<http://www.diva-portal.org>

Postprint

This is the accepted version of a paper presented at *International Conference on Wireless Communications and Signal Processing (WCSP 2011)*.

Citation for the original published paper:

Zhong, Y., Tufvesson, F. (2011)

A Dual Input-channel Software Defined Receiver Platform for GSM WCDMA and Wi-Fi.

In: *Wireless Communications and Signal Processing (WCSP)*

<http://dx.doi.org/10.1109/WCSP.2011.6096830>

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-189193>

A Dual Input-channel Software Defined Receiver Platform for GSM WCDMA and Wi-Fi

Yang Zhong*, Fredrik Tufvesson

Dept. of Electrical and Information Technology

Lund University

Lund, Sweden

Email: yang.zhong@tfe.umu.se, fredrik.tufvesson@eit.lth.se

Abstract—In this paper a synchronized dual input-channel multi-mode Software Defined Radio receiver platform that we built originally is presented. The receiver platform compatible with the GSM, WCDMA, and Wi-Fi standards can detect and identify the surrounding base stations and access points. It features wide frequency range, high adaptive sampling rate and especially dual phase coherent receiving channels synchronized both in frequency and time. A detailed structure of the platform and the principle of the software decoders are shown in this paper. Performance of the receiver platform for signal reception is precise and stable. Benefiting from the flexibility of the receiver function, it is not only capable of various functions, such as cognitive radio development and distributed antenna system measurement for academic research, but a dynamic platform for testing new algorithms and ideas.

Keywords- *Software Defined Radio; dual input channels; multi-mode; synchronization; GSM; WCDMA; Wi-Fi*

I. INTRODUCTION

Recently, there is a trend that the radio receivers are made very generic to cover multiple radio bands and compatible with different communication standards. However, it is quite hard for a single receiver to follow an increasing number of communication standards while maintaining various receiver functions due to the hardware restrictions. Therefore, what is needed for future receiver is a flexible, universal radio platform for receive and transmit, which can be programmed to steer to any band, tune to a channel of any bandwidth, and receive any modulation [1]. Solving this problem, the Software Defined Radio (SDR) is a promising general receiver platform solution due to its high flexibility.

The SDR is a radio communication system where components that have been typically implemented in hardware are instead implemented in terms of software on a personal computer or embedded computing devices [2]. The idea of the SDR is to put Analog to Digital Converter (ADC) right after antenna stage so that all RF and baseband signal are digital [1]. Therefore, the SDR is built on a general hardware structure but different receiver functions are implemented in terms of software, which results in a general platform with more flexibility to work with multiple standards and functionalities. Since the users define the receiver functions in software, it is convenient to modify and customize the receiver functions.

Benefiting from the plug-and-play features, the SDR provides an open and convenient platform for various academic researches without bothering the physical radio components.

In this paper a synchronous dual input-channel SDR receiver platform compatible with the most desirable GSM, WCDMA and Wi-Fi standards is presented. The SDR platform can detect surrounding transmitters, i.e. base stations and access points, record the RF signal and decode in the downlink channel. It replaces a conventional hardware radio with programmable modules and offers researchers free space to test receiver functions based on its skeleton.

The paper is organized as follows: Section II details the receiver structures of the hardware configuration and the software block diagram; the Physical Layer specifications, synchronization and decoding methods for the GSM, WCDMA and Wi-Fi standards are described in Section III. In Section IV some results from the SDR platform and receiver performance analysis on time and frequency synchronization is presented. Conclusions are made in Section V.

II. RECEIVER ARCHITECTURE

The hierarchy of the SDR platform is shown in Fig.1. It is composed by hardware components and software including operating system which controls the modules and LabVIEW where receiver functions are programmed.

The SDR receiver platform we built is composed by two RF down converters, one Intermediate Frequency (IF) transceiver and a controller. All these components are installed on a chassis. Each RF downconverter covers an input frequency ranging from 9 kHz to 2.7 GHz with a real-time bandwidth of 20 MHz. All frequency content within ± 10 MHz

Figure 1. Platform Hierarchy

Figure 2. Receiver Chain

of the RF down converter's center frequency is transferred to the IF frequency at 15 MHz [3]. Each input channel on the IF transceiver featuring 14-bit resolution has an ADC with a sampling capability up to 100 MSamples/s, and followed by a Digital Down Converter (DDC) with a maximum bandwidth of 20 MHz [4]. Both input channels of the IF transceiver receive the IF signal from the RF downconverters and convert the signal into baseband complex samples with an adaptive oversampling rate. There is also a FPGA module on this transceiver which can be exploited for powerful digital signal processing and advanced receiver functions. The operating system with the LabVIEW is installed on the controller.

The superheterodyne receiver structure is applied for translating the received RF signal via IF to the baseband. Fig. 2 illustrates the receiver chain. The downlink signal is first received and filtered in both RF down converters. After being amplified, the received RF signal is translated to the IF transceiver where the signal in either channel is digitized and the in-phase and quadrature components are produced for each channel. Adjustable sampling rate in the complex output signal is realized through decimation.

Perfect frequency synchronization should be maintained among the local oscillators on the two RF down converters and IF transceiver to realize phase coherent input channels. The solution is, as shown in Fig. 2, sharing the local reference clock on one of the RF downconverters with the other RF downconverter and the IF transceiver (due to the high stability on the internal oscillator on the RF down converter). The frequency stability of the time base is ± 20 ppb [3]. The reference clock of channel 0 is exported to override the other reference clock signal on channel 1 and the IF transceiver's local reference clock (shown as dashed in Fig. 2) so that all the RF components are controlled by the same local oscillator. Timing synchronization for both input channels is achieved by programming in the block diagram so that both channels will record the signal simultaneously after being triggered.

Three major functions are realized in this platform: real time spectrum measurement, RF signal recording, and downlink signal decoding. The first two functions are achieved by adding additional software receiver modules of the Fast Fourier Transformation (FFT) and data-saving functions to the receiver respectively. A panel is created as the interface for users to control the receiver platform. Fig. 3 shows the block diagram for the receiver software modules.

Figure 3. Structure of Block Diagram

III. PRINCIPLES

A. Brief on Specifications

For the considered communication standards, the broadcast channel carries identity information for distinguishing one base station from another. In GSM standard the base station identity information is transmitted in the Synchronization Channel (SCH) [5][6][7], while the UMTS standard separates base stations use the scrambling code [8]. Access Points (APs) are uniquely identified by the Media Access Control (MAC) address in Wi-Fi standard.

The downlink frequency allocations, bandwidth, and the corresponding modulation techniques for the broadcasting channels in the GSM [9][10], WCDMA [11], and Wi-Fi [12] are summarized in Table I.

B. Initial Cell Search

The so-called initial cell search refers to the process that the SDR platform searches through the spectrum and locks to the carrier frequency with the highest transmission power. The initial cell search procedure in our SDR platform is implemented according to the GSM, UMTS, and WLAN specifications. The receiver platform first senses the strongest beacon channel through the corresponding frequency range and then tunes itself to it. The decoders receive the baseband signal

Table I. Downlink Specifications for the Physical Layer

	GSM900	UMTS	Wi-Fi
Freq. Span	925 ~ 960 MHz	2.11 GHz ~ 2.17 GHz	2.4 ~ 2.5 GHz
Bandwidth	200 kHz	~ 5 MHz	~20 MHz
Modulation	GMSK ¹	DSSS ²	DPSK ³
Bit Rate/ Chip Rate	270.8 kbps	3.84 Mcps	1 or 2 Mbps*

1. GMSK: Gaussian Minimum Shift Keying

2. DSSS: Direct Sequence Spread Spectrum

3. DPSK: Differential Phase Shift Keying

* Data rate may vary for package data

from RF signal recorder and execute synchronization and decoding procedures.

C. Synchronization

Time synchronization in received samples of the GSM and WCDMA is accomplished using matched filter that matched to specific training sequence or downlink synchronization code defined in the SCH correspondingly.

The SCH for GSM modulated with GMSK scheme contains a 64-bit training sequence for time synchronization and two 39-bit payloads where the base station identity information such as Base transceiver Station Identity Code (BSIC) is embedded [5][6][7]. Channel estimation in the GSM receiver is implemented using the training sequence in SCH.

The WCDMA downlink signal is channelized and scrambled with an exception of SCH; a base station is identified by the scrambling code serving the cell. The SCH in WCDMA includes two sub-channels: the Primary Synchronization Channel (P-SCH) and the Secondary Synchronization Channel (S-SCH), which both have 256 chips long synchronization code [13]. The P-SCH and the S-SCH are transmitted parallel in time and are located in the beginning of each timeslot. Therefore, synchronization is achieved in three steps: first, slot synchronization using P-SCH, then the frame synchronization using S-SCH, and finally search the downlink scrambling code serving the current cell. The code group of the serving scrambling code is indicated by the codeword given by the Secondary Synchronization Code (SSC) within the frame. 15 out of the 16 SSCs generate 64 secondary synchronization code words that correspond to 64 primary scrambling code groups, where each has 8 primary scrambling codes [14]. When the SSC is determined, the serving scrambling code can be found from the code group that SSC indexed.

Wi-Fi devices use Direct Sequence Spread Spectrum (DSSS) technique to transmit low data rate packages on the wireless channel. The frame structure for 802.11b standard is shown in Fig. 4 [12]. The Physical Layer Convergence Procedure (PLCP) preamble and header, which are transmitted using DBPSK at 1Mb/s, provide synchronization and demodulation information within the package. The MAC address can be filtered out from the MAC Protocol Data Unit (MPDU).

Figure 4. Frame Structure of Wi-Fi

IV. RESULTS AND ANALYSIS

A. Experimental Results

Fig. 5 shows the power spectrum of a GSM base station at 939.8 MHz during the timeslot of the Frequency Correction Burst (FCB). The FCB has 148 zeros in the burst, which creates an obvious frequency spike 67.7 kHz above the carrier frequency after modulated. It is also used for fine tune the local oscillator frequency on the mobile terminals. By decoding the SCH, the country code from the base station is 6, which is the code assigned to Sweden [7], and the ID code is 2.

Figure 5. Spectrum of a Beacon Base Station

In WCDMA, one of 512 primary scrambling codes, which are further divided into 64 groups, can be selected to serve a cell [14]. After achieve synchronization, we have found the downlink scrambling code serving our campus to be the 7th primary scrambling code in code group 22.

When transmitting identity information, APs works under 802.11b mode and modulates the packages using spread spectrum techniques. The spectrum of a Wi-Fi access point working under DSSS mode is shown in Fig. 6. The decoded MAC address by our receiver platform matches the ones printed on the back plane of the APs perfectly.

Figure 6. Spectrum of a WLAN Access Point

Channel estimation is also available in our decoder module. The estimated channel impulse response can be extracted from the measurement data using the SCH in GSM and WCDMA. Fig. 7 shows a Power Delay Profile (PDP) which is estimated in the WCDMA downlink after synchronization.

Figure 7. Estimated Channel for WCDMA downlink
[Oversampling Rate = 4]

B. Performance Analysis

High frequency stability is significant for the receiver platform. In order to verify the frequency accuracy in our SDR platform, we applied frequency offset to the received FCB, since it is generated by an extremely stable oscillator on the base station. The phase change in FCB, which was modulated by continuous phase modulation, is an ascending slope. After we introduce a frequency offset with a negative frequency of $f_{\text{offset}} = -67.708$ kHz to the samples in the FCB, the local frequency on our SDR platform is precise if there is no phase drift in the offset data samples. Fig. 8 shows the continuous phase change of the data samples in a randomly selected FCB after we apply the frequency offset. For comparison, linear regression is used to check the phase change ratio. Here we see from the regression equation given by Matlab, the frequency drift through the timeslot after offset is negligible. Therefore, the local frequency on our SDR platform performs very stable.

Timing synchronization for signal recording in both input channels is also achieved perfectly. We use the SCH channels in the GSM and WCDMA respectively to check if the same timeslot starts at the same sample in each channel. The results

Figure 8. FCB after frequency offset
[Oversampling Rate =6]

show that the RF signal recording is triggered in both of the channels simultaneously and continuous recording is also guaranteed, i.e. no data samples are missing during the recording period. Phase coherence in input channels are also verified by checking the phase error between input channels.

V. CONCLUSIONS

Hundreds of downlink signal measurements have been made for testing the validity and reliability of the hardware components and the software modules in our SDR receiver platform. Based on experimental results, the synchronization in both of the input channels in the SDR receiver is well accomplished under the current hardware structure and software programming. The SDR receiver is reliable in the signal recording and is capable of providing an adaptive oversampling rate for signal recording under the GSM, WCDMA and Wi-Fi standards. The decoders implemented according to the relevant technical specifications working with the signal recording function are able to provide any of the GSM base station ID codes, WCDMA downlink scrambling codes, and the MAC address of APs, which are the unique identifications of the transmitters. Advanced digital processing functions can be developed using the FPGA module in the future.

REFERENCES

- [1] A.A. Abidi, "The Path to the Software-Defined Radio Receiver," IEEE J. Solid-State Circuits, vol. 41, no. 6, pp. 984-966, May 2007.
- [2] M. Dillinger, K. Madani and N. Alonistioti, "Software Defined Radio: Architectures, Systems and Functions," John Wiley & Sons Ltd., pp. xxxiii, 2003
- [3] <http://sine.ni.com/nips/cds/view/p/lang/en/nid/11535>, accessed in April 2010
- [4] <http://sine.ni.com/nips/cds/view/p/lang/en/nid/207050>, accessed in April 2010
- [5] 3GPP TS 45.002, "Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path. Ver. 9.2.0, Release 9."
- [6] R. Steele, C. Lee and P. Gould, "GSM, cdmaONE and 3G Systems," John Wiley & Sons, 2001.
- [7] 3GPP TS 23.003, "Digital cellular telecommunication system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification. Ver. 8.6.0, Release 8."
- [8] 3GPP TS 25.213, "Universal Mobile Telecommunications System (UMTS); Spreading and modulation (FDD). Ver. 9.1.0, Release 9."
- [9] 3GPP TS 45.005, "Technical Specification Group GSM/EDGE Radio Access Network; Radio transmission and reception. Ver. 9.0.0, Release 9."
- [10] R. Steele and L. Hanzo, "Mobile Radio Communications 2nd edition," John Wiley & Sons, 1996.
- [11] 3GPP TS 25.101, "Technical Specification Group Radio Access Network; User Equipment (UE) radio transmission and reception (FDD). Ver. 9.0.0, Release 9."
- [12] IEEE Std 802.11-2007, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications."
- [13] H. Holma and A. Toskala, "WCDMA For UMTS: Radio Access For Third Generation Mobile Communications", John Wiley & Sons, 2000.
- [14] 3GPP TS 25.213, "Universal Mobile Telecommunications System (UMTS); Spreading and modulation (FDD). Ver. 9.1.0, Release 9."