Abstract—Network Layer with Radio networks High Performance Platform™ being developed under the NSF NeTS ProWIN (programmable wireless networks) grant CNS-0435370. The network-centric cognitive radio architecture under consideration in this project is aimed at providing a high-performance platform for experimentation with various adaptive wireless network protocols ranging from simple etiquettes to more complex ad-hoc collaboration. Particular emphasis has been placed on high performance in a networked environment where each node may be required to carry out high throughput packet forwarding functions between multiple physical layers. Key design objectives for the cognitive radio platform include: 1. multi-band operation, fast frequency scanning and agility; 2. software-defined modem including waveforms such as DSSS/QPSK and OFDM operating at speeds up to 50 Mbps; 3. packet processor capable of ad-hoc packet routing with aggregate throughput 100 Mbps; 4. Spectrum policy processor that implements etiquette protocols and algorithms for dynamic spectrum sharing.

I. COGNITIVE RADIO ARCHITECTURE & DESIGN

The cognitive radio prototype’s architecture is based on four major elements: (1) MEMS-based tri-band agile RF front-end, (2) FPGA-based software defined radio (SDR); (3) FPGA-based packet processing engine; and (4) embedded CPU core for control and management. These components will be integrated into a single prototype board which leverages an SDR implementation from Lucent Bell Labs as the starting point. A proof-of-concept demonstration board is planned for the end of year 2 (Sept 2006), and several prototype boards will full functionality are expected to be ready at the end of year 3 (Sept 2007).

The network-centric cognitive radio architecture under consideration in this project is aimed at providing a high-performance platform for experimentation with various adaptive wireless network protocols ranging from simple etiquettes to more complex ad-hoc collaboration. The basic design provides for fast RF scanning capability, an agile RF transceiver working over a range of frequency bands, a software-defined radio modem capable of supporting a variety of waveforms including OFDM and DSSS/QPSK, a packet processing engine for protocol and routing functionality, and a general purpose processor for implementation of spectrum etiquette policies and algorithms. The proposed architecture along with the associated partitioning of design/prototyping responsibilities between Rutgers, GA Tech and Lucent is shown in Figure 1.1 below.

Figure 1.1 - Architecture of network-centric cognitive radio networks platform

In the original proposal, we identified the need for a baseband and network processor board that would interface to the RF front-end and allow dynamically reconfigurable software and hardware implementations of multiple wireless links supporting individual data rates up to 50Mb/s and a maximum aggregate data rate of 100 Mbs. It was expected that this board would contain some mix of DSP and FPGA block together with their required memories. At the first coordination meeting in 4Q2004, we made a decision to avoid the use of DSP’s because of the difficulty associated with programming these devices. Rather, we decided to use a combination of FPGA for hardware implementation and embedded RISC for software implementation. Embedded RISC cannot match the cost and power efficiency of a DSP, but it was felt that ease of programming was of more importance in an experimental platform—especially one that would be used by students. The group also decided to aim for triband(700 MHz, 2.4 GHz and 5.1 GHz) capabilities using a novel MEMS device from GA Tech. This was viewed as an important flexibility feature for an experimental platform of this type. The analog front-end would also support two channels, one for measurement and one for data, with bandwidths selectable in 1MHz increments.

A. Hardware architecture

Even though the prototyping effort is focused on an FPGA-based design, we are also exploring the architectural benefits of custom integrated circuitry, primarily related to power consumption and the silicon area, which are important performance parameters for hardware designs used in...
mobile/portable platforms. The approach we have chosen to take involves identifying the hardware architecture appropriate for low-power configurable design based on heterogeneous blocks (i.e., blocks that are highly optimized for a particular function, yet flexible enough to support a variety of configuration parameters) as a compromise for the tradeoff between programmability and power consumption/area. In addition to fast prototyping, the additional benefits of using modern FPGAs (e.g., Xilinx Virtex 4) are the availability of highly optimized features implemented as non-standard configurable logic blocks (CLB) like phaselocked loops, low-voltage differential signal, clock data recovery, lots of internal routing resources, hardware multipliers for DSP functions, memory, programmable I/O, and microprocessor cores. These advantages simplify mapping from hierarchical blocks to FPGA resources.

The hardware design effort started with an evaluation of architectures presently available for base band SDR processing at rates of 50-100 mbps. All these architectures use massive hardware parallelism to sustain high data rate. We also looked at the base band processing requirements of different wireless standards such as 802.11a/b, Bluetooth and WCDMA, and found that different stages of base band processing have very different hardware needs. Thus, using a generic hardware design leads to inefficient usage of chip area and power consumption. As a result, we proposed a “heterogeneous block-based architecture” which would help implement SDR baseband processing in an efficient way. An additional feature is the ability to efficiently reconfigure blocks in a few clock cycles to facilitate fast changeover between multiple SDR physical layers.

B. Heterogeneous block-based architecture

The heterogeneous-block based architecture (see Figure 1.2 below) combines a general microprocessor with special purpose hardware blocks. The microprocessor containing multiplier/accumulator units handles control intensive operations such as channel estimation, synchronization, and programming and interconnection of the heterogeneous blocks, while data intensive operations are handled by the heterogeneous blocks. The following heterogeneous-blocks have been identified:

1. Channel utilization Block: A configurable multi-stage filter used to select a sub-band and/or decimate the input signal for different standards
2. FFT/MWT Block: A configurable architecture which can handle FFT operations used in OFDM and also handle the modifier Walsh transform used in 802.11b
3. Rake Block: A generic four finger Rake accelerator for channel estimation, de-spreading in DS/SS and CDMA.
4. Interleaver Block: Using a block-based memory and multiplexer-based address handler, a multi-mode architecture can handle de-interleaving for different standards.
5. Data and Channel Encoding/Decoding Block: A configurable architecture can handle both Viterbi (for 802.11a) and Encoder/Turbo Decoder (for WCDMA). Both the Data and Channel Encoder have a similar connection pattern, but only the Data Encoder needs feedback. A common block is proposed which can be configured in one clock cycle to perform either of the two functionalities.

6. Detection and Estimation Block:
   Common interference detection block.

![Figure 1.2 - Heterogeneous Blocks based Baseband Processor Architecture](image)

The hardware design effort started with an evaluation of architectures presently available for base band SDR processing at rates of 50-100 mbps. All these architectures use massive hardware parallelism to sustain high data rate. We also looked at the base band processing requirements of different wireless standards such as 802.11a/b, Bluetooth and WCDMA, and found that different stages of base band processing have very different hardware needs. Thus, using a generic hardware design leads to inefficient usage of chip area and power consumption. As a result, we proposed a “heterogeneous block-based architecture” which would help implement SDR base band processing in an efficient way. An additional feature is the ability to efficiently reconfigure blocks in a few clock cycles to facilitate fast changeover between multiple SDR physical layers.

Ongoing work is aimed at creating a implementation of the above SDR design using available FPGA boards and conducting evaluations on flexibility and performance. The packet processing engine’s architecture will also be considered during the remainder of this reporting year. The goal is to have both SDR and packet processor FPGA implementations tested and evaluated by the end of 2005.

II. Spectrum Scanning Algorithms

An important aspect of the cognitive radio platform is its ability to opportunistically use portions of the spectrum that are not being used, which requires the ability to efficiently scan spectrum usage. Furthermore, it is very important to detect and identify types of interference that the platform is facing. This becomes increasingly difficult for arbitrary radiosystems. Thus we can focus on an OFDM radio platform because it allows a simple characterization of interference in terms of the OFDM sub carriers. A project on spectrum detection algorithms was carried out in order to understand the computational complexity and response times for the scanning receiver. In order to solve this detection and estimation problem, we used an eigen value decomposition of the sample covariance matrix of the received signal. This analysis was performed using...
computer simulations for two common sources of interference: a microwave oven and a Bluetooth radio. Simulations carried out show that the influence of an interfering signal on the OFDM system depends on the power of the interfering signal and the data rate in the OFDM system (this system supports the following data rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps). As expected, the BER of the system increases with the increasing power of the interfering signal and increasing data rate of the OFDM system. In the presence of the microwave oven signal, only one of the 64 eigen values of the covariance matrix is affected. In the presence of the Bluetooth radio interference, several eigen values will be affected. The number of affected eigen values in this case is proportional to the power of the interfering signal. In the future work, we will examine how multiple radios can collaborate in the detection of interferers, including the development of protocols for the exchange and aggregation of measurements.

III. ADAPTIVE NETWORK PROTOCOLS

In parallel to SDR and packet processor design work described above, a project has been started on adaptive network protocols and related algorithms. In particular, we are studying the concept of an adaptive wireless network bootstrapped from the CSCC etiquette protocol previously developed at WINLAB. The CSCC protocol (which uses a broadcast beacon mechanism to inform neighboring radio stations) is being extended to include information necessary for self-organization into a collaborative network of cognitive radios. Information on transmit power, PHY speeds, channel quality and aggregated routing information is added to the beacon to facilitate self-organization. This concept is shown in Figure 1.3.

Figure 1.3 - Concept for CSCC-based self-organization
In a cognitive radio network

A preliminary evaluation of the protocol concepts is planned for year 2 of the project using a GNU radio extension to the ORBIT radio grid test bed. A GNU radio kit has been procured and an RF front end module is being developed for subsequent use as software-defined ORBIT radio node extension.

IV. SECURITY

One of the factors which should be considered during design process of CRN emergency network is security of the network infrastructure and security of transmitted information. Without proper network security, terrorists responsible for the disaster would be able to eavesdrop emergency information and utilize it for future attacks. Moreover, some of the possible methods of attacks on CRN include:

**Licensed user emulation attack:** Because cognitive radios cannot be completely sure whether a licensed spectrum is free and available for transmission, they simply defer from licensed bands and utilize other non-licensed parts of the bandwidth if they are not sure if it is really free. Suppose that an attacker knows in which specific area CRN works. Knowing which licensed bands CRN might use, an attacker can simply transmit signal in the licensed band emulating real transmission and thus limiting overall CRN capacity. Until now we don't know any method of prevention against this attack.

**Common control channel jamming:** One of the possible solutions for common control channel deployment is the use of UWB. In this case, the potential attacker can simply transmit periodical pulses which have the same spectrum as common control channel of CRN but with a higher power than legitimate users. Through jamming of just one control channel, the attacker blocks the possibility of communication between all CR nodes. This is the reason for building sophisticated UWB transmission methods for control channels utilizing UWB. It has to be underlined that a need for special care in control channel usage is the same for any type of approach (dedicated channel, channel hopping, etc.).

**Attacks on spectrum managers:** We cannot allow having one central spectrum manager responsible for assigning frequency bands for nodes (see paragraph 2.3) because it constitutes a single point of attack. Whenever the spectrum manager is not available for CR nodes, the communication process becomes impossible. That is why information about spectrum availability should be distributed and replicated as possible. This constraint is inline with the requirement for more accurate measurements of spectrum availability (see paragraph 2.3). One of the preventing ways for this attack is to use specific pilot channel elements due to their poor security. This could become a target of attack. Because cognitive radio constitute a new approach for building wireless networks, it simultaneously opens a door for new methods of attacks on their physical structure. Below we outline each license band. It would inform secondary users about the reservation of the nodes.

**Eavesdropping:** Usually, in the infrastructure-based corporate WLAN it was assumed that signal will not leave the building due to its short distance and will be limited to eavesdropping and sniffing. However, cognitive radios are allowed to work in the bands lower than UNII and ISM. This means that they can perform longer transmission distances with the same power. It also allows for easy physical data collection from locations far from the CRN location where attackers invisible to emergency services. This yields a need for strong data encryption at the physical level. Frequent leaving and joining the emergency network...
network must be preceded by authentication process. It is open for discussion which layer should be responsible for this step. Currently the most possible approach is that application layer will perform all the necessary authentication procedures. Moreover the entire WEP infrastructure should be the basis for authentication procedures in CRNs.

VIII. CONCLUSIONS

The rapidly changing radio environment, more radio channels to utilize, number of parameters to choose during decisions taken by MAC and routing protocols, etc. makes design of CRNs very challenging. In this deliverable we have outlined some specific parameters and constraints which have to be taken into consideration while designing protocols for layers above PHY. Many protocols have the same design requirements (like robustness, no clock synchronization or localizing capabilities) which simplify design by small fraction. Moreover we can state that UWB as a common control channel might become a good solution for realizing certain functions outlined in this document. We also outline that cooperation between physical and link layer is essential for accurate operation of CRN. We have to emphasize that new requirements might occur during design process so this document will be constantly updated.

V. REFERENCES


2) Linkopings University Programmable Base band Processor Website http://www.da.isy.liu.se/research/bp/bbp1.html

3) Cavallaro, J.R.; Vaya, M.; Viturbo: a reconfigurable architecture for Viterbi and turbo decoding; Proceedings of


6) Eric Tell, Dake Liu; A Hardware Architecture for a Multi Mode Block Interleaver; International Conference on Circuits and Systems for Communications (ICCSC), Moscow, Russia, June 2004


8) Sridhar Rajgopal, Joseph R. Cavallaro; A Programmable Base band Processor Design for Software Defined Radios.

9) IEEE Mid West Conference on Circuit and Systems, Tulsa, USA, August 2002