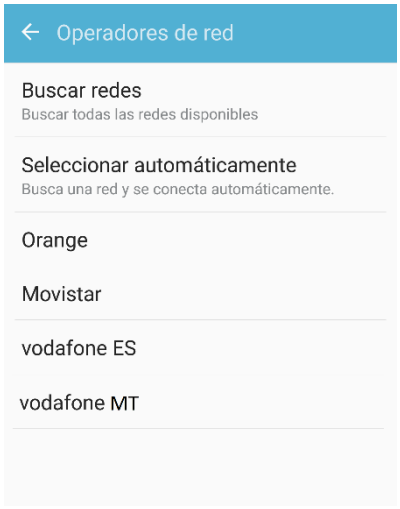


Figura 40: Búsqueda de redes con el IMSI-Catcher activo

Una vez registrado el dispositivo, el módulo Network in a PC nos envía un SMS en el que se nos indica nuestro número asociado dentro de la red. Esto lo podemos ver en la Figura 41.

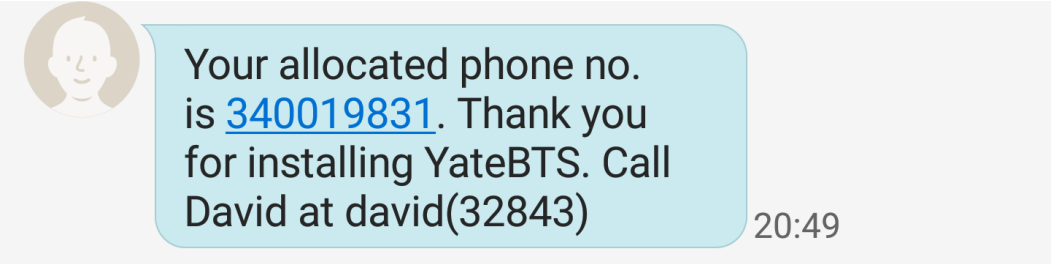


Figura 41: SMS de bienvenida de YateBTS indicando el número que recibe el dispositivo

Una vez el dispositivo se ha registrado, podemos ver dentro del IMSI-Catcher el IMSI de los dispositivos.

```
2021-08-11_11:11:00.861522 <nipc:INFO> Got user.register for
imsi='26 Confidencial 6', tmsi=''

2021-08-11_11:11:00.862291 <nipc:INFO> Allocated random number

2021-08-11_11:11:00.875838 <nipc:INFO> Registered imsi 2( Confidencial )76
with number 340136876
```

Posteriormente, podemos ver en la Figura 42 SMS y llamadas realizadas entre dispositivos que se encuentran en la misma red.

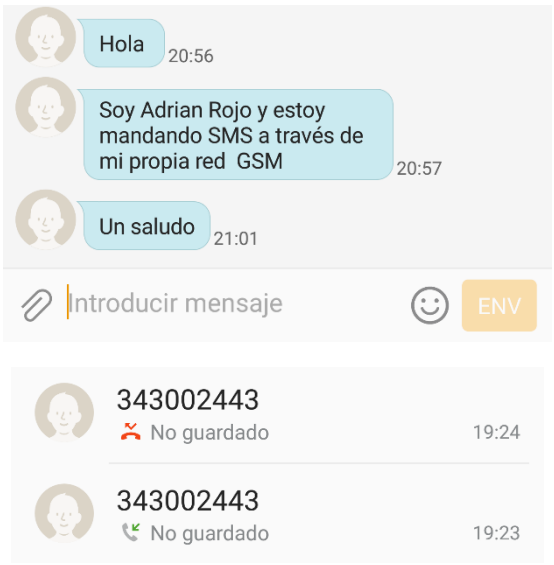


Figura 42: SMS y llamadas realizadas a través del IMSI-Catcher

Dentro del IMSI-Catcher podemos ver también estas comunicaciones sin que el usuario sea consciente de la intercepción.

```
2021-09-09_20:57:53.568522 <ybts:INFO> MT SMS 'Soy Adrian Rojo y estoy
mandando SMS a través de mi propia red GSM' to (0x7fe72c002960)
TMSI=007b0001 IMSI=26 Confidencial 1 finished

2021-09-09_20:57:53.568796 <nipc:INFO> Delivered sms from imsi
2 Confidencial 3 to number 340019831
```

Dentro de las funcionalidades de Network in a PC tenemos la opción de listar a los usuarios registrados:

```
nipc list registered

IMSI            MSISDN

--------------- -------------

2 Confidencial 31 | 340019831

2 Confidencial 57 | 342032057

2 Confidencial 43 | 343002443
```

Capítulo 8: Pruebas de detección del IMSI-Catcher

Una vez vistas las herramientas disponibles en el mercado y desarrollado el IMSI-Catcher vamos a evaluar la eficiencia de detección de estas herramientas. Para ello de las presentadas hemos elegido aquellas que no precisan acceso root, puesto que no serían muy eficaces para el público general.

8.1 First Point

Para la prueba, tal y como se indicó es necesario emplear su tarjeta USIM, así como conectarse a un punto de acceso de red específico. Eso les permite realizar el reenvío del tráfico a través de SS7 a su red de análisis y tener un seguimiento del dispositivo que se puede ver mediante un panel de mandos en un servidor que contiene una pila de Elasticsearch-Logstash-Kibana.

Como se ha mencionado este registro es individual por cada número. Esta prueba se realizó de forma síncrona, para poder controlar de forma adecuada el estado de los dispositivos.

Para la conexión se encontraron múltiples problemas, pues en múltiples ocasiones la red a la que se conectaba quedaba sin servicio durante un rato. Se reportó y se lo comunicaron a su proveedor en España. Esto fue un problema recurrente durante las pruebas

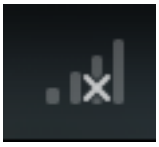


Figura 43: Fallo ocasionado al realizar el reenvío del tráfico.

Una vez estabilizados los servicios se procedió a conectar IMSI-Catcher en las inmediaciones del dispositivo con la USIM modificada. Tras realizar la conexión y encontrarse registrado en la red, las primeras veces no pasó nada y el servicio continuo de la forma habitual, aunque aparecía que el servicio de red se bloqueaba, al igual que pasaba al estar conectado a una celda legítima. Tras varios intentos el pop-up anunciado apareció en el dispositivo indicando la presencia de IMSI-Catcher.

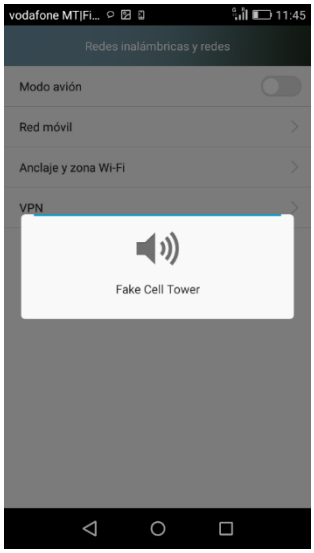


Figura 44: Pop-up anunciando la presencia de un IMSI-Catcher

Me comentaron que el pop-up aparecía tras el vencimiento de un temporizador, por lo que probando a desconectar el IMSI-Catcher este pop-up seguía apareciendo. Lo podemos ver en

Cómo, aunque no haya servicio el pop-up sigue apareciendo.

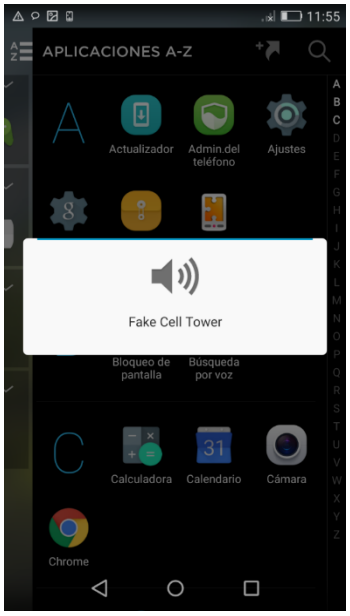


Figura 45: Pop-up apareciendo con el IMSI-Catcher apagado.

Lo que aparecía en el panel de mandos en el servidor que contiene una pila de Elasticsearch-Logstash-Kibana lo podemos ver en la Figura 46 en que podemos ver a la hora que el IMSI-Catcher se ha conectado.

Figura 46: Panel de mandos con la información de seguridad detectada por la USIM

Según el fabricante tras el registro de la información en la plataforma debería llegar un SMS con la información del IMSI-Catcher, pero no llegó nada.

8.2 Cell Spy Catcher

Cuando conectamos nuestro dispositivo a un IMSI-Catcher, nos aparece la siguiente pantalla que podemos ver en la Figura 47 como pop-up.

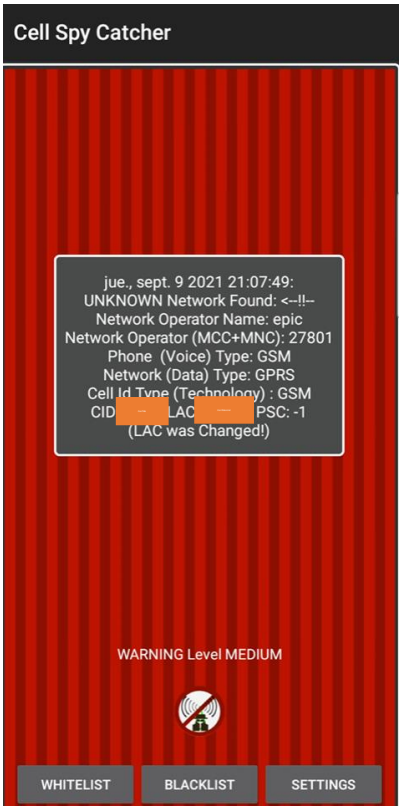


Figura 47: Alerta de IMSI-Catcher generada por Cell Spy Catcher

En ella podemos ver como se nos avisa de que la celda a la que nos hemos conectado es sospechosa. Se nos adjunta la información de la celda, como sería el PLMN id, MCC+MNC, los servicios que esta oferta y sus identificadores (Cell ID y LAC). Además, se nos indica el motivo por el que esta red es sospechosa para la herramienta. Una vez realizado esto la herramienta nos da la opción de seleccionar si esta red va a estar en la lista blanca (Permitidas) o negra (No permitidas) de redes. Sin embargo, aunque seleccionemos que deseamos añadirla a la lista negra el dispositivo seguirá conectado a ella.

Lo que se ha observado con esta herramienta es la ingente cantidad de falsos positivos que arroja, aunque seleccionemos una red como legítima tras el proceso de aprendizaje. Si accedemos al reporte de las redes detectadas por las herramientas podemos ver como multitud de ellas son catalogadas como ilegítimas.

DateAndTime	**Event**	**NetworkOperatorName**	**MCC+MNC**	**PhoneVoiceType**	**NetworkDataType**	**CellTechnology**	**CID/BID/CI**	**LAC/NID/TAC**	**PSC/SID/PCI**	**Comment**	**WarningLevel**	**Duration**
11/08/2021 11:12	UNKNOWN Network Found	Movistar	21407	GSM	UNKNOWN	Unknown	0	0	-1	(LAC was Changed!)	MEDIUM	36 sec

11/08/2021 11:11	UNKNOWN Network Found	000000	0	GSM	UNKNOWN	Unknown	0	0	-1	(LAC was Changed!)	MEDIUM	26 sec
11/08/2021 11:10	UNKNOWN Network Found	vodafone MT |	27801	GSM	GPRS	GSM	Confidencial		-1	(Warning Suppressed)	LOW	53 sec
11/08/2021 11:07	New Network Found	vodafone ES |	21401	GSM	EDGE	GSM	Confidencial		-1			

Tabla 3: Resultados obtenidos por Cell Spy Catcher de redes legítimas e ilegitimas

Podemos ver como la red del IMSI-Catcher con MCC+MNC 27801 es detectada, con riesgo bajo mientras que redes legítimas son marcadas como riesgo medio.

Cómo conclusión de la evaluación de estas dos herramientas, podemos considerar que la más eficaz es Cell Spy Catcher ya que, aunque arroja bastantes falsos positivos no tuvo en ningún caso como sí tuvo la otra herramienta de falsos negativos.

Capítulo 9: Conclusiones

La realización de este proyecto ha sido muy gratificante ya que me ha permitido aunar conocimientos de las ramas principales de la ingeniería de telecomunicaciones, como serían las comunicaciones radio, la electrónica encarnada en las FPGA, así como el software y conocimiento de protocolos que cubre el área de telemática. Una vez más la organización a la hora de realizar el proyecto ha sido un aspecto fundamental, y gradezco a mis tutores el haber insistido en ello.

Para el desarrollo del proyecto ha sido necesario un aprendizaje a mayores respecto a las comunicaciones móviles mediante radio, ya que, aunque las había visto durante mis estudios no a la profundidad requerida ni enfocándose en los aspectos de seguridad de las diferentes generaciones de comunicaciones móviles.

Encontrar una necesidad y tratar de solucionarla haciendo uso de las herramientas disponibles ha sido muy enriquecedor. Probar múltiples herramientas alternativas con la intención de ver si estas cumplían las necesidades del proyecto o sin embargo eran más adecuadas para otro tipo de escenario, me ha permitido explorar una gran cantidad de soluciones.

Una vez realizada la selección de las herramientas a evaluar en nuestro proyecto, se ha pasado a realizar el desarrollo de un IMSI-Catcher funcional, siendo la tecnología elegida GSM. Tal y como se ha visto, se realizaron dos implementaciones con 2 SDR distintos que arrojaron resultados similares pero la complejidad de Osmocom respecto a los resultados obtenidos fue diferencial para decantarme por el uso de YateBTS.

La implementación del IMSI-Catcher fue un proceso arduo, tanto por la cantidad de parámetros a configurar como por la dificultad de encontrar las casusas de fallo, el contar con el analizador de espectro facilitó el trabajo.

El haber podido usar varios SDR ha sido una suerte, ya que ha permitido hacer más pruebas, pero el software de código abierto que hay disponibles para ellos es muy complejo y propenso a fallar.

Una vez desarrollado el IMSI-Catcher, siendo la celda creada funcional, para la realización de llamadas, así como el envío y recepción de SMS procedimos a obtener el IMSI de los usuarios. Este fue obtenido como se vio en el capítulo 6, revelando que es una vulnerabilidad fácilmente explotable.

Tras probar el IMSI-Catcher comenzaron las pruebas con las herramientas de detección. Ambas herramientas realizaron una detección de la presencia del IMSI-Catcher, pero la que más eficaz fue sin ninguna duda fue Cell Spy Catcher ya que, aunque arroja bastantes falsos positivos no tuvo en ningún caso como la herramienta de la empresa israelí falsos negativos.

Como conclusión, en los dispositivos móviles de los usuarios la introducción de las nuevas generaciones de redes de telefonía ha ido reduciendo el alcance de este tipo de ataques. Pero son relativamente fáciles de ejecutar sin un gran dispendio. Para redes IoT o M2M que siguen empleando la red GSM este tipo de ataques sigue motivando una amenaza real. Además, la existencia de *Jammers* que provocan que se pueda forzar a los usuarios a emplear tecnologías anteriores hace que esta vulnerabilidad esté al orden del día.

Aunque con la introducción de las nuevas redes de 5G este tipo de ataques van a disminuir en eficacia, tal y como se ha comentado no debemos caer en el error de considerar que estamos

completamente seguros, ya que parte de la red de 5G será 5G non-standalone manteniendo operativa parte de la red 4G que si se puede ver más expuesta a este tipo de ataques.

9.1 Objetivos conseguidos

En la siguiente lista se van a detallar los objetivos conseguidos durante la realización del proyecto:

- Planificación con hitos de un proyecto y presentación periódica de avances.
- Mayor conocimiento de la arquitectura de las redes móviles en todas sus generaciones.
- Investigación sobre los IMSI-Catchers.
- Recopilación de herramientas en el mercado para la detección de
- Creación de una celda de telefonía GSM funcional y su uso como IMSI-Catcher.
- Empleo de un SDR para tal fin, implementado en una FPGA.
- Evaluación de las herramientas recopiladas en un caso de uso real.

Capítulo 10: Futuras líneas de trabajo

En este capítulo, vamos a explorar futuras líneas de trabajo para el proyecto desarrollado. Debiendo partir de la base del proyecto que se he realizado, es decir la investigación sobre los IMSI-Catchers y el IMSI-Catcher desarrollado plantean las siguientes opciones como principales vías de trabajo

10.1 Perfeccionar las herramientas de detección

Partiendo de la aplicación de la aplicación más eficaz de las analizadas que sería Cell Spy Catcher mejorar su índice de falsos positivos, ya que como hemos visto estos son muy numerosos. Cell Spy Catcher incorpora algunos de los posibles métodos de detección, pero no todos, como los que se basan en interactuar con la estación de telefonía.

Tratar de vincularlo además con otras bases de datos distintas a OpenCellID, como Radiocells [27] o Cell mapper [28] podrían reducir los falsos positivos detectados.

10.2 Desarrollo de rastreadores en LTE o 5G

Haciendo uso de los SDR con los que contamos, una opción que sería tratar de realizar una celda de telefonía de tecnologías superiores a GSM con la que tal y como hemos mencionado rastrear el GUTI.

Hay proyectos de código abierto como srsRAN [29] que han desarrollado una suite de programas con los que poder realizar estas implementaciones. Aunque hay que tener en cuenta que al precisar de SDR muy específicas para su manejo el no tener el modelo pedido puede significar no lograr realizar la implementación.

10.3 Desarrollo de Jammer

Tal y como se ha comentado el uso de IMSI-Catchers junto a *Jammers* es muy habitual. Estos pueden ser implementados haciendo uso de SDR muy económicos, como el HackRF One visto anteriormente. Una futura línea de trabajo sería implementar en conjunto el IMSI-Catcher junto al *Jammer.*

Anexo 1. Instalación de YateBTS en la FPGA BladeRFx40

En primer lugar, debemos obtener el código fuente de la FPGA del repositorio Git del fabricante. Para no tener problemas con el Git debemos resetear el repositorio.

```
git clone https://github.com/Nuand/bladeRF.git ./bladeRF

cd ./bladeRF
```

git reset --hard 3a411c87c2416dc68030d5823d73ebf3f797a145

Una vez obtenido el código fuente debemos compilarlo para obtener el código máquina que empleará la FPGA.

```
mkdir build

cd build

cmake -DCMAKE_BUILD_TYPE=Release -DCMAKE_INSTALL_PREFIX=/usr/local -
DINSTALL_UDEV_RULES=ON ../
```

Una vez preparado el sistema debemos emplear los siguientes comandos para crear el proyecto e instalar los ficheros de la FPGA.

```
make && sudo make install && sudo ldconfig
```

Ahora debemos obtener el software de Yate y YateBTS el cual descargamos en la dirección del fabricante de a FPGA para asegurarnos su compatibilidad con la FPGA.

```
mkdir ~/software/bts/

cd ~/software/bts/

wget https://nuand.com/downloads/yate-rc-2.tar.gz

tar xfz yate-rc-2.tar.gz
```

Se debe compilar e instalar ahora desde sus códigos fuente Yate y YateBTS, respectivamente.

```
cd ~/software/bts/yate

./autogen.sh

./configure --prefix=/usr/local

make
```

En este paso todo debería ir sin ningún problema, ni código de error.

```
sudo make install

sudo ldconfig

cd ~/software/bts/yatebts

./autogen.sh

./configure --prefix=/usr/local
```

```
make
```

En este paso todo debería ir sin ningún problema, ni código de error.

```
sudo make install
```

```
sudo ldconfig
```

Con esto estaría listo el software que debe ser configurado con el fichero *ybts.conf* del que hemos visto en el capítulo 7 parte de su configuración.

Una vez editado el fichero para ejecutar el sistema debemos ejecutar el comando

```
yate
```

Referencias

[1] https://voyager.jpl.nasa.gov/mission/interstellar-mission/, última visita: septiembre 2021

[2] https://defence.nridigital.com/global_defence_technology_special/the_evolution_of_electronic_warfare /última visita: septiembre 2021

[3] https://www.ericsson.com/en/mobility-report,última visita: septiembre 2021

[4] https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf, última visita: septiembre 2021

[5] A. Kukushkin, "Introduction to mobile network engineering GSM, 3G-WDMA, LTE and the road to 5G", WILEY, USA, 2018

[6] A. Dabrowski, N. Pianta, T. Kleep, M Mulazzani, E. Weippl "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers", 2014

[7] https://github.com/nuand/bladeRF/, última visita: septiembre 2021

[8] https://www.ettus.com/all-products/un210-kit/, última visita: septiembre 2021

[9] https://greatscottgadgets.com/hackrf/one/, última visita: septiembre 2021

[10] http://bibing.us.es/proyectos/abreproy/11458/fichero/PFC%252FCapitulo05+-+Java+Card+en+los+dispositivos+moviles.pdf/, última visita: septiembre 2021

[11] https://www.cse.iitb.ac.in/~vishalprajapati08/Study/CS649/GSM%20and%20UMTS%20Security%20Report.pdf, última visita: septiembre 2021

[12] https://www.netmanias.com/en/post/blog/5929/lte/lte-user-identifiers-imsi-and-guti, última visita: septiembre 2021

[13] https://www.gsma.com/spectrum/wp-content/uploads/2020/06/Legacy-mobile-network-rationalisation.pdf, última visita: septiembre 2021

[14] https://www.techplayon.com/5g-reference-network-architecture/, última visita: septiembre 2021

[15] https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication, última visita: septiembre 2021

[16] R. Borgaonkar, A. Shaik, "5G IMSI Catchers Mirage", última visita: septiembre 2021

[17] https://securcube.net/bts-tracker/, última visita: septiembre 2021

[18] https://opensource.srlabs.de/projects/snoopsnitch/wiki, última visita: septiembre 2021

[19] https://opensource.srlabs.de/projects/snoopsnitch/wiki/IMSI_Catcher_Score, última

visita: septiembre 2021

[20] https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector, última visita: septiembre 2021

[21] https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/wiki/Technical-Overview, última visita: septiembre 2021

[22] https://www.fp-mg.com/imsi-catcher-protection/, última visita: septiembre 2021

[23] https://osmocom.org/projects/cellular-infrastructure, última visita: septiembre 2021

[24] https://yatebts.com/, última visita: septiembre 2021

[25] https://www.sqimway.com/gsm_arfcn.php, última visita: septiembre 2021

[26] https://www.mcc-mnc.com/, última visita: septiembre 2021

[27] https://radiocells.org/, última visita: septiembre 2021

[28] https://www.cellmapper.net/map?lang=es, última visita: septiembre 2021

[29] https://www.srslte.com/, última visita: septiembre 2021