Comparison of GSM Link Quality Performance: OpenBTS versus Test Equipment

Comparación del rendimiento de la calidad de enlace GSM: OpenBTS versus equipo de prueba

Edith Paola Estupiñán-Cuesta[1], Juan Carlos Martínez-Quintero[2], José de Jesús Rugeles[3]

Abstract

The implementation of wireless communication systems such as GSM on SDR (Software Defined Radio) platforms is increasingly common not only in order to reduce costs in the deployment of a network, but also to find and exploit vulnerabilities in the security of systems with this technology. The development of BTS (Base Transceiver Station) in GSM based on free software and SDR as OpenBTS has allowed different investigations such as IMSI catcher implementations and man-in-the-middle attacks by impersonating a real cell. This Research show and analyze the physical parameters for a channel in the GSM900 band with OpenBTS on a USRP N210 compared to a vector signal generator. There was defined 5 scenarios to

[1] Ingeniera en Telecomunicaciones egresada de Universidad Militar Nueva Granada Ingeniera en Telecomunicaciones, Universidad Militar Nueva Granada, Colombia. Magister en Ingeniería Electrónica, de la Pontificia Universidad Javeriana, Colombia. Docente Universidad Militar Nueva Granada, Bogotá, Colombia. /Programa de Ingeniería en Telecomunicaciones. E-mail: edith.estupinan@unimilitar.edu.co ORCID: https://orcid.org/0000-0002-4100-4943

[2] Ingeniero Electrónico egresado de la Universidad Manuela Beltrán, Colombia. Especialista en Seguridad física e informática, Escuela de comunicaciones Militares, Colombia. Magister en Sistemas automáticos de producción de la Universidad tecnológica de Pereira, Colombia. Docente Universidad Militar Nueva Granada/Programa de Ingeniería en Telecomunicaciones. E-mail: juan.quinteroq@unimilitar.du.co ORCID: https://orcid.org/0000-0001-9893-6592

[3] Ingeniero Electrónico egresado de la Universidad Industrial de Santander, Magíster en Ingeniería Electrónica egresado de la Universidad Industrial de Santander, Colombia. Docente Universidad Militar Nueva Granada/Programa de Ingeniería en Telecomunicaciones. E-mail: jose.rugeles@unimilitar.edu.co, https://orcid.org/0000-0003-4235-8580

evaluate the quality of the GSM burst with different configurations. The experiment analyzes the frequency error, phase error and power vs. time for the downlink channel. Results shown that it is possible to detect a fake cell implemented with OpenBTS by analyzing the behavior of its parameters in relation to the specialized equipment or the actual cell. The measured parameters are also a reference for the normal operation of OpenBTS over USRP N210. These parameters can be used for the detection of false BTS or identification of errors in the deployment of networks with this technology.

Keywords: Frequency error, GSM, OpenBTS, Phase Error, Intrusion detection.

Resumen

La implementación de sistemas de comunicación inalámbrica como GSM en plataformas SDR (Software Defined Radio) es cada vez más común no solo con el fin de reducir costos en el despliegue de una red, sino también para encontrar y explotar vulnerabilidades en la seguridad de sistemas con esta tecnología. El desarrollo de BTS (Base Transceiver Station) en GSM basado en software libre y SDR como OpenBTS ha permitido diferentes investigaciones como implementaciones de catcher IMSI y ataques man-in-the-middle al hacerse pasar por una celda real. Esta investigación realiza un muestro y análisis de los parámetros físicos de un canal en la banda GSM900 con OpenBTS en un USRP N210 en comparación con un generador de señales vectoriales. Fueron propuestos 5 escenarios para evaluar la calidad de la ráfaga GSM con diferentes configuraciones. El experimento analiza el error de frecuencia, el error de fase y la potencia frente al tiempo para el canal de enlace descendente. Los resultados mostraron que es posible detectar una celda falsa implementada con OpenBTS analizando el comportamiento de sus parámetros en relación con el equipo especializado o la celda real. Los parámetros medidos también son una referencia para el funcionamiento normal de OpenBTS sobre USRP N210. Estos parámetros se pueden utilizar para la detección de falsas BTS o identificación de errores en el despliegue de redes con esta tecnología.

Palabras clave: Detección de intrusos, Error de frecuencia, Error de Fase, GSM, OpenBTS.

1. Introduction

The GSM (Global System for Mobile Communications) technology has been of great importance in extending mobile telephony networks because it is a robust system for voice communication and short messages. Despite operators migrating to more advanced systems with more efficient modulation schemes and secure links, GSM is still among the most widely used mobile telephony schemes and is supported by the vast majority of user terminals [1]. The increase in users, cellular operators, and equipment manufacturers leads to the evolution of these systems. Proposed GSM system implementations seek to offer advantages in terms of cost and operation over existing ones; for example, in terms of cost, GSM systems based on Software Defined Radio (SDR) are a good alternative. These platforms consolidate as an option in terms of versatility, operation, and cost compared to other RF equipment used [2]. SDR has enabled reconfigurable radio projects like Open Base Transceiver Station (OpenBTS) to use these types of platforms to achieve the implementation of robust communication projects with technologies that remain relevant. OpenBTS aims to create an open-source software-based GSM access point that allows compatible mobile phones to make calls and send messages without needing to be connected to an existing commercial network [3]. The fact that OpenBTS uses SDR as physical support in its GSM system makes the technical validation of physical parameters in transmission important.

OpenBTS has the potential to be implemented for various purposes. For example, some studies have demonstrated that OpenBTS can be used to extract relevant information from a mobile device and then impersonate a commercial GSM cell. In [4], an analysis of vulnerabilities in GSM mobile networks is presented through the execution of active/passive man-in-the-middle attacks. A malicious GSM system was established using USRP and OpenBTS to send modified

SMS messages to multiple users in order to obtain their IMSI. The analysis was conducted in a controlled environment, successfully executing the attack and demonstrating authentication vulnerabilities for mobile users. In [5], the implementation of a mobile network using OpenBTS and USRP Ettus N210 is presented. A replica of a BTS station was created to generate VoIP traffic using Asterisk. The traffic generated between mobile devices when establishing a call was captured using Wireshark, aiming to identify security vulnerabilities in mobile user authentication processes, analyzing aspects such as bilateral authentication and mobile location registration. These analyses can be useful for preventing man-in-the-middle attacks. In [6], the implementation of an IMSI catcher using USRP and OpenBTS is presented, sending malicious SMS messages to multiple users. During the execution of the attack, unencrypted traffic was captured by the BTS, determining that one of the main vulnerabilities of GSM networks is that the attacker can completely isolate a user from the mobile network without their knowledge, thus forcing them to connect to a base station. However, the attack has distance restrictions due to the power of the USRP and must be executed as close as possible to the users.

Another application in which GSM technology implemented on SDR remains relevant is communication in disaster situations. In the event of a disaster, communication infrastructure may be affected by structural damage or power outages. In such cases, the use of OpenBTS can be operational for communication among rescuers as well as for locating or contacting trapped individuals. For example, [7] presents a prototype of a rapidly deployable GSM network to provide voice service in emergency situations. Service quality is evaluated with a variable number of calls using two OpenBTS nodes connected by a WiFi link. [8] proposes the use of an unmanned aerial vehicle to transport a GSM cell implemented with OpenBTS to provide coverage to relief agencies in case of disaster. [9] offers rescue teams a mobile OpenBTS cell that allows predicting the distance to the victim, in addition to voice and text messaging

services. The system design takes advantage of the fact that most people have a mobile phone, and when trapped, the device automatically connects to OpenBTS in the absence of other mobile telephony infrastructure. Furthermore, OpenBTS is shown as a solution to provide voice and text messaging (SMS) coverage in remote areas where it is not profitable for operators to deploy mobile telephony infrastructure due to low population density or the reduced income of the communities residing there. [10] and [11] describe the implementation of a mobile telephony network using OpenBTS in a rural area of Macha in Zambia. To achieve this goal, each base station had a 1W power amplifier, providing coverage of approximately a 3km radius. To establish communication with other networks, a long-distance WiFi link already implemented in the area was used.

Likewise, studying quality parameters in GSM cells allows evaluating their operational condition and determining performance thresholds. Over the years, various studies have been conducted on this topic. In [12], a method based on digital signal processing is proposed, leveraging the time/frequency properties of GSM signals over a commercial cell. Once digitized, the GSM signal is transformed, producing a spectrum image for each time interval, and with this information, measurements of phase and frequency error are conducted at the receiver. Results determined a frequency error of 12 Hz, and phase errors of 10º (peak) and 3º (RMS). Additionally, [13] introduces a method involving comparison of the phase of the reconstructed signal with that of a received signal, and subsequent estimation of frequency error using neural networks, measured in static and dynamic propagation scenarios involving multipath reflection, Doppler effect, and fading. Measurements with the proposed method determined frequency errors not exceeding 12 Hz.

Recently, the use of OpenBTS has also been demonstrated as a viable network solution for IoT devices [14], and the feasibility of using OpenBTS in portable infrastructure for deployment in remote areas of Indonesia has been suggested [15].

This research highlights the behavior of the physical layer of OpenBTS on USRP N210. The conducted measurements allow characterization of its behavior and establishment of differences between this implementation and implementation with specialized equipment. In this regard, the contribution of this article lies in utilizing the results for potential identification of SDR hardware used for impersonation. This identification is possible because conventional SDR hardware operates within different ranges in the measured parameters compared to professional equipment. The results can be applied in detecting "fake" GSM cells and IMSI catchers implemented with USRP. This contribution is significant as no similar findings have been found in the literature on OpenBTS and attack detection. Furthermore, it is noteworthy that the same principle can be applied to applications aimed at similar objectives but using other technologies implemented on SDR. Characterizing OpenBTS on USRP also facilitates detection of possible errors in infrastructure installed with this technology. The study was conducted on a GSM downlink radio channel, analyzing parameters such as frequency error, phase error, and channel power versus frame time, and performance limits were determined. Section I provides a theoretical description of the quality parameters to be evaluated and the fundamental concepts of SDR and OpenBTS. Section II presents proposed scenarios for evaluating physical parameters in the 900 MHz band and the data acquisition process; finally, sections III and IV present the analysis of the obtained measurements and the respective conclusions

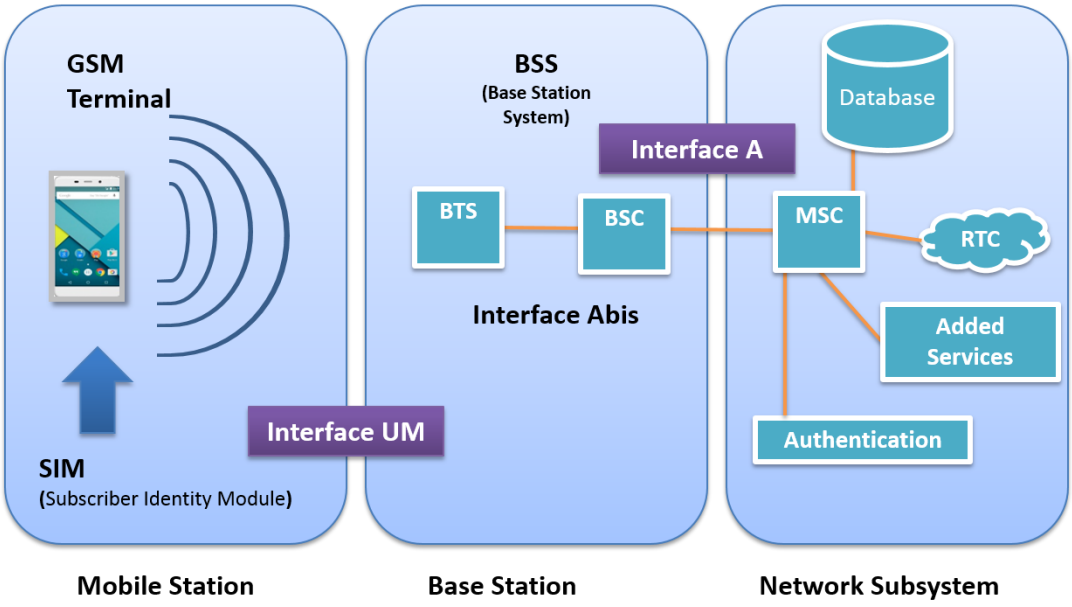
1.1. GSM Concepts and Quality Parameters in the Physical Layer

1.1.1 GSM

GSM (Global System for Mobile Communications) technology was defined by the ETSI (European Telecommunications Standards Institute) for mobile communications. It is considered the second generation of mobile network standards, originally known as GSM 900. Among its features, it operates over the

frequency bands of 850MHz, 900MHz, 1800MHz, and 1900MHz. It generally employs Gaussian Minimum Shift Keying (GMSK) modulation, which uses a clock frequency specific multiple of 13 MHz to achieve synchronization between the phone and the Base Transceiver Station (BTS) [16] [17] [18]. A GSM system consists of Mobile Stations (MS), Base Stations BTS, and a Base Station Controller (BSC). BSCs are responsible for handovers between mobile cells and power control, among other tasks. Interconnections between BSCs are made through a switching center called Mobile Switching Center (MSC), which controls call management processes such as call setup, routing, control, and termination. Figure 1 provides an overview of the elements comprising a GSM system.

Figure 1. General structure of a GSM network



Source: Taken from [17]

Two terms commonly used in mobile telephony systems are uplink and downlink. Uplink specifies the frequencies used from the mobile device to the base station, while downlink specifies the link from the base station to the mobile device. The choice of these frequencies is determined by the Absolute Radio-Frequency Channel

Number (ARFCN), which refers to the channel number being used for transmitting and receiving data at a given time. For example, in GSM900, channel 1 uses a frequency of 935.2MHz for downlink and 890.2MHz for uplink [17] [18] [19].

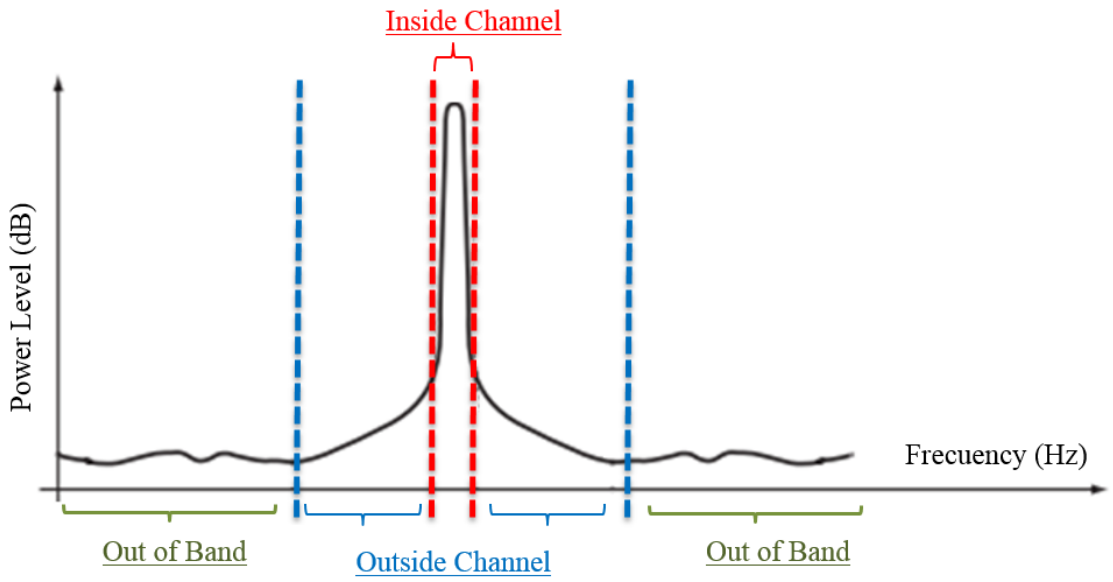
1.1.2. GMSK

Gaussian Minimum Shift Keying (GMSK) is the modulation scheme characterized by reducing the spectrum compared to Minimum Shift Keying (MSK) modulation. The unmodulated signal passes through a Gaussian low-pass filter before being applied to the modulator. This filter smooths the phase transitions of the signal during transmission, resulting in the reduction of the transmitted signal's bandwidth. In GMSK modulation, one symbol is equivalent to one bit. In GSM, GMSK operates at a symbol modulation rate of 270.833 Kbit/s and defines complete bursts of 147 symbols of useful duration [20] [21] [22] [23]. Disadvantages of this modulation include its low noise immunity and implementation complexity [18].

1.1.3 GSM Performance Parameters

For a GSM system, hardware plays a significant role in its operation. The behaviors of the physical components determine the quality of data transmission and reception, with the expectation that each component operates within the limits for which it was designed. Critical physical performance metrics of GSM systems can be evaluated at the transmitter and receiver in three areas: within the transmission channel (in-channel), outside the channel (out-of-channel), and out of band (out-of-band). Figure 2 illustrates this description.

Figure 2. Link Quality Parameters in a GSM Channel



Source: Own work

These measurements can detect errors in modulation and accuracy in power, among others. Assessing these parameters can provide an estimation of the operational accuracy of the architecture and determine whether the measured parameters fall within the defined standards. Stakeholder groups such as 3GPP and ETSI have established guidelines for validating the operation of GSM components through standards like 3GPP TS 05.05.V8.12.0 [24] and 3GPP TS 11.21 V8.6.0 [25]. In-channel measurements determine link quality and include phase error, frequency error, RF carrier frequency power, carrier power vs. time, among others. Out-channel measurements assess the level of interference caused by a GSM user to other users. They include modulation-generated spectrum, noise bandwidth, TX and RX spurious bandwidth, among others. Out-of-band measurements determine the interference caused by a GSM user to non-GSM users, including harmonics and spurious emissions [26] [27] [28] [29] [16]. In this case, the research focuses on the in-channel operation study of the GSM system, describing the main characteristics of these measurements.

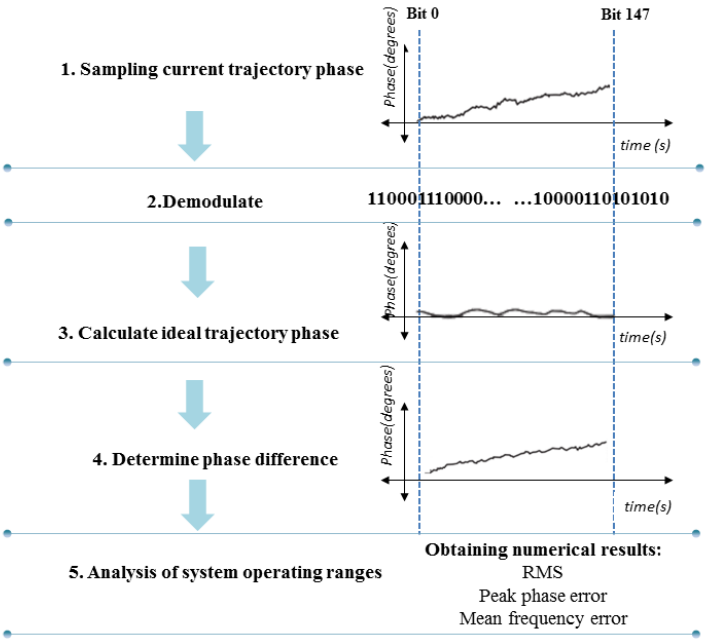
1.1.4 Frequency error

It is defined as the deviation of the carrier frequency from the expected value. The error can be determined by calculating the difference between the measured signal and the reference signal. Typically, the reference signal is generated by specialized measuring equipment [27]. This type of error can cause problems in the system and compromise synchronization tasks with the BTS and their controllers, which can lead to the loss of communication from the mobile station (MS) in motion. This error occurs in GSM systems due to faults in electronic cards and can be measured using different methodologies and measuring instruments. Regulations specify that the frequency error is limited to an average frequency deviation of no more than 0.05 ppm with respect to its desired output frequency [21].

1.1.5 Phase Error

Phase error is a parameter that allows determining the accuracy of modulation. The general process for phase error detection can be seen in Figure 3.

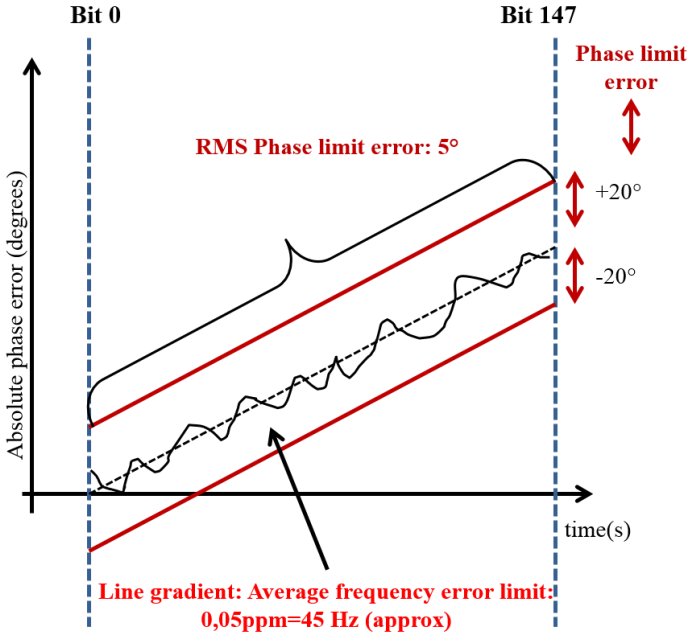
Figure 3. Defined Process for Measuring Phase Error Parameters



Source: Own work

The difference between the phase of the transmitted wave and the expected phase determines the phase error, and according to the specification, it should not exceed 5° RMS with a maximum peak deviation during the useful part of the burst less than 20°, as shown in Figure 4 [21]

Figure 4. Operating limits of link quality parameters in GSM900 for frequency error and phase error.



Source: Own work

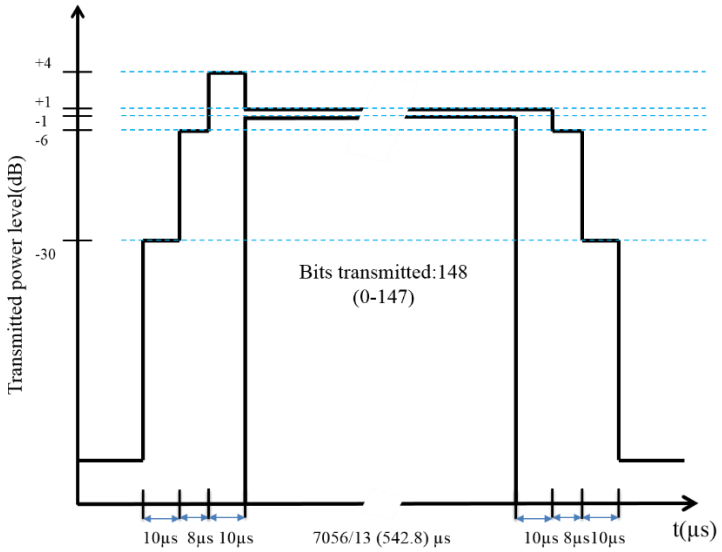
The phase error limits are commonly generated by the hardware components of the transmitter (filters, amplifiers, modulators). Phase error reduces the likelihood of the GSM receiver performing a correct and accurate demodulation process. When transmitting an information burst, the phase accuracy of the signal can be validated with respect to the theoretical modulated waveforms defined in the 3GPP TS 45.004 standard, thus determining the system's performance.

1.1.6 RF Carrier frequency power versus time

This parameter allows evaluating the power of the carrier signal frequency in the time domain against a predefined mask. If a transmitter fails this measurement, it typically indicates a problem with power control. For GMSK modulation, the term output

power refers to the measurement of power when averaged over the useful part of the burst. The BTS must be able to not transmit a burst in a time interval unused by a logical channel. The behavior of the output power relative to time at the end of a burst can be seen in Figure 5 [30]

Figure 5. Time mask with a typical duration for GMSK modulation



Source: Own work

1.2. SDR y OpenBTS

The ITU-R in 2009 formalized in its report SM.2152 the definition of SDR as "*a radio transmitter and/or receiver that can use a technology allowing the setting or modification of RF operating parameters, including, among others, the frequency range, modulation type, or output power, except for changes to operating parameters occurring during the normal pre-installed and predetermined operation of a radio system according to a system specification or standard*."

On the other hand, USRP is an SDR platform developed by ETTUS, with the USRP N210 being a prominent hardware within its lineup. This is a system structured around a motherboard with the ability to integrate daughter cards (RF front-ends), enabling operation across various frequency bands for the implementation of powerful and flexible radio

systems. This system is ideal for applications requiring high RF performance in wireless technology testing. Technically, a USRP employs an In-phase (I) and Quadrature (Q) Quadrature Amplitude Modulation (QAM) system. Physically, a USRP consists of a baseboard that includes a Xilinx Spartan 3A-DSP 3400 FPGA, two 14-bit analog-to-digital converters (ADCs) with 100 MS/s, and two 16-bit digital-to-analog converters (DACs) with 400 MS/s; these conversion speeds require a Gigabit Ethernet interface to ensure processing of all information. The daughterboard WBX has a bandwidth covering different GSM bands.

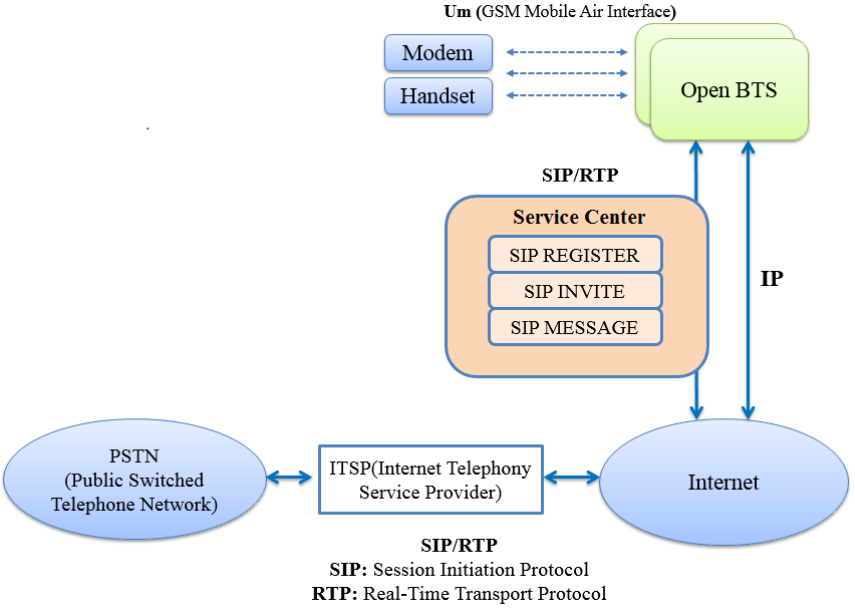
The WBX allows operation as a transmitter and receiver from 50 MHz to 2.2 GHz, with a transmission gain ranging from 0 to 25 dB and a reception gain from 0 to 31.5 dB. The system's main clock is a 10 MHz TCXO type located on the main USRP board, with an accuracy of 2.5 parts per million (ppm). An external synchronization clock can also be used, such as a GPS source or MIMO source [31]. From the main clock, an integrated programmable clock generation and distribution chip AD9510 is used, which includes dividers, PLLs, and multiplexers to deliver signals of different frequencies through different outputs to the system components that require them, including the synthesizers in the transmission and reception stages, which serve as a reference clock.

1.3. OpenBTS

It is a collection of open-source software components that allows the implementation of a mobile network using traditional telephony protocols. The interface proposed by OpenBTS for GSM at its physical layer clearly adheres to the specifications of GSM standards 05.01, GSM 05.05, and their entire series. OpenBTS is supported at the hardware level by an SDR platform, allowing it to emulate a GSM cell and provide call and text messaging services to devices compatible with GSM technology. Communication in OpenBTS is converted into SIP and RTP packets on the IP part of the network, and it interacts with these components to form the core

network. For its operation, OpenBTS replaces the traditional GSM configuration, and the USRP is responsible for receiving and transmitting GSM signaling, as it interacts directly with the computer through the Gigabit Ethernet network interface. For the implementation of a GSM network with OpenBTS, complementary components are used, such as: Asterisk, SIPauthserve, and SMQueue. Asterisk is a platform that allows the simulation of a mobile telephony exchange under the SIP protocol. SIPauthserve is a software platform that processes the SIP protocol registration request generated by OpenBTS when a mobile station attempts to join the GSM network. When the mobile station successfully connects, SIPauthserve is responsible for updating the database with the information of this new device so that other devices in the network can communicate with each other. SMQueue is an application that processes SIP protocol requests when a mobile user sends an SMS and manages all related tasks. This application schedules the sending of messages and is also capable of rescheduling them if the destination device is not available on the network [32]. The architecture of OpenBTS is shown in Figure 6.

Figure 6. Hybrid OpenBTS/IP Architecture



Source: Own work

2. Proposed Scenario

For the evaluation of downlink link quality parameters in transmission, 5 measurement scenarios are proposed. The equipment used includes: USRP N210 (USRP 2), WBX daughterboard, GPSDO Kit, VERT900 antenna (USRP), Agilent N5172B vector signal generator, Anritsu MS2722C spectrum analyzer, and measurement kit. Table 1 specifies the 5 proposed scenarios and their characteristics. The first four scenarios allow measuring the quality of the OpenBTS downlink GSM burst in the absence of mobile stations with two different clock configurations: The first using the 10MHz TCXO clock of the USRP baseboard (scenarios 1 and 2), and subsequently using a GPS module as an external clock source instead (scenarios 3 and 4). Figure 7 illustrates this scenario. In the last scenario, the same measurements are conducted on a GSM burst transmitted by a vector signal generator, as shown in Figure 8.

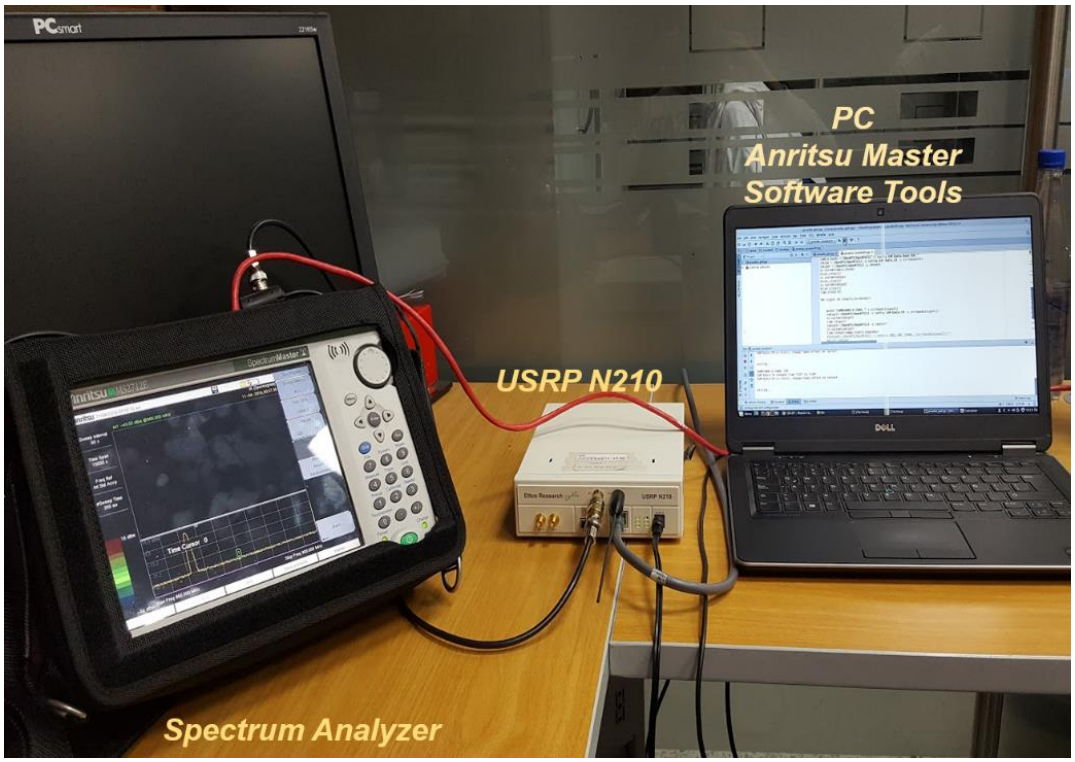
Table 1. Description of Proposed Scenarios for Evaluating Link Quality Parameters for a GSM900 Downlink Channel

N°	*ID*	*Channel*	*USRP with GPS*	*Frequency (MHz)*	*Connection to the Spectrum Analyzer*	*GSM Burst Generation*
1	E1	1	Not	935,2	Wired	OpenBTS
2	E2	1	Not	935,2	Wireless	OpenBTS
3	E3	1	Yes	935,2	Wired	OpenBTS
4	E4	1	Yes	935,2	Wireless	OpenBTS
5	E5	1	Does not apply	935,2	Wireless	Vector Generator

Source: Own work

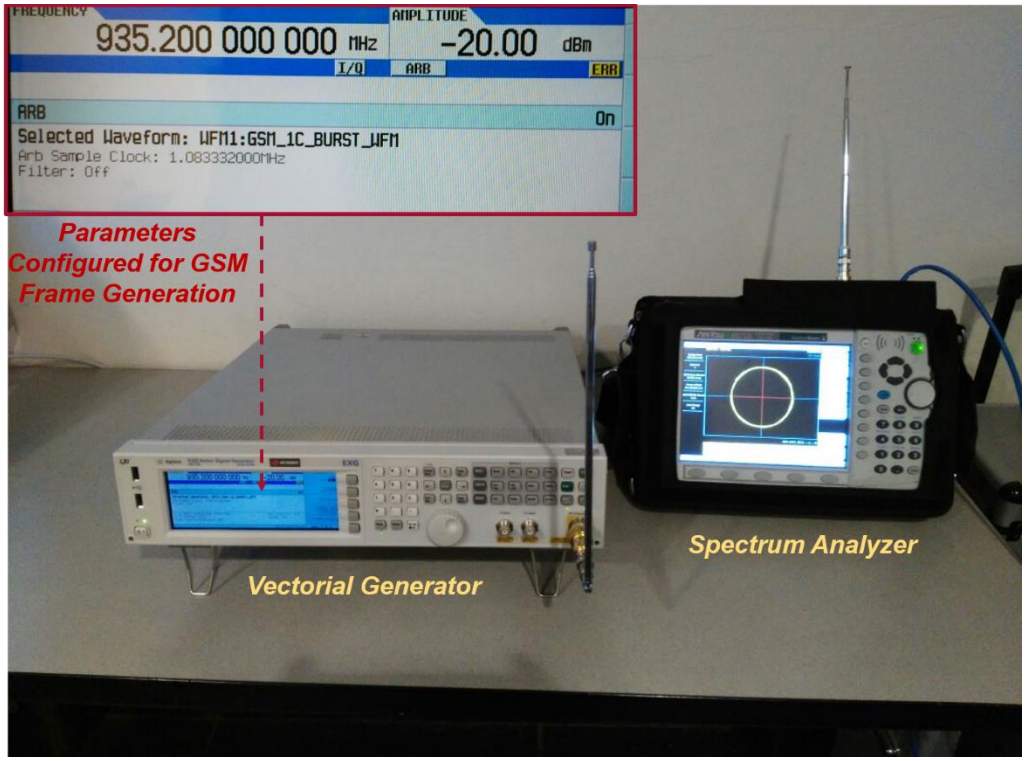
In both setups, the bursts are generated by software with the same characteristics: GMSK modulation, transmission rate of 270,833 Kbit/s, and baseband generation with 4 samples per symbol. Both setups employ IQ modulation scheme in the hardware.

Figura 7. Wired Scenario for Measuring Parameters of GSM Burst Generated by OpenBTS, USRP N210, GSM900 Channel 1 (935.2 MHz)



Source: Own work

Figura 8. Scenario 5 for measuring parameters of GSM burst transmitted by Agilent N5172B vector signal generator, GSM 900 Channel 1 (935,2 MHz)



Source: Own work

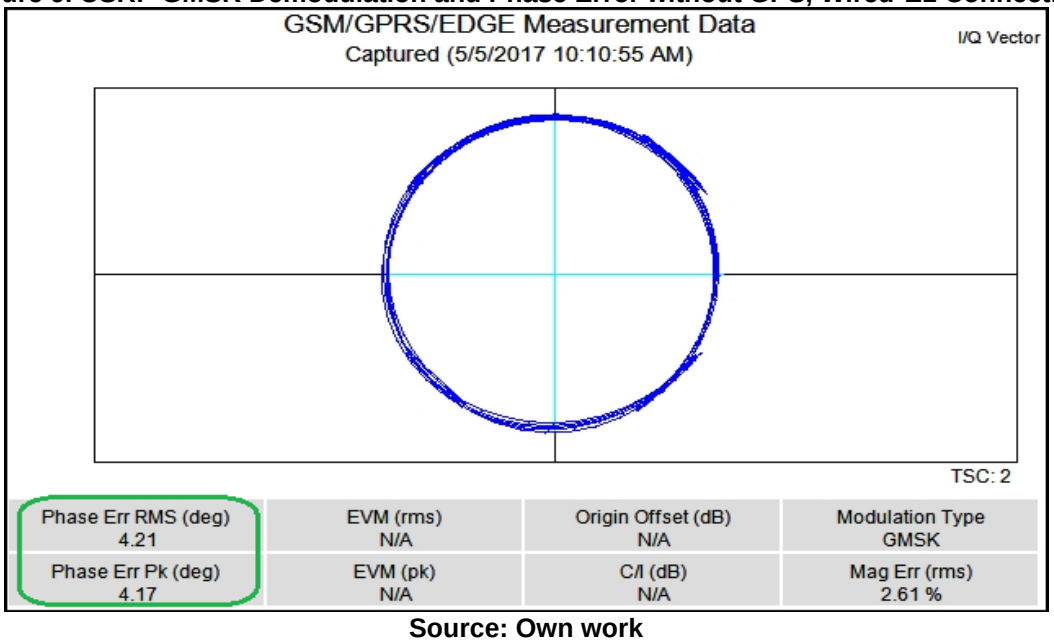
3. Results

Once the scenarios are implemented, the obtained results for the signal quality parameters of a GSM cell based on OpenBTS are presented alongside those of a GSM burst transmitted with the vector signal generator. This comparison provides insight into the modulation quality of a conventional SDR equipment with a basic clock configuration (USRP 2) compared to the signal quality generated by a high-precision instrumentation equipment. Upon completion of the measurements, the aim is to identify different behaviors of the two types of hardware and determine if these behaviors can serve as a means to identify which equipment is transmitting. The spectrum analyzer used for the measurements is equipped with the necessary firmware options to measure the GSM parameters under investigation.

3.1. GMSK Demodulation - Phase Error

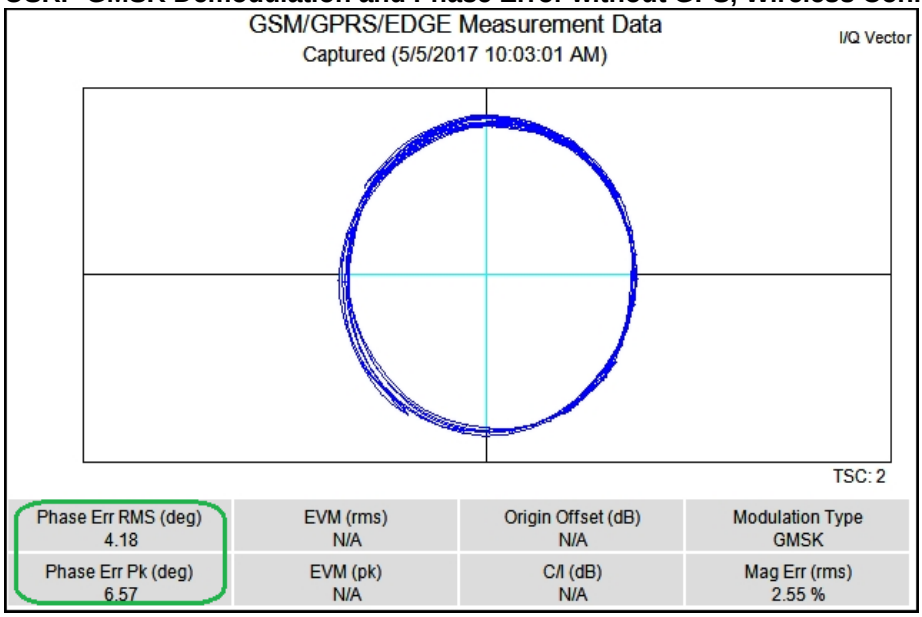
Figures 9, 10, 11, 12, and 13 depict the results provided by the spectrum analyzer for the phase error in each of the scenarios from 1 to 5 as defined in Table 1.

Figure 9. USRP GMSK Demodulation and Phase Error without GPS, Wired-E1 Connection



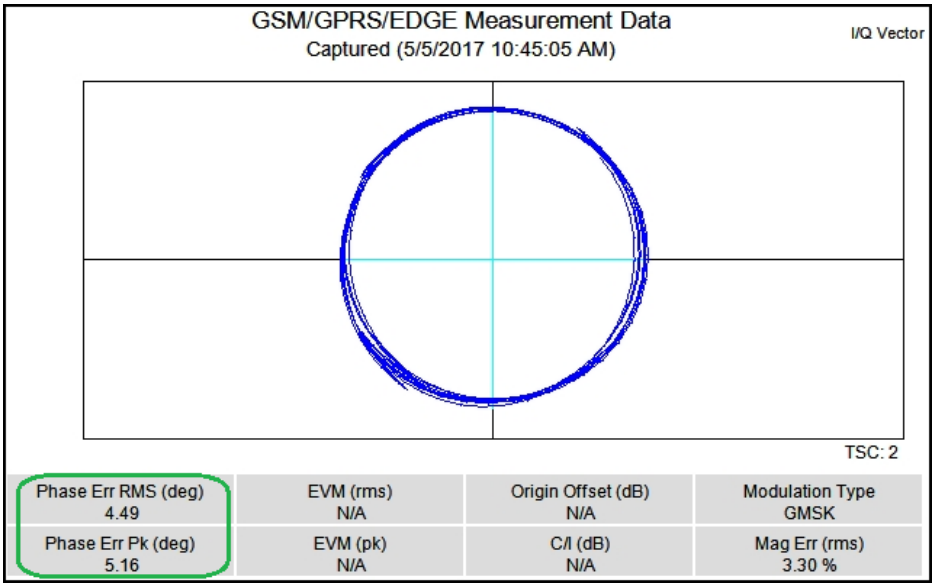
Source: Own work

Figure 10. USRP GMSK Demodulation and Phase Error without GPS, Wireless Connection-E2



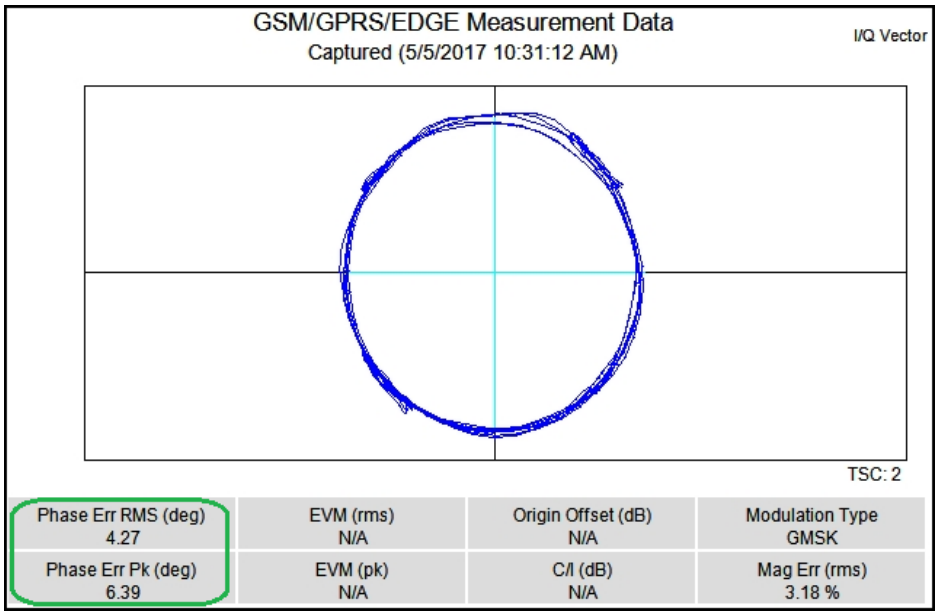
Source: Own work

Figure 11. USRP GMSK Demodulation and Phase Error with GPS, Wired Connection - E3



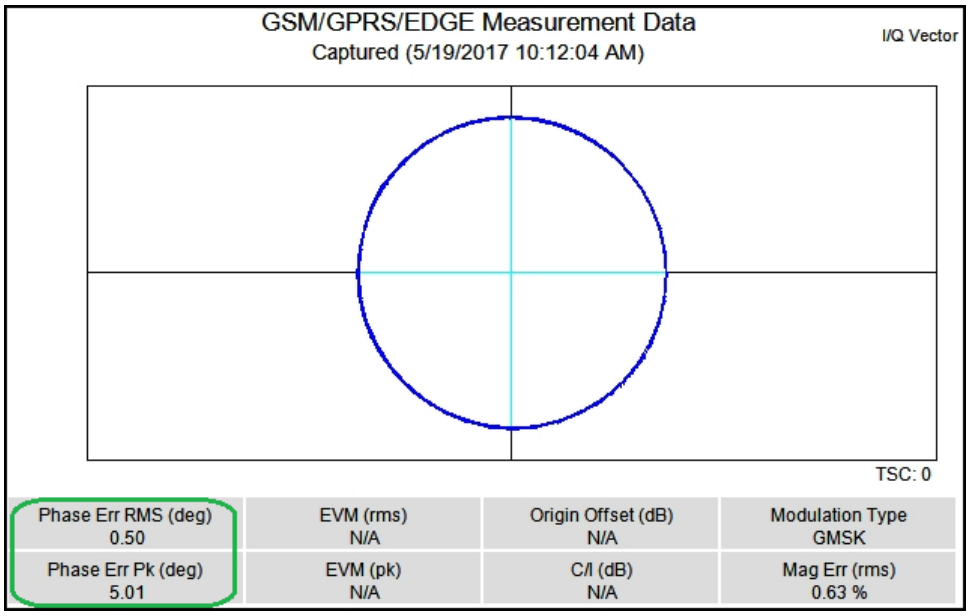
Source: Own work

Figure 12. USRP GMSK Demodulation and Phase Error with GPS, Wireless Connection E4



Source: Own work

Figure 13. Demodulation and Phase Error of GSM Burst emitted by Agilent N5172B Vector Signal Generator, Wireless Connection E5



Source: Own work

Table 2 summarizes the phase error measurements for the 5 scenarios. The lowest RMS phase error was observed in scenario 5, corresponding to the transmission of a GSM burst by the vector signal generator. All RMS phase errors were within the established operating limits for a GSM cell, which are less than 5° RMS error and less

than 20° peak phase error. The phase error is partly related to the electronic components of the GSM equipment; in the USRP and front-end used, amplifiers, filters, or other radio frequency components may influence it. On the other hand, it is observed that in the vector signal generator, the phase error was low despite both generating a GSM burst with the same characteristics, and the baseband signals were generated by software. For scenario 5, the vector signal generator is calibrated to work with minimal errors in the offered modulations; the manufacturer specifies a baseband I/Q phase resolution of 0.01°, resulting in low error during measurements. It is noteworthy that in Table 2, all scenarios exhibit errors within the permitted ranges; however, substantial differences, especially in phase error, are observed between scenarios using USRP (E1-E4) and the one employing the vector signal generator (E5).

Table 2. GMSK Phase error measurements GSM network GMSK modulation

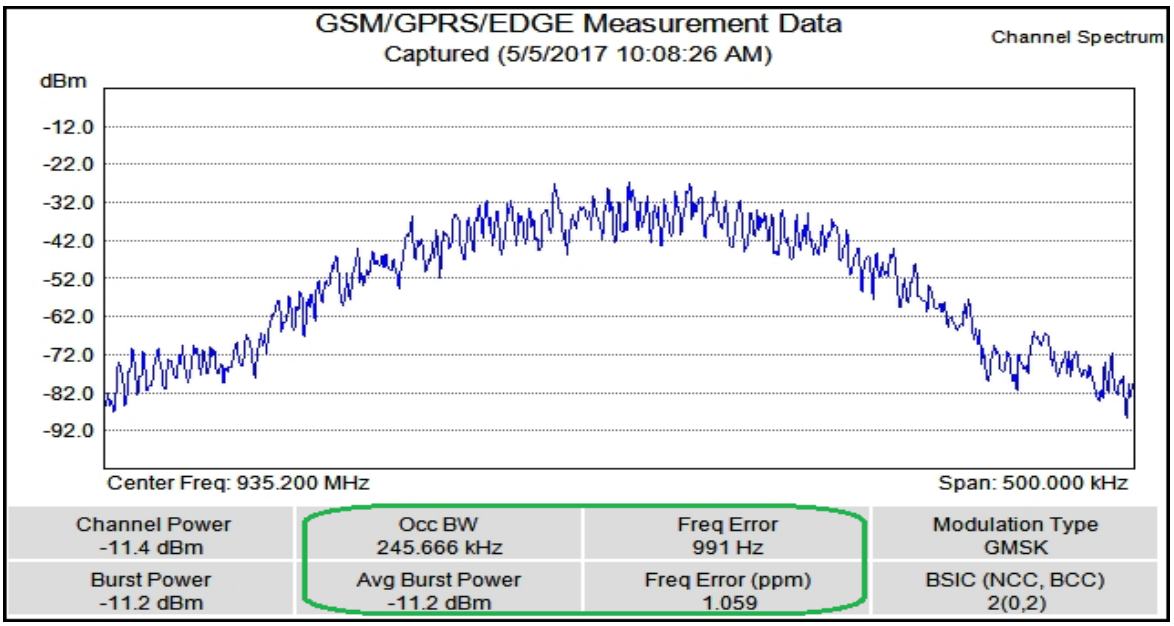
Scenario	Phase error RMS(˚)	Phase error Pk(˚)	Error range%(RMS)
E1	4,21	4,17	2,61
E2	4,18	6,57	2,55
E3	4,49	5,16	3,30
E4	4,27	6,39	3,18
E5	0,50	5,01	0,63

Source: Own work

3.2 Spectrum and Frequency Error

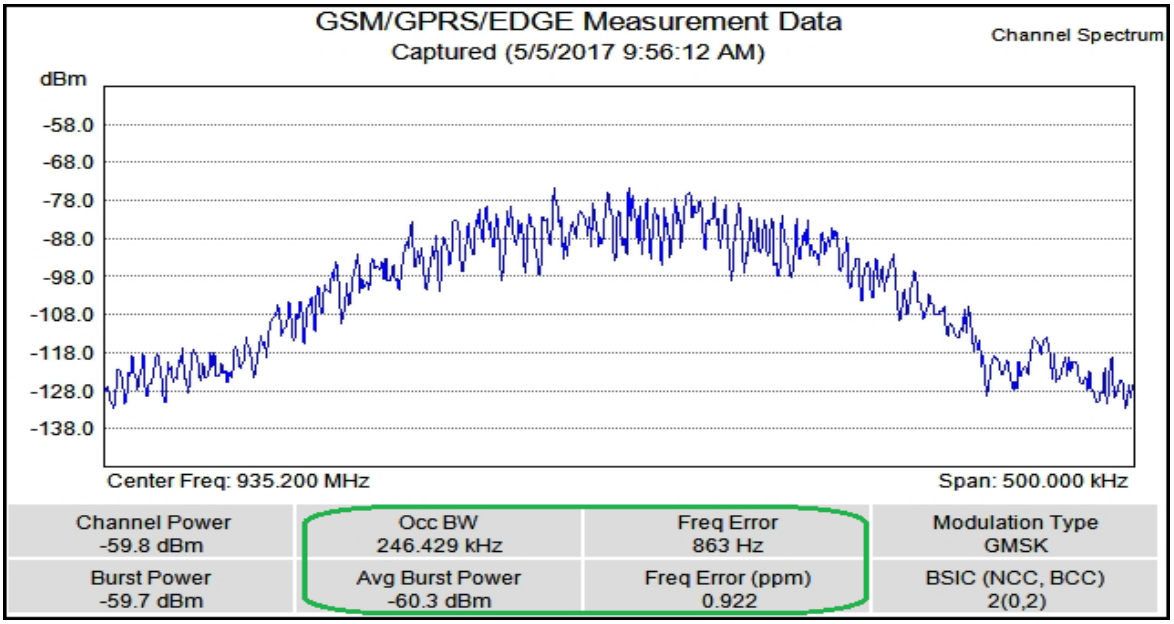
Figures 14, 15, 16, 17, and 18 depict the results provided by the spectrum analyzer for frequency error and occupied bandwidth in each of the proposed scenarios based on Table 2.

Figure 14. Frequency error measurement USRP without GPS, wired connection E1



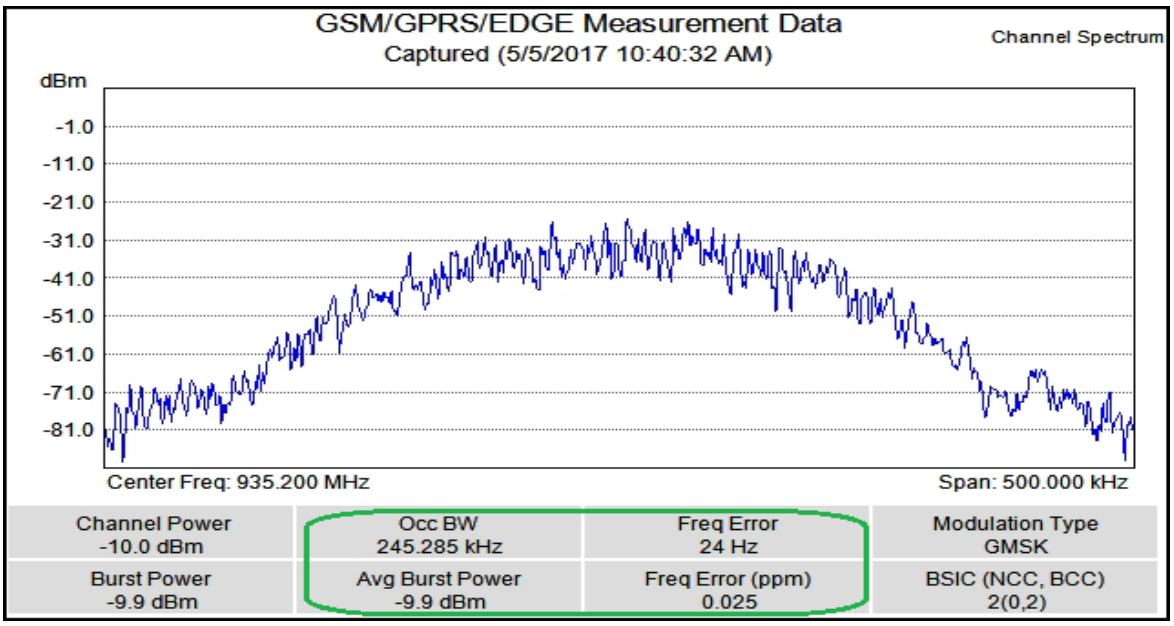
Source: Own work

Figure 15. Frequency error measurement USRP without GPS, wireless connection E-2



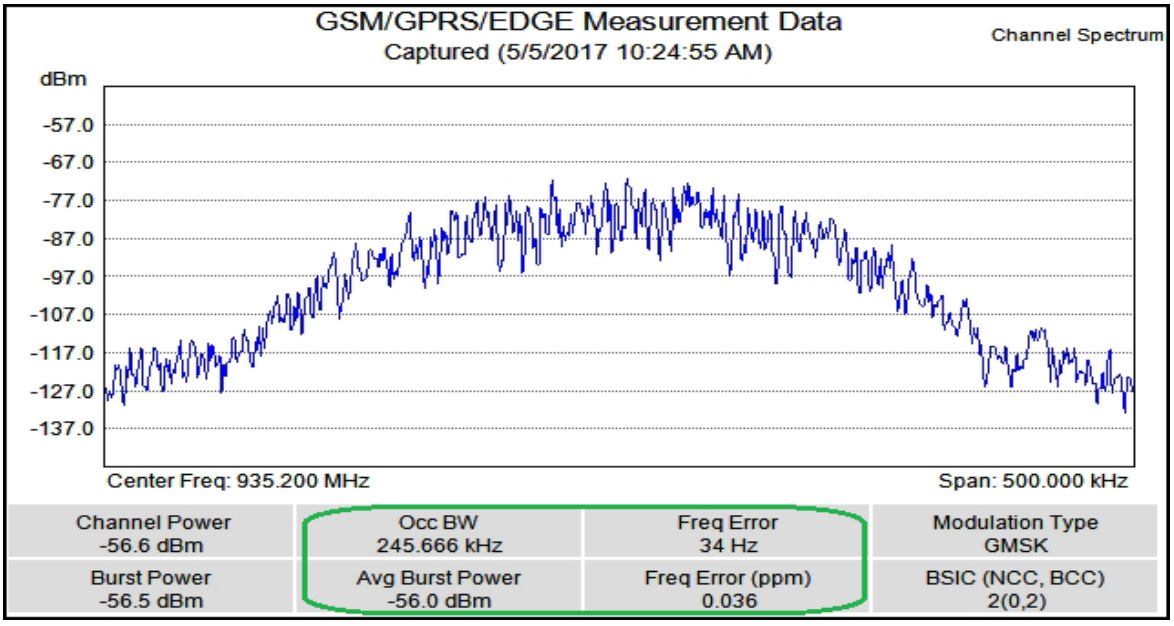
Source: Own work

Figure 16. Frequency error measurement USRP with GPS, wired connection E3



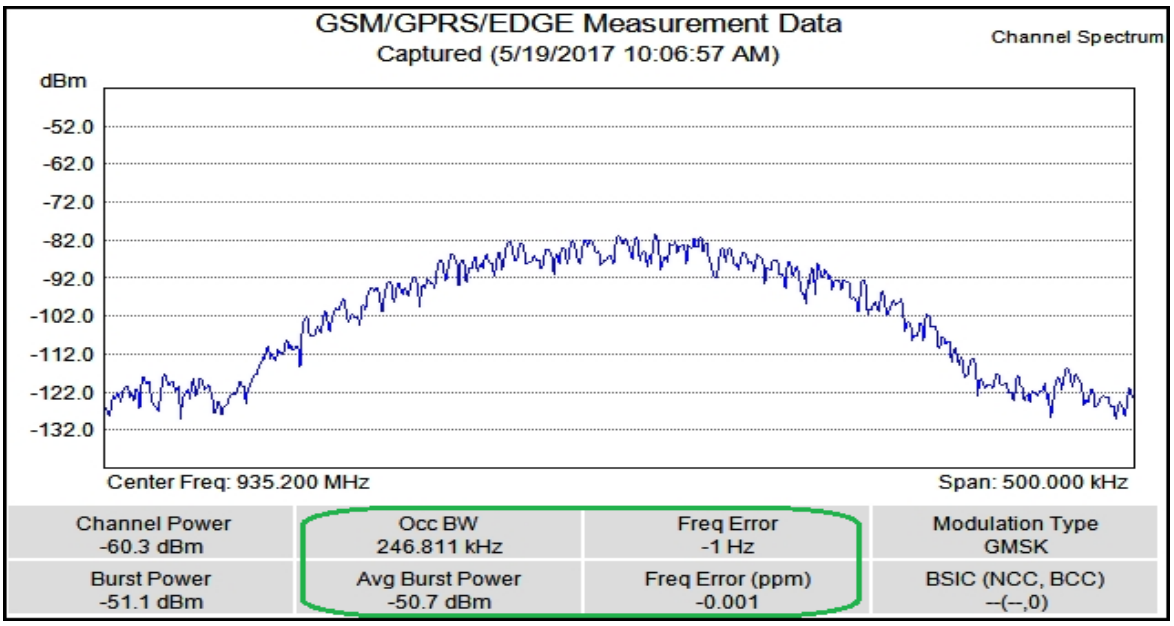
Source: Own work

Figure 17. Frequency error measurement USRP with GPS, wireless connection E4



Source: Own work

Figure 18. Frequency error measurement of GSM burst emitted by Agilent N5172B Vector Signal Generator E5



Source: Own work

Table 3 summarizes the measurements of frequency error and occupied bandwidth for the 5 proposed scenarios. The lowest frequency error was observed in scenario 5, corresponding to the generation of a GSM burst by the vector signal generator. According to the 3GPP TS 05.05 standard, the maximum allowable error is 46.76 Hz for this channel, equivalent to 0.05 ppm. With these limits, the scenarios with USRP that do not include a GPS do not meet the condition for this performance parameter. Scenario 1 exceeds the allowed error by approximately 21 times, and scenario 2 by approximately 18 times. This is based on the fact that the USRP N210 has a TCXO main oscillator with an accuracy of 2.5 ppm without GPS, and including GPS increases its accuracy to approximately 0.01 ppm. This means that for scenarios where the OpenBTS cell does have a GPS (Scenarios 3 and 4), compliance with the defined operating regulations is achieved. For scenario 5, the vector signal generator specifies an initial calibration of 40 parts per billion (ppb), which is notably reflected in the measurements. In this case, the measuring instrument does not provide frequency errors with a decimal point, so an

exact value of this parameter is not shown. Once again, the difference in the measured parameters in the scenarios with USRP and those measured on specialized equipment is evident. This confirms that these results aid in the identification of BTS impersonation using USRP.

Table 3. Frequency Error Measurements Based on USRP N210

Scenario	Frequency error (Hz)	Frequency error (ppm)	Occupied bandwidth Occ (kHz)
E1	991	1,059	245,666
E2	863	0,922	246,429
E3	24	0,025	245,285
E4	34	0,036	245,666
E5	-1	-0,001	246,881

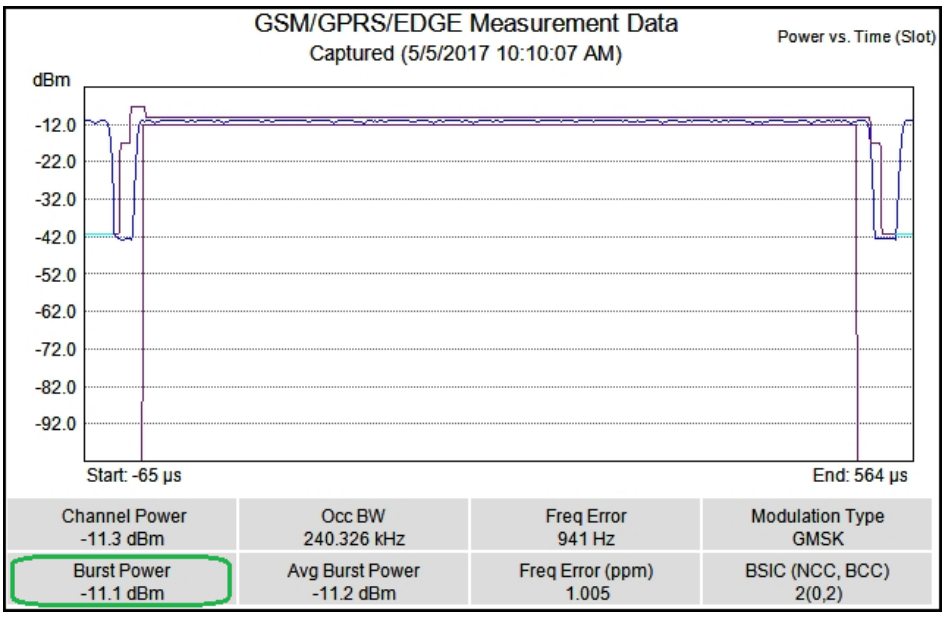
Source: Own work

Regarding the occupied channel bandwidth, it is observed that it has similar values across all measurements and aligns with the expected range for a GSM channel (approximately between 230 kHz and 280 kHz). This measurement indicates the spectrum occupied by 99% of the RF signal power.

3.3 Power vs time (Slot)

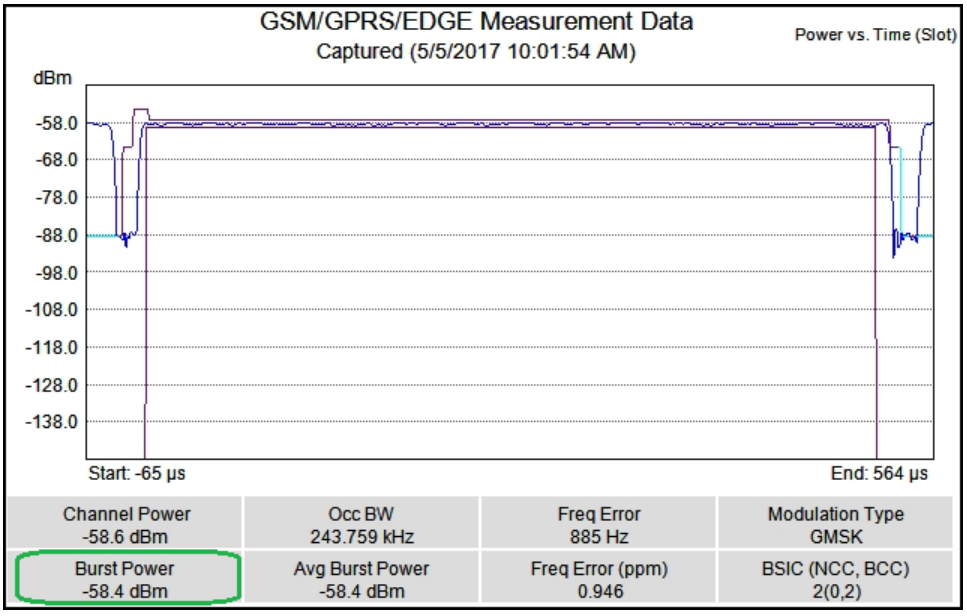
Figures 19, 20, 21, 22, and 23 show the results provided by the spectrum analyzer for the power vs. time slot measurement for the proposed scenarios.

Figure 19. Power vs. time measurement for USRP without GPS, wired E1 connection



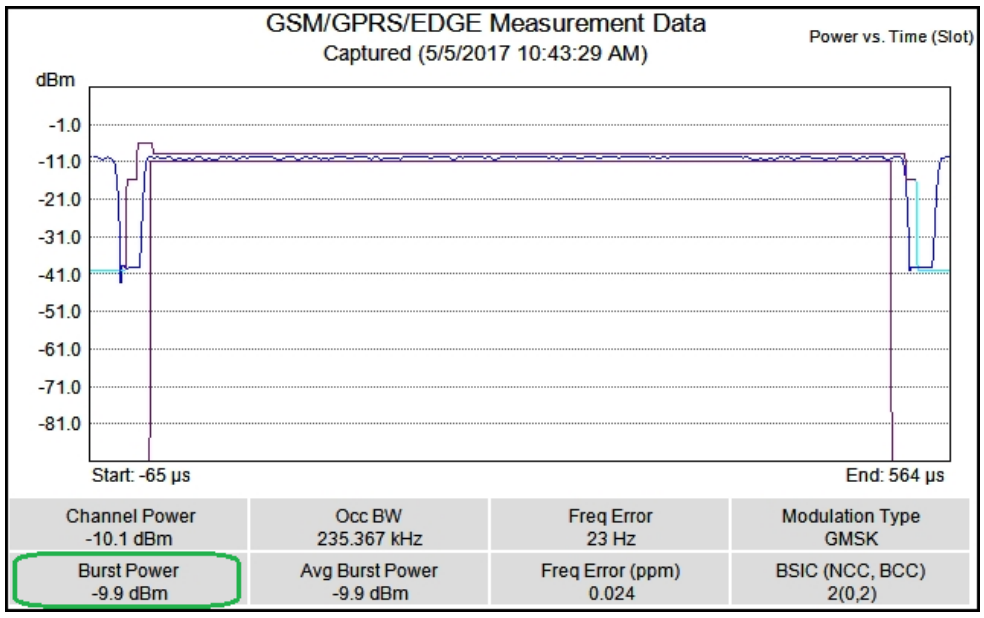
Source: Own work

Figure 20. Power vs. time measurement for USRP without GPS, wireless E2 connection.



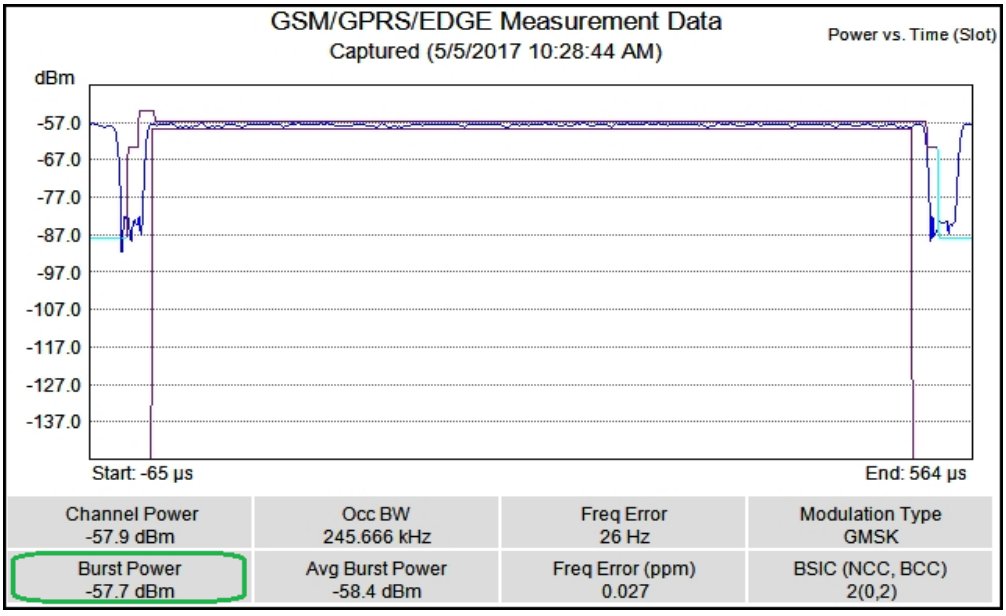
Source: Own work

Figure 21. Power vs. time measurement for USRP with GPS, wired E3 connection.



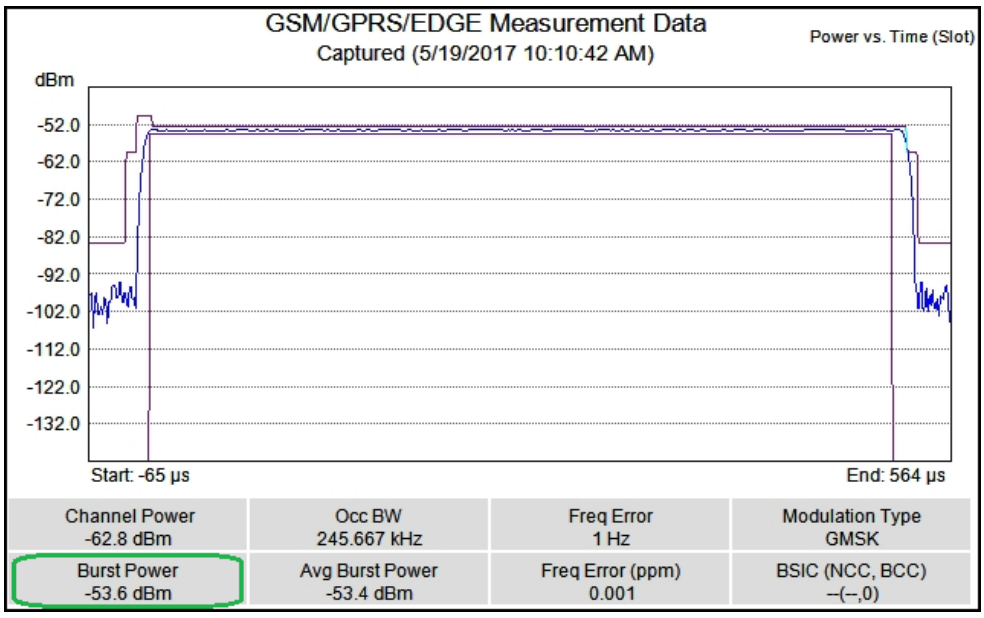
Source: Own work

Figure 22. Power vs. time measurement for USRP with GPS, wireless E4 connection



Source: Own work

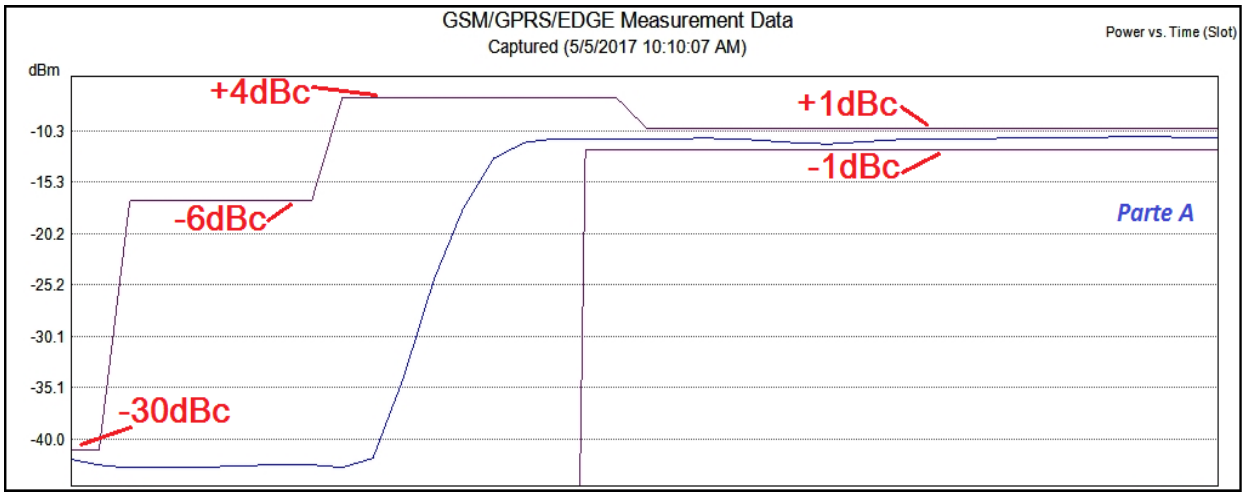
Figura 23. Power vs. time measurement for GSM burst emitted by Agilent N5172B vector signal generator E5.

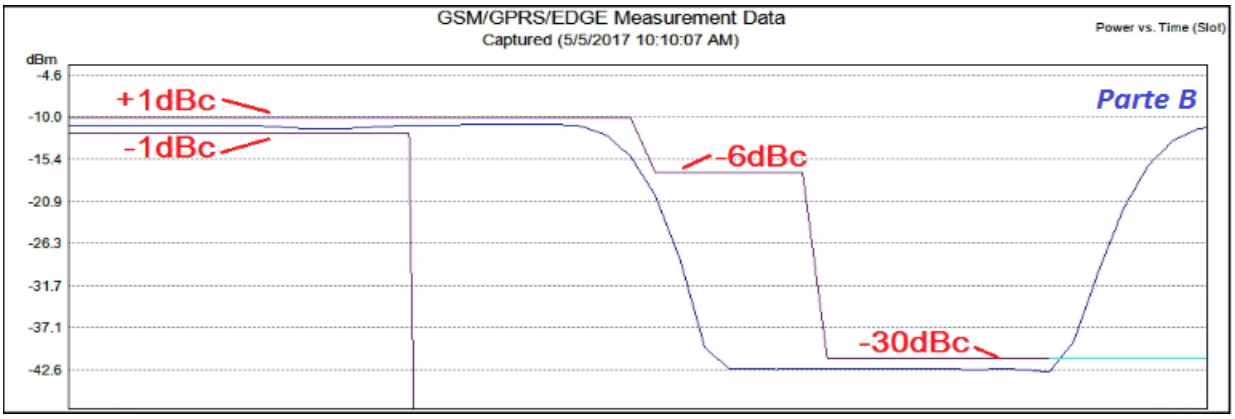


Source: Own work

The objective of the power vs. time measurement is to ensure precise timing at the rising and falling edges of the transmitted carrier and to maintain relative stability throughout the transmission of the 147 symbols. Figure 24 illustrates the rising and falling edges of a power slot over time for the OpenBTS burst. It is evident that the rate of change falls within the boundaries defined by the mask. The mask, as stipulated by the standard, encompasses a range of temporal and amplitude values to mitigate interference with adjacent slots and uphold guard periods inherent in the time-division multiple access scheme of GSM technology. The mask mandates a power level below -30dBc in the absence of symbol transmission, a maximum overshoot of +4dBc at the onset of the burst, and during symbol transmission, it must remain stable within a tolerance of ±1dBc. All scenarios comply with the mask criteria, thus affirming that the RF power amplifier of the WBX card responds promptly and consistently, as does the vector signal generator.

Figure 24. Power vs. Time Measurement of a) Rising Edge b) Falling Edge Slot





Source: Own work

In Table 4, a summary of the parameters that comply within each scenario according to the standard is shown.

Table 4. Parameters compliant according to the standard in each scenario

Scenario	Phase error RMS(˚)	Phase error Pk(˚)	Frequency Error	Occupied bandwidth	Power vs time
E1	Meets	Meets	Fails	Meets	Meets
E2	Meets	Meets	Fails	Meets	Meets
E3	Meets	Meets	Meets	Meets	Meets
E4	Meets	Meets	Meets	Meets	Meets
E5	Meets	Meets	Meets	Meets	Meets

Source: Own work

4. Conclusions

Scenarios E3, E4, and E5 comply with the parameters specified by the standard, as indicated in Table 4, which was an expected outcome. However, significant differences are observed in the numerical values provided in Tables 2 and 3 for scenarios E3 and E4 compared to scenario E5 (generator). For instance, the RMS phase error for E5 is 0.5°, whereas for the other scenarios, it consistently exceeds 4°. The same applies to the frequency error; in scenario E5, it is -1Hz, while in the other scenarios, it exceeds 20Hz. In a commercial cell, these errors are below 1° and 2Hz, respectively [33]. These results suggest that the detection of a false cell based on SDR is possible through this type of measurement. It is evident that the modulation quality of a conventional SDR device is inferior to that of a professional-grade equipment, which can be a differentiating factor in detecting potential attacks, such as man-in-the-middle attacks. At the hardware level, both the USRP and the vector signal generator use quadrature modulation in the RF front-end, and much of the signal processing is performed by software in baseband. In this regard, the architectures employed are similar, and it can be concluded that an SDR system may respond better depending on the components used in its construction. However, one of the attractions of using SDR technology is its low cost, and therefore, lower precision components are commonly used. In this sense, the performance of purpose-built hardware will be superior.

The deterioration of oscillation, amplification, and filtering circuit components over time of use may cause BTS stations to operate outside the ranges established by standards. This is not an exception in systems implemented on SDR. An increase in frequency error and phase error can affect cell coverage. Therefore, the results of this research serve as a reference for the operating ranges of OpenBTS implemented on USRP for attack detection, etc.

Regarding power vs. time measurement, future work proposes the classification of commercial cells and SDR cells using intelligent algorithms based on the behavior of this parameter. This proposal is made due to the observed behavior in Figures 22 and 23 for the two different types of hardware. On the other hand, the use of high-quality instrumentation for the generation and measurement of signals from different wireless technologies is very useful for determining the proper operation of these technologies on software-defined radio platforms, as well as for verifying compliance with standards or regulations related to such technologies.

Acknowledgment

Acknowledgments This work was funded by Universidad Militar Nueva Granada and developed by the GISSIC research group associated with the research project ING-INV 2388.

References

[1] 5gamericas, “5gamericas: Statistics - Latin America.” [Online]. Available: http://www.5gamericas.org/en/resources/statistics/statistics-latin-america/.

[2] A. Navarro Cadavid, A. Arteaga, L. Vargas, J. Renteria, and M. Arciniegas, “Spectrum Monitoring System and Benchmarking of Mobile Networks Using Open Software Radios SIMONES,” IEEE Lat. Am. Trans., vol. 13, no. 11, pp. 3592–3597, 2015.

[3] M. Iedema and H. Samra, Getting Started with OpenBTS. 2015.

[4] A. Dubey, D. Vohra, K. Vachhani, and A. Rao, “Demonstration of vulnerabilities in GSM security with USRP B200 and open-source penetration tools,” in Proceedings - Asia-Pacific Conference on Communications, APCC 2016, 2016, pp. 496–501.

[5] B. Harmat et al., “The Security Implications of IMSI Catchers,” in International Conference on Security and Management (SAM’15), 2015, pp. 57–62.

[6] Mesud Hadžialić; Mirko Škrbić; Kemal Huseinović; Irvin Kočan; Jasmin Mušović, “An Approach to Analyze Security of GSM Network,” 22nd Telecommun. forum TELFOR 2014, 2014.

[7] S. Ghafoor, K. N. Brown, and C. J. Sreenan, “Experimental evaluation of a software defined radio-based prototype for a disaster response cellular network,” in Proceedings of the 2015 2nd International Conference on Information and Communication Technologies for Disaster Management, ICT-DM 2015, 2016, pp. 57–63.

[8] K. Guevara, M. Rodriguez, N. Gallo, G. Velasco, K. Vasudeva, and I. Guvenc, “UAV-based GSM network for public safety communications,” in Conference Proceedings - IEEE SOUTHEASTCON, 2015, vol. 2015-June, no. June.

[9] T. Di. Putri and T. Juhana, “Mobile-openbts implementation of natural disaster victims search,” in Proceedings - ICWT 2017: 3rd International Conference on Wireless and Telematics 2017, 2018, vol. 2017-July, pp. 149–154.

[10] J. Mpala and G. Van Stam, “Open BTS, a GSM experiment in rural Zambia,” Africomm, Yaounde, Cameroon, pp. 1–9, 2012.

[11] M. Zheleva, A. Paul, D. L. Johnson, and E. Belding, “Kwiizya: Local Cellular Network Services in Remote Areas,” in MobiSys, 2013, July, p. 417.

[12] L. Angrisani, P. Daponte, and M. D'Apuzzo, “A measurement method based on time-frequency representations for testing GSM equipment,” IEEE Trans. Instrum. Meas., vol. 49, no. 5, pp. 1050–1056, 2000.

[13] A. Aiello and D. Grimaldi, “Frequency error measurement in GMSK signals in a multipath propagation environment,” IEEE Trans. Instrum. Meas., vol. 52, no. 3, pp. 938–945, 2003.

[14] E. P. G. Pinto, J. D. A. Monroy, and J. C. M. Quintero, “Analyzing OpenBTS Performance as a viable network solution for IoT devices,” Ingeniare, vol. 31, pp. 1–11, 2023.

[15] F.H. Partiansyah, S. Kusmaryanto, R. Ambarwati, and S.H. Pramono, “Experimental Study of USRP N210 as Simple GSM OpenBTS 5.0 for Remote Areas,” 2022 11th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS), Malang, Indonesia, pp. 185-190, 2022.

[16] K. Paul, “Introduction to GSM and GSM mobile RF transceiver derivation.

[17] Union Internacional de Telecomunicaciones., “Definiciones de sistema radioeléctrico determinado por programas informáticos (RDI) y sistema radioeléctrico cognoscitivo (SRC),” vol. 2152, 2009.

[18] T. ETSI Specification, “Digital cellular telecomm mmunications system (Phase e 2+) (GSM); GSM/EDGE Multiplexing and multiple access on the radio path (3GPP TS 45.0.002 version 13.3.1 Release 13)”.

[19] J. M. HUIDOBRO, Comunicaciones móviles: sistemas GSM, UMTS Y LTE, 2012th ed.

[20] ETSI, Digital cellular telecommunications system (Phase 2+); Release independent frequency bands; Implementation guidelines (3GPP TS 05.14 version 7.2.0 Release 1998), vol. 0. 2001, pp. 0–31.

[21] ETSI, Digital cellular telecommunications system (Phase 2+); Radio transmission and reception (3GPP TS 45.005 version 12.4.0 Release 12), vol. 0. 2008, pp. 0–40.

[22] T. Specification, “ETSI TS 145 002,” vol. 0, pp. 0–112, 2014.

[23] T. ETSI Specification, Technical Specification Group GSM/EDGE Radio Access Network; Digital cellular telecommunications system (Phase 2+); Modulation TS 05.04, vol. 0. 2003, pp. 1–28.

[24] 3GPP, 3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Digital cellular telecommunications system (Phase 2+); Radio subsystem synchronization. 1999.

[25] ETSI, Digital cellular telecommunications system (Phase 2 and Phase 2+); Base Station System (BSS) equipment specification; Radio aspects (3GPP TS 11.21 version 8.6.0 Release 1999), vol. 0. 2008, pp. 0–40.

[26] ETSI, EN 300 910 Digital cellular telecommunications system (Phase 2+); Radio transmission and reception (GSM 05.05 version 8.5.1 Release 1999), vol. 1. 1999, pp. 1–10.

[27] Keysight Technologies, “Understanding GSM/EDGE Transmitter and Receiver Measurements for Base Transceiver Stations and their Components.”

[28] E. No. O. . U. S. A. Gbadamosi A. M. Aibinu, “Towards Independent Measurement of End to End Bit Error Rate in GSM Network,” pp. 1–4, 2014.

[29] R. Communications, “Laboratory works in Radio Communications GSM Transceiver Measurements.” Prentice-Hall Inc, 1995.

[30] T. ETSI Specification, 3GPP TS 05.05 3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Radio transmission and reception, vol. 0. 2005.

[31] E. Research, “USRP Hardware Driver and USRP Manual Version: 003.010.001.001-41-g6abf277.” [Online]. Available: http://openbts.org/hardware/.

[32] R. Networks, C. C. Attribution-sharealike, and U. License, “OpenBTS Application Suite,” 2014

[33] Agilent Technologies, “Making the Phase and Frequency Error Measurement.” [Online]. Available: http://literature.cdn.keysight.com/litweb/pdf/ads2001/vsaedgemeas/gsmmeas6.html.