Detection of Different Wireless Protocols on an FPGA with the Same Analog/RF Front End

Suranga Handagala, Mohamed Mohamed, Jieming Xu, Marvin Onabajo, and Miriam Leeser(✉)

Northeastern University, Boston, MA 02115, USA
{handagala.s,mohamed.m,xu.jiem}@husky.neu.edu, {monabajo,mel}@ece.neu.edu
https://www.northeastern.edu/rcl/

Abstract. The surge in smart phones, tablets, and other wireless electronics has drastically increased data usage and wireless communication, creating massive traffic spectrum demand. Congestion is mainly due to inefficient use of spectrum, rather than spectrum scarcity. Spectrum coexistence schemes provide opportunities for efficient use of the spectrum. Furthermore, software-defined hardware reconfiguration after signal detection can be completed to reduce the power consumption of adaptive analog/RF front ends. In this paper, we propose a Wi-Fi and LTE protocol coexistence architecture, and present its implementation using a Xilinx evaluation board and ADI RF front end.

Keywords: Software defined radio · Wireless protocols · RF front end FPGA

1 Introduction

Wireless protocols are rapidly changing as more and more devices are interconnected wirelessly. These include both devices with high throughput and low latency requirements such as cell phones and tablets, and devices with low throughput communications such as is exhibited with many devices in the Internet of Things (IoT). At the same time, research efforts for 5G are examining higher flexibility and adaptability in implementations [10]. Researchers would like to easily prototype existing protocols and experiment with new concepts, while still being able to meet real time communications requirements. For many years FPGAs have been used for Software Define Radio to meet such needs. As requirements for wireless communications have become both more difficult to meet and more diverse, capabilities of FPGAs have grown as well.

Our research targets an environment where a single hardware platform can be used to support multiple different protocols. We envision a scenario where this hardware platform does not know *a priori* which protocol it will be supporting. It

I. Moerman et al. (Eds.): CROWNCOM 2018, LNICST 261, pp. 25–35, 2019.
https://doi.org/10.1007/978-3-030-05490-8_3

senses the environment, determines what packets it is receiving, and then loads the optimum processing for the rest of the receive and transmit chain. This paper focuses on the first step of this processing; namely, sensing the environment and choosing which protocol to support. We limit our discussion to 802.11a and LTE; however the model will be extended to other protocols in the near future.

The hardware platform we use is an Analog Devices ADI FMCOMMS3 board[1] connected to a Xilinx ZC706 Evaluation board. The FMComms3 board supports a relatively wide bandwidth range of 70 MHz–6 GHz and 2 × 2 MIMO. It connects to the FPGA board through an FMC connector. The Xilinx ZC706 board is an evaluation board with Xilinx Zynq XC7Z045 with embedded ARM processor as well as reconfigurable FPGA hardware resources. This represents very popular hardware setups for radio researchers working at the PHY layer [6,7].

The main contribution of this paper is a platform with common RF front end, settings and reconfigurable hardware that can accurately detect different wireless waveforms and thus be deployed in various different settings. The approach is flexible and extensible to waveforms of the future.

2 Background

2.1 Radio Technology and Hardware Trends

When observing analog/radio frequency (RF) front end design trends for software-defined radio (SDR) applications, reconfigurable analog integrated circuits help to reduce power consumption while improving performance [2,11]. Ongoing circuit and system design trends create a great need to co-design analog and mixed-signal circuits together with computing resources for the control of optimizations, particularly to support future reconfigurable and cognizant radios that will be realized as SDRs. FPGAs can play a key role in this process [4]. Integrated analog/RF transceiver circuits for Wi-Fi and LTE increasingly include signal processing and control methods to continuously tune components for high performance and reliable operation under varying conditions [1,8]. Hence, these digitally-assisted analog design and calibration approaches are significantly gaining importance to enhance the performance and reliability of low-power mixed-signal systems-on-a-chip in ubiquitous complementary metal-oxide-semiconductor (CMOS) technologies. Such calibrations can incorporate existing or dedicated analog-to-digital converter (ADC) and digital signal processor (DSP) resources for computation of corrective actions and automatic tuning with digital-to-analog converters (DACs). However, reconfigurable analog front-ends for SDRs require different settings and digital calibrations, depending on the mode of operation and the type of signal that is received at a given time. For example, Wi-Fi and LTE have different receiver sensitivity specifications, which leads to different requirements for the gain, noise figure, and linearity of the RF/analog frond end blocks in the receiver path. Similarly, the two standards have different requirements with regards to the suppression of interference

[1] https://wiki.analog.com/resources/eval/user-guides/ad-fmcomms3-ebz.

signals having specified power levels and offset frequencies relative to the channel of interest. This results in different baseband filtering requirements, which can also be changed through settings that reconfigure active filter circuits. A universal digital hardware implementation for all modes of operation would incur excessive power overhead in many applications. The signal detection research described in this paper is in part motivated by the need to extract information for real-time optimizations and power reductions of reconfigurable analog/RF front ends. An AD9361 Agile RF transceiver was employed in the experiments reported in this paper for a proof of concept, but it is envisioned that future reconfigurable application-specific integrated RF front ends will benefit through adaptive optimizations based on the information obtained through on-board FPGA processing.

2.2 Wi-Fi and LTE Waveforms

Wi-Fi is a wireless local area network (WLAN) protocol that allows devices such as smart phones, laptops, and tablets to communicate wirelessly. Long Term Evolution (LTE) was developed by 3GPP to enhance the performance of 3G systems in terms of data throughput, spectrum utilization, and user mobility, and works on the uplink (UL) and downlink (DL). The LTE DL channel uses an OFDMA interface, which supports multiple input multiple output (MIMO). Using OFDMA increases stability against multipath distortion, reduces latency, and allows for multiple data rates. The LTE radio frame is 10 ms long, consisting of ten 1 ms sub-frames. In frequency-division duplexing (FDD) operating mode, each sub-frame contains two 0.5 ms slots. Each slot contains 7 OFDM symbols for the normal cyclic prefix and 6 OFDM symbols for the extended cyclic prefix.

3 Coexistence Architecture

The goal of our approach is to use the same RF front end and FPGA based processing hardware to detect which waveform is being communicated with the

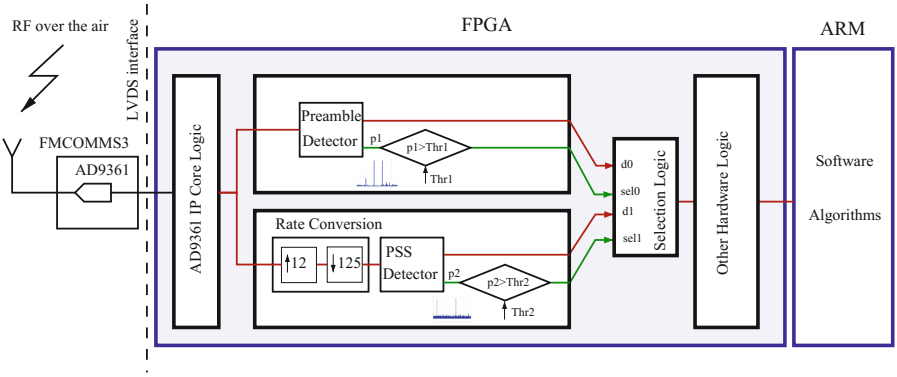


Fig. 1. Proposed coexistence setup

intent of later adjusting RF front end settings and downloading the appropriate processing to tune the transceiver to the current waveform. Jiao et al. [6] take a complementary approach by supporting multiple protocols on the same platform at the same time. While this is very similar to our goal, it is not extensible as the number of protocols continues to grow. Figure 1 shows our architecture, including the block diagram for each receiver. Note that these make use of a common RF front end and common sampling rate of 20 MHz. The receiver chains for each are described in this section, as well as steps taken to deal with different bandwidths.

3.1 802.11a Receiver Chain

All WiFi standards use a preamble for timing synchronization, frequency offset compensation and channel estimation. In an 802.11a frame, there are two types of preambles; a short training sequence consisting of 10 identical patterns each of which has 16 samples, and two identical long training sequences each of which has 64 samples. The short training sequence can be used to obtain a coarse estimate of the start of a frame while the long training sequence produces a more accurate estimate. We use a 64 tap, hardware friendly, matched filter for detecting the long preamble based on multiplier-free efficient implementation techniques [3].

3.2 LTE Receive Chain

In FDD operating mode, the Primary Synchronization Signal (PSS) is located in two locations in each 10 ms LTE radio frame. The first one is in the last OFDM symbol of the first time slot of the first subframe, where each subframe is 1 ms and each slot is 0.5 ms. The PSS is repeated in the last OFDM symbol in subframe 5. LTE uses a synchronization channel (SCH) inserted periodically in the DL LTE radio frame. The SCH is composed of a PSS and a Secondary Synchronization Signal (SSS). The PSS is generated from a 63-length frequency-domain Zafoff-Chu (ZC) sequence whose root index determines the sector identity. Detection of PSS in the TD is implemented by cross-correlating the TD signal with the three PSS coefficients in which one of the three correlation outputs will display two peaks, indicating both PSS locations within one LTE radio frame [9]. The cell search process is done by detecting the position of the PSS within the received DL signal in order to acquire timing information and determine the sector index by identifying which sequence has been transmitted out of the three ZC sequences. The received DL is then cross-correlated with each of the three ZC sequences in which one of the correlation outputs will demonstrate two peaks, indicating the successful detection of an LTE radio frame.

3.3 Adjusting Sampling Rate for LTE

In the 802.11a standard, the sampling rate is fixed at 20 MHz. For LTE, the sampling rate varies from 1.92 MHz to 30.72 MHz. However, the PSS signal is always located at the center frequency of the LTE transmission band regardless of the sampling frequency. This feature allows us to detect the PSS signal at a fixed frequency by applying filters to the received signal. The PSS signal only and always occupies the central 63 subcarries in the whole band. For the smallest sampling rate, which is 1.92 MHz, the IFFT size is 128 points. As a result, the received signal sampled at 20 MHz shall be downsampled to 1.92 MHz for matched filter processing. The resample ratio is:

$$\frac{1.92 \times 10^6 \text{Hz}}{20 \times 10^6 \text{Hz}} = \frac{12}{125} = \frac{2 \times 2 \times 3}{5 \times 5 \times 5} \tag{1}$$

The resample ratio shows that the 20 MHz signal should be downsampled by 125 and upsampled by 12 to achieve the 1.92 MHz sampling rate. Directly implementing the sampling rate conversion filter requires 3000 taps, which is almost impossible to implement in hardware. An optimized FIR design that factors the downsample and upsample ratio to $2 \times 2 \times 3$ and $5 \times 5 \times 5$ still requires a 405 tap filter. As a result, for symmetric FIRs, at least 200 DSP slices would be consumed by the sampling rate converter.

To reduce the consumption of DSP blocks on the FPGA, we replace the traditional FIR by a CIC filter. The CIC filter for sampling rate conversion was first introduced by Hogenauer in [5]. This multiplier free FIR filter can be implemented in an economical way for decimation and interpolation to reduce the usage of registers and adders. The goal is to keep the resampling filter small to be able to accommodate other processing, including OFDM demodulation and channel equalization which consume a large amount of resources.

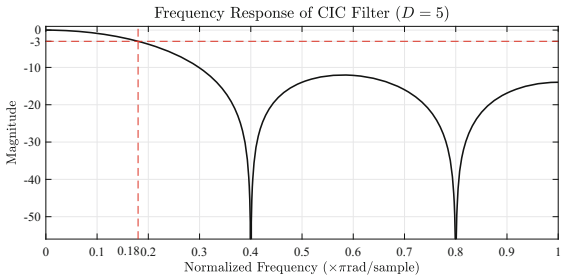


Fig. 2. CIC filter frequency response.

From Eq. 1, we can see that the downsample factor is larger than the upsample factor. Hence, only one low-pass filter for the downsampler is needed to implement the whole conversion system. In our design, we use three cascaded CIC filters with a factor of 5 for the low-pass filter. The frequency response of

a downsampling CIC filter with a factor of 5 is shown in Fig. 2. This design can be used to detect the PSS in any LTE signal.

4 Results

The target hardware for this design consists of an ADI FMCOMMS3 RF front end and Xilinx Zynq ZC706 Evaluation Board. We detect both 802.11a and LTE signals using this setup. We present simulation results as well as results on running hardware. Transmission using an SMA cable between two boards was used to detect LTE signals, while over the air transmission using one board was used to detect Wi-Fi signals. The results on running hardware consist of both Built-In Self-Test (BIST) loopback as well as over-the-air experiments.

4.1 Software and Hardware Configuration

Our setup includes two processors, the embedded ARM processor that is part of the Xilinx Zynq XC7Z045 chip on the ZC706 board, and the host CPU in the computer attached to the platform. The ADI 9361 has its own device drivers that control all transmit/receive chain parameters of the AD9361 chip such as local oscillator frequency, bandwidth, sampling frequency, TX/RX path automatic gain control mode, and gains of analog front end blocks. In addition to including device drivers, a user needs the LibIIO framework installed for applications to communicate with ADI hardware. For simulation results, which do not include any FPGA hardware, we run Analog Devices IIO Oscilloscope on the host PC.

For experiments that involve the Zynq processor, we use Petalinux, a version of Linux supported by Xilinx, on the embedded ARM processor. The interaction between ARM and the AD9361 device is performed using two platform device drivers built into the kernel. There is also an AD9361 FPGA core driver for the

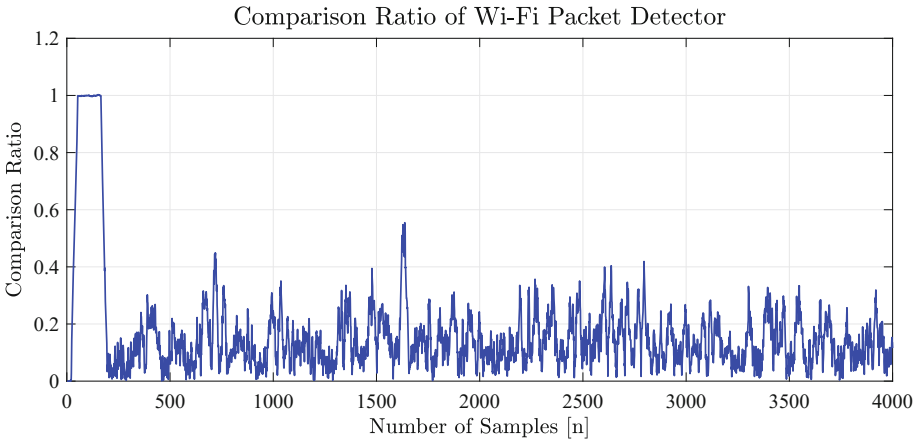


Fig. 3. Packet detector output of detected Wi-Fi signal.

FPGA fabric that provides the user with an option to correct IQ imbalances and DC offsets on the receiver side.

4.2 Simulation

Simulations, using MATLAB R2017a with the Signal Processing, Communication, and LTE System Toolbox have been performed based on the block diagram presented in Fig. 1, where signals are received using the AD9361 FMCOMMS3 at a sampling rate of 20 MHz. Each signal is passed through both the Wi-Fi and LTE paths in parallel and using peak-to-average ratio thresholds, the signal is determined to be either Wi-Fi or LTE. Figure 3 shows the packet detection of a Wi-Fi packet in discrete samples, where a comparison ratio of an autocorrelation of x[n] and x[n−16], where x[n] indicates the received samples and 16 is the length of the short training sequence, and the variance of x[n] for the received samples is displayed. In this figure, the falling edge position, located at sample 165, indicates the beginning of the Wi-Fi packet. The packet detection flag is asserted when the peak-to-average ratio threshold is met, indicating the presence of a Wi-Fi signal.

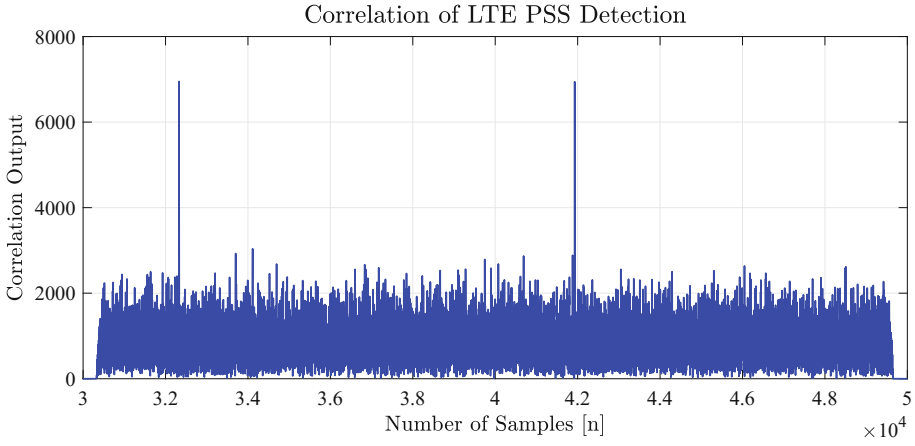


Fig. 4. LTE PSS correlation output.

The LTE PSS detection is performed using the cross-correlation of the received TD signal with the PSS coefficients. Since one LTE radio frame contains two PSS signals, two peaks indicating the positions of each one of the PSS signals are shown in Fig. 4. Another peak-to-average ratio threshold is used to indicate the received signal is indeed an LTE signal.

4.3 Hardware Experiments

Our hardware setup is shown in Fig. 5. Two antennas are used on the ZC706, one for transmit and one for receive. In experiments not depicted here, two separate

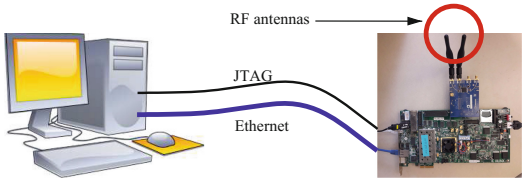
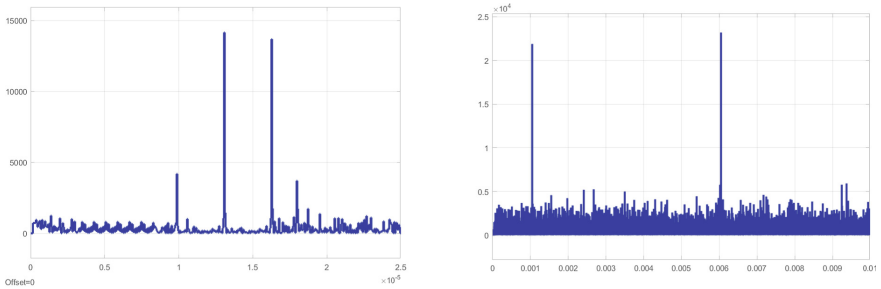


Fig. 5. Hardware setup and host PC interfacing over JTAG and ethernet connections

setups were used with one functioning as transmitter and one as receiver. We use pre-created 802.11a and LTE signals which are stored in a text file. We use a C program to read these complex I and Q samples, and send them through a DMA channel along the transmit chain. One set of experiments bypassed the RF section by using the BIST loopback feature available in the AD9361 chip, so that the accuracy of the received signal could be verified in the digital domain. Once the digital design had been verified, over the air experiments were undertaken.

The detection logic that was mapped to FPGA hardware for 802.11a and LTE receiver chains were designed using the Mathworks Simulink HDL code generation workflow (version 2017b) and implemented using Xilinx Vivado version 2016.4 with an FPGA clock frequency of 100 MHz. The PL also consists of AD9361 AXI IP core which provides the digital interface to the FMCOMMS3 card. For the receiver chain, this core has been configured to compensate for IQ imbalances and DC offsets.

The detection logic mapped onto the FPGA could be used to identify the presence of either 802.11a or LTE signals received via the common RF front end. Figure 6(a) corresponds to an 802.11a signal where the entire receive chain operates in real time. For LTE, the rate conversion takes place offline. This converted signal is passed through the LTE matched filter implemented in FPGA fabric, resulting the peaks in Fig. 6(b).



(a) (b)

Fig. 6. (a) 802.11a (b) LTE hardware friendly matched filter outputs of two real world signals received with the common RF front-end

4.4 FPGA Utilization

Vivado post-implementation utilization figures (Table 1) revealed that a significant reduction in resources, especially for the DSPs, can be achieved by using hardware friendly matched filtering without compromising the detection capability. Had the conventional discrete FIR been used, the DSP resource count would have been four times the number of filter coefficients. Although this number can be reduced by 25% by using 3 DSP48s per complex multiplication, accommodating other complex logic could still be challenging because of high receiver complexity. Detection results in Fig. 6 show that the 802.11a preamble and LTE PSS can be successfully detected even at the expense of peak-to-average ratio. This reduction is quantified in Table 2.

Table 1. FPGA resource utilization statistics (percentages given are with respect to the total number of resources available in the device).

	Discrete FIR (802.11a)	Hardware friendly (802.11a)	Discrete FIR (LTE)	Hardware friendly (LTE)
LUT	8726 (3.99%)	4246 (1.94%)	15238 (6.97%)	7261 (3.32%)
FF	17004 (3.89%)	5905 (1.35%)	30135 (6.89%)	9844 (2.25%)
DSP48	258 (28.67%)	2 (0.22%)	514 (57.11%)	2 (0.22%)

Table 2. Peak to average ratio comparison for 802.11a and LTE matched filter outpus.

	802.11a	LTE
Discrete FIR	62	47.5
Hardware friendly	43	38

Through these experiments, it was possible to accommodate both detection algorithms on the same device, while consuming a small amount of FPGA resources, and more importantly keeping the detection accuracy intact. This resource saving can potentially be capitalized to accommodate multiple protocols on low end FPGAs as well.

5 Conclusions and Future Work

We have successfully demonstrated that a common hardware platform can be used to distinguish between 802.11 and LTE signals. The ADI RF front end receives samples at 20 MHz; which are downsampled to 1.92 MHz for LTE. The hardware design recognizes either the preambles in the 802.11 stream or the

Primary Synchronization Signal (PSS) in LTE with sufficient accuracy to determine which signal is being received. The RF front end uses common settings for parameters such as the automatic gain control mode.

In the future, we plan to take this base design into several different directions. Once the type of signal being received has been determined, we can download the receive chain for the rest of the processing onto the FPGA fabric. We plan to investigate using partial reconfiguration for this process. Our current implementation takes up a very small portion of the FPGA fabric, such that the first few steps for each receive chain could be included as part of the implementation without loss of data. In a typical coexistence scenario where multiple protocols work over the same channel, we plan to reuse the same components with different configurations in order to minimize resource utilization. It is our expectation that switching from one protocol to another should not create a negative impact on the receiver performance since FPGAs can be clocked at much higher rates than the baseband frequencies of such protocols. We also plan to investigate supporting other protocols, including 802.15.4 and Zigbee. The result will be an agile, flexible PHY layer platform that can support a variety of protocols, including some which have not yet been standardized.

Acknowlegdements. This research is funded in part with support from Mathworks.

References

1. Banerjee, A., Chatterjee, A.: Signature driven hierarchical post-manufacture tuning of RF systems. IEEE Trans. VLSI **23**(2), 342–355 (2015)
2. Bazrafshan, A., Taherzadeh-Sani, M., Nabki, F.: A 0.8–4-GHZ software-defined radio receiver with improved harmonic rejection. IEEE TCAS I **65**, 3186–195 (2018)
3. Dick, C., Harris, F.: FPGA implementation of an OFDM PHY. In: Asilomar Conference on Signals, Systems Computers, vol. 1 (2003)
4. Dinis, D.C., Cordeiro, R.F., Oliveira, A.S.R., Vieira, J., Silva, T.O.: A fully parallel architecture for designing frequency-agile and real-time reconfigurable FPGA-based RF digital transmitters. IEEE Trans. Microw. Theory Tech. **66**(3), 1489–1499 (2018)
5. Hogenauer, E.: An economical class of digital filters for decimation and interpolation. IEEE Trans. Acoust. Speech Signal Process. **29**(2), 155–162 (1981)
6. Jiao, X., Moerman, I., Liu, W., de Figueiredo, F.A.P.: Radio hardware virtualization for coping with dynamic heterogeneous wireless environments. In: Marques, P., Radwan, A., Mumtaz, S., Noguet, D., Rodriguez, J., Gundlach, M. (eds.) CrownCom 2017. LNICST, vol. 228, pp. 287–297. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76207-4_24
7. Machado, R.G., Wyglinski, A.M.: Software-defined radio: bridging the analog-digital divide. Proc. IEEE **103**(3), 409–423 (2015)
8. Onabajo, M., Silva-Martinez, J.: Analog Circuit Design for Process Variation-Resilient Systems-on-a-Chip. Springer, New York (2012). https://doi.org/10.1007/978-1-4614-2296-9
9. Setiawan, H., Ochi, H.: A low complexity physical-layer identity detection for 3GPP LTE. In: Advanced Communication Technology (ICACT). IEEE (2010)

10. Sexton, C., Kaminski, N.J., Marquez-Barja, J.M., Marchetti, N., DaSilva, L.A.: 5G: adaptable networks enabled by versatile radio access technologies. IEEE Commun. Surv. Tutor. **19**(2), 688–720 (2017)
11. Yksel, H., Yang, D., Boynton, Z., et al.: A wideband fully integrated software-defined transceiver for FDD and TDD operation. IEEE JSSC **52**(5), 1274–1285 (2017)