The sensible approach to spectrum sharing

The term *cognitive radio* (CR) is still evolving. It is most often used to describe a wireless communications device that has the ability to collect data about its physical and networking environments and then use that information to improve the quality and efficiency of its transmissions. By coordinating channel usage, positioning, power levels, polarization, and transmission time between devices, CR can facilitate impressive frequency reuse.

Over the past two years, the FCC has issued and proposed a number of new rules that would allow for the commercialization of CR based equipment in areas where incumbent operators are not making use of allocated radio frequencies. The primary objective of these regulations has been to make additional spectrum available for use by consumer devices and for the provisioning of wireless broadband services.

Industry, incumbent licensees, and government are now negotiating a framework for spectrum sharing in a variety of forums, and these proceedings have illuminated a number of novel issues. The first of these arise from the fact that it is not always possible for a transmitter to identify all of the devices that it might interfere with. This problem is exemplified in the bands currently reserved for over the air television. An unlicensed device can never be completely certain as to the location of a television by listening for it because TVs do not transmit a signal. This leads to the challenging prospect of an unlicenced device having to identify the coverage area of a TV station by analyzing its signal.

Secondly, as different types of wireless devices and multiple service providers attempt to make use of the same channels in the same area, it will become increasingly difficult for a device to sense an incumbent; advocates talk about a "sensing window" in which all unlicensed devices would stop transmitting and listen for incumbents attempting to use the channel, but, without coordination between all unlicensed devices, it is unclear how the timing for this window would be agreed to.

Finally, in some cases, incumbents are allowed to make use of spectrum for a secondary use, and these devices are entitled to protection from harmful interference as well. For example, broadcasters may use vacant TV channels for the operation of wireless microphones, on a temporary basis, for production and news gathering activities. The wireless microphone industry has proposed the idea of a radio beacon that would warn unlicensed devices that a channel is in use. Such a device would have to be portable enough to be carried by a camera crew, and capable of contacting all of the networks in a radius of at least 40 km. The impracticality of this solution is revealed when one imagines a reporter and a cameraman running down the street with a 10 meter high antenna and a car battery to power their beacon.

Why all the confusion?

Until recently, the primary use for cognitive radios has been in military equipment that is designed to use sensing to identify the least conspicuous clear channel (using dynamic frequency selection or DFS) and then to transmit with the minimum power necessary in order to be heard (known as transmit power control or TPC). In reality, although it is undesirable to cause interference to existing users, there are methods of disguising a signal sufficiently such that not causing any interference has never been an absolute requirement in this application.

Unfortunately, industry and government have not clearly differentiated the military application of CR, in which the primary objective is to facilitate the best possible link between devices with the least chance of interception, from the application that would allow new devices to share spectrum with incumbent licensees. There is mounting evidence that sensing alone does not provide all of the information a device needs in order to allow DFS and TPC to provide an acceptable level of assurance that a device will not interfere with an incumbent operator.

The issue is further confused because there are a few frequency bands in which sensing may be a practical solution. An example of this is the 5 GHz bands in which Wi-Fi equipment will be able to operate on channels currently assigned to military radars. There are a number of reasons that this particular scenario is likely to be successful; the most important being that the radars themselves were designed to overwhelm any interference they encounter. This is not the case for civilian incumbent operators' equipment. The majority of incumbents have neither the ability nor the regulatory authority to over power devices that might be allowed to share their bands.

Finally, when competing devices are unable to identify one another, co-existence can be very challenging. In reality, the more non-coherent co-channel interference that overlapping networks cause to each other, the more processing power each device needs in order to sense, and eventually, within areas where many networks overlap, the noise level will rise to the point that sensing will fail. Technology developments that are enabling CR actually exacerbate this problem because devices are gaining the ability to dynamically alter the modulation schemes of their transmissions. After identifying the operating characteristics of a competing radio, there is no longer any guarantee that it will be recognizable in the future.

What is the answer?

The proposed model for allowing CR assisted operation of unlicensed and lightly licensed devices in licensed bands is ineffective because it relies on sensing at the point of transmission to determine the radio frequency environment at the edge of the area of a transmitters effect.

The only way to ensure that transmissions do not interfere with existing users, and that individual contenders do not monopolize a channel, is to define the perimeter of each independent network, and then have an out of band mechanism award channels based on a predefined priority and contention criteria.

The Sensible solution

Sensible Radio proposes the following solution, which uses location, terrain and device profile information, in order to co-ordinate secondary users in licenced bands out of band.

1. The perimeter of an incumbents existing deployments would be mapped onto a digital topographic map. This data exists for 3650-3700 MHz, and is on going in the TV bands as part of an FCC NOI (Satellite-Delivered Network Signals 05-182). In the interim, a union of the FCC grade B contour and a more modern predictive algorithm such as Longley-Rice or TIRAM could be used.

2. Service providers would then have the right to use sensing to prove that there were no detectable incumbent signals operating in an area. After a mandated number of samples were taken, if no signal was detected, the perimeter of protection would be reduced. At the same time, incumbents could be given the right to prove that their signal propagate beyond the perimeter of their protected contour. If there was a detectable signal, their perimeter of protection would be increased.

3. All devices would have a certified interference potential profile (IPP). An IPP is a series of three dimensional models that define the perimeter at which a device has the ability to generate interference above regulatory limits. Both in band and out of band emissions are calculated at each transmit power control step and for each channel that a device is capable of operating on.

4. Using the following assumptions, an IPP would be plotted on the map to insure that an incumbents protected area is not violated:

    a. Non-professionally installed equipment would be treated as omni-directional radiators regardless of any directionality of their transmitter.

    b. Professionally installed devices, and consumer installed equipment which had been professionally audited, would be given credit for the directional characteristics of that equipment, and would therefore be able to operate closer to a contour of protection.

c. Location information and sensing data obtained from a professionally installed base station could be used to grant "partial credit" for the positioning of highly directional customer premise devices.

This scenario allows for equipment to be installed by users in truly rural areas, where there are many channels available, and a professional installation is neither necessary nor economically viable.

5. There are a number of methods a device could employ to find an appropriate non-interfering channel when first used. In the case of wireless broadband access equipment, the simplest would be an automated phone-in system in which the customer entered their zip code, a WISP ID and a product ID; the appropriate base station would then transmit channel and power permission information to the new device. This could also be accomplished over the air, either by using existing unlicensed bands or by the allocation of a dedicated "control channel".

6. Incumbents wishing to use an authorized legacy device (such as a wireless microphone that operates under FCC Part 74 rules), would simply enter their location and a priority code into the system, and an operating bubble would be created. Essentially, the system would alert all networks that overlapped the perimeter of a bubble that they must reduce power or change channels. This method would protect new devices from sensing "false alarms" created by the many existing legacy devices that have no legal right to protection from interference.

6. If, due to propagation or installation anomalies, the incumbents signal was being interfered with, the system could draw bigger and bigger exclusion zones around the location until the offending transmitter is found. This would be possible to do for adjacent channels as well.

7 Any fixed wireless device that has a verified location could pass permission to operate and channel assignment information to low power devices. This permission would not even have to happen in channel. Channel and power selection would be based on variables derived from the IPPs of both the low power and the controlling devices.

Benefits of a data driven solution include:

The amount of information processing that is required for a single device to sense could manage the allocation of more than 1000 channels per hour with an accuracy comparable to that of the natural variations in propagation.

In the event the sensing components of a customer premise device fail, technicians could be hours, or even days away. In contrast, a data driven solution will be located in controlled environments, completely redundant, and will be monitored 24 hours a day.

A data driven solution allows for dynamic changes to the DFS and TPC parameters of all the devices in an area in the event of propagation anomalies or if incorrect assumptions about a device have been made.

Allowing for the use of much higher powered equipment in truly rural and remote *areas* would be easily accomplished by defining *a perimeter of allowable operation*, and confining placement of a device based on its IPP.

"First in line first in time" operation is specifically forbidden in the 3650 MHz R&O, but applications, such as streaming encrypted security video, would effectively monopolize a channel for an indefinite period of time. Not only does this violate the principle of fair use, it makes it impossible for other networks to use sensing effectively. A data driven solution ensures that a frame work can be established in which all users are compelled to comply with the spirit of the rules.

Why has a data driven solution been discounted?

Fear of an unreliable FCC database is repeatedly raised by the advocates of sensing, but the more cost effective and functional solution is for industry to work with government and facilitate the creation of a data driven system that is robust and reliable.

Why has it been difficult to agree on an effective solution?

The incumbent licensees have identified the flaws in the rules and the resultant solutions as proposed. Unfortunately, some have taken the reactionary position that spectrum sharing must be stopped. This posturing is hardly surprising given that many incumbents have little expertise in networking, have had their expertise in propagation dismissed by the wireless industry, and believe that their operational realities have been ignored by government.

Regulators and equipment manufactures need to be educated about the constituent parts of CR systems, and that sensing is not the only option for their dynamic control. Further, they need to be educated as to the differing operational characteristics of incumbent equipment in different bands. Finally, they need to understand that broadband wireless access (BWA), point to point network bridging, and low power broadcasting are different applications, and, while there is every reason to believe that they can coexist, the issues are not trivial. The current situation, in which technologies are being developed in parallel yet independent of each other, will have a negative impact on a devices ability to avoid causing interference to incumbents, will have a negative impact on the long term functionality of consumer devices, and will have a negative impact on the ability of shared spectrum BWA to be competitive with wired solutions.

The bottom line…

Sensing will continue to play an important role in the realization of spectrum reuse technologies, but sensing alone will never allow a radio to reliably predict the effect that its transmissions will have on unidentified devices.

Radios in one network can be shielded from sensing devices that are operating within range of their transmissions.

When incoherent networks overlap, the ability of an individual device to make correct choices and to abide by rules is compromised when relying on sensing techniques alone.

Unlicenced devices using modulation schemes that are employed by incumbents' equipment, such as wireless microphones and low powered TV transmitters, will be sensed as licenced operators and they could be given inappropriate priority.

The protection beacon concept is overly complex, costly, of questionable effectiveness, easily spoofed and puts unreasonable operational demands on incumbents.

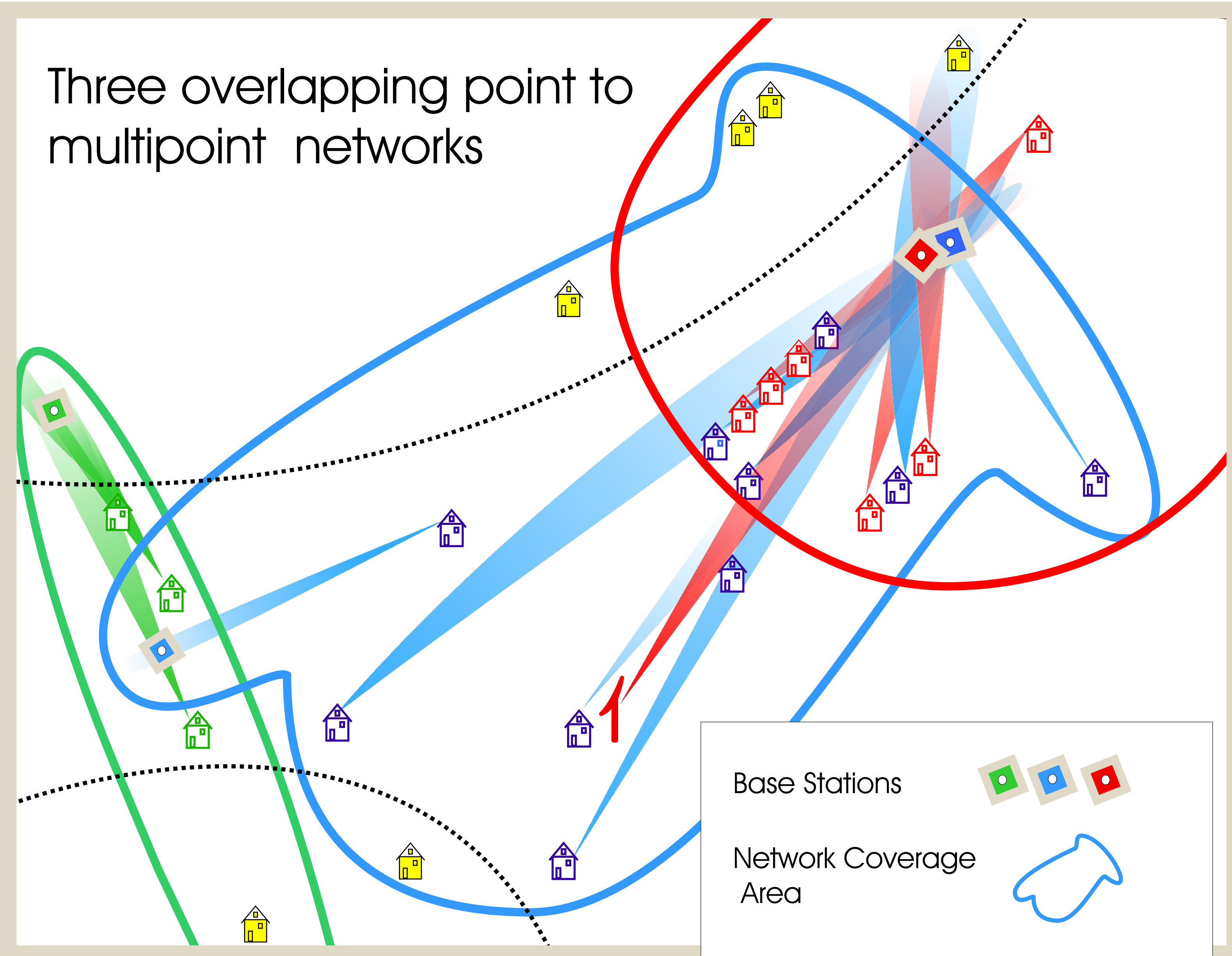
How can you help?

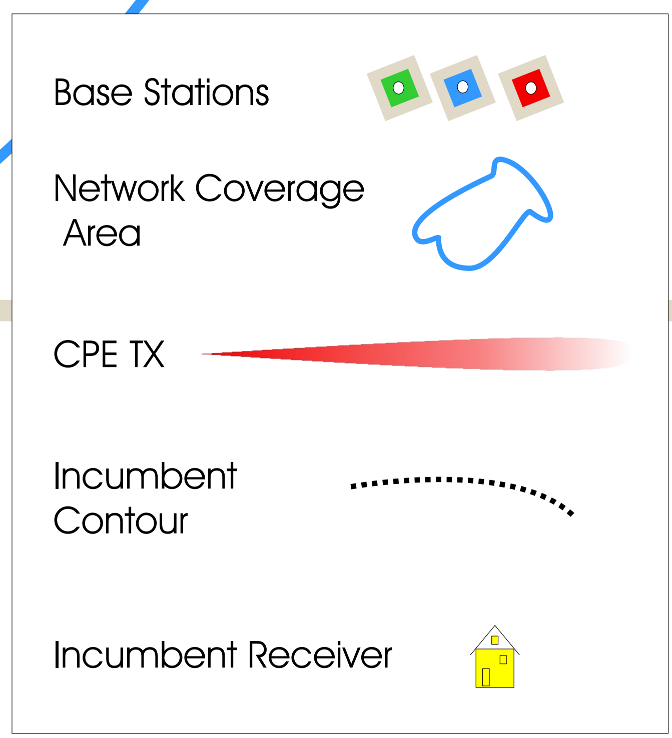
1. Sensible Radio is soliciting support from government and industry for the establishment of a certification body that will define interference potential profiles (IPPs) for all equipment that would operate on an unlicensed or lightly licensed basis, in frequency bands in which there are non-military licensees that have priority.

2. Sensible Radio is soliciting support from government and industry to build and operate the online frequency coordination system that will make use of IPPs to:

- address the technical concerns of the incumbent operators
- allow a diverse range of devices to co-exist as secondary users of spectrum
- provide dynamic protection to legitimate incumbent operations that is more effective and less expensive than " beacons"
- allow Wisps to offer services that are competitive with traditional broadband
- eliminate the colossal security vulnerabilities of publicly available databases
- provide a mechanism for higher power devices to operate in remote environments
- lower the cost of consumer devices by negating the requirement of a separate omni-directional antennae, GPS, and receiver dedicated to sensing

Three overlapping point to multipoint networks





A number of parties have advocated the development of a co-existence protocol that would allow for over the air coordination between unlicensed or lightly licensed networks that use different technologies.

Unfortunately, due to issues related to both proximity and transmitter directivity, it cannot be assumed that interfering devices from competing networks will actually be able to communicate with each other.

It should be noted that the diagram shows the simple perimeters of coherent communization between highly directional devices. It does not the show the potential to cause interference, nor does it attempt to account for terrain attenuation or hidden nodes.