The Effects of Interference on Video Over Wi-Fi

A Farpoint Group Technical Note

Document FPG 2006-329.3
January 2008

While not yet common, Farpoint Group expects the transmission of many forms of video over Wi-Fi-based wireless LANs (WLANs) to become common over the next few years in both residential and enterprise settings. The application of video over Wi-Fi in the residence is obvious – the point of presence for video service (a cable box or similar element) is seldom located near where the video will be watched. As a typical residence is much more difficult to wire than the typical enterprise, using wireless as a link between where the video is brought into the house and where it will be consumed makes perfect sense. And, of course, we expect locally-mobile distribution of video to become very popular as well, using such products as Pinnacle's PC TV To Go HD Wireless [http://www.pinnaclesys.com/PublicSite/us/Products/Consumer+Products/ PCTV+Tuners/PCTV+Analog_Digital+PVR/PCTV+To+Go+HD+Wireless.htm], the Slingbox from Sling Media [http://us.slingmedia.com/page/home], Sony's LocationFree TV [http://www.learningcenter.sony.us/assets/itpd/locationfreetv/index.html], and software from suppliers like Orb Networks [http://www.orb.com/]. And while not as common in the enterprise, the increasing use of streaming video for Webcasts, Webinars, corporate news and announcements, trip reports, and even news feeds, will also become popular over the next few years, again with distribution over a wireless LAN.

Streaming video represents perhaps the greatest possible challenge to LAN performance, wired or wireless, because it involves two key constraints that fundamentally push the limits of the LAN. The first of these is the sheer volume of data - video is a large object that can require the transfer of hundreds of megabytes (or more) of data. While multicasting can reduce network bandwidth requirements, an on-demand video environment, which we believe will become increasingly the norm, can place a strain on any LAN infrastructure even when interference isn't a problem. And second, and even more importantly, streaming video is by its very nature *isochronous*, or *time-bounded*. This means than not only is the volume of data high, but it must be prioritized and expedited. And, even with buffering on the receiving end, time is indeed of the essence in the success of streaming video. Video might, then, be thought of as the ultimate test of LAN performance.

This situation becomes all the more complex when we add interference to the mix. Most digital video transmissions are of necessity compressed to conserve bandwidth. While video purists have contended for some time that compression results in numerous observable visual artifacts, and thus have provided the motivation for uncompressed video formats such as the High-Definition Multimedia Interface (HDMI), interference clearly holds the potential regardless for a less-than-satisfactory viewing experience. And radio interference of the type that can clearly cause damage to WLAN-based communications is thus a core concern as video-over-Wi-Fi becomes more popular, and, indeed, common.

It was with this in mind that we undertook a series of experiments regarding the effect of interference on streaming video sent over a Wi-Fi connection. This project builds upon the work we initially began in the development of our White Paper FPG 2006-321.2, *The Invisible Threat: Interference and Wireless LANs*, and further upon the methodology defined in our Technical Note FPG 307.2, *Evaluating Interference in Wireless LANs: Recommended Practice*. In general, evaluating the effects of interference is based upon the difference between throughput observed on an unimpaired link (as verified by appropriate monitoring for interference if the test is conducted in freespace) and that of the same link subject to controlled interference. Some percentage of degradation is usually observed and is easily quantified in the general case. For an example, see our Tech Note FPG 2006-328.3, *The Effects of Interference on General WLAN Traffic.*

Unfortunately, this methodology is incomplete when evaluating the effect of interference on streaming video on WLANs, the subject of this Tech Note. And the reason for this is that video quality is fundamentally subjective. While we have been able to apply excellent analytical techniques to the evaluation of that other streaming medium, voice traffic, such is not common today in evaluating video quality. This means that a more subjective evaluation of video quality is required in work of this type, and that is what we used in this project. As an aside, we hope at some point to find (or develop) a tools for the direct analytical frame-by-frame comparison of two video streams, and to develop (or adopt) a figure of merit for describing the result.

Test Scenario and Methodology

The geometry and elements of the video quality testing we performed can be seen in Figure 1. We used the same facility as in FPG 2006-328, and an essentially identical test geometry with two different interference sources – a "short" location, approximately 25 feet from both the video source and destination, and a "long" location approximately 50 feet from our video destination and 75 feet from our video source. The video source and destination were approximately 25 feet apart, and located in cubicles in a typical office environment.

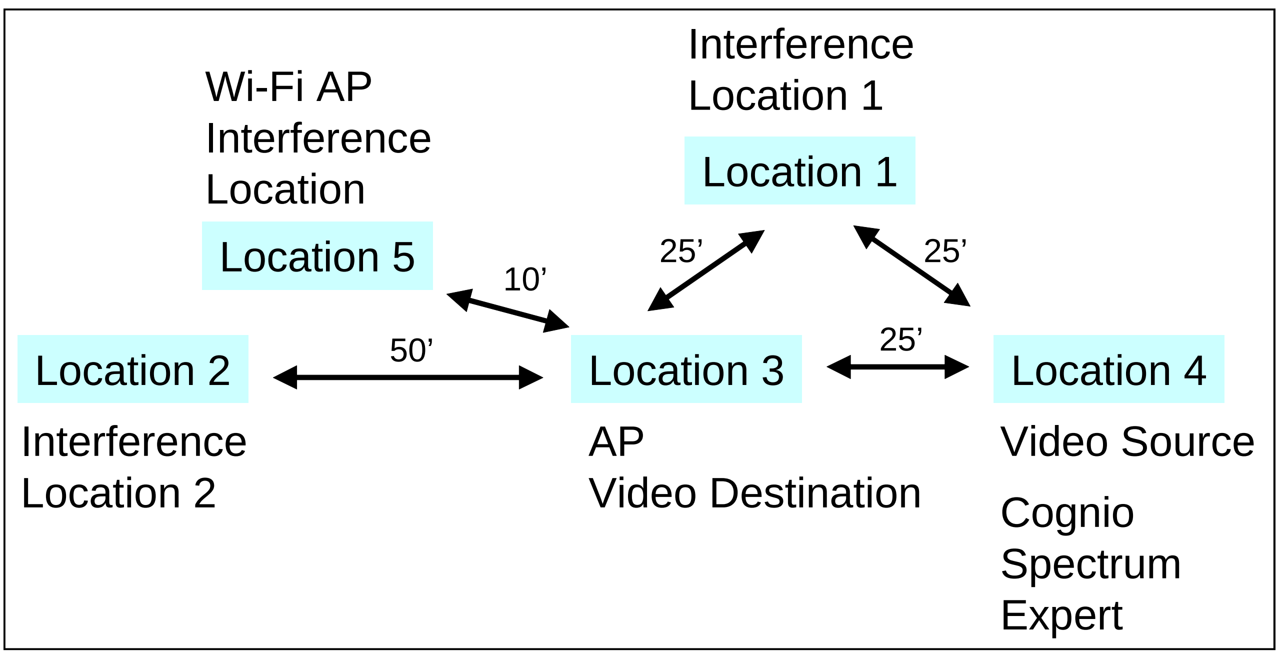

Figure 1 - The configuration of elements used in this testing. Location 1 is also referred to as the "short" test, and Location 2 as the "long" test; both were used for siting the interferers. Video was sent from Location 4 to Location 3. Location 5 was used only for the AP-end of the interfering Wi-Fi system. *Source:* Farpoint Group.

Because the evaluation of video performance and quality can be both analytical (quantitative) and subjective (qualitative), we decided to run two different sets of tests. The first of these used the Iperf benchmark [http://dast.nlanr.net/Projects/Iperf/] to generate UDP traffic typical of a streaming video source. We used the following command lines for our analytical testing:

iperf –u –c <IP Address> -w 768k –i .5 –t 180 -b 10m (client)
iperf –u –s –w 768k –i .5 (server)

A baseline result was obtained by sending the UDP stream unimpaired from the source (Location 4) to the destination server (Location 3). We then repeated each test with the interferers in turn in Locations 1 and 2, and recorded the results. Due to time constraints, only a single run of each case was performed. We did, at this point, have sufficient experience with the environment to have confidence in the results of only a single run. And, of course, the use of Cisco's (formerly Cognio's) *Spectrum Expert* product at Location 4 enabled us to monitor for extraneous interference, and none was noted during any test run.

For subjective testing, we used the popular (and freely available) VideoLAN VLC application [http://www.videolan.org/]. We used version 0.8.2 of VLC for our work here. VLC, like Iperf, can function as both a client and a server, depending upon configuration, and can provide high-quality streaming video. We used a portion of a commercial DVD for source material. We ran this connection, again from Location 4 to Location 3, noting any video artifacts (errors) observed, and rated (by group consensus) video quality with each interferer as one of the following:

Unwatchable	Severe degradation and/or screen freezes
Impaired	Occasional artifacts
Minor	Artifacts noted only very rarely
Flawless	No difference from baseline

Artifacts were usually the "blockiness" and freezes typically observed when an MPEG decoder lacks sufficient key-frame information to successfully produce an image. To be fair, these can be observed on occasion even on cable television and satellite-television images due to network congestion, but on these media the impairment is seldom more than very minor indeed.

The Interferers

A number of interference sources were used in this test. All were operated with default configurations other than setting channels for maximum overlap where appropriate. These sources 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 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 selected a channel overlapping Wi-Fi Channel 7, and therefore 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 equipped with the Intel PRO/Wireless 2915ABG radio (the same as was used for the video link), and tested this connection at the two interference locations. The traffic generated in this case was a continuous IP stream.

- *DECT Phone* – We used a Panasonic KX-TG2740 handset here. This phone is based on (but not identical to) 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 is based on frequency hopping, using narrowband channels across (in the US) the entire 2.4 GHz. band.

- *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, and we 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 compare the results of the above devices interfering, in two locations, with our previously-baselined configuration, and 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. We repeated the runs while using VideoLAN to obtain subjective results.

Test Results

The results for the analytical testing as presented in Table 1 and Figure 2. The key metric is total bytes transferred, and this is the value used to compute the percentage of the original baseline throughput available under conditions of the various interference sources. As we expected, the TDD phone handset and video camera caused very large (total at short tange) reductions in effective throughput. The DECT phone and Bluetooth headset, on the other hand, had no impact whatsoever, with in fact slightly greater throughput than the baseline noted in the results. This was due to statistical variations essential in the nature of radio and is not otherwise significant. The microwave oven also caused serious degradation, and, in every case, we observed that the closer the interferer, the greater the degradation of throughput, as expected. We also obtained results for both jitter (minute variations in timing that can result in packet errors and packet loss) and packet loss itself, the latter expressed as a percentage of total packets sent. The microwave oven was the only interference source causing large amounts of jitter.

	Location 1 (Short)				
	Throughput (Mbps)	**Total Transferred (MB)**	**Jitter (ms)**	**Packet Loss %**	**% of Baseline**
Baseline	9.99	214.00	0.000	0.1100%	100.00%
Microwave Oven	4.07	87.90	64.512	59.0000%	40.74%
TDD Phone	0.00	0.00			0.00%
Wi-Fi	8.03	173.00	4.156	20.0000%	80.38%
DECT	10.00	215.00	2.683	0.2600%	100.10%
Video Camera	0.00	0.00			0.00%
BT Headset	10.00	215.00	2.341	0.0059%	100.10%
	Location 2 (long)				
	Throughput (Mbps)	**Total Transferred (MB)**	**Jitter (ms)**	**Packet Loss %**	**% of Baseline**
Baseline	9.99	214.00	0.000	0.1200%	100.00%
Microwave Oven	6.51	135.00	65.259	36.0000%	65.17%
TDD Phone	3.61	77.70	4.634	64.0000%	36.14%
Wi-Fi	6.49	140.00	6.993	35.0000%	64.96%
DECT	10.00	215.00	2.379	0.0026%	100.10%
Video Camera	0.00	0.00			0.00%
BT Headset	10.00	215.00	2.075	0.0039%	100.10%

Table 1 - Results of the testing. The key metric is throughput in megabits per second (Mbps). Note that performance was actually better than baseline in the case of some interferers; this is due to minor statistical variations between runs and is not otherwise significant. *Source:* Farpoint Group.

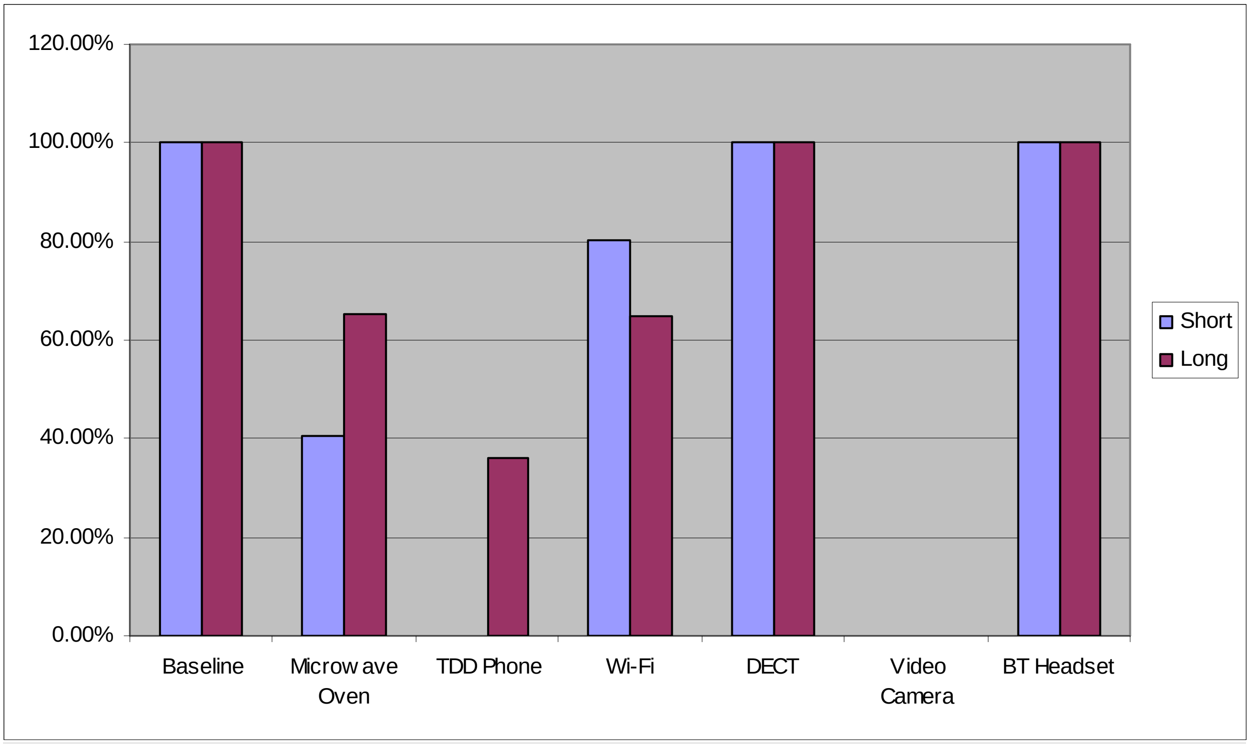

Figure 2 - A graphical view of the data presented in Table 1. Note the complete obliteration of the video signal by the TDD phone (short range) and the video camera. *Source:* Farpoint Group.

The subjective results (see Table 2) obtained from watching VideoLAN correlated nicely with the analytical results. All but the DECT phone and the Bluetooth headset caused enough interference that the result would have been unacceptable under any circumstances. Again, LAN-based video is typified by a demanding combination of large data objects and strict time-boundedness constraints (again, subject to buffering). Note here, however, that buffering would be of no value in interactive applications such as videoconferencing. There really is no substitute in the case of LAN-based video – wireless or otherwise – for lots of unimpaired bandwidth, making interference management all the more critical.

Interferer	Short	Long
Microwave Oven	Unwatchable	Impaired
TDD Phone	Unwatchable	Unwatchable
Wi-Fi	Unwatchable	Unwatchable
DECT	Minor	Minor
Video Camera	Unwatchable	Unwatchable
BT Headset	Flawless	Flawless

Table 2 - The results of a subjective analysis of video performance under the same conditions of interference as evaluated in the analytical tests. Note the high degree of correlation between the analytical tests and the subjective evaluation. The scale used in this table is described on page 4 of this report. *Source:* Farpoint Group.

Conclusions

As we demonstrated via the work described in this Tech Note, overall LAN performance can have a major impact on the quality of video delivered over that LAN - and interference can have a correspondingly major impact on the performance of wireless LANs. This situation may become serious in residential settings over the next few years, as an increasing number of VidFi (we hesitate to coin this term, but there it is) products appear on the market.

But we also believe that video-over-WLAN performance will be important in enterprise settings as well, as greater use is made of streaming video for presentations, videoconferencing, and live feeds from devices as diverse as video-equipped cell phones and Wi-Fi surveillance cameras. As we discussed in our earlier Tech Note on the effects of interference on general LAN traffic (FPG 2006-328.3), interference of any form will need to be managed in enterprise settings no matter what the application.

We believe that the use of Spectrum Assurance (SA; Cisco calls this *Spectrum Intelligence*) tools, such as those now included in Cisco's Wireless Control System (WCS), is the best approach to addressing the challenge of interference, especially in the near term. Over time, as SA capabilities are further integrated into enterprise-class wireless-LAN products themselves, we expect a significant degree of automation will be applied to solving interference problems, eventually rendering the challenge essentially transparent for network managers and operations staff – not to mention users. In the interim, however, these constituencies need to be aware of the potential challenge interference represents to VidFi and to avail themselves of the tools now available.

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.