Evaluating Interference in Wireless LANs: Recommended Practice

A Farpoint Group Technical Note

Document FPG 2006-307.1
October 2006

R adio interference remains a core concern among wireless LAN (WLAN) users, network administrators, and operations staff alike. After all, the potential for interference is a fact of life in the unlicensed bands where WLANs operate, and, even worse, it is often very difficult to evaluate the effects of interference on a particular wireless-LAN (WLAN) installation at any given moment in time. The primary reason for this state of affairs has until quite recently been a lack of effective enterprise-oriented tools for monitoring the airwaves, and detecting and evaluating the impact that interference might be having. But this situation is changing, and the ability to understand, evaluate and manage interference is now within the reach of essentially every enterprise.

While many assume that any interference affecting a given WLAN is likely to be from another WLAN, there are many other possible sources of interference in the unlicensed bands. The impact that these potential interferers can have ranges from negligible to severe depending upon the type of traffic being moved by the wireless LAN and the characteristics of the interfering signals - the evaluation of which is the subject of this Tech Note.

Farpoint Group has for some time been studying the issue of interference and has developed a core set of recommendations for evaluating and dealing with the interference challenge. Given the broad deployment of WLANs in both metro-scale and enterprise settings, it is important that interference at least be on the radar screens of network managers today, and even more likely that it will become an issue in almost every installation in the future.

The Nature of Interference

We have reached the conclusion that enterprises need a method for monitoring and evaluating, increasingly on a continual basis, the effects of interference on wireless LANs. We can divide the world of potential interference into two broad categories – interference from other wireless LANs, and that arising from non-WLAN traffic in the bands used by WLANs, primarily at 2.4 GHz. The former is of common concern to residential users, especially in high-density housing, and this same challenge carries over to multi-tenant office settings as well. Even larger firms occupying an entire building can see interference from nearby WLANs (increasingly, those implemented for municipal, metro-scale access) and other radio-based devices. Non-WLAN traffic includes a variety of cordless phones (both Wi-Fi and not), Bluetooth devices of many forms, wireless video cameras (again, both Wi-Fi and not), cordless headsets, wireless bridges, cordless video-game controllers, and, of course, microwave ovens.

To be complete here, there is one other form of interference that, while unlikely, is still important to consider. This is a wireless denial-of-service (WDoS) attack using a broadband jammer that essentially blankets a given band with Gaussian white noise or a similar relatively-high-amplitude signal. Devices of this form are surprisingly easy to buy or build (there are some that are commercially available, and plans can even be found on the Web), and a device with an output of a few Watts, more than sufficient to jam one or more 802.11 channels, could be battery-operated and small enough to conceal in a briefcase or even a coat pocket. While we have not seen any of this (with sufficient transmit power, illegal) behavior,

we advise a strategy of constant vigilance, especially as wireless LANs take on an ever-increasing array of mission-critical enterprise-networking functions.

Specific Interference Scenarios

As a result of our study of various interference sources on wireless LANs, Farpoint Group will shortly publish a set of reports detailing the impact of a variety of sources of interference on asynchronous WLAN (typically data) traffic, voice over IP over Wi-Fi (VoFi), and Wi-Fi-based video traffic. In general, the symptoms of interference in each of these cases are as follows:

- *Asynchronous LAN traffic* – Primarily, decreased or highly-variable throughput, occasionally resulting in very low or even non-existent service rates. In most cases, users will continue to see a strong signal represented by the common bar-graph or other indicator in a given computer's tooltray, leading to the conclusion that all is well – other than the lack of throughput, of course.

- *Voice over IP over Wi-Fi (VoFi)* – Evaluating the performance of voice systems is often difficult, and, as we will discuss below, requires specialized test equipment in most cases for meaningful results. The most common symptoms noticed by a typical VoFi user in the presence of interference will be dropouts, as packets are lost due to collisions. These dropouts can and will occur in both directions. These symptoms should be familiar to anyone who has used a cell phone, although in the case of cell phones these problems most commonly result from issues related to various forms of fading rather than interference.

- *Video* – It is convenient to think of streaming video traffic as being very similar to voice, although with much higher duty cycles and data rates. While voice might require effective throughput of 100 Kbps in each direction, video can require 400 Kbps and potentially much more (to tens of megabits per second), albeit in only one direction as video is usually sent using UDP or multicast protocols. As with voice, a human is consuming the information in real time, and users will typically notice dropouts and square boxes in the video, or even screen freezing, when interference is a problem. These artifacts are the result of errors in the MPEG or other decoding process as interference damages key information required to re-construct video frames. Of course, the degree of degradation will be a function of frame size, frame rate, video resolution, and the amount and type of interference present.

Note that a complicating factor in each of the above situations is the fact that network congestion in either or both of the wired and wireless segments of a given network can have very similar detrimental results. As a consequence, it's important to be able to monitor both LAN and wireless-LAN traffic along with the general state of the airwaves. We thus recommend two forms of interference analysis, as follows:

- *Protocol analysis* – Contention is a fact of life on shared media; indeed, Ethernet is based on the concept to begin with. It's thus important to be able to analyze how a given protocol is responding to channel conditions that are both normal and the result of interference. A variety

of products exist for the evaluation of wireless LAN systems; we generally call these *Wireless LAN Assurance* tools.

- *Energy analysis* – But since potential wireless interferers will not necessarily be using a wireless-LAN protocol, it's also critical to be able to examine other signals as *energy*, identifying (*characterizing*) them and their source if possible. The tool traditionally used for this purpose is the *spectrum analyzer*, most often implemented as a piece of (rather expensive; $US20,000 and more is not uncommon) electronic test equipment designed for use by engineers. Unfortunately, most spectrum analyzers are far too expensive and complex for use in enterprise WLAN settings. But a new class of very cost-effective PC-based spectrum analyzers has now appeared, and we will discuss these in more detail below.

While it is safe to assume that performing real-time analysis on only one of the above domains and finding no issues implies that the problem is in the other domain, any reasonably-sized wireless-LAN installation should be equipped for both forms of network performance and integrity assurance. Indeed, a key direction for the Wireless LAN Assurance industry is the integration of spectral analysis tools. We recommend that enterprise installations with more than a few access points (APs) installed have both.

Evaluating the Effects of Interference

It is actually relatively easy to evaluate the effects of interference on given types of traffic in an enterprise setting, thanks again to the increasing availability of relatively simple and low-cost tools now on the market. We recommend that enterprise network and operations managers and staff gain hands-on experience with situations involving various forms of interference so as to more quickly resolve these when they occur. The following is the procedure we use and recommend for this purpose. Note that the following can apply to any enterprise, public-access, or even residential setting.

1. *Decide what to evaluate* – This involves selecting an application or synthetic workload (benchmark) to use in evaluating interference. In general, this will be some combination of the traffic types noted above (Web/typical network traffic, VoFi, and/or video). We recommend the very capable (and free) Iperf benchmark [http://dast.nlanr.net/Projects/Iperf/] for synthetic workload generation; it can simulate many forms of traffic (including TCP, UDP, and multicast), is easy to use, and can produce robust output. Other benchmarks can certainly be used, as can actual applications, but repeatability (and, we believe, ease-of use) are key.

   We recommend that the scope of interference studies be kept fairly compact, at least until baseline results are obtained and the behavior of benchmarking and analysis tools is well-understood. An exception to this is, of course, when attempting to localize and remedy sources of interference in production networks, which we will discuss below.

2. *Establish a baseline traffic/interference measurement* – This is done with a WLAN assurance tool, from companies such as AirMagnet [http://www.airmagnet.com], Fluke Networks [http://www.flukenetworks.com], or WildPackets [http://www.wildpackets.com], and a tool for

energy-based spectrum analysis. As was mentioned earlier, spectrum analysis can be accomplished with traditional spectrum analyzers, but we recommend newer (and more WLAN end-user focused) PC-based tools from the above companies and Cognio. Cognio's *Spectrum Expert* [http://www.cognio.com/solutions_mobile.html], a combined hardware/software tool (see Figure 1), runs on notebook computers equipped with a PC Card slot, is very easy to use, even by non-engineers (radio and otherwise), and displays a great

deal of information useful in identifying, evaluating, and remedying interference. The use of these tools provides initial information as to the nature of RF traffic, regardless of device or protocol, allowing a baseline to be established and from that the identification and ideally correction of any obvious interference or traffic-related problems.

Figure 1 - Cognio's Spectrum Expert PC Card. An external antenna is also available. *Source:* Cognio, Inc.

This step is used to select the best WLAN channel for subsequent tests, and to note any other traffic in the channel selected. In many cases the traffic will be so weak as to be inconsequential, but it may be necessary to disable any potential interference sources at least for the duration of the test (restricting use of a microwave oven, for example). Also, no production traffic should be allowed in the selected channel during the test. Note also that this step is very useful in the initial deployment of a WLAN system in terms of picking the most lightly-used channel in a given area, at least as of the time of deployment.

3. *Establish a baseline benchmark result* – The synthetic or other workload is run and the results noted. The spectrum analysis tool is used during the run to monitor and record any anomalous or other interference. The geometric relationships of all active elements should be carefully noted.

4. *Perform an impairment test* – In the next step, we repeat the benchmark run identically, except that we introduce a known interferer into the spectrum being used. It is again important to note any other interference using the spectral analysis tool. Again, the geometric relationships of all active elements should be carefully noted here as well.

5. *Compare results* – This is, of course, easy in the case of a synthetic benchmark. When examining voice quality or video quality directly, it may be necessary to perform multiple runs and sample the opinions of a number of people. In the case of voice, some monitoring and analytical tools, such as Vo-Fi Analyzer from AirMagnet [http://www.airmagnet.com/ products/vofi.htm], OmniPeek from WildPackets [http://www.wildpackets.com/products/omni/ overview/omnipeek_analyzers], and the VoIP QoS Service Assurance Test from Veriwave [http://www.veriwave.com/products/vowlan_performance.asp], among others, can be used to obtain an analytically-generated Mean Opinion Score (MOS) number and R-values, which are analytical measures of voice quality directly are directly related to MOS values. These pro-
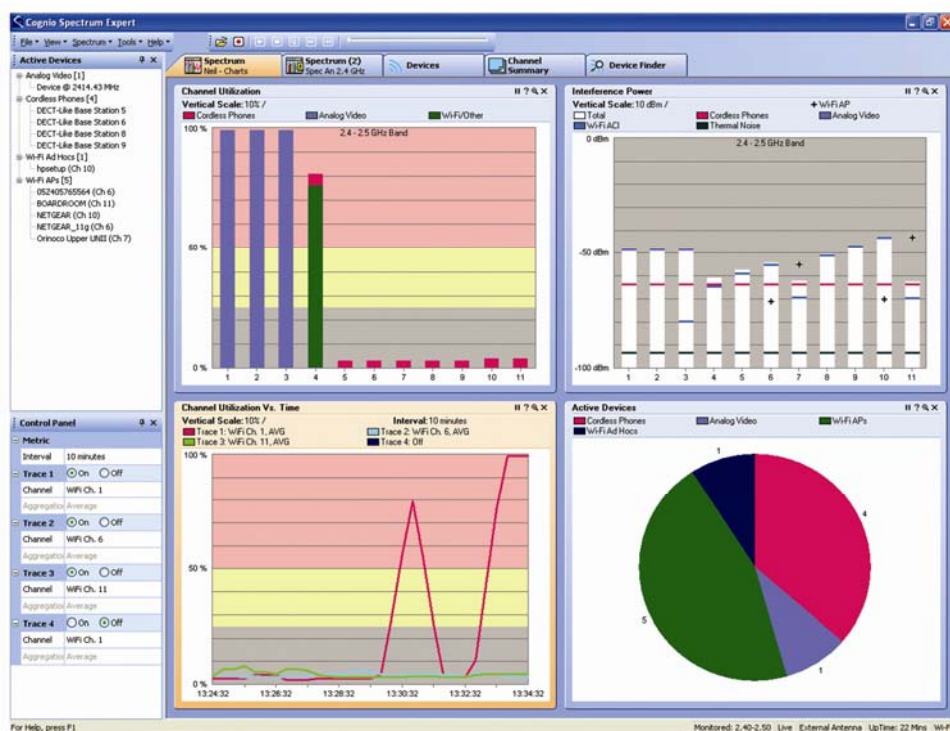
vide a computationally-sound method of comparing voice benchmark results, and remove human variability from the process.

When using Iperf or other synthetic benchmark, it is easy to compare differences in throughput resulting from interference. While a gross throughput number obtained at the end of each run is usually sufficient for comparative purposes, gathering intermediate data at regular intervals (every second or so) can also be useful in identifying any extraneous variables.

Interference Remediation Strategies

A major concern, of course, is how to deal with unknown sources of interference in production environments. The tools noted above for use in benchmarking are also most useful in operational WLANs, with appropriate alarms set. Again, both protocol- and spectrum-based tools are required, and we highly recommend both of these in any production environment with more than about ten access points or in any WLAN based on a centralized architecture. Indeed, we are

Figure 2 - An example of the information displayed by Cognio's *Spectrum Expert* product. Information on this screen includes instantaneous channel utilization, types of interferers and their power levels, channel utilization over time, and classes of active devices *Source:* Cognio, Inc.

now seeing the huge array of functionality in Cognio's tools (see Figure 2) being integrated into a variety of WLAN Assurance products, and look forward to what we believe will be their eventual inclusion in WLAN system products as well.

It should be noted that all enterprise-class WLANs include some form of RF Spectrum Management functionality (RFSM, see Farpoint Group White Paper 2003-201.1, *Beyond the Site Survey: RF Spectrum Management for Wireless LANs*), and many of these products can do a credible job of working around simple interference by adjusting AP transmit power and optimally

(given their limited knowledge of the radio environment, anyway) selecting channels. While RFSM is certainly valuable, today's RFSM tools usually do not perform energy-based analysis, and thus a more effective strategy is to monitor for interference and then take steps to remediate the source when located. Additional spectral-based monitoring is essentially because today's wireless-LAN access points cannot detect or deal with non-Wi-Fi sources of interference.

Another obvious suggestion is to use the 5 GHz. ("U-NII") bands for enterprise wireless networks. The ".11a" bands have been notoriously underutilized, usually as a result of the mistaken assumption that .11a has less effective range than .11g/b. In reality, both have roughly the same effective range when operating at maximum throughput (note that all 802.11-based wireless LANs will upshift and downshift physical-layer modulation rates in response to changing channel conditions), and, regardless, the enterprise should be thinking in terms of dense deployments to improve capacity (see Farpoint Group White Papers 2004-193.1, *Rethinking the Access Point: Dense Deployments for Wireless LANs* and 2005-083.1, *Wireless LAN Dense Deployments: Practical Considerations*) and not, in most horizontal applications, anyway, maximum range.

But while we heartily recommend going to 5 GHz., it stands to reason that eventually even the .11a channels will become fairly crowded at least with other WLAN traffic, and possibly other signals as well. Thus the ability to deal with interference in the 5 GHz. bands will become, we believe, very important over time.

Conclusions and Next Steps

Farpoint Group is now completing empirical studies, based on the Recommended Practice outlined above, of the effects of interference in various forms on general, voice, and video WLAN traffic, and we will shortly publish Tech Notes on the results of these tests. We will also discuss, in a separate Tech Note, the effect of interference both on and from metro-scale Wi-Fi networks, a large number of which are now being installed on a global basis. While we believe that the increasing use of wireless devices of many forms, but most importantly wireless LANs, will continue to grow quite rapidly and on a global scale and thus drive concerns about interference, we are convinced that the proper application of energy-based monitoring and analysis tools and energy-augmented RF Spectrum Management techniques will minimize if not eliminate any interference-based impairment of production applications on enterprise wireless LANs. At any rate, we have outlined in this document the techniques that any enterprise can use to satisfy itself on this score.

Farpoint
Group

Ashland MA 01721
508-881-6467
www.farpointgroup.com
info@farpointgroup.com

The information and analysis contained in this document are based upon publicly-available information sources and are believed to be correct as of the date of publication. Farpoint Group assumes no liability for any inaccuracies which may be present herein. Revisions to this document may be issued, without notice, from time to time.