The Effects of Interference on General WLAN Traffic

A Farpoint Group Technical Note

Document FPG 2006-328.3
January 2008

Farpoint Group

As we discussed in our recent White Paper FPG 2006-321.2, *The Invisible Threat: Interference and Wireless LANs*, we expect radio-frequency (RF) interference to become an increasing concern for operators of enterprise-class and residential wireless LANs (WLANs) alike. Interference can result from traffic on other nearby WLANs, as well as non-Wi-Fi devices simultaneously using the unlicensed bands where WLANs operate. As we noted in the above document, interference is a fact of life in these bands and will only grow worse as the usage of these bands continues to increase. Network managers have no choice but to develop a strategy for addressing the challenge of RF interference in order to maximize WLAN performance and reliability.

In our related Technical Note FPG 2006-307.2, *Evaluating Interference in Wireless LANs: Recommended Practice*, we discussed a methodology for evaluating the impact of interference on WLAN traffic via real-world experiments. This procedure enables network managers to see for themselves - in a simple but effective and, we believe, conclusive fashion - how interference might be affecting their WLAN operations. This methodology is, in fact, the result of many days of experimentation with many aspects of interference, including real-world tests which produced some occasionally surprising results.

This Tech Note, and two others in this series (FPG 2006-329.3, *The Effects of Interference on Video Over Wi-Fi*, and FPG 2006-330.3, *The Effects of Interference on VoFi*) present the results of those experiments. This document deals with the effects of a variety of interference sources on general WLAN traffic obtained via real-world testing. Our objective here is to show just how detrimental interference can be to WLANs, and to discuss some of the measures for dealing with what is certain to become an increasingly difficult challenge in the future.

Test Scenario

For this series of tests, we chose a typical open-architecture office consisting primarily of cubicles and a few closed offices and conference rooms. We operated within a single suite of a very large multi-tenant building, and our suite was occupied by typical office workers during the tests conducted. For all testing, we carefully monitored the radio channels we used with Cisco's (formerly Cognio's) *Spectrum Expert* [http://www.cisco.com/en/US/products/ps9393/index.html], a Spectrum Assurance (SA; Cisco refers to this as *Spectrum Intelligence*) tool which we have used in similar exercises before and which we highly recommend. Spectrum Expert is a spectrum analyzer designed for WLAN environments, and is capable of monitoring, identifying, and evaluating essentially all forms of interference in the 2.4 and 5 GHz. bands. We used Spectrum Expert both to measure the level of energy in the 2.4 GHz. Wi-Fi channels and to visually monitor the level of interference as the individual tests were run.

The test configuration and geometry can be seen in Figure 1. Following the general procedure outlined in FPG 2006-307.1, we set up a Proxim ORiNOCO AP-700 access point (AP) [http://www.proxim.com/products/ap_700/index.html] at Location 3, and connected it to a notebook computer running the Iperf 1.7 benchmark [http://dast.nlanr.net/Projects/Iperf/] as a server. We then set up two notebook computers at Location 4, approximately 25 feet away, and ran one copy of Iperf on each, using different port numbers so as to create multiple streams at the server end. The traffic generated TCP packets in both directions for three minutes, and was designed to simulate a heavy load of non-time-bounded traffic. The two command lines involved were (on the client) iperf –c 192.168.1.200 –p <port> –w 128k –i .5 –r –t 90 ><file>.txt and (on the server) iperf –s –w 128k –p <port>. The ports used were 5001 and 5002.

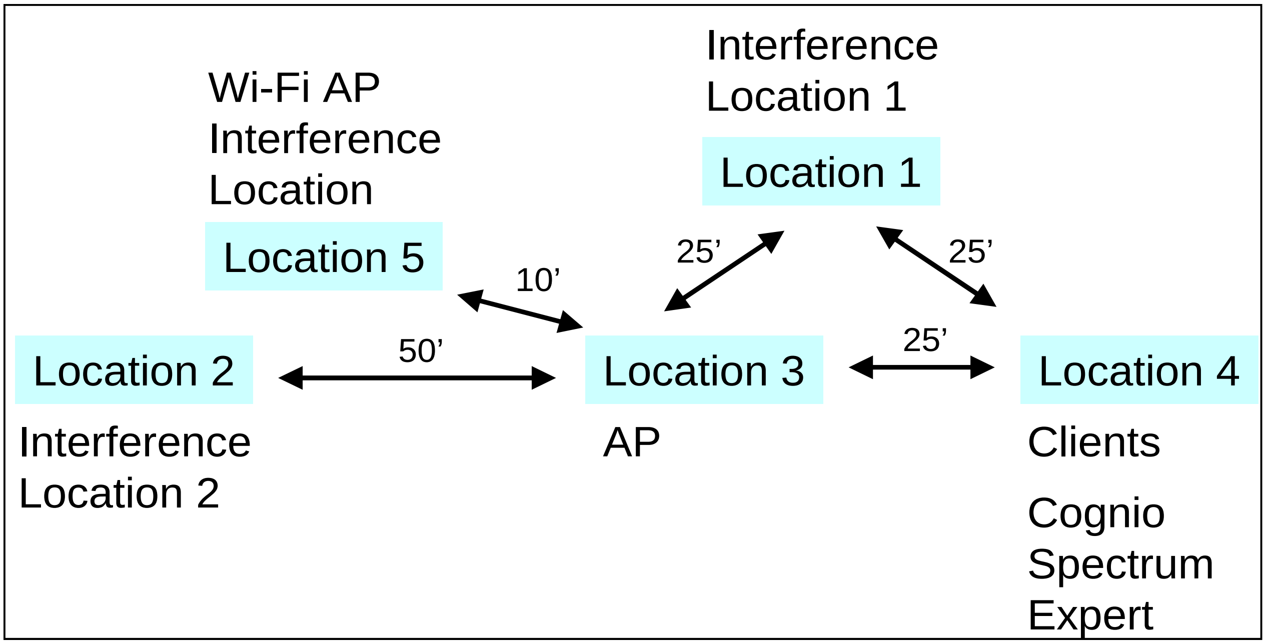

Figure 1 - Test geometry. Equipment was moved from Location 1 to Location 2 and the Iperf runs repeated. Location 5 was used only for the AP end of the interfering Wi-Fi system. *Source:* Farpoint Group.

Both notebooks were equipped with internal Intel PRO/Wireless 2915ABG radios [http://www.intel.com/network/connectivity/products/wireless/prowireless_mobile.htm], and we verified the use of the latest available drivers for all devices. We also set up Cisco's Spectrum Expert at Location 4, which we used to perform an initial RF sweep and as a monitor during benchmark runs. The key result of the former was the selection of Wi-Fi channel 7 for testing, as it appeared to be the best choice overall for minimal background traffic of any form (i.e., it was the "cleanest" of the 2.4 GHz. channels at the time of testing). Again, we also monitored for any other interference during the test runs.

The general strategy was to test a number of potentially interfering devices at two different locations, one (Location 1) approximately 25 feet from both the AP and the clients ("short range"), and the other (Location 2) approximately 50 feet from the AP and 75 feet from the clients ("long range"). We obtained an initial baseline result in an interference-free environment by running the two Iperf streams for two iterations, obtaining four results. These were averaged to a single number which we used for comparison with exactly the same test run under conditions of varying forms of interference. We also averaged four results per interference test run as well for consistency.

Test Procedures

Interference sources were set up, in turn, at Locations 1 and 2. Each was operated with default settings during the execution of three-minute Iperf runs identical to those used to obtain the baseline. The interference sources tested included:

- *Microwave Oven* − An Emerson MW8987B oven was used because it was available and regularly used by workers in the office. The oven cavity was occupied by a glass of water. Microwave ovens operate at a 50% duty cycle, with energy centered at 2.45 GHz., the resonant frequency of water. The Emerson MW8987B operates at 900 Watts, much less than the 1200 now common. All microwave ovens are allowed a small amount of leakage, measured in milliWatts (mW) at a distance of a few centimeters, and this value is allowed to increase as the oven ages (see http://www.access.gpo.gov/nara/cfr/waisidx_03/21cfr1030_03.html for more information). Regardless, the leakage value is set very low for safety reasons, as the typical human body is approximately 70% water. It should be noted, then, that the presence of humans in the vicinity of the test might have had an effect on the outcome, but since approximately the same number of humans were present in each case, and, since these humans would absorb both WLAN traffic and the interference sources, we do not believe their presence materially affected the test results in this or any case covered by this report. Regardless, the specific amount of interference from microwave ovens varies widely with brand, model, and the age of the oven, but essentially all will interfere to some degree.

- *TDD Cordless Phone* − A Uniden TRU4465 was used in this case. The handset was placed off-hook with the base station, both in close proximity at the interference locations. This phone uses direct-sequence spread-spectrum (DSSS), which places a fairly low level of wideband RF across a portion of the 2.4 GHz. band. While we could have selected a non-interfering channel for the phone, our objective was after all to see how it might affect WLAN traffic. We therefore selected a channel overlapping Wi-Fi Channel 7, and expected severe interference with our Wi-Fi signal.

- *Interfering Wi-Fi System* − For this equipment, we selected a Netgear WG602 (Version 2) AP [http://www.netgear.com/Products/WirelessAccessPoints/WirelessAccessPoints/WG602.aspx], and placed it at Location 5. We then used a client PC, also equipped with the Intel PRO/Wireless 2915ABG radio, and tested this connection at the two interference locations. We operated only a single Iperf stream between the two, but traffic was otherwise identical to that used for our benchmark.

- *DECT Phone* − We used a Panasonic KX-TG2740 handset here. This phone is based on (but not precisely compatible with) the Digital Enhanced Cordless Telecommunications (DECT) [http://www.dect.ch/] specification particularly popular in European products, but also seen in many cordless phones sold elsewhere in the world. DECT uses frequency hopping, with narrowband channels across the entire 2.4 GHz. band (in the US).

- *Video Camera* − We chose a XC18A camera from X10, a popular manufacturer of residential home automation products. The camera's signal is analog, not digital, and designed for long-range (100+ feet operation) via a directional antenna. We expected severe interference from this device.

- *Bluetooth Headset* – We used a Jabra BT-200. Cordless headsets are by far the most popular (and common) application for Bluetooth. Bluetooth, however, typically operates at very low transmit power levels (about 1 mW), and we thus expected little interference from this device at the ranges tested.

While some of these devices are no longer current models, all were chosen because they display quantifiable interference characteristics and represent the types of interferers WLAN users are likely to encounter in an office setting. We did not worry very much about the detailed specifications for any of the above devices, nor did we calibrate or otherwise characterize them (although Spectrum Expert did in fact accomplish the latter, correctly identifying all sources of interference by type). Rather, it was our intent to simply gather data regarding the above devices interfering, in two locations, with our previously-baselined configuration, and then to evaluate the results. The process here was simple: we re-ran our baseline test with each of the above interferers running at both the "short" and "long" locations, and noted the Iperf results.

Test Results

The results of testing are shown in Table 1 and Figure 2. All results are in Mbps, except for percentage numbers, which show the percentage of the original throughput still available in the presence of each interferer. As expected, we saw greater interference when the interferers we placed closer (Location 1), and less at longer range.

		Location 1 - Short (Mbps)				Location 2 - Long (Mbps)			
	Port	Run 1	Run 2	Average	% of Baseline	Run 1	Run 2	Average	% of Baseline
Baseline	5001	10.60	10.40						
	5002	10.30	10.40	10.43					
Microwave Oven	5001	3.88	3.68			4.67	4.77		
	5002	3.79	4.24	3.90	37.39%	5.09	5.21	4.94	47.34%
TDD Phone	5001	0.00	0.00			0.00	0.00		
	5002	0.00	0.00	0.00	0.00%	0.00	0.00	0.00	0.00%
Wi-Fi	5001	0.22	0.99			4.26	1.17		
	5002	2.15	1.00	1.09	10.44%	3.35	1.56	2.59	24.80%
DECT	5001	9.08	8.42			9.57	9.23		
	5002	8.16	8.39	8.51	81.65%	9.61	9.25	9.42	90.31%
Video Camera	5001	0.00	0.00			1.64	7.26		
	5002	0.00	0.00	0.00	0.00%	1.87	7.17	4.49	43.02%
BT Headset	5001	8.40	8.10			9.34	8.42		
	5002	9.00	8.07	8.39	80.50%	8.42	8.44	8.66	83.02%

Table 1 - The results of two bidirectional runs (four values in total) were averaged to obtain a figure of merit in each case. Of interest was the percentage of original baseline throughput available when the link was subjected to each interferer; this value is noted in the table for each location. *Source:* Farpoint Group.

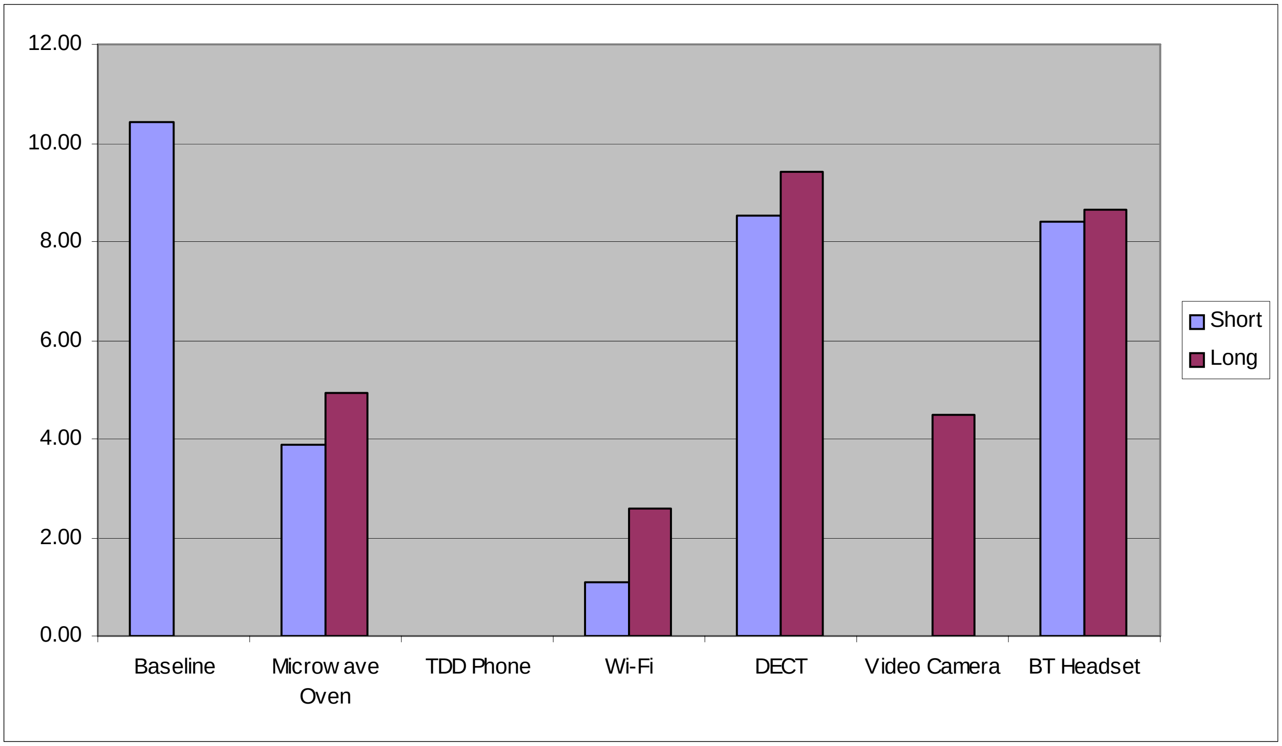

Figure 2 - A graphical version of Table 1. The value on the Y-axis is megabits per second. Note the complete obliteration of the Wi-Fi signal by the TDD phone and the video camera when operated in the "short" location (Location 1). *Source:* Farpoint Group.

We were surprised to see the *complete* obliteration of the Wi-Fi signal by the TDD phone, but not by the video camera, although this signal was less of a factor at longer range than we expected. Both the DECT and Bluetooth devices caused more degradation than we expected, especially in the case of Bluetooth, because its signal is so weak to begin with. Both reduced throughput at short range by about 20%, significant although still much less than the other sources. Also surprising was the degree of interference between the two Wi-Fi systems. One network reduced the throughput of the other by 75%, while its own throughput was reduced by 90%. Granted, both test networks were fully loaded, but it's very clear that Wi-Fi's listen-before-talk protocol was overwhelmed by this situation.

Overall, it was easy to see that common wireless devices can ruin the day of both users and network managers unless steps are taken to identify and mitigate their impact. And, of course, without proper SA tools, it could be very difficult indeed to determine exactly the cause of the problem in any given case.

Conclusions and Recommendations

It is quite obvious from this work that common sources of interference can have a significant – and even *dramatic* − impact on the performance of WLANs carrying typical LAN data traffic. All applications, including Web access, e-mail, and access to shared data and other network resources, can be adversely affected. Our tests were designed to see how sources of interference might affect a heavily-loaded wireless LAN. While it can be argued that most WLANs today do not see such a high level of use, we believe that this will increasingly become common as WLANs become the default and even primary means of access in many if not most enterprise settings. An increase in utilization is driven by the shared nature of a WLAN AP and, of course, the ever-increasing number of users and their increasing traffic demands, with respect to both raw volume and time-boundedness. Since both the number of potential interferers and the volume of WLAN traffic itself will increase over time, we can conclude that interference will become a challenge in many, if not most, WLAN shops over the next few years.

Because interference from both Wi-Fi and non-Wi-Fi sources will manifest itself as a reduction in throughput, and because such can result from non-RF problems, such as congestion on the wired network, and because lower throughput will almost always impact user productivity, it therefore behooves any enterprise-class installation to have the tools necessary to recognize, characterize, localize, and monitor any potential sources of interference. Such functionality is today available in standalone Spectrum Assurance tools, like the Spectrum Expert products we used in these tests, and has also been integrated into some Wireless LAN Assurance (WLA) tools. WE are also seeing this functionality being integrated into wireless LANs themselves, such as via Cisco's Wireless Control System 4.2 [http://www.cisco.com/en/US/products/hw/modules/ps2797/prod_bulletin0900aecd806b7f8a.html], over the next few years. And we believe that the eventual coupling of RF Spectrum Management (RFSM) capabilities (implemented to varying degrees in all enterprise-class products today) and SA tools will result in significant intelligence and automation being applied to the identification and remediation of radio interference, minimizing the potential load on network operations staff, and thus improving productivity and lowering overall operational expense (OpEx) and total cost of ownership (TCO).

Of course, interference remediation may still require manual intervention, such as replacing an interfering device with non-interfering equivalent, reconfiguring elements of the WLAN, or even having a chat with a nearby operator of interfering wireless equipment. Regardless, we believe that interference will become as manageable as any other element of LAN operations, and that users and network managers alike should feel free to embrace wireless LANs as a mission-critical capability in enterprises of all sizes and types.

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