

Detecting Primary Receivers for Cognitive Radio Applications

Ben Wild
EECS Department
UC Berkeley
benwild@eecs.berkeley.edu

Kannan Ramchandran
EECS Department
UC Berkeley
kannanr@eecs.berkeley.edu

Abstract— A cognitive radio must detect the presence of primary users to avoid interfering with them. However, it has been assumed that many devices in primary networks such as televisions and cellular phones are passive, i.e. the cognitive radio cannot find their locations. In this paper we show how we can take advantage of the Local Oscillator (LO) leakage power that all RF receivers emit to allow cognitive radios to locate these receivers. We show that our detection approach can detect the LO leakage with very high probability and takes on the order of milliseconds to make a decision. We then propose a new architecture consisting of sensor node detector devices that detect the LO leakage and communicate the channel usage to the cognitive radios. We also compare the performance of our proposed solution to that of architectures assuming passive primary receivers.

Keywords—cognitive radio; software defined radio; sensor networks; local oscillator leakage

I. INTRODUCTION

Recently there has been great interest in re-evaluating the spectrum usage policy in the US. This stems from the fact that studies have shown that spectrum in the United States is vastly underutilized [1]. One way to increase the utilization of spectrum is by building smarter radios that can detect temporal and spatial “holes” in the spectrum. These radios have been termed Cognitive Radio (CR) by Joseph Mitola III [2].

A large technical hurdle to overcome is the design of a CR that could predict the interference it would cause on nearby users. The FCC calls this the “interference temperature”. Guaranteeing that the interference temperature at a primary receiver will be below a given threshold is very difficult. A technical challenge to overcome involves reducing the uncertainty in the primary receiver location. Recent work on the subject has looked at the detection of weak signals from primary transmitters [4] where it was shown that the problem becomes very difficult when there is uncertainty in the receiver noise variance. The authors suggest the use of a pilot tone from the primary transmitter to help improve detectability. In [3, 4] the authors tacitly assume that the locations of the primary receivers are unknown. This leads to the CR needing to rely on using possibly weak primary transmitter signals to make a decision. In

[5], the authors show that detectability of weak signals could be significantly improved by having cooperation among the CRs.

This work is driven by the question: “How valid is the passive primary receiver assumption?” Specifically, we explore the possibility of detecting primary receivers by exploiting the local oscillator (LO) leakage power emitted by the RF front end of primary receivers. It is widely believed that LO leakage detection is used by the British Broadcasting Corporation to find TV license fee evaders [6]. One aim of this paper is to verify the feasibility of LO detection. Detection of LO leakage is described in more detail in section II. *This leads to the possibility of reliably locating the primary receivers and using this information to guarantee that a CR will not interfere with primary receivers.* By using this additional information we describe a novel cognitive radio system architecture consisting of low cost sensor nodes placed in close proximity to the primary receivers. These nodes would work in concert with the CRs. The architecture is described in section III. Finally, in section IV, we quantify the performance improvements of the proposed architecture and compare it to an architecture where primary receivers are assumed to be passive.

II. DETECTING LO LEAKAGE

Modern day radio receivers are based to a large extent on the superheterodyne receiver architecture invented by Edwin Armstrong in 1918. This architecture is shown in Figure 1. The architecture has been popular since it allows the RF signal to be converted down to a fixed lower intermediate frequency (IF), replacing a low Q tunable RF filter with a low-cost high-Q IF filter. In order to down-convert an RF band to IF, a local oscillator (LO) is used. This local oscillator is tuned to a

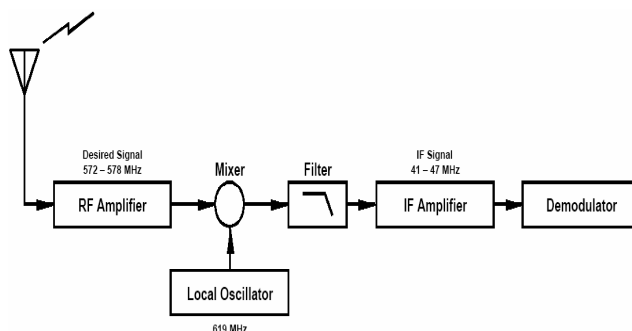


Figure 1. Superheterodyne receiver [7].

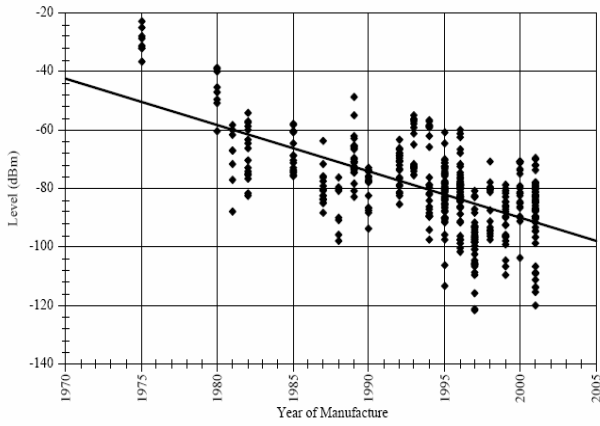


Figure 2. TV LO leakage versus model year [7].

frequency such that when mixed with the incoming RF signal, the desired RF band is down-converted to the fixed IF band. In all of these receivers, there is inevitable reverse leakage, and therefore some of the local oscillator power actually couples back through the input port and radiates out of the antenna [7]. In a direct conversion architecture, where the RF is converted directly down to baseband, the LO frequency will fall within the band of interest. The LO leakage radiation will then mix back into the receiver and cause a DC offset to be added to the signal of interest. This problem is called “self mixing” and is also solved by using an IF. In most television receivers, the LO frequency is set to 41MHz above the channel of interest. Over the years, improvements have been made to receiver architectures, resulting in reduced LO leakage power. Figure 2 shows the leakage power of television receivers versus model year. Detecting this leakage power directly with a CR would be impractical for two reasons. Firstly, it would be difficult for the receive circuitry of the CR to detect the LO leakage over larger distances. From the calculations shown on the next page, it can be shown that a distance of 20m, it would take on the order of seconds to detect the LO leakage with a high probability. For a practical system, the detection would need to be made on the order of milliseconds at worst. The second reason that it would be impractical to detect the LO leakage directly is that the LO leakage power is very variable, depending on the receiver model and year. If the CR used this variable power level to estimate proximity to the primary receiver, there would be too much error introduced by this variability. We propose to build tiny, low cost sensor nodes that would be mounted close to the primary receivers. The node would first detect the LO leakage to determine which channel the receiver was tuned to. It would then relay this information to the CR through a separate control channel using a fixed power level. Communication between sensor node and CR is discussed in more detail in section III.

Several detection schemes exist to detect low energy signals. Regardless of the detection scheme, the front-end architecture of the node will be the same. It would consist of an RF amplifier, filter, and a bank of local oscillators each tuned such that the desired incoming LO leakage signal will fall into a fixed IF band. After the IF filter, the signal would be sent to the detection circuitry. One detector would be implemented for each channel that the node is supervising. This architecture is shown in Figure 3. The input into the detector is the desired down-converted LO leakage signal in addition to additive

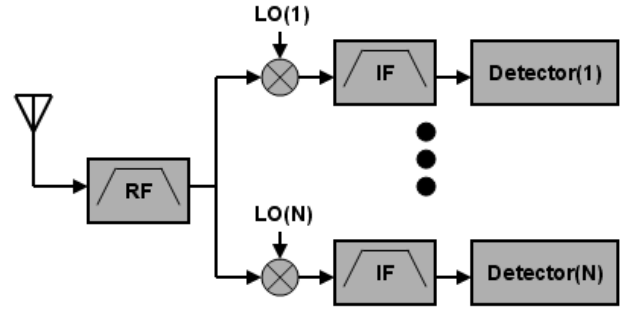


Figure 3. Sensor node receiver architecture.

Gaussian noise. The noise power will be directly proportional to the IF filter bandwidth. Consequently, the IF bandwidth should be kept as narrow as possible. However, it must be wide enough to account for uncertainty in the LO leakage frequency.

We first consider the case where each detector is a matched filter. This is the optimal detector to use but requires synchronization. The detector is shown in Figure 5. In the diagram $v(t)$ represents the down-converted LO leakage signal in addition to additive Gaussian noise, $n(t)$. Each detector takes $v(t)$ as an input and correlates it with a sinusoid with frequency corresponding to the LO frequency of one of the N channels, $s_i(t)$. Since this is a coherent detector, phase synchronization is critical. A Phase Locked Loop (PLL) can be used to match the phase of $s_i(t)$ to $v(t)$. In many broadcast signals such as television, a pilot carrier is transmitted to aid in phase synchronization. For the case of television broadcast, we would need one detector for each of the channels broadcast. An error occurs when one or more of the detectors determines that an LO signal is not present when one actually is. The converse case, where we detect a LO signal, when one is actually not present is not as important and can be assigned a lower probability. For simplicity, the following analysis assigns equal probabilities to both cases. For a coherent detector and White Gaussian noise statistics, the probability of error from elementary communication theory [8] is:

$$P_e = Q\left(\frac{\sqrt{E_s}}{2\sigma}\right), \quad (1)$$

where E_s is the energy in the LO signal, σ^2 is the receiver noise power, and $Q(x) = 1 - F(x)$, where $F(x)$ is the standard normal distribution function. Let the transmitted LO power be denoted by P_T and the received LO power at the sensor node be denoted by P_R . For line of sight propagation, it is reasonable to use the free space path loss equation given by:

$$P_R = P_T - 20 \log\left(\frac{4\pi D}{\lambda}\right). \quad (2)$$

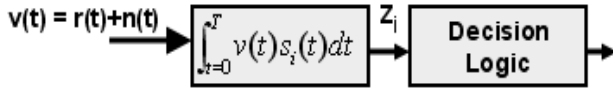


Figure 4. Matched filter detector.

Where D is the distance between transmitter and receiver and λ is the wavelength of the RF radiation. The above path loss equation is simplified in that we are ignoring the antenna gains. We also have that the received LO power is related to the received LO energy by:

$$E_s = P_R t, \quad (3)$$

where t is the receiver integration time. For an ideal receiver, the noise power is given by:

$$\sigma^2 = K T B F, \quad (4)$$

where K is Boltzmann's constant, T is the temperature, B is the receiver bandwidth and F is the noise factor. To achieve acceptable performance the probability of error and integration time must be kept small. To get a feel for the feasibility of building this sensor node, we use the parameters in Table 1. In this example a sensor node is used to detect the leakage from a television receiver. Using the parameters from Table 1 we can find the minimum integration time necessary. Using (1) we find that the SNR for a probability of error of 10^{-4} is:

$$\sqrt{E_s} / \sigma = 7.44. \quad (5)$$

Finally, using (2), (3) and (4) we get:

$$P_R = -100 \text{ dbm} - 20 \log\left(\frac{4\pi 1m}{0.46m}\right) = -129 \text{ dbm} \quad (6)$$

$$10 \log P_R + 10 \log t - 10 \log(\sigma^2) = 17 \text{ dB} \quad (7)$$

TABLE 1: EXAMPLE SENSOR NODE PARAMETERS.

Probability of Error	10^{-4}
Receiver Bandwidth	100 Hz
Receiver Noise Factor	2
Receiver Temperature	290 K
TV LO Leakage power	-100dbm
Number of TV Channels	35 (ch. 2-36)
Distance between sensor node and TV antenna	1m

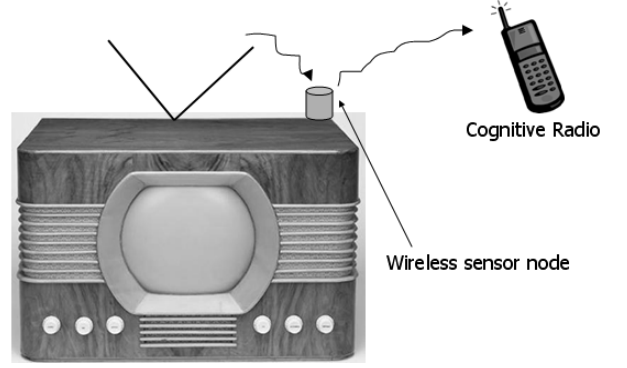


Figure 5. Sensor node notifying cognitive radio.

$$-129 \text{ dbm} + 10 \log t + 151 \text{ dbm} = 17 \text{ dB} \quad (8)$$

In (6) we use a (worst-case) wavelength of 0.46m corresponding to a maximum LO frequency of 649MHz (channel 36). Solving (8) we find that the integration time must be set to 346ms. For television LO detection we can also increase the LO leakage received power by connecting the sensor node directly between the television's input port and antenna. This could be done by using a 20dB coupler. The coupler would couple 1/100th of the RF power into the sensor node. If this technique was used, the received power would increase from -129dbm to -120dbm in the calculation above, resulting in an integration time of 43ms. For this case, we plot the required integration time versus probability of error in Figure 6. This technique is also attractive because the sensor node would not need to have its own antenna, rather it could use the television's antenna for transmission. There exist alternate approaches that allow us to further reduce the integration time. For example, one could build a sensor with multiple detectors and take a majority vote to make a decision.

The above coherent detector analysis assumes that the detector has perfect knowledge of the LO leakage frequency and phase. In reality this would be difficult to achieve. A sub-optimal approach that would be simpler to implement would be to use an energy detector. In this approach the signal is detected by first down-converting the RF to an IF frequency. A high speed A/D converter would digitize the IF band, and then a Fast Fourier Transform (FFT) would be performed on a block of samples. Several blocks of the FFT output can be averaged

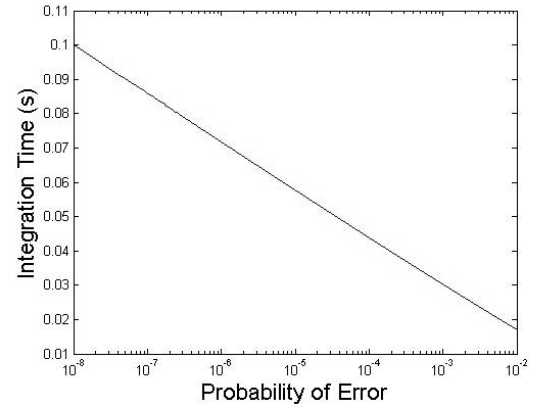


Figure 6. Integration time vs. probability of error.

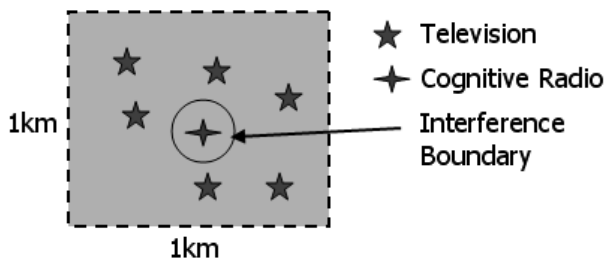


Figure 7. Cognitive radio in urban environment.

to reduce the noise level. The LO leakage would then be found by analyzing the magnitude of the FFT output and finding the peak. To detect the presence of a sinusoid in a non-coherent fashion would approximately require an additional 1dB of SNR to get the same error performance as the coherent approach [8].

It is important to note that although the above example considered the case of a television receiver as the primary receiver, this does not limit the application of these sensor nodes to other receivers such as cellular phones. Ideally, receivers would be designed with the capability to transmit their channel usage information to Cognitive Radios. In the case where radios are not designed with this capability, a LO leakage detecting sensor node can be mounted on the radio, assuming that a sensor node can be manufactured to be small enough to fit seamlessly on a particular radio.

III. SYSTEM ARCHITECTURE

In section B we explored the feasibility of building sensor nodes that can detect LO leakage radiation from a passive receiver. We now show how these sensor nodes work together with the CRs as a system.

When a sensor node detects the presence of a LO, it must notify any CR in the region of the channel usage by means of a control channel. For example, the control channel can use part of the unlicensed spectrum from 420MHz to 450 MHz. To simplify the system, the sensor node can transmit a pilot tone to indicate which channel is used. Different frequency tones would be used to indicate different channels. One problem with this approach is that the CR could be confused if two nearby sensor nodes transmit the same frequency pilot tone. Since the CR would receive a stronger signal at that frequency, it would assume that the primary receiver is much closer than it actually was. As a result, the CR would be more limited in its region of operation. To decrease the magnitude of this problem, we can randomly assign pilot tones to different sensor nodes. The number of possible frequencies the sensor node would use per channel would depend on the bandwidth available on the control channel. This scheme would greatly decrease the probability that several sensor nodes within range of the CR are using the same pilot tone frequency. This random assignment could be hard-wired when the nodes are manufactured.

The sensor node is designed to transmit at a fixed power level. This level is chosen such that the cognitive radio will be able to detect the pilot tone if it is within interference range of the primary receiver. This assumes that the principle of

reciprocity holds. When the principle holds, the attenuation of the CR's transmit signal received at the sensor node will be the same as the attenuation of the sensor node's transmit signal received at the cognitive radio. This means that if the sensor node transmit signal goes through a multipath and shadowing environment to reach the CR, then the CR's transmit signal will also go through the same environment to reach the sensor node. Reciprocity will not hold exactly, so an additional power margin must be added to the sensor node transmit signal to account for this. To combat the effects of frequency selective fading, the CR could transmit multiple pilot tones at different frequencies to indicate that a channel is used. The chances of all tones being in a fade would thus be dramatically decreased. If the CR finds that a channel is available, it first coordinates among the other cognitive radios on a mechanism to share the spectrum using a suitable MAC protocol. Once a channel is found, it can begin transmitting. The CR will then check periodically if the channel that it is using becomes invalid. When the CR detects that its channel is unavailable, it will stop transmitting immediately and check if another channel is available. The CR must stop transmitting in a small enough time period so that the interference caused to the primary receiver is negligible. The CR will maintain an up to date list of unused channels so that it can quickly hop to an unused band when the channel being used becomes unavailable.

IV. PERFORMANCE IMPROVEMENTS

We showed in the previous section that building sensor nodes to detect primary receiver channel usage is feasible. Even in the case where these sensors are communicating channel usage to the CR, there is no guarantee that a channel will be available. As the density of the primary receivers increase, we naturally expect the probability of having an available channel should decrease. To quantify this we will consider the case where the CR is operating in environments with varying densities of primary receivers. The following assumptions are made for this model:

- Density of the primary receivers: D/km^2 .
- Number of channels: M
- Interference Radius of CR: R

We assume that all of the channels are equally likely to be used at any instance of time and that the receivers are uniformly distributed. Let $A_{N,i}$ denote the event that channel i is free when there are N primary users within the interference radius. Let C_N denote the event that at least one of the N channels is available. In this setup, the probability of event $A_{N,i}$ is given by:

$$P(A_{N,i}) = \left(1 - \frac{1}{M}\right)^N \cdot \quad (9)$$

The probability of event C_N is given by:

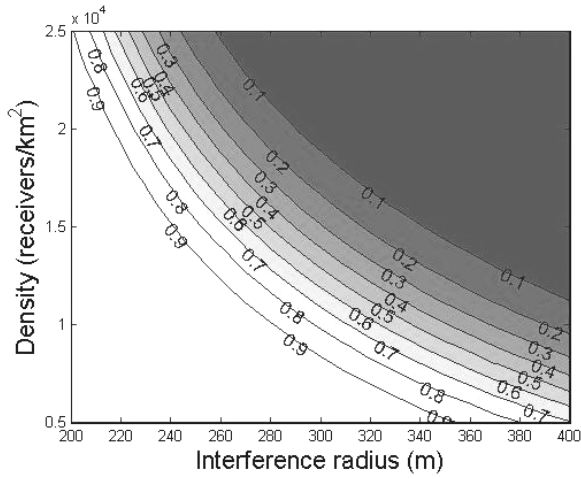


Figure 8. Probability of at least one channel available.

$$\begin{aligned}
 P(C_N) &= \bigcup_{i=1}^M P(A_{N,i}) \\
 &= \sum_{i=1}^M (-1)^{i-1} \sum_{1 \leq k_1 < \dots < k_i \leq M} P(A_{N,k_1} \cap \dots \cap A_{N,k_i})
 \end{aligned} \quad (10)$$

(10) is simply the classical Inclusion-Exclusion formula for a union of M events. Let F_b be the event that b of M channels are free. Then we find $P(F_b)$, the probability of any combination of b of M channels being free to be:

$$P(F_b) = \binom{M}{b} \left(1 - \frac{b}{M}\right)^N. \quad (11)$$

Finally, we find $P(C_N)$ to be:

$$\begin{aligned}
 P(C_N) &= \bigcup_{i=1}^M A_{N,i} = \sum_{i=1}^M (-1)^{i+1} P(F_i) \\
 &= \sum_{i=1}^M (-1)^{i+1} \binom{M}{i} \left(1 - \frac{i}{M}\right)^N.
 \end{aligned} \quad (12)$$

To get the overall probability of having at least one channel available for a density of D primary receivers per km^2 we make N a random variable and condition (12) on the value of N . We then sum over all possible values of N to get:

$$P = \sum_{r=1}^D P(C_N | N = r) P(N = r) \quad (13)$$

$$= \sum_{r=1}^D \left\{ \sum_{s=1}^M (-1)^{s+1} \binom{M}{s} \left(1 - \frac{s}{M}\right)^r \right\} \binom{D}{r} q^r (1-q)^{D-r},$$

where q is the probability a primary receiver is within the interference radius, and is given by:

$$q = \frac{\pi R^2}{10^6 m^2}. \quad (14)$$

In (13) we used the fact that the probability that there are r users in a radius R is a binomial distribution with parameter q . Figure 8 shows the probability of having at least one channel available as a function of receiver density and interference radius. To generate the plot, we assume a setting where the primary receivers are televisions. In this case we used $M=35$. Additionally, only approximately 15% of all households use broadcast television. Televisions are also turned on approximately 25% of the time. Assuming that the on time of televisions is uniformly distributed (which is clearly not the case, but good enough for a first order analysis) we get an effective television density of:

$$D_{eff} = D(0.15)(0.25). \quad (15)$$

We notice from Figure 8 that the probability that the CR will have at least one channel available is high across a wide range of interference radii and primary receiver densities. For example, at a receiver density of $10,000/\text{km}^2$ and an interference radius of 250m the probability is 0.99 that at least one channel is available. On the other hand, if the primary receivers were passive, the CR would have to rely on its proximity to the primary transmitter to make a decision. This would make it very likely that the CR would not be able to function in an urban environment, where the likelihood of a television transmitter in the region would be very high.

In summary, we notice that even when there is a large density of primary receivers, such as can be found in urban environments, there is still a high probability that a CR can find free spectrum to use. In the case of television broadcast, if the CR senses that a channel is available, it may still have interference to contend with from the television broadcast transmitter. In this case the capacity that is available on the channel will mainly depend on the power output by the transmitter, the proximity of the secondary receiver to the transmitter, and the distance between secondary transmitter and receiver. To get a feel for the capacity, we assume the following conditions:

- Primary transmitter output power: 100,000W
- Secondary transmitter output power: 100mW
- Distance between secondary tx and rx : 10m
- Secondary receiver noise figure: 3dB

We used the standard Hata model [9] to find the path loss for large urban environments. In the model, we assumed that the primary transmitter was 800 feet above ground level, which is typical of large broadcast antennas. We also assume free space path loss for the secondary transmitter to secondary receiver path. Furthermore, we assume that the secondary receivers employ direct sequence spread spectrum with a spreading gain of 10 to reduce the effects of fading, giving us a unspread bandwidth of 600KHz. The capacity (assuming white Gaussian noise and interference) is then calculated as follows:

$$C = B \log\left(1 + \frac{S}{N + I}\right), \quad (16)$$

where B is the unspread bandwidth, S is the received signal power from the secondary transmitter, N is the secondary receiver noise power, and I is the interference power received at the secondary receiver due to the primary transmitter. For a spread spectrum system, the noise bandwidth is the unspread bandwidth, and the interference power is calculated using only the portion of the interference power that lies within the unspread band. The capacity for this scenario is shown in Figure 9. The capacity curve shows that even when we are fairly close to the transmitter (~1000m), we can still achieve throughputs greater than 1 Mbps. To put this in perspective, in a city such as San Francisco, 99% of the population would live outside of this 1000m radius, assuming that the antenna is located in the center of the city.

V. EXPERIMENTAL RESULTS

To demonstrate the feasibility of detecting LO leakage from radio receivers we built a prototype sensor from off the shelf components. The receiver under test was a Hauppauge computer based TV receiver. We attached a 10dB attenuator to the input port of the television to simulate a 10dB coupler. The output of the attenuator was connected to a broadband RF amplifier. The amplifier output was fed into the RF input of a mixer. The oscillator input of the mixer was driven by a signal generator whose frequency was set so that the LO leakage frequency of the TV receiver would get mixed down to a fixed IF band. An IF filter was chosen centered at 100KHz, with a 3dB bandwidth of 3KHz. The output of the IF stage was further

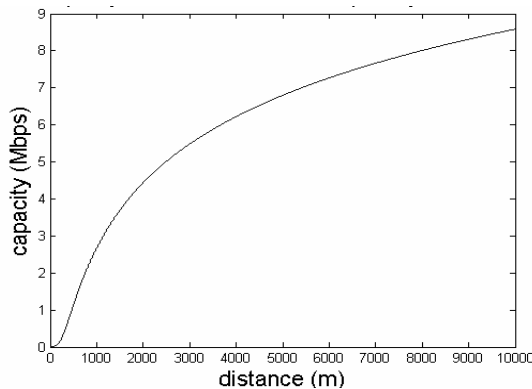


Figure 9. Capacity versus Distance.

amplified and sent to an envelope detector. The output of the enveloped detector gave us a DC signal whose level was proportional to the LO leakage power. This DC signal was fed to a comparator whose voltage threshold was set at the average of the DC level obtained when the LO leakage was present (indicating that the TV tuner was tuned to the corresponding channel) and the DC level obtained when the LO leakage was not present (indicating that the tuner was not tuned to the corresponding channel). The output of the comparator drove a light emitting diode (LED) to indicate the presence of the LO leakage at the specified channel. This setup is shown in Figure 10. The detection time of the circuit was very small, almost instantaneous to a human observer. We are currently working to replace the signal generator in the setup with a frequency synthesizer that will be able to scan all of the television channels and report the channel usage information to a cognitive radio.

VI. FUTURE WORK

In the future we would like to exploit the fact that the interfering signal is an NTSC signal. The capacity curve that we calculated assumed that the interfering signal was Gaussian. Since Gaussian interference provides a lower bound on the capacity, we can potentially code the transmitted signal to take advantage of the NTSC signal statistics. We believe that “dirty paper” type coding methods [10] could dramatically improve the data rates. As broadcasters transition from analog to digital television we believe that our work is still applicable since digital receivers also have LO leakage that indicates the channel usage. Furthermore, dirty paper type coding could also be used in the case of digital broadcast. We would also like to use more accurate statistical models of the spatial distributions and usage patterns of primary receivers in urban environments. Additionally, we would like to look at how the architecture scales with the number of cognitive radio users. Lastly, we would like to continue developing our prototype sensor node to verify our theoretical results. Since the cost of these sensor nodes will be vital if they are to be deployed, we would like to show that these can be manufactured at a low cost.

VII. CONCLUSIONS

In this paper we showed that the assumption that primary receivers are always passive severely constrains the utility of cognitive radios. A sensor node that was capable of detecting the LO leakage from superheterodyne receivers was described. We showed that these sensors could detect the exact channel that a primary user was tuned to and transmit this information to the cognitive radios through a control channel. Using this information we showed that the cognitive radios could operate in dense urban environments without interfering with primary receivers. The system that we described is fully compatible with legacy receivers, allowing the system to be implemented in a very short time frame.

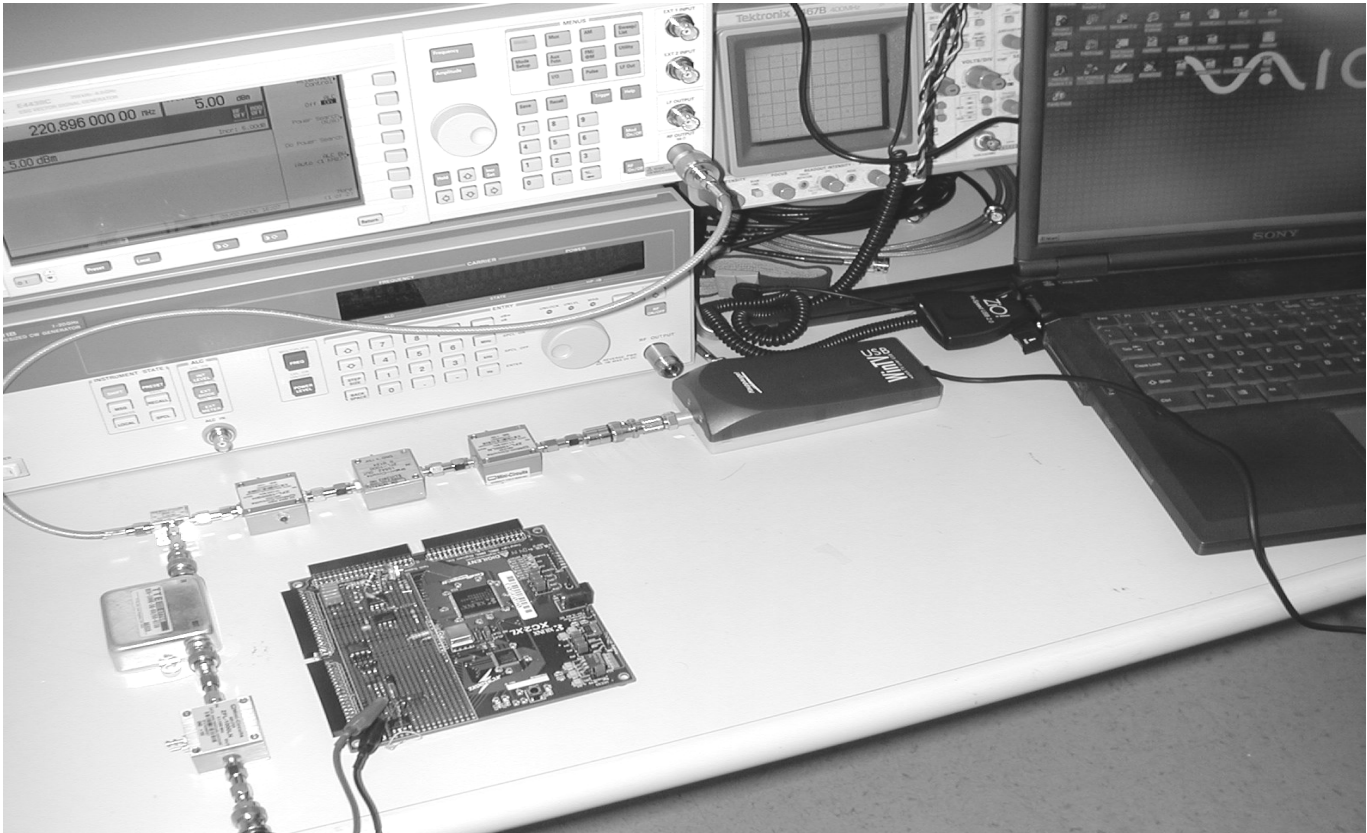


Figure 10. Test Setup

ACKNOWLEDGMENT

We would like to thank Professor Ali Niknejad, Abhik Majumdar and Rohit Puri for their helpful suggestions.

REFERENCES

- [1] R.W. Brodersen, A. Wolisz, D. Cabric, S.M. Mishra and D. Willkomm. (2004) White paper: Corvus: A cognitive radio approach for usage of virtual unlicensed spectrum. [Online]. Available: http://bwrc.eecs.berkeley.edu/Research/MCMA/CR_White_paper_final1.pdf
- [2] Mitola, J. III, Maquire, G.Q. Jr. Cognitive radio: making software radios more personal. IEEE personal communications. Aug. 1999.
- [3] A. Sahai, N. Hoven, and R. Tandra. "Some fundamental limits on cognitive radio." Allerton Conference on Communication, Control, and Computing. Oct. 2004.
- [4] N. Hoven. "On the feasibility of cognitive radio," Master's thesis. University of California at Berkeley. Berkeley, CA, 2005.
- [5] Cabric, D., Mishra, S.M., Brodersen, R.W. "Implementation issues in spectrum sensing for cognitive radios" Signals, Systems and Computers, 2004.
- [6] [Online] Available: <http://www.tvlicensing.biz/detection/>
- [7] Weiss, S. Merrill, Weller, Robert D., Driscoll Sean D. "New measurements and predictions of UHF television receiver local oscillator radiation interference" [online]. Available: h-e.com/pdfs/rw_bts03.pdf
- [8] Proakis, John G. Digital Communications. McGraw-Hill College, 2000.
- [9] Hata, M. "Empirical formula for propagation loss in land mobile radio services", IEEE Transactions on Vehicular Technology, Sept. 1981.
- [10] M. Costa, "Writing on dirty paper", IEEE Transactions on Information Theory, vol. 29, pp 439-441, May 1983.