Coexistence in the 2.4-GHz band: bridging Bluetooth and Wi-Fi

Winston Sun and Niraj Trivedi - April 30, 2007

Picture this: You're at the airport waiting for your flight. To pass the time, you're working on your laptop and talking to your loved one using a hands-free cellular headset. All of a sudden, you hear popping noises over your Bluetooth headset, or your Bluetooth mouse skips. What's going on? Are the technologies that enable this convenient, untethered connectivity conspiring against you?

Bluetooth and Wi-Fi attach rates are growing rapidly, not only in notebook computers but also in all mobile consumer electronics, such as smart phones, MP3 players and even digital cameras. Research firm In-Stat predicts Bluetooth device shipments will top 600 million units this year and climb to nearly 800 million in 2008. As for Wi-Fi, in North America it's almost impossible to buy a notebook computer that does not feature built-in wireless-LAN capabilities. In addition, the trend is for portable consumer electronics devices to include both Bluetooth and Wi-Fi.

While the value-adds of untethered connectivity are obvious, a problem is brewing with the rapid adoption of Bluetooth and Wi-Fi: The most popular WLAN solution currently (802.11g) and Bluetooth share the same, 2.4-GHz unlicensed spectrum--opening the door to interference that can compromise performance.

Further, in the near future, 802.11n will become the mainstream WLAN protocol and bring with it added complexity, since 802.11n can occupy a 40-MHz-wide channel instead of the 20-MHz standard channel used by legacy WLAN devices. The .11n variant also allows for aggregated packets, an accommodation that increases frame length and thus raises the probability of interference.

These over-the-air collisions can result in popping sounds on your Bluetooth headset, an unresponsive Bluetooth keyboard or mouse, or increased file download times when the Wi-Fi connection slows down. To ensure that consumers have a positive experience when using the latest wireless mobile connectivity products, the industry has been addressing the coexistence issue.

(Strictly speaking, WLAN refers to the IEEE 802.11 protocols, whereas Wi-Fi refers to WLAN devices that have undergone interoperability testing by the Wi-Fi Alliance. In this article, however, the terms WLAN and Wi-Fi are used synonymously.)

There are two typical scenarios where wireless interference can occur: Bluetooth and WLAN are co-located in the same device, or Bluetooth and WLAN are in proximity but not co-located. The industry
has proposed solutions for each type, and silicon vendors have implemented those remedies.

The portable consumer electronics industry has recognized that the co-located device has several advantages. Aside from the value-add that each wireless feature brings, sharing many of the components cuts cost. Indeed, everything from the antenna, power amplifier and low-noise amplifier can potentially be shared and thereby reduce overall cost.

For the Bluetooth/WLAN co-located scenario, time-division multiplexing of the spectrum is a feasible solution. In other words, spectrum is shared over time between Bluetooth and Wi-Fi as appropriate. Since the WLAN and Bluetooth are co-located, there can be a way to communicate between the devices to coordinate the multiplexing.

The industry has settled on de facto standards for the communication protocols--known as the two-, three- and four-wire protocols--between Bluetooth and Wi-Fi. The protocols handle arbitration, master/slave selection and priorities between the two devices. There is a caveat, however: Silicon vendors vary slightly in their implementations of the protocols. Thus, there may be an advantage to using Bluetooth and Wi-Fi solutions from the same silicon vendor.

Bluetooth operates using a frequency-hopping spread-spectrum modulation where it pseudo-randomly hops among 79 channels. In the non-co-located scenarios where Bluetooth and Wi-Fi devices are in proximity to each other, adaptive frequency hopping will help prevent collision interference. AFH requires the Bluetooth device to scan for WLAN traffic (or any other interferers) and avoid those channels, which may contain significant energy like Wi-Fi traffic. AFH is not suitable for co-located scenarios, however, since the signal power from the Wi-Fi may overwhelm the AFH circuitry that is scanning for potential interferers. AFH is required by the 2003 Bluetooth spec 1.2 and beyond. (The March 2007 Bluetooth 2.1+EDR is the most current version of the spec.)

The IEEE requires a coexistence assurance (CA) document, which includes all the analysis required to ensure compatibility between new and existing IEEE communications protocols. In the case of 802.11n, compatibility with 802.15.1 (personal-area networks, Bluetooth), 802.16 (broadband wireless access) as well as cordless telephony are considered. The CA document (see reference) for 802.11n covers the Bluetooth case extensively with two types of analysis.

The first type is geometric, where there is a physical separation between the WLAN and Bluetooth interferer (no AFH). The second is temporal and takes into account 802.11n's 40-MHz operation as well as packet aggregation.

Using geometric analysis, one can determine the amount of interference a Bluetooth signal imparts on WLAN and vice versa, based on distances between the interferer and the "interferee." Simulations theorize the minimum separation needed between the interfering Bluetooth device from a Wi-Fi client that would enable the WLAN connection to maintain its performance. These were carried out using the maximum transmission power allowed by the FCC and the path loss over free space.

Simulations for legacy Wi-Fi traffic show that when the Wi-Fi application processor-client distance is
15 feet, 30 feet or 60 feet, the minimum Bluetooth (BT) separation distance is 7 feet, 13 feet or 27 feet, respectively.

These theoretical computations show that even for legacy Wi-Fi, close physical proximity of Bluetooth devices to Wi-Fi-connected laptops will definitely hinder the WLAN performance, unless AFH or other collision-avoidance mechanisms are in place. To maintain 802.11n performance, it is anticipated that the separation between the interferer and “interferee” would need to grow.

The temporal analysis takes into account both the aggregated packet length and the use of 40-MHz-wide channel mode with 802.11n to determine Wi-Fi performance vs. Bluetooth occupancy of the spectrum (in percent). Simulations show the following results:

**Wi-Fi: 20 MHz, packet size: 10 kbytes**

10% **BT overlap** 2% Wi-Fi degradation

50% **BT overlap** 25% Wi-Fi degradation

**Wi-Fi: 40 MHz, packet size: 10 kbytes**

10% **BT overlap** 10% Wi-Fi degradation

50% **BT overlap** 30% Wi-Fi degradation

**Wi-Fi: 20 MHz, packet size: 40 kbytes**

10% **BT overlap** 9% Wi-Fi degradation

50% **BT overlap** 40% Wi-Fi degradation

**Wi-Fi: 40 MHz, packet size: 40 kbytes**

10% **BT overlap** 10% Wi-Fi degradation

50% **BT overlap** 45% Wi-Fi degradation

On the Wi-Fi side, the clear channel assessment (CCA) mechanism is used to avoid over-the-air collisions (CCA/CA) with other Wi-Fi traffic. It can also be used to prevent collisions with Bluetooth. CCA is similar to Bluetooth's AFH in that the Wi-Fi device must scan for potential interferers in its own spectral band. Whereas Bluetooth avoids transmitting signals on channels where it suspects other traffic, Wi-Fi simply refrains from transmission until the "air is clear."
So, how well do AFH and CCA work? Even for low-bandwidth applications, sharing the same 2.4-GHz medium can affect performance. Real-life over-the-air testing was performed by Atheros Communications to subjectively compare the results between those from simulations in the CA document and real user experiences. To measure the performance degradation on Bluetooth, various off-the-shelf Bluetooth 2.0 devices with AFH such as a keyboard, mouse, headset and handset were used in the presence of Wi-Fi. The following Wi-Fi usage cases were generated for the non-co-located case: 802.11g traffic; high-throughput 20-MHz (HT20) 802.11n traffic; high-throughput 40-MHz (HT40) 802.11n traffic; and finally HT40 + 802.11g traffic. In the last case, the 802.11g and HT40 channels were separated so as to not cause interference with each other, only to the Bluetooth traffic.

The Bluetooth user experience suffers when more Wi-Fi traffic shares the airwaves with Bluetooth devices. The onus is on Bluetooth and Wi-Fi solution providers to boost detection and avoidance algorithms so the degradations are minimized in coexistence environments.

For the co-located case, measurements were taken by Atheros Communications to determine the performance degradation that a voice-over-Internet Protocol application running over 802.11g experiences in the presence of Bluetooth interferers. For this experiment, packet loss measurements were taken with and without the two-, three- and four-wire protocol in place.

Bluetooth and Wi-Fi share the 2.4-GHz unlicensed spectrum and can cause undesired performance degradation. For the non-co-located scenario, there’s AFH for Bluetooth and CCA/CA for Wi-Fi.

For the co-located scenario, prevention of collisions/interference is aided by implementing an arbitration protocol between the Bluetooth and Wi-Fi devices. Implementing such a scheme in an 802.11g Wi-Fi/Bluetooth embedded combo environment has shown a 179-138?90 percent reduction in lost data packets. Similar schemes will be needed when 802.11n becomes the mainstream Wi-Fi protocol, since it can cause higher Bluetooth interference.

There are many experts tackling the coexistence issue so that consumers can have Bluetooth and WLAN connectivity in their laptops and smart phones. The challenge remains to make these technologies transparent to the user. The solutions need to be simple, reliable and unobtrusive to the device’s primary application.

Reference. IEEE 802.11-06/0330r4: p802.11n Coexistence Assurance Document, Eldad Perhia, Sheung Li

PWinston Sun (wsun@atheros.com) is technical marketing manager at Atheros Communications Inc., with a BS in electrical engineering from the University of California at Los Angeles, and a PhD and MS in electrical engineering from the University of California at Berkeley.
Niraj Trivedi (ntrivedi@atheros.com) is technical marketing engineer at Atheros Communications Inc., with a BS in electrical engineering from Saurashtra University in India and an MS in electrical engineering from San Jose State University.