An Analysis of Unlicensed Device Operation in Licensed Broadcast Service Bands

Timothy X Brown
Interdisciplinary Telecommunication Program
Electrical and Computer Engineering Department
University of Colorado Boulder, CO 80309-0530
timxb@colorado.edu

Abstract – **Recent FCC proceedings have considered the notion of unlicensed device operation in licensed bands. Licensed users are concerned about harmful interference while unlicensed device manufacturers are concerned that harmful interference is an imprecise design concept. This paper addresses three elements to this debate. First, it advocates for an explicit model of harmful interference to be included in unlicensed device rules. Such a model provides explicit bounded protection to the licensed user while providing assurances and performance goals to the unlicensed device manufacturers. Second, it assesses several proposed methods for unlicensed devices to avoid licensed users and develops variants of each that can achieve the necessary accuracy. Third, it presents an analytic model for assessing harmful interference that not only provides quantitative analysis, but, also provides insight into how factors such as directional antennas, power control, and licensed channel avoidance strategies affect the aggregate interference. Further, it suggests that complex factors such as unlicensed device modulation schemes can be captured in a simple measurement. These ideas are applied to the notice of proposed rulemaking on Unlicensed Operation in the TV Broadcast Bands.**

I. INTRODUCTION

The FCC 04-186 proceedings discussing the notice of proposed rulemaking, Unlicensed Operation in the TV Broadcast Bands[1], the recent Ultra Wideband rules, and existing Part 15 rules open the possibility for unlicensed devices to coexist with licensed devices in licensed broadcast bands. The traditional approach (UWB and Part 15) limits the unlicensed devices to low powers in order to minimize the potential for harmful interference. Today's technology enables more sophisticated radios that can use means other than simply limiting power to avoid harmful interference. This technology in turn enables more sophisticated operational rules. These rules should encourage investment in socially meaningful unlicensed devices while protecting the existing licensed users. We foresee three challenges to this goal which we denote the harmful interference process; interference parameter setting; and the channel avoidance mechanism.

In the NPRM, the commenters question what criterion should be used to evaluate the impact of unlicensed devices operating in the TV broadcast bands. Many comments make worst-case assumptions to show that any unlicensed device could have a negative impact on licensed devices, while others argue that the impact will be minimal. This uncertainty has the effect of delaying or preventing the adoption of any rules. But, more fundamentally it points to a general lack of consensus on how the impact should be measured and codified in rules such as these. The FCC has a long-standing notion of “harmful interference”, but this is not precisely defined and is mainly used in a context of evaluating existing interference in post facto proceedings. This ambiguity about what eventually will and will not be allowed can deter investment in technologies that would provide unlicensed access to these bands. Therefore, a clearer standard of what defines harmful and acceptable interference is needed to be articulated in policy and unlicensed device rules. Further a proactive process is needed that specifies how the harmful interference is measured and remedied over time.

Once a potential interference process is defined there will be parameters to be defined such as the maximum power levels or the required fidelity of a channel avoidance mechanism. Fielded deployments are expensive and time consuming. Laboratory tests can be artificial and deriving parameter relationships laborious. An analytic model can help expose these relationships clearly so that parameter tradeoffs can be made more intelligently and can provide insights into the harmful interference and channel avoidance processes.

A key element to any coexistence strategy is the method for avoiding licensed users. Avoiding licensed users requires some mechanism for identifying channel usage. Ideally an unlicensed device would like to know for every possible frequency and mode of operation the maximum power it could use without causing degradation to existing licensed devices. Even in the heart of a licensed service, an unlicensed device can communicate without causing interference if the transmit power is low enough. But, knowing the allowed power level requires detailed knowledge of licensed transmitters, receivers, and the various pathlosses among these devices. This level of detail is generally not known and so a simpler approach is taken. The idea is to identify spectrum “white spaces,” blocks of spectrum that are not being used by licensed devices in the area. This is a more conservative approach and generally is required to go further so that it avoids not only channels that are used but also adjacent channels to avoid problems with

---

[1] Notice of Proposed Rule Making, Unlicensed Operation in the TV Broadcast Bands, FCC 04-186 Released May 25, 2004.

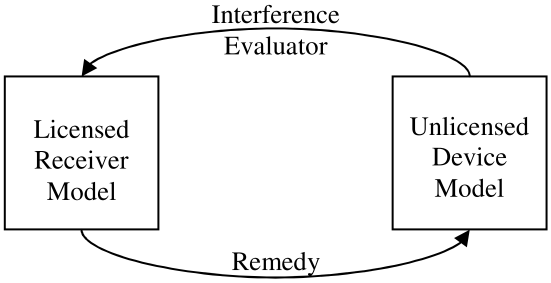

Figure 1: Elements of an Interference Measurement Scenario

licensed receivers that do not have filters sufficiently sharp to attenuate interferers on nearby bands.

Accordingly, this paper provides three contributions. First, the paper decomposes the ongoing process of regulating and enforcing harmful interference requirements. It presents the choices available to regulators at each stage in the process and the relative merits of each. These ideas are applied to the NPRM to show their impact on the regulatory process. Second, it develops an analytic interference model that predicts the fraction of licensed devices affected as a function of parameters in an unlicensed device deployment. This model points to a need for unlicensed devices to reliably avoid licensed channels. As a third contribution, the paper analyzes different channel avoidance methods to assess their viability to meet these reliability requirements.

II. HARMFUL INTERFERENCE PROCESS

This section presents the concept of a measurement scenario that is a framework for defining proactive harmful interference definitions. The framework is a set of interference notions that policymakers can choose from when setting policy and defining unlicensed device rules. Who should evaluate if there is harmful interference and potential remedies are also considered. These ideas are developed in more detail in the following sections.

A. *Measurement Scenario*

We assume that unlicensed devices are built and deployed according to a set of unlicensed rules. These rules can not be assessed unless a clear measurement scenario is defined. The measurement scenario consists of four parts. It specifies (1) a model for the licensed receivers and what constitutes harmful interference to them; (2) a model for the unlicensed devices and the conditions under which they can be considered to be causing harmful interference; (3) the interference evaluator who measures the level of interference; and finally (4) the remedy path if unlicensed devices are found to be causing harmful interference as shown in Fig. 1.

As an example, harmful interference can be defined as a condition where a single licensed receiver suffers any service outage due to the operation of an unlicensed device in any setting as measured by the licensee. If this occurs, then the licensee can request the unlicensed device to turnoff. Each of these elements can have a much richer realization than this simple example. The remaining sections describe models for each of the four elements.

B. *Licensed Receiver Model*

Interference must be carefully defined. Interference is a receiver phenomenon. When a radio device receives both desired and undesired signals at the same time, the undesired signals at the receiver are interference. Signals that are present at the receiver when it is not receiving; that are on the path from the transmitter to receiver; or that are at the transmitter are not directly relevant.

In practice any radio device radiates electromagnetic energy across a wide swath of spectrum that extends beyond its nominal channel. The signal power propagates beyond where it can usefully be received. Many sources unintentionally emit power in the form of radio signals. Low-power unlicensed devices are already permitted in many bands. Thus a licensed device receives not only desired signals, but also unwanted signals from transmitters in nearby bands, distant transmitters in the same band, unintentional radiators, and unlicensed devices. It is impossible to stop all of these unwanted signals. An absolute interference ban in a band is impossible. Therefore wireless receivers are designed to accommodate a certain level of interference.

It is when the interference power becomes too large relative to the received signal that performance degradation occurs. Performance degradation can manifest itself as lower data throughput, lower voice quality, or video distortions, depending on the service. A definition of when this degradation is too much is required for each service. In principle it should only be considered too much if it is observable by the end user. For instance, a source of interference may cause more errors in a digital signal, but, if the end user can not differentiate the performance with and without the interferer, then it is negligible. A period where the degradation to a received signal is significant is defined as an *outage*. It is beyond the scope of this paper to define an outage since it will vary by service. We emphasize that this definition is the heart of any interference framework. Though we do not define it here, we assume an outage can be and is defined by the unlicensed rules.

Harmful interference should be defined in terms of these outages. We define some potential licensed receiver models that define how interference is measured and classified as harmful relative to the licensed receiver.

a) Conceivable per Receiver Interference: If there exists some conceivable configuration of licensed and unlicensed device that can cause an outage in the licensed receiver.

b) Observed per Receiver Interference: If a licensed receiver outage occurs under typical usage of the licensed and unlicensed device.

c) Extended per Receiver Interference: If a licensed receiver outage occurs under typical usage for more than a specified fraction of the time (e.g. no receiver can experience an outage more than X minutes per year).

d) Widespread Interference: If more than a specified frac-

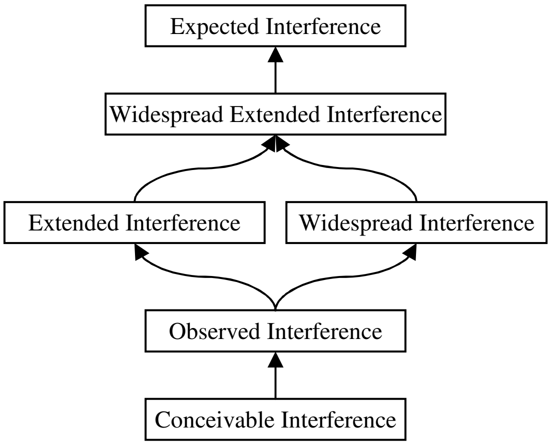

Figure 2: Licensed Receiver Model Relationships

tion of licensed receivers experience an outage at any time (e.g. not more than Y% of receivers experience an outage at any time).

e) Widespread Extended Interference: If more than a specified fraction of licensed receivers experience an outage for more than a specified fraction of the time (e.g. outages affecting more than Y% of receivers can not exceed X minutes per year).

f) Expected Interference: If more than a specified fraction of licensed devices experiencing an outage, averaged over time (e.g. no more than Z% of devices experience an outage on average).

The relationship is shown graphically in Fig. 2. As indicated by the arrows, a licensed receiver model lower on the graph can be used to satisfy a model higher on the graph. For instance, if no outages are ever observed than all of the higher models of interference are automatically satisfied.[2]

The first three models are on a per device basis. It is enough for even one licensed receiver to violate the model conditions in order for harmful interference to be claimed. Extended per Receiver Interference is defined for a given measurement period. Too short a period (e.g. one hour) will not properly capture long term unlicensed performance. Longer periods will better capture this long term performance and can also capturing egregious violators quickly. As an example if the outage allowed per year is one hour and this is met in the first day an unlicensed device begins operation, then the model is already violated. The next three are aggregate standards[3] defined for some set of licensed receivers. Individual licensed receivers may have sporadic or long outage periods as long as the set of licensed receivers meet the aggregate criteria. The licensed receiver set could be defined by geographic area, type of usage, and type of device; for instance, television receivers in the Denver MTA[4]. Note also that the criteria (except the first) are defined for actual outages of operating licensed receivers. A receiver that is turned off can not experience an outage. In particular a receiver that is on for less than X minutes can not ever violate the extended interference criteria.

Outages can occur even with a stringent limit on other devices on or near the licensed band. Users may be operating far from the licensed receiver outside the defined coverage area and therefore have signals too weak to be reliably received.[5] Similarly the device may be located in an area where coverage was not intended such as in the basement. The defined coverage area may specifically allow that some licensed devices suffer outages.[6] The signal may be susceptible to natural interference such as caused by lightning or solar flares or variations due to season and weather. The receiver device itself may suffer outages that cause loss of service (e.g. when there is a power utility outage, or when a user misconfigures the device). Finally, the licensed transmitter might have planned or unplanned service outages for maintenance or due to equipment failure. Thus, when evaluating harmful interference caused by a new unlicensed device it must be within the context of these pre-existing outage events. In particular, a harmful interference standard can not be set more stringent than is caused by these preexisting outages.

C. *Unlicensed Device Model*

For a licensed receiver model selected from the choices in the previous section, under what conditions do we measure whether the unlicensed rules comply with the standard? We define several unlicensed device models that specify the scope of unlicensed device activity that is considered relevant to harmful interference:

a) Per Usage: a particular usage of a single unlicensed device.

b) Per Device: a single unlicensed device under every allowed usage.

c) Bounded Deployment: a deployment of up to x devices under every allowed usage.

d) Unbounded Deployment: any size deployment under every allowed usage.

Enforcing according to per usage is the weakest. If some particular usage in the field is assessed for harmful interference and found in non-compliance, the unlicensed user could continue operating the unlicensed device(s) in other complying uses. Conversely, by specifying the usages for which compliance is measured, other extreme uses that might surely lead

---

[2] To clarify the relationships, two further examples are given here: If no device ever experiences an outage more than X minutes per year (extended interference) than an outage exceeding Y% of the devices will not occur for more than X minutes per year (widespread extended interference). Similarly given the X and Y of widespread extended interference, the expected interference is $Z = (100 - Y) X/M + Y$, where M is the number of minutes in a year.

[3] Aggregate here refers to the total effect across many licensed receivers. It is not related to the issue that a receiver may suffer an outage as a result of the sum of multiple unlicensed device signals. This concept is captured in the unlicensed device model.

[4] Major Trading Area, Rand McNally 1992 Commercial Atlas & Marketing Guide, 123rd Edition, pp. 38-39.

[5] Despite being unreliable, it still may be a useful service. A user may prefer the programming of a distant radio station even though the signal quality is poor.

[6] TV bands allow for outages at the defined edge of coverage.

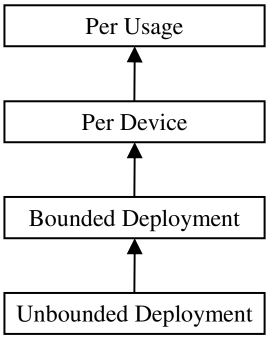

Figure 3: Unlicensed Device Model Relationships

to noncompliance can be excluded (for instance operation of a device in an airplane). Thus in this approach permitted and excluded uses are specified as part of the license rules. Per device enforcement implies that if any permitted usage of an unlicensed device is found to be in non-compliance, then the unlicensed device rules are not in compliance. These compliance models apply to a single device.

The aggregate licensed receiver models are unlikely to be violated by a single device. In some cases it may be the usage of many devices that is required in order to violate an aggregate measurement. Or, the aggregate of signals from multiple unlicensed devices may be required to generate outages in any single licensed receiver. Therefore, the last two unlicensed device models consider the aggregate effect of unlicensed devices. Like the aggregate measurement models they are for a given set of unlicensed devices defined by geographic area, type of usage, and type of device. For some unlicensed uses it may be possible to show that each unlicensed device contributes some finite component to the interference and an exceedingly dense deployment might cause harmful interference according to the measurement models. Therefore the first aggregate compliance model allows for an upper bound on the number of unlicensed devices considered for harmful interference. This does not imply that the number of unlicensed devices will be limited; it only provides a standard for judging compliance.[7] The most stringent model is the last which allows for an unlimited deployment of unlicensed devices. In a situation where it might be conceivable for an unbounded deployment to cause harmful interference suggesting the bounded deployment model, if it is expected that other factors will provide sufficient bounds, then for the sake of simplicity and to provide assurances to the licensed users the unbounded deployment might be used.[8] The relationships between models are shown in Fig. 3. The arrows indicate that achieving a lower level of compliance implies the higher compliance models are also satisfied.

D. *Interference Evaluator*

Several parties are involved in the unlicensed operation. These include the licensee, the unlicensed device manufacturer, the licensed receiver user, the unlicensed device user, and the regulator. With whom is the burden of showing compliance or non-compliance? And to whom is it necessary to show?

Embedded in these questions are several models and these should be explicit. The first is whether the burden of proof is on showing non-compliance or on showing compliance with the standard. One might argue that existing licensed services have enjoyed operation without the additional interference permitted by a new set of unlicensed rules and therefore the burden is on the owners and manufacturers of the unlicensed devices to demonstrate compliance. Alternatively, a licensed band may be viewed as under-utilized and the burden is on the licensee to monitor and demonstrate any harmful interference as part of their continued use of the band.

Historically the licensee has claimed harmful interference to the FCC or in courts of law. But, if unlicensed devices wish to use more aggressive measurement models that are more difficult to substantiate compliance or non-compliance then the burden may be on the unlicensed device users and manufacture to monitor the compliance. These efforts can be financed by, for instance, a fee on the sale of the unlicensed devices.

As more computing and sensing capabilities can be integrated into radio devices, there is the potential for certain levels of self monitoring by the licensed or unlicensed devices.

As in the previous sections, we do not advocate a specific model. We only advocate that some model should be made explicit in the unlicensed device rules.

E. *Remedy*

If harmful interference is shown according to a model, what are the possible remedies? First, it should be emphasized, that harmful interference caused by devices that are not following the unlicensed device rules has a clear remedy which is for these devices to cease operation. So, the question applies to the case when devices are following the unlicensed rules but yet harmful interference is determined. Broadly, the answer is to change either

a) the unlicensed device rules,

b) the definition of harmful interference, or

c) the rules for licensed use.

Changing the unlicensed device rules might be as simple as creating or adding to a list of unlicensed device excluded usages[9]. At an extreme, the unlicensed operation rules might be abolished. Or, they might add stipulations on installation such as requiring professional installers. Or, they might change operational parameters such as allowed power levels. If there is an expectation that operational parameters might be changed over time, then, the unlicensed rules should contain

---

[7] It might be as few as two devices to reflect the need for more than one device to lead to significant interference. Or, it might be set to a large number like 100,000. In the latter case, many licensed devices may be suffering outages because of a very large unlicensed device deployment. The bound can be used to set a threshold of importance for the unlicensed devices where their activity can not be considered harmful.

[8] For instance, while unbounded density in garage door openers might be a problem, typically only one or two garage doors are deployed per dwelling.

[9] For instance, some rules explicitly prohibit the use of certain unlicensed bands for radio control toys.

provisions that mandate updating the firmware that controls the unlicensed device. These rules might integrate prompting mechanisms such as generating warnings or refusing to interoperate when a device with older firmware attempts to communicate with a device having a later firmware.

The second alternative is to redefine harmful interference. Over time, it might be shown that more harmful interference is acceptable (changing the parameters of the licensed receiver model) or that it can be measured in a better way (change the model itself). The unlicensed rules may spawn socially important applications that overshadow the original licensed usage and more leeway might be given to the unlicensed devices such as allowing more minutes of outage per year. Minutes of outage may be found inappropriate and a different model chosen that better reflects the impact on licensed users. Another possibility is that the licensed user wants to claim harm even though no harmful interference is shown according to the measurement model. This might lead to a tightening of the parameters or the model.

Finally, the licensed use might be changed. For instance some licensed channels might be set aside for unlicensed use. In the case of the microwave links in the 1910–1930MHz band, a close substitute (fiber optic cables in this case) was found and a mechanism for moving these users out of the band was established. The licensed rules might be modified to better accommodate the unlicensed user. For instance, licensed receivers might be required to include a beacon so that unlicensed users can better avoid the licensed usage. Or, licensed users might be permitted higher transmit powers.

It should be clear that potential remedies should be considered at the time the unlicensed rules are formulated. If remedies are explicitly incorporated into the rules, then, licensed users will be more willing to accept the harmful interference potential and less likely to insist on extremely limiting definitions of harmful interference. Conversely, unlicensed device manufacturers are more likely to invest in a technology if the potential for it being banned or made obsolete is minimized and a potential future migration path is already defined.

III. A STANDARD FOR HARMFUL INTERFERENCE IN THE TV BROADCAST BANDS

For the licensed operator, interference from unlicensed devices is unavoidable since both intentional and unintentional radiators can produce radio frequency power in the licensed band. This unwanted power can impact licensed performance in the worst case if the unlicensed source is placed sufficiently close to the licensed receiver antenna.[10] The FCC has recognized that assuming a worst-case interference regime will not maximize the social benefit of the spectrum.[11] The Spectrum Policy Task Force concluded that for unlicensed devices, "Using typical worst case predictive interference models would significantly reduce the potential of these devices to operate."[12] Licensed devices always have the potential of degraded performance from unlicensed devices. Yet, in practice most licensed devices work well. This suggests that the harmful interference of unlicensed devices should be measured according to their impact in practice and a conceivable device interference model is inappropriate.

In the Multichannel Video Distribution and Data Service (MVDDS) proceedings[13] the FCC reiterated that "impacting some existing customers of a service to an extent that did not rise to the level of harmful interference was outweighed by the benefits of adding new services or capabilities to a frequency band."[14] In the proceedings, the FCC set operational parameters based on a criterion that MVDSS does not increases the baseline Digital Broadcast Satellite (DBS) outage rate by more than ten percent per year. This requirement is interpreted as an average standard and not for each individual receiver.[15] "The ten percent benchmark represents an insubstantial amount of increased unavailability and does not approach a level that could be considered harmful interference."[16] In this way the FCC set a standard that it deemed as conservative for the existing licensed operators while providing entry for other services. This suggests that a similar expected interference standard can be applied to unlicensed devices in the TV broadcast bands.

To determine a reasonable outage probability, we look at Broadcast TV availability. Broadcast TV availability is not monitored by regulators but even if it were 100% available, other factors would limit its use by TV receivers. For instance, the availability of power from utilities varies (between utilities and from year to year) from 99.9% to 99.99%,[17] and so receivers and hence the broadcast service is unavailable for use for 0.1% to 0.01% of the time. DBS service is similar to TV and is considered "extremely reliable with typical service availabilities on the order of 99.8 to 99.9 percent."[18] Broadcast TV

---

[10] For instance operating a power saw or drill near a TV or radio readily produces strong "static".

[11] Margie, Paul. *Efficiency, Predictability and the Need for an Improved Interference Standard at the FCC.* Telecommunications Policy Research Conference (TPRC) Arlington, VA, Sept. 19, 2003 He provides several examples that illustrate this point.
(http://tprc.org/papers/2003/214/HarmfulInterference.pdf)

[12] *Spectrum Policy Task Force Report*, ET Docket No. 02-135. November 2002. pg. 13. (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-228542A1.pdf)

[13] In Re Amendment of Parts 2 and 25 of the Commission's Rules to Permit Operation of NGSO FSS Systems Co-Frequency with GSO and Terrestrial Systems in the Ku-Band Frequency Range; Amendment of the Commission's Rules to Authorize Subsidiary Terrestrial Use of the 12.2-12.7 GHz Band by Direct Broadcast Satellite Licensees and Their Affiliates; and Applications of Broadwave USA, PDC Broadband Corporation, and Satellite Receivers, Ltd. to Provide A Fixed Service in the 12.2-12.7 GHz Band, *Memorandum Opinion and Order and Second Report and Order*, 17 FCC Rcd. 9614 (2002) (hereinafter *MVDDS MO&O and Second R&O*).
(http://wireless.fcc.gov/auctions/53/releases/fc020116.pdf)

[14] *MVDDS MO&O and Second R&O*, at para. 32

[15] *MVDDS MO&O and Second R&O*, at para. 84

[16] *MVDDS MO&O and Second R&O*, at para. 72

[17] *Electric System Reliability Annual Reports*, California Public Utilities Commission. January 24, 2005.
(http://www.cpuc.ca.gov/static/industry/electric/reliability/reliability_reports.htm) These contain measures of the so-called SAIDI, minutes of sustained outages per customer per year. They range from 50 to 600 minutes per year or 99.99% to 99.9% reliability. Further within a single service provider, the SAIDI varies by large factors of at least two from year to year.

[18] *MVDDS MO&O and Second R&O*, at para. 67

TABLE I
DIFFERENT KINDS OF OUTAGES.

Case	TV Sched.	TV Signal	Cable Signal	Line Power
Normal	On	Good	Good	Good
Interference Outage	On	Bad	Good	Good
Cable Outage	On	Good	Bad	Good
Broadcast Outage	On	Bad	Bad	Good
Power Outage	On	X	X	Bad
Scheduled Outage	Off	X	X	X

coverage is defined by the $F(50,90)$ curves which nominally provides 90% service availability to 50% of the users at the edge of each station's service.[19] When considering new higher power operation, broadcasters advocated "that a *de minimis* standard for permissible new interference is needed to provide flexibility for broadcasters in the implementation of DTV."[20] They argue that a 2% absolute increase in interference between TV stations is acceptable. This data collectively suggests that 99.9% is a conservative upper bound on the availability of broadcast service. This bound with the above FCC MVDSS 10% standard suggests a standard for the broadcast TV bands of no more than 0.01% (1 in 10,000) TV's can be adversely affected by the unlicensed devices on average. Given the range of availability values and the small fraction that results, this value is small in both a relative and absolute sense and exercises an abundance of caution.

So far, we have defined the licensed receiver model as an expected interference model with a limit on expected outages at any time of 0.01%. It is expected that the unlicensed devices in this band will be widely deployed. The question then is whether the unlicensed device model should be for a bounded or unbounded deployment. An analysis model presented later in this paper shows that indeed an unbounded deployment will exceed this definition of harmful interference. The model also shows it is well within the technology of the unlicensed devices to achieve unlicensed device densities in excess of 1000 devices per square kilometer in typical urban and suburban areas without violating this harmful interference standard. In dense urban areas unlicensed device densities in excess of 20,000 devices per square kilometer can be supported. These numbers are similar to their respective population densities.[21] Given the densest likely deployment is bounded by one unlicensed device per person; effectively an unbounded deployment can be used.

The main challenge in this measurement scenario is defining an evaluation method. A direct approach would monitor TV signals around the TV signal coverage area to sample the expected outage probability. Simple units could monitor the television signal as measured over the air. It could also measure the same signal as measured via cable and also the input utility power. It could track the times when the broadcast, cable, and power signals are good and bad to determine the different kinds of outages as shown in the Table I.[22] Further fidelity can be gained by determining which broadcast outages are scheduled (e.g. every night between 2am and 6am), and which are unscheduled.

With this data, the total outage time (Interference plus Power plus Unscheduled Broadcast outage times), t_{out}, can be recorded as well as the Interference Outage time, t_{int}. Unfortunately, t_{int} does not discriminate between other types of interference (e.g. natural sources) and unlicensed device interference. But, it does bound the outages that can be attributed to the unlicensed devices. Who should be responsible for monitoring? The monitoring data is most valuable to the broadcasters since in additional to monitoring for harmful interference, they can monitor their general program quality as it is presented to their viewers.

What combinations of outages would constitute harmful interference? By the logic developed above, harmful interference occurs when

$$t_{int} > T \times 0.0001 \quad \text{AND} \quad t_{int} > (t_{out} - t_{int}) \times 0.1,$$

where T is the total length of the observation period (e.g. one year). In words this says that the interference outage must be greater than an absolute threshold and above a threshold relative to other types of outage.

What remedy is available when harmful interference is determined? The unlicensed devices that operate in the licensed TV bands are expected to be relatively capable devices able to avoid licensed channels, select different power levels, and generally have a sophisticated software model. In this case, a remedy for harmful interference would be to require manufacturers to include software updates as an integral feature in their design. These updates could either lower maximum transmit powers or tighten the criteria used in avoiding licensed TV bands. The latter might be preferable since it is less likely to affect existing unlicensed services. In rural areas higher power is important and there are plenty of unused spectrum opportunity alternatives even if the choice is more conservative. In urban areas, the devices are likely already operating below the maximum allowed power and so the main opportunity to reduce interference is through better avoidance. The point is not to decide here what the precise remedy is, but, to show that it is something that could be included in the unlicensed rules.

So in conclusion we argue the measurement scenario for unlicensed device operation in the TV broadcast bands should be based on an expected increase in service outages of 0.01%

---

[19] Advanced Television Systems and Their Impact upon the Existing Television Broadcast Service. FCC 87-268. Fifth Report and Order. Released April 21, 1997. Appendix A, "Rule Changes", Part 73.625, (a).

[20] Advanced Television Systems and Their Impact upon the Existing Television Broadcast Service. FCC 87-268. Memorandum Opinion and Order on Reconsideration of the Sixth Report and Order. Released February 23, 1998. at para. 79.

[21] The density of New York County, the densest in the US, is 27,000 people per square kilometer according to 2003 population estimates by the US Census Bureau. *New York County Quick Facts*, http://quickfacts.census.gov/qfd/states/36/36061.html

[22] We reiterate that a definition of outage is necessary in order to apply a measurement scenario.

in an unlimited deployment of unlicensed devices as measured by television signal monitors operated by TV broadcasters. The remedy would be based on including a method for post-purchase modification of the radio parameters.

IV. INTERFERENCE MODEL

An interference model is developed in this section. The model computes the fraction of licensed devices made unavailable because of unlicensed operation. It considers factors such as the type of unlicensed signal modulation, antennas, ability to detect active licensed channels, power control, and activity levels of the licensed and unlicensed devices. Examples using the model suggest that the small increase in interference advocated in the previous section allows unlicensed device densities over 1,000 unlicensed devices per square kilometer. A high density apartment building example is also analyzed. It is found that there are mitigating factors in this case that supports over 20,000 unlicensed devices per square kilometer.

A. *General Setting*

The model considers a large area that is covered by some licensed broadcast service. There are many licensed receivers within the area. In this area is a deployment of unlicensed devices. The concern is the interaction of the transmitted unlicensed signals with the licensed broadcast signal at the licensed receivers. The combination of multiple unlicensed signals is not considered. Given that propagation tends to spread signal powers over many orders of magnitude, it is likely that one of the interfering signals is much stronger than the others and any service outage is a result of this one strongest signal. Conversely, a single unlicensed device, if it is well designed, is unlikely to interfere with many licensed receivers, if any. Hence, the interference is in the context of a widespread and dense deployment of the unlicensed devices and we examine the expected total number of licensed devices that will experience an interference outage.

In this section we capture the notion of an outage through a parameter $r_{\min}$. This is how close an unlicensed device can approach a licensed receiver before the licensed receiver performance degrades. It is performed under worst case conditions of the two device antennas aimed at each other and so on. In principle this is a simple measurement to make in a laboratory setting and could be the basis of a device compliance model.

But, $r_{\min}$ is a worst case measurement. The unlicensed devices can have mechanisms to avoid interference. They might have mechanisms for avoiding the broadcast channels; use directional antennas; control their power to only what is needed; transmit only part of the time; and use sophisticated modulation schemes. Further some licensed devices may obtain their signal from cable or a recording device and thus be immune to interference.[23] The model is designed to capture these factors.

B. *Model Summary*

Mathematically, the model consists of a series of factors that account for the different elements that influence the number of disrupted licensed devices:

$$F = r_{\min}^2 PCEG_{UL}G_L MN_{UL} / A$$

where

F	is the expected fraction of licensed devices with service disrupted.
$r_{\min}$	is the minimum separation between the unlicensed and licensed device in order to prevent the unlicensed device from interfering with the licensed device under typical operating conditions near the boundary of the broadcast coverage area. This is done under worst case conditions of the licensed device transmitting at maximum power on the same channel as the licensed device with both devices antennas pointing at each other.
P	accounts for the use of power control by the unlicensed device. $P \le 1$.
C	accounts for the ability of the device to avoid communicating on the same and adjacent channels as the licensed device. $C \le 1$.
E	is the fraction of devices on and eligible to interfere with each other $E \le 1$.
G_{UL}	accounts for the antenna gain pattern of the unlicensed device. $G_{UL} \le 1$.
G_L	accounts for the antenna gain pattern of the licensed device. $G_L \le 1$.
M	captures all the model constants. A typical value is $M = 2.9$.
N_{UL}	is the number of unlicensed devices in the area.
A	is the size of the area.

Most of the factors are less than or equal to one. In some cases they are very small and are the key to achieving a small F. The last four factors are outside the influence of the unlicensed device designer. But the first five factors can be affected by the unlicensed device design. Different modulation techniques, maximum transmit power, etc. can all affect $r_{\min}$. The sophistication of power control algorithms affects P. The fidelity of channel detection techniques strongly affects C. The level of device activity affects E. The unlicensed device's antenna affects G_{UL}. Technical readers are encouraged to read the model details in Appendix A as important assumptions and derivations are presented there. Less technical readers may safely go to the next section.

C. *Examples*

To help interpret the model we give several examples. For the examples we will use an unlicensed device density of $N_{UL}/A = 1000$ devices/km^2.

---

[23] Some studies have shown that an unlicensed device could potentially affect cable TV reception, but, the measurement conditions are highly unlikely to occur in practice.

Consider a low power device operating under the following conditions: r_{min} = 100m; the unlicensed devices have an omnidirectional antenna; the licensed antennas are approximated by 60 degree ideal sectorized antennas; the broadcast pathloss exponent is $a = 2$, the pathloss exponent for unlicensed devices is $b = 4$; the joint shadow fading is σ = 7dB; and power is controlled uniformly over a log scale between max power and 20dB below max power. The fraction of: unlicensed devices turned on is 25%; licensed devices turned on is 25%; and licensed devices listening to broadcast channels is 25%. As a reference, we consider the worst case that the licensed device is using a random channel. In this case, $P = 0.39$; $C = 0.02$; $E = 0.016$; $G_{UL} = 1$; $G_L = 0.17$; and $M = 2.9$. Combining these factors yields an expected fraction of disrupted licensed devices of about 6/10,000. This suggests that even limited additional work to avoid using known TV channels would reduce the expected number of disrupted devices to an insignificant level. For instance if the unlicensed device could determine the presence of and avoid licensed broadcast channels (and adjacent channels) 90% of the time and the remaining 10% of the time the channel choice is random, then $C = 0.0022$, and the fraction of disrupted licensed devices is less than 1/10,000. We emphasize that these number are for device densities that correspond to millions of unlicensed devices across a major metropolitan area. A suburban or rural area, which we might expect to have factors of 10 to 100 lower density, would have similarly reduced fraction of disrupted devices. For example a rural area with 100 devices per square kilometer would have a fraction of disrupted devices less than 1/10,000 even if the unlicensed devices chose channels randomly.

Consider next a high-power device operating under the same conditions as for the low power device except that: r_{min} = 10km; the unlicensed antennas are high-gain 30 degree sectors; $b = 2$; the fraction of unlicensed devices turned on is 50%; and again random channel selection. In this case, $P = 0.21$; $C = 0.02$; $E = 0.031$; $G_{UL} = 0.083$; $G_L = 0.17$; and $M = 5.8$. Combining these factors yields an expected fraction of disrupted devices of close to 1. This implies the unlicensed devices must be much more reliable in detecting and avoiding broadcast channels. For instance, if the licensed channel could be detected and avoided 99.99% of the time (all but 50 minutes per year) then, $C = 2.\mathrm{x}10^{-6}$ and the expected fraction of disrupted licensed devices is less than 1/10,000. The same level could be achieved in a rural area if licensed channels could be detected 99.9% of the time (all but 8 hours per year).

The greatest potential for interference exists in dense settings, for instance in apartment buildings where the effective density could be above 1000 devices per square kilometer. There are several mitigating factors in this case. Such buildings are more likely to have wired Internet access (i.e., less likely to be high-power unlicensed devices). Similarly, they are more likely to have cable TV. Such buildings are often in urban areas where broadcast signals are stronger and easier to detect. For low-power devices used within these apartments, the communication distances are likely much smaller and thus require less transmit power. Social factors should not be ignored either. If some neighbor is too loud, you can ask them to be quieter. Similarly, if a neighbor places a wireless device too close to your TV, you can ask them to move it.[24]

We can incorporate these factors into the model by assuming half as many licensed devices listening to broadcast channels, channel detection can be twice as accurate, the power is controlled uniformly over a log scale between 10dB below max power and 20dB below max power, and half of all potential disruptions can be solved by social means (i.e., $P = 0.19$; $C = 0.0012$; and $E = 0.0039$). With these changes to our illustrative examples, more than 20,000 unlicensed devices per square kilometer could be supported without exceeding the harmful interference threshold.

D. Discussion

The interference model shows that high-power and low-power unlicensed devices can successfully coexist with licensed devices. The model estimates the fraction of licensed devices disrupted by the presence of the unlicensed devices. It incorporates a range of factors that can influence the final result. All of the factors can be easily estimated or directly measured. In particular, one of the most influential factors, r_{min}, could be measured through direct measurement. This suggests that a device compliance model can be developed based on factors inherent to the device. In other words, the definition of compliance could be defined in terms of a bound on r_{min} as measured in a lab.

The examples indicate high-power devices will need to pay special attention to how they choose transmit channels since they have a strong potential to interfere over a large area if they choose an active licensed channel. Low-power devices can be much less reliable in this procedure and yet have minimal impact on licensed devices. They are helped by being lower power. Because they are envisioned as being used indoors or at ground level, the walls and clutter (as expressed by the larger pathloss exponent) provide more isolation. But, since the licensed channel avoidance procedure is likely to be more ad hoc its reliability may be more difficult to assess.

The examples in this paper assume a harmful interference standard defined as no more than 1 in 10,000 licensed devices will suffer outages because of the unlicensed devices. Such a standard exercises an abundance of caution considering that other sources of interference may cause more than 10 times as many outages. It should be clear from the model that such extreme caution imposes direct and substantial penalties on the deployment of unlicensed devices. For instance, if the harmful interference standard admitted 10 times more outages, the model would immediately support a 10 times higher unlicensed device density.[25] Therefore, the harmful interference

---

[24] General guidelines used in Part 15 rules development are (a) self-interference between two devices operated by the same household is not considered; and (b) between households a working assumption is 10m separation and wall attenuation of at least 10dB. The original NPRM, supra 1, footnote 50 reiterates this assumption. This suggests that some disrupting interference in such high density settings may not be considered harmful interference.

[25] Or, it would ease the design challenge for the same density by a factor of 10. For instance, using a 1 in 1000 standard in the illustrative example of a high-power device, the unlicensed devices would have to detect and avoid licensed devices 99.9% of the time (i.e., incorrect no more than 8 hours per

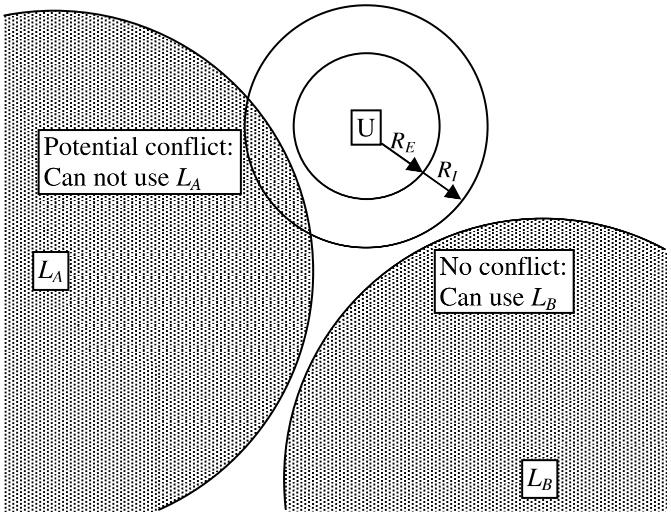

Figure 4: Unlicensed device, U, considers its location error, R_E, and interference range, R_I, when deciding if it can avoid interference with licensed channels L_A and L_B.

standard in the previous section should be considered a model and the specific interference level should be set with careful consideration.

V. CHANNEL AVOIDANCE

As described in the previous section avoiding licensed channels is a key factor in enabling non-interfering operation, especially for high-power unlicensed operation. It is not possible to always avoid these unlicensed channels and so it is a matter with what probability the licensed channel usage can be identified and avoided. Low-power unlicensed operation requires a mildly accurate method (at least 90% of the time). High-power usage must avoid licensed channels with an accuracy of more than 99.99%. Each of these cases may need different methods to achieve the necessary accuracy. Further the methods need techniques for assessing their reliability.

The NPRM suggests three methods for avoiding licensed channel usage: combine unlicensed device geolocation with a channel usage database; use dedicated beacon signals such as from broadcast stations; and directly detecting transmitted broadcast signals.[26] Other papers and NPRM comments have addressed these methods piecemeal or within a narrow context. This paper attempts to make a comprehensive view of these methods and their variants in order to assess which would be viable in a widespread deployment of unlicensed devices and to differentiate the relative merits of each. The analysis shows that there exist technically viable variants for each of these methods and it is a matter of deciding where to place the relative burden of implementation. The next three sections examine the three NPRM options in detail followed by a discussion and conclusion.

A. *Channel Usage Database*

In this method, a device estimates its position and checks a database in order to identify channels that are being used for licensed services in the vicinity of the unlicensed device. To work, a device must have an estimate of its position, an estimate of its position error, an estimate of its interference range, and access to a database of potential licensed service areas. Conceptually, the unlicensed device creates an area that accounts for its position, position accuracy, and interference range and intersects this with licensed channel service areas. An empty intersection implies the channel can be considered unused by the unlicensed device. The concept is shown in Fig. 4.[27]

More accurate position estimates can enable more channels to be used. But, even low accuracy can yield unused channels if the error is accounted for. For instance, a position error of 10 km and an interference range of 1 km can yield many unused channels, especially in rural areas where channels go unused over larger areas[28]. So, position methods should be judged on their ability to bound the error rather than the magnitude of the error. In particular the standard for the devices should be that they have an "X% localization error bound," where the value of X is specified in the standard. For instance, if a device claims to have a 99% localization error bound of 100m, then the device locates itself to within 100m 99% of the time. Other devices may have a wider or narrower 99% localization error bound. If low error is important then market forces will drive the adoption of more accurate methods.

The location methods can be divided into three categories: self-localization, operator-configured location, and network-based location. The device can use information that it automatically collects itself such as using GPS or broadcast information from cellular base stations. The position can be obtained from an external source. It can be hand configured by the installer or the end-user. Or, it can be determined from communicating with other unlicensed devices that may have a known position. These methods are described below and can be used individually or jointly.

GPS is generally accurate and reliable for open outdoor locations. For instance it is widely used on CDMA2000 cellular base stations for position and timing. Indoors and in cluttered terrain that blocks satellite signals accuracy degrades or localization fails. The GPS receivers also add expense to the unlicensed device. Therefore GPS is better suited to fixed outdoor tower sites rather than indoor or low-cost unlicensed devices. GPS is not the only or necessarily the best localization choice and other methods might be considered.

When configured by an operator, the accuracy can be as high as needed. There is a possibility of misconfiguration especially for devices that move often or are configured by end-

---

year) instead of 99.99% of the time (i.e. incorrect no more than 50 minutes per year).

[26] NPRM, para. 20.

[27] The circular areas are for illustration. The service areas can be based on sophisticated propagation models or measurements yielding complex service areas. The licensed service areas need to be generated only once and so could be quite complex. Unlicensed interference areas are regenerated many times for mobile devices and might use conservatively computed circles for simplicity. Fixed unlicensed devices could afford to generate more precise areas.

[28] The poorest county in the US is located in central South Dakota. The least densely populated county in the US is located in central Alaska. Location errors of 100 kilometers in these areas would still yield unused channels.

users. This method is better suited to fixed sites that only have to be correctly configured once and are more likely to be professionally installed.

Network-based approaches allow devices to learn of their position from other devices which may have an accurate position. In this approach only a subset of the unlicensed devices need a localization method. For example, if an indoor unlicensed device can communicate with another outdoor device which is able to self-localize via GPS, then it could use the GPS position with a bound on the position offset to make the localization. To emphasize, as long as such techniques have a reliable bound on the error, then the interference avoidance can be made reliable.

The database requires a database provider, an access method, and a model for updating the information in the database. Providing a reliable database for this type of information is similar to many commercial applications and it is expected that commercial database software can easily support the location database. Who should provide this database or pay for it is outside the scope of the paper to discuss in detail. The cost per licensed device is small and might be supported by an unlicensed device surcharge. [29] Since it is in the licensed service providers' interest for the database to be accurate, they might pay to operate and maintain the database. Or, it might be treated as a public good provided by the federal government.

The database is most likely available over the Internet since it is pervasive, flexible, and low cost. Of course, not all devices have access to the Internet or the device is intending to use the wireless connection to gain access to the Internet. The database could be preloaded into the device but this would not address changes over time. The device might be temporarily connected to the Internet via another means to load a version of the database. Finally, the device could learn about the current state of the area from a network of existing devices.

Licensed usage is dynamic. Licensed broadcasters turn off transmitters at night. The digital TV transition is bringing TV channels in and out of service. Secondary users such as Part 74 users can come and go. Simple web based access to the database can enable these dynamics to be entered easily and potentially automatically by the licensed users. Clearly, it is in the licensed service providers' interest to keep its entries up-to-date. Database queries should be simple for the unlicensed devices and provide flexibility for the database to respond. For instance if the unlicensed device entered its position, position error, and EIRP transmit power[30], then the database could compute what channels could be used without interference based on the location of licensed receiver service areas.

How often should an unlicensed device query the database? If the database is purely reactive, in which updates are entered only when a licensed usage changes, then the answer depends on how much ahead of time the changes are entered. For instance if changes are entered one hour in advance, then the database should be queried on an hourly basis. It could be argued that there is no satisfactory time period. Longer periods make the database less reactive especially to short term licensed uses. Shorter periods will cause excessive queries to the database and add more overhead to the unlicensed device communication.

The database may not always be available due to scheduled or unscheduled service outages. These can prevent access to the database and cause floods of queries when the database returns to service. Making the database and the network connectivity more reliable may be prohibitively expensive. Even if the database is reliable the unlicensed device connectivity may not be reliable and suffer availability outages.

These access problems would be alleviated if the databases incorporate new information proactively rather than reactively. For instance if a new channel will be used starting on a certain date, the database would include this information many days in advance so that unlicensed devices could plan and avoid the new channel even if the database is unavailable on the transition day. Similarly, Part 15.244 devices could enter planned event usages (time period and location) into the database well in advance. It would not be unreasonable for the database to be maintained so that information is valid over a future period (e.g., 48 hours). A query would enable an unlicensed device to operate over this period, even if the database was down at the moment the unlicensed device wished to operate. Unlicensed devices which do not have a valid query would not be able to operate. Such a failsafe, "no database, no transmit" rule would be one way to provide a highly reliable approach to avoiding interference.

Devices which are not connected to the Internet can use requests obtained through other devices. For instance, consider the following high-power operation model. An operator wishes to provide broadband Internet access over a large area. A central radio base station is installed outdoors. The base station is connected to the Internet through a wired connection. At the time of installation or using an integral geolocation method, the radio estimates its location. It makes a worst case assumption of its interference range (i.e. an overestimate that includes its client devices), queries the channel usage database over the Internet and assesses what channels it has available for operation. Meanwhile, radio transceivers are installed at customer premises. These radios, when turned on, passively scan and listen for the base station signal. This signal identifies valid uplink channels that can be used by the customer radio. The base station queries the channel database periodically (e.g., hourly) to ensure it has the latest information and adjusts beacon information accordingly. In this way, the customer radios can be kept simple and low-cost (techno-

---

[29] As an example of the cost of such a database, consider 10 million unlicensed devices that connect to a database hourly. This yields 3000 transactions per second. Using data from 2001 for a Dell server running Microsoft SQL Server 2000, the approximate cost for the hardware, software, storage, and 3 years of maintenance in a 3000 transactions per second database with a 4 hour maximum down time is about $200,000. Transaction Processing Performance Council, TPC-W results, http://www.tpc.org/tpcw/results/tpcw_perf_results.asp (accessed June 1, 2005).

[30] Transmit power may be too restrictive a concept. The use of r_{min} could be more direct.

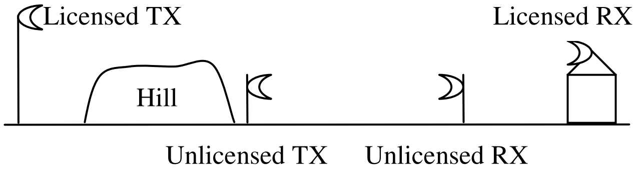

Figure 5: The hidden terminal problem and network detection.

logically equivalent to a cellular telephone)[31] while providing licensed channel protection assurances.

Security plays a significant role in this approach. Licensed devices rely on data from the database and from other licensed devices for channel information or localization. The devices need methods to authenticate the source of the information, and methods to prevent sources from repudiating information they provide. The database needs secure access to authenticate licensed users and to authorize appropriate updates. These updates should be subject to nonrepudiation methods. Privacy or anonymity methods are necessary to avoid network eavesdroppers from tracking device locations embedded in database queries. Finally, the database should be robust to denial of service attacks that could prevent legitimate database queries and updates. These security issues have efficient solutions today, but, must be considered an integral part of this approach to be effective.

B. Detecting Broadcast Signals

In this approach, the unlicensed devices attempt to detect the broadcast signals directly. This approach requires the least effort on the part of licensed service providers. The challenge in this method is the so-called hidden terminal problem as shown in Fig. 5. The unlicensed transmitter can have a good line-of-site to a receiver, but, not be able to detect the transmitter. Two solutions can be applied to this problem: better detection and networked detection. Signals can be detected at signal levels below what can be received.[32] Generally these techniques are more expensive and require detectors customized for each licensed service. They can be made less expensive by integrating the detection over longer periods, but, this directly reduces the available communication time and may not be fast enough to detect new licensed channel activity.[33] In networked detection, as is shown in Fig. 5, other unlicensed devices may be in a better position to detect the licensed transmitter and they can exchange information on license services that are detected.

We develop a model to assess the advantage of networked detection. In this model we consider unlicensed devices in an area that can communicate with each other. An individual device can sense potential licensed transmitters and detect a transmitter with probability D. Because the devices may be distributed in different places relative to the transmitter some unlicensed devices can detect the transmitter when others can not. It is enough for just one device to detect the transmitter for all devices it is able to communicate with to know about the transmitter. Therefore, the probability an unlicensed device detects a licensed transmitter is a function of whether it or any of its neighbors detects the licensed transmitter and whether it can communicate with any neighbor that has made a successful detection. Putting these factors together we derive in Appendix B:

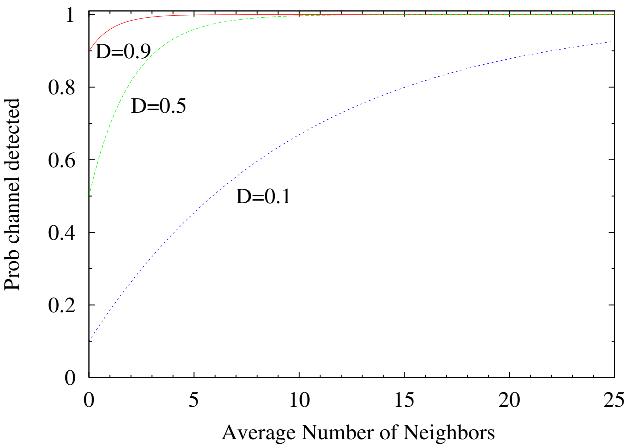

Figure 6: Networked detection probability vs. network size for different base detection probabilities, D.

$$\Pr[Detect] = 1 - (1 - D)e^{-DN},$$

where N is the average number of unlicensed neighbors able to communicate with an unlicensed device. Results of this model are shown in the Fig. 6. For a relatively high individual detection probability D (0.5 or higher) network detection quickly provides reliable detection as the number of neighbors increases. As few as 3 neighbors is enough to guarantee a greater than 90% network detection probability. For lower D more neighbors are required, but, high network detection probabilities are possible if enough unlicensed devices are networked together.

Network detection increases in reliability with unlicensed device density. As shown in the analytic model, the required detection accuracy increases in proportion to the unlicensed device density. However, the number of (one-hop) neighbors is proportional to the device density. Thus the detection gets exponentially better with device density. This shows that network detection has a positive feedback as the number of unlicensed devices increases that more than compensates for the increase in interference.

These detection methods are passive. They require the frequent monitoring of channels to detect the presence of new transmitters and to exploit channels that open up. These reduce the efficiency of this approach.

C. Beacon Signals

A transmitter beacon can consist of four types: per transmitter, area transmitter, unlicensed signaling, and receiver beacons.

---

[31] Cellular telephones follow a similar base station access procedure.

[32] Mark McHenry, ***"Dynamic Spectrum Sharing"*** Presentation to IEEE Communications Society, Joint Northern Virginia & Maryland/DC Section Meeting in McLean, VA, January 25, 2005

[33] The integration time may be longer than the longest period allowed without checking for new channel activity.

1) Per-Transmitter Beacons:

A direct approach to alerting the presence of a licensed service to unlicensed devices is for each licensed transmitter to have a standardized, easy to detect, simple to receive beacon. To simplify the search for these beacons, they should be located at carrier frequencies that are standardized for each licensed band. The beacon could be as simple as a carrier tone. This has the potential to interfere with the licensed signal or for spurious signals and harmonics from other bands to be detected. A more reliable approach would be to modulate the carrier with a random direct sequence spreading code[34]. The spreading code would make it much less likely that unwanted signals could lead to false positive detections. It could also spread the signal over a greater bandwidth so as to cause less interference to the desired licensed signal. There is an inherent tradeoff with the detection time (time that the spread spectrum correlator integrates to find a potential beacon), and the required power in the beacon signal. Longer detection time implies less power is needed in the beacon. However, it reduces the time an unlicensed radio can use for active transmission. This tradeoff can be exploited to determine an optimal balance between beacon power, detection time, and range. The beacon can encode information on the beacon signal such as the location of the transmitter, its transmit power, or a definition of its coverage area.

The advantage of this approach is more reliable channel detection while keeping full control of the beaconing with the licensed service provider. The beacon has the potential to degrade the service provider's service signal.

2) Area Beacons:

Instead of each transmitter having to integrate a beacon into its signal, a small amount of bandwidth could be set aside for dedicated beacons that would act as a service for all the licensed transmitters in an area. Being in a dedicated channel, they can be higher power. Using spread spectrum techniques similar to CDMA cellular service, the same beacon channel can be used throughout the country, with different offsets of the same spreading code used for different beacons to prevent inter-beacon interference. Each beacon can provide a low-data rate service that announces the frequency band, location, and coverage area of each licensed transmitter in the area. The required bandwidth can be small (e.g. 12.5kHz). The power can be relatively high (relative to the bit rate) so that the coverage is large at modest power (e.g. 100W). Approximately 1000 area beacons could cover the continental U.S.[35]

In essence this would be a push model for the database method in Section III with the exception that the information is limited to licensed transmitters in the area of the beacon. Like the database, the reliability and utility of this approach would be greatly improved if the information was provided on a proactive basis. For instance, if the information was certified as reliable for the next one hour, then, the unlicensed devices would use only a tiny fraction of their bandwidth to make hourly checks of the beacon. The beacon information would be derived from a licensed database. Like the database method, secure methods for licensed users to update their information are necessary. The beacons can independently choose the information they broadcast depending on their location and intended coverage area. The licensed users can be shielded from when beacons are added, moved, or removed. This provides a level of separation between the licensed users and the beacons. Licensed users edit the database. The beacons read the database. To avoid malicious overriding of the beacon information, it should be encrypted using a public key encryption technology where the private key is held at the central database. The beacons could go through a licensing process such that only licensed beacons can access the database. This would reduce the load on the database and help prevent denial of service attacks on the database.

Who would operate these licensed beacons? It is believed that since the beacons are low-power they would require modest investment to set-up. The beacon stations would benefit from using the high locations used by licensed broadcasters. Further it is in the broadcasters' interest that they are operated and setup well. This suggests that the broadcasters, either on their own or as a sub-contract from another entity, would be well suited to operate the beacons.

This method has the advantage of providing a dedicated standardized access to the licensed user database that avoids the need for Internet access. Since presumably there are relatively few beacons, (in the thousands instead of 10's of millions of unlicensed devices), the load on the central database would be minimal and therefore the database could be simpler and lower cost. Like the data base method it requires the unlicensed devices to have a location for themselves, although the beacons themselves provide a crude localization. For instance, the beacon might include a list of channels that can be used by any unlicensed device that can receive the beacon signal. In congested areas this list may be empty, but, in rural areas this is sufficient precision to identify many unused channels. The disadvantage to this approach is that in remote areas, beacons may be unreliable and the lack of detection could prevent operation in precisely the area where it could be most useful. Having default bands set aside that could be used in these areas would avoid this problem.

3) Unlicensed Signaling:

A more distributed option is to set aside a small frequency band for unlicensed devices to exchange information about licensed transmitters. It would provide a known open channel that the unlicensed devices could use to signal each other about the presence of licensed and unlicensed services in the area. Like the area beacons, the format could be standardized as an etiquette protocol that would enable disparate devices to communicate with each other. This would be used to augment any of the other methods in this paper and enable new methods. For instance, unlicensed users might set up dedicated

---

[34] Rappaport, T.S., *Wireless Communications Principles and Practice*, 2nd Ed. Prentice Hall, 2002. Ch. 6

[35] The continental U.S. covers an area of approximately $A = 8\text{x}10^6$ km^2. A low rate beacon can be designed to cover a radius of $r = 50$ km. Thus, $A/\pi r^2 =$ 1000 beacons would be required. Alaska could simply reserve some channels for unlicensed usage and anyone that is located in Alaska would be free to use these channels. Other large sparse spaces could be treated similar.

monitoring devices at prominent locations to identify and locate licensed transmitters. These would in turn broadcast their findings for a user community. This could all be done on an existing unlicensed band, but, usable bands like the 902-928MHz ISM band are far from the licensed bands below 100MHz and would add expense to the unlicensed radio antenna and front end if it was required to operate over this wide a range of frequencies. Alternatively, a small amount of spectrum could be set aside in or near each licensed service frequency band.

4) Receiver Detection:

Technically, interference does not take place at transmitters. Unlicensed devices should detect and avoid licensed signal receivers since this is where interference takes place. Detecting the existence of licensed transmitters is only a proxy for detecting licensed receivers. Detecting broadcast transmitters (or beacons announcing such transmitters) will cover either too much or too little of the coverage area (i.e. the area where the transmitted signal is being received). Detecting receivers would have the advantages (a) nearby receivers could be detected regardless of transmitted signal levels; (b) broadcast channels could be used according to actual use rather than inferred use from detecting transmitted signals.

We see several methods for detecting receivers:

1. The unlicensed device detects receiver signatures such as the LO signal emitted by a TV during reception.
2. The receiver has a beacon attached that sends out a periodic pulse.
3. The receiver has a device connected to the antenna input that detects the receiver signature and then transmits a beacon out the antenna path.
4. The receiver actively announces its channel usage.

Every receiver emits signals as part of the reception process. These signals are typically low power. To see the efficacy of this detection, we focus on TV. TV emits a carrier signal at the local oscillator (LO) frequency used during TV signal reception.[36] This signal is weak, but, can be used to detect the channel being received by a TV that is turned on and tuned to a specific channel.[37] Thus, if a LO detector could be incorporated into unlicensed devices, it would allow direct detection of receivers in the area and the channels that are being used. We performed some experiments in our lab to assess the potential of this detector.[38] Depending on the TV, the maximum LO detection range was found to vary from 3-15m.[39] This is likely only a fraction of the interference range of the unlicensed device. More sensitive techniques might yield further detection range but would require more measurement time and more expensive hardware that might be prohibitive for low-power unlicensed devices. The TV bands have many spurious signals that are similar to the LO signal and would yield many false positive detections.[40] Further this method does not work for devices other than TVs.

Receiver avoidance is more direct if the receiver has a dedicated beacon designed to turn on when the licensed receiver is turned on and announce the receiver's presence to unlicensed devices. The LO signal when measured directly at the antenna input was at most a weak -80dBm. A low-power tag could broadcast at a higher, but modest signal level such as -10dBm. This level would ensure a high probability of detecting nearby receivers.[41] The frequency and format of the beacon would need further definition.[42] Unlicensed devices would be required to listen for the beacons before they begin any transmissions and periodically afterwards. If heard, the unlicensed device would not operate. While straightforward, this approach has several flaws. First it signals the presence of the receiver at the receiver and not at the antenna which might be on the roof and highly directional. Second, it announces the presence of receivers even when they might be receiving cable TV, recorded programming or other non-broadcast signals. Third, it announces the presence of the receiver, but, not the channel used by the receiver.

The third approach combines the first two. A simple device can be built that is placed between the antenna cable and the receiver antenna input. This device can easily detect the LO oscillator and then send a low-power beacon out the antenna path. The beacon would be slightly more complex in that it

---

[36] Robert D. Weller, et al., "New Measurements and Predictions of UHF Television Receiver Local Oscillator Radiation Interference," *Proceedings of the 2003 IEEE Broadcast Technology Society Symposium,* 2003.

[37] In the UK it is used to detect unregistered TV's. See the UK TV Licensing website. http://www.tvlicensing.co.uk/information/tvdetectorvans.jsp

[38] A procedure similar to that as reported by Weller, et al. supra 36. A TV was equipped with a rabbit ears antenna. An HP 8594E spectrum analyzer with a similar antenna was used as a detector with the settings:

Resolution BW	10 KHz
Video BW	1 KHz
Sweep time	50ms
Attenuation	0dB
Ref level	-30dBm

The signal detection sensitivity was -104dBm. Three TVs were tested, a 1991 Emerson 13", a 1991 Mitsbishi 24" TV, and a 2000 JVC 20" TV. The TVs were tuned to channel 11. The furthest distance where a LO signal could be seen above the noise floor was measured. Then the output of the TV was connected to a splitter that connected to the antenna and to a coax cable that was connected directly to the spectrum analyzer input. The antenna was required so the tuner would lock on to a broadcast station and the LO signal would stabilize. The power of the LO signal was measured on the spectrum analyzer.

[39] These measurements are consistent with Weller et al. supra 36.

[40] Private communication with Mark McHenry of Shared Spectrum.

[41] It is enough to detect any receiver using a channel to mark it as used. Interference is more likely when a licensed device is closer to the unlicensed device, but, beacon detection is also more likely. This implies that such a technique becomes more reliable in high-density scenarios exactly as is needed to avoid harmful interference.

[42] It is beyond the scope of this document to give specific beacon recommendations. One would expect that the beacon would be a) in a band within the TV bands or on a nearby band (e.g. the 433.050-434.790MHz band used by active RFID tags) so that existing antennas can be used; b) low duty cycle so that collisions between different receiver beacons would be minimized; and c) low data rate since the information conveyed is minimal (e.g. channel used and type of receiver). These suggest a simple low-power radio device.

TABLE II

FEATURES OF THE DIFFERENT CHANNEL DETECTION METHODS.

Method	Accurately:		Requires:				Appropriate for:		Cost Burden on:		
	Avoids Interference	Exploits Whitespace	Constant Monitoring	Positioning	Standard	BW	High Power	Low Power	Unlic.	Lic. Trans.	Lic. Rec.
Database	X	X		X	X		X			X	
Detecting Transmitters	X		X				X		X		
Transmitter Beacons	X		X		X		X	X	X	X	
Area Beacons	X	X		X	X	X	X	X		X	
Unlicensed Signaling	X		X			X	X	X	X		
Receiver Beacons	X	X	X		X		X	X	X		X

would encode the channel used by the receiver. Since it sends the beacon along the same path followed by potential interference, it more accurately identifies the interference location (i.e., the receiver antenna). Unlicensed devices could operate in the vicinity of receivers with non-broadcast inputs since the low-power beacon signal is sent into a cable instead of the antenna and the beacon would not be detected by unlicensed devices.[43] Finally, the beacon announces directly the receiver channel and type. An unlicensed device would use the set of beacons that it receives to choose an unused channel. The concept can be applied to a variety of licensed devices. In the future, the device can also be incorporated directly into the licensed receiver (e.g., as part of the Tuner Mandate[44]). This would use the tuner control logic circuitry to command the beacon rather than the indirect LO detection and could be integrated into the existing circuitry at minimal cost.

Such a proactive beacon system would be an alternative to database or transmitter measurement methods. It might prove even more reliable and does not depend on having Internet connectivity or an expensive signal detector for weak licensed signals. It would allow low power devices to use channels that are being used generally in an area, but, not in the immediate vicinity of the unlicensed device. It therefore would expand the possible applications of the unlicensed technology. Against these advantages is the need for the unlicensed device to monitor the beacon channel for changes as receivers turn on or change channels. The path for adoption by licensed receiver owners would require careful planning.

D. Discussion

Licensed channel avoidance is possible through a number of different means as tabulated in Table II. As discussed in this document, there is some version of each method with which it is possible to accurately avoid interfering with licensed channels. It is these versions which are assessed here.

A database approach works well if it proactively lists changes that occur over a defined future horizon. In this way unlicensed devices can continue to operate even through outages in the database or lost connectivity to the database. Unlicensed devices can know in advance changes in licensed spectrum usage and exploit unused channels accordingly. The burden of updating and implementing the database falls on the licensed transmitters since they hold this information. The database approach requires the licensed transmitters to maintain the database information. Standards are required for the update and access to this database. The unlicensed users require an Internet connection. Because of the need for an Internet connection it is most appropriate for fixed high-power unlicensed devices.

This method also requires the unlicensed device positions in order to assess the database information. This can be done one time at installation, which is appropriate for fixed high-power unlicensed devices or through a localization system such as GPS or other signals such as cellular base station signals. It is important to note that almost any positioning method can be used even if it is prone to large errors, as long as the errors can be bounded. Large error bounds mean that the unlicensed devices must conservatively exclude more channels, but, especially in rural areas, licensed channels go unused over large areas and can be labeled as unused even with large location errors.

Much less infrastructure is required when the unlicensed devices directly detect the licensed transmitters. The approach requires either sensitive detectors customized for each licensed service, or, a network of monitors in order to accurately detect the licensed channel use. Further, it requires frequent monitoring of the licensed channels in order to detect changes in usage. Because of the implied expense per unlicensed device, this method is better suited to fixed high-power unlicensed devices which are more likely to be mounted on prominent locations that are well-suited for detecting other devices.

The final set of approaches depends on various versions of active beacons. Transmitter beacons use an easy to detect unambiguous beacon associated with each licensed transmitter. By using a standard signal for the different possible licensed transmitters, the detection is simplified. This method requires a beacon standard to be developed and the licensee to install a

---

[43] In the NAB comments to the 04-186 NPRM they included a study that showed an unlicensed device could interfere with cable reception if the unlicensed device had a high-gain antenna that was sufficiently close to the cable. In this scenario, the beacon would be received by the unlicensed device and thus could be used to detect this situation.

[44] Review of the Commission's Rules and Policies Affecting the Conversion to Digital Television, FCC 00-39, Second Report and Order and Second Memorandum Opinion and Order, August 9, 2002.

beacon on each of its transmitters. The unlicensed devices are required to monitor the beacons frequently to react to licensed usage changes.

The area beacon is more an extension of the database approach. It consists of transmitters set up across the country to broadcast local information on licensed transmitters as derived from a licensed transmitter database. It is an even simpler one-stop method for unlicensed devices to detect licensed transmitters and like the database can provide proactive licensed usage information that can be exploited. The method requires the set of area beacon transmitters, a radio and database interface standard, and the bandwidth to operate on. The unlicensed devices would require positioning information in order to use the data, although the beacons themselves would provide crude, but usable, positioning.

The unlicensed signaling is simply a bandwidth set aside for unlicensed devices to exchange their own information on licensed channel usage. If no existing unlicensed band is suitable, it would require a bandwidth to be set aside. A standard for exchanging this information is not required, but, would facilitate better information exchange between different unlicensed devices. Most of the methods can use a networked approach where detection or position information is shared. This sharing of information was shown to allow individually low reliabilities to be aggregated into increasing reliability as more devices network together. Even very low individual reliability can yield high reliability if enough devices network together and this reliability increases super-linearly as unlicensed device density increases.

Receiver beacons use small low-power transmitters at licensed receivers since this is where the interference takes place. Receivers emit signals without any explicit transmitter, but, these signals are found to be too weak to detect reliably. The best approach is a beacon placed on the receiver antenna input, since this will broadcast the beacon on the same path that the receiver reception follows. In particular when the antenna is connected to other than an antenna (e.g. to a VCR) the beacon is not broadcast. This method allows for the most aggressive exploitation of the licensed channel usage but requires the licensed devices to listen frequently to detect changes in licensed channel reception and requires licensed receivers to install the beacon.

These approaches are not mutually exclusive and different unlicensed devices might use different methods. But, clearly there is an economy of scale if a single primary approach is followed. The area beacons appear to be the most reliable approach. The installation and operation of the database and beacon transmitters would require a national investment. If these transmitters utilize existing radio towers and facilities, they will not be expensive to install and operate relative to the bandwidth resource that they open up.[45]

VI. CONCLUSION

This paper considers the process of formulating rules for unlicensed devices to operate in licensed service bands. The current process does not directly address the issue of harmful interference and leaves a significant uncertainty for the licensed operators and unlicensed device manufacturers. This paper develops the notion of a measurement scenario for assessing harmful interference. The framework starts with a definition of a service outage. It then consists of a menu of options for how the licensed receiver, unlicensed devices, interference evaluation and remedy are taken into account. The key idea is that the process of making definitions and choices within this framework is made when the unlicensed rules are formulated in order to provide specific protections to the licensed operators and to provide assurances and design goals to the unlicensed device manufacturers.

This process was applied to the specific case of the NPRM on unlicensed operation in the TV broadcast bands. A set of choices was selected in order to exemplify how the process could be applied. Some details were left open. Further proceedings would be required for the FCC to make a fully informed and complete set of choices.

An analytic interference model is developed so that rules can be assessed a priori and the dependency on different choices and parameters can be better assessed. The model suggests that when applied to the NPRM licensed and unlicensed devices can coexist at densities exceeding 1000 unlicensed devices per square kilometer. When applied to a worst-case scenario of a high-density apartment building, it is found that densities over 20,000 devices per square kilometer can be supported. The model also shows clearly the tradeoff between protecting licensed users from potential harm and the extent that unlicensed devices can proliferate. Modest increases in potential harm to licensed users yields large increases in the number and easier implementation for the unlicensed devices.

Licensed channel avoidance mechanisms were assessed. It was found that within each class of licensed channel avoidance strategies; there exists at least one approach that could meet stringent channel avoidance requirements. The most viable approaches depended on proactive databases maintained by licensed operators whose content is distributed over the Internet or via simple broadcast beacons.

Overall the paper advocates that with modest effort and cost to broadcasters a large social benefit can be gained by opening unlicensed device operation in the licensed broadcast bands. It will require a well-defined regulatory process and a clear and open assessment of costs in order for the current licensees and new entrants to invest in this technology. The ideas in this paper are intended to facilitate this process.

APPENDIX A: ANALYTIC MODEL DETAILS

A. Model Assumptions

The basic idea of the model is that licensed receivers and

---

[45] As an example of computing this cost: A 100 W transmitter mounted on an existing infrastructure and an Internet might cost $20,000 to install and $200 per month to operate and maintain. For 1000 transmitters this yields a $20M investment and $2.4M yearly cost which is small relative to the bandwidth that would be opened up across the country. The database would be a minor fraction of this investment.

unlicensed devices will be spread over a large area such as a metropolitan or rural area. A conceptual notion is that this area consists of the area covered out to some maximum distance (such as to the Grade B contour of a typical broadcast station). The shape of this contour is not particularly important as long as it is reasonably compact. A key concept is $r_{\min}$, the minimum non-interfering distance separation between unlicensed transmitter and licensed receiver when the licensed device is transmitting at full power on the same channel as the receiver is listening and both devices antennas are pointed toward each other. This, of course, is the worst case situation and other factors come into play to mitigate this situation. It is precisely the point of this model to make these factors explicit so that the mitigating role of smart unlicensed devices can be expressed concretely.

The basic model makes the following assumptions:

1. Only two-dimensional scenarios are considered.
2. Received power at a licensed device from an unlicensed transmitter is $P_{int} = K_{int}\ g_{UL}\ g_L\ P_{UL} S_{int}/r^b$, where K_{int} is a constant related to antenna heights, cable losses, and other constants; g_{UL} and g_L are the unlicensed and licensed device antenna gains along the path connecting them; P_{UL} is the transmit power; r is the separation between the unlicensed transmitter and licensed receiver; b is the pathloss exponent for signals between the unlicensed and licensed device; and S_{int} is the shadow fading factor representing the variation in received power due to terrain, clutter, and other environmental factors.[46]
3. Received power at a licensed device from a broadcast tower is $P_{sig} = K_{sig} S_{sig}/R^a$, where K_{sig} is a constant related to broadcast power, antenna heights, cable losses, etc.; R is the separation between the transmitter and receiver; a is the pathloss exponent between the transmitter and receiver; and S_{sig} is a shadow fading factor representing the variation in received power due to terrain, clutter, and other environmental factors. Note the specific effects for the broadcast power and antenna gains are not broken out as separate factors since they will likely be constants and not vary over time.
4. The licensed device is disrupted if $P_{sig}/P_{int} < T$ for some defined threshold T. Note that this threshold depends on the nature of the interference signal, and whether it is in the same channel as the licensed receiver or another nearby channel. Combining the previous assumptions, the signal to interference ratio is $P_{sig}/P_{int} = K\ S\ r^b/(g_{UL}\ g_L\ P_{UL}\ R^a)$, where $K = K_{sig}/K_{int}$, and $S = S_{sig}/S_{int}$.
5. The shadow fading S is well modeled by a log-normal distribution (i.e. log S is normal) with log normal standard deviation σ. If S_{sig} and S_{int} are both log normal with log-normal standard deviation σ_{sig} and σ_{int}, then their ratio is also log normal. In practice, S_{sig} and S_{int} are correlated. A TV in the basement will receive weaker signals from both the broadcaster and the unlicensed device. Thus, $\sigma^2 < \sigma_{sig}^2 + \sigma_{\text{int}}^2$.
6. The licensed devices are uniformly distributed over the broadcast coverage area. The coverage area is a circle of radius R_B. The probability a device is within R of the center is $\frac{R^2}{R_B^2}$. Let A be the coverage area, N_L the number of unlicensed devices in this area, and N_L/A the average density of licensed devices. For simplicity, all broadcast channels have the same coverage area.
7. The unlicensed devices are uniformly distributed over the broadcast coverage area and the number of these devices is N_{UL}. The licensed and unlicensed device separation, r, is small relative to the radius of the broadcast coverage so that r is independent of R.
8. A device which is turned off can not disrupt or be disrupted. A licensed device not using the broadcast channel (e.g. using cable) can not be disrupted.
9. Unless otherwise stated, antennas have a uniform random azimuth orientation.

Some notes on these assumptions are in order. The limitation to two-dimensional does not apply well to built-up metropolitan areas such as New York City. It does apply to urban environments with few high-rise buildings and typical suburban and rural environments. Later work will expand this model to three-dimensional environments.

The pathloss exponent is allowed to differ for the unlicensed and broadcast transmitters. It is expected that the broadcast transmitter will be close to a free-space pathloss model ($a = 2$). The unlicensed device will differ depending on the device. For low-power devices without special antenna mounting, the pathloss will be closer to the two-ray ground model ($b = 4$). For higher power transmitters mounted on outdoor poles, it will be between 2 and 4 depending on antenna height and location.

Shadow fading can have log-normal standard deviations as large as 10dB for both S_{sig} and S_{int} suggesting a total of 14dB for the log normal standard deviation for their ratio. Because of correlations between them we might expect a total variation equal to half of this value or 7dB.

With the uniform distribution of unlicensed devices the expected number of licensed devices in a ring of thickness dr and radius r from the unlicensed device is $2\pi r\ N_L/A\ dr$.

B. *Model Derivation*

There are three main random variables in this model. The distance of the licensed device to the broadcast transmitter, R; the distance from the licensed device to the unlicensed trans-

---

[46] The model for assumptions 1-5 is derived from standard texts such as Rappaport, T.S., *Wireless Communications Principles and Practice*, 2nd Ed. Prentice Hall, 2002. Ch. 3-5

mitter, r; and the shadow fading value S. Once these are accounted for, secondary random variables can be easily admitted.

We are interested in computing expected number of licensed devices disrupted by an unlicensed device. First we compute the expected number disrupted by a single unlicensed device and then scale to more than one unlicensed device. Consider a single unlicensed device. Given r and S, a licensed device is disrupted if $\frac{P_{sig}}{P_{\text{int}}} = \frac{SKr^b}{g_{UL} g_L P_{UL} R^a} < T$, i.e. $R > \left(\frac{SKr^b}{g_{UL} g_L P_{UL} T}\right)^{1/a}$. T is the threshold given the current channels of the licensed and unlicensed devices; and the modulation scheme used by the unlicensed device. It follows from assumption 6:

$$\Pr\left\{R > \left(\frac{SKr^b}{g_{UL} g_L P_{UL} T}\right)^{1/a}\right\} =$$
$$\begin{cases} 1 - \frac{1}{R_B^2}\left(\frac{SKr^b}{g_{UL} g_L P_{UL} T}\right)^{2/a} & \text{if } \left(\frac{SKr^b}{g_{UL} g_L P_{UL} T}\right)^{1/a} \le R_B \\ 0 & \text{otherwise} \end{cases}$$

The expected number of licensed radios at a distance r to $r + dr$ is $N_L/A\ 2\pi r\ dr$. To get the total expected users disrupted by the unlicensed device we integrate over all distances r, and for each r, over all possible S.

$$D = \int_0^\infty \int_0^\infty \frac{N_L}{A} 2\pi r \Pr\left\{R > \left(\frac{sKr^b}{g_{UL} g_L P_{UL} T}\right)^{1/a}\right\} p_S(s)\, dr ds$$

where p_S is the distribution of S. Switching the order of the integration and integrating yields:

$$D = \pi \frac{N_L}{A}\left(\frac{R_B^a g_{UL} g_L P_{UL} T}{K}\right)^{2/b} \frac{b}{b+a} e^{\frac{2\sigma^2}{b^2}} .$$

This is the expected number of licensed devices disrupted by a single unlicensed device. For N_{UL} unlicensed devices, we conservatively overestimate[47] the number of disrupted devices as simply N_{UL} times larger.

An alternative form of this equation is derived as follows. Consider the worst case when a licensed device is at the edge of the broadcast area, the unlicensed device is at maximum power on the same channel as the licensed device with both antennas pointing at their maximum gain towards each other. Let $S = 1$ and consider the distance r_{min} that would just meet the signal to interference criteria for an interferer on the same channel. In this case (with obvious notation):

$$\frac{P_{sig}}{P_{\text{int}}} = \frac{K r_{\min}^b}{g_{UL}^{\max} g_L^{\max} P_{UL}^{\max} R_B^a} = T_S$$

$$r_{\min} = \left(\frac{g_{UL}^{\max} g_L^{\max} P_{UL}^{\max} R_B^a T_S}{K}\right)^{1/b}$$

Combining these results we get

$$D = \pi \frac{N_L N_{UL}}{A} r_{\min}^2 \left(\frac{g_{UL}}{g_{UL}^{\max}} \frac{g_L}{g_L^{\max}} \frac{P_{UL}}{P_{UL}^{\max}} \frac{T}{T_S}\right)^{2/b} \frac{b}{b+a} e^{\frac{2\sigma^2}{b^2}}$$

The role of the broadcast path loss exponent, a, is somewhat subdued in this equation. This is because it is implicitly subsumed in the definition of the coverage area. A bigger a would lead to a smaller coverage area and vice versa. Here it reflects how quickly the licensed signal power increases above the threshold as the center of the coverage area is approached. Since most licensed devices are closer to the edge than the center this effect has only a small impact on the final result.

There are four final random variables that need to be considered: the distribution of the unlicensed and licensed antenna gains; the distribution of unlicensed power levels; and the distribution of device thresholds. These are assumed to be independent of each other and the other random variables.

The unlicensed antenna has an antenna pattern, $g_{UL}(\theta)$. The expected contribution to the number of disrupted receivers is:

$$\int_0^{2\pi} (g_{UL}(\theta))^{2/b} p_{g_{UL}}(\theta) d\theta = \frac{1}{2\pi} \int_0^{2\pi} (g_{UL}(\theta))^{2/b} d\theta$$

where the distribution $p_{g_{UL}}$ is assumed to be uniform.[48] Define

$$G_{UL} = \frac{1}{2\pi} \int_0^{2\pi} \left(\frac{g_{UL}(\theta)}{g_{UL}^{\max}}\right)^{2/b} d\theta$$

Typical values are

$G_{UL} = 1$ if the antenna is omnidirectional

$G_{UL} = w/360$ if the antenna is an ideal sectorized antenna of width w in degrees.

Similarly we define the licensed antenna gain factor:

$$G_L = \frac{1}{2\pi} \int_0^{2\pi} \left(\frac{g_L(\theta)}{g_L^{\max}}\right)^{2/b} d\theta$$

Power control would result in a distribution of power levels. Similar to the antenna gains we define the power control gain factor:

$$P = \int_0^{P_{UL}^{\max}} \left(\frac{P_{UL}(x)}{P_{UL}^{\max}}\right)^{2/b} p_{P_{UL}}(x) dx .$$

where $p_{P_{UL}}$ is the distribution of power levels. Example values are

---

[47] If two different unlicensed devices disrupt the same licensed device it counts as two licensed devices disrupted.

[48] A receiver detection technique might lead to null steering or other techniques so that the antenna angle distribution would not be uniform.

$P = 1$ when the unlicensed device always transmits at maximum power

$P = b/(b+2)$ if power is uniform between 0 and $P_{UL}^{\max}$.

$P = \frac{b}{2} \frac{1-\left(P_{UL}^{\min} / P_{UL}^{\max}\right)^{2/b}}{\ln P_{UL}^{\max} / P_{UL}^{\min}}$ if $\ln P_{UL}$ is uniform between $\ln P_{UL}^{\min}$ and $\ln P_{UL}^{\max}$ (i.e. it is uniform in dB between the min power in dB and the max power in dB).

The distribution of required thresholds depends on the likelihood of choosing the same channel, or one of the neighboring channels, or more separated channels. Even if the unlicensed device is working on a channel far removed from the channel used by the licensed device, a sufficiently strong signal can overwhelm the receiver. So, all channels must be considered. Therefore we define:

$$C = \sum_i p_i \left(T_i / T_S\right)^{2/b}$$

where if N is the channel used at a licensed receiver, p_i is the probability of the unlicensed device being on channel $N + i$, and T_i is the threshold required in this case. For instance, for DTV[49]

I	T_i/T_s(dB)
0	0.0
+/–1	48.5
+/–2	74.2
+/–3	78.2
+/–4	84.2
+/–5	86.2
+/–6	80.2
+/–7	87.2
$\lvert i \rvert>7$	90.2

As a worst case example, let the channels be chosen randomly and we ignore effects at the edge of the licensed band. Then

$C = 0.020$ if $b = 2$

$C = 0.020$ if $b = 4$

If the unlicensed radio avoids the same and adjacent channels of the licensed receiver (i.e. is at worst at N +/– 2) then at worst:

$C = 3.8\text{x}10^{-8}$ if $b = 2$

$C = 2.0\text{x}10^{-4}$ if $b = 4$

If the unlicensed radio can always avoid any channel within +/– 7 of a receiver channel, then

$C = 9.6\text{x}10^{-10}$ if $b = 2$

$C = 3.1\text{x}10^{-5}$ if $b = 4$

We let all the model factors be denoted by M

$$M = \pi \frac{b}{b+a} e^{\frac{2\sigma^2}{b^2}}$$

Then

$M = 5.8$ if $a = 2$, $b = 2$, and $\sigma = 7$dB

$M = 2.9$ if $a = 2$, $b = 4$, and $\sigma = 7$dB

Licensed receivers or unlicensed transmitters may simply be turned off and not part of creating or suffering interference. A licensed receiver may be receiving its signal via cable and not through over-the-air broadcasts. The last factor captures the fraction of devices eligible to participate in the device interaction:

$E = F_{ONUL} F_{ONL} F_{BC}$

Where F_{ONUL} is the fraction of the unlicensed devices that are turned on at any time, F_{ONL} is the fraction of licensed receivers that are on, and F_{BC} is the fraction of receivers that listen to over-the-air broadcasts as opposed to cable TV.

Putting all these factors together and noting $F = D/N_L$ yields the main result:

$$F = r_{\min}^2 PCEG_{UL}G_L MN_{UL} / A$$

APPENDIX B: NETWORK DETECTION MODEL

This appendix develops a model of network detection. It assumes that

1. Unlicensed devices are distributed uniformly in an area such that they can be modeled as a Poisson point process with density λ devices per unit area.
2. The individual licensed transmitter detection probability is independent and equal to D for all unlicensed devices.
3. Unlicensed device can send licensed transmitter information to other unlicensed devices. The received power between unlicensed devices is $P = KS/r^b$, where P is the received power, K is a factor that accounts for the antenna gains, transmitted power, etc., S is a shadowing factor that account for variations in received signal power between devices at random locations with separation r, and b is the so-called pathloss exponent.[50] S is distributed as a log-normal distribution which in decibels has mean 0 and standard deviation σ_{dB}.
4. The licensed information is received if $P > T$ where T is the minimum receive power threshold.

From assumption 3, the maximum range that two devices can communicate ignoring shadowing is $r_0 = (K/T)^{1/b}$. From assumption 4, two devices at separation r receive each other if $S > (r/r_0)^b$. By assumption 1, the expected number of neighboring unlicensed devices that can communicate, N, is given by

---

[49] ATSC A-74 *DTV Receiver Performance Guidelines*

[50] More detail on this model can be found in textbooks such as Rappaport, T.S., *Wireless Communications Principles and Practice*, 2nd Ed. Prentice Hall, 2002. Ch. 3-5

$$N = \int_{r=0}^{\infty} \lambda 2\pi r \Pr\left[S > \left(\frac{r}{r_0}\right)^b \right] dr = \int_{r=0}^{\infty} \int_{S=(r/r_0)^b}^{\infty} \lambda 2\pi r p(S) dS dr \,,$$

where $p(S)$ is the log-normal shadow fading distribution. Exchanging the order of the integration we get:[51]

$$N = \int_{S=0}^{\infty} \int_{r=0}^{r_0 S^{1/b}} \lambda 2\pi r p(S) dr dS = \lambda 2\pi r_0^2 \int_{S=0}^{\infty} \frac{S^{2/b}}{S\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\ln S}{\sigma}\right)^2} dS$$

$$= \lambda 2\pi r_0^2 e^{\frac{2\sigma^2}{b^2}}$$

Therefore the expected number of neighbors that have detected a given licensed transmitter is, by assumption 2, DN. As a Poisson point process, the random subsampling, via D and the connectivity requirement, is also a Poisson point process with mean DN. Therefore the probability that no neighbor detects licensed transmitter is e^{-DN}. A licensed transmitter will not be detected if the unlicensed device does not detect it itself and none of its neighbors detect it, i.e. Pr[NoDetect] = $(1- D)$ e^{-DN}.

Note that N can be determined either from the model and equation above or by direct measurements in a working system. In a fully networked system where nodes can relay detection information beyond their immediate neighbors, then the same equation for the probability of no detection applies where N, in this case, is the number of nodes connected in the network.

ACKNOWLEDGMENT

The author received support from the New America Foundation and NSF grant CNS 0428887 in preparing this document. The author acknowledges the laboratory assistance of Siddharth Shetty and the comments of Dale Hatfield, Mark McHenry, Douglas Sicker, Jim Snider, and Phil Weiser.

---

[51] In this equation, $\sigma = (\sigma_{\mathrm{dB}}/10)\ln 10$.