UNIVERSIDAD DON BOSCO
VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN
SEGURIDAD EN SISTEMAS DE RADIO COMUNICACIÓN MÓVIL CELULAR

PARA OPTAR AL GRADO DE MAESTRO
EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMATÍCOS

ASESOR: MG. MELVIN GARCÍA ARDÓN
PRESENTADO POR: BAYARDO ALVARENGA MARTÍNEZ

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.
Agosto 2018

Dedicatoria

A mi familia por su apoyo incondicional.

Agradecimientos

A Dios por permitirme realizar este trabajo el cual enriquecerá y dará un aporte importante en mi vida profesional.

A mis padres Celina Martínez y Luis Alfonso por todo el apoyo brindado.

A mi Tía Dina Gamero, por haberme motivado a iniciar mis estudios de postgrado.

A mi amada esposa Alicia Mejía, por su incondicional apoyo a lo largo de cada asignatura cursada.

Al cuerpo docente, por los conocimientos aportados sobre todo en aquellas áreas relacionadas con el estudio de la criptografía, en un ambiente de respeto, confianza y aprendizajes compartidos.

A Melvin García, por fungir su rol como asesor y brindar el acompañamiento metodológico durante el proceso de la presente Tesina.

Resumen

En el presente escrito se busca realizar una investigación que permita explorar y explicar el funcionamiento de la seguridad en las redes de telefonía móvil, al mismo se pretende investigar y documentar sobre el funcionamiento de los posibles vectores de ataques a los que estas tecnologías están expuestas. No obstante aunque en el presente escrito se hace mención sobre algunas de las debilidades en la criptografía de estos sistemas, se hará especial énfasis en el ataque de suplantación de estación base transmisora (BTS), mejor conocido como ataque de estación base falsa, con el propósito de abordar la temática con un enfoque desde una perspectiva orientada a la práctica, dado que este tipo de ataque en particular funciona como un punto de partida hacia otros vectores de ataque. Adicionalmente se busca aportar las bases para la creación de normativas, estándares y recomendaciones de seguridad de la información para dichos sistemas.

Índice

Capítulo 1 1
1.1 Introducción 1
1.2 Objetivos Generales 2
1.3 Objetivos Específicos 2
1.4 Alcances y Limitaciones 3
Capítulo 2 4
2.1 Redes Móviles de Segunda Generación 4
2.2 Arquitectura de una red GSM. 5
2.3 Arquitectura de red GPRS. 16
2.4 Arquitectura de red EDGE. 18
2.5 El Módulo SIM. 21
Capítulo 3 24
3.1 Seguridad en Comunicaciones Móviles de Segunda Generación 24
3.2 Proceso de autenticación en GSM, GPRS y EDGE. 25
3.3 Esquema de seguridad en GSM mediante el uso del algoritmo A5/1. 26
3.4 Cifrado de datos basados en algoritmos de flujo LFSR. 29
Capítulo 4 31
4.1 Redes Móviles de Tercera Generación 31
4.2 Arquitectura de red UMTS.. 32
Capítulo 5 36
5.1 Seguridad en Comunicaciones Móviles de Tercera Generación 36
5.2 Esquema de Seguridad en UMTS/WCDMA. 37
5.3 Mecanismo de Autenticación en UMTS/WCDMA. 38
5.4 Mecanismo de control de integridad en UMTS/WCDMA. 39
5.5 Mecanismo de control de confidencialidad en UMTS/WCDMA. 40
5.6 Algoritmo de cifrado por bloque KASUMI. 41
Capítulo 6 45
6.1 Vectores de Ataques 45
6.2 Ataque de estación base falsa. 46
6.3 Ataque de degradación en UMTS. 53
Capítulo 7 55
7.1 Conclusiones 55
8. Fuentes de Información y Referencias 57
9. Anexos 58
9.1 Anexo A. 58
9.2 Anexo B. 59
9.3 Anexo C. 60
9.4 Anexo D. 61

Capítulo 1

1.1 Introducción

Los avances tecnológicos en las comunicaciones móviles han demostrado en los últimos años un crecimiento exponencial y la prueba más palpable de ello es la masificación y diversificación de los servicios de banda ancha, lo cual ha llevado a que algunos de los aspectos que mayor importancia han tomado, es el hecho de contar con mayores velocidades que estén al nivel de las exigencias que los servicios antes mencionados demandan, asimismo hacer un uso racional y eficiente del espacio radioeléctrico utilizado para brindar dichos servicios. No obstante el tema de la seguridad en los canales de comunicación en las distintas tecnologías destinadas a las comunicaciones móviles es un tema poco explorado pero dado que el uso de las redes móviles se ha vuelto parte de la vida cotidiana del público en general, se vuelve un tema que es tan importante considerarlo, de la misma manera en que se aborda en las redes fijas, sobre todo por el simple hecho que los servicios fijos y móviles son en alguna medida complementarios.

El enfoque metodológico en el presente consiste en llevar a cabo una exploración del tema propuesto, desde una perspectiva cualitativa basada en la técnica de investigación de tipo documental, la cual consistirá en la recopilación de información, documentar o hacer referencia a antecedentes de diversos autores que puedan sustentar y aportar al desarrollo del proyecto.

Entonces tomando como base los puntos expuestos anteriormente, algunas de las preguntas iniciales que pueden formularse son: ¿Qué tan seguras son las redes móviles? ¿Cómo funciona la seguridad en las redes móviles?, ¿Qué tan vulnerables pueden ser?, ¿Existen vectores de ataques?, ¿Cuáles podrían ser dichos vectores de ataques?, ¿qué tan complejo o factible puede ser para un posible atacante vulnerar la seguridad en una red móvil? y ¿Qué herramientas existen actualmente, que permitan un posible ataque y que tan accesibles pueden ser dichas herramientas?

1.2 Objetivos Generales

Al final del proyecto se busca sentar una base para la elaboración de normas, medidas y recomendaciones en temas de seguridad en las redes de telefonía móvil, tomando como base los distintos vectores de ataques, así como también normativas como la ISO 27001, recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), OWASP, entre otros.

1.3 Objetivos Específicos

- Estudiar, comprender y analizar el funcionamiento de los mecanismos de seguridad en las radiocomunicaciones móviles.
- Fundamentar un precedente que motive la creación y estandarización de procesos de auditorías de seguridad en las comunicaciones móviles de banda ancha.

1.4 Alcances y Limitaciones

Entre los aportes más relevantes que se busca proporcionar son los cimientos que permitan no solo futuras propuestas para la creación de una norma que permita parame trizar los aspectos de gestión de la seguridad de la información, sino también fomentar la formación de especialistas en El Salvador, acerca del tema propuesto.

Se investigarán los principales aspectos de la seguridad en las redes de comunicación móvil, que permitirán el estudio y la comprensión de los posibles vectores de ataques e identificación de vulnerabilidades, con el propósito que sirvan como punto de partida para futuras propuestas que puedan normalizar los aspectos de seguridad en los procesos de comunicación para banda ancha en servicios móviles.

Es importante mencionar que en este documento no se mostrarán pasos concretos para realizar ningún tipo de ataque, dado que el espacio radioeléctrico utilizado por los operadores que poseen los derechos de explotación del mismo, es un bien demanial propiedad del estado y el propósito de esta investigación no es fomentar ningún tipo de acto delictivo, por el contrario busca fomentar la importancia que tiene desarrollar normativas que aporten a la seguridad en las comunicaciones móviles de tipo celular.

Capítulo 2

2.1 Redes Móviles de Segunda Generación

Global System for Mobile Communications o (GSM) por sus siglas en inglés, se considera un punto de partida para la segunda generación móvil celular, el cual es un sistema desarrollado a partir de 1982, a través de un grupo de trabajo multidisciplinario conformado por diversos sectores, el cual tenía como principal misión desarrollar un estándar europeo para un nuevo esquema para la telefonía móvil que fuera completamente digital. Durante su implementación se tuvo como primordial objetivo subsanar muchos de los inconvenientes técnicos que presentaban los sistemas analógicos de telefonía móvil celular, que se habían implementado en Europa años antes, sin embargo existieron algunos problemas de compatibilidad los cuales fueron resueltos paulatinamente y se pasó por varios procesos y pruebas, aun cuando se utilizaban estándares similares. En el grupo multidisciplinario a cargo participaron cerca 26 compañías de diferentes países europeos de telecomunicaciones. A inicios de los años 90´s se concluyeron con los parámetros técnicos para la primera versión del estándar el cual se conoce como GSM-900, por haber sido implementado originalmente para la banda de 900 MHz, luego se siguió con la versión para 1800, 1900 y 850 MHz, respectivamente.

2.2 Arquitectura de una red GSM

Uno de los mayores retos que se presentan durante la etapa de diseño de una red móvil celular, son las limitantes en cuanto al ancho de banda de asignado

para el establecimiento de llamadas o para tráfico de datos por lo que juega un papel muy importante la planificación para realizar una distribución efectiva de las frecuencias asignadas para dichos servicios. Los operadores telefónicos tienen asignadas porciones de espectro radioeléctrico donde dichas porciones son utilizadas para establecer y organizar todos los segmentos de comunicación entre el terminal del usuario y la red, es esa razón que para temas de cobertura se planifican con base a arreglos de antenas para formar las celdas, ya que hacer mediante un único sistema radiante tendría grandes inconvenientes, haciendo ineficiente la gestión de las frecuencias disponible, esto también se relaciona con la distribución de los canales, lo cual se relaciona directamente con las técnicas de multiplexación, ya sea por tiempo, frecuencia, código, entre otros. Para el caso específico de GSM es muy común utilizar técnicas de multiplexación por tiempo o mejor conocido como Time Division Multiple Access, por sus siglas en inglés, acceso múltiple por división de tiempo TDMA, para la separación entre las bandas contiguas tanto en la recepción como en la transmisión.

En casos donde se requiere separar las bandas de frecuencias que subdividen canales adyacentes los cuales utilizan técnicas de multiplexación por frecuencias o mejor conocido como Acceso Múltiple por División de Frecuencia o FDMA, existen otras técnicas para propósitos específicos brindan las condiciones técnicas para que las celdas puedan convivir en un entorno electromagnético de manera eficiente. Tal es el caso del Acceso Múltiple por división de espacio SDMA, el cual brinda una

mejor distribución del espacio entre bandas. También se cuenta con técnicas que permiten la reutilización de frecuencias a través de saltos de portadoras de manera aleatoria, como es el caso de FHMA por sus siglas en ingles Acceso Múltiple por Saltos de Frecuencia.

Dentro de la arquitectura convencional utilizada en GSM, se tienen algunos elementos que cumplen con tareas específicas, como es el caso del subsistema de estación base transceptora BSS que está conformado por la estación base, la etapa de control de las estaciones conocida como MSC, además de las bases de datos donde se llevan los registros de la red del operador tanto para los usuarios como el anfitrión, conocidos como VLR y HLR, respectivamente. Cabe destacar que en una red GSM generalmente se definen distintos canales que cumplen con diferentes propósitos, como por ejemplo hay canales definidos para señalización, tráfico de voz y datos, canales de control, entre otros.

En la división en celdas a través de estaciones base, el sistema debe tener la capacidad de sobrellevar un tráfico considerable de usuarios, con muchos de ellos utilizando la red al mismo tiempo. En caso de que sólo estuviera disponible una única antena para todos los usuarios, el espectro radioeléctrico aprovechable se reduciría considerablemente debido a un uso ineficiente del mismo. La alternativa más práctica para subsanar este problema es hacer uso una técnica de planificación del espectro conocida como reutilización de frecuencias disponibles.

Esto implica que en vez utilizar una sola antena que lo único que hará es hacer ineficiente el sistema, se colocan estratégicamente varias antenas según temas de interés de cobertura, el sistema se configura de manera tal que cada una de las antenas utilice frecuencias diferentes a las que son adyacentes, y reutilizando aquellas frecuencias para todas las antenas que no sean adyacentes. Se reserva un determinado rango de frecuencias con sus correspondientes canales asignados. A dichos rangos se les conoce como enlace subida y enlace de bajada (Uplink y Downlink).

Por lo general una estación base en GSM puede lograr un radio de cobertura en sus alrededores de varios kilómetros en zonas urbanas y puede alcanzar para efectos prácticos hasta unos 30 kilómetros aproximadamente para zonas rurales, esto varía según parámetros técnicos como su potencia, banda de frecuencias ya que a mayor frecuencia menor longitud de onda, por consiguiente menor alcance y el perfil orográfico del entorno. Sin embargo, la cantidad de usuarios que puede soportar cada estación base depende mucho el ancho de banda asignado el cual para efectos de eficacia del aprovechamiento del espectro asignado se divide en canales, que el controlador de estación establece para cada una de las estaciones, lo anterior permite que las estaciones base gestionen de manera eficiente la potencia para cubrir una mayor área, por lo general manejan potencias nominales entre 8 vatios a 12 vatios, aproximadamente. Un aspecto muy característico de estos sistemas radiantes es el hecho emiten con niveles de potencia lo más bajo

posible con el propósito de impedir interferencias con celdas fuera del área de cobertura que pudieran utilizar el mismo rango de frecuencias, por tal razón es inusual que se instalen sistemas de más de 50 vatios. Es más, en zonas urbanas con mayor densidad poblacional usualmente se instala un mayor número de estaciones base con una potencia muy limitada inclusive menor a 1.5 vatios, con el propósito de permitir la generación de llamadas para pico y micro celdas, que a su vez permiten una mejor reutilización de las frecuencias, cuantas más estaciones, más reutilización de frecuencias y más usuarios conectados al mismo tiempo.

Debido a estas y otras razones, ubicaciones donde coexista una gran densidad poblacional, como grandes ciudades, urbes, zonas populosas, etc., es necesario instalar un número considerable de estaciones base de potencia muy restringida, contrario a lo que ocurre en zonas con una menor cantidad de usuarios que demandar el servicio, como es el caso zonas poco pobladas algunas áreas rurales, entre otros. En estos casos es posible reducir el número de radio bases y tener menos restricciones de potencia. Esto asegura una mayor duración de la batería de los terminales de los usuarios y menor uso de potencia de las estaciones base.

Cabe mencionar, que los terminales no se encuentran emitiendo durante el transcurso de toda la llamada. Para ahorrar batería y permitir un uso más eficiente del espectro, se emplea el esquema de multiplexación TDMA (por sus siglas en ingles Time Division Multiple Access, o acceso múltiple por división del tiempo). El

tiempo se divide en unidades cercanas a 4,615 ms, y éstas a su vez se dividen en 8 time slots o ranuras de tiempo de aproximadamente 576,9 µs. Mientras una llamada es establecida, se asigna un time slot para sincronía, enviada por la estación base; unos slots más tarde, el terminal emplea un slot para enviar de terminal a estación base y otro para recibir, y el resto quedan libres para el uso de otros usuarios en la misma BTS y canal. Así se permite un buen aprovechamiento del espectro disponible y un rendimiento energético más eficiente, al no usar el emisor del terminal constantemente sino sólo una fracción del tiempo.

El controlador de estaciones base o BSC, entre otras funciones, debe mantener la ininterrumpida que pueda generarse por diversos motivos, ya sea porque un usuario se desplace (roaming) y salga de la zona de cobertura de una BTS, tanto el terminal del usuario como la BS calibran o realizan los ajustes necesarios en los niveles de potencia con que envían y reciben las señales e informan de ello al controlador de estaciones base o BSC (Base Station Controller). Además, normalmente varias estaciones base al mismo tiempo pueden recibir la señal de un terminal y medir su potencia. De este modo, el controlador de estaciones base o BSC puede detectar si el usuario va a salir de una celda y entrar en otra, y avisa a ambas MSCs (Mobile Switching Center, Central de Conmutación Móvil) y al terminal para el proceso de salto de una BS a otra: es el proceso conocido como hand-over o traspaso entre celdas, una de las tres labores del BSC, que permite hablar aunque el usuario se desplace.

Este proceso también puede darse si la estación más cercana al usuario se encuentra sobrepasada en capacidad, es decir si todos los canales asignados a la estación base están en uso. En ese caso el controlador de la estación (BSC) envía al terminal móvil a otra estación contigua que se conoce como estación vecina la cual deberá estar menos solicitada por otros usuarios, inclusive aunque el terminal tenga que emitir con una mayor potencia. Por eso es frecuente apreciar disrupciones en la comunicación sobre todo en áreas en donde existe una gran demanda de usuarios que buscan conectarse al mismo tiempo. De lo anterior puede destacarse que una de las de las funciones más importantes del controlador de la estación (BSC), que son fiscalizar la potencia y la frecuencia a la que emiten tanto los terminales como las BTS para evitar cortes con el menor consumo energético posible.

Cabe mencionar que existen una infinidad de canales asignados para aplicaciones específicas sin embargo el propósito de este documento no es el estudio de la canalización como tal, por tal razón solo se hará mención de aquellos que se consideren más relevantes, entre estos canales pueden ser mencionados:

- (Traffic Channels, TCH): Canales de tráfico, se encargan de gestionar las llamadas y tráfico de datos.

- Canal de control broadcast (Broadcast Control Channel, BCCH): Los terminales constantemente se reportan con las radio bases, con el propósito de fiscalizar ciertos parámetros, como potencia, el identificador de celda, calidad de recepción RxQual, entre otros.

- (Frequency Control Channel, FCCH): Se encarga de informar al terminal móvil desde la estación transceptora hacia el canal de control de frecuencia, basicamente su principal tarea es la gestión de la señal portadora de la estación transceptora.

- (Synchronization Control Channel, SCCH): Canal de control de sincronía, Se encarga de informar al terminal móvil sobre la secuencia de instrucción en la estación transceptora, para que el móvil la agregue a su señal de sincronía.

También es importante mencionar que los canales, pueden ser asignados de forma ascendente o descendente, según el sentido de la comunicación, asimismo pueden ser compartidos o dedicados, según la comunicación o el objetivo.

El subsistema de red y conmutación mejor conocido por sus siglas en inglés (NSS), que también se le conoce como núcleo de red (core network), básicamente se encarga del encaminamiento, señalización de llamadas, almacenamiento de información de registros tanto de la red como de los suscriptores. Nótese que anteriormente se había definido el proceso en que se establecía la comunicación

entre una estación móvil (MS) y la red del operador a través de elementos esenciales como la estación base (BTS) y el controlador de estación base (BSC). No obstante como complemento al proceso de funcionamiento básico en una red de telefonía celular, es importante mencionar que hasta momento no se había indicado el proceso para establecer la comunicación con usuarios de otras redes. Para ello cada BSC se comunica con el subsistema (NSS) y es este elemento el que se gestiona diferentes procesos para que la comunicación entre usuarios de distintas redes sea posible. Cabe mencionar que si bien es cierto existen diversos elementos involucrados durante el proceso, en este documento se hará referencia a aquellos que se consideran los más importantes.

La central de conmutación (MSC) comisiona los procesos de inicialización, finalización y encaminamiento de las llamadas por medio del controlador de estación base BSC y su correspondiente estación BS a la que se conecta el suscriptor que recibe la llamada. El proceso es muy similar al proceso que se da en una central telefónica para servicio fijo, con la variante que debido a que los usuarios tienen la posibilidad de moverse internamente en la red, esta a su vez ejecuta reajustes en las bases de datos dentro de la misma. En términos simples la MSC se conecta a la BSC de su región de dominio, pero a su vez al VLR, el cual debe tener conectividad e interconexión hacia a los HLR pertenecientes a las redes de telefonía de los diferentes operadores.

El registro de ubicación base (HLR) consiste en una base de datos que recopila la ubicación de cada suscriptor dentro de la red, adicionalmente fiscaliza ciertos patrones como por ejemplo si el usuario se encuentra dentro del registro o no, además de características propias como estados de cuenta, facturación, tarificación, entre otros. Cada uno de los números telefónicos de los suscriptores se encuentra adscrito a un HLR definido, previamente determinado y gestionado por el operador de la red.

Cuando un suscriptor recibe una llamada, el MSC se comunica inmediatamente con su correspondiente HLR este a su vez verifica si el número consultado se encuentra disponible y en que segmento de la red se localiza, en otras palabras consulta a qué BSC le corresponde notificar la llamada entrante, para luego definir la ruta que tomara la llamada.

El registro de ubicación de visitante (VLR) consiste en una base de datos más etérea que recopila, información de registro correspondiente al área de cobertura para la MSC. En el momento en que un suscriptor se registra dentro de la red, el VLR que corresponde al usuario adscrito se comunica con el HLR asignado y este identifica si dicho suscriptor puede realizar llamadas con base al tipo de cuenta que este tenga. Toda la información antes descrita permanece almacenada en el VLR durante el tiempo que el MS del usuario se encuentra en sesión y este a su vez se actualiza frecuentemente con el propósito de impedir estafas y fraudes, por ejemplo el más común cuando un usuario con un tipo de servicio determinado ya sea

prepago o pos pago si el suscriptor termina con su plan de llamadas y su VLR no lo tiene en el registro, podría aprobar ejecutar llamadas.

Es importante tener presente que los sistemas GSM por lo regular mantienen acuerdos y convenios entre operadores con el propósito de compartir algunos elementos de red, como estrategia para ahorrar costos de operación, optimizar recursos, entre otros. De tal manera que por ejemplo un usuario que se encuentre en el extranjero consigue conectarse a una red de un operador diferente, proceso que se le conoce como roaming o itinerancia. Esto es posible desde que el usuario enciende el terminal y realiza el registro correspondiente en la red del operador en extranjero, para ello el VLR del operador en el extranjero registra la información del usuario que solicita el servicio, este a su vez realiza las consultas necesarias con el HLR del operador móvil del país de origen y confirma si la información de registro del solicitante es válida para permitirle el acceso a realizar llamadas. Para que todo este proceso descrito sea posible es necesario, que tanto el VLR en el extranjero como el HLR en el país de origen estén interconectados. Para estos propósitos existen técnicas de señalización, como es el caso de SS7 entre las más conocidas o para el caso de Estados Unidos el estándar el IS-41. Cada operador en su país correspondiente decide qué estándar le es más factible escoger en sus convenios de itinerancia y de interconexión.

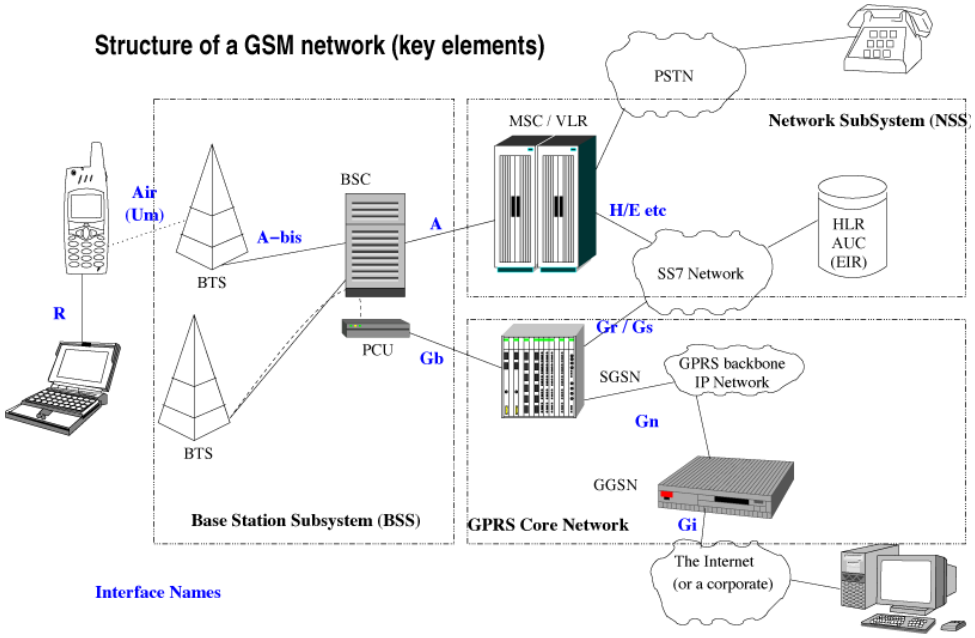


Figura 1. Esquema de típico de una red GSM.

2.3 Arquitectura de red GPRS

La arquitectura de red GPRS por sus siglas en inglés General Packet Radio Service, está instaurada principalmente por una estructura conocida como punto de acceso o Access Point Network por sus siglas en inglés (APN). Algunas de las mejoras de GPRS con respecto a su anterior versión GSM es el hecho que permite utilizar además de mensajes cortos por sus siglas en inglés (SMS) y realizar llamadas, permite la introducción de servicios de mensajería multimedia (MMS), brindar acceso a internet, aunque con una velocidad de navegación bastante limitada en ancho de banda.

El establecimiento de una conexión en GPRS, el suscriptor deberá especificar el APN al cual se enlazara el suscriptor, generalmente se realiza por medio de una

cuenta de usuario proporcionada por el operador. La transmisión de tráfico de datos en GPRS se factura por kilobytes transferidos. En el caso de GPRS es un servicio que va encaminado a sistemas de enlaces de radio, el cual tiene como una de sus principales características brindar un mejor rendimiento a la red conmutación de paquetes. Entre las mejoras más destacables con respecto a su predecesor GSM, es la integración de los siguientes servicios:

- Servicios de red para terminales, mediante el protocolo Wireless Application Protocol (WAP)
- Servicios de mensajería (SMS)
- Integración de dispositivos para ordenadores como módem USB compatibles con la red
- Servicio de mensajería multimedia (MMS)
- Servicios de conexión punto a punto (Peer to Peer) a través de IP

El procedimiento para la trasmisión de tráfico de datos utilizado en GPRS, inicia en el momento de establecer la comunicación entre el terminal de origen y el de destino, básicamente se inicia con un paso lógico entre ellos, utilizando un canal de comunicación, que se reserva hasta que dicho canal deje de ser utilizado. Este tipo de redes se caracterizan por utilizar circuitos conmutados se encargan de transportar los bits de información a partir del sitio de origen hacia el punto de destino, sin embargo una de las debilidades que restan eficiencia al sistema es su

falta de capacidad para identificar paquetes de datos, conocidos como (PDU) por sus siglas en ingles Protocol Data Unit. El ente transmisor fracciona la información que se va a transmitir en paquetes de datos cada uno de manera autónoma, luego en la parte receptora se reciben dichos paquetes y se reordenan de manera tal que se sea posible reconstruir el mensaje original por completo. Los paquetes de datos son transmitidos y viajan de un nodo a otro y cada uno de ellos incluye información de registro tales como el recorrido tanto de origen como destino. Los paquetes permanecen almacenados en cada en cada uno de los nodos por los que viaja mientras aguarda para ser transmitido al siguiente nodo. En términos generales y para efectos de eficiencia de la red esto implica un acrecentamiento en el retardo sobre todos cuando se trata de un volumen de tráfico considerable con respecto a la capacidad del canal.

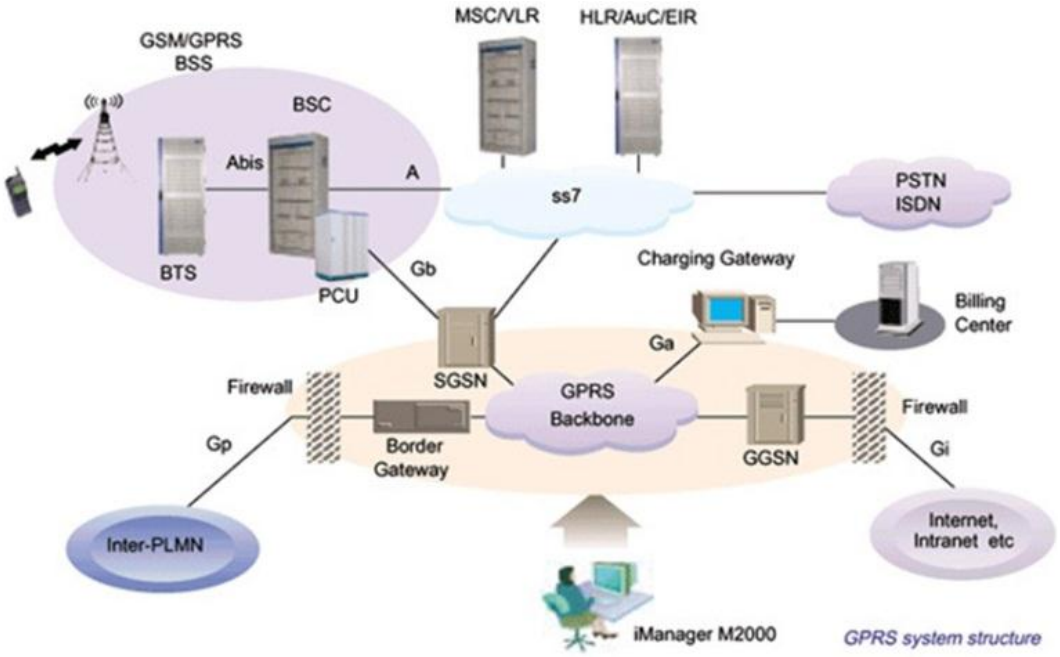


Figura 2. Esquema de una red GPRS.

2.4 Arquitectura de red EDGE

Es una tecnología empleada en la telefonía móvil celular, que se despliega como un punto medio entre las tecnologías de segunda y tercera generación. EDGE se define como el siguiente paso en la evolución de la telefonía móvil siendo su antecesor GPRS. Esta tecnología trabaja específicamente con arquitecturas GSM, sobre todo funciona con aquellas que ya tienen implementado GPRS. Básicamente el operador implemente todas aquellas actualizaciones tanto en hardware como software que son necesarias para el funcionamiento de esta tecnología. EDGE, también es conocido como EGPRS o Enhanced GPRS.

EDGE puede ser utilizado específicamente para la transferencia de información fundamentada en conmutación por paquetes, el caso más importante respecto a este tema va orientado a la conexión a Internet. Algunas de las mejoras de EDGE respecto a su predecesor GPRS, se encuentran el uso de aplicativos que demandan una tasa de transferencia de datos relativamente alta para su momento, requiriendo un mayor ancho de banda además de su capacidad de prestar servicios multimedia.

Esta tecnología utiliza además del esquema de modulación digital Gaussiano por sus siglas en inglés (GMSK), utiliza también el esquema de modulación por

desplazamiento de fase Phase Shift Keying (8PSK), debido a que cuenta con cinco capas de modulación digital y codificación de canales. En las cuatro primeras capas se utiliza GPRS tal y como se describió en el apartado anterior.

La modulación por desplazamiento de fase 8PSK es una técnica que como su nombre lo dice consiste variar o realizar cambios en la fase de la señal portadora en valores discretos, la idea central es producir una palabra de bits por cada desplazamiento en la fase de la portadora. Una de las ventajas más importantes es que al desplazar la fase de la portadora, permite liberar ancho de banda haciendo un uso más eficiente del mismo, además permite un mejor control en la tasa de errores, simplifica los diseños de amplificadores en etapas de transmisión y recepción, entre otras ventajas. Los niveles a utilizar en la transmisión utilizando 8-PSK, dependerán de las condiciones respecto a la relación señal a ruido (S/N) en la frecuencia fundamental. De manera similar a lo que ocurre en GPRS, en EDGE se utiliza un algoritmo que se encargar de adaptar las tasas de transferencia de bits, el cual sirve para adaptar la técnica de modulación utilizada y a su vez la codificación de canal. Otro detalle importante mencionar es que en EDGE se añade una técnica que se conoce como redundancia incremental, la cual consiste en transmitir paquetes redundantes en lugar reenviar aquellos paquetes que presentar errores al ser enviados, lo cual permite ampliar la probabilidad de obtener una decodificación correcta, aun cuando exista pérdida de paquetes durante la transmisión. Otro detalle que vale la pena mencionar es que en EDGE no se requiere de un cambio

demasiado drástico en cuanto a hardware o software se refiere. Para que sea compatible, basta con que en los equipos de transmisión este instalado y en el subsistema de la estación tenga actualizado el soporte para EDGE. Cabe mencionar también que la actualización más reciente de esta tecnología es compatible con los principales fabricantes de equipos y dispositivos para redes GSM y UMTS. En la figura 3 se presenta el esquema de la arquitectura de una red EDGE.

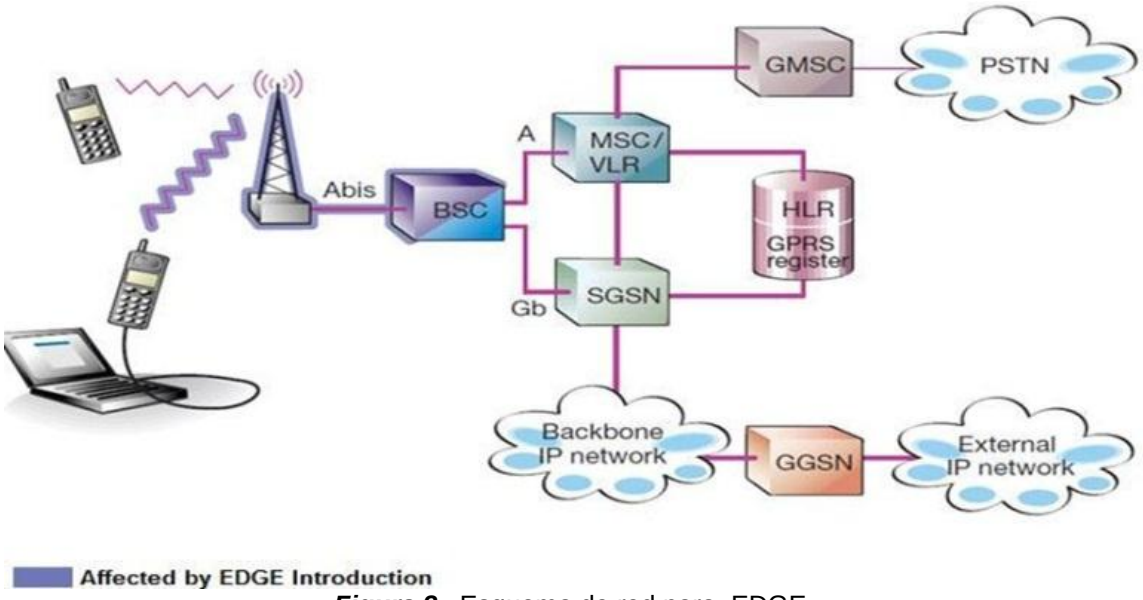


Figura 3. Esquema de red para EDGE.

2.5 El Módulo SIM

El módulo o tarjeta SIM por sus siglas en inglés Subscriber Identity Module, en español módulo de identificación de suscripción es un dispositivo inteligente utilizada en terminales móviles y módems USB para ordenadores. Las

tarjetas SIM en términos sencillos recopilan información como por ejemplo la clave de servicio del suscriptor con la cual puede identificarse en la red del operador.

La tarjeta SIM es de obligatorio uso en las redes GSM. Su semejante en las redes UMTS se designa USIM o también por sus siglas en ingles Tarjeta Universal de Circuito Integrado (UICC).

Las tarjetas SIM recopilan la información específica de la red la cual es utilizada para autenticar e identificar a los suscriptores dentro de la misma, existen diversos códigos que ordenan y gestionan dicha información siendo los más importantes para el tema bajo estudio en el presente documento, Identificador Internacional de la Tarjeta de Circuitos por sus siglas en inglés (ICC-ID), el código IMSI, la clave identificación de área local (LAI) y la clave de autenticación (Ki). La tarjeta SIM asimismo recopila otros datos específicos del operador como por ejemplo el número del centro de servicio de mensajes cortos por sus siglas en inglés (SMSC), el nombre del proveedor de servicio por sus siglas en inglés (SPN), los números de servicio de marcado (SDN) y aplicaciones de servicios de valor agregado (VAS). Todas las especificaciones de estos códigos dentro la tarjeta SIM se describe a detalle en la especificación GSM 11.11. Cada SIM se identifica internacionalmente por medio de su ICC-ID. Este código consta de un número de identificación constituido por lo general de 20 dígitos.

El código IMSI por sus siglas en ingles Identidad Internacional de Abonado Móvil consiste en un código con el propósito de brindar la identificación correspondiente para cada dispositivo que se conecta a la red de telefonía móvil, dicho código se encuentra almacenado en la tarjeta SIM del terminal del suscriptor, el cual permite identificar información como por ejemplo la MSC a la que conecta el usuario, el operador al que pertenece, entre otros. Por ejemplo cuando un usuario viaja fuera de su país y requiere el servicio de Roaming al operador local al que pertenece, este a su vez insta al operador del país de destino permitir la activación del servicio utilizando el código IMSI contenido en la tarjeta SIM del usuario. La llave de autenticación (Ki) es una cantidad que consta de 16 bytes la cual como su nombre lo indica su principal función es autenticar las tarjetas SIM registradas en la red. Cada tarjeta SIM contiene una Ki única establecida por el operador como parte del proceso de registro del suscriptor. La Ki también se encuentra almacenada en una base de datos definida conocida como centro de autenticación por sus siglas en inglés Authentication Center (AuC), la cual forma parte integral del HLR en la red.

Figura 4. Funcionamiento del código IMSI.

Capítulo 3

3.1 Seguridad en Comunicaciones Móviles de Segunda Generación

En el caso particular de GSM y demás tecnologías de segunda generación se manejan varios algoritmos diferentes de cifrado, para determinar la identidad del usuario, es decir su autenticación y para la transmisión de datos y voz de forma cifrada. Estos algoritmos están distribuidos entre el operador de la red GSM, el terminal móvil del usuario y la tarjeta SIM. Algunos de estos algoritmos existen diferentes versiones, debido a que cumplen con diferentes propósitos. El suscriptor se identifica con un código único, llamado IMSI (International Mobile Subscriber Identity), guardado en la tarjeta SIM. Esta a su vez contiene una la clave única de usuario (Ki), el algoritmo de generación de claves de cifrado conocido como (A8), el algoritmo de autenticación (A3) y el PIN. En el terminal móvil se encuentra el algoritmo de cifrado (A5). El primer paso es autenticar al usuario en la red. Se acredita que el código IMSI y el PIN de la SIM son correctos y los algoritmos de

cifrado tanto de la SIM como del móvil están registrados dentro de la red del operador.

3.2 Proceso de autenticación en GSM, GPRS y EDGE

En el momento que el terminal MS es encendido este se reporta enviando su IMSI a la red del operador y solicita acceso y autenticación. El operador de la red en respuesta indaga en su base de datos si el IMSI enviado es válido a través de clave de autenticación (Ki). El operador de la red genera un número aleatorio conocido como (RAND) y lo firma con la Ki de la SIM, generando una cantidad que se conoce por sus siglas en inglés como respuesta firmada 1 (SRES-1). El operador de la red envía el numero RAND al móvil del suscriptor, este a su vez lo envía a la tarjeta SIM. La tarjeta SIM firma el RAND con su Ki y envía el resultante que conoce por sus siglas en inglés como respuesta firmada 2 (SRES-2), a la red del operador. El operador hace una comparación entre su SRES-1 con la SRES-2 formada por la tarjeta SIM. Si ambas cantidades coinciden, la SIM es autenticada correctamente y se le brinda acceso a la red. El algoritmo criptográfico que se utiliza para calcular la respuesta firmada (SRES-2) posee una vulnerabilidad bastante importante, la cual

consiste en que es posible la extracción de la Ki de la tarjeta SIM y esto como consecuencia hace posible la elaboración de duplicados o clones de la misma [9]. Una vez autenticado, el algoritmo A5, que se utiliza para transmitir datos por la red, Por motivos del funcionamiento de la seguridad en dicho algoritmo, la clave única del usuario, almacenada en la SIM, no se envía a través de la red. El operador se almacena una copia de dicha clave y con el propósito que el suscriptor pueda transmitir de manera cifrada, le envía un paquete en forma aleatoria. El algoritmo A8 se encarga de generar una clave de sesión (Kc) en el extremo del receptor, mientras que a través del algoritmo A5, se genera una respuesta tomando como base la clave de sesión Kc junto con el paquete aleatorio enviado por el operador de red. El operador de la red realiza el mismo cálculo de manera interna y compara si los resultados coinciden.

3.3 Esquema de seguridad en GSM mediante el uso del algoritmo A5/1

Si el cálculo entre las claves de sesión del usuario y el del operador coincide, significa que el usuario ha sido correctamente autenticado dentro de la red del operador. Una vez que el proceso de autenticación es válido, la voz digitalizada y los datos se van dividiendo en paquetes, y cada uno de estos paquetes son cifrados con la clave única, y posteriormente se transmiten en ambos sentidos. Para poder descifrarlos, es indispensable conocer la clave Kc única. Sin embargo para

calcular esa clave única, la única información disponible es la secuencia aleatoria enviada por el operador de la red y la respuesta que envía el usuario.

Uno de los mayores retos que pueden presentar es el hecho que la operación matemática que utiliza el algoritmo A5 no tiene inversa función. Es decir, que conociendo el resultado, no hay ninguna operación matemática que pueda calcular cuál era la clave única de usuario que ha utilizado el algoritmo para obtener ese resultado.

Existen tres variantes del A5, denominados A5/1, A5/2 y A5/3. Sin embargo tanto para el A5/1, como para el resto de especificaciones, en un principio eran un secreto sin embargo fue posible obtener muchas de sus especificaciones por medio de ingeniería inversa. Oficialmente, utiliza claves de 64 bits, lo que actualmente es sumamente ineficiente. Originalmente esas claves de 64 bits contienen siempre 10 bits que son fijos, por lo que en realidad es de 54 bits (aunque las tarjetas SIM posteriores utilizan los 64 bits).

El A5/2 quedo completamente en desuso, debido a que se trata de una versión más débil y de menor costo en cuanto exigencia de recursos de cómputo, en el caso del A5/1 este fue dado de baja al poco tiempo. El A5/3 es más reciente y robusto, de 128 bits, pero su uso es muy limitado. Ya que implica actualizar hardware, pocos operadores de red se han gastado lo necesario para actualizar sus equipos para que lo soporten.

El grupo 'The Hackers Choice' creó un proyecto en 2008 para desarrollar un ataque práctico sobre A5/1 (en el sentido de que fuera posible ponerlo en práctica, y no sólo a nivel teórico). Para ello hacía falta construir una tabla de búsqueda de unos 3 terabytes, que permitiera que dada cualquier combinación de secuencia aleatoria y resultado del cálculo con A5/1, cuál es la clave de usuario que daría ese resultado a partir de esa secuencia. Sumado a un proyecto de escaneo de redes GSM, sería posible grabar cualquier llamada o SMS de la red GSM, cifrados con A5/1, y en unos minutos disponer de la clave de cifrado y así poder conocer el contenido con un mínimo retraso. Esa tabla se generaría aplicando A5/1 sobre todas las secuencias aleatorias que puede enviar el operador con cada una de las posibles claves de sesión usuario, y calculando el resultado.

Una vez interceptada la clave, es posible escuchar una conversación entre el usuario y el operador de red. El operador manda la secuencia aleatoria, y el usuario responde con una cadena generada a partir de su clave de sesión única. Se interpolan ambos datos en la tabla y dependiendo de las capacidades de cómputo de un posible atacante es completamente factible realizar el cálculo de la clave Kc única que daría ese resultado sobre esa secuencia aleatoria. Una vez conocida la clave de cifrado de las comunicaciones de ese usuario. La clave Kc varía cada cierto tiempo, pero al tener disponible la tabla, resulta viable recalcular la nueva clave.

3.4 Cifrado de datos basados en algoritmos de flujo LFSR

Un LFSR de longitud L contiene L pasos numerados 0; 1; … ; L - 1, cada uno capaz de almacenar un bit, teniendo un sola entrada y una sola salida; también cuenta con un reloj que controla el desplazamiento de los datos. Durante cada período de tiempo se realizan las siguientes operaciones:

(i) el contenido del paso 0 es la salida que forma parte de la secuencia de salida;
(ii) el contenido del paso i se desplaza al paso i – 1 para cada i, $1 \leq i \leq L - 1$; y
(iii) el nuevo contenido del paso L - 1 es el bit de retroalimentación sj el cual es calculado sumando los contenidos de los pasos anteriores. El algoritmo A5/1 funciona como un cifrador de flujo de datos, y el flujo cifrado se consigue por medio de la operación xor de tres registros (controlado por medio de un reloj) con el flujo a cifrar. El bit que controla el reloj de cada uno de los registros, es un bit resultante de una función mayoritaria entre los tres bits centrales de cada registro (i.e. a cada paso habrá dos o tres registros en movimiento). La longitud de los tres registros 1 2 3 R R R son 19, 22 y 23 bits respectivamente (por lo que la longitud de la llave es de 64 bits).

Los polinomios que representan la función f(x) para cada uno de los registros son:

$$f(x_1) = x^{19} + x^{18} + x^{17} + x^{14} + 1 \qquad (1)$$

$$f(x_2) = x^{22} + x^{21} + 1 \qquad (2)$$

$$f(x_3) = x^{23} + x^{22} + x^{21} + x^{8} + 1 \qquad (3)$$

La figura 5 muestra el diagrama general de funcionamiento del algoritmo A5/1.

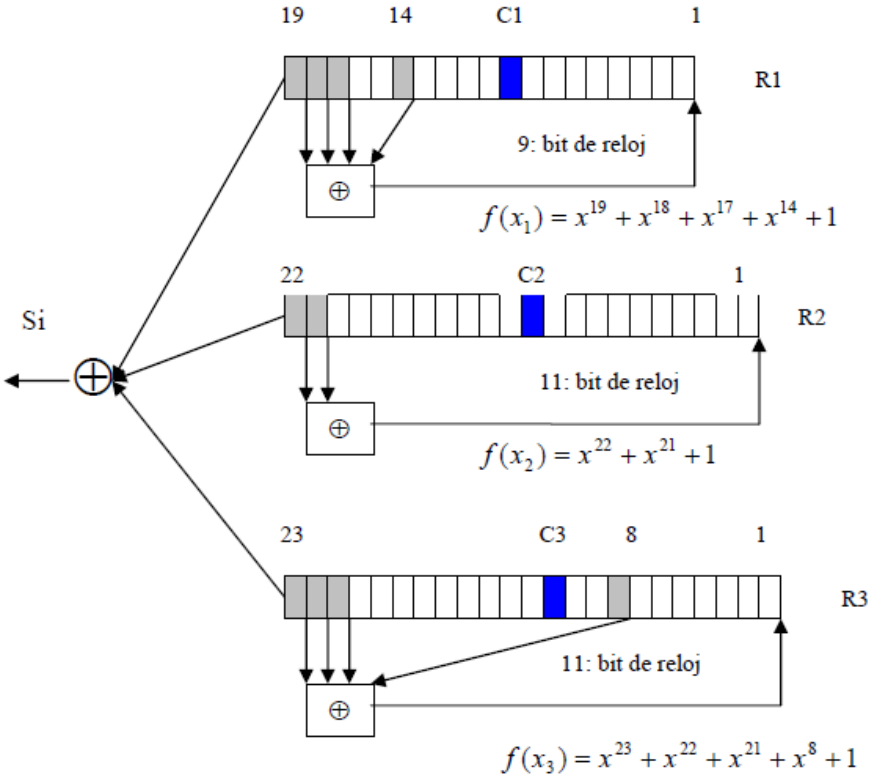


Figura 5. Diagrama de funcionamiento del algoritmo de flujo A5/1.

Capítulo 4

4.1 Redes Móviles de Tercera Generación

Las tecnologías de tercera generación son la respuesta a la especificación IMT-2000 de la Unión Internacional de Telecomunicaciones. En Europa y Japón se seleccionó el estándar UMTS (Universal Mobile Telecommunication System), basado en la tecnología W-CDMA. UMTS está gestionado por la organización 3GPP, también responsable de GSM, GPRS y EDGE. En 3G también está prevista la evolución de redes 2G y 2.5G. GSM y TDMA IS-136 son reemplazadas por UMTS, las redes cdmaOne evolucionan a CDMA2000.

High-Speed Packet Access (HSPA) es una fusión de dos protocolos móviles, High Speed Downlink Packet Access (HSDPA) y High Speed Uplink Packet Access (HSUPA) que extiende y mejora el rendimiento de las redes de telecomunicaciones móviles de tercera generación (3G), como son el 3.5G o HSDPA y 3.5G Plus, 3.75G o HSUPA existentes utilizando técnicas de acceso al medio WCDMA.

A finales de 2008 se lanzó el estándar 3GPP, Evolved High Speed Packet Access (también conocido como HSPA Plus), posteriormente adoptado a nivel mundial a partir de 2010. Este nuevo estándar permitía llegar a velocidades de datos tan altas tanto en el enlace descendente (Downlink) como en el enlace ascendente (Uplink).

Sin embargo, las velocidades que se consiguen en la práctica dependerán del ancho de banda disponible.

4.2 Arquitectura de red UMTS.

El esquema utilizado en UMTS está integrado por dos grandes pilares el primero de ellos la red de comunicación como tal, que se encarga de establecer y sostener la transferencia de información entre los cada uno de los extremos de una conexión, mientras que por otro lado se tiene la red encargada de gestionar los insumos para temas de registro en los diferentes servicios, todo lo relacionado con temas tarifarios y de facturación, sistemas de detección de fallas y situaciones irregulares en el funcionamiento de la red. Cabe mencionar que la red de gestión es objeto de estudio para una temática diferente en lo que se refiere a la arquitectura de UMTS. Por tal razón en este documento se dará especial énfasis al sub sistema de comunicación e interconexión, para brindar los diferentes servicios a los suscriptores, dentro del cual se analizará el funcionamiento a un nivel técnico esencial que permita la comprensión de cómo se constituyen los elementos y subsistemas encargados de brindar la seguridad, en una red de tercera generación.

UMTS utiliza un sistema comunicación terrestre basado en una interfaz de radio que se conoce como como UMTS Terrestrial Radio Access (UTRA). Utiliza técnicas de duplexación por división de tiempo (TDD) y división de frecuencia (FDD). Ambos modelos ofrecen rangos de información de hasta 2 Mbps.

Una red UMTS se compone de los siguientes elementos:

Core Network ó núcleo de red: El núcleo de red comprende elementos propios en las redes de transporte e introduce conceptos de ingeniería de tráfico. Básicamente tienen como principal función el transportar la información tanto para tráfico de voz como datos, entre otras funciones gestiona y fiscaliza la señalización y conmutación de paquetes. La señalización habita en tareas de gestión de ingeniería de tráfico, que constituyen asistencias como la capacidad y control de diferentes servicios que se brindan mediante una serie de que cumplen con propósitos específicos y bien definidos; ciertamente también se incluyen elementos que permiten el control de la movilidad entre celdas. Otro elemento importe a destacar es que el núcleo de red, permite la interconexión con otras arquitecturas y modelos de telecomunicaciones, de manera que sea factible la comunicación tanto entre suscriptores de la red UMTS, como también con los suscriptores o abonados que se conectan a través de otras tecnologías, como GPRS, redes PSTN, entre otros.

Red (UTRAN): En UMTS se conoce como red UTRAN por sus siglas en inglés (Acceso Universal Radioeléctrico Terrestre) y está constituida por diferentes subsistemas uno de ellos se conoce como red de radio (RNS) que básicamente cumple con la tarea de establecer la comunicación de toda la red UMTS. El RNS también es garante de gestionar los recursos de interconexión en un número determinado de celdas, está constituido un subsistema llamado Radio Network Controller por sus siglas en inglés (RNC) y el nodo B. El nodo B es aquel elemento de la red que se encargar de comunicar los terminales de los suscriptores o

usuarios con una o más celdas de la red UMTS. El controlador de la red de radio (RNC) está a cargo de todas las tareas de control, gestión y fiscalización de los recursos de la Estación Base Transceptora (BTS).

User Equipment (UE): Básicamente está integrado por el terminal móvil del usuario y el correspondiente módulo de identidad de servicios de usuario por sus siglas en ingles se abrevia (USIM), dicho modulo es el homologo a la SIM-Card utilizada en el escenario de GSM y GPRS.

La integración de los elementos que intervienen en una red UMTS toman como punto de partida que para el establecimiento de la comunicación en un escenario aplicado a tecnologías de tercera generación, ya sea desde un terminal móvil o un modem para computadores que sea concurrente con esta red, la información de tráfico se envían hacia el Nodo B el cual como se menciona anteriormente se encarga de gestionar la comunicación entre los terminales de los suscriptores y las celdas de la red, para luego enviar dicho trafico al controlador de la red de radio (RNC) , con el propósito de ser clasificado, procesado y enviado hacia el Core Network o núcleo de la red, básicamente estos dos elementos conforman el concepto de red UTRAN, desde la cual luego de pasar hacia el núcleo de la red que a su vez está conformado por etapas de conmutación que se encargan de distribuir el tráfico hacia los diferentes subsistemas, según sea el esquema de comunicación hacia el otro extremo pasaran por el Mobile Services Switching Center por sus siglas en inglés (MSC), o por el Serving GPRS Support Node por

sus siglas en inglés (SGSN) o en su defecto pasando por el Gateway GPRS Support Node por sus siglas en inglés (GGSN).

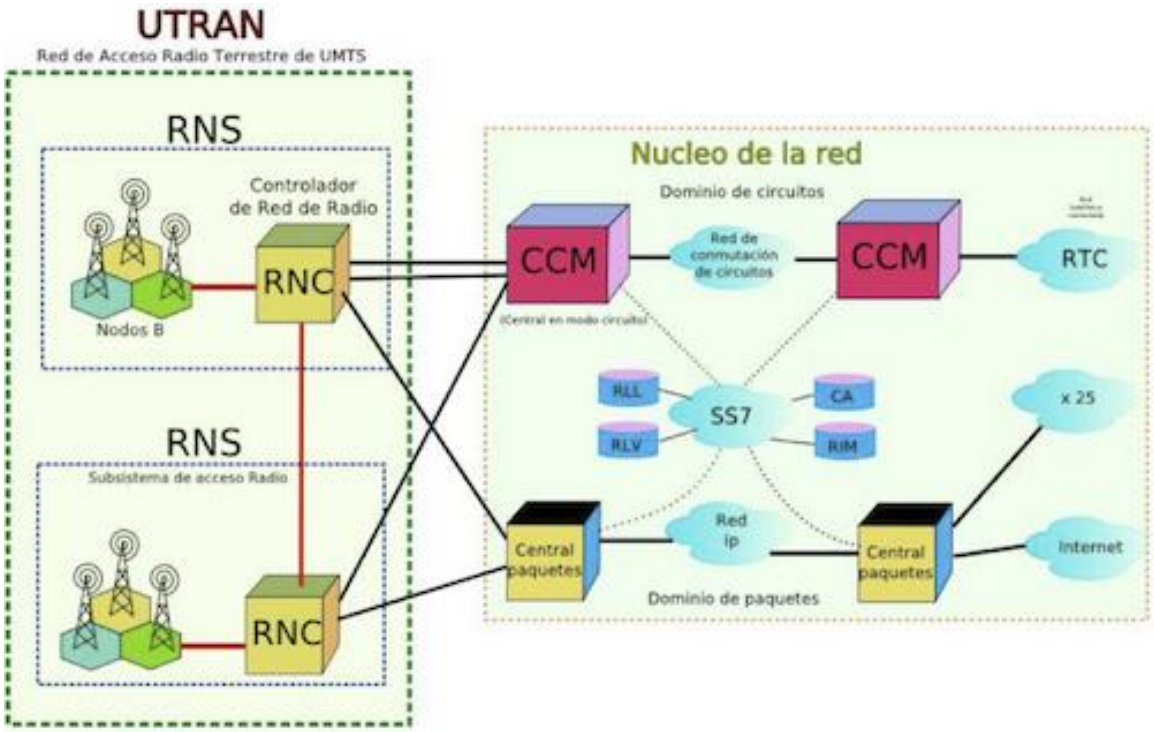


Figura 6. Arquitectura de Red UMTS.

Capítulo 5

5.1 Seguridad en Comunicaciones Móviles de Tercera Generación

Las redes de telefonía móvil de tercera generación, por sus características radioeléctricas, sus vulnerabilidades son en cierta medida no tan conocidas como ocurre en otros entornos que involucran redes de telecomunicaciones. Sin embargo la importancia que tienen actualmente las redes de telefonía celular, implica un gran reto definir la seguridad en este tipo de redes debido a que la mayor parte de la responsabilidad recae en el dominio del operador. En el caso específico de UMTS (Universal Mobile Telecommunications System), de telefonía para tercera generación define un esquema de seguridad específico que intenta garantizar la confidencialidad y la integridad de la información enviada a través de la de emisiones en el espacio libre, ya sea información de tráfico del suscriptor o de la red en sí misma.

Es importante mencionar que las distintas generaciones de redes móviles celulares coexisten como capas que se encuentran superpuestas dentro de la red del operador, por lo tanto los sistemas encargados de validar los servicios y la autenticación incluidos en el esquema GSM serán potencialmente utilizados por nuevas capas incluidas en generaciones posteriores a GSM. Esto implica que las vulnerabilidades documentadas para los sistemas de segunda generación podrían continuar comprometiendo la seguridad en sistemas posteriores, aunque con el tiempo se implementen nuevas tecnologías esto dependerá de la planificación y el esquema en el que el operador desea mantener todas las redes implementadas de forma operativa.

5.2 Esquema de Seguridad en UMTS/WCDMA

En UMTS se tienen cinco grupos de características de seguridad, cada uno orientado a hacer frente a ciertas amenazas y alcanzar determinados objetivos.

- Seguridad en el acceso a la red; el cual proporciona acceso seguro a los servicios y protege contra ataques en el enlace radio.
- Seguridad en el dominio de red: Permite a los nodos del operador de red intercambiar datos de señalización de forma segura, y protege contra ataques en la red cableada.
- Seguridad en el dominio del usuario: Permite a los usuarios disponer de acceso seguro a las terminales móviles.
- Seguridad en el dominio de aplicación: Permite que las aplicaciones en el dominio de usuario y en el dominio del proveedor intercambien mensajes de forma segura.
- Visibilidad y configuración de seguridad: Permite al usuario obtener información sobre las características de seguridad que se están utilizando.

En UMTS, por otra parte, existen tres grandes mecanismos de seguridad: el sistema de autenticación y acuerdo de claves; los algoritmos de integridad y confidencialidad; y el cifrado por bloques KASUMI.

5.3 Mecanismo de Autenticación en UMTS/WCDMA

En UMTS el mecanismo que gestiona todo el proceso de autenticación, se base en un protocolo de tipo desafío-respuesta. Son los que suelen utilizarse para que un sujeto verifique la identidad de otro sin dar a conocer una clave compartida común.

El proceso de autenticación en UMTS es gestionado por el registro de ubicación de visitante (VLR), y se constituye por los siguientes pasos:

- El VLR envía al (HLR) del suscriptor solicitud de autenticación.
- El HLR calcula un conjunto de segmentos de autenticación (AV1:AVn) tomando como punto de partida la clave privada Ki del suscriptor que se almacena únicamente en la USIM y en el HLR/AuC, para luego exportarlo al VLR.
- El VLR selecciona uno de los segmentos de autenticación (AVi), para luego enviar un algoritmo de desafío/respuesta a la USIM exportándole los elementos RAND y token de autenticación (AUTN) del segmento seleccionado.
- La USIM del suscriptor procesa el token de autenticación y a través de la clave privada Ki puede demostrar que los datos recibidos son válidos, de esta forma la red es autenticada ante el suscriptor. Luego la USIM genera una clave de confidencialidad (CK), una clave de integridad (IK) y una respuesta para la red (RES).

La USIM exporta la RES al VLR el cual puede calcular la respuesta esperada (XRES) y comprobarla con la RES que recibe. De esta manera el suscriptor es autenticado ante la red.

5.4 Mecanismo de control de integridad en UMTS/WCDMA

- El terminal de suscriptor calcula un código de autenticación de mensaje con una longitud de 32 bits, conocido como MAC-I, a partir de ciertos parámetros de entrada definidos previamente en el proceso de autenticación.
- El MAC-I calculado se asocia a la información de señalización y se remite al controlador de red.
- Una vez que el controlador de red recibe la información de señalización con el MAC-I asociado y calcula, utilizando el mismo procedimiento que el MS del suscriptor, el XMAC-I.
- La integridad de la información de señalización se comprueba a través de la comparación de los códigos MAC-I y XMAC-I respectivamente.

Los pasos del proceso antes detallado se muestran en la figura 7.

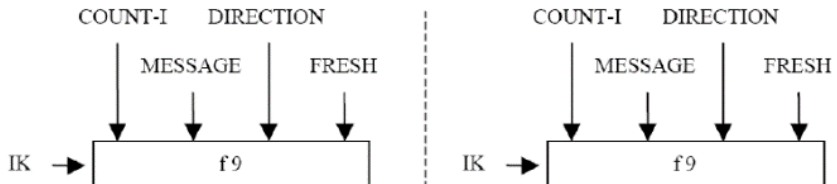


Figura 7. Control de integridad en UMTS

5.5 Mecanismo de control de confidencialidad en UMTS/WCDMA

La confidencialidad de la información transmitida es esencial tanto para el usuario como para el operador. De la parte de comprobación de la confidencialidad se encarga el algoritmo conocido como f8, el cual funciona de la siguiente manera:

- El MS del suscriptor, tomando como punto de partida la clave confidencialidad CK previamente calculada durante el procedimiento de autenticación, adicionalmente se calcula una secuencia de cifrado.
- Se realiza una operación XOR durante dicha secuencia de cifrado, dando como resultado un bloque de bits cifrados.
- Los datos cifrados se remiten a la red a través del espacio libre.
- El RNC, a partir de los mismos parámetros que utiliza el MS del suscriptor conteniendo la clave autenticación CK, forma la misma secuencia de bits cifrados.

- Se realiza una operación XOR durante la nueva secuencia de bits cifrados recibidos, se realiza una comparación con los datos originales.

Los pasos del proceso antes descrito se muestran en la figura 8.

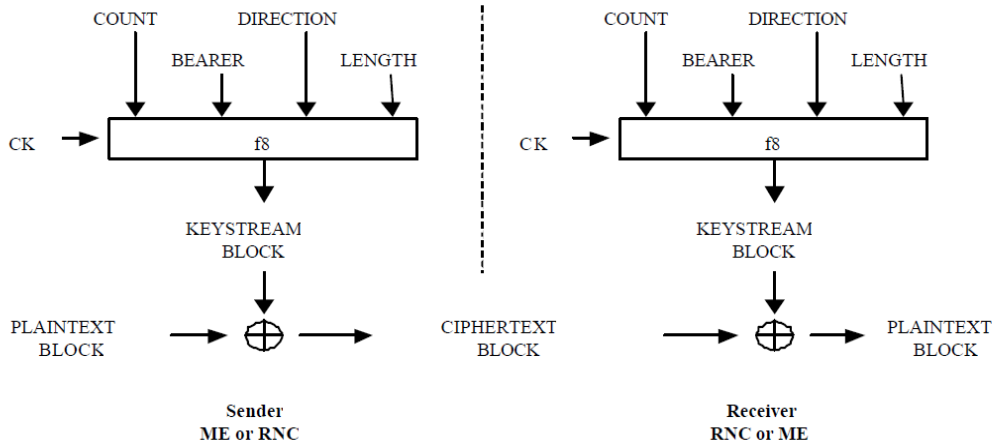


Figura 8. Control de confidencialidad en UMTS

5.6 Algoritmo de cifrado por bloque KASUMI

Los algoritmos f8 y f9 de integridad y confidencialidad se basan en el algoritmo KASUMI. Este es un algoritmo de cifrado por bloque el cual fue desarrollado tomando como base el algoritmo MISTY-1, y se caracteriza desplegar una distribución de Feistel que funciona con una clave de 128 bits por medio de entradas y salidas de 64 bits.

En el algoritmo KASUMI se realizan ocho iteraciones y para cada una de ellas se genera un acumulado de claves por cada ronda tomando como punto de partida la primera clave de 128 bits. Con dichas claves de ronda se calcula una función f, la

cual será diferente en cada ronda. Cada una de las funciones estará conformada por dos subfunciones, FLi y FOi, las cuales dependerán de los datos de entrada en la ronda correspondiente y de las claves que en ese momento se generen.

La función FL básicamente consta de operaciones lógicas y desplazamientos de cantidades binarias, la función FO representa una estructura de Feistel que consiste de tres rondas, donde para cada una de las cuales se calcula una sub-función FI que a su vez consta de otras tres rondas. El algoritmo KASUMI debido a la complejidad en su estructura ofrece un grado de seguridad bastante elevado. Fue seleccionado por la 3GPP para la ejecución de los algoritmos tanto de confidencialidad como integridad en redes UMTS, además de implementarse posteriormente en redes de segunda generación. No obstante, algunos equipos de investigación han pretendido romperlo. En el año 2003 se realizó una inicial proximidad, que si bien es cierto no conseguía romper el cifrado, lograba eludirlo, haciendo posibles ataques de tipo El Hombre en el Medio que se abrevian como MITM (Man In The Middle por sus siglas en inglés) en GSM. Posteriormente, en 2005, investigadores israelíes propusieron un tipo de ataque conocido como ataque de boomerang, para implementarlo contra KASUMI, el cual no resultaba nada práctico debido a su excesiva complejidad y debido a que requería de grandes recursos de cómputo, sin embargo fue la pauta para encontrar otros métodos más eficientes para romper el algoritmo. Finalmente, en el año 2010, investigadores del Weizmann Institute of Science de Israel consiguieron romperlo, obteniendo la clave completa en menos de dos horas utilizando un ordenador personal, ellos

desarrollaron una tabla que fue previamente computada con meses de antelación. Este ataque, sin embargo, no es efectivo contra el cifrado MISTY-1, que ha probado ser más robusto pero su principal desventaja es su alta exigencia de recursos computacionales, haciendo que no sea factible su implementación.

En UMTS el algoritmo KASUMI fue vulnerado por completo en 2010, por lo cual un medida de seguridad desde la perspectiva del operador sería utilizar el algoritmo MISTY-1, basado siempre en una estructura de feistel pero utilizando claves más robustas con longitudes de 256 y 1024 bits aunque esto implica un mayor empleo de recursos de computo.

Los pasos que describen el proceso de funcionamiento en el algoritmo KASUMI, se muestran en la figura 9.

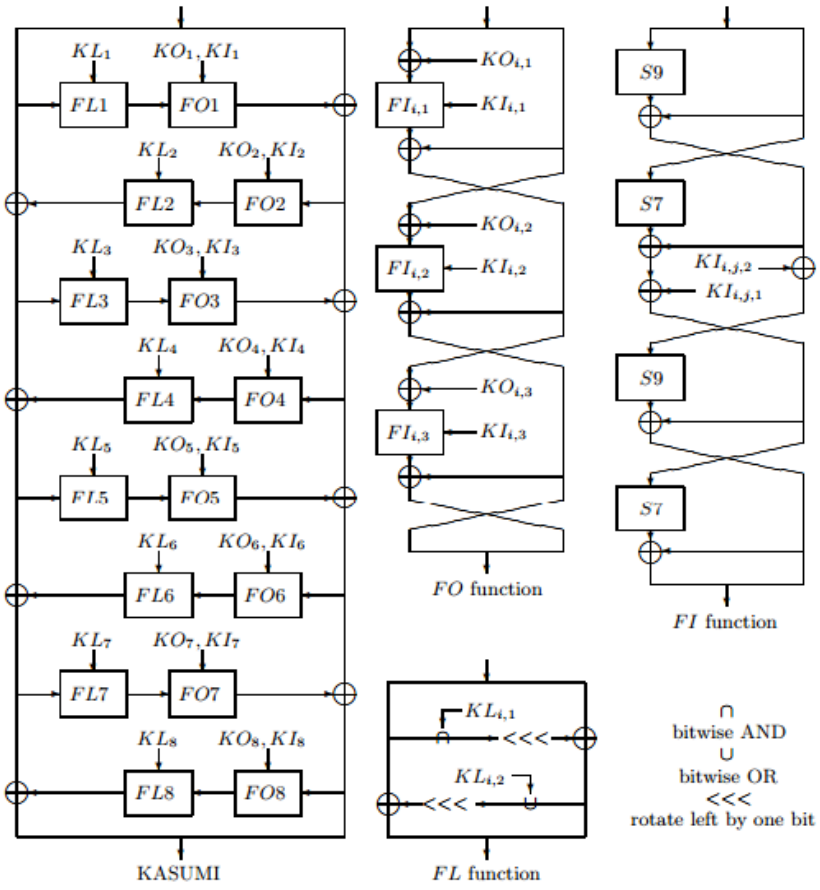


Figura 9. Esquema de funcionamiento del algoritmo KASUMI

Capítulo 6

6.1 Vectores de Ataques

En la actualidadad en El Salvador la telefonía móvil de cuarta generación es ya una realidad y pudiera parecer que la tecnología GSM (2G) ha quedado relegada a un segundo plano. Sin embargo aún existen muchos suscriptores siguen haciendo uso GSM cada día y en la práctica la gran mayoría de los terminales móviles UMTS/WCDMA son compatibles con GSM el cual es muy débil en cuestión de seguridad. Se puede suponer que una tecnología con un número tan alto de usuarios, dispone de mecanismos que garantizan la seguridad de las comunicaciones de tantos usuarios. Sin embargo es más factible de lo que parece la posibilidad de que conversaciones o mensajes de texto acaben en manos de un tercero**.** Es importante mencionar que a pesar que pueden existir vectores de ataques de diversos tipos, tal y como se menciona en el abstracto del presente documento, se dará especial énfasis en el ataque de suplantación de estación base transmisora o de estación base falsa como comúnmente se le conoce, el principal motivo es que este vector de ataque en particular, es el punto de partida para otros posibles ataques, como por ejemplo el ampliamente conocido ataque del hombre en el medio (*por sus siglas en ingles MiTM)* o el ataque de regresión a tecnologías inferiores, entre otros.

6.2 Ataque de estación base falsa

Realizar un ataque de hombre en el medio (MITM) en GSM podría resultar una tarea relativamente sencilla siempre y cuando se cuente con ciertos conocimientos técnicos concretos y los recursos tecnológicos adecuados. A continuación en esta sección se estudiara el por qué se puede hacer, cómo se puede hacer y qué se podría conseguir.

Para entender cómo funciona un ataque de estación base falsa es necesario familiarizarse con los conocimientos técnicos acerca del funcionamiento de la arquitectura GSM en general.

En GSM tal y como se detalló anteriormente, existen dos subsistemas definidos: por un lado el (NSS) o Network and Switching Subsystem, que constituye básicamente el core o núcleo de la red y su principal función es la de realizar tareas de conmutación, gestión de movilidad y autenticación de usuarios por medio los registros de ubicación local y visitante HLR y VLR respectivamente. A su vez el Subsistema de estación base (BSS), se encarga de implementar las interfaces radioeléctricas para el establecimiento de la comunicación con los dispositivos de los usuarios. Estas etapas están conformadas por el controlador de estaciones base (BSC) que como se menciona anteriormente es el encargado del sistema de control que gestiona los recursos de una o diversas estaciones base. Además se encarga de asignar frecuencias y controlar las potencias en las emisiones. Las

estaciones base proporcionan cobertura en un área establecida y previamente planificada denominada celda. Las estaciones base informan sus operaciones a través del canal de control, de manera que los terminales móviles puedan ser geo referenciados y registrarse en las distintas celdas.

El estándar GSM presenta desde su concepción ciertos puntos débiles que le hacen especialmente vulnerable. Uno de ellos afecta al IMSI (identificador de suscriptor). El IMSI es una información considerada altamente confidencial, porque a partir de ella se puede inferir la localización geográfica de un usuario. El IMSI es un valor único que podría llegar a identificar a un usuario. Si quedara registrado en las torres en las que se suscribe el usuario, se podría literalmente "espiar" por dónde se mueve. Para solucionar este problema de privacidad, la norma establece que por defecto el IMSI no debe ser enviado por el interfaz radioeléctrico, y que en su lugar ha de utilizarse el TMSI (identificador temporal de suscriptor) al realizar actualizaciones de posición (registros en nuevos VLR). Aun así es posible recuperar el IMSI. Un VLR guarda una tabla de correspondencias IMSI-TMSI, pero si por algún motivo es incapaz de resolver un TMSI determinado, la red puede solicitar a la MS el envío de su IMSI en texto claro.

Por otra parte, atendiendo a la confidencialidad de las comunicaciones, el estándar establece el A5/1 como algoritmo de cifrado por defecto. Pero también obliga a que todos los terminales GSM soporten A5/0 (transmisión sin cifrar). Además, la MS no

tiene capacidad para decidir el método de cifrado, teniendo que aceptar el que le imponga la red.

Sin embargo, el verdadero problema en GSM es su protocolo de autenticación. A diferencia de las redes UMTS, donde se analizó que la autenticación se realizaba en los dos sentidos, el estándar GSM sólo autentica al usuario frente a la red, mientras que la identidad de la red no se verifica. Esta carencia hace que sea relativamente fácil para un atacante suplantar a una estación base legítima y de esta manera interceptar y alterar las comunicaciones. Pero si se pretende suplantar una estación base, cabe plantearse por qué una MS (que ya está recibiendo servicio de una estación base legítima) se conectaría a la de un atacante. Existen varios eventos que pueden desencadenar un proceso de re selección de celda, y todos ellos pueden ser forzados por el atacante. Por ejemplo, con un inhibidor de frecuencias es posible provocar una pérdida de cobertura.

Antes de ahondar en el estudio de los vectores de ataque, debe tomarse en cuenta que existen vectores de dos tipos, en función de cómo se comporta el atacante respecto a la red. Y a partir de dichos vectores pueden derivarse otros tipos de ataques más complejos.

El primer tipo de vector se conoce como ataque completo, en este tipo de ataque no solo se suplanta a la estación base sino que además de ellos se suplanta al suscriptor que se conecta a la red. De esta manera la comunicación es completamente bidireccional y las posibilidades a disposición son diversas. El mayor inconveniente es que este tipo de ataque es muy complejo mayormente al momento de sincronizar la señalización entre BTS, atacante y víctima, así mismo las herramientas necesarias no son tan accesibles tanto en precio como en capacidades técnicas.

Por otra parte existe la alternativa de realizar un ataque parcial, en el que únicamente se suplanta la estación base, en este tipo de ataque se restringe la comunicación en un único sentido, sin embargo suele ser más efectivo debido a su factibilidad en cuanto a las herramientas necesarias para llevar a cabo un ataque exitoso.

Para realizar un ataque de esta naturaleza, el atacante (tomando en cuenta que este posee conocimientos previos en informática y telecomunicaciones lo suficientemente extensos) necesita un conjunto de elementos hardware y software muy específicos. Respecto a la parte hardware, el elemento principal es un dispositivo capaz de emitir en la banda de frecuencias de GSM para bandas en los rangos de 900 MHz y 1800 MHz, como por ejemplo alguno de la familia Rtl- Sdr de

RealTek. El precio de estos equipos oscila entre los 60 y los tres mil dólares dependiendo de sus capacidades como potencia de transmisión, ganancia y calibración de las antenas entre otros parámetros técnicos (véase como ejemplo la figura 10). Al mismo tiempo, es indispensable contar con al menos dos antenas direccionales para la transmisión y recepción de los datos o de preferencia un dispositivo capaz de realizar ambas tareas simultáneamente (transmisión y recepción), así como un modulador-demodulador de GMSK, que es la modulación empleada en GSM.

Figura 10. Transmisor/receptor tipo donggle para la banda UHF Rtl-Sdr.

En general, el hardware del atacante tendrá una potencia de transmisión y una capacidad de gestión muy inferior a las de una estación base real, lo que obligará a situarse en una zona próxima al objetivo.

Con respecto al software, existe una gran variedad de herramientas de libre distribución que desempeña las funcionalidades de una estación base de GSM. Por un lado se cuenta con la herramienta de código abierto OpenBTS (véase como ejemplo la figura 11), que realiza la función de un punto de acceso software de GSM, implementando toda su infraestructura de gestión de protocolos asociados. Y por otro lado se tienen a disposición herramientas como Asterisk, que permiten desarrollar las funciones de una central de conmutación. Por último, también será necesaria alguna herramienta que permita capturar el tráfico que circula a través de una red, como por ejemplo Airprobe, WireShark, o cualquier otro que realice funciones similares.

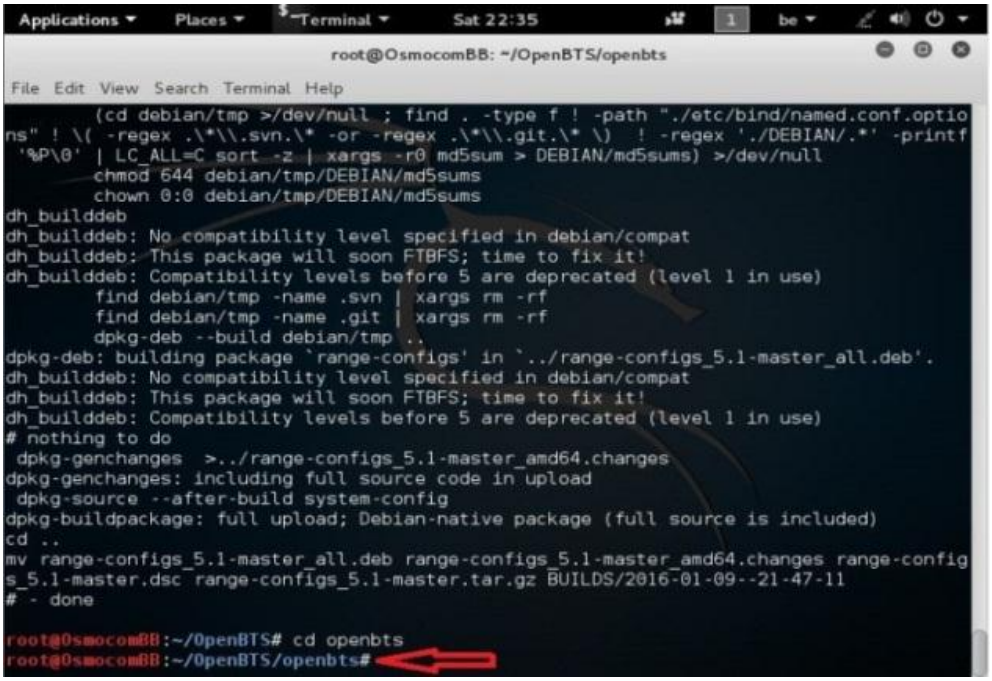


Figura 11. Herramienta de software OpenBts

En la figura 12. Se describe de manera esquemática un ataque del hombre en el medio a través de una estación base falsa, en una red de segunda generación.

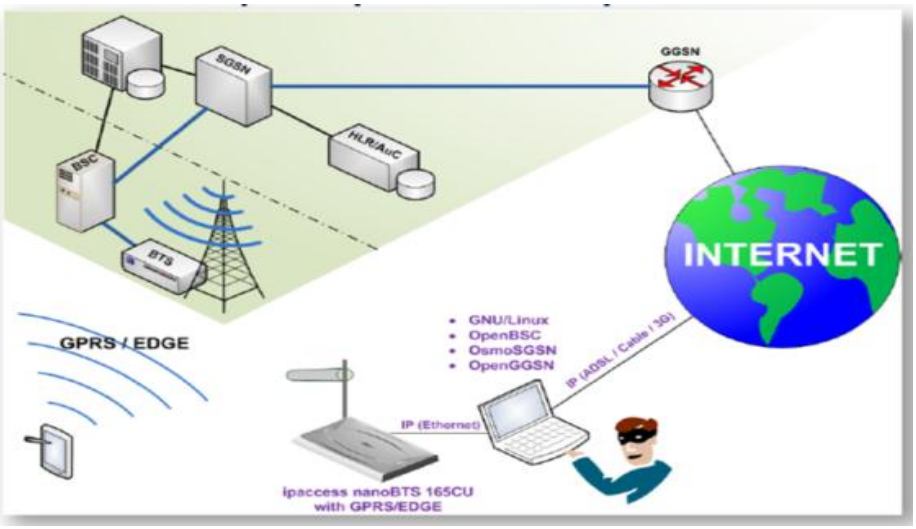


Figura 12. Ataque MiTM, utilizando una estación base falsa

6.3 Ataque de degradación en UMTS

Este tipo de ataque consiste básicamente en obligar al terminal de la víctima a pasar a una tecnología inferior como por ejemplo de UMTS a EDGE, esta estrategia aprovecha la posibilidad que tienen la gran mayoría de terminales móviles de última generación, que permiten al usuario seleccionar el tipo de red que el operador tenga disponible (véase como ejemplo la figura 12).

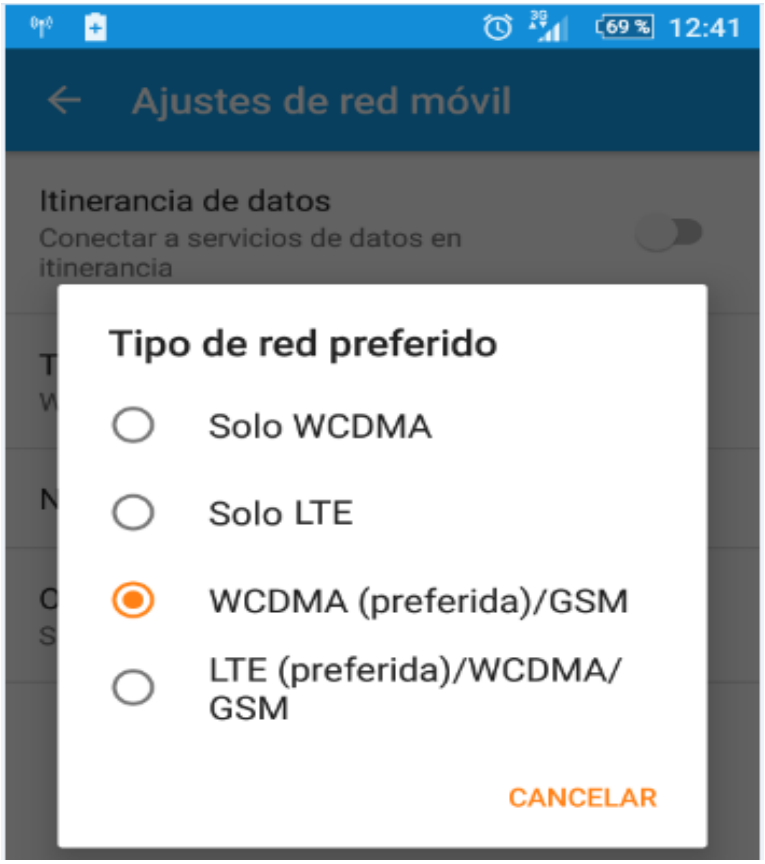


Figura 13. Menú de selección del tipo de red en un terminal móvil

La opción que se muestra seleccionada en el figura 12, permite al terminal conectarse a una tecnología inferior en caso de no encontrar la cobertura adecuada para la primera alternativa que en este caso particular es UMTS/WCDMA. Esta posibilidad representa una oportunidad muy factible para un posible atacante que

no tenga los recursos suficientes para lidiar con la compleja tarea de romper las paredes criptográficas que se presentan en UMTS.

Para llevar a cabo este ataque básicamente consta de tener a disposición el hardware adecuado, que permita inhibir las frecuencias en la porción de espectro utilizada para WCDMA, lo cual obliga al terminal a buscar una red de anterior generación como EDGE o GPRS, es decir el objetivo es llevar al terminal del usuario a un escenario más vulnerable en donde una intrusión a la red o un ataque del hombre en el medio sea más factible la probabilidad de tener éxito. En cuanto al hardware para inhibir ciertas bandas de frecuencias en algunos países se les conoce como Jammers y existen modelos y fabricantes de diversos tipos, para diferentes propósitos (véase como ejemplo la figura 14), los precios en el mercado pueden variar dependiendo de sus capacidades así como también de sus características técnicas.

Figura 14. *Inhibidor de frecuencias de propósitos generales*

Capítulo 7

7.1 Conclusiones

Las tecnologías celulares han evolucionado a lo largo de los años, junto con las medidas de seguridad utilizadas para proteger el tráfico de voz y datos. El cifrado GSM de segunda generación (2G) fue roto hace mucho tiempo, pero las tecnologías UMTS y HSPA hicieron mejoras significativas, y ahora LTE ofrece nuevos avances.

GSM introdujo la autenticación con tarjeta Módulo de Identidad del Suscriptor (SIM) para permitir que los operadores de redes celulares autenticaran los dispositivos de los usuarios, lo que dificultaría las llamadas fraudulentas. GSM también soportó el cifrado opcional A5/1 para proteger el tráfico de voz y datos del usuario sobre el enlace aéreo, y fue diseñado para detener a los posibles atacantes de utilizar el tráfico GSM para rastrear la ubicación de un usuario. No obstante, incluso el tráfico cifrado en GSM puede ser grabado y decodificado usando herramientas como GnuRadio y Kraken.

GSM fue el punto de partida para las tecnologías segunda y tercera generación, que fueron mejoradas para corregir las deficiencias y mejorar la seguridad de los datos en las redes móviles celulares. En concreto, los estándares de seguridad 3GPP utilizan tarjetas SIM y autenticación universal, y protocolos con claves más robustas además buscan brindar una autenticación bidireccional, asegurando a los abonados que se conectan a una auténtica red celular segura. Además, 3GPP

agregó protección de la integridad obligatoria para los mensajes de señalización, lo que dificultaría el secuestro de la conexión. Un nuevo algoritmo de cifrado, conocido como f8, y claves más largas también se introdujo para disuadir el espionaje en la señalización o los mensajes de usuario los mensajes enviados a través del enlace aéreo.

En general, los mecanismos de confidencialidad, integridad y autenticación, hacen de UMTS un estándar relativamente seguro para la comunicación. Especialmente la doble autenticación (usuario-red y red-usuario) hace que UMTS sea difícil de vulnerar frente a ataques de hombre en el medio de falsa estación base, mientras perpetrar estos ataques en GSM resulta sencillo. Aunque el cifrado pueda considerarse fácil de romper, obtener el tráfico cifrado a través de ataques Man in the Midle (MiTM) resultaría muy complejo para el atacante.

Las recientes tecnologías de cuarta generación, por otra parte, buscan mitigar los problemas de la anterior generación. Entre las prestaciones de seguridad de LTE se tiene por ejemplo: la reutilización de la autenticación y acuerdo de claves UMTS, nuevos algoritmos para integridad y confidencialidad (SNOW 3G, AES) y una jerarquía de claves más profunda, con claves de hasta 256 y 1024 bits de longitud.

La seguridad de la transmisión de datos móviles LTE va más allá, tal como se define en el estándar 3GPP TS 33.401. LTE añade un token de Tarjeta de Circuito Universal Integrada (Universal Integrated Circuit Card) para proporcionar almacenamiento de hardware para información sensible, incluyendo claves y la

identidad de Suscriptor Móvil Internacional. LTE utiliza AKA para la autenticación mutua y la generación de claves para la confidencialidad e integridad, ahora proporcionadas como múltiples niveles a través de LTE. Por ejemplo, LTE puede ahora utilizar tres algoritmos para el cifrado de enlace aéreo: AES, SNOW 3G o ZUC. Además, los túneles IPsec se pueden utilizar para proteger la confidencialidad del tráfico LTE de retorno, de nodo a nodo, dentro de la red del operador.

La confidencialidad de los datos del usuario sigue siendo una opción del operador de red, sin embargo, incluso en LTE, los ataques de renegociación se pueden utilizar para rebajar de LTE a GSM para el cifrado, si el teléfono no insiste en una conexión en LTE.

En última instancia, los abonados de la red tienen relativamente poco control sobre la seguridad de los datos celulares. Ellos, sin embargo, sí tienen cierto control sobre cuál generación de tecnología celular utilizan. Sustituir un teléfono antiguo con un dispositivo más moderno con capacidad LTE es un buen comienzo para asegurar de manera más eficiente los datos celulares. Pero es importante tener en cuenta que las medidas vitales, tales como el cifrado de enlace aéreo, todavía pueden sufrir una baja o estar ausentes, sobre todo en caso de roaming. Por esta razón, siempre es una buena práctica añadir medidas de seguridad de extremo a extremo, como HTTPS o VPN, al enviar datos confidenciales a través de redes celulares.

8. Fuentes de Información y Referencias

ETSI ES 282 001: "TISPAN - Telecommunications and Internet converged Services and Protocols

For Advanced Networking (TISPAN): NGN Functional Architecture for NGN Release 1".

ETF RFC 3947 (2005): "Negotiation of NAT-Traversal in the IKE".

IETF RFC 3948 (2005): "UDP Encapsulation of IPsec ESP Packets".

IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions'.

IETF RFC 5626 (2009): "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".

IETF RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms".

IETF RFC 3329 (2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

IETF RFC 3602 (2003): "The AES-CBC Cipher Algorithm and Its Use with IPsec".

IETF RFC 3263 (2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

3GPP2 S.S0055: "Enhanced Cryptographic Algorithms".

9. ANEXOS

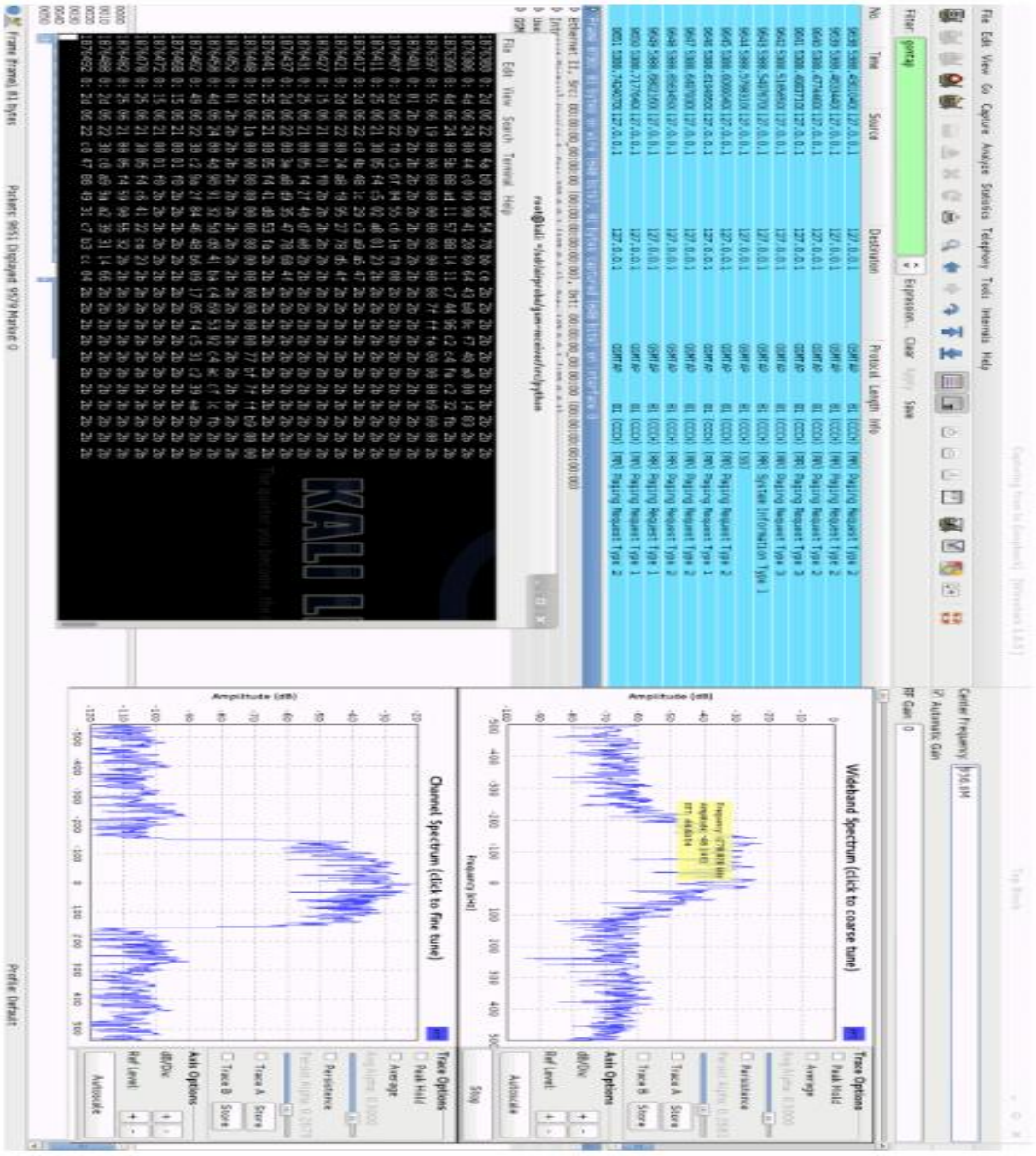
9.1 Anexo A. Glosario de Términos Utilizados

Perfil Orográfico: Hace referencia al concepto de orografía el cual es de gran utilidad para comprensión sobre el relieve zona o una región determinada, por lo general se representa cartográficamente por medio mapas a gran escala esta puede variar entre 1:100 y 1:50 o inclusive mayor, es ampliamente efectiva en temas de planificación de obras civiles, en telecomunicaciones para propósitos de planificación de radio enlaces, análisis de cobertura, estudios de compatibilidad electromagnética, entre otros.

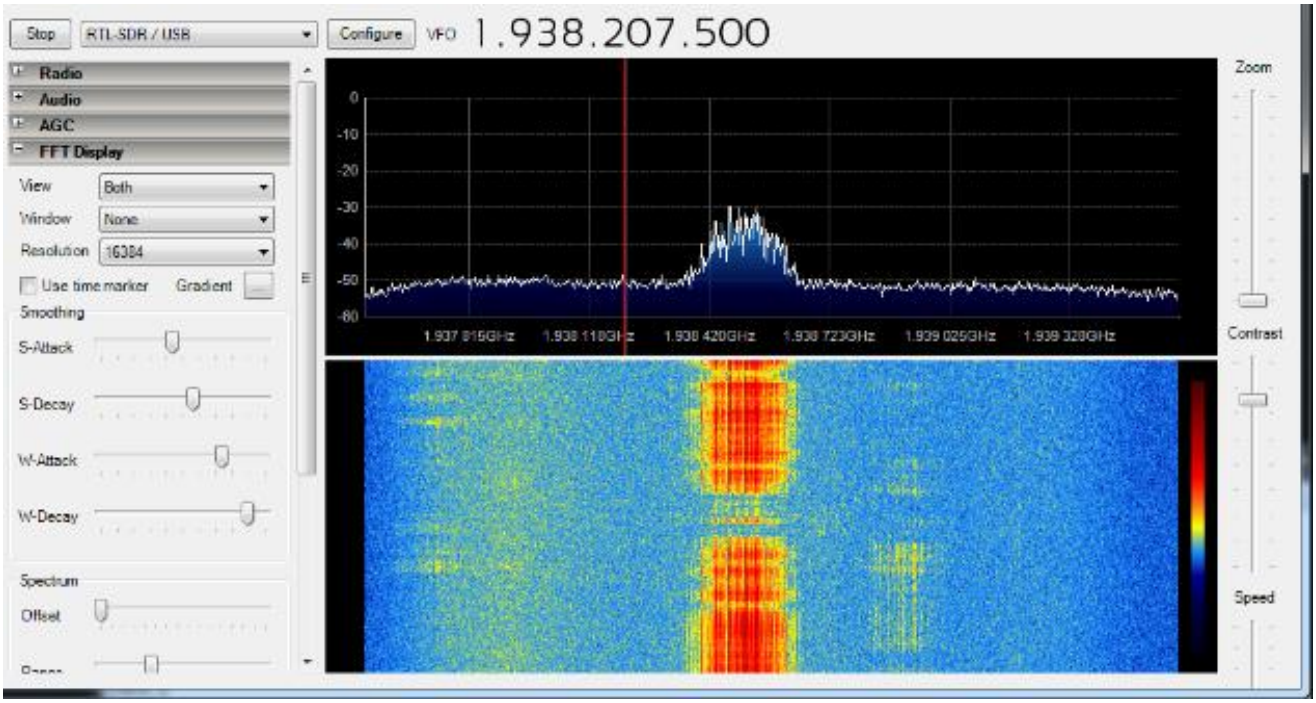
UMTS: Siglas en inglés del acrónimo Sistema universal de telecomunicaciones móviles (Universal Mobile Telecommunications System), es una tecnología ampliamente utilizada en la tercera generación de telefonía móvil celular. Inicialmente fue pensada para ser utilizada en terminales móviles, sin embargo debido a sus características, capacidades para brindad conectividad y brindar acceso a servicios diferenciados no se circunscribe únicamente a estos dispositivos y puede ser utilizada en otras aplicaciones.

EDGE: Es una tecnología empleada en la telefonía móvil celular, que se despliega como un punto medio entre las tecnologías de segunda y tercera generación. EDGE se define como el siguiente paso en la evolución de la telefonía móvil siendo su antecesor GPRS. Esta tecnología trabaja específicamente con arquitecturas GSM, sobre todo funciona con aquellas que ya tienen implementado GPRS.

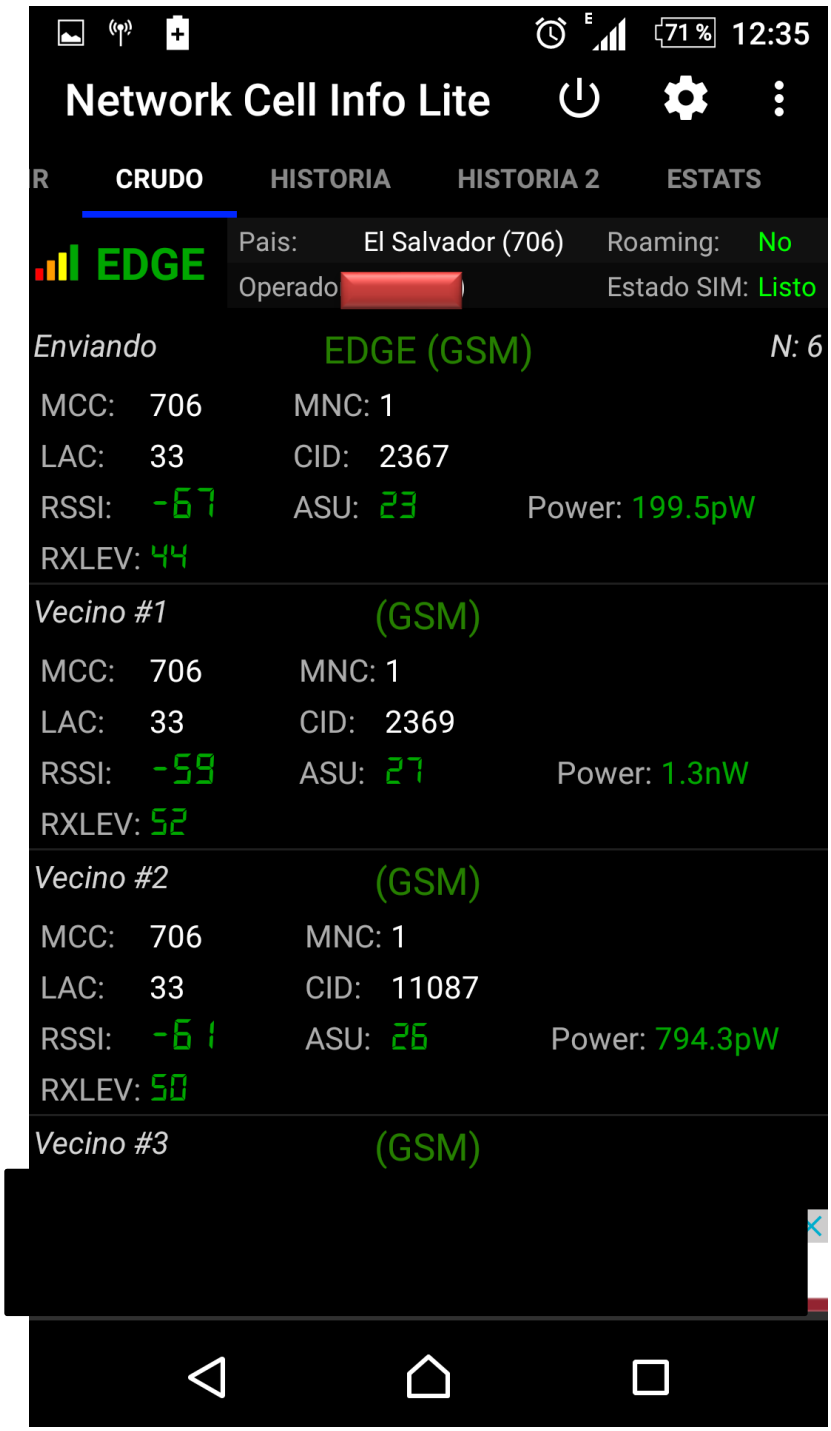
9.2 Anexo B. Recepción, Decodificación y Descifrado de Señales GSM utilizando las herramientas de software Open BTS y Wireshark mediante una plataforma con linux

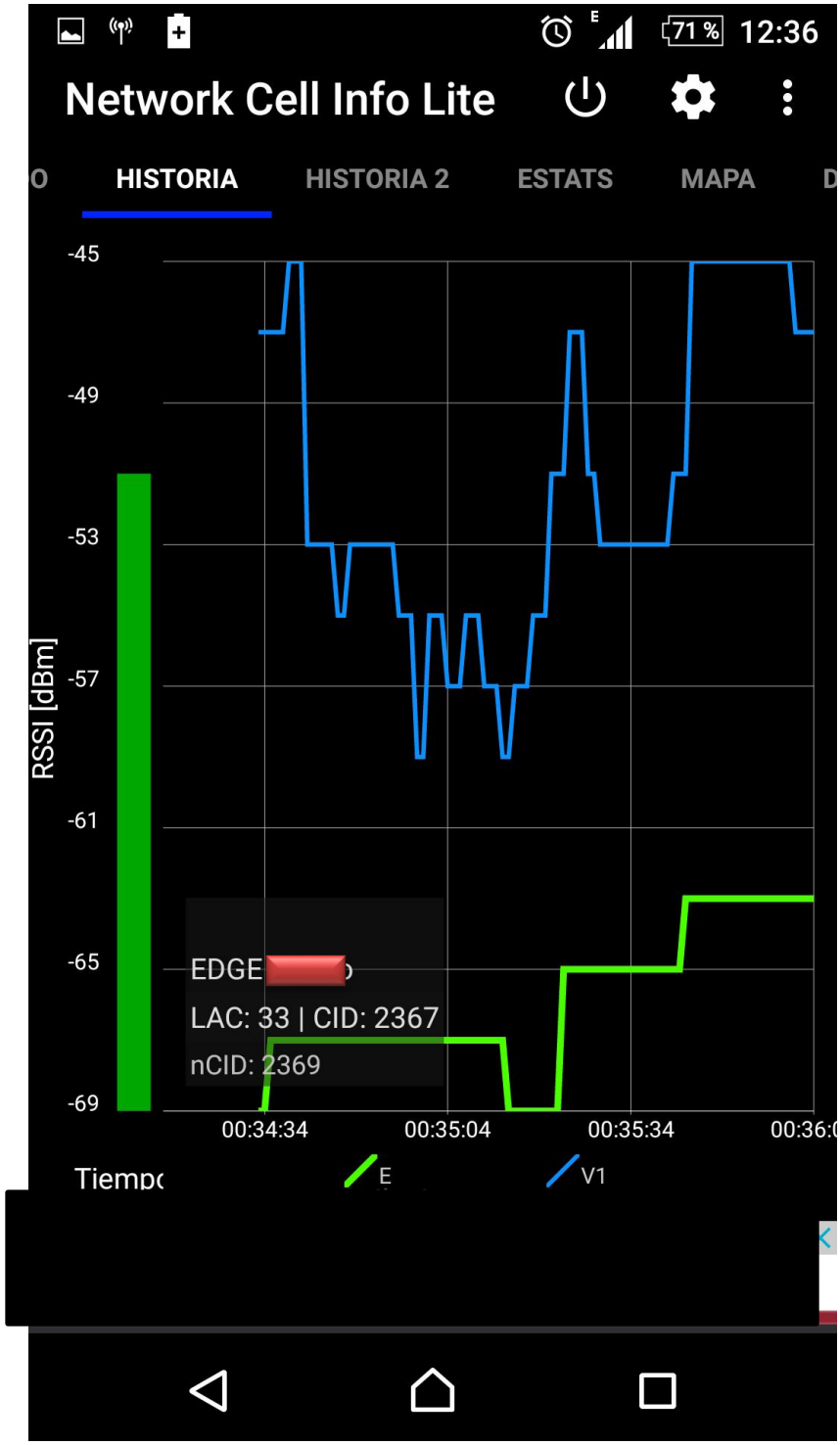


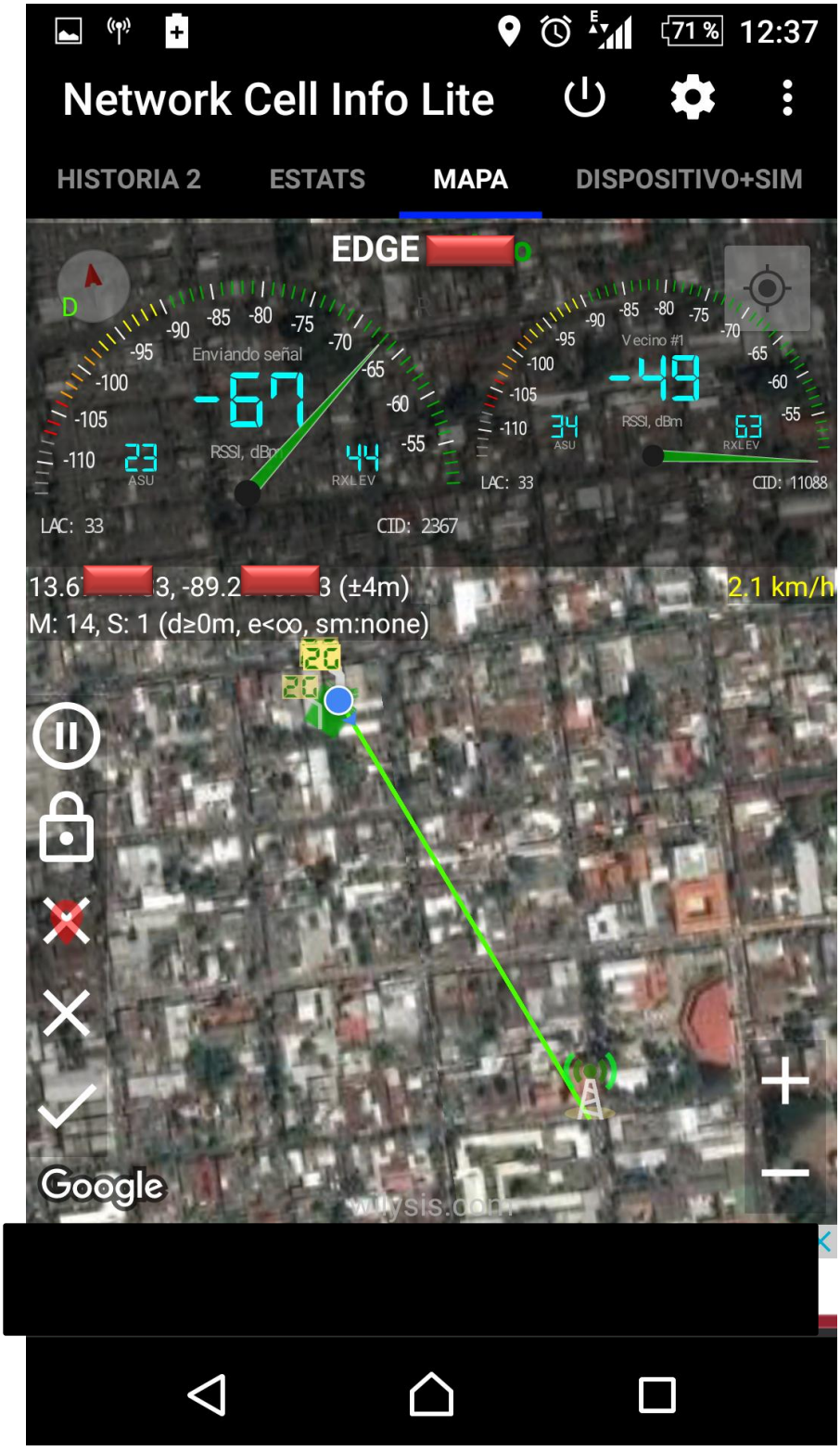
9.3 Anexo C. Recepción, Decodificación y Descifrado de Señales GSM con el hardware RTL-SDR



9.4 Anexo D. Recopilación de información de celda mediante la aplicación Network Cell Info

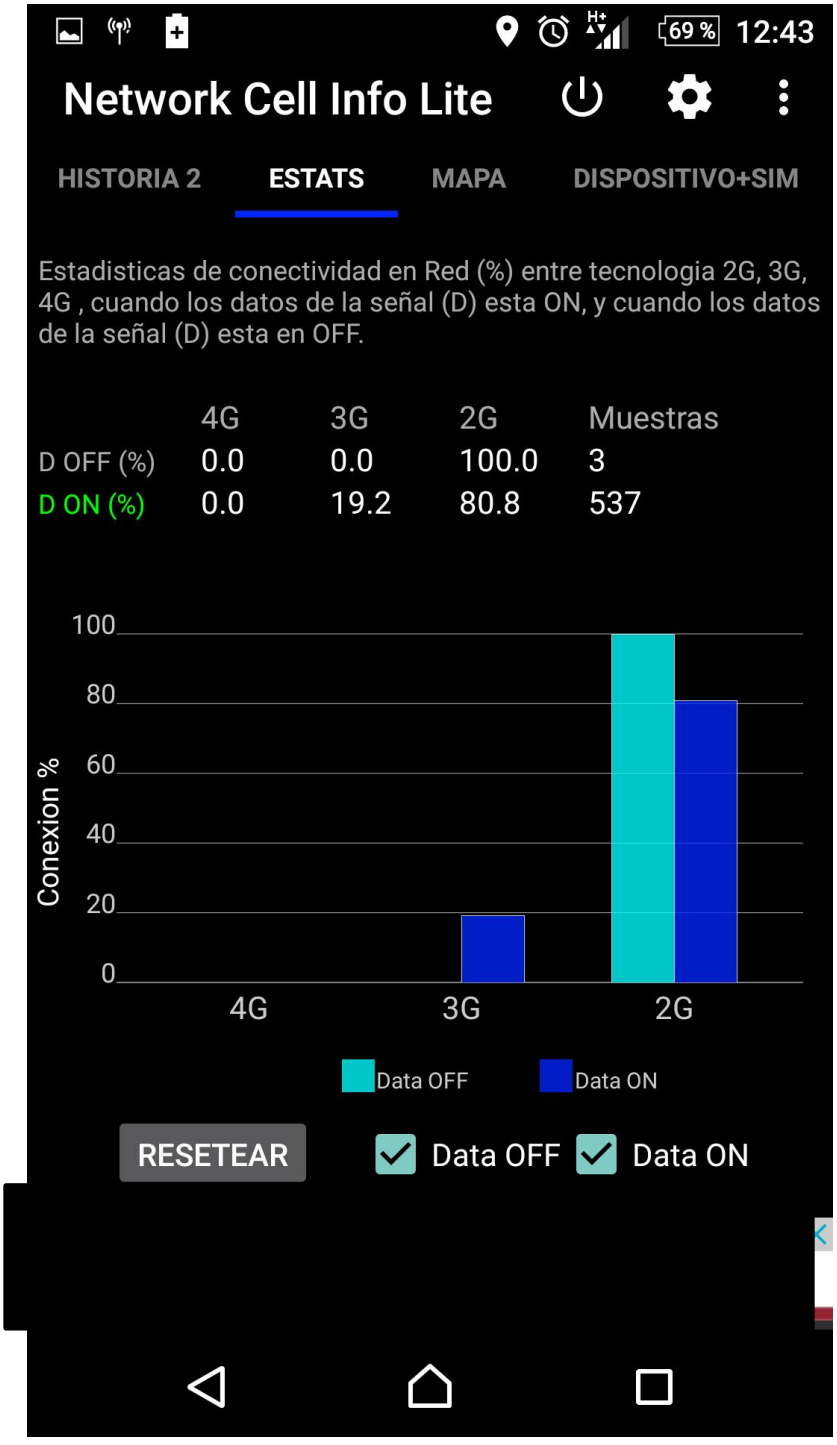


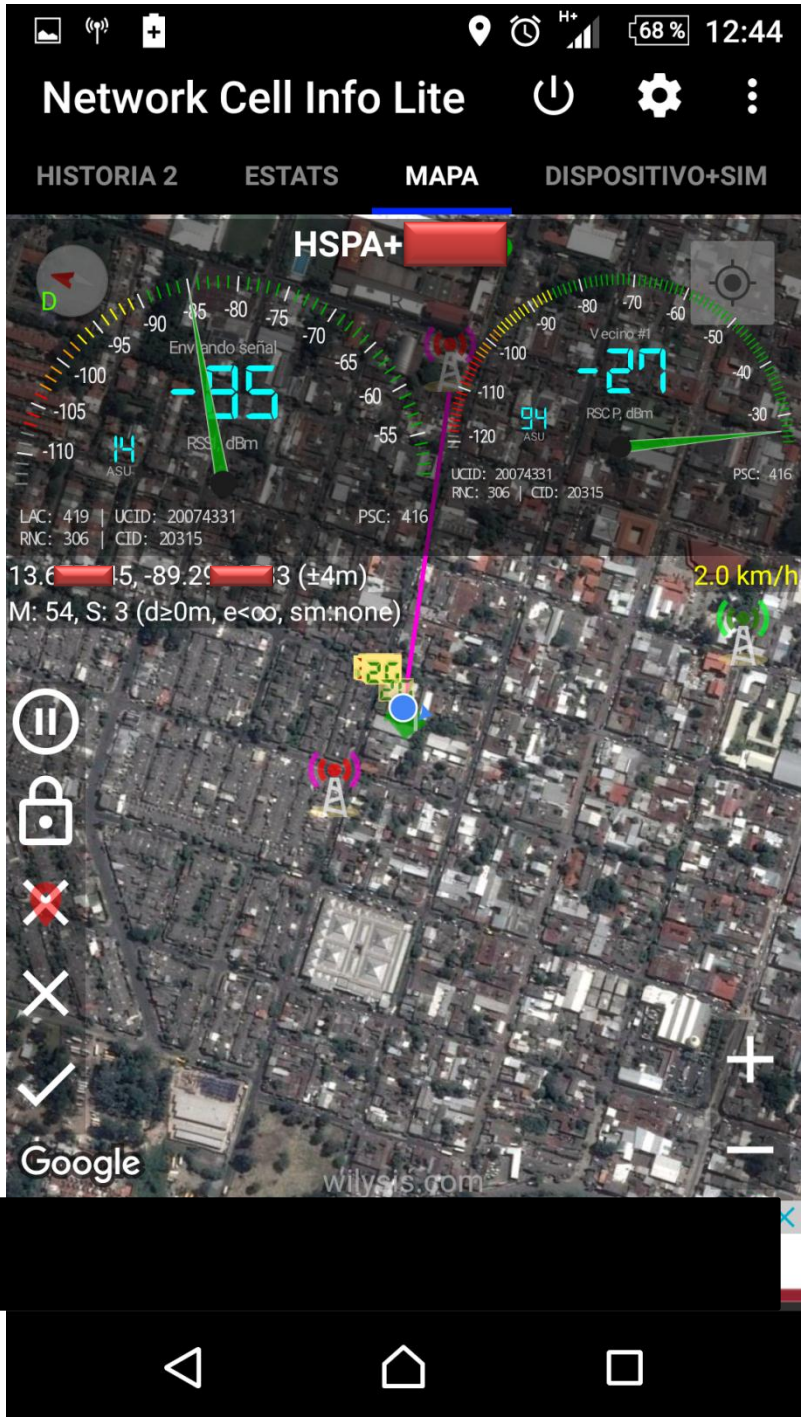

71 %
12:36
Network Cell Info Lite
HISTORIA
HISTORIA 2
ESTATS
MAPA
-45
-49
-53
-57
-61
-65
-69
RSSI [dBm]
EDGE
LAC: 33 | CID: 2367
nCID: 2369
00:34:34
00:35:04
00:35:34
E
V1


71 % 12:37
Network Cell Info Lite
HISTORIA 2
ESTATS
MAPA
DISPOSITIVO+SIM
EDGE
Enviando señal
-67
RSSI, dBm
23
ASU
44
RXLEV
LAC: 33
CID: 2367
Vecino #1
-49
RSSI, dBm
34
ASU
63
RXLEV
LAC: 33
CID: 11088
13.6[redacted]3, -89.2[redacted]3 (±4m)
2,1 km/h
M: 14, S: 1 (d≥0m, e<∞, sm:none)
Google

70 % 12:41
Network Cell Info Lite
HISTORIA 2
ESTATS
MAPA
DISPOSITIVO+SIM
Ocultar infomacion sensible
Info SIM
Actualizar
Pais: El Salvador
Telefono #: No mostrar
IMSI: No mostrar
Operador:
ID Operador: 70601 (MCC: 706, MNC: 1)
Tarjeta #: No mostrar
Estado SIM: Listo
Estado de servicio: In-Service
Roaming: No
Telefonia Dispositivo
Telef. Tipo: NONE/GSM/CDMA/SIP
IMEI: No mostrar

69 %
12:42
Network Cell Info Lite
R
CRUDO
HISTORIA
HISTORIA 2
ESTATS
HSPA+
Pais: El Salvador (70...
Roaming: No
Operado
Estado SIM: Listo
Enviando
HSPA+ (UMTS)
N: 1
MCC: 706
MNC: 1
LAC: 419
UCID: 20074328
PSC: 416
RNC: 306
CID: 20312
RSSI: -85
ASU: 14
Power: 3.2pW
Vecino #1
(UMTS)
MCC: 706
MNC: 1
LAC: 419
UCID: 20074328
PSC: 416
RNC: 306
CID: 20312
RSCP: -31
ASU: 90
Power: 794.3nW


69 % 12:43
Network Cell Info Lite
HISTORIA 2
ESTATS
MAPA
DISPOSITIVO+SIM
Estadisticas de conectividad en Red (%) entre tecnologia 2G, 3G, 4G , cuando los datos de la señal (D) esta ON, y cuando los datos de la señal (D) esta en OFF.
4G 3G 2G Muestras
D OFF (%) 0.0 0.0 100.0 3
D ON (%) 0.0 19.2 80.8 537
Conexion %
100
80
60
40
20
0
4G
3G
2G
Data OFF
Data ON
RESETEAR
Data OFF
Data ON


68 % 12:44
Network Cell Info Lite
HISTORIA 2
ESTATS
MAPA
DISPOSITIVO+SIM
HSPA+
Enviando señal
-85
RSS dBm
14
ASU
LAC: 419 | UCID: 20074331
RNC: 306 | CID: 20315
PSC: 416
Vecino #1
-27
RSCP, dBm
94
ASU
UCID: 20074331
RNC: 306 | CID: 20315
PSC: 416
M: 54, S: 3 (d≥0m, e<∞, sm:none)
2.0 km/h
Google
wilysis.com