Implementation of a 4G/5G Base Station Using the srsRAN Software and the USRP Software Radio Module

Wojciech Flakowski, Maciej Krasicki, and Rafał Krenz

Poznan University of Technology, Poznan, Poland

https://doi.org/10.26636/jtit.2023.3.1298

Abstract — This article presents the potential applications and scenarios for the implementation of a software-defined radio (SDR) module operating as a base station in 4G/5G networks. The paper presents test configurations of the srsRAN software environment in conjunction with various types of programmable radio modules. Then, the key performance metrics of the mobile telephony system and potential problems that may be encountered while implementing hardware and software layers are presented.

Keywords* — *base station, radio access network, radio channel power, radio link throughput, software-defined radio, user equipment

1. Introduction

This article presents the implementation of a cellular base station using SDR programmable radio. Such a concept allows for a significant development and improvement of radio applications. This requires smooth and quick changes in the operating parameters of the radio module to adapt to the current application scenario. This is possible thanks to the use of an FPGA-based system which enables the operating parameters to be reconfigured quickly.

An important role in ensuring the versatility of the SDR module is played by the transfer of some of the data processing and signal processing to the software domain. Such an approach results in a significant scalability of signal processing algorithms. SDR radio modules may be successfully used to implement the radio access layer for 2G, 3G, 4G and 5G digital cellular networks. In such a case, the signal is processed and the parameters of the carrier are controlled in the digital domain, with the aid of a computer. Having been processed in the software layer, the signal samples are sent to the SDR module. Using built-in FPGA and analog components of the RF path (i.e., amplifiers, filters and oscillators), the carrier is generated for the downlink and tracked in the uplink. The software-defined structure of the programmable radio and the extensive configuration possibilities enable the base station to quickly adapt to the specific type and standard of the wireless transmission supported by the user's mobile terminal.

The increasing computational power of standard PCs and the wide availability of programmable radio modules have resulted in the design and development of software working as a complete base station. The srsRAN package is one of the most popular open-source projects of this type. It offers the ability to emulate a base station using a PC and a programmable radio. The modular structure of the software package enables separate emulation of the core part of the network and the radio access layer (Radio Access Network, RAN), as well as the client part (User Equipment, UE). Thanks to such an approach, it is possible to observe the parameters of the data transferred between the individual modules.

In recent years, implementation work has been in progress to verify the operation of emulated base stations and UE for cellular systems. However, the propagation conditions of the complete radio path using commercial terminals have not been evaluated.

In [1], the authors tested an srsRAN system using USRP and LimeSDR modules. The measurements of the radio modules' transmit power were carried out using wires connecting the transmitter and the receiver. This allowed the absolute power values of the generated RF signal to be measured, but it did not take into account free-space losses and radio wave propagation mechanisms. On the other hand, there were also some implementations of software radio systems working in earlier RAN generations. As an example, a GSM system developed with the use of the OpenBTS software package and the USRP N210 radio module was described in [2]. The said paper provided an overview of the modular software configuration of the system, but failed to describe either 4G or 5G RAN.

The system described in this paper is used to test the open-source software of the srsRAN radio package and to measure its performance. Link capacity tests and power measurements are carried out in real world conditions. Such an approach allows to simulate and validate the system model in various radio environments. Therefore, it is possible to improve the transmission and receiving parameters. According to the authors' best knowledge, this is the first hardware implementation using a commercial UE and USRP radio module.

The paper is structured as follows. Section 2 presents the software components of the srsRAN package, as well as describes their functionality and operating characteristics. Next, in Section 3, the capabilities of the SDR programmable radio module and its cooperation with the software layer are described. Section 4 is a detailed description of the system's implementation, its features and functionalities. It shows the detailed parameters of the computers responsible for emulating base station functions. In Section 5, the process of configuring, starting up and connecting the system is described. That part contains the settings of individual software modules, the SDR module and network functions. Such presets are necessary to establish a connection between mobile terminals. Then, in Section 6, radio link throughput measurements are presented, taking into account various configurations of the radio module, terminal location and transmission status. Similarly, high-frequency power measurements are carried out in an operational system, in the downlink and uplink channels, in Section 7. Additional experiments are conducted in Section 8, with some remarks regarding the stability of the system's operation under specific radio conditions and with different base station settings added.

2. Characteristics of the Software Layer

2.1. Overview of Software Layer Modules

In the application scenarios under consideration, the base station system is implemented using open source srsRAN software [3]. The srsRAN software package is characterized by a modular structure and is a complete solution that is required to run the base station and emulate user equipment (UE) on a PC computer. It also includes a communication layer with an SDR controller, making it a universal tool to run 4G and 5G networks.

The basic modules of the srsRAN package include: srsEPC, srsENB, and srsUE modules.

2.2. srsEPC Module

The srsEPC module emulates the core network for the 4G solution. It consists of four basic components performing strictly defined tasks. The first one is the mobility management entity (MME) subsystem. It is the main control element of the 4G core network, managing mobility and the connection of a mobile terminal to the network. It is also responsible for exchanging mobile terminal authentication data with the home subscriber server (HSS) database. The srsEPC module also connects (through the S1-AP interface) with the srsENB module that is responsible for the radio access layer. The MME sends information via the radio resource control (RRC) protocol to activate the terminal's idle or active mode.

The HSS database is the second component closely cooperating with the MME subsystem. In the srsRAN environment, it is implemented using the *user_db.csv* file which contains the authentication data of SIM cards installed in mobile terminals. It should be noted that the identification of terminals is done by authorizing the international mobile subscriber identity (IMSI) number which enables network services to be launched on any terminal with a registered SIM card. The MME main control unit is connected to the HSS register subsystem via a virtualized S6a interface.

The third important component of the srsEPC module is the service gateway (S-GW) subsystem which is responsible for routing packets between the UE and the external P-GW network gateway. It sets up GPRS tunneling protocol (GTP) sessions between the srsENB module and the P-GW gateway subsystem. It is also responsible for assigning IP addresses to mobile terminals communicating with the base station and is connected directly to the srsENB module through the virtualized S1-U interface.

The fourth subsystem included in the srsEPC module is the packet data network gateway (P-GW) which redirects network traffic between the S-GW subsystem and the external Internet network. The Internet connection is physically provided by connecting a PC network card to a LAN network via the Ethernet port. The P-GW subsystem does not have a direct connection with the srsENB module, but it connects to the S-GW unit through virtualized S5 and S8 interfaces. The S-GW unit is connected to the MME unit through the S11 interface.

2.3. srsENB Module

The srsENB module performs the function of the base station: eNodeB in the 4G network and gNodeB in the 5G network, respectively. In the test configuration, the srsENB module shares a computing unit with the srsEPC module. It is also possible to run the srsENB and srsEPC modules on separate PCs. When both modules work on a single PC unit, communication takes place via the IP address of the local loopback system interface. The srsENB program supports the LTE/4G mode in the 1.4, 3, 5, 10, 15 and 20 MHz bands, providing a wide range of configuration options for the available channels.

It is possible to connect the srsENB module to an external 5G core network module in order to implement a 5G SA (standalone) network in a scenario in which the srsEPC module is not used. The third available operating mode of the srsENB enables a 5G NSA non-standalone connection. This mode allows to set up two radio channels using 4G and 5G technology. In that case, the UE establishes a connection with the 4G channel to exchange authorization and control data. Simultaneously, it establishes an additional connection using the 5G carrier in order to implement a broadband channel dedicated to the user's data traffic. The srsEPC module is still responsible for managing data transmissions with the external network. In the case of a 5G NSA connection, the srsENB module creates two virtual base stations (eNodeB and gNodeB), but the data within the core network is exchanged between the subsystems of the eNodeB station only (via S1 interfaces). In addition, communication between the eNodeB and gNodeB subsystems is established via the X2 interface inside the srsENB module, so the gNodeB subsystem does not have a direct connection to the srsEPC module.

In the case of the 5G SA operating mode, where the srsENB module activates the gNodeB subsystem only, the connection established via N2 and N3 interfaces requires an independent software module that performs the functions of the 5G core network. The N2 interface is then used to transmit information from the srsENB to the access and mobility management function (AMF) subsystem of the 5G core network. The AMF is responsible for management, access control and authorization of a terminal connecting to the 5G network. The N3 interface is used to connect srsENB to the user plane function (UPF) subsystem which is responsible for routing data packets between the UE and the external Internet network.

In addition to the basic single-input single-output (SISO) transmission mode (mode 1), three 2 × 2 multiple-input multiple-output (MIMO) modes are supported by the srsENB and selected SDR modules. Mode 2 is the broadcast diversity mode, where replicas of the signal are transmitted through all antennas using individual frequency resources and coding schemes. This mode of operation boosts the signal-to-noise ratio (SNR) and also makes the transmission more resilient to channel interference. Mode 3 is based on open-loop spatial multiplexing and cyclic prefix delay diversity. This means that each of the ports transmits the subcarriers using a different cyclic prefix delay. This solution increases resistance to interference in channels exhibiting a high degree of variability. The last of the implemented transmission modes is the spatial multiplexing mode using a closed feedback loop (mode 4). In this mode, each antenna transmits a separate data stream used to increase the radio connection's total bit rate.

In order to perform the correct channel estimation on the mobile terminal side, the base station transmits reference signals (RS) in specific resource blocks and time slots. Those reference signals are used to reduce the error rate in the transmission between eNodeB and the UE. It is worth noting that the terminal sends channel quality reports, including the selection of the appropriate precoding matrix. The precoding matrices are selected using their associated codebook indexes – precoding matrix indicators (PMIs) for each antenna.

The srsENB software works in the frequency domain division (FDD) mode, where the downlink channel and the uplink channel transmit on separate frequencies with a defined channel spacing (this is made possible by specifying the EARFCN parameter).

2.4. srsUE Module

The srsUE module is an independent software package that may be run on a separate PC computer together with the software radio module (SDR). SDR is responsible for communicating, via the physical layer, with the base station. The srsUE software also supports authentication by emulating a virtual SIM card whose parameters are defined in a file known as *ue.conf* (soft USIM). However, it is possible to use a hardware SIM card reader connected to the PC. In the test scenario, a virtual USIM card is used.

The srsUE module performs all UE functions. It supports both 4G and 5G in NSA and SA modes. This module cooperates directly with the SDR hardware module, as such an approach offers great configurability along with easy software setup of the available bands and frequency resources. It is possible to rely on frequency division duplex (FDD) or time division duplex (TDD) techniques. In addition, all MIMO transmission modes listed above and all available radio channel widths of the LTE standard (1.4, 3, 5, 10, 15 and 20 MHz) are supported.

2.5. Radio Controller Command Interpreter

It is important that both srsUE and srsENB modules have a built-in interpreter of radio controller commands, as this allows to define the operating parameters of the radio module based on respective configuration files: *ue.conf* (for the srsUE module) and *enb.conf* (for the srsENB module).

3. Hardware Layer Characteristics

3.1. Internal Structure of the Radio Module

The scalability of the solution based on virtualized cellular networks is additionally enhanced by the support of various types of radio modules available on the market. srsRAN software may communicate with them using hardware drivers which manage the operation of specific radio modules. The programmable radio controller works as an interface between the antenna and the L1 (physical or PHY) layer. It contains RF front-end as well as analog-to-digital (ADC) and digital-to-analog (DAC) converters. The srsENB software emulates the entire protocol stack of L1, L2 (MAC, RLC, PDCP) and L3 (S1-AP, RRC, GTP-U) layers. It initiates communication with the programmable radio controller and processes signal samples in the digital domain. The tested hardware platform uses various types of programmable radios from the USRP Ettus Research family, but it is possible to use stations with other types of radio modules, such as BladeRF and LimeSDR. In the case of the USRP radio modules, the UHD hardware driver is used. USRP 1, USRP B210, USRP N200/N210 and USRP E320 modules are employed for the tests, assuming a wide range of carrier frequencies (from 70 MHz to 6 GHz in the case of USRP B210 and E320).

The SDR modules can be divided into two main categories, namely those responsible for the individual stages of processing received and transmitted signals. The first component is the motherboard. It is tasked with processing the signal in the baseband and the intermediate frequency (IF) band. Meanwhile, in the daughterboard, the target radio frequency (RF) carrier is generated by local oscillators and the mixers multiply the IF signal with the carrier. Such a structure is present in the USRP N200/N210 and USRP 1 radio modules, where it is possible to physically replace the daughterboard with a model operating in a different band. All components of USRP B210 and USRP E320 modules are integrated on a single PCB and cannot be reconfigured.

3.2. Radio Front-end Tuning Process

The programmable radio tuning process is divided into two stages. Coarse tuning is performed by specifying the frequency of the local oscillator. Such an approach enables the carrier frequency to be tuned in the full range offered by a given module. Fine tuning is realized in the digital domain and consists in FPGA programming. By default, the signal in the digital domain is sampled with a frequency of the main system clock. This limits the maximum tuning range in the digital domain to the master clock rate. The maximum signal bandwidth is also restricted by the main system clock. Fine tuning of the carrier frequency can be done by shifting the frequency in the digital domain within the tuning range (*lo_offset*), so that the center frequency (which is the frequency of the local oscillator) determines a central point in the tuning range. It must be pointed out that the maximum frequency of the TX radio channel should not exceed the limit defined by the maximum tuning range, since it may cause signal leakage and aliasing. In the case of radio modules equipped with an anti-aliasing filter, if the permissible tuning range is exceeded, the center frequency will be shifted and wrapped to the lowest allowable frequency. For example, if the maximum allowable tuning frequency is contained in the tuning range of 180 – 200 MHz and a 15 MHz digital frequency shift is added to the oscillator (190 MHz), the tuning range is increased to the value of 205 MHz. When the anti-aliasing filter is activated, the final carrier frequency will be moved to the value of 185 MHz.

3.3. Principles of Channel Mapping in Radio Module

In the case of radio modules using a distributed hardware structure (separate motherboard and daughterboard), the channel mapping rule is defined by the input parameters of the UHD driver. Channel mapping parameters are specified in the *enb.conf* file in the *device_argsfield* using the *rx_subdev_spec* formula for RX channels and the *tx_subdev_spec* formula for TX channels. A general channel mapping scheme is A:0 B:0, where variables A and B specify the daughterboards (corresponding to the slots on the motherboard), while 0 identifies the antenna port of the daughterboard. Note that the daughterboard may have two antenna ports (indexed as 0 or 1). The direction of subsequent ports is specified by individual variables: *tx_subdeb_spec* (group of TX ports) and *rx_subdev_spec* (group of RX ports). In the case of a radio module that can accommodate two daughterboards, the channel mapping configuration is the following: *tx_subdev_spec*=A:0 B:0, *rx_subdev_spec*=A:0 B:0. It enables TX port 0 and RX port 0 on both (A and B) daughterboards.

Such a configuration is possible only for the USRP 1 module which enables installation of two daughterboards. The N210 module has only one slot for an external daughterboard, so it is possible to configure the channels of one daughterboard only – A:*x* A:*y* where *x*, *y* are the daughterboard's port numbers. In the case of modules where the RF front-end and the ADC and DAC converters are integrated (B210 and E320 models), there is a different, specific type of channel mapping. In the case of the B210 model, which has two TX ports and two RX ports, the channel mapping scheme is the following – A:A A:B. In this case, they are virtually connected to one motherboard. In the E320 model, the channel mapping scheme is A:0 A:1, i.e., there are also two channels (2 TX ports and 2 RX ports).

3.4. Configuration of Internal Oscillators

The internal configuration of local oscillators is an additional aspect that affects the individual programmable radio models. In the case of the USRP B210 and E320 radio modules, two local oscillators are available sharing their carrier frequencies between the TX and RX ports. This means that basic tuning of individual TX and RX channels cannot be performed separately. Instead, one can set a common carrier frequency for all TX channels and a common frequency for all RX channels. As a consequence, the USRP B210 and E320 modules support only the 2 × 2 MIMO transmission mode. This prohibits the use of the 5G NSA mode using separate frequency bands in the FDD mode, e.g., 1800 MHz band for the 5G broadband channel and 2600 MHz band for the 4G control data channel. The manner in which channels are mapped by the srsENB program is an additional implementation problem. In the case of the USRP B210 radio, it is not possible to use the RF B port to generate a separate, independent carrier due to the unusual specificity of the channel mapping scheme – A:A A:B. As a result, the B210 radio cannot be used to set up a 5G network in the NSA mode. However, it is still possible to use the 2 × 2 MIMO mode for a single 4G network cell.

3.5. Multiple Radio Modules Configuration Problem

It is not possible to use two B210 or E320 modules to generate two independent carriers, because these models are not supported by the *multi_usrp* function which enables physical binding of more USRP modules into one virtual device. However, this is possible with the use of USRP N210 modules. The UHD driver is responsible for the process of combining individual modules into one logical device.

It should be mentioned that the USRP N200/N210 module is not supported by the srsENB program due to the conflict in providing the information necessary to initialize the UHD driver. For proper operation, the USRP N210 module requires specifying the reference time source, defined by the *time_source* argument. In the latest revision of the srsRAN suite, this function is not supported by the srsENB software. The *time_source* parameter cannot be defined manually in the *enb.conf* configuration file and the UHD driver does not initialize correctly in that case.

3.6. System Bandwidth Requirements

The width of the radio channel is an important implementation aspect as well. When the srsENB software module operates in the 5G NSA network mode, it is possible to set up two 10 MHz channels: a 10 MHz channel for the 4G standard carrier and a 10 MHz channel for the 5G NSA standard carrier. Such a configuration requires a total processing bandwidth of 20 MHz. Although the USRP 1 radio module meets the requirements of channel mapping through the srsENB application, it does not have the ability to process the total signal bandwidth. In fact, the available total bandwidth with 8-bit sampling is 16 MHz – the value is too low for 5G NSA mode transmissions.

3.7. Digital Frontend Tuning Procedure

Despite the inability to separate the carrier frequencies for individual frequency bands in the case of the USRP E320

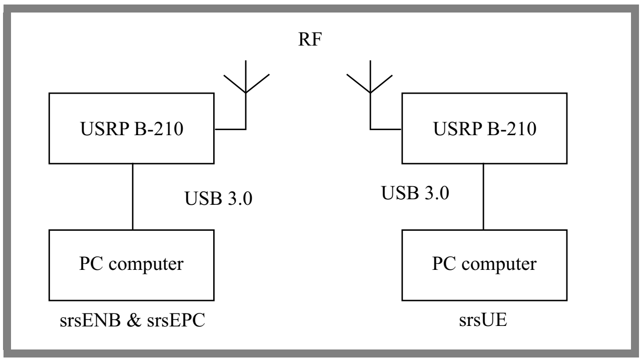


Fig. 1. eNodeB and srsUE system configuration.

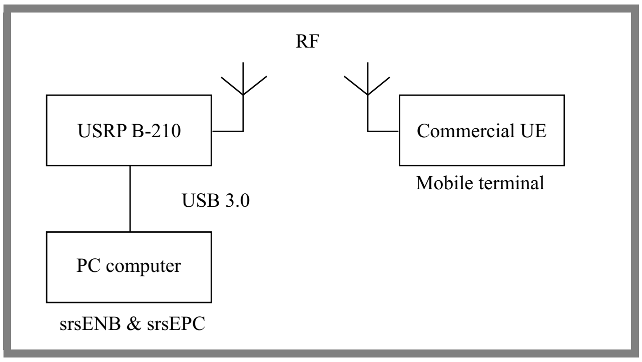


Fig. 2. eNodeB and commercial UE terminal configuration.

module, it is possible to run the 5G NSA mode thanks to the digital domain tuning. In this scenario, identical values of EARFCN and ARFCN parameters need to be entered for both carriers, e.g., 2600 MHz range. EARFCN and ARFCN values allow to set downlink and uplink frequencies for 4G and 5G carriers by specifying a set of frequencies defined by EARFCN (for 4G) and ARFCN (for 5G). These settings can be set in the *rr.conf* file describing the radio resources of the eNodeB station. Thereafter, using the *lo_offset* command, the frequencies need to be separated in the digital tuning range, with the tuning range defined by the main system clock – *master_clock_rate*. It needs to be borne in mind that clock frequencies have to be used that are integer multiples of the signal sampling frequency.

3.8. Interface Bandwidth Requirements

Another problem encountered when implementing a 5G NSA network using the USRP E320 platform is that the bandwidth of the 1 Gbit/s Ethernet communication port is too low. This port is capable of transferring up to 25 Mbaud/s, which translates into the maximum available bandwidth of 20 MHz. In the case of the 5G NSA mode, four 10 MHz channels are indispensable, meaning that a total system bandwidth of 40 MHz is required. To fulfill such a requirement, it would be necessary to equip a PC-class unit, responsible for emulating the functions of the 5G NSA base station, with a 10 Gbit/s Ethernet card. Replacing the card can provide a throughput of 200 Mbaud/s. Using the available system clock frequency of 46.08 MHz, it is possible to set up 4 channels with a total bandwidth of 40 MHz – 2 RX channels and 2 TX channels.

4. 4G Base Station System Implementation

4.1. Description of Hardware Components

This section describes the process of configuring and optimizing the 4G cellular network developed with the use of the USRP B210 programmable radio hardware platform. As a test platform, a PC equipped with an AMD Ryzen 5 3600 processor, an Nvidia GeForce GTX 1650 graphic card and 16 GB of RAM is used. The srsRAN software containing the srsENB and srsEPC modules is used to emulate the complete functionality of the base station. The srsUE software is launched on a separate PC with the same hardware configuration and the USRP B210 radio module. In addition, system performance tests with the commercial UE are carried out. The UE used in the described system supports both 4G and 5G solutions. Communication of the radio module with the PC computer is set up via the USB 3.0 port.

4.2. System Performance Measurement Procedure

The transmission rate and power received in the downlink and uplink channels are measured at a distance of 3 m from the base station for the UE and USRP B210, and 10 m for the UE only. System performance tests are carried out with the channel bandwidth of 10 MHz and 20 MHz, in the following transmission modes: 1 – SISO mode, 2 – broadcast diversity mode (2×2 MIMO), 3 – spatial multiplexing mode with cyclic delay diversity (CDD), and 4 – closed-loop spatial multiplexing mode. In addition – for transmission mode 4 – performance measurements are made with active automatic gain control (AGC) in the RX path. In that case, 80 dB, 100 dB or 120 dB transmit gain levels (*TX_gain*) are considered. The transmission takes place in the 2600 MHz frequency band, combining the downlink channel at the frequency of 2680 MHz and the uplink channel at the frequency of 2560 MHz. Performance of the system is verified using the iPerf tool [4] which generates network traffic of a specified intensity, using both TCP and UDP protocols. The tool is launched on both srsUE mobile terminals (USRP B210), commercial UE, and the eNodeB base station (USRP B210).

Figure 1 shows the connection between the USRP B210 modules and PC-class computers using the srsUE client, while Fig. 2 illustrates the connection between the eNodeB station and the commercial UE.

5. Installation and Configuration of the 4G Station

5.1. Additional Software Packages

In order to properly install the srsRAN package, it is necessary to install the *libuhd_dev* radio driver package and the *uhd_host* package first. This allows to control the state of the radio module in Linux.

5.2. srsGUI Suite Description and Functionality

The srsRAN environment is integrated with the srsGUI graphical package. This enables the observation of the constellation of the transmitted signal in the shared uplink physical channel (PUSCH) and the PUCCH control channel. The graphical package is launched by running the srsENB module. Similarly, a graphical environment may be installed for the srsUE package. This allows one to view the transmitted signal constellation for the downlink shared channel (PDSCH) and the downlink control channel (PDCCH). The srsGUI desktop environment must be installed prior to the main installation of the srsRAN package to ensure proper operation of the latter.

5.3. Software Module Configuration Options

After installing the srsRAN environment and the auxiliary components, it is recommended to move the configuration files to the *etc/srsran* system folder. The complete system configuration is stored in files with the *.conf* extension. This enables the parameters to be edited in a text editor, so that the configuration of the srsEPC, srsENB and srsUE modules can be easily modified. *enb.conf*, *sib.conf*, *rr.conf* and *rb.conf* files configure the following operating parameters of the srsENB module: transmission mode, transmitted power (*enb.conf*), resource allocation (*rr.conf*), and band aggregation (*rb.conf*). The operating parameters of the srsEPC module are controlled by variables stored in *epc.conf* and *user_db.csv* files. In the *epc.conf* file, IP addresses of the srsENB module (*mme_bind_addr* field) and an external DNS server are to be defined. This allows Internet access via the UE interface (to be specified in the *dns_addr* field). Authentication data of UEs, required to establish a connection with the station, are stored in the *user_db.csv* file; the type of the identification algorithm (XOR or Milenage), and the IMSI number of the SIM card of the UE can be set. The path to the *user_db.csv* file is defined in the *epc.conf* file in the *db_file* field, which enables access to the authentication data. This file is read during the procedure of connecting the UE to the network.

The srsUE module also has the ue.conf configuration file which stores various terminal configuration details, including the transmission mode and uplink transmit power. With that borne in mind, neither the eNodeB station nor the srsUE terminal feature a transmission power control mechanism, so the transmit power must be set before turning on the srsENB and srsUE modules.

The srsEPC, srsENB and srsUE modules on a separate machine are launched in individual terminal windows.

In the case of the srsENB module, it is also possible to specify the connection status display in real time. This function displays aggregated control information concerning downlink and uplink bit rate, the channel quality indicator reported by the mobile terminal (the *cqi* parameter) or the modulation and coding scheme (*mcs* parameter).

Additionally, the UHD controller is initialized automatically when starting the srsENB or srsUE modules. Therefore, communication with the programmable radio module is set up automatically.

6. 4G Network Performance Measurements

6.1. Testbench Configuration

In the first phase of the performance measurement process, a connection between the srsENB and srsEPC programs and srsUE modules was established. For this purpose, two B210 radio modules were configured, one as the eNodeB and the other as the UE. Each of these modules was connected to a PC running Ubuntu 22.04 LTS with the srsRAN package installed. The iPerf program was used to carry out the tests.

The srsRAN software enables the collection of diagnostic data from all srsRAN software modules which were saved in the *tmp* directory in the *.log* and *.pcap* file formats. Thanks to that, one can analyze the transmitted data frames e.g. in the Wireshark app. Complete files were created when all modules of the srsRAN package ended their operation.

The configuration details are as follows:

Resource blocks and bandwidth configuration. The tests were carried out using channel bandwidths of 10 MHz and 20 MHz, which corresponded to using 50 and 100 resource blocks (*n_prb* is set to either 50 or 100 in the *enb.conf* file).

MIMO mode configuration. Depending on the 2 × 2 MIMO antenna configuration selected, it was necessary to set the following parameters accordingly: $t_m = 2$ (transmit diversity), $t_m = 3$ (transmission using the CCD cyclic prefix shift), $t_m = 4$ (multiplexing with closed feedback loop). For multi-antenna transmission modes, the number of active

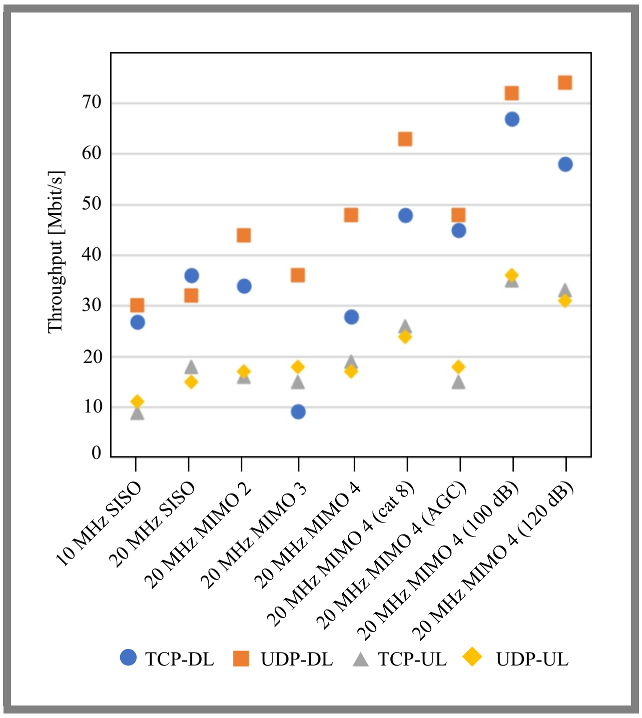


Fig. 3. Iperf performance test – srsUE.

TX ports should be set to 2 (*nof_ports*=2 command in the *enb.conf* file).

Transmission frequency configuration. The transmission frequency was determined by the *dl_earfcn*=3350 parameter which corresponds to the setting of the downlink channel frequency (2680 MHz). The uplink channel frequency was then set automatically at 2560 MHz.

Transmission gain setup. The transmit gain (*tx_gain* parameter) was set at 80 dB, then 100 dB and 120 dB.

AGC mechanism configuration. The tests were initially carried out with a constant RX channel gain of 40 dB (*rx_-gain*=40 command). In the subsequent measurements, the AGC mechanism was activated by commenting out respective configuration line #*rx_gain*=40.

Miscellaneous radio module settings. In order to improve the efficiency of the USRP B210 radio module, additional arguments, such as *device_args* = (. . .) *num_send_frames*=64 and *num_recv_frames*=64, were set. These allowed to increase the number of RX and TX buffers for the transmitted frames from 32 to 64, thereby improving overall performance of the system. In the case of UE emulated by the srsUE software, the same modifications regarding the channel gains were made. Note that the AGC mode was available for RX channels only. In the case of the MIMO mode, the *nof_antennas* parameter had to be set to 2 in the *ue.conf* file. The arguments passed to the UHD driver in the *device_args* field were defined in the same way as in the *enb.conf* file.

Performance tests were conducted for category 4 and category 8 terminals. In the latter case, 64-QAM modulation was used in the uplink. The current mobile terminal category was defined in the *ue_category* field.

Configuration of srsUE virtual network interface. To provide the Internet connection to the mobile terminal emulation station using the srsUE software, it was necessary to add a default IP traffic routing gateway on the UE client computer. Then, the default gateway address was linked with the virtual network interface emulated by the srsUE program called *tun_srsue*. In this case, the IP address was the address of the S/P GW subsystem which acted as a virtual network gateway. It also enabled the routing of packets to UEs connected to the eNodeB station. It is important to note that the *tun_srsue* virtual interface was active only when the srsUE module was running.

Downlink channel performance test. In order to check the downlink throughput at the client station (UE), the iPerf service server was started on a separate terminal. TCP and UDP traffic was generated using the iPerf client.

In the case of TCP traffic, the maximum throughput was not defined by the user, while for UDP traffic, the value of the maximum traffic throughput was set arbitrarily to 100 Mbit/s. Note that the value defined above exceeded the maximum system throughput obtained.

Uplink channel performance test. The uplink channel throughput test was carried out in a similar way, but the iPerf service server listening to the network traffic was launched on the eNodeB station. Simultaneously, a client sending queries was run on the station emulating a UE.

6.2. Radio Channel Performance Test Results – srsUE

Radio link throughput results are presented in Fig. 3. Most of the measurements were carried out with the transmit gain of 80 dB. Only for the "20 MHz – MIMO – 4 (100 dB)" and "20 MHz – MIMO – 4 (120 dB)" setups, the gains of 100 and 120 dB were applied, respectively. The AGC was also set active and category 8 UE was selected. The distance between the antennas of the USRP stations was constant throughout all of measurement tests – it was 3.2 m in line of sight (LOS) conditions. The higher data rates observed in the downlink resulted from the use of a higher-order modulation than that used in the uplink.

6.3. srsENB Configuration – Commercial UE Terminal

The second series of measurement tests was carried out using commercial off-the-shelf UE. This device was configured to work with the base station by programming accurate SIM card parameters in the *user_db.csv* file. The following properties have been filled in: Name – the name of the UE defined by the user, Auth – authentication algorithm mode selected – XOR or Milenage, IMSI – identification number of the SIM card installed in the UE, Key – authorization key in hexadecimal format, OP_Type – type of the used operator code, OP/OPc – value of operator code assigned to the specified SIM card, AMF – authentication management field, SQN – UE sequential number, used when restarting the identification procedure), QCI – a field specifying the identifier associated with the management class of the quality of service (QoS) mechanism, IP_alloc – the method of assigning the IP address to the UE – static or dynamic.

Having made changes to the configuration in the *user_db.csv* file, it was necessary to specify the configuration of the APN. For this purpose, a point called default has been defined in the UE settings field (APN tab). This setting was identical to the value of the *apn=default* field contained in the *epc.conf* file. Determining the correct APN point in the UE was necessary to get access to data transmission services via the 4G network, and then connect to the Internet.

The remaining parameters were configured similarly to the process of setting up a connection with a virtual UE, emulated by the srsUE program. The base station maintained the same configuration as in the previous tests i.e. using the srsUE client.

6.4. Channel Performance Test – Commercial UE Terminal

Connection tests were carried out using the iPerf tool (with the use of the UDP protocol) in the same way as relied upon for the previous measurement scenario. However, the UE was located at a distance of either 3.2 m or 7.8 m from the base station antennas. The aim of running an additional series of measurements over a distance of 7.8 m was to evaluate the effectiveness of the power control mechanism in the uplink. Unlike the USRP B210, the commercial UE was equipped

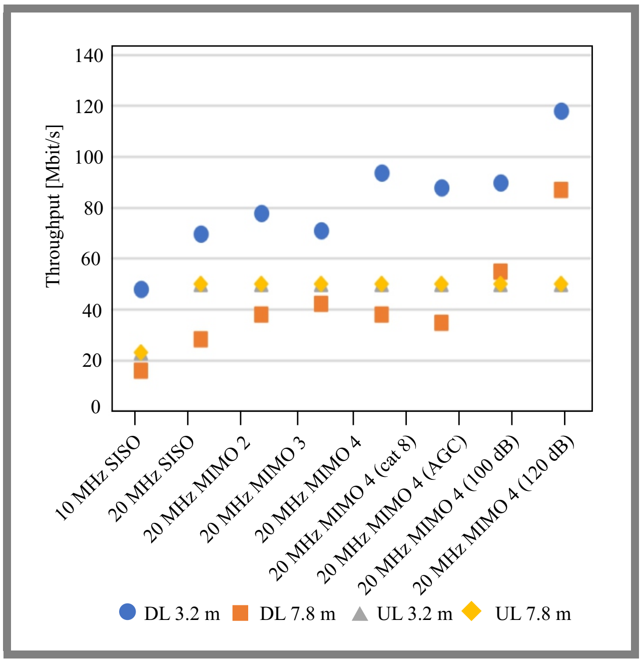


Fig. 4. Iperf performance test – commercial UE.

with a transmission power control mechanism. The implementation of the iPerf server and client on UE was carried out using the iPerf2 for Android application.

Radio link throughput results are shown in Fig. 4. The measurements were carried out with three levels of transmit gain at the 2680 MHz carrier in the downlink. In the case of measurements with TX gain of 100 dB and 120 dB, the AGC mechanism remained active. The other measurements were carried out with a transmit gain of 80 dB. In this case, the "20 MHz – MIMO – 4 (AGC)" measurement was made using the automatic gain control mode and MIMO multi-antenna transmission mode 4 (closed loop spatial diversity).

7. Radio Channel Power Measurements

In addition to radio link throughput measurements, the received and transmitted power in the uplink and downlink channels was measured as well. For the srsUE, a Rohde & Schwarz FSH4 spectrum analyzer with an Ettus Research VERT 2450 antenna was used. Similar antennas were used in the USRP B210 modules operating as an eNodeB station and an UE client. Downlink channel power measurements were made at three measurement points – 10 cm from the base station, 10 cm from the srsUE mobile terminal station, and 30 cm from the base station (1.2 m from the UE station). The measurements were repeated with active data transmission and in with the UE in idle mode (no active transmission). The uplink channel power was measured during active packet transmission at a distance of 10 cm from the base station (eNodeB). The received power values have been averaged.

A separate series of power measurements was conducted for commercial UE. This kind of terminal features an internal microstrip antenna. Power measurements were carried out for two UE positions – it was located at a distance of 3.2 and 7.8 m from the base station. The measurements were made at a distance of 10 cm from the base station, 30 cm from the base station and 10 cm from the UE.

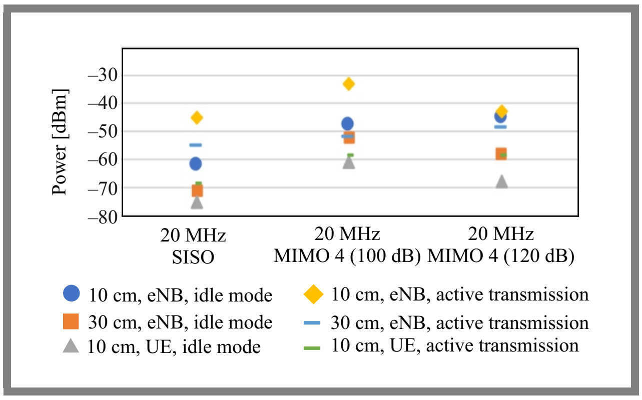


Fig. 5. Power measurements: downlink – srsUE.

7.1. Results for srsUE

The results of power received in the downlink and in the uplink for the srsUE mobile terminal are shown in Fig. 5 and Fig. 6, respectively.

Figure 7 presents the power spectral density (PSD) of the downlink signal in the idle mode at a distance of 10 cm from the base station, assuming a 20 MHz bandwidth and a 100 dB transmit gain.

Figure 8 shows the PSD of the downlink signal in the active transmission mode at a distance of 10 cm from the base station, with a 20 MHz bandwidth and a 100 dB transmit gain

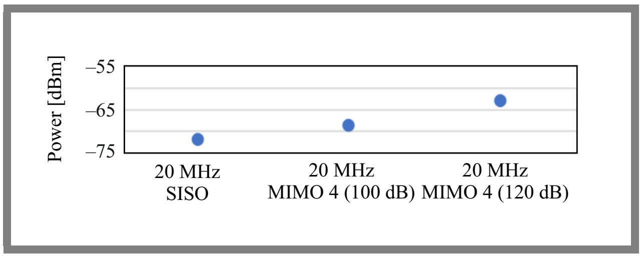
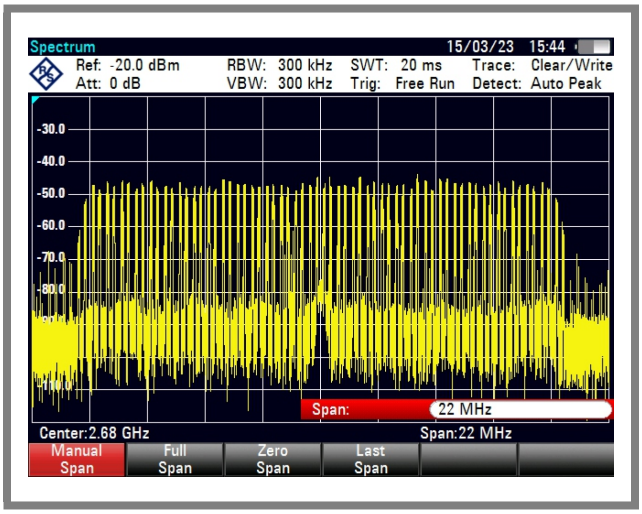


Fig. 6. Power measurements: uplink – srsUE.


Spectrum 15/03/23 15:44

Ref: -20.0 dBm RBW: 300 kHz SWT: 20 ms Trace: Clear/Write

Att: 0 dB VBW: 300 kHz Trig: Free Run Detect: Auto Peak

Span: 22 MHz

Center:2.68 GHz Span:22 MHz

Fig. 7. Spectrum measurements: downlink – 10 cm – idle mode.

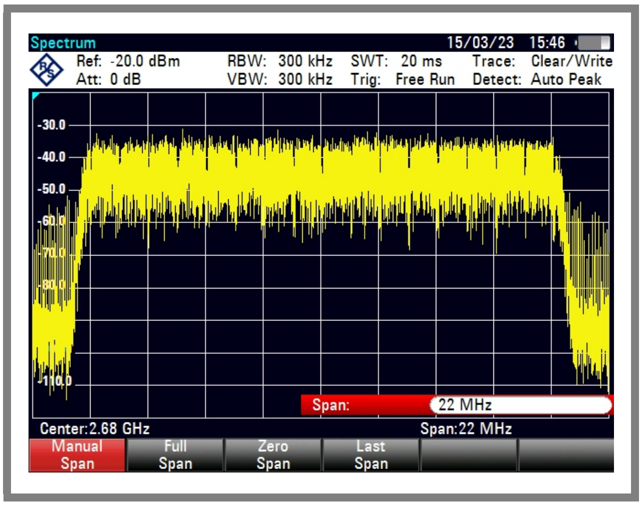

Spectrum 15/03/23 15:46
Ref: -20.0 dBm RBW: 300 kHz SWT: 20 ms Trace: Clear/Write
Att: 0 dB VBW: 300 kHz Trig: Free Run Detect: Auto Peak
Span: 22 MHz
Center: 2.68 GHz Span: 22 MHz

Fig. 8. Spectrum measurements: downlink – 10 cm – active transmission.

assumed again. Figure 9 illustrates the PSD of the uplink signal in the active transmission mode at a distance of 10 cm from the base station for a 20 MHz bandwidth and a 100 dB transmit gain.

7.2. Commercial UE Terminal

Figure 10 shows the power transmitted in the downlink for the terminal located at a distance of 3.2 m from the base station. Figure 11 presents the values of the power transmitted in the downlink for the UE located at a distance of 7.8 m from the base station, while Fig. 12 shows the values of the power transmitted in the uplink for the UE located at a distance of 3.2 m and 7.8 m from the base station, i.e. during active data transmission.

Figures 13 and 14 present the PSD of the uplink signal at the base station input situated 3.2 m and 7.8 m from the UE, respectively, for a 20 MHz bandwidth and a 100 dB downlink TX gain.

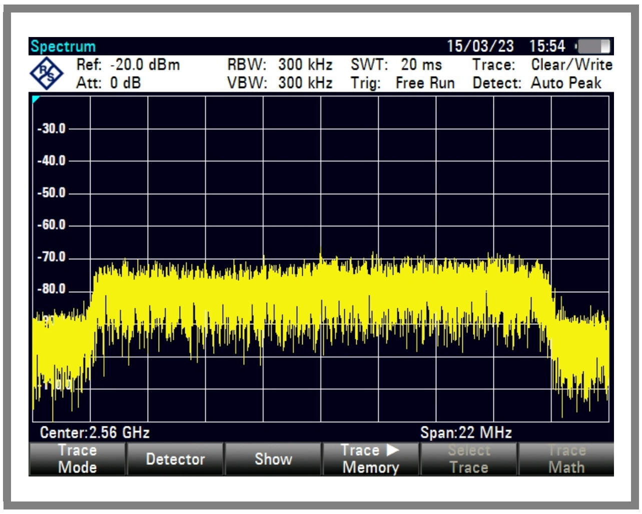

Spectrum 15/03/23 15:54
Ref: -20.0 dBm RBW: 300 kHz SWT: 20 ms Trace: Clear/Write
Att: 0 dB VBW: 300 kHz Trig: Free Run Detect: Auto Peak
Center: 2.56 GHz Span: 22 MHz

Fig. 9. Spectrum measurements: uplink – active transmission – 20 MHz bandwidth and 100 dB transmit gain.

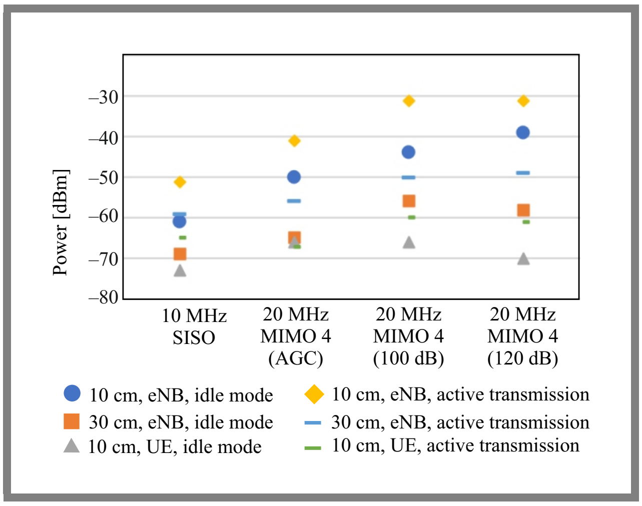


Fig. 10. Power measurements: downlink – 3.2 m – commercial UE.

8. Conclusions

In the case of radio link throughput tests using the USRP B210 module acting in the capacity of UE, a radio channel bandwidth increase from 10 to 20 MHz has resulted in boosting the link throughput by approx. 25%. Activation of the multi-antenna transmission mode failed to offer a significant gain in the link throughput, but increased its stability. Upgrading the UE category to level 8 resulted in the link throughput

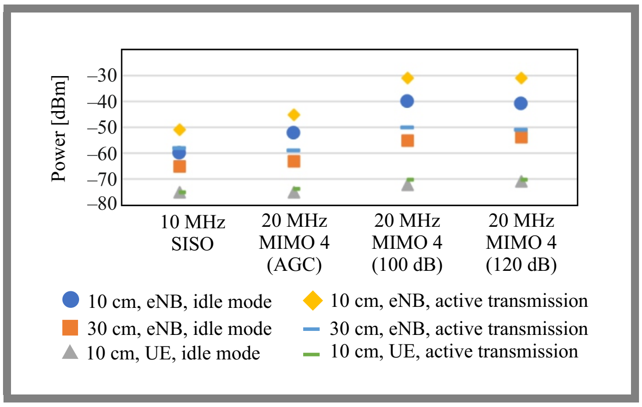


Fig. 11. Power measurements: downlink – 7.8 m – commercial UE.

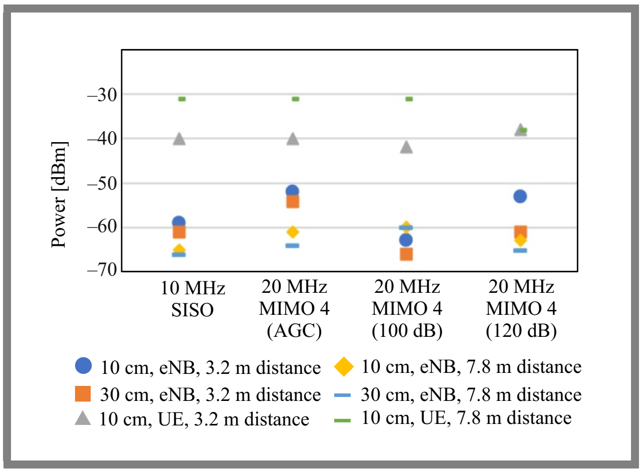
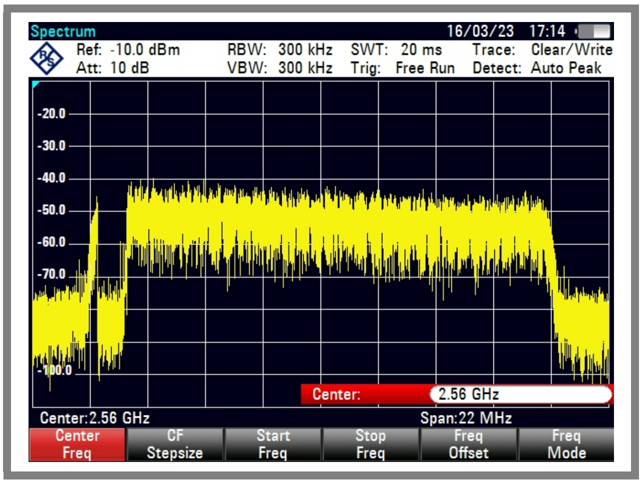


Fig. 12. Power measurements: uplink – commercial UE.



Spectrum 16/03/23 17:14

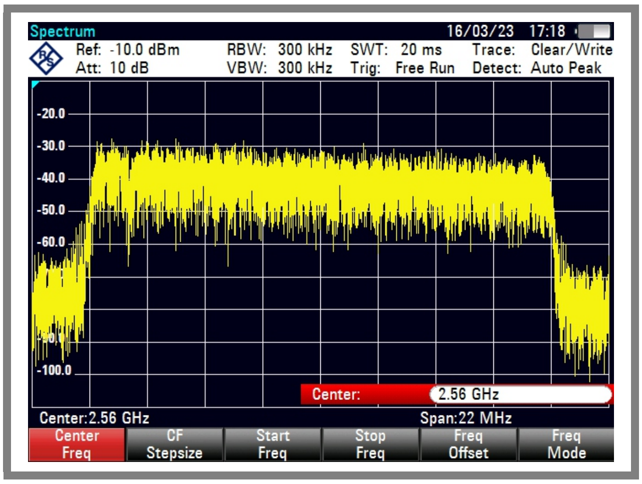
Ref: -10.0 dBm RBW: 300 kHz SWT: 20 ms Trace: Clear/Write

Att: 10 dB VBW: 300 kHz Trig: Free Run Detect: Auto Peak

Center: 2.56 GHz

Center:2.56 GHz Span:22 MHz

Fig. 13. Spectrum measurements: uplink – distance 3.2 m – 20 MHz bandwidth.



Spectrum 16/03/23 17:18

Ref: -10.0 dBm RBW: 300 kHz SWT: 20 ms Trace: Clear/Write

Att: 10 dB VBW: 300 kHz Trig: Free Run Detect: Auto Peak

Center: 2.56 GHz

Center:2.56 GHz Span:22 MHz

Fig. 14. Spectrum measurements: uplink – distance 7.8 m – 20 MHz bandwidth.

being increased by approx. 50 % (using the UDP test protocol). This is due to the change of the modulation scheme to 64-QAM on the UE side. Activation of the AGC mode caused a drop in link throughput. This resulted from the observed RX gain being lower than in the case of the static setting, which diminished SNR. On the other hand, a significant increase in the link throughput (up to 74 Mbit/s) was observed when the TX gain in both the base station and the UE increased to 120 dB. Any increment in the TX gain boosted the radiated power which, in turn, improved SNR. At a higher SNR range, it was possible to use a higher-order modulation and coding scheme. Exceeding the gain value of 100 dB failed to offer a significant increase in the link throughput. this is caused mainly by the saturation of the radio module power stages. No significant increase in the carrier power level was recorded.

In the case of radio channel throughput tests using commercial grade UE (a phone), the results were similar. The activation of the AGC mode, once gain degraded the link throughput. The decreased link throughput was noticeable when the terminal had moved away from the base station – a higher distance entailed a higher free-space attenuation and an SNR decrement. On the other hand, a drop in SNR caused the station to use lower-order modulation and coding schemes. This mechanism decreased the link throughput with the aim to limit the bit error rate (BER).

During the power measurements, the carrier power increased proportionally to the value of the defined transmit gain. The difference in the downlink carrier power between the idle mode of the UE and active transmission was 10 dB, on average. It is important that the downlink OFDM subcarriers were transmitted continuously and their power increased in the case of active data transmission. The uplink power was measured only during active transmission. With no active user data transmission from the UE, control data were transmitted using the selected pilot subcarriers of the uplink channel bandwidth only. This was unlike with active data transmission, where all subcarriers were used. In the idle mode i.e., without active data transmission on user plane, pilot subcarriers were transmitted only occasionally. As a consequence, signal spectrum measurements required long averaging times. Commercial-grade off-the-shelf UE, unlike the srsUE virtual terminal, was equipped with a transmission power control mechanism. The effects of this mechanism were visible when the UE was being moved away from the base station. The transmission power on the uplink channel varied between –42 and –38 dBm when the UE was located 3.2 m from the base station. If the distance between the UE and the base station increased to 7.8 m, the transmitted power increased to –31 dBm measured at a distance of 10 cm from the UE.

The cellular system setup considered in this publication enables the development of an open-source radio access network. This is useful for analyzing the operation of the protocol layers of the LTE network standard. The system can be used for propagation tests in the evolving radio environment at a desired location. This is possible thanks to the high degree of hardware mobility and flexibility of software configuration, as well as the fact that a wide range of radio modules and various antenna types are supported. On the other hand, high scalability of this system allows to optimize the configuration using a small-scale network. Finally, it is possible to reproduce it in a large, commercial RAN system.

Acknowledgments

The work has been performed in 2023 under the project no. 0312/SBAD/8163 titled “New methods of signal transmission and reception, design, and testing of radio communication systems”.

References

[1] B. Maqsood, “Implementation and performance analysis of software defined radio (SDR) based LTE platform for truck connectivity application”, Master Thesis, KTH Royal Institute of Technology, Stockholm, Sweden 2019 (http://www.diva-portal.org/smash/record.jsf?pid=diva2:1413149).

[2] A. Kaszuba, R. Chęciński, and J. Łopatka “Capture information about GSM users using software defined radio platform USRP”, *Bulletin of the Military University of Technology*, vol. 62, no. 3, pp. 27–36, 2013

(http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-8a873ca8-67c3-4ec6-bad0-e802b8d08741/c/Kaszuba.pdf) (in Polish).

[3] P. Sutton *et al.*, "Open Source RAN", Software Radio System RS RAN Project, 2023 (https://www.srslte.com)

[4] "The TCP, UDP and SCTP network bandwidth measurement tool", iPerf, 2019 (https://iperf.fr).

[5] "Software Radio Systems" – srsRAN Documentation, Release 22.10, 24 Nov 2022 (https://docs.srsran.com/_/downloads/4g/en/rfsoc/pdf).

[6] "Knowledge Base", Ettus Research, 2023 (https://kb.ettus.com/Knowledge_Base).

[7] B. Schulz, "LTE Transmission Modes and Beamforming – White Paper", Rohde & Schwarz Company, 2015 (http://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma186/1MA186_2e_LTE_TMs_and_beamforming.pdf).

[8] R. Hu and Y. Qian, "*Heterogeneous Cellular Networks*", Wiley 2013 (ISBN: 9781119999126).

[9] "5G Core Network" Whitepaper", Telcoma Global Whitepaper, (https://telcomaglobal.com/courses/6g-5g-4g-white-papers/lectures/34560661).

[10] J. Sungho, "LTE and Network Evolution", *ITU-T Workshop on Bridging the Standardization Gap and Interactive Training Session*, Nadi, Fiji, 2011 (https://www.itu.int/dms_pub/itu-t/oth/06/4D/T064D0000020072PDFE.pdf).

[11] Recommendation ITU M.2150, "Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications 2020 (IMT–2020)" – ITU-R, 2022 (https://www.itu.int/rec/R-REC-M.2150/en).

Wojciech Flakowski, M.Sc.
Institute of Radiocommunications, Faculty of Computing and Telecommunications
https://orcid.org/0000-0001-6915-3687
E-mail: wojciech.flakowski@doctorate.put.poznan.pl
Poznan University of Technology, Poznan, Poland
https://cat.put.poznan.pl

Maciej Krasicki, Ph.D., Associate Professor
Institute of Radiocommunications, Faculty of Computing and Telecommunications
https://orcid.org/0000-0001-7726-3114
E-mail: maciej.krasicki@put.poznan.pl
Poznan University of Technology, Poznan, Poland
https://cat.put.poznan.pl

Rafał Krenz, Ph.D., Associate Professor
Institute of Radiocommunications, Faculty of Computing and Telecommunications
https://orcid.org/0000-0001-5354-9812
E-mail: rafal.krenz@put.poznan.pl
Poznan University of Technology, Poznan, Poland
https://cat.put.poznan.pl