How Bluetooth and Wi-Fi Interfere….and Coexist

Spread spectrum technology allows Bluetooth and Wi-Fi technologies to coexist and at the same time to interfere with each other. Both Bluetooth and Wi-Fi use spread spectrum in their signaling structure where a narrowband signal is expanded to a wideband signal. The advantage of spreading the signal is that a wideband signal is less susceptible to jamming (intentional blocking) and noise or interference (unintentional blocking). Here we very briefly cover the technology behind spread spectrum to lay a foundation for understanding how it is used in Bluetooth and Wi-Fi technology, followed by a discussion of the coexistence issues surrounding the collocation of these wireless technologies in modern chips and wireless devices.

The 2.4GHz Industrial, Scientific and Medical Device Band (ISM)

Bluetooth and Wi-Fi are two of the most widely used wireless technologies in consumer electronics. Both use the 2.4 GHz ISM band for the RF transmission medium but are different in every other aspect. While Wi-Fi continuously transmits, Bluetooth uses a slotted transmission method for the purpose of power efficiency. It is these and other technological differences that create the interference. Bluetooth transmissions look like noise to Wi-Fi receivers, and Wi-Fi transmissions look like noise to Bluetooth receivers. This would not be a problem except for the common use of the 2.4 GHz ISM band and the popularity of consumer wireless devices that simultaneously use Bluetooth and Wi-Fi technology. The close proximity of these technologies compounds the interference issues. In some devices, such as smartphones, Wi-Fi and Bluetooth share the same chipset and antenna. When interference occurs there is degradation in data rates or throughput. Received data packets that contain errors are retransmitted. Retransmissions result in reduced data rates.

Spread Spectrum

Fundamentally, spread spectrum uses wideband noise-like signals that are hard to detect, intercept, or demodulate. Hence the technology was originally intended for military use. However there is one feature that makes spread spectrum ideal for Wi-Fi and Bluetooth applications: The spread of energy over spread spectrum and narrowband signals can occupy the same band with little or no interference.

Wi-Fi technology arrived on the scene well before Bluetooth technology, and the developers used spread spectrum methods to mitigate unintentional interference from other sources using the ISM band, e.g. microwave ovens and cordless phones. Wi-Fi technology use Direct Sequence Spread Spectrum (DSSS) that divides the original narrowband signal and combines it with a pseudo-random number called a chipping code. The chipping code spreads multiple copies of the original signal across a wider portion of the operating band to form a channel. Each channel is 22 MHz wide but the channel carrier stays at a fixed frequency. The power in the original narrowband signal and the spread signal is the same giving a lower power density in the spread signal that is less susceptible to creating interference. The Wi-Fi receiver uses the same chipping code as the transmitter to de-spread the channel and to raise the power density. The de-spreading has the effect of spreading any received interference and lowering the interference signal power density and reducing the possibility of signal degradation.

When Bluetooth first appeared in 1994, it interfered with Wi-Fi. The Bluetooth developers used a spread spectrum method that is different than DSSS used by the Wi-Fi technology. Frequency Hopping Spread Spectrum (FHSS) spreads the narrowband signal by hopping around to different carrier frequencies within a frequency band. Bluetooth transmits on any one of 79 (for Classic Bluetooth) or 40 (for Bluetooth low energy) 1-MHz channels or frequencies in the ISM band. Channels change 1,600 times per second, or every 625 microseconds. The Bluetooth transmitter and receiver share and adhere to the same hopping sequence within a session. By hopping to different frequency at a different time the likelihood of encountering interference is reduced.

Differences arise between DSSS and FHSS methods. FHSS needs more power than DSSS to achieve the same signal-to-noise ratio. DSSS must only synchronize the transmitter and receiver chipping code, while FHSS must synchronize in both time and frequency. Frequency hopping needs time to search for the next signal and lock to it increasing timing latency. FHSS is better at multi-path situations—reflected signals caused by obstructions—because it does not stay at one frequency very long, and a null at one frequency is usually not a null at another frequency.

There is one essential problem when Wi-Fi and Bluetooth coexist in close proximity: DSSS and FHSS are different and incompatible. To Wi-Fi, Bluetooth appears as noise because it is unrecognizable as a coherent signal. To Bluetooth, Wi-Fi DSSS appears as noise.

Can Bluetooth and Wi-Fi Collide?

A Wi-Fi channel is 22 MHz wide and a Bluetooth channel is 1 MHz wide. So, approximately 22 Bluetooth channels will fit into the range of a Wi-Fi channel. Of the 79 Classic Bluetooth channels available for FHSS, 22 (27%) will appear within the same frequency space as a given Wi-Fi channel.

A DSSS receiver cannot decode a FHSS transmission, and vice versa. One spread spectrum method is nothing but interference to a receiver using another spread spectrum method. The probability of a collision between Wi-Fi using DSSS and Bluetooth using FHSS is about 27%. If this unintentional blocking is sufficiently strong such that either the Wi-Fi or the Bluetooth receiver cannot decode the transmission, the transmission must be resent. Retransmissions have a negative impact on throughput.

> "The coexistence and collocation of wireless technologies in modern consumer products have a good probability of interfering."

Let's explore a simple example. Assume a situation with a device using collocated Wi-Fi and Bluetooth. Also assume that the Wi-Fi and Bluetooth are simultaneously active, e.g. making a Wi-Fi phone call while using a Bluetooth headset. If a Bluetooth channel hops into the middle of a transmitting Wi-Fi packet, it can corrupt it. After a few of these instances, the Wi-Fi transmitter will back off to a lower speed, resulting in more time to deliver a complete packet—decreased throughput. We know that the probability of another collision with that packet is 27%. Should that collision happen, the Wi-Fi will further reduce throughput.

Should the Wi-Fi signal corrupt the Bluetooth packet,

Bluetooth will hop to the next channel and try again if the Bluetooth transmission were asynchronous, and the result would be reduced throughput. However, since this example is a voice transmission using Synchronous Connection Oriented (SCO) links, packets can be lost because these links do not use Automatic Repeat Requests (ARQ).

Are Wi-Fi and Bluetooth collisions inevitable? When operating in close proximity, as on a chipset and sharing one antenna, the answer has be "yes". The coexistence and collocation of wireless technologies in modern consumer products have a good probability of interfering. Collisions will likely cause interference resulting in degradation of either or both the Wi-Fi and Bluetooth device. There are current solutions to the sharing of space and spectrum, but even these solutions present challenges for the designer/developer.

Isolation: Temporal, Spatial, Frequency, and Power

Successful solutions to Wi-Fi and Bluetooth coexistence and interference problems usually involve isolation of the radios. Four spheres of influence are often used: temporal or time separation, space separation, frequency separation, and channel RF power separation.

Temporal isolation most often uses Time Division Multiplexing (TDM) where the collocated Wi-Fi and Bluetooth radios with a single antenna are allotted time slots to transmit. Taking turns to signal is one collaborative mechanism whereby the radios communicate with each other, with a transmitting radio asserting itself via wired connection to idle the other radio. The asserting radio is isolating the other radio by controlling access to the antenna to avoid interference. TDM can work well with Bluetooth asynchronous data, but for SCO a Bluetooth priority control line would be necessary. Implementation of a TDM system to mitigate interference requires that the developer design controlling mechanisms into the hardware and software.

Spatial isolation involves physical separation and isolation of the radios and using separate antennas. The use of spatial isolation depends on the specifics of the product application. This is a non-collaborative mechanism because the radios have no physical or software link, and this mechanism is not compatible with the latest generation of Bluetooth/Wi-Fi chips and modules.

Another non-collaborative mechanism that was implemented with Bluetooth specification 1.2 is Adaptive Frequency Hopping (AFH) spread spectrum, which is found in every Bluetooth device in operation today and is a frequency isolation mechanism. With AFH, the Bluetooth radio can only use a certain set of frequencies as part of its hopping sequence. The radio scans the operating band for interference on all 79 channels and it makes a list of clear and noisy channels. This radio shares its scanned-channel list will all radios to which it is paired. Both radios in a link adapt their frequency hopping patterns to avoid the noisy channels, operating only in clear channels. Since DSSS channels appear as noise to Bluetooth, AFH is a mechanism to avoid a collision. The AFH algorithm must consider the following when deciding how many channels to block:

- The RF front-end components and respective isolation.

- The transmit power level of the Wi-Fi and Bluetooth devices. The higher the Wi-Fi device transmission power, the more Bluetooth channels that are needed to be masked to insure low packet error rate (PER).
- The flexibility of allowing simultaneous transmitting and receive activities on the Wi-Fi and Bluetooth devices.
- Maximum adjacent channel rejection of the Wi-Fi and Bluetooth devices.

RF isolation and gain adjustment is a mechanism to reduce interference caused by one device overpowering the other. Most Wi-Fi and Bluetooth implementations offer transmit power control algorithms to increase or decrease transmit power depending on link conditions. If the RF isolation between the Wi-Fi and Bluetooth devices is not enough, transmissions from either of the two devices can saturate the receive path of the other device, assuming the transmit power to be considerably high. This condition could cause a link to disconnect or cause high PER resulting in degraded throughput.

"Coexistence testing is difficult unless you can synchronize the Wi-Fi and Bluetooth packet streams"

There are many ways that the designer/developer can improve coexistence. The coexistence mechanisms described herein are just the tip of the ice berg, but they to present the most commonly implemented. Many of these interference mitigation mechanisms are software implementations. Designer/developers should thoroughly test their coexistence algorithms.

Testing to Improve Coexistence

Coexistence testing is difficult unless you can synchronize the Wi-Fi and Bluetooth packet streams. In any session, hundreds of thousands of data packets from both wireless technologies are transmitted over the air. You must have testing devices suitable for capturing the transmissions from links in each technology and displaying those packets in coexistence in a meaningful manner. These devices are normally air sniffing analyzers for Wi-Fi or Bluetooth.

- The analyzer should be able to synchronize the timeline of the Wi-Fi and Bluetooth packet streams.
- The test equipment should be able to display the Wi-Fi and Bluetooth packets in coexistence view that shows both the Wi-Fi packets synchronized with the Bluetooth packets as they occur in real-time. If the technology displays are not synchronized in time you will gain little if any information from the coexistence display.
- Wireless packets should contain information on protocol, profile, timestamp, power level, data, etc. The more information that you have about a packet the more likely you are to accurately describe the operating environment at that point in time.
- Wireless technology collisions should be obvious and identifiable in time. Wi-Fi packets that appear at the same time as Bluetooth packets are an indication of a collision.

- Additionally, each technology packet throughput should appear in the coexistence view and also synchronized to the timeline. Sudden drops in throughput can help identify when interference is present.
- Power levels or spectrum level displays will help identify potential interference sources. For example, if a strong Wi-Fi power level appears in synchronism with a Bluetooth throughput decrease, you would look for retransmitted packets and packets with errors to help identify interference issues.

Precise identification of coexistence issues will help the developer refine their coexistence algorithms, speeding their product to markets, and give the consumer with an error free wireless technology experience.

Author: John Trinkle

Published: July 2016