EZURiO

Wireless Connectivity out of the box

Bluetooth® and 802.11 coexistence

Despite sharing the same 2.4 GHz spectrum, it's possible for Bluetooth and 802.11 to be good neighbours, even if they're implemented within the same device.

This application note explains the problems of coexistence and shows how EZURiO's modules can be used within the same device.

Nick Hunn
CTO - Ezurio Ltd

EZURiO Ltd
Saturn House
Mercury Park
Wycombe Lane
Wooburn Green
Bucks HP10 0HH
United Kingdom

Tel: +44 1628 858 940
Email : info@ezurio.com
Web: www.ezurio.com

Bluetooth and 802.11 Co-existence

Both Bluetooth and 802.11 work in the same portion of radio spectrum at 2.4GHz. This means that in cases where both are operating at the same time and within range of each other, there is scope for interference between the two radios, which will result in a loss of performance for both systems. Given the success of both technologies, this is now an inevitable reality.

The effect of interference will depend on the relative location of the two transceivers, the frequency with which they transmit and also the type of data that is being transmitted. Bluetooth employs a frequency hopping scheme, where a burst of data is contained within a segment of spectrum 1MHz wide, which randomly changes to a different frequency 1,600 times every second. 802.11 transmitters do not hop, but transmit at a static frequency, using 22 MHz of spectrum. Both have mechanisms to deal with interference from another similar system, although in each case this results in steadily degraded performance. However, when they are mixed together, the opportunity for disruption increases.

The most common problem with mixing the two systems (or even having multiple asynchronous deployments of the same technology) is that of normal interference, where uncoordinated transmissions from multiple devices disrupt the reception of received packets at another device.

A more serious effect occurs when two transmitters are close together. In this case, the output power of one transmitter can overload the receiver of the adjacent device, resulting in a condition known as front-end overload. Depending on the design of the receiver, this can result in a sustained loss of receive capability that lasts past the removal of the interfering signal.

The real effect of interference also depends on the type of data being transmitted. Where both systems are transmitting data, the perceived effect of interference is normally minimal. Because data is not generally time critical, perturbations in the transmission of either device are hidden by the higher level applications and rarely noticed. Interference between multiple 802.11 access points that are located too close together is normally more of a problem than interference between 802.11 and Bluetooth.

The issue becomes more severe when BOTH systems are transmitting streaming media, such as voice or video, or time critical data. In these cases perceived interference becomes more obvious, increasing as the data transfer rate across each link increases. As the data rates exceed approximately half of the bandwidth of each technology the likelihood of noticeable problems become significant.

In all cases front end overload results in an even more serious incidence of noticeable degradation.

Mitigating Interference

Two different cases need to be considered in determining implementation schemes.

1. Both 802.11 and Bluetooth devices are co-located and can be physically connected to each other.

2. 802.11 and Bluetooth devices are within range of each other, but in separate, autonomous devices.

The second case is the more common. There is currently only one practical solution, but it is easy to implement, so will be considered first.

802.11 and Bluetooth interference in adjacent devices

In the most common case where devices are in the same general area, there is no ability to co-ordinate transmissions between them, so any attempt to reduce interference must rely on a local method of pre-empting it.

802.11 devices have no relevant interference mitigation techniques and rely on more thoughtful behaviour from other transmitters within the spectrum. Since version 1.2, Bluetooth devices have implemented a technique know as Adaptive Frequency Hopping (AFH), where each device regularly scans the spectrum looking for fixed sources of essentially static interference, such as an 802.11 transmitter. If they find portions of the spectrum are already being used, the Bluetooth device adapts its frequency hopping pattern, both for itself and the other Bluetooth device connected to it, to avoid these frequencies. It repeats this process regularly to keep up to date with the local interference. That's important as Bluetooth is most commonly used in mobile devices that will move through areas where different radio transmitters are present.

Although it helps to avoid interfering signals, this technique reduces the amount of spectrum that a Bluetooth device can utilise. Taken to the extreme, it would stop a Bluetooth device from transmitting on any channel. In practice a compromise is necessary and hence there is a lower limit on the number of channels to ensure that Bluetooth will continue to transmit reliably. FCC regulations also require that a Bluetooth device reassesses it hopping pattern at least every 30 seconds. EZURiO Bluetooth modules do this significantly faster, typically every four seconds.

802.11 and Bluetooth interference in adjacent devices

Having two radios within the same device is the worst possible case for interference as the transmitters are so close to each other. This increases the possibility of front end overload, which can have a major negative effect on throughput. To address this, a number of schemes have been developed to allow communication and arbitration between co-located devices to achieve the best utilisation of spectrum.

These schemes are in addition to AFH within the Bluetooth device, and rely on two techniques – Time Division Multiplexing and Channel Skipping.

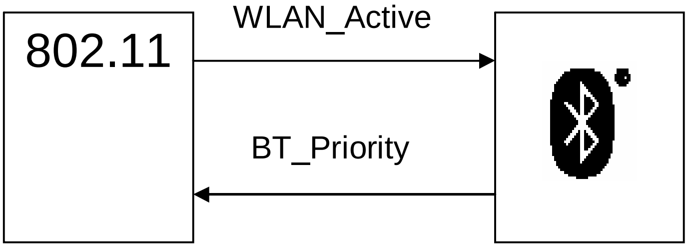
Channel Skipping is the simpler concept and is akin to AFH. It takes advantage of the fact that in a collocated environment the 802.11 and Bluetooth devices can be connected together. This provides a means for the 802.11 radio, which uses a static range of frequencies, to inform the Bluetooth baseband directly of these channels, so that the Bluetooth device can pre-emptively remove them from the range of frequencies it is hopping over. As the 802.11 device is static in terms of frequency usage, channel skipping can be implemented by the host processor determining the channels used by the 802.11 radio and communicating these to the Bluetooth device. If channel skipping is the only collocation strategy used it will sacrifice Bluetooth spectrum to the demands of 802.11. Note that AFH can still be deployed over the remaining spectrum.

An alternative approach is Time Division Multiplexing, which uses the communication available between devices to permit one radio to take precedence over the other. Initial, simple schemes sought to stop Bluetooth activity whenever an 802.11 baseband was active, by producing a WLAN_ACTIVE signal. As an 802.11 packet is much longer than a Bluetooth packet this could be disruptive for SCO communications. To address this, more sophisticated approaches have evolved, balancing the 802.11 activity demands by granting a BT_PRIORITY signal from the Bluetooth baseband to request control for high priority Bluetooth signals. Further refinements provide priority information as to whether an 802.11 transmission is imminent. If it is, then the Bluetooth transmission can be deferred, resulting in a best usage, non-contention formula.

One of the limitations with Time Division Multiplexing is that the host system is rarely fast enough to provide information from one device to another in real time. By the time either radio has communicated its immediate requirement up the stack, the information is out of date. To be effective the baseband controllers of both 802.11 and Bluetooth need to be able to talk directly to each other. This has resulted in the development of a number of hybrid schemes which provide direct communication between Bluetooth and 802.11.

Hybrid Schemes

Today, most approaches to co-location use hybrid schemes which employ a mixture of algorithms to implement a combination of TDM and Channel Skipping, along with the inherent AFH features of Bluetooth. These require a two or three wire connection between the 802.11 baseband and the Bluetooth baseband chips. They also require complementary algorithms within both devices. The most common implementations use a proprietary signalling scheme devised by Intel, known as WCS signalling, or a hybrid scheme supported by CSR.

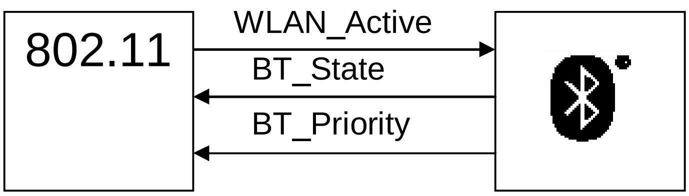


2-wire

In 2-wire schemes, only two signals are used to connect the Bluetooth and 802.11 sections. These typically convey the status of the wireless LAN transmissions to the Bluetooth device and the Bluetooth high priority transmissions to the 802.11 baseband.

An important refinement of the 2-wire scheme is Intel's WCS signalling algorithm, where the WLAN_Active signal also carries the wireless LAN channel information.

Three wire solutions typically add a BT_STATE signal to alert the 802.11 baseband to the presence of a Bluetooth transmission:



3-wire

In order for any of these schemes to operate, it requires the appropriate, complementary algorithms to be implemented and activated in both devices. Simply connecting up signal lines will not result in any co-location strategies being used.

EZURiO's Bluetooth and 802.11 modules provide support for all of the interference avoidance strategies mentioned above, with inbuilt algorithm support and a full range of co-existence signals available on the GPIO lines.

Because of the proprietary nature of these schemes, detailed implementation information is commercially confidential. For more information on implementing specific co-location strategies, please contact EZURiO.