Taller de Telecomunicaciones Modalidad SDR

Proyecto Final GSM Base Transceiver Station

Santiago Castro

23 de diciembre de 2016

1. Introducción

Este trabajo se trata de una brevísima introducción al estándar GSM (Global System for Mobile Communication) de redes celulares digitales. Se describirá a grandes rasgos de qué se trata esta tecnología y luego se pasará a realizar algunas demostraciones en las cuales se podrá ver cómo funciona GSM.

El acrónimo GSM se debe en realidad al Groupe Spéciale Mobile que tuvo la tarea de definir un nuevo estándar para las comunicaciones móviles que trabajara en las bandas de 900MHz y 1800MHz. En la actualidad también se utilizan las bandas 850MHz y 1900MHz como se verá más adelante. Este estándar utiliza radiobases terrenas para servir a los clientes, a cada estación se le asigna una porción de la banda para operar con el fin de evitar interferencias entre radiobases cercanas. Esto significa que pueden haber dos radiobases que utilicen la misma frecuencia pero deben estar lo suficientemente alejadas como para no interferir una con otra. La Figura 1 ilustra esta idea.



Figura 1: Radio de cobertura de las celdas.

La tecnología GSM utiliza una combinación de FDMA (Frecuency Division Multiple Access) y TDMA (Time Division Multiple Access), lo que resulta en un canal de dos dimensiones, temporal y frecuencial. Esto significa que el tiempo se divide en slots, y para transmitir cada equipo deberá hacerlo dentro de los slots asignados.

Para ver con más detalle el funcionamiento de GSM, se escaneará el espectro en busca de alguna señal y se analizarán tramas GSM. El hardware utilizado es un USRP B100 de Ettus Research. Los programas que se utilizaran son grgsm_livemon para capturar señales GSM, kalibrate-uhd para detectar las señales GSM que se encuentren en el espectro, wireshark para capturar los paquetes recibidos. Wireshark es necesario pues grgsm_livemon entrega la señal cruda, es decir devuelve una tira de bytes imposible de interpretar a simple vista.

El LiveCD de GNU-Radio en su versión ubuntu-14.04.5-desktop-amd64-gnuradio-3.7.10.1 ya viene con varias herramientas cargadas, y una de ellas es el grgsm_livemon por lo que no será necesario instalarla. Instalación de Wireshark:

sudo apt-get install wireshark Instalación de kalibrate-uhd:

git clone http://github.com/ttsou/kalibrate-uhd.git./bootstrap./configure make Esto creará una carpeta llamada src que adentro tiene el binario kal. Para realizar

un escaneo ejecutaremos ./kal -s GSM850 -g 40, esto busca frecuencias que tengan señales GSM en la banda 850MHz. Las frecuencias obtenidas se muestran en la Figura 2, allí puede verse que el canal 250 (893.6MHz) es el que tiene mayor potencia, usaremos ese para las pruebas.

Al ejecutar grgsm_livemon y setear la frecuencia 893.6MHz se observa el espectro de la señal y por otra parte se vé como comienzan a decodificarse los bytes recibidos.

Esos bytes recibidos pueden interpretarse mediante Wireshark, para ello lo ejecutamos con privilegios y capturamos lo que ingresa por la interfaz 127.0.0.1. Lo que se obtiene son un montón de tramas que transportan información del sistema y datos entre el usuario y la celda. Las tramas System Information Type 1 contienen datos referentes a la descripción del canal de la celda y parámetros de control RACH. Las Type 2 contienen información acerca de las celdas vecinas, PLMN permitidos y parámetros RACH. Las Type 3 tienen información de la identidad y localización de la celda, descrición del canal de control y parámetros de selección de celda. Luego están los paquetes Paging Request, que es el tráfico entre la celda y algún cliente identificado por el número TMSI, un número aleatorio que asigna la radiobase cuando algún cliente establece un enlace.

```
👂 亘 🗉 ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ kal -s GSM850 -g 40
linux; GNU C++ version 4.8.4; Boost_105400; UHD_003.009.004-0-g2b5a88bb
-- USRP-B100 clock control: 10
    r_counter: 2
     a_counter: 0
     b_counter: 20
     prescaler: 8
     vco_divider: 5
     chan_divider: 5
     vco_rate: 1600.00000MHz
     chan_rate: 320.000000MHz
     out_rate: 64.000000MHz
UHD Warning:
    The hardware does not support the requested RX sample rate:
    Target sample rate: 0.270833 MSps
    Actual sample rate: 0.271186 MSps
kal: Scanning for GSM-850 base stations.
        chan: 184 (880.4MHz + 25Hz)
                                        power: 15361.27
        chan: 185 (880.6MHz + 47Hz)
                                        power: 6273.27
        chan: 186 (880.8MHz + 83Hz)
                                        power: 3205.17
                                        power: 7999.44
        chan: 188 (881.2MHz + 44Hz)
        chan: 191 (881.8MHz + 33Hz)
                                        power: 12927.18
        chan: 197
                            - 16.972kHz)
                  (883.0MHz
                                                power: 5726.98
        chan: 199 (883.4MHz - 110Hz)
                                        power: 2778.03
        chan: 201 (883.8MHz + 68Hz)
                                        power: 10898.44
        chan: 205 (884.6MHz -
                               47Hz)
                                        power: 7301.01
        chan: 241
                  (891.8MHz
                               10Hz)
                                        power: 17834.15
        chan: 242 (892.0MHz
                               22Hz)
                                        power: 8713.27
        chan: 244 (892.4MHz +
                               6Hz)
                                        power: 4146.83
        chan: 245 (892.6MHz +
                               25Hz)
                                        power: 9354.28
        chan: 250_(893.6MHz +
                                        power: 33015.60
                               18Hz)
ubuntu@ubuntu:~$
```

Figura 2: Bandas GSM encontradas.

Por ejemplo, en este caso puede verse que la señal corresponde a una celda de Movistar, de códigos MCC=748, MNC=07, LAC=8311, CI=8837. El sitio http://cellidfinder.com/cells permite saber donde se encuentra una celda a partir de estos códigos.





Figura 3: Espectro de la señal.

8) (ut	ount	:u@	ubu	ntu:																	
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
01	06	03	8f	4c	00	12	10	ЬO	12	88	00	00	00	00	00	00	00	00	2b	2b	2b	2b	
05	06	07	60	00	25	22	aa	30	45	f3	08	7с	7с	04	17	42	с5	e1	2b	2b	2b	2b	
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
25	06	21	20	05	f4	c1	20	8d	80	2b													
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
49	06	22	a0	37	32	67	4e	20	24	57	c2	17	05	f4	03	20	0C	88	сb	2b	2b	2b	
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
31	06	3f	10	0d	90	67	7c	8c	15	01	01	07	с8	04	32	20	2b	2b	2b	2b	2b	2b	
49	06	1b	22	85	47	f8	70	20	77	C8	01	28	17	45	05	ad	00	00	80	00	47	1b	
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
25	06	21	20	05	f4	04	37	44	35	2b													
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
41	06	21	a0	05	f4	c1	7d	94	6d	17	05	f4	C0	84	ad	df	2b	2b	2b	2b	2b	2b	
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
25	06	21	20	05	f4	cc	65	f3	0d	2b													
15	06	21	00	01	f0	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	
41	06	21	a0	05	f4	05	28	d4	a1	17	05	f4	45	2a	38	cf	2b	2b	2b	2b	2b	2b	
25	06	21	20	05	f4	44	23	3f	d5	2b													
31	06	1c	47	f8	70	20	77	45	05	ad	00	00	80	00	7b	2b							
31	06	3f	10	0d	90	а7	72	8c	98	02	01	07	c1	0c	67	03	26	2Б	2b	2b	26	26	

Figura 4: Captura de bytes.

2. Instalación del GSM Transceiver

Para la implementación de la celda GSM, se utilizó: Yate, un motor de telefonía YateBTS, una implementación de red celular GSM/GPRS basada en Yate



(a) System Information Type 1.

(b) System Information Type 2.

Figura 5: Tramas GSM.

NO. Time	source	Destination	Protocot Ler	igtr Into		No.	Time	Source	Destination	Protocol Leng	th Info	
425 9.976679000	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH)	(RR) Paging Request Type 1	5	84 34.32420000	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) System Information Type 2
426 9.995139000	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH)	(RR) Immediate Assignment	5	85 34.342641006	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Immediate Assignment
427 10.02726700					(RR) System Information Type 3	5	86 34.370891000	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Immediate Assignment
▼GSM CCCH - System	Information Type 3					5	87 34.389230006	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Immediate Assignment
▼L2 Pseudo Length	,,					5	88 34.417185000	127.0.0.1	127.0.0.1		81 (CCCH) (RR) Paging Request Type 1
0100 10 = L2 P	seudo Length value: 18	3				5	89 34.436372008	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
♥Protocol Discrimi	nator: Radio Resources	Management messages				5	90 34.462752000	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
0110 = Prot	ocol discriminator: Ra	adio Resources Manageme	ent messages (G	x06)		00	oo = Skin	Indicator, No. ind	ication of colocted DIMN	(0)		
0000 = Skip	Indicator: No indicat	tion of selected PLMN (0)			Mes	same Type: Pagi	na Request Type 1	Ication of selected PENN	(0)		
Message Type: Sys	tem Information Type 3	3				w Pag	e Mode	ing incluence type a				
▶Cell Identity - C	I (8837)					riug	ARRA = Page	Mode: Normal pagi	ng (A)			
▼Location Area Ide	ntification (LAI)					▶ Cha	nnel Needed	nouter normat pogz				
▼Location Area Id	entification (LAI) - :	748/07/8311				▼ Mob	ile Identity -	Mobile Identity 1	- TMSI/P-TMSI (0xc0363dbe	2)		
Mobile Country	Code (MCC): Uruguay (I	Eastern Republic of) (7	748)			Le	ngth: 5	,				
Mobile Network	Code (MNC): Movistar	(07)				11	11 = Unuse	d: 0x0f				
Location Area C	ode (LAC): 0x2077 (83	11)					0 = 0dd/e	ven indication: E	ven number of identity dig	gits		
▶Control Channel D	escription							e Identity Type:	TMSI/P-TMSI/M-TMSI (4)			
▶Cell Options (BCC)	H)					TM	SI/P-TMSI: 0xc0	363dbe				
▶Cell Selection Pa	raneters					▼ Mob	ile Identity -	Mobile Identity 2	- TMSI/P-TMSI (0xc276f5d8	B)		
▼RACH Control Para	meters					El	ement ID: 0x17					
10 = Max	retrans: Maximum 4 ret	transmissions (2)				Le	ngth: 5					
10 11 = Tx-1	nteger: 16 slots used	to spread transmission	n (11)			11	11 = Unuse	d: 0x0f				
0. = CELL	BARR_ALLESS: The cel	L is not barred (0)					0 = 0dd/e	ven indication: E	ven number of identity die	gits		
= RE:	Irue					1.00	100 = Mobil	e Identity Type:	TMSI/P-TMSI/M-TMSI (4)			
0000 0000 0000 0	000 = ALC: 0X0000					TM	SI/P-TMSI: 0xc2	7615d8				
PSI 5 Rest Octers						▶P1	Rest Octets					
0000 00 00 00 00 01	0 00 00 00 00 00 00 0	0 08 00 45 00	E.			6626	00 01 ba 03 12	79 00 2f fe 42 0	92 04 01 00 <u>00 00</u> y	./ .B		
0010 00 43 11 b3 40	0 00 40 11 4a t4 7t 0 70 00 25 5 43 03 0	0 00 01 7† 00 .C@.(0. J			0030	c6 00 00 03 4b	61 02 00 03 00 4	1 06 21 a0 05 f4Ka	A.!. <mark></mark>		
0020 00 01 DE 20 1.	2 79 00 21 12 42 02 0 > a8 61 66 66 69 49 6	6 1h 22 85 47 s	·/ ·P			0040	C0 30 30 De 17	05 T4 C2 70 T5 0	18 20 20 20 20 20	··· V···++++++		
						0050	20					
🔘 💅 🛛 Frame (frame),	81 bytes Pac	kets: 427 · Displayed: 427 (100.0%) · Droppe	ed: 0 (0.0%)		0 💅	Text item (text),	5 bytes	Packets: 599 · Displayed: 599	(100.0%) · Dropped	d: 0 (0.0%)	

(a) System Information Type 3.

(b) Paging Request Type 1.

Figura 6: Tramas GSM.

Para la interfaz web de YateBTS es necesario Apache HTTP Server PHP 7.0 MySQL Server La instalación de Apache, PHP y MySQL se hará de forma sencilla omitiendo varios

aspectos de seguridad ya que se utilizará solo a modo de probar el sistema. Instalación de Apache: sudo apt-get update sudo apt-get install apache2 Instalación de MySQL Server:

sudo apt-get install mysql-server



Figura 7: Ubicación de la celda.

Instalación de PHP: Primero agregamos los repositorios para PHP7.0 sudo apt-add-repository ppa:andrej/php sudo apt-get update sudo apt-get install php libapache2-mod-php php-mcrypt php-mysql

Descargamos Yate y YateBTS de https://launchpad.net/~sico/+archive/ubuntu/yate y http://yatebts.com/download.php

Luego para compilar e instalar Yate: cd yate ./autogen.sh ./configure --prefix=/usr/local make -j4 sudo make install sudo ldconfig cd .. Para YateBTS: cd yatebts ./autogen.sh ./configure --prefix=/usr/local make -j4 sudo make install sudo ldconfig Ahora creamos un link en la carpeta www del Apache a la web de YateBTS: cd /var/www/html/

sudo ln -s /usr/local/share/yate/nib_web nib Otorgamos permisos a los archi-

vos de configuración:

sudo chmod -R a+w /usr/local/etc/yate Ahora resta configurar los Virtual Hosts

de Apache. Primero cambiamos los permisos para que el servidor pueda mostrar las páginas:

sudo chmod -R 755 /var/www

Luego creamos un nuevo archivo de Virtual Hosts:

sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/nib.conf Lo editamos con nano y cambiamos el DocumentRoot para que levante nuestra web:

sudo nano /etc/apache2/sites-available/nib.conf
DocumentRoot = /var/www/nib

Guardamos, y habilitamos el sitio con sudo a2ensite nib.conf. Ahora reiniciamos el servidor con sudo service apache2 restart y ya se puede acceder a la web a través de http://localhost/nib.

En la interfaz web pueden setearse diversos parámetros, lo que interesa en este caso son la banda, la frecuencia y la potencia. El resto son parámetros de identificación de la red que pueden quedar como están. También está la posibilidad de ponerle un nombre a la red, pero no todos los teléfonos lo mostrarán. Luego en la pestaña Transceiver, se debe indicar qué imagen tiene que utilizar, en este caso por ser un USRP se elije UHD.

Ya estamos en condiciones de correr Yate con sudo yate -s. Si todo salió bien, se verá algo como lo que muestra la Figura 10.

Escaneando las redes disponibles con un teléfono aparece inmediatamente una red nueva llamada 00101. Este nombre que no es el que se seteo, es la concatenación del MCC y el MNC. Sucede que por motivos de seguridad los teléfonos no muestran el nombre de red que uno establezca sino que recurren a algunos registros internos para los cuales los operadores tienen registrados sus códigos. De hecho haciendo pruebas con códigos de compañías de otros países (se utilizó el MMC=722 y MNC=341 correspondiente a la compañía Argentina Personal) se puede ver efectivamente cómo cambia el nombre automáticamente.

Al registrarse en la red el teléfono recibe un número via SMS con el que es posible enviar mensajes y realizar llamadas a otros móviles dentro de la red, con una calidad sorprendentemente buena.

Las Figuras 11(a), (b) y (c) son capturas de pantalla del teléfono que muestran todo esto.

GS	M GSM Advanced	
	Finish writting Warning! Field ChannelCodingContr normally be Radio.RSSITarget + 10	sections in ybts.conf file without issues. ol.RSSI doesn't have a recommended value. This value should dB, value added from tab GSM, from GSM Advanced that has the value: -50.
	Set parameters value	es for section [gsm] to be written in ybts.conf file.
	Radio.Band	EGSM900 • ?
	Radio.C0	#95: 954 MHz downlir • ?
	Identity.MCC	001 ?
	Identity.MNC	01 ?
	Identity.LAC	1000 ?
	ldentity.Cl	10 ?
	Identity.BSIC.BCC	2 7
	Identity.BSIC.NCC	0 . ?
	Identity.ShortName	tcom ?
	Radio.PowerManager.MaxAttenDB	10 🔹 ?
	Radio.PowerManager.MinAttenDB	0 2
		Submit Reset

Figura 8: Interfaz web de YateBTS.

BAS NIB	>				
ubscribers	BTS Configuration	Outgoing			
GSM	GPRS Contro	ol Transceiver	Tapping	Test	YBTS
V n	Varning! Field ChannelCoding ormally be Radio.RSSITargel	gControl.RSSI doesn't ha t + 10 dB, value added f the value: -{	ave a recomment rom tab GSM, fre 50.	ded value. This va om GSM Advance	alue should ed that has
	Set parameters va	lues for section [transce	iver] to be writter	n in ybts.conf file.	
	Path	./transceiver-uhd	• ?		
	Args			2	
	-				
	MinimumRxRSSI	-63		?	
	MinimumRxRSSI RadioFrequencyOffset	-63 Factory calibrated	•?	?	
	MinimumRxRSSI RadioFrequencyOffset TxAttenOffset	-63 Factory calibrated	▼ ?▼ ?	?	
	MinimumRxRSSI RadioFrequencyOffset TxAttenOffset Timeout.Clock	-63 Factory calibrated Factory calibrated	▼ ? ▼ ? ▼ ?	?	

Figura 9



Figura 10



Figura 11: Capturas de pantalla del celular.