SOFTWARE IMPLEMENTATION OF IEEE 802.11B WIRELESS LAN STANDARD

Suyog D. Deshpande
(Sr. MTS: HelloSoft, Inc, San Jose, CA, USA; suyog@hellosoft.com)

ABSTRACT

Software-Defined Radio (SDR) is a rapidly evolving technology that is receiving enormous recognition and generating widespread interest in the telecommunication industry. Over the last few years, analog radio systems are being replaced by digital radio systems for various applications in military, civilian and commercial areas. In addition to this, programmable hardware modules and high performance Digital Signal Processors (DSPs) are increasingly being used in digital radio systems at different functional levels. SDR technology facilitates implementation of some of the functional modules in a radio system such as modulation/demodulation, coding, signal generation, and link-layer protocols in software. This helps in building reconfigurable software radio systems where dynamic selection of parameters for each of the above-mentioned functional modules is possible. A complete hardware based radio system has limited utility since parameters for each of the functional modules are fixed. A radio system built using SDR technology extends the utility of the system for a wide range of applications that use different protocols and modulation/demodulation techniques.

In this paper, we discuss the software implementation details of IEEE 802.11b Wireless LAN (WLAN) standard on Texas Instruments' TMS320C6416 DSP based hardware platform.

1. INTRODUCTION

The term Software-Defined Radio refers to the use of software-programmable hardware to provide flexible radio solutions. The concept behind the technology is that it will provide software control of radio functionality. Traditional radio designs are constructed of fixed analog or digital components. Such designs also are custom built for each application. By comparison, SDR technology offers an inherent flexibility and serves as the main incentive to engage in this methodology.

SDR is a rapidly evolving technology that is receiving enormous recognition and generating widespread interest in the telecommunication industry. It has generated tremendous interest in wireless communication industry for its wide range economic and deployment benefits. It facilitates implementation of some of the functional modules in a radio system such as modulation/demodulation, coding, signal generation, and link-layer protocols in software. This helps in building reconfigurable software radio systems where dynamic selection of parameters for each of the above-mentioned functional modules is possible. It can be used to implement a wide range of radio applications like WLAN, Bluetooth, and Cellular wireless (GSM, GPRS, CDMA, and UMTS) standards.

In this paper, we discuss the software implementation details of IEEE 802.11b WLAN standard on Texas Instruments' TMS320C6416 DSP based hardware platform. The problem associated with the physical layer (PHY) of 802.11b standard is that it requires very high computational power. One way to achieve this efficiency is by implementing the PHY completely in hardware. Introduction of high performance DSPs and our IP rich PHY algorithms [1] have made it possible to run the entire 802.11b PHY on a single DSP. The 802.11b Medium Access Control (MAC) layer software (including WEP encryption) runs on the ARM core. This software implementation approach provides ease of design modifications at any stage of the product cycle and also in the field even after deploying the solution. It also facilitates addition of new features into the deployed solution with minimal changes in the software architecture. Most importantly it gives great deal of flexibility to make custom changes at both PHY and MAC layers, for security related applications in military, civilian and commercial areas.

The important aspects of SDR technology and its salient features are presented in section 2. A brief description about current WLAN standards that are widely used in commercial, home, office, and industrial applications is given in Section 3. Section 4 describes the software implementation details of IEEE 802.11b WLAN standard on Texas Instruments' TMS320C6416 DSP based hardware platform. Finally, the concluding remarks are presented in section 5.

2. SOFTWARE DEFINED RADIO TECHNOLOGY

SDR technology is defined as "radios that provide software control of a variety of modulation techniques, wide-band or narrow-band operation, communications security functions (such as hopping), and waveform requirements of current & evolving standards over a broad frequency range." [2]

SDR has generated tremendous interest in the wireless communication industry for the wide range economic and deployment benefits it offers for military, civilian and commercial applications. The momentum of SDR in defense applications has been spearheaded by the United States Government's JTRS program. The program requirement calls for "affordable, high-capacity tactical radios that meet the bandwidth needs of various echelons. Therefore, a software-programmable and hardware-configurable digital radio system is required to provide increased interoperability, flexibility, and adaptability to support the varied mission requirements of the war fighters". Some of the key features of SDR technology are

Co-existence and Dynamic Configurability: SDR allows co-existence of multiple software modules implementing different standards on the same system allowing dynamic configuration of the system by just selecting the appropriate software module to run. It facilitates implementation of future-proof, multi-service, multi-mode, multi-band, multi-standard terminals and infrastructure equipment.

Connectivity: SDR enables implementation of air interface standards as software modules and multiple instances of such modules that implement different standards can co-exist in infrastructure equipment and handsets. This helps in realizing global roaming facility.

One of the major incentives for using the SDR technology is to overcome the problems faced by the wireless communication industry due to implementation of wireless networking infrastructure equipment and terminals completely in hardware.

Commercial wireless network standards are continuously evolving from 2G to 3G and then further onto 4G. Each generation of networks differ significantly in link-layer protocol standards causing problems to subscribers, wireless network operators and equipment vendors. The air interface and link-layer protocols differ across various standards like WLAN, Bluetooth, GSM, GPRS, CDMA, and UMTS. This problem has inhibited the deployment of global roaming facilities causing great inconvenience to subscribers who travel frequently from one continent to another. Subscribers are forced to buy new handsets whenever a new generation of network standards is deployed. Wireless network operators face problems during migration of the network from one generation to next due to presence of large number of subscribers using legacy handsets that may be incompatible with newer generation network.

Handset vendors face problems in building viable multi-mode handsets due to high cost and bulky nature of such handsets. The network operators also need to incur high equipment costs when migrating from one generation to next. They also face deployment issues while rolling-out new services/features to realize new revenue-streams since this may require large-scale customizations on subscribers' handsets. Equipment vendors face problems in rolling out newer generation equipment due to short time-to-market requirements.

SDR technology enables implementation of radio functions in networking infrastructure equipment and subscriber terminals as software modules running on a generic hardware platform. This significantly eases migration of networks from one generation to another since the migration would involve only a software upgrade. Further, since the radio functions are implemented as software modules, multiple software modules that implement different standards can co-exist in the equipment and handsets. An appropriate software module can be chosen to run (either explicitly by the user or implicitly by the network) depending on the network requirements. This helps in building multi-mode handsets and equipment resulting in ubiquitous connectivity irrespective of underlying network technology used.

However, SDR technology has some drawbacks like higher power consumption, higher processing power (MIPS) requirement and higher initial costs. SDR technology may not be suitable for all kinds of radio equipment due to these factors. For e.g., SDR technology may not be appropriate in pagers while it may offer great benefits when used to implement base-stations. Hence these factors should be carefully considered before using SDR technology in place of a complete hardware solution.

3. IEEE 802.11 WLAN STANDARDS

Currently, three WLAN standards are in wide commercial, home, office, and industrial use: 802.11a, 802.11b, and the recently IEEE-ratified 802.11g. Several chip manufacturers are building chipsets that work with both 11b and 11g, and a smaller number are building a chip capable of working on both 11a and 11g or with 11a, 11b, and 11g.

802.11b products, available since 1999, operate in the unlicensed 2.4-gigahertz (GHz) ISM (Industrial Scientific and Medical) radio spectrum; support average data rates of 1, 2, and 5.5 megabits per second (Mbits/s); and can achieve a maximum of 11 Mbits/s [3].

802.11a products, available since 2002, operate in unlicensed portions of the 5-GHz radio spectrum, with maximum achievable data rates up to 54 Mbits/s [4].
802.11g products operate in the same 2.4-GHz radio spectrum that 802.11b products operate in and therefore provide backward compatibility with them, but their higher data rates resemble those of 802.11a products. The IEEE ratified the 802.11g standard [5] on 12 June 2003 after three years of working-group deliberations. 11g will now undergo a lengthy period of testing and certification, even though 11g-enabled products are already flooding the market.

The frequency band in use constitutes one key difference among these three standards. The 11b and 11g standards both use the 2.4-to-2.4835-GHz band, and each runs on 3 channels only; 11a, which uses the 5.725-to-5.850-GHz band, is currently capable of operating with up to 12 channels. This capability potentially makes 802.11a valuable for large-scale enterprise installations: More transmission channels in 11a also support a higher density of users per access point in a given space than either 11b or 11g supports. Because 11a uses a frequency band different from that of 11b and 11g, 11a is not backward compatible with either 11b or 11g.

Data rate constitutes another key difference among these three standards: The 11b standard provides a much lower data-throughput performance than do the 11a and 11g standards. Implementations of 11a and 11g provide up to a maximum best data level of 54 Mbits/s; 11b is limited to 11 Mbits/s. In other words, 11a and 11g transfer data roughly five times faster than does 11b. However, actual data rates of data communications networks are lower than nominal maximum rates because of packet overhead. And wireless packet networks suffer from interference, which further erodes actual data rates.

Different wireless LAN standards also rely on different modulation techniques and the implementation complexity depends on the modulation scheme being used. Both 11a and 11g products rely on orthogonal frequency-division multiplexing (OFDM). OFDM is what gives the two standards a higher throughput than that of 802.11b, which uses the less-efficient direct-sequence spread-spectrum (DSSS) method.

Since full software implementation of 11a or 11g PHY layers is not realizable, our discussion will be focused on implementation details of 11b PHY only.

4. 802.11B IMPLEMENATION DETAILS

This section describes the software implementation aspects of IEEE 802.11b WLAN standard on Texas Instruments' TMS320C6416 DSP based hardware platform. The problem associated with 802.11b PHY is that it requires very high computational power. One way to achieve this efficiency is implementing it completely in hardware. Almost all standard 11b chipsets implement 11b PHY in hardware. The MAC is implemented as a combination of hardware and software. This is very efficient implementation in terms of power consumption and die size area. But this implementation does not provide any flexibility in making custom changes to both PHY and MAC layers.

Our IP rich PHY algorithms in conjunction with high performance DSPs have made it possible to run the entire 802.11b PHY on a single TMS320C6416 DSP. The 802.11b MAC software including WEP encryption runs on the ARM core. This software implementation approach provides ease of design modifications at any stage of the product cycle and also in the field even after deploying the solution. It also facilitates addition of new features into the deployed solution with minimal changes in the software architecture. Most importantly it gives great deal of flexibility to make custom changes at both PHY and MAC levels, for security related applications in military, civilian and commercial areas.

To establish the proof of concept and demonstrate interoperability of the 802.11b technology, we have developed a reference board centered on TI TMS320C6416 and ALTERA's Excalibur FPGA chip. A brief block diagram of the reference board is shown below.

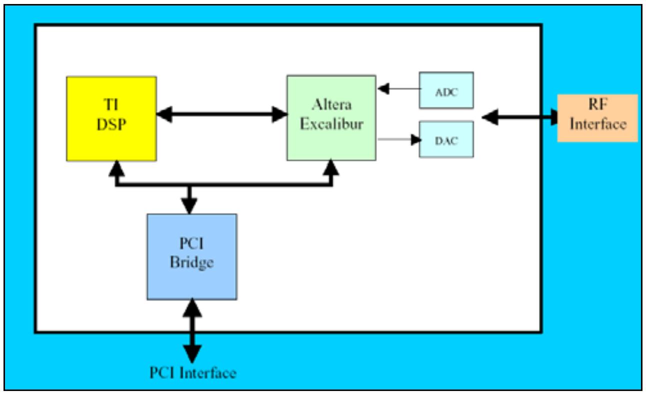

Figure 1: WLAN Reference Design Block Diagram

The IP rich PHY algorithms and optimized implementation on TMS320C6416 has made is possible to run the entire IEEE 802.11b PHY on a single TMS320C6416 DSP chip running at 600 MHz (without using any of the available co-processor engines). The 802.11b MAC including WEP encryption runs on the ARM core that is present inside the Excalibur. Communication between the MAC and PHY as well as the communication between the RF Front end and PHY is aided by the glue logic implemented on the Excalibur FPGA.

The transmitter architecture for 1 & 2 Mbps is shown in Figure 2. The bit stream received from the MAC is passed through 32-bit CRC and Scrambler. Scrambler whitens the incoming bit stream. The whitened bits are differentially encoded using DBPSK or DQPSK modulation schemes. The resulting symbol is spread using 11 chip Barker sequence. The Barker spreaded symbol is up sampled by a factor of 2 and given to 8-bit DACs operating at 22 MHz.

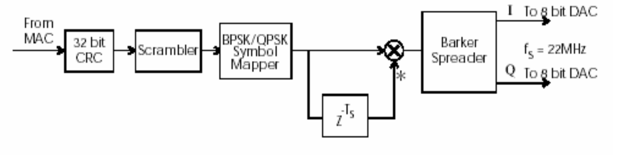

Figure 2: Block Diagram for 1 & 2 Mbps Transmitter

The transmitter architecture for 5.5 & 11 Mbps transmitter is shown in Figure 3. It is same as that of 2 Mbps data rate with the only difference in the spreading sequence. It is a complex sequence of length 8 (CCK code). For 5.5 Mbps data rate, 2 bits are used to select one of 4 CCK codes where as for 11 Mbps data rate, 6 bits select one of 64 possible CCK codes.

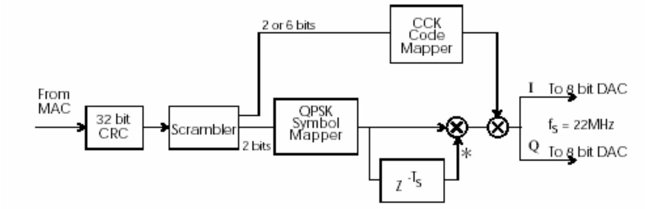

Figure 3: Block Diagram for 5.5 & 11 Mbps Transmitter

The receiver architecture for 1 & 2 Mbps data rates with Barker despreading is shown in Figure 4. The signal received from the receive antenna is down converted from RF to Baseband. The analog I and Q samples are fed to 8-bit ADCs operating at 22 MHz. The RAKE engine combines up to 8 paths at 22 MHz in a very efficient way to enhance the receiver performance. Decision Feedback Equalizer (DFE) is also included in the receiver to minimize the effect of inter-symbol-interference (ISI) thereby reducing the packet error rate (PER).

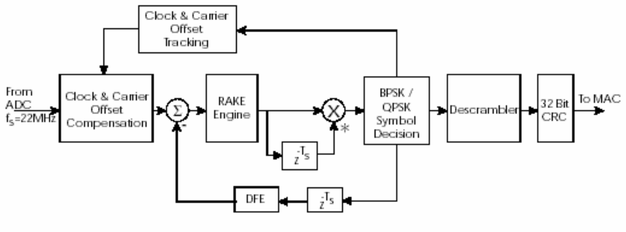
Clock & Carrier Offset Tracking
From ADC f_s=22MHz
Clock & Carrier Offset Compensation
Σ
RAKE Engine
z^{-T_s}
*
BPSK / QPSK Symbol Decision
Descrambler
32 Bit CRC
To MAC
DFE
z^{-T_s}

Figure 4: Block Diagram for 1 & 2 Mbps Receiver

The receiver architecture for 5.5 & 11 Mbps data rates with CCK despreading is given in Figure 5. Matched filter interpolator modules serves the purpose of matched filtering and interpolating the chip sampling instant to generate output at 11 MHz rate. An efficient implementation of the correlation banks, which significantly reduces the computational complexity, is through Fast Walsh Transform (FWT) algorithm.

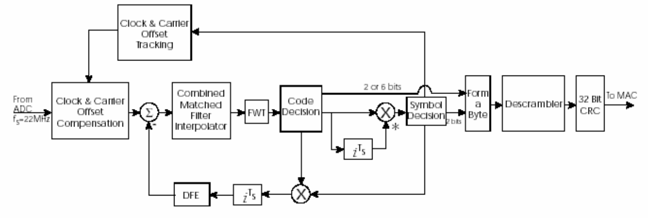

Figure 5: Block Diagram for 5.5 & 11 Mbps Receiver

The cycle count requirements for data mode receiver modules are given in Table 1.

Module name	**Cycles 1& 2 Mbps**	**Cycles 5.5 Mbps**	**Cycles 11 Mbps**
Rotor	065	55	55
CMF	155	90	90
FWT + BP	-	70	115
De-Spreader	025	-	-
Dqpsk Demod	025	25	25
Symbol Decision	-	20	20
DFE	015	25	25
CRC	015	15	15
De-Scrambler	010	10	10
Fsm + Overheads	090	70	70
Total	**400/600**	**380/436**	**425/436**

Table 1: Cycle Count for Data Mode Receiver Modules

IEEE 802.11b PHY is completely implemented in TMS320C6416 running at 600 MHz and is arguably the world's first single DSP solution. Given the very short symbol time of 11b PHY (1 micro-sec for 1 & 2 Mbps and 727 nano-sec for 5.5 and 11 Mbps), the challenge is to fit the entire computationally complex algorithms in real-time. The C6000 family of TI with the VelociTI architecture and our IP rich physical layer algorithms address the demands of this high processing requirement. At clock rate of 600 MHz, the TMS320C6416 DSP can process information at a rate of 4800 MIPS. In addition to clock rate, more work can be done each cycle with the VelociTI.2 extensions to the VelociTI architecture allowing a maximum of 8 instructions per clock cycle. These extensions include new instructions to accelerate performance in key applications and extend the parallelism of the architecture. The complete code is written with a mix of ANSI C and assembly coding. Real-time critical modules are hand-coded in assembly and the non real-time modules are in 16-bit fixed point ANSI C.

Although, TMS320C6416 DSP provides many peripherals, we have used only the following - EDMA to receive data in real-time from the ADC's and transmit data to the DACs, McBSP for communication between the MAC (on the ARM Processor) and the PHY (on the C64x) and GPIO for general debugging and external interrupt generation.

The major drawbacks of this approach are higher power consumption, higher processing power (MIPS) requirement and higher costs. This approach may not be suitable for all kinds of radio equipment due to these factors but may offer great benefits when used to implement base-stations.

5. CONCLUSIONS

In this paper, we discussed the software implementation details of IEEE 802.11b WLAN standard on Texas Instruments' TMS320C6416 DSP based hardware platform. This approach provides ease of design modifications at any stage of the product cycle and also in the field even after deploying the solution. It also facilitates addition of new features into the deployed solution with minimal changes in the software architecture. Most importantly it gives great deal of flexibility to make custom changes at both PHY and MAC layers, for security related applications in military, civilian and commercial areas.

6. REFERENCES

[1] HelloSoft's 802.11b PHY Layer – Detailed Design Document

[2] Software-Defined Radio (SDR) Forum (www.sdrforum.com)

[3] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, ANSI/IEEE Std 802.11b-1999 (Supplement to ANSI/IEEE Std 802.11, 1999 Edition)

[4] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band, ANSI/IEEE Std 802.11a-1999 (Supplement to ANSI/IEEE Std 802.11, 1999 Edition)

[5] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, ANSI/IEEE Std 802.11g-2003