Software Defined Radio for Education: Spectrum Analyzer, FM Receiver/Transmitter and GSM Sniffer with HackRF One

2018 2nd Borneo International Conference on Applied Mathematics and Engineering (BICAME) 978-1-5386-7725-4/20/$31.00 ©2020 IEEE 10.1109/BICAME45512.2018.1570509150

Ihan Martoyo, Paul Setiasabda, Herman Y. Kanalebe, Henri P. Uranus, Marincan Pardede
Electrical Engineering Dept., Universitas Pelita Harapan
Jl. M.H. Thamrin Blvd 1100, Lippo Village (Karawaci), 15811 Tangerang, Indonesia

ihan.martoyo@uph.edu, herman.kanalebe@uph.edu, henri.uranus@uph.edu, marincan.pardede@uph.edu

***Abstract*—Software Defined Radio (SDR) technology enables a programmable radio platform that can serve as a multimode transceiver. One such example of SDR is the HackRF One, which covers the frequency of 30 MHz – 6 GHz and can be programmed as an FM receiver/transmitter, a GSM receiver, or a simple spectrum analyzer. Compared to an expensive spectrum analyzer, the HackRF One provides an affordable solution for education and simple research projects. We compare the measurement of HackRF One with a spectrum analyzer and found that spurious signals were seen with HackRF One due to the mixing and down-conversion process. However, such imperfections may offer opportunities for hands-on learning and deeper understanding of the radio signal processing. Due to its half-duplex operation, HackRF One cannot be used as a GSM BTS. However, it can still function as a GSM signal sniffer. The flexibility and programmability of SDR provide an ideal platform for project-based learning in telecommunication engineering.**

Keywords—SDR, HackRF One, Radio Characterization, Spectrum Analyzer, FM receiver/transmitter, GSM receiver

I. INTRODUCTION

Joseph Mitola first envisioned the Software Radio for military radio applications that have the capability for a multimode, multisystem, and multiband communications [1]. Because it is based on software, different needs of communication can be fulfilled by simply reprogramming the Software Radio, or by over-the-air downloading the appropriate software [2]. If programmed with certain algorithms, the Software Radio can be equipped with "cognitive" capability to adapt to different mobile channel conditions or personal requirements [3].

However, like many ambitious visions, soon the realities of the technological limit kicked in. To realize an ideal Software Radio, an analog-to-digital converter (ADC) must be put right after the antenna so that all the following signals can be turned digital, thus fitting for processing with software. However, such an ADC is prohibitively very expensive. To cover the frequency band from 800 MHz to 5.5 GHz, an ADC of 12 bit and 11GS/s would be needed [4], which is quite impossible today and for the foreseeable future.

The Software Defined Radio (SDR) is a compromised version of the *ideal* Software Radio. An SDR uses hardware (FPGA), which is not very flexible; but the hardware can be programmed by software, thus providing limited flexibility. The key for the front-end is not to receive the whole available bandwidth, but to tune electronically to a certain bandwidth of interest [5].

Table I displays the basic parameters of some available SDR systems. The price of the SDR is usually proportional to the bandwidth of the system. USRP, the most expensive of the three, can operate with a bandwidth up to 61.44 MHz, with the highest sample rate of up to 128 Msps, and is operating in full-duplex. The HackRF One is the most economical of the three and is operating in half-duplex, with a bandwidth of 20 MHz. However, the HackRF One can cover the frequency from 30 MHz to 6 GHz, thus encompassing the frequencies of FM radios, GSM and WiFi systems, which is useful for educational purposes and simple research projects.

TABLE I. SDR TYPES & PARAMETERS

SDR	HackRF One	BladeRF	USRP
Frequency	30 MHz – 6 GHz	300 MHz – 3.8 GHz	50 MHz – 2.2 GHz / 6 GHz
Bandwidth	20 MHz	28 MHz	16 MHz / 61.44 MHz
Duplex	Half	Full	Full / 2x2 MIMO
Sample Rate	20 Msps	40 Msps	64 Msps / 128 Msps

Several suggestions have been published on using SDR for education. SDR can be used to demonstrate analog and digital modulations: FM, SSB, OOK, BPSK and 8-PSK [6, 7]. Even the graphical open source software GNU Radio Companion (GRC) is already useful for demonstrating communication techniques without the SDR hardware [6]. The flexible programmability of SDR is very useful for hands-on learning experience, which provides more rounded learning than just simulation systems [8].

In this work, we explore the basic functionalities of SDR that could be useful for education. The HackRF One – the most economical in Table 1 – is chosen for the project. Compared to other cheaper SDRs, such as variants of RTL-SDRs, HackRF One can cover a much wider bandwidth and has a higher frequency range. HackRF One can also be set as a transmitter, which RTL-SDR cannot do. Although it can hardly be set as a GSM mini BTS (due to its half-duplex operation), the HackRF One can still function as a GSM

signal sniffer. Thus, cheaper than the BladeRF and USRP, the HackRF One can still perform various RF functions and can be used as a low-cost spectrum analyzer, which is very useful for education purposes.

Working with SDR also requires the effort of a do-it-yourself approach with open-source resources, which is very productive for learning purposes. We also found that the frequency measurement with the SDR HackRF One is showing "ghost frequencies" or spurious readings as artifacts of the mixing and sampling processes of the SDR. Although they could become disturbing for serious applications, such imperfections could be very useful for learning purposes.

The following sections report the setting up and characterization of a spectrum analyzer, FM receiver/transmitter and a GSM sniffer using the HackRF One. The next section will describe the system, followed by measurement results and discussions in Section III. Section IV closes with some conclusions.

II. SDR WITH HACKRF ONE

A. Receiving RF signals with HackRF One

HackRF One can be installed to work on Linux operating systems (Linux Pentoo or Ubuntu) and can be programmed by using GNU Radio Companion (GRC) via a (graphical) block diagram programming interface. A simplified GRC diagram block for an FM radio receiver is shown in Fig. 1.

The Osmocom Source is the block that communicates with the HackRF hardware and provides signal from the hardware for further processing. The sample rate, frequency and IF gain can be set in the Osmocom Source block. The WX FFT Sink displays the received signals in the frequency domain. The frequency of the received FM radio signal can be set according to the *multiplication* term of the frequency in Osmocom Source (f_1) and the frequency of the Signal Source block (f_2). The received FM signal will be at f_1-f_2.

After low pass filtering and resampling, the FM signals can be demodulated with the WBFM Receive block and can then be sent to the Audio Sink for listening. The Low Pass Filter block is also doing a down-sampling. With a sampling rate of 20Msps and a decimation factor of 100, the output rate of the filter will be 200 ksps, which are sent to the Rational Resample block (interpolation = 12 & Decimation = 5), which sets the output to 200 k * 12 / 5 = 480 kHz. The WBFM Receive is also doing a down-sampling with a decimation factor of 10, giving the output at 48kHz which is supported by sound cards.

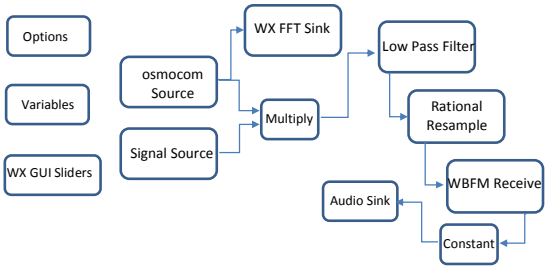

Fig. 1. Simplified GNU Radio Companion block diagram for FM Radio receiver [9].

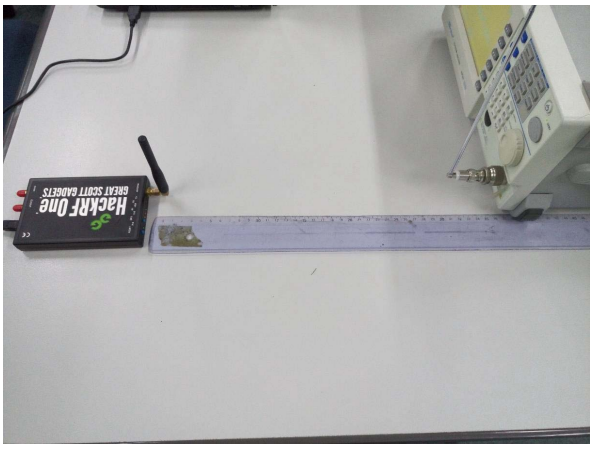

Fig. 2. HackRF One measuring RF signals compared to traditional spectrum analyzer.

It is possible to receive several FM stations concurrently by duplicating the FM signal receiving blocks and adding the received signals before sending them to the Audio Sink. Such capability can be useful for a multi-station monitoring system [10].

The FFT Sink in Fig. 1 also provides spectrum analyzer functionalities. We set up and compare the received RF signals from the HackRF One with traditional spectrum analyzer as displayed in Fig. 2.

B. Transmitting FM signals with HackRF One

The HackRF is capable of half-duplex operation, thus it can be set as a transmitter as well. The simplified FM transmitter block in GRC is shown in Fig. 3. The low-pass-filtered output of the Audio Source signal will go through a resample process and WBFM Transmit for the FM modulation before being sent to the SDR hardware (Osmocom Sink) for RF transmission.

C. Sniffing GSM transmission with HackRF One

The HackRF One cannot function as a GSM mini BTS due to its half-duplex operation. For a GSM mini BTS, the full-duplex BladeRF can be utilized [11]. However, the HackRF One can still be programmed to listen to GSM transmission. GRC programs for GSM sniffing can be obtained at [12], which uses the following main blocks: GSM input adaptor, GSM Receiver, BCCH + CCCH Demapper, SDCCH Demapper, Decryption, and Control channels decoder.

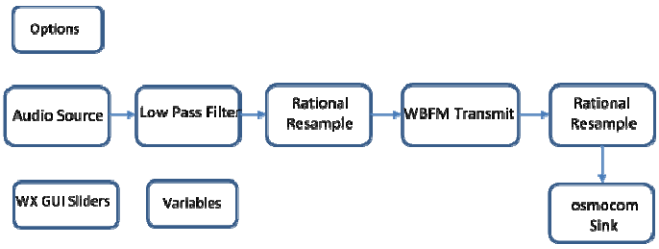

Fig. 3. Simplified GNU Radio Companion block diagram for FM Radio transmitter.

III. Measurement Results, FM Transceiver & GSM Sniffing

A. FM Transceiver signals with HackRF One

The FM receiver with HackRF One is set to receive the Heartline FM (100.6 MHz) transmission, a local radio station in Tangerang, Indonesia, which is located only 2.9 km away from the lab where the measurements were carried out [13]. The received signal with HackRF One FFT block is shown in Fig. 4. The spike in the middle is due to DC offset of the direct conversion receiver, which is always shown at the center frequency, in this case at 100 MHz. Fig. 4 shows other spurious signals beside the Heartline transmission at 100.6 MHz. The largest spurious signal is at 107.3 MHz.

Spectrum measurements with other SDR (BladeRF) is also showing spurious signals, which seem to come from the mixing/sampling process of the SDR [11]. A comparison with the measurement from a traditional spectrum analyzer (Fig. 5) shows no significant signals within the 20 MHz bandwidth around the Heartline FM signal at 100.6 MHz.

Ossman discussed the causes and positions of the spurious signals with the HackRF One [14]. The HackRF One is using MAX2837 direct conversion RF transceiver and RFFC5072 wideband synthesizer/mixer. The spurious signals are related to the intermediate frequency (IF) of the MAX2837 and the local oscillator (LO) of the RFFC5072. The radio frequency of interest (RF) is RF = |IF - LO| or RF = |IF + LO|. Bad spurs occur when LO or multiple integer of LO is within 10 MHz (half the bandwidth of the baseband filter) near RF or IF.

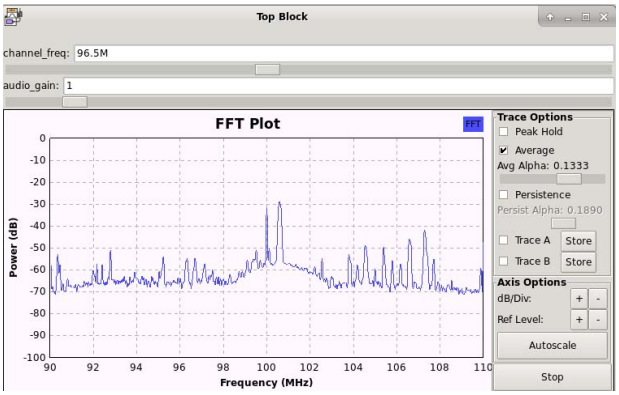

Fig. 4. Heartline FM at 100.6 MHz measured by HackRF One.

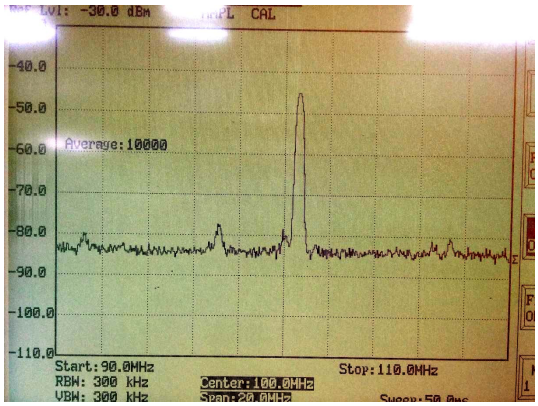

Fig. 5. Heartline FM at 100.6 MHz measured by traditional spectrum analyzer.

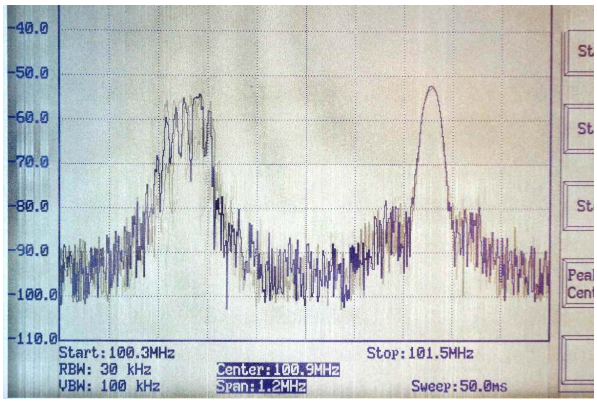

Fig. 6. Heartline FM at 100.6 MHz (left), HackRF One sine-wave transmission at 101.2 MHz (right) with 60 dB IF gain.

If the HackRF is set as an FM transmitter, it can also function as a jammer for certain frequency in a very limited range. Fig. 6 shows the Heartline FM transmission (100.6 MHz) with a roughly equal received power from the nearby HackRF One at 101.2 MHz. If the HackRF One is set to transmit at 100.6 MHz, then the Heartline FM will be jammed. Such FM transmitter could be useful for emergency communication or in remote areas. If more transmission distance is needed, an additional power amplifier could be used to increase the typical power output of about 10 dBm of the HackRF One (typical output of ISM device).

B. GSM Signals with HackRF One

The HackRF One can sniff GSM signals. After installing the necessary GSM program package [12], we can use **kalibrate-hackrf** to first scan the available GSM signals by hopping around known GSM frequencies [15]. The detected GSM signal can then be observed with **gr-gsm** as shown in Fig. 7. We captured the downlink signal of one of the largest GSM operators in Indonesia at 947.2 MHz.

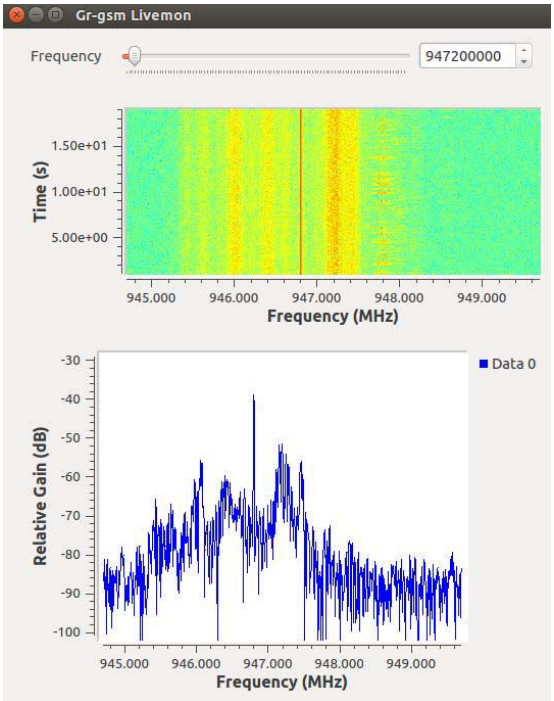

Fig. 7. Receiving GSM signal at 947.2 MHz with GR-GSM on HackRF One.

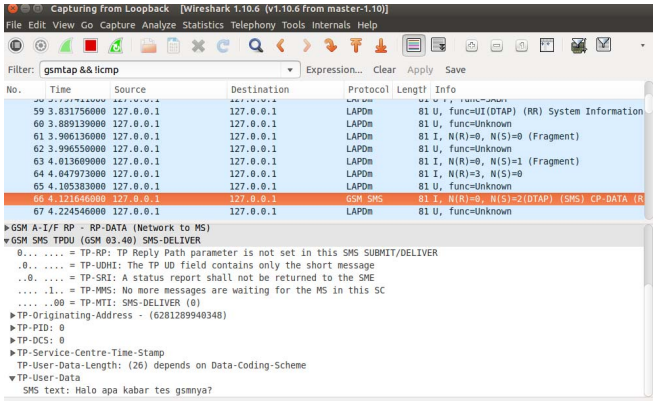

Fig. 8. Receiving GSM signal at 947.2 MHz with GR-GSM on HackRF One.

By using **Wireshark**, the data from the downlink signal can be decoded, and the number for the cell identity can be retrieved. Our mobile phone can then be set manually to connect with the cell with that certain ID. We used an old Blackberry phone, where the TMSI (Temporary Mobile Subscriber Identity) and Kc (encryption key) code of the phone can be accessed via the engineering screen. The TMSI and the Kc are needed to decode the SMS information [16].

After sending an SMS message, the TMSI of the device can be used to identify the SDCCH channel and time-slot used by the transmission. With the SDCCH information and Kc, the received signal can be decoded with **gr-gsm** to retrieve the SMS information as can be seen in Fig. 8. The line at the bottom shows the message, "Halo apa kabar tes gsmnya?" which was sent from the originating number of the phone: 6281289940348.

We tested different antennas for the transmission of HackRF One. The ANT500 antenna that comes with the HackRF One has the range from 75 MHz to 1 GHz. We also used two other dipole antennas: ANRD82421703 (GSM 824 MHz – 960 MHz and 1710 MHz – 2170 MHz), and ANRD245X05 (WiFi 2400 – 2485 MHz and 5.1 GHz – 5.8 GHz). We found that using an inappropriate antenna for a certain range can give 10 dB – 20 dB less power in the signal received by a spectrum analyzer.

We also tested jamming GSM and WiFi system by transmitting on the particular GSM and WiFi frequencies. Manually connected GSM can be disconnected from the BTS by transmitting at the active frequency. However, GSM uses a handoff mechanism to reconnect to stronger cells. We can also disconnect WiFi connection by targeting a certain active WiFi frequency. But the WiFi system can be reconnected to other undisturbed WiFi channels.

C. The Toylike HackRF One for Education

It can be claimed that the HackRF One cannot be used for serious communications. It is difficult to set up HackRF One for a GSM BTS. Not only because it operates in half-duplex, but also because the GSM downlink and uplink frequencies can be separated by more than 20 MHz, beyond the bandwidth of HackRF One.

Spectrum measurements with HackRF One also show artifacts of spurious signals from its down-conversion and mixing operation. As a serious spectrum analyzer for laboratory use, HackRF One might not be adequate. However, if envisioned as an education tool, HackRF One is very promising. The spurious measurement signals may invite questions and efforts for explanation, which are perfect for learning experience.

The FM receiver and transmitter with HackRF One is easy to implement for learning purposes. If a larger distance or coverage is needed for the FM transmitter, additional power amplifier could be employed.

Sniffing GSM signals is more complicated to implement. If the TMSI and Kc of the mobile device are not available, eavesdropping on GSM signals might include cracking the A5/1 encryption, which might require more efforts. However, in an educational setting, a handset with known TMSI and Kc can be used for demonstrating the capturing of GSM information.

IV. CONCLUSIONS

The HackRF One can easily be set as an FM transceiver, while at the same time providing a spectrum measurement via the FFT block. Because the spectrum measurement of HackRF One shows spurious signals due to its mixing/down-conversion process, the HackRF One offers many promising applications for hands-on learning experience. Activity modules that accentuate the phenomenon of the spurious received signals can be designed to illustrate the process of down-conversion of RF signals. "Shaking off" spurious signals from real signals can also be done by looking at the spectrum with different sampling or frequency settings.

Setting the HackRF One for GSM signal sniffing is more complicated. It involves scanning the known GSM frequencies and identifying the channel and time-slot used by specific transmission with known TMSI. Decoding the GSM information can be done by using known encryption key Kc. The more complicated steps would be a good educational illustration for the operation of the GSM systems.

Educational activities that include hands-on experience (not just simulations) are therefore possible without expensive RF equipment and spectrum analyzers. The HackRF One is flexible enough to be programmed as a spectrum analyzer, FM receiver/transceiver and a GSM signal sniffer, which can be integrated into the learning process for courses in telecommunications. Similar testing was also done with the BladeRF and reported elsewhere [11].

ACKNOWLEDGMENT

This work is supported by the Indonesian Ministry of Research and Higher Education no. 021/KM/PNT/2018, March 6, 2018; Kontrak Penelitian Dasar Unggulan Perguruan Tinggi no. 149/LPPM-UPH/IV/2018.

REFERENCES

[1] J. Mitola, "The Software Radio Architecture," *IEEE Communications Magazine*, vol. 33, no. 5, pp. 26-38, 1995.

[2] E. Buracchini, "The Software Radio Concept," *IEEE Communications Magazine*, vol. 38, no. 9, pp. 138-143, 2000.

[3] J. Mitola & G.Q. Maguire, "Cognitive Radio: Making Software Radios More Personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13-18, 1999.

[4] A. A. Abidi, "The Path to the Software-Defined Radio Receiver," *IEEE Journal of Solid-State Circuits*, vol. 42, no. 5, pp. 954-966, 2007.

[5] T. Hentschel, M. Henker, G. Fettweis, "The Digital Front-end of Software Radio Terminals," *IEEE Personal Communications*, vol. 6, no. 4, pp. 40-46, 1999.

[6] M. R. Doallo & Jorge Nestor Rodriguez Mallo, "Analog and Digital Demodulation Process Examples Using GNU Radio," *2018 IEEE World Engineering Education Conference (EDUNINE)*, 2018, pp. 1-5.

[7] H. Miyashiro, M. Medrano, J. Huarcaya & J. Lezama, "Software defined radio for hands-on communication theory," *IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON),* August 2017, pp. 1-4.

[8] K. VonEhr, W. Neuson & B. E. Dunne, "Software Defined Radio: Choosing the Right System for Your Communications Course," *Proceedings of the American Society for Engineering Education (ASEE),* 2016, pp. 1-19.

[9] M. Ossman, "Software Defined Radio with HackRF, Lesson 1," *Greatscottgadgets*, 2015. Accessed on: Nov 4, 2018. [Online]. Available: https://greatscottgadgets.com/sdr/1/

[10] T. Juhana & S. Girianto, "An SDR-based multistation FM broadcasting monitoring system," *11th IEEE International Conference on Telecommunication Systems Services and Applications (TSSA),* 2017, pp. 1-4.

[11] I. Martoyo, A. Coandi, D. Pratignyo, H.Y. Kanalebe, H.P. Uranus, M. Pardede, "Software defined radio applications for mini GSM BTS and spectrum analyzer with BladeRF," in *IEEE International Conference on Radar, Antenna, Microwave, Electronics and Telecommunications (ICRAMET),* 1-2 Nov. 2018.

[12] P. Krysik, "Gr-gsm," *Github*, Accessed on: Nov 4, 2018. [Online]. Available https://github.com/ptrkrysik/gr-gsm

[13] Heartline 100.6 FM Radio [Online]. Available http://heartline.co.id/

[14] M. Ossman, "HackRF One RX Spectrum," *Github Mossman HackRF,* Accessed on: Nov 4, 2018. [Online]. Available https://github.com/mossmann/hackrf/issues/109

[15] Z4ziggy, "Sniffing GSM traffic with HackRF," May 17, 2015. Accessed on: Nov 4, 2018. [Online]. Available https://z4ziggy.wordpress.com/2015/05/17/sniffing-gsm-traffic-with-hackrf/

[16] C.K. "GSM: Sniffing SMS Traffic." *CKN*, Nov 29, 2015. Accessed on: Nov 4, 2018. [Online]. Available https://www.ckn.io/blog/2015/11/29/gsm-sniffing-sms-traffic/