Crowd control: short-range devices in the 2.4-GHz ISM band

Can we really expect all this diverse equipment to work as expected, or even work at all, when brought together in the modern home or an industrial environment?

By Dag Grini, Chipcon

The attractiveness of the unlicensed, 2.4-GHz ISM (industrial, scientific and medical) band (2400 to 2483.5 MHz) stems from the simple fact that it is virtually license-free all over the world. As a consequence, a global marketplace lies open for numerous vendors and products. A significant amount of the growth in 2.4-GHz devices is in entertainment, home/building automation, and personal communication.

The microwave oven has been part of the kitchen for years. Now, cellular phones, PDAs containing Bluetooth as well as IEEE 802.11b/g-enabled WLAN (wireless-LAN) access points, and network-interface cards providing PCs and laptops with access to the Internet have started invading the home. Consumer electronics, such as wireless game controllers and consoles and wireless audio and video systems, are also currently finding their way into the "digital home." The next big thing will likely be home control and building automation, with ZigBee solutions based on the IEEE 802.15.4 standard expected to soon dominate. Numerous other 2.4-GHz wireless applications—both standardized and nonstandardized, such as alarm systems, remote controls, toys, cordless phones, and computer-centric peripherals, such as mice, keyboards, and USB dongles—will add to the mix.

Whether all this diverse equipment will work as expected, or even work at all, when brought together in the modern home or in an industrial environment remains a topic of great discussion. For obvious reasons, coexistence in the 2.4-GHz band, particularly between Bluetooth and WiFi (WLAN) devices, has recently attracted quite a bit of attention.

Standardized and nonstandardized operation

Both the IEEE and independent organizations, such as the Bluetooth SIG (Special Interest Group), define within the 2.4-GHz ISM band several short-range-device radio standards. Some of the 2.4-GHz standards, typically WLAN standards, target data transfer using DSSS (direct sequence spread spectrum). Other standards, such as Bluetooth, which uses FHSS (frequency-hopping spread spectrum), fall into the WPAN (Wireless Personal Area Network) category.

ZigBee is a new global standard for wireless connectivity, focused on standardizing and enabling product interoperability within home control, building automation, and industrial control and monitoring. It is based on the robust radio (PHY) and MAC (medium access control) communication layers that the IEEE 802.15.4 standard defines. On top of this framework, ZigBee defines mesh, star, and cluster-tree network topologies with data-security features and interoperable application profiles. IEEE 802.15.4 and ZigBee have been defined for operation not only within the 2.4-GHz ISM band but also within the 868- and 915-MHz ISM bands targeting European and US markets, respectively. **Table 1** provides examples of frequently used or emerging 2.4-GHz standards.

In addition to systems and devices obeying the above standards, numerous applications use nonstandardized operational modes. Proprietary systems and protocols tailored for unlicensed 2.4-GHz operation—using, for example, a subset of functions defined within a standard—are common.

Regulations

Established regulations in different parts of the world govern the 2.4-GHz ISM band. The following overview is not a complete reference of the applicable worldwide regulations;

rather, it is limited to the United States, Japan, and most European countries. (Annex F of **Reference 1** provides a good overview of all regulations.) Before submitting a product to compliance testing, review the applicable national legislations in each of the locales where you will sell the product; some countries have national exceptions from, for instance, the applicable European standards. An approved compliance test house can often provide such information.

In the United States, the FCC (Federal Communications Commission) approves radio-frequency standards and regulates the usage of the 2.4-GHz ISM band under the 47th part of the Code of Federal Regulations (**Reference 2**). Sections 15.205, 15.209, 15.247, and 15.249 apply to 2.4-GHz short-range devices. Previously, FCC regulations called for spread-spectrum (DSSS or FHSS) systems. On May 30, 2002, the FCC replaced the former spread-spectrum requirement in 15.247 with a "digital modulation" requirement but continues to allow spread-spectrum systems.

In Japan, the ARIB (Association of Radio Industries and Businesses), an industry association acting on behalf of the Japanese government, develops standards covering regulatory mandates and government requirements facilitating efficient use of the radio spectrum. ARIB STD-T66 regulates the operation of the 2.4-GHz ISM band (**Reference 3**). The MPT (Ministry of Post and Telecommunications) is the approval authority.

The R&TTE (Radio & Telecommunications Terminal Equipment) Directive is the applicable directive for radio equipment within most European countries (**Reference 4**). Within this directive are requirements regarding EMC and effective use of the radio spectrum, electrical safety, and health. The ETSI (European Telecommunications Standards Institute) develops normative technical standards on behalf of the CEPT (European Conference of Postal and Telecommunications Administrations) for the membership countries. CEPT ERC Recommendation 70-03 on short-range devices is a good starting point for understanding European low-power-radio operation (**Reference 5**). Type approval testing for spread-spectrum, 2.4-GHz radio devices is normally performed according to EN 300 328-1 and EN 300 328-2 (**references 6** and **7**, respectively); generic unlicensed, 2.4-GHz short-range devices must comply with EN 300 440-1 and EN 300 440-2 (**references 8** and **9**, respectively).

Coexistence and operational alternatives

Due to the increasing popularity of the 2.4 GHz ISM band, the issue of coexistence has attracted quite a bit of attention, particularly in the industrial, home-control, and building-automation segments. The IEEE has invested much energy in analyzing and simulating various coexistence scenarios between IEEE 802.15.1 (Bluetooth)- and IEEE 802.11b-compliant systems, resulting in a recommended practice (**Reference 10**). This practice essentially defines the features, such as AFH (adaptive frequency hopping), that is implemented within the Bluetooth 1.2 specification. Because the 2.4-GHz ISM band is unlicensed, it is open to all kinds of standardized and nonstandardized applications, including TDMA (time-division multiple access) and FDMA (frequency-division multiple access) systems, wideband and narrowband systems, frequency-hopping and direct-sequence systems, and fixed-frequency and frequency-agile systems. However, all systems must comply with the applicable regulations. In general, however, an ISM band will contain various short-range devices using different frequency-selection methods when competing for airtime. A unifying approach, offering all these short-range devices a frequency-selection scheme based on a centralized control mechanism, is utopian.

The IEEE defines coexistence as "the ability of one system to perform a task in a given shared environment where other systems have an ability to perform their tasks and may or may not be using the same set of rules." In general, coexistence issues arise during simultaneous operation—for example, when a wireless device comes into proximity with other wireless devices using the same frequency band. You normally express a theoretical analysis of coexistence as a single number: the probability of collisions due to interference occurring. You express results obtained from practical testing as normalized data rate. Both parameters are examples of throughput. In the noncongested case, there are enough

frequencies and channels available for the operating devices; in the congested case, several users compete for simultaneous airtime.

Customers often ask chipmakers to explain the situation with coexistence and guarantee that their chips will continue to operate reliably under interference conditions. Responding to these customers is difficult, because coexistence depends on many parameters, including the distance between the interfering systems, the protocols used, the number of radios operating simultaneously, and the frequencies occupied. Other important parameters are the operating environment and each radio's transmit power, duty cycle, IP3 (third-order intercept point), and jamming resistance, which the receiver's in-band selectivity and blocking performance determine. In collocated (combo) devices, which may incorporate Bluetooth and IEEE 802.11b/g on the same board, distances between the incorporated chip sets and antennas are typically small. Coexistence-facilitating mechanisms, such as interantenna isolation achieved through orthogonal antennas and further improved RF front-end filtering will be necessary for simultaneous device operation. Some collocated devices operate autonomously, and others use a collaborative coexistence mechanism to minimize mutual interference. You optimize the overall performance through frequency-collision-avoidance techniques according to predefined rules. You normally implement the exchange of coordinating and prioritizing information between collocated wireless systems within a central controller.

Various operational alternatives and interference-reduction techniques for frequency-band sharing are available. **Table 2** summarizes the coexistence performance of these operational alternatives. Please also note that more systems are combining two or more techniques to obtain robust operation.

A fixed-frequency device operates only on a predefined frequency. Typical applications are first-generation wireless game controllers and low-cost wireless mice. Several game controllers also have physical switches enabling them to switch between typically two to four frequencies. Fixed-frequency solutions are generally quite vulnerable to interference. Normally, the user must detect the interference through reduced performance and manually switch frequency.

2.4-GHz operational alternatives

Fixed-channel operation is implemented in, for example, IEEE 802.11b, IEEE 802.11g, and IEEE 802.15.4/ZigBee applications, as well as a number of proprietary systems. Each channel in IEEE 802.11b occupies 22 MHz, and in IEEE 802.15.4, each channel occupies approximately 2 MHz. A coordinator device—for example, a WiFi access point or an IEEE 802.15.4 PAN coordinator node—can change the operating channel. DSSS systems such as these rely on a technique in which you obtain the spread signal by multiplying (XORing) a narrowband signal with a high-speed pseudorandom code sequence. The processing gain resulting from the spread-spectrum techniques in IEEE 802.11b will help reduce the impact of, for example, an IEEE 802.15.4 interferer that will look like a narrowband interferer to an IEEE 802.11b receiver. In the same fashion, relatively wideband interference, such as IEEE 802.11b would appear like white noise to an IEEE 802.15.4 receiver.

DSSS systems are generally robust against narrowband noise but less likely than FHSS systems to tolerate hostile RF environments with noise, interference, and channel collisions. Other drawbacks of DSSS systems are the relatively high DSP overhead as well as the requirement for the received signals from all subscribers of an access point to be nominally equal. The latter requirement is necessary to avoid a "near-far" problem, which requires you to prevent subscribers near the access point from drowning out signals from distant subscriber stations. Please note that all of the aforementioned IEEE defined standards also feature other interference reducing techniques.

LBT (Listen Before Talk, sometimes called Listen Before Transmit), systems employ CSMA (carrier sense multiple access). DSSS systems typically combine this feature with channelized operation to avoid interference. All of the aforementioned DSSS systems feature CCA (clear channel assessment) through CSMA/CA (carrier sense multiple access with collision avoidance). Before transmitting any information, the LBT device will determine

whether the channel is occupied by performing energy detection in the actual channel. If the channel is occupied or a collision occurs (no acknowledgement is received during an initiated transmission), the device backs off for a random time period before attempting once more. After a predefined time, or a predefined number of attempts, the device will normally switch frequency or channel. LBT improves coexistence by allowing transmission backoff if the channel is occupied by any device, regardless of the communication protocol.

Frequency hopping is normally based on a pseudorandom frequency-hop algorithm. Bluetooth devices are typical FHSS devices using a frequency-hopping protocol. FHSS systems are generally more robust against interference than DSSS systems. However, for large networks, the frequency channel synchronization between nodes makes it challenging to obtain low-power operation, and network association typically consumes more time than DSSS systems using LBT.

An AFH (adaptive frequency-hopping) system adds further refinement and intelligence to a frequency-hopping protocol. The best-known AFH system is probably Bluetooth 1.2, which uses a dynamic frequency-selection algorithm, omitting frequencies in which it detects interference (energy). Bluetooth 1.2 and other FHSS systems typically perform an RSSI (received signal strength indicator) scan to classify and dynamically select the optimum frequencies or channels according to certain criteria. However, a truly congested environment will reduce the throughput of an AFH system, because no single channel will be free of interference. The FCC requires you to use at least 15 nonoverlapping channels, and the maximum peak output power of the intentional radiator (if using less than 75 hop frequencies) may not exceed 0.125W (~21 dBm) (**Reference 2**).

A very slow frequency-hopping system transmitting at two or more frequencies or channels to avoid interference is known as a frequency-agile system rather than a frequency-hopping system. A device operating according to this scheme typically resides on a frequency or channel until the system detects interference, perhaps through a missing acknowledgement or energy detection. Alternatively, it can switch frequency or channel between each transmission. A manual switch-button game controller could be considered a special case of a frequency-agile system.

An AFA (adaptive frequency-agile) system further enhances the coexistence performance of devices already capable of frequency agility: The system performs a dynamic frequency, a timeslot selection, or both in response to an analysis of the prevailing environment at the time of use (**Reference 11**). Given available frequencies or channels, an AFA system can identify such frequencies or channels. In the congested case, where all frequencies or channels are occupied, a new AFA device trying to use the band will receive no service.

Combining adaptive frequency agility with LBT provides the best overall coexistence results (**Reference 11**). Rather than a sudden loss of service, as with the congested case using AFA, it provides a graceful degradation of the throughput.

IEEE 802.15.4 coexistence features

Annex E of **Reference 1** thoroughly describes the standard's coexistence-enhancing mechanisms, which develop a robust protocol for devices based on the IEEE 802.15.4 standard, such as soon-to-come ZigBee-compliant devices. As IEEE 802.15.4 and ZigBee solutions are seeing commercial deployment only just now, few real-world systematic test cases establishing the interference performance between ZigBee and, for example, WiFi and Bluetooth systems, have been published. Chipcon has performed several ad-hoc coexistence tests using its CC2420 chip with promising results. In one test, two CC2420DBs passed data back and forth, while an 18-dBm, frequency-hopping, 2.4-GHz transmitter-receiver pair using 15 channels operated approximately 1m away from both CC2420s. Neither system exhibited any performance degradation. Similarly, two CC2420DBs placed close to a laptop transferring a file across a 2.4-GHz IEEE 802.11b connection exhibited no performance drop. Most of the coexistence-enhancing features defined within IEEE 802.15.4 are described below.

Coexistence-enhancing features

IEEE 802.15.4-compliant devices provide the capability to perform CCA through the CSMA/CA mechanism. Three CCA methods exist: energy detection over a certain threshold, detection of a signal with IEEE 802.15.4 characteristics, and a combination of these methods. Chipcon's CC2420 supports all three CCA modes where indication is available on a pin.

IEEE 802.15.4/ZigBee-compliant devices use a modulation scheme in which each symbol is represented by one of 16 nearly orthogonal pseudorandom sequences. According to **Reference 1**, "This is a power-efficient modulation method that achieves low signal-to-noise ratio (SNR) and signal-to-interference ratio (SIR) requirements at the expense of a signal bandwidth that is significantly larger than the symbol rate." The ad-hoc tests performed using the CC2420 show the robustness of this modulation format.

Energy-detection measurements provide estimates of the received signal power within an IEEE 802.15.4 channel, and the LQI (Link Quality Indication) measures the received energy level, SNR, or both for each received packet. Combining energy-detection- and LQI-measurement information can reveal whether corrupt packets result from low signal strength or from high signal strength plus interference. CC2420 offers the opportunity to use the RSSI value directly to calculate the LQI value. With this method, a narrowband interferer inside the channel bandwidth increases the LQI value. However, it actually reduces the true link quality. CC2420 therefore also provides an alternative for LQI based on the average correlation value from the DSSS demodulator/despreader for each incoming packet, as well as the opportunity to combine the RSSI and average correlation value to generate the LQI value.

IEEE 802.15.4-compliant devices at 2.4 GHz are operating at a fixed data rate of 250 kbps. Normal applications for such devices, such as wireless sensor networks, are typically low-power and battery-operated with low to ultralow duty cycles. The low duty cycle implies that IEEE 802.15.4/ZigBee applications cause negligible interference to other systems.

Obtaining the required range using a lower output-power setting could reduce the interference originating from an IEEE 802.15.4-compliant radio, given that the transceiver has power control implemented for the transmitter part. In battery-operated applications, it is wise to implement an adaptive-power control scheme ensuring that the device uses no more transmit power than strictly necessary.

In the presence of three nonoverlapping IEEE 802.11b systems, there are four IEEE 802.15.4 channels that fall in the guard bands between (or above) the three IEEE 802.11b channels (**Figure 1**). Although the energy in this guard space is not zero, it is lower than the energy within the channels; operating an IEEE 802.15.4/ZigBee network on one of these channels will reduce mutual interference between systems.

Networking mechanisms and robustness of ZigBee

A number of companies are currently developing standardized ZigBee or proprietary 2.4-GHz mesh-networking systems for a variety of low-power applications. Above the PHY and MAC layers defined by IEEE 802.15.4, ZigBee defines reliable and secure mesh, star, and cluster-tree network topologies with interoperable application profiles (**Figure 2**). Mesh networks enable high reliability and scalability by providing more than one path through the network for any wireless link. Thus, such systems can typically establish alternative communication paths if you permanently or temporarily lose a node due to, for example, local interference. Because of the "self-healing" capabilities that such networks generally provide, the user will experience little, if any, performance degradation.

Blocking and in-band selectivity, which IEEE 802.15.4 terms adjacent and alternate channel rejection, significantly influence radio-interference resistance. All radios are not created equal in this respect, and these parameters are often key differentiators in terms of robustness. The linearity of different transceivers, which IP3 describes, is another important parameter to carefully consider before choosing a transceiver. When a generally nonlinear device, such as a transceiver, picks up two interfering signals, the output generally exhibits intermodulation components that when falling into the band of interest can corrupt the

desired signal.

Critical success factors

The success of any 2.4-GHz product operating in a congested environment will be judged by a number of factors, including communication reliability, system performance, and quality of service. Devices that fail to deliver the required performance in one or more of these areas are unlikely to succeed long-term. Furthermore, user experience is vital. Imagine the frustration of a 12-year-old who can't reach the next level in a favorite game because a WiFi system's interference is preventing the game controller from responding quickly. The child, who may not know the reason behind the lack of performance, might throw the game controller against the wall!

Because other devices will potentially operate simultaneously in the 2.4-GHz band, you need to address the issue of coexistence. Analyze the actual application and its importance, the coexistence performance requirements (such as jamming resistance and transmitted output power), as well as the operating environment. The latency of data packet delivery in an application transmitting temperature data to a collector unit once an hour would unlikely be considered critical, but the performance requirements of a 2.4-GHz real-time voice application is absolute. Radio development will certainly improve jamming resistance, but relying on future performance enhancements alone is not recommended.

Join the band

The virtually worldwide license-free, 2.4-GHz ISM band is already crowded, and the situation is expected to worsen as more applications are launched. Although few applications will need significant interference-performance improvement, new and more sophisticated coexistence algorithms will be necessary to maintain a sufficient performance level in systems depending on high to critical reliability. The best way to optimize crucial coexistence parameters in dense traffic is through techniques for actively avoiding interference. Factors expected to receive considerable emphasis in determining product success include communication reliability, system performance, quality of service, and end-user experience—especially for systems providing important infrastructure services of considerable value to the end user, such as a corporate WiFi network. Fortunately, regulations in the 2.4-GHz band prevent any device from using more than its fair share of the band.

References

1. IEEE Std. 802.15.4-2003 IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).

2. FCC Code of Federal Regulations 47, Part 15.

3. ARIB STD-T66, Second Generation Low Power Data Communication System/Wireless LAN System 1999.12.14 (H11.12.14) Version 1.0. Association of Radio Industries and Businesses (ARIB), Japan.

4. Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on Radio equipment and Telecommunications Terminal Equipment (R&TTE) and the mutual recognition of their conformity.

5. ERC Recommendation 70-03, Relating to the use of Short Range Devices (SRDs), October 2004.

6. ETSI EN 300 328-1, Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Part 1: Technical characteristics and test conditions.

7. ETSI EN 300 328-2, Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4

GHz ISM band and using spread spectrum modulation techniques; Part 2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.

8. ETSI EN 300 440 -1 V1.3.1 (2001-09) Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 1: Technical characteristics and test methods.

9. ETSI EN 300 440 -2 V1.1.1 (2001-09) Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 2: Harmonized EN under article 3.2 of the R&TTE Directive.

10. IEEE Standard 802.15.2 -2003 IEEE Recommended Practice for Information technology – Telecommunications and Information exchange between systems – Local and metropolitan area networks - Specific requirements - Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands.

11. Long, Nick, "Living with the enemy: Accommodating multiple users in the 838 to 870 band," Proceedings from LPRA Radio Solutions 2003, Sophia Antipolis, France.

Author's biography

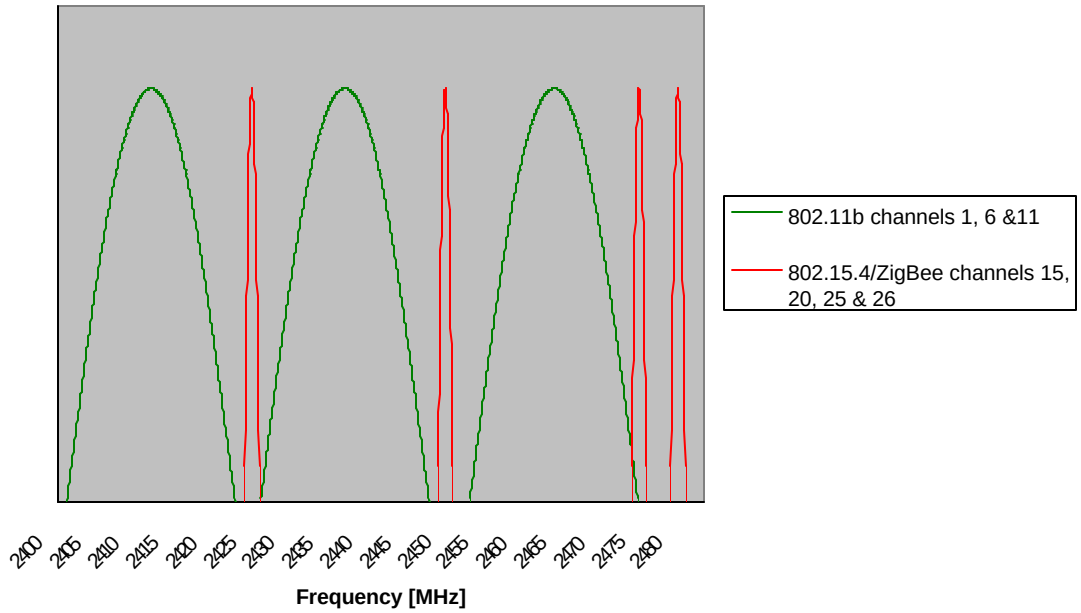
Dag Grini is director of technical support at Chipcon AS, where he is responsible for customer support, including reference designs, application examples, and documentation. He received his Master of Science degree from the Norwegian University of Science and Technology (formerly the Norwegian Institute of Technology), Norway in 1994.

Table 1—2.4-GHz standards

Standard	**WLAN/WPAN**	**Operational mode**	**Modulation method**	**Data rate**
IEEE 802.11b	WLAN	DSSS	DBPSK	1 Mbps
			DQPSK	2 Mbps
			CCK	5.5 Mbps
			CCK	11 Mbps
IEEE 802.11g	WLAN	DSSS	OFDM	54 Mbps
IEEE 802.15.1 (Bluetooth)	WPAN	FHSS	GFSK with BT=0.5	1 Mbps
IEEE 802.15.4 (ZigBee)	Low-rate WPAN	DSSS	O-QFSK[1] with half-sine chip shaping	250 kbps

Table 2—Coexistence performance of the 2.4-GHz operational alternatives in a nearly congested interference environment

Operational alternative	**Diversity scheme**	**Coexistence performance**
Fixed-frequency operation	FDMA/TDMA	Poor
Fixed-channel operation with Listen Before Talk	TDMA	Good
Frequency hopping	TDMA	Good
Adaptive frequency hopping	TDMA	Very good
Frequency agile operation	TDMA	Good
Adaptive frequency-agile operation	TDMA	Very good



Adaptive frequency-agile operation plus Listen Before Talk	TDMA	Very good

Figure 1— In the presence of three nonoverlapping IEEE 802.11b systems, there are four IEEE 802.15.4 channels that fall in the guard bands between (or above) the three IEEE 802.11b channels.

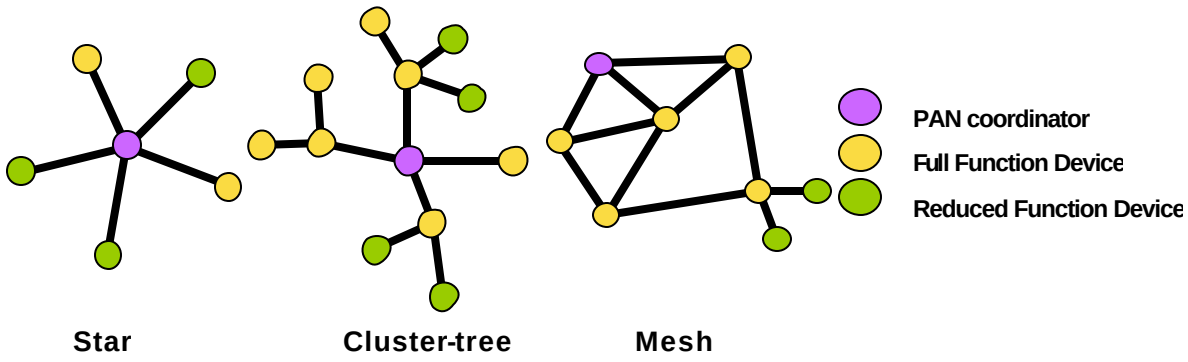


Figure 2— Above the PHY and MAC layers defined by IEEE 802.15.4, ZigBee defines reliable star, cluster-tree, and mesh network topologies.