Understanding the ZigBee Stack and Application Profiles

Tim Gillman and Drew Gislason

There are many emerging wireless standards. Some seem to overlap in the space that they occupy in the market. ZigBee fulfills a unique space in that it is short range (10-70 meters) and is designed specifically for low data rates. This design enables ZigBee to have extremely long battery life for “sleepy” end devices and extremely robust networks that can reliably operate for years.

Sensor control networks have unique requirements. The networks must be able to form by themselves, scale to large sizes and operate for years without manual intervention. As many devices must continue to operate without the benefit of mains power, extremely long battery life (years on AA cell) is also required. If these devices are to become as ubiquitous and helpful as we would like, they need low infrastructure cost (low device & setup costs) as well as low complexity and small size. Unlike wireless networks for downloading movies and music via the internet, sensor control networks have low device data rate and quality of service needs. Generally, they need to take readings such as time, temperature or the state of a device and send it within a reasonable time period. If certain parameters are reached they can trigger other devices to fulfill their mission. If the alert is sent within a couple of seconds it is usually sufficient.

The addition of standardized protocols allows multiple vendors’ products to interoperate. This frees the end customer from relying on a single vendor, which may go out of business or simply lack the capacity to release the variety of products one could expect with a common standard. As many participants are involved in producing the standard, the combined experience and reduced individual investment raises the bar while freeing time for greater innovation and product differentiation. Of course it takes longer, with the meetings, approval levels and coordination, but the product is inevitably superior. Within the ZigBee Alliance an ecosystem has developed, so that member companies can focus on what they do best, while developers are able to get what they need.

The ZigBee Alliance is a growing community of around 200 companies. It includes major names in the semiconductor, software developer, end product, manufacturer and service provider industries including major telecom carriers. The ZigBee Alliance has made its specification publicly available, including ZigBee 2006, released at the end of that year. There have been more than 38,000 downloads to date. There are more than 30 compliant platforms. While there are some well known companies that have invested in ZigBee, there are no dominating elements or companies.

In addition to formulating the specification and promoting the standard, the ZigBee Alliance also governs the certification process. The purpose is to protect the ZigBee name and assure that the proper levels of interoperability are met.

There are two levels of ZigBee certification (figure 1).The first level of certification is the Compliant Platform. This is the combination of a transceiver, microcontroller and ZigBee

networking stack. The first products from multiple vendors deemed to have past all of the tests are considered “golden units”, used in the testing of all subsequent units. The compliant Platform certification ensures all parts of the stack other than the application are compliant with the ZigBee Standard.
In this way we get network interoperability but it does not imply interoperability at the application layer. The devices can form networks, route messages and prevent intrusion of devices into the network that are not intended to be part of it.

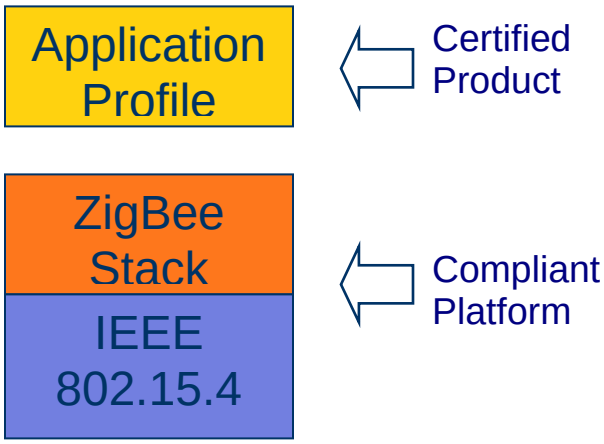

Figure 1 Two levels of certification

ZigBee Certified Products must be built on ZigBee Compliant Platforms. The ZigBee certified products are finished end devices certified on their application profile. Application profiles define what messages are sent over the air for a given application. Devices with the same application profiles interoperate end to end. For example, within the Home Automation Profile, a light switch from one vendor can turn on or off a light from another vendor. Taking it a step further, a smoke alarm in the basement of a home can set off the other smoke alarms in the rest of the house and turn on the lights in the bedrooms and hallways. This is not only safer for the family but may reduce the amount of damage that occurs. The products can work together even though they come from multiple vendors.

ZigBee Public Profiles guarantee interoperability among products all running the same public application profile. Product vendors may add additional features to the public profiles to make their products unique and create greater value for end users. All certified products that are using ZigBee Public Profiles can use ZigBee language and logos on their product.

ZigBee publishes a set of public profiles, but vendors may create manufacturer specific profiles as well. These allow a vendor to build specialized products with a ZigBee Compliant Platform. The certification testing for manufacturer specific profiles ensures the product does not harm other ZigBee networks only. These applications are not intended to interoperate at the application layer among multiple vendors’ products as with the ZigBee Public Profiles mentioned above. Of course, the manufacturer may open their

specific profile to a partner company and their combined products may be capable of interoperability at the application level. This level of certification does allow product vendors to use ZigBee language and logos on their products as well. Companies electing to choose the manufacturer specific profile path may be laying the foundation for a public profile at a later time. They may choose to open the profile to others. A minimum of three different companies are required to produce products meeting the published standard in order for the profile to become adopted as public.

Devices built on ZigBee interoperate on different levels. There is a wide spectrum of interoperability choices. It's a designer choice as to which level of vendor interoperability to support.

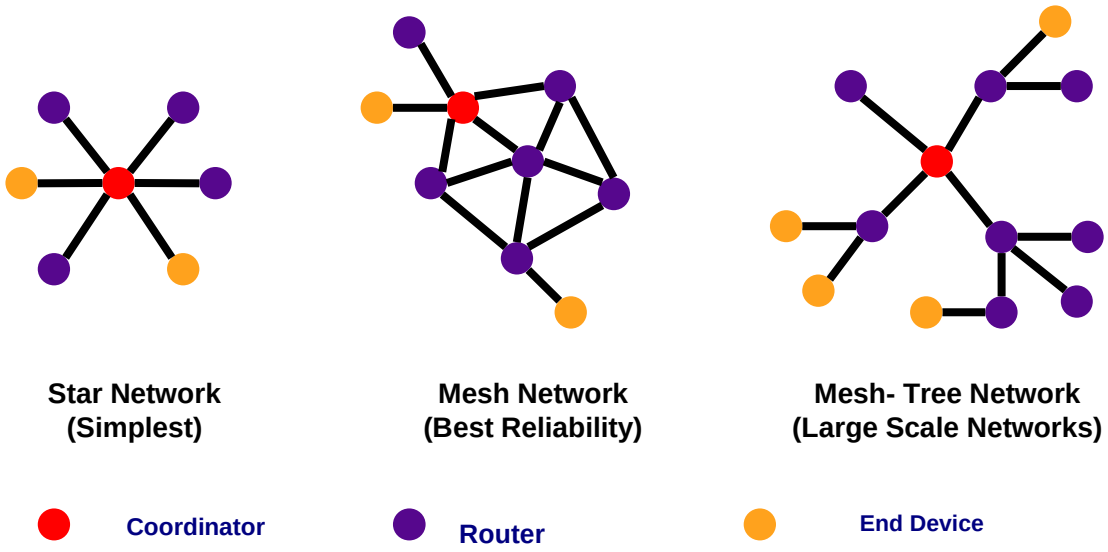

Figure 2 The ZigBee protocol has three topologies

The ZigBee protocol includes three different network topologies (figure 2). In each there is one and only one coordinator. A star network is the simplest. All messages are routed through the coordinator, similar to a network hub.

The mesh network uses a modified version of Ad hoc On Demand Vector routing (AODV). Mesh networks are self forming and self healing. Therefore they have the best reliability. As the coordinator is only needed to start the network, there is no single point of failure. Adding more transceivers or "nodes" to form a denser network, increases its reliability.

A mesh-tree network uses an algorithm called C-Skip to determine the layout of nodes depending on whether they are coordinator, routers or end devices. Every router knows whether a device is one of its children and can use a formula to determine which way to pass a message when it is received. A pure tree network is inherently unreliable as links

are inevitably broken over time. Adding mesh capability allows for self healing to repair broken links.
ZigBee is already being implemented in a wide array of manufacturer specific application profiles. There are also seven subgroups currently working on public profiles within ZigBee. Several are complete or nearly complete and some are just getting started. Here are a few more interesting areas in which ZigBee solutions are being implemented.

Asset Management in Shipping Containers

Homeland Security in the U.S.A. has identified a weakness in our defenses as only about 5% of the shipping containers reaching U.S. ports are able to be searched. In many ports shipping containers can take weeks clearing customs. This means that billions of dollars of inventory and assets are tied up in the process. The U.S. government is instituting a fast track system for containers. At least one company is planning to use ZigBee to send an alert if a container is opened in transit. Within each container, sensors can be added to detect restricted substances, radiation or the presence of humans. These sensors form a mesh network. The multiple containers in a ship can also form a mesh to report sensor data. Mains powered routers are run around the perimeter of the ship. The ship includes a gateway to satellite and ship-to-shore communications. Because manifest data and sensor data are known before ship docks at port, containers can be processed faster.

Sensor data can be recorded throughout a voyage and report excessively rough handling, or whether temperatures have gone outside of specified parameters. The recipient can be alerted to possible problems with the cargo even before it is unloaded.

In-Home Patient Monitoring

Patients can receive better care at a reduced cost with more freedom and comfort by using sensor networks in lieu of hospital or nursing home care. Patients can remain in their own home where they are most comfortable. Vital statistics can be monitored and uploaded to medical staff via the internet. Doctors can adjust medication levels or ask that a patient come in for further study if vital signs fall outside of the desired parameters.

With an aging population in many countries, dementia can strike family members quickly. Sensors can allow passive monitoring of elderly family members. For example a motion detector can be placed in a light switch near the door of a bedroom. If an elderly person does not get out of bed by a predetermined time an alert can be sent to a relative or other person to check and be sure they are all right.

The same device might turn on lights when the elderly person gets out of bed. Other sensors may send an alert to the person if the stove or other appliance is left on. A wireless panic button can be carried for falls or other problems. The ZigBee network extends the range to the yard or garden.

These same networks can be used in hospital or nursing home care. The motion detectors can record when a patient last got out of bed or in the case of patients with dementia, that

they are up and about and even send an alert to an attendant when the patient is approaching an exit. Patients are allowed greater movement and this can reduce the use of heavy medication to keep patients from leaving their beds (an all too common practice in many institutions). Because the staff can receive notification quickly if they are needed, rather than having enough staff to monitor the patients, the staff to patient ratio can be reduced.

Commercial Lighting Control

Wireless lighting control is an important use of ZigBee. With both economic and social pressures to reduce energy consumption, lighting can be more intelligent without high costs. Dimmable intelligent ballasts are used in the lighting. Light switches/sensors can be located anywhere saving on the initial cost of copper wire installation. Lights can be turned off during evening and weekend hours in businesses if not in use. The network can tie together lights, switches and blind control to make better use of natural light and reduce the lighting closest to the windows producing quantifiable energy savings. Another feature is customizable lighting schemes. In this way you can set the lighting in the way that you want. For instance in a hotel ballroom, the lighting may be set to minimal levels around the perimeter when a speaker is up on a stage and off everywhere else. It may be set to mid levels for a party or evening event. A daytime luncheon may require full lighting. Each of these modes can be set up in advance and selected easily. You may want to inactivate a switch for a predetermined time period to prevent guests from playing with the lighting. The same ballroom can have the lights and switches sub-divided to fit the subdivisions created by the partitions as it is broken up into smaller spaces and then controlled for the whole ballroom by a single switch when the partitions are removed. Lighting networks can be integrated with and/or be used by other building control solutions such as BACnet, or DALI.

HVAC Energy Management in Hotels

Hotel energy management can save each location hundreds of thousands of dollars per year. Guests often turn air conditioning levels on high before leaving their rooms for the day, so that when they return hours later the room will be properly chilled. Door sensors combined with motion detectors can tell when a guest has left a room. If there is no movement within 20 minutes of a door opening, the air conditioning can be gradually reduced to an economical temperature. When the door is opened again and movement is detected in the room the air conditioning is returned to initial settings. If a room is vacant, the temperature control can be reduced to even lower outputs. When the room is rented, the temperature can be automatically activated before the guest arrives. If the guest is a frequent guest, past comfort levels can be tracked and set accordingly. The wireless aspects make it easy to retrofit. Battery operated thermostats, occupancy detectors, and humidistats can be placed for convenience. The same system can of course turn off lights and the entertainment system, restoring them to previous settings when the door is opened.

Advanced Metering Platform with ZigBee

Power plants tend to produce a constant amount of electricity. However, energy usage has peaks and valleys. For all practical purposes, the electricity can not be stored for matching these peaks and valleys. Advanced metering initiatives are a rapid method to help manage global electric generation shortages and meet existing and pending legislation for energy control. The electrical company can send a message to the power meter which networks with other ZigBee devices in the home for load control, such as heating, air conditioning, lighting, dishwashers, washing machines and dryers. These can be turned off or reduced during peak demand, and turned back on when demand drops. Customers who have agreed in advance to participate in load shedding programs are eligible for reduced energy rates.

ZigBee Networking Stack

Multiple vendors provide ZigBee stacks and they are tested for interoperability only through the frames coming out of the radios. They are checked for conformance to the specification and to application profiles, but it is important to note that there is no common C API among stack vendors. Therefore, it is not as easy as cross compiling if you want to move from one vendor's stack or platform to another.

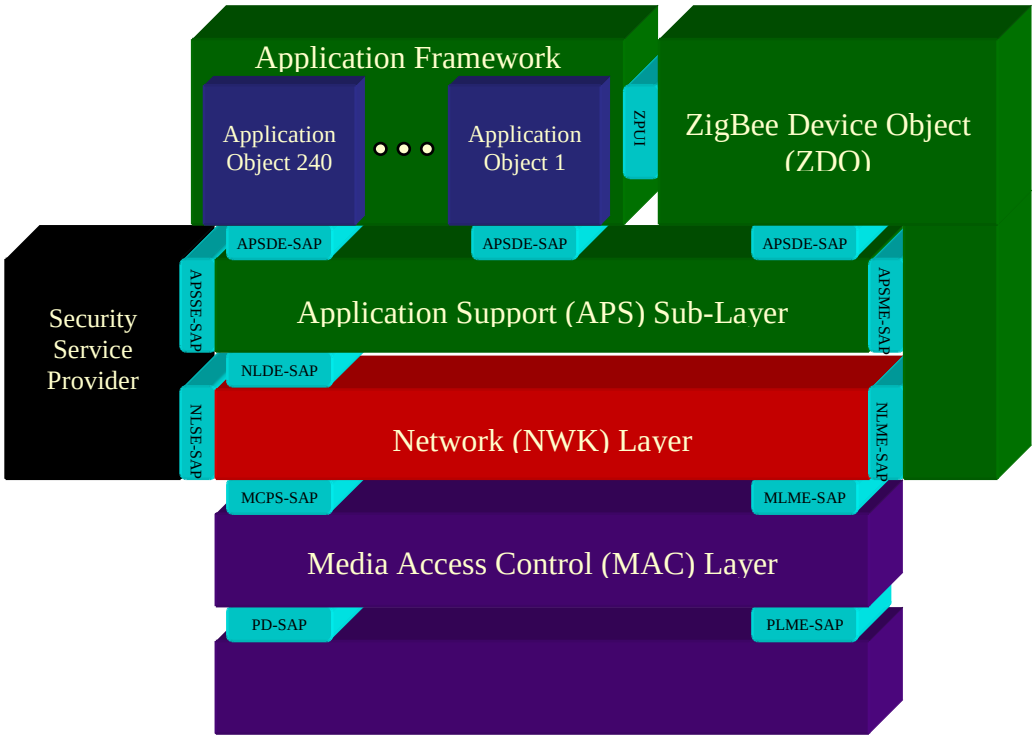

Figure 3 ZigBee Stack Architecture

ZigBee Networking Stack

Vendor devices may implement multiple profiles on a single device (figure 3). The additional application profiles exist on different endpoints within the device. This allows the creation of vendor specific extensions on ZigBee public profiles. The ZigBee Device Object (ZDO) resides on endpoint 0. Endpoints 1-240 are for applications. Endpoints 241-254 are reserved and endpoint 255 is reserved for broadcasting to all endpoints.

The ZigBee specification is designed to support large networks with up to 65,536 network nodes. Although currently there are no ZigBee stack implementations that large, it is important for standards to be forward thinking and not become the limiting factor to new technologies. A typical network would be much smaller than this as the traffic could overwhelm the network if each node is frequently passing messages across multi-hop paths. Some applications such as lights and mains powered switches may need to pass only a few messages per day. In these situations the network could be quite large (in the thousands) without overwhelming the network. Additionally, ZigBee allows network bridges to connect sections into one network. As the sections may be physically far apart, the network can tolerate more traffic without being overwhelmed. Mains powered devices typically are routers and quiet until asked to perform a task, while battery powered end devices are more "chatty" as they need to wakeup and check for messages on a periodic basis.

There are 27 channels over 2 bands. In the sub GHz range, there is a single channel (0) in Europe at 868.3 MHz, and 10 channels (1-10) in the 902-928 MHz range in the Americas. Worldwide there are 16 channels (11-26) in the 2405 to 2480 MHz range. All are in the unlicensed ISM bands.

The 2.4GHz range has a raw data rate of 250Kbps. The overhead varies depending on a number of factors, such as the level of security and number of hops, but the practical payload is only 10-20% of that data rate.

The transceivers are optimized for timing-critical applications and power management. They can quickly be brought up from a quiescent state send and receive messages and go back to sleep to conserve battery life. When transmitting or receiving the radios are not more efficient than similar technologies. It is in the quiescent state that they are so efficient. For that reason the battery life is inversely correlated to the duty cycle. Although it is counterintuitive, receiving tends to use more power than transmitting.

The ZigBee protocol is very reliable. The ZigBee specification includes full mesh networking support. Each transceiver is capable of passing messages to its neighbor. This mesh networking protocol provides redundant paths that are self healing in case devices drop out of the network or barriers are introduced which create interference. If the message fails, it automatically retries three additional times. The use of acknowledgements assures that the message gets through to its intended recipient. In the case of low power end devices, parents keep track of messages for sleeping children.

The underlying IEEE 802.15.4 radios have high intrinsic interference tolerance. Direct Sequence Spread Spectrum provides excellent performance in low SNR environments. CSMA-CA is used for collision avoidance. Since the radios are half duplex, they can not transmit and receive at the same time. So they listen before transmitting the way that a person might do in a conversation. When the network is being initialized the coordinator scans various channels to find the choice with the lowest traffic. Offset Quadrature Phase Shift Keying (O-QPSK) on the 2.4GHz band and Binary Phase Shift Keying (BPSK) on the subGHz band minimize power consumption and reduce complexity. IEEE 802.15.4 has built upon the successes of previous IEEE 802 standards by selecting those mechanisms proven to ensure good reliability without seriously degrading system and device performance. It has been said that the IEEE 802.15.4 radios are like the cockroach that survives the nuclear storm. All of these factors contribute to the reliability of the ZigBee protocol.

The ZigBee protocol is secure. It utilizes AES 128-bit encryption. In addition it uses the concept of a “trust center” (presumed to be the coordinator) to manage access to the network. It can use both link and network keys. These keys can be passed in line or for greater security they can be “hard-wired” into application at the time of manufacture. Authentication with rolling codes is also used to prevent spoofing. Security can be customized for the application. In the case of a light and switch, you might only want to prevent a neighbor’s device from joining your network accidentally. In the case of an alarm or access (e.g. doorlock) application it is necessary to step up the security level to prevent intentional breaches from intruders.

Devices are pre-programmed for their network function. The coordinator scans to find an unused channel to start a network. Routers (mesh device within a network) scan to find an active channel to join, then permit other routers and end devices to join the network. Devices discover other devices in the network providing complementary services (e.g. lights and switches). Service and Device Discovery can be initiated from any device within the network. Queries are unicast and/or broadcast and request statically held information within the device(s). Once located, devices can be bound to other devices offering complementary services. Binding provides a command and control feature for specially identified sets of devices.

Network Formation Management

As ZigBee becomes ubiquitous networks will start to overlap. There needs to be a way to control which devices are allowed to join a network. The Permit Join function can be enabled or disabled on routers and the coordinator (network wide). Permit Join can be managed by an application to allow devices to enter the network upon: a button press on a designated device or any other application defined action. Security keys may be exchanged upon managed network formation as well. When purchasing a product prepackaged as a set, a home owner may have the devices preconfigured already. However, even in these circumstances a device may need to be replaced at some point. Having a button to press on both the new device and the coordinator, allows a simple method for enabling Permit Join without a commissioning tool. But what about the office

building implementing a widespread ZigBee network, with lighting, HVAC, alarm systems blind controls, etc.? It would be too difficult to join devices to the network and bind control functions on such an installation. In this scenario, a commissioning tool is desirable.

The commissioning tool scans to find networks and joins the network selected by the installer. It then performs device discovery on neighbor devices or the whole network. It identifies to the installer which device is which through blinking an LED, turning on and off a light, an audible signal or some other identifying device. Once devices are identified, the installer may create binding records, groups and scenes with a collection of other specified devices. The commissioning tool may also be used for network maintenance, and trouble shooting.

ZigBee is designed for low-cost, low-power, low-data rate, highly-reliable, highly-secure wireless applications. It is built on IEEE 802.15.4 standard. ZigBee hardware and software are available along with an ecosystem of tools and services from multiple vendors today. Simple development environments equate to fast time to market. Using a standards based implementation reduces risk to developers and product manufacturers.