Building low power into wireless sensor networks using ZigBee technology

By Jon Adams

A typical industrial network can have a large number of attached devices, presenting a challenge in power consumption. In this article, the benefits of ZigBee technology for industrial networks are discussed along with how to address the power challenge. Particular focus is given to how to get the most life out of battery powered ZigBee-enabled devices.

The industrial, commercial, and residential sensor communities have wanted low power, cost-effective wireless sensors ever since sensor technology was born. The ability to collect information in a simple yet robust fashion, while avoiding the high cost and reliability issues that the traditional backhaul or homerun wiring creates, has the potential to completely change the metrics against which the cost of data collection is measured. With the recent release of the ZigBee specification to the public, it is now practical to build and deploy wireless sensing devices that are at once capable of operational lifetimes measurable in months to years to decades from the batteries that power them as well as meeting the cost, security, and reliability requirements that the network developer expects.

ZigBee technology and other wireless standards

There is a wide, nearly unmanageable, range of choice when it comes to wireless technologies available for deployment of wireless sensing systems. There are both licensed and license-exempt technologies, standards-based and proprietary, on the market, all with their own potentials for addressing a developer's product problem. Figure 1 shows a 5 order-of-magnitude data rate range and a variety of wireless technologies developed to address specific market needs.

The ZigBee Alliance, an open industry group, identified a number of application spaces, including industrial control, building automation, consumer electronics, personal health care, PC and peripherals, and residential/light commercial control as targets for ZigBee networking technology, which was recently released to the public. ZigBee technology takes advantage of the robust and reliable IEEE 802.15.4 low-rate wireless standard, and adds to this mesh networking, sophisticated security features, interoperability, and end-product certification. The combination of the IEEE standard bound with the ZigBee networking approach makes a significant paradigm shift in standardizing wireless sensor and control communications. Within the markets defined, the Alliance chose to concentrate initially on residential/light commercial lighting control and HVAC, and industrial monitoring.

A custom-designed proprietary wireless system might at first seem to be the best approach to solving a wireless developer's dilemma. With intimate knowledge of the sensor environment and its needs, a custom system might be the optimal approach from a communications performance point of view. With a more holistic view, the developer might discover that the incremental value that the customized wireless system provides may be offset unfavorably by cost, added project complexity, radio testing and certification, and interoperability challenges.

A standards-based approach can ensure interoperability between products, which can be very valuable in a sensor data mining application as it can broaden the number of sensors that are available to provide data. From a customer's point of view, this can mean OEM independence, which can often make investment in a technology more palatable to the customer since they see that they have multiple, competing sources for the technology, providing them price, feature, and service competition. With standardized products available from a multiplicity of OEMs, increased product innovation is important for the vendors to maintain differentiation and value in the eyes of their customers. From the OEM point of view, standards-

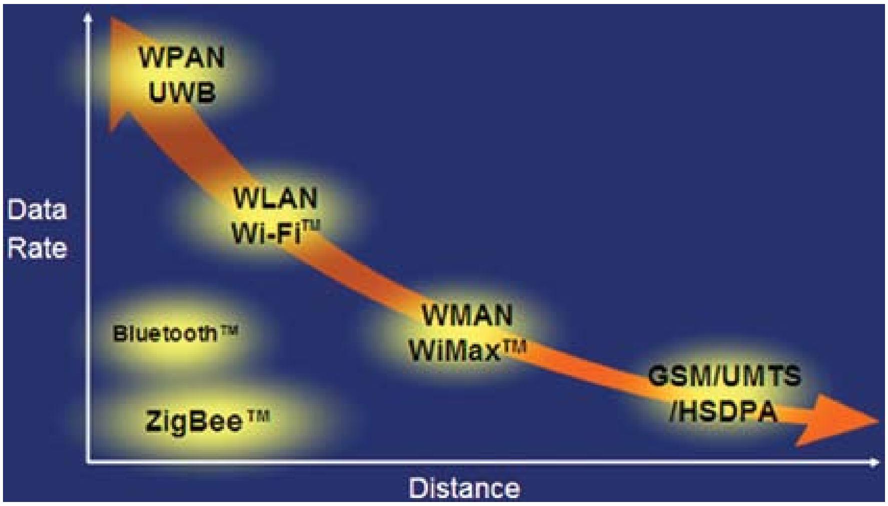

Figure 1

based approaches allow them source independence and competition in pricing and availability, and distance them from radio function and interoperability issues since these items are addressed by the silicon vendor. In the case of ZigBee technology, there are already multiple silicon platform vendors out there with highly cost-optimized solutions, and the natural cost reduction through competition and volume production allows an OEM to benefit from the volume market generated by their competitors.

Picking the right wireless depends on the sensor

It's apparent that depending on the needs of a sensor network, any of these wireless methods (as well as other, less standardized ones) might fit the bill. Designers are interested in wireless sensors that are not just low power, but more importantly, energy efficient, allowing them to operate on battery for months to years to decades or potentially through energy scavenging techniques.

There are a few other factors that sometimes need to be considered when defining the right kind of wireless for a sensor. Number 1 is probably data volume per unit time. Consider an image sensor that captures one compressed 100 Kb image every hour, and that frame is required to be available at a remote point within one minute after capture. This means that 100 Kb of information needs to be transferred from the sensor to a network within 60 seconds, about 1.7 Kbps. Add protocol overhead, other network usage, and the occasional retry and it sets the requirement for the overall network at probably something on the order of 3-5 Kbps. Not a tremendous data volume for most wireless systems. However, if that same sensor is capturing 30 frames per second continuously, that's 3,000 Kbps of raw data, which is way out of the class of many low-rate protocols.

Some sensors are extremely power efficient, where the sensor function itself uses a very small amount of power (think of a simple photodetector like a phototransistor or magnetic reed switch security sensor), or is power-managed in such a way that even though the sensor during operation consumes significant power that the sensor function is shut down and cycled on an as-needed basis.

Then again, there are sensors and more likely, control devices, that consume significant amounts of power at all times or are permanently tied to the mains. These considerations may prove important in the choice of wireless technology to use.

IEEE 802.15.4 primer

IEEE 802.15.4, a simple packet data protocol, is now available as silicon-based products from a number of semiconductor companies, with more vendors on the horizon every day. The quantity of platforms now available means that the "cost-effective" mantra has become a reality, and the breadth of OEMs taking advantage of this straightforward radio technology in a tremendous variety of applications presages a long and successful life for products based on the standard. IEEE 802.15.4 was designed for sensor/control systems with specification of the RF channels, physical layer characteristics and behavior, and a simple set of MAC primitives when compared to either Bluetooth or Wi-Fi technology. A fundamental advantage of using a standards-based technology is that it is continuously vetted for quality and robustness, with the members of the IEEE focused on improving the technology and reducing the overall complexity and cost.

In the 2400 MHz band, the standard specifies 16 channels, each 5 MHz wide. It uses two forms of Phase-Shift Key (PSK) modulation depending on the frequency band – PSK has been used by NASA for deep-space communications for decades because of its ability to provide robust performance even with very low Signal-to-Noise Ratios (SNR). In the past, PSK was infrequently used in simple systems due to complexity and cost, but the modern silicon systems have resolved this to provide easy access to the approach. Figure 2 shows the difference in performance between the ZigBee wireless technology, which is based on IEEE 802.15.4, and other wireless protocols.

Basic RF channel access is via Carrier Sense Multiple Access including Collision Avoidance (CSMA-CA), which means "make sure the channel's clear before you talk." By doing this simple step, collisions between individual transmitters can be reduced and the overall channel capacity improves. There's also an optional TDMA operation for completely battery-operated networks, which takes advantage of regular timing beacons between nodes to align communications opportunities. The physical layer employs four simple packet types:

- Data
- Acknowledgement
- Beacon
- MAC Command

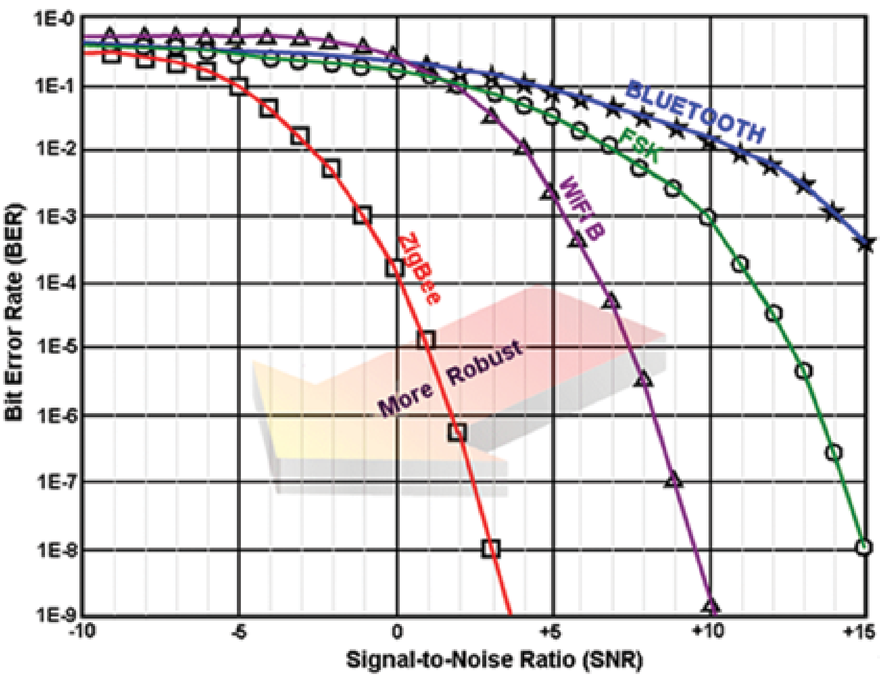

Figure 2

It supports communications in multiple regionally unlicensed frequency bands, of which only the 2400-2483 MHz band is available worldwide. Configured for maximum battery life, a device using IEEE 802.15.4 has the potential to last as long as the shelf life of the batteries powering it.

In the MAC layer, the standard provides a set of primitives that give strong flexibility to the network developer, but it does not explicitly specify a network topology. The standard uses IEEE 64-bit addresses so that each radio is uniquely identified, and to reduce overhead when a device joins a network, this address is replaced with a locally generated 16-bit address, which provides the capability for that local network to have more than 65,000 active nodes. AES 128-bit encryption is a built-in feature, absolutely important in a wireless system. The Acknowledgement packet ensures that when device A sends a message to device B, device A will keep trying until the data is transferred successfully.

Real platforms and ZigBee wireless technology

Figure 3 shows a next-generation IEEE 802.15.4 silicon platform, this one from Freescale Semiconductor. A single-package system, the MC13213 (due later this year) contains all the required functionality to take full advantage of ZigBee or 802.15.4 technology. On the left side of the block diagram are the 2.4 GHz radio circuits, while the right side is the 8-bit MCU as well as various peripheral devices that are available for application development.

Within the transceiver are all the necessary mechanisms to manage the RF channel as well as the protocol's management of packets. This means that the MCU doesn't have to deal with RF channel timing issues at the symbol or bit level, and is free to sleep or do other work while messages are being received or transmitted. In addition, the transceiver contains timers and interrupt inputs that can further offload other protocol chores from the MCU. The MCU contains functions that a sensor or control device needs, including ADCs, timers and I/O bits, and performs the high-level management of the RF data modem as well as hosting the sensor/control application. Because of sophisticated power management

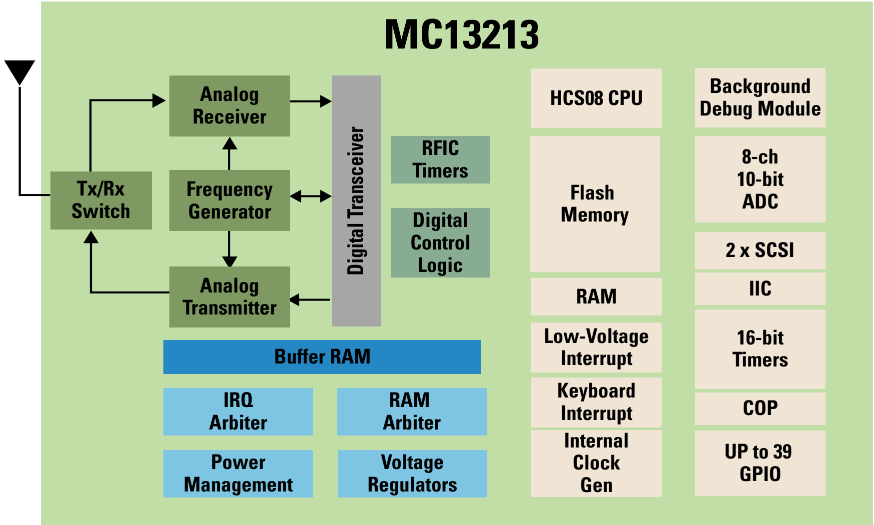

Figure 3

features built in to both devices, there are a number of power-down states available that allow the application developer to trade functionality, latency, and average power consumption.

So where is the ZigBee technology? Remember that ZigBee takes advantage of the IEEE standard's functionality and adds network function, security management, and application profiles. ZigBee in effect sits atop the IEEE protocol, managing it as well as adding an applications interface to which the developer writes their end application. Figure 4 shows the conceptual diagram of how ZigBee and IEEE technology complement one another.

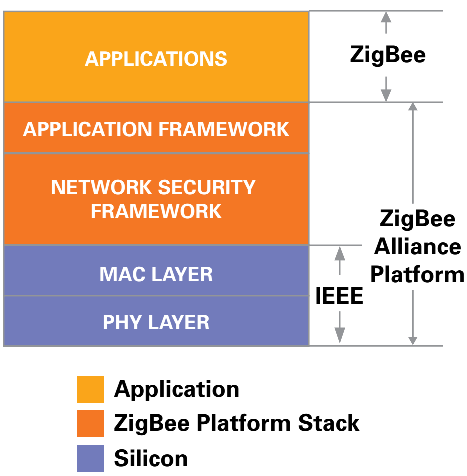

Figure 4

A sensor/control network must have good reliability, and that's where ZigBee mesh networking adds to the equation. ZigBee networks contain three kinds of networked device: the Coordinator, the Router, and the End Device. Both Coordinators and Routers establish and maintain routing tables defining network connectivity; in addition, the Coordinator has the special role of establishing the base network topology through assignment of the 16-bit network-specific addresses. End devices do not handle traffic other than their own. In most ZigBee networks the Routers and Coordinator are contained within products that are connected to the mains – devices like lighting load controllers, HVAC pumps and air handlers, smoke alarms and the like, as typical sensor networks ultimately interface to control devices. This allows the End Devices to spend most of their life asleep, waiting for user input or preprogrammed action like temperature, humidity, or occupancy measurement. It's straightforward to design devices that minimize their average power consumption while remaining "connected" to the network.

Figure 5 is a network diagram that shows the initial *tree routes* (red), established strictly due to the assigned address scheme, are quickly augmented by mesh routes (blue) between the routing nodes. These added routes mean that as propagation changes in the network due to events (doors open, furniture moved, people walk), or interference occurs (bursts from other radio systems, microwave ovens), there's a secondary path to move the data.

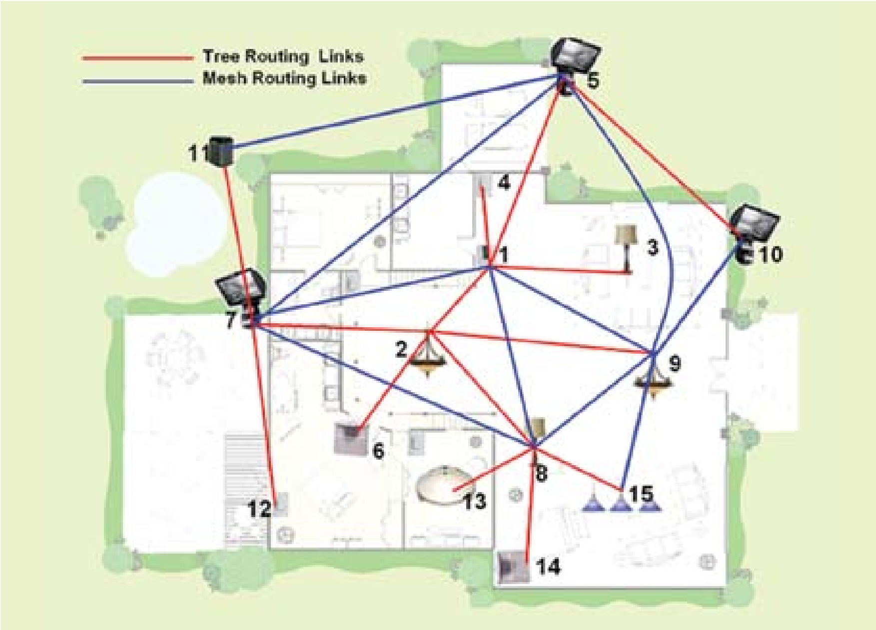

Figure 5

Controlling average power consumption is the key

For a simple security sensor as shown in the schematic of Figure 6, the average power consumption can be made very low to allow exceedingly long battery life, if the situation calls for it. In addition to the MCU and the RF data modem, there's a crystal for the RF oscillator and about 10 capacitors and resistors needed to finish out the basic circuit. RF design requirements are very minimal, as most of the complexity is contained completely within the transceiver, removing the need for the designer to be an RF expert. What's not shown in the schematic is whatever circuitry that the sensor might need, but in this example, the sensor is a simple magnetic door switch.

Now that the sensor has been connected and batteries installed, what kind of functionality does this device have and how does it interact with the sensor and the network? Figure 7 is a ladder timing diagram that shows how an End Device communicates with the network, allowing the device to quickly wake up to an event, make its observation, move the data into the network, receive a network acknowledgement, then go back to sleep as necessary. The steps in the process are specific to the IEEE 802.15.4 protocol requirements; there may be sensor processes that are not reflected here as every sensor is different. However, as long, as the base timing rules are followed, it's practical to keep the transceiver powered down until necessary, or to shut off the MCU while the transceiver is interacting with the network. The first network message time, 650 µs, represents a message with 5 or 6 bytes of data payload, as does the third network message. This time period will vary depending on the need to transfer data, but for most simple sensors transferring battery voltage and sensor state (on or off for a switch, temperature or otherwise) fits easily into this payload.

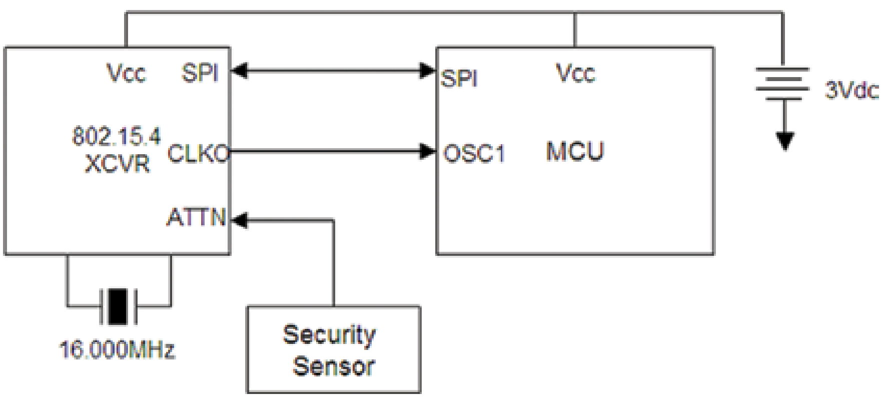

Figure 6

Alkaline cells are commonly advertised with a seven-year shelf life nowadays – wouldn't it be nice if the product came with a pair of batteries already installed and good for more than half a decade? The sensor that Freescale has designed using the IEEE 802.15.4 protocol can hit the kind of average power consumptions that make this practical.

All batteries have a *self-discharge* characteristic. This is due to internal finite high resistance paths between the battery anode and cathode that causes the cell to very gradually discharge. For a typical alkaline AA cell, that self-discharge current is between 10 and 20µA, meaning that every three weeks or so of shelf time the cell loses approximately 0.05 percent of its total capacity. Thus, the battery will lose about 50 percent of its capacity in seven years even if it never leaves the original blister pack. The goal for a long-battery-life sensor is to have an average current no more than 10 to 20 percent of the self-discharge rate.

Figure 8 shows the sensor's battery life when powered from those two AA alkaline cells. For a typical security system, it's good to know that the sensor is working and has not been tampered with or removed – this sensor is probably expected to report in on a regular basis to the network, not just when an event occurs tripping the sensor's magnetic switch. However, this requires the sensor to go through the above process on a regular basis; turning on a radio transmitter and receiver pulls a substantial amount of power over a very short time, but it can add up. The chart shows the *check-in interval* versus the expected battery life. For a check-in interval 18 seconds or longer, the average current is low enough that the sensor can outlast the batteries' shelf life. Since many security systems expect a report interval between 15 seconds and 10 minutes, this design greatly exceeds the typical sensor requirement. It's even practical to consider resizing the batteries to AAA and saving a little volume and mass, where the lifetime will still be longer than the user's memory of when the batteries were fresh.

Low power, efficient radio technology that is represented by the IEEE standard and ZigBee networking technology allow for an entirely new class of sensors where only simple measurement is necessary, but until now, there was no cost-effective wireless method to move even that simple data with reliability and the knowledge that the information will get to the network due to the persistence of the sensor itself. With these powerful tools, it's practical now to develop entire sensor systems that can last for a very long time on batteries while always providing the reliability that the user and developer have come to expect from wired sensor systems.

__Jon Adams__ is currently Director of Radio Technology for the Wireless Mobile Systems Group, Freescale Semiconductor. Jon has more than 20 years of experience in the high technology industry. His current focus is the chipset/platform for a new IEEE protocol called 802.15.4, and the network layer atop that standard called ZigBee. Jon is also an expert on wireless communication technologies such as Ultra Wideband and Bluetooth, and has spoken frequently on both. Prior to Freescale, Jon spent 17 years as a rocket scientist and was part of the team involved with developing and deploying the Mars Network. During this time, Jon received several awards including the NASA Achievement Award (for years 1986, 1992, and 2000) and the JPL Award for Excellence.

To learn more, contact Jon at:
Freescale Semiconductor
2100 E. Elliot Rd
Tempe, AZ 85284
Tel: 480-413-3439
E-mail: jta@freescale.com
Website: www.freescale.com

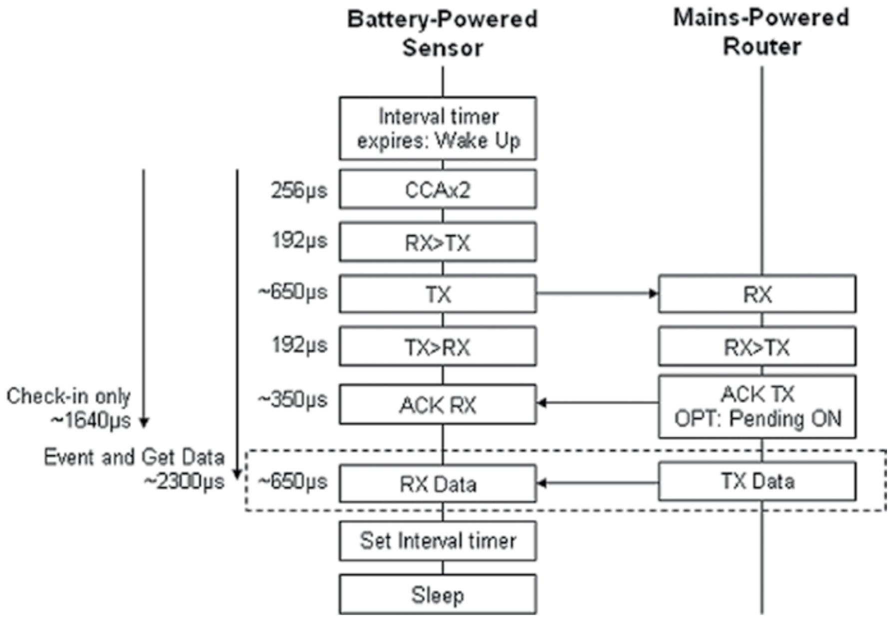

Figure 7

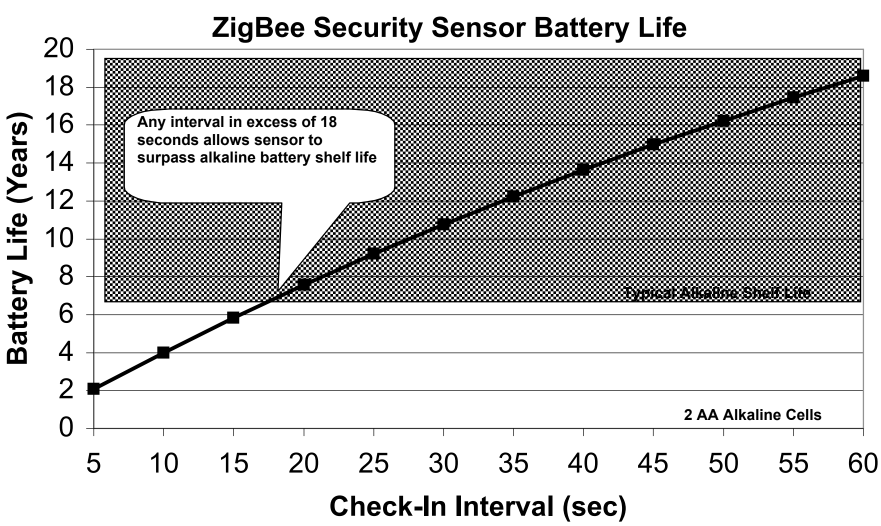

Figure 8