Making Sense of the Sensor Network Value Chain
Jay Werb
Chief Technology Officer, Sensicast Systems, Inc.
Technical Editor, ZigBee Gateway Working Group

OVERVIEW OF WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) using embedded radio technology have burst from the research laboratory into the mainstream over the past year. Well-funded startups are promoting technology to early adopters such as Motorola, Eaton, Leviton, Honeywell, IBM, General Electric, and the United States government. More than a dozen companies are developing chipsets, and wireless mesh sensor networks are being deployed today in various monitoring and control applications. According to ON World Research, more than half a billion wireless sensor nodes will be deployed by 2010, making wireless sensor networks an active area for academic research and product development.

WSNs are intended to carry small amounts of data, infrequently and at low speed. Performance takes a back seat to cost and battery life. Typical applications periodically report a short packet of information, such as a temperature reading every two minutes. The devices are expected to run for years powered by tiny batteries.

Basic Principles

WSN is an area of active computer science research. There are several academic conferences on the subject each year, featuring a wide range of peer-to-peer architectures that can baffle the neophyte. In the commercial world, elegance takes a back seat to engineering realities, causing most systems to converge on the network design generalized in Figure 1.
In most WSN designs, the networks support three basic types of wireless devices:

**End Devices**, also called Nodes, Edge Nodes, Devices, or Reduced Function Devices (RFDs), are battery-powered devices that wake up periodically and send data to a host. To conserve battery power, they spend most of their lives in a low-powered sleep state.

**Routers**, also called Mesh Nodes, Coordinators, or Full Function Devices (FFDs), form a wireless backbone that ferries messages in a multi-hop fashion across the network. Routers allow messages to flow in various directions on demand and buffer messages for nearby End Devices that are currently sleeping. Routers need to expend energy handling traffic on behalf of other network devices and therefore tend to use more power than End Devices. In most implementations, Routers run their receivers continuously and thus require a continuous power source. Routers can also act as application nodes.

**Gateways**, also called Bridges, Controllers, Internet Interfaces, or PAN Coordinators, are usually envisioned as Internet appliances that provide an interface between the WSN and the Internet. Gateways control and monitor the WSN, consolidate data from various nodes, execute business logic, and provide a TCP/IP interface to the outside world. Gateways provide scalability, enabling subnets of WSNs within the enterprise to operate in a collaborative fashion.

Gateways, together with their related system software, are a key component of WSNs. Their duties include protocol conversion; acting as proxy servers (thus eliminating the need to poll every node from an application or management tool); and performing sensor management functions such as network definition, monitoring, deployment, and configuration. Additional duties may include alert and alarm processing; sensor logging and database management; application programming interfaces (APIs); security key management; traffic analysis and optimization; application integration; and routing management.

Gateway TCP/IP application programming interfaces enable developers to leverage WSN technology using familiar Internet programming paradigms. Protocol conversion will break down barriers between WSNs and other types of networks. Gateway standards such as Universal Plug and Plan (UPnP) and OPC support integration of diverse devices, including computers, electronics, security and automation components, and other networked devices spanning wireless and wired networks.

**IEEE 802.15.4 AND ZIGBEE**

More than any other single factor, the sudden interest in WSNs is fueled by two new and related standards: IEEE 802.15.4 and ZigBee.

The IEEE 802.15.4 standard\(^2\), approved in 2003, targets “a low data rate solution with multi-month to multi-year battery life and very low complexity.” IEEE 802.15.4
operates in an unlicensed, international frequency band. IEEE 802.15.4 defines the PHY (physical layer) and MAC (medium access layer). The PHY comes in two variants. One is intended for unlicensed use in international markets, operates in the 2.4 GHz band at a rate of 250 kbps. The other runs in the 915 MHz band (at 40 kbps) in North America and 868 MHz in Europe (at 20 kbps) and is intended for applications such as automated meter reading that need additional range. Both variants are relatively simple direct sequence spread spectrum radios, and the standard was crafted to comply with international regulations for unlicensed use. Above the PHY, the MAC defines how packets are exchanged between pairs of devices in a star configuration. AES-128 symmetric encryption is included in the standard. The standard does not define how radios communicate in multi-hop configurations. Mesh networking and other higher-level issues are covered by ZigBee.

The IEEE 802.15.4 standard is widely considered to provide a simple, clean, and effective baseline for WSN applications. The success of this standard is largely attributable to the designers’ intent to define a straightforward standard based on mature and proven direct sequence radio technology. While inexpensive proprietary radios have been available for a few years, IEEE has raised the bar both by specifying a higher level of performance and by ensuring that there will be multiple sources of compatible transceivers moving forward. As a direct result, an interesting cross section of sophisticated OEMs are quietly building the IEEE 802.15.4 standard into their product roadmaps, and long-term market forecasts for compatible transceivers run in the hundreds of millions of units.

The 802.15.4 standard was ratified in 2003, and more than a dozen vendors have announced plans to provide compliant chipsets. A handful of radio transceivers have become available in 2004. As a group, they provide impressive features and performance. Some transceivers can receive full packets, check the CRC, automatically send an acknowledgement, and provide AES-128 encryption or decryption.

Today, in the early stages of this technology, chip vendors claim that it is possible to build a complete wireless subsystem at a parts cost of approximately $6. In the next generation, it is expected that the microprocessor will be integrated with the radio transceiver in a single package, thus driving the cost of a radio/microprocessor chip into the $2-3 range.

Building upon the IEEE 802.15.4 standard, the ZigBee Alliance was formed to create a specification defining mesh, peer-to-peer, and cluster tree network topologies with data security features and interoperable application profiles – essentially the higher levels of the communications stack that were not within the scope of IEEE. The standard incorporates a set of design tradeoffs that were necessary to achieve a focused set of objectives that included support for a variety of configurations and a requirement to fit in a very small memory footprint. Future versions of ZigBee and IEEE 802.15.4 are
currently being designed to incorporate new technologies and meet the needs of an evolving marketplace.

To support a vision of enterprise scalability, ZigBee recently formed the Gateway Working Group to standardize the interface between ZigBee networks and the Internet. Two basic types of interfaces will be standardized. First, a bridge between ZigBee and IP will enable the creation of IP applications that actively participate in the ZigBee network. Subsequently, gateway functionality will be defined, where the gateway abstracts the operation of the ZigBee network, most likely based on UPnP or another pre-existing standard. These interfaces will enable scalable enterprise applications in which a set of IP hosts interact with a widely distributed collection of WSN devices.

KEY COMPONENTS OF WSN SOLUTIONS

Figure 2 illustrates the building blocks involved in a WSN system.

WSN solutions are based on low-cost radio technology, with basic point-to-point communications at the MAC level. IEEE 802.15.4 radios are preferred by users who wish to follow an international standard. Proprietary options are also available for specialty applications.

The ZigBee Alliance has defined an interoperable standard for building mesh networks. In addition, proprietary alternatives are available from multiple sources. ZigBee has defined a “one size fits all” networking protocol, but it lacks key features such as frequency diversity and router power management. ZigBee’s limitations enable proprietary alternatives to flourish for some classes of applications. In this author’s opinion, key features required by the marketplace will be added to ZigBee over the next few years, thus enabling future versions of ZigBee to prevail. In the interim, early adopters wishing to enter the market in 2005-2006 may need proprietary extensions or alternatives to meet their product requirements.
The ZigBee Gateway provides a logical point of convergence. The philosophy of the Gateway design team is to define an interface standard that isolates the IP programmer from the details of ZigBee operation. Thus, enterprise applications written to that interface can remain unchanged as vendors add proprietary extensions to the ZigBee protocol and as the ZigBee protocol itself evolves.

**EVOLUTION OF THE VALUE CHAIN**

Figure 3 illustrates the current picture of the WSN value chain. A fully integrated solution includes chips, hardware reference designs, modules, firmware, gateways, and server software, all targeted at the end user. Today, the lack of integrated and proven offerings is the biggest obstacle to the adoption of WSN technology. Currently, the market is being flooded with chips, software stacks, and service offerings that may not fit easily together. Companies wishing to build new products in this space need to act as their own integrators of various new technology components.

As the market matures, it is expected that vendors will begin to specialize, with some focusing on hardware components and others focusing on node firmware, gateways, or server software. This is illustrated in Figure 4. Different suppliers will provide each of the necessary components for a complete WSN solution. As vendor specialization occurs, integration will be required to enable successful end-to-end solutions. Integrated and field-proven “plug and play” offerings are needed for companies who wish to bring new WSN applications to market in 2005.
REAL-WORLD APPLICATIONS

Real-world applications of wireless sensor networks include:

- Heating/Ventilation/Air Conditioning (HVAC), including systems that adjust dynamically for changing conditions in different areas of a building
- Biological/chemical agent detection, including systems that raise alerts when the level of a monitored agent exceeds a certain threshold
- Security systems, both for assets and for physical plants
- Process control monitoring
- Home automation
- Structural monitoring, such as real-time corrosion monitoring and crack detection for mission-critical equipment
- Soil monitoring and other environmental monitoring, including systems that manage water dispersal, monitor habitats, and detect undesirable conditions

Example: Wireless Temperature Monitoring in Industrial Motors

In industrial applications, large electric motors regularly fail, disrupting operations, creating scrap, and costing billions of dollars. Temperature monitoring can alert users of impending motor malfunction; however, such monitoring can be costly. Manual data collection is error-prone and unreliable. Wired monitoring systems are inflexible, with wiring and conduit installation accounting for as much as 60% of the cost. The cost of traditional wireless (802.11) solutions is similar to the cost of wired solutions, largely due to the number of industrial-grade access points needed reliably to cover an extended area.

For motor temperature monitoring in an industrial environment such as a nuclear power plant, a number of key benefits have been identified:

- The elimination of wiring lowers installation costs by 80% and installation time by 90% while enabling fast and simple future system reconfigurations.
- WSN installation is simple, self-scaling, and resilient. IEEE 802.15.4 provides link-to-link encryption. IT configuration time is reduced by 80% as compared to solutions that require a grid of wireless access points.
- A low-overhead networking protocol provides years of battery life.

Example: Wireless Object Security Systems

Museum curators face a paradox: Priceless artwork must be protected from the same public for which it is so proudly exhibited. Existing touch prevention systems are either too expensive or create an unusually large number of false alarms, quickly
overtaxing a museum security force. Anecdotal evidence suggests that museums may stop using their systems if false alarms become burdensome. A well-designed touch detection system should reduce or eliminate false alarms.

A WSN solution targeted at art museums offers several unique features, including:

- Near-instant feedback (such as an alarm) to deter touching and notify security.
- Archiving of unauthorized touch instances to alert museum staff to a potential problem (such as a particular painting that is repeatedly bumped).
- Real-time reporting of unauthorized touches to alert museum staff to attempted theft or other mischief.

As in the earlier example, this WSN solution provides a number of benefits, including decreased cost, the ability to leverage the WSN infrastructure for future applications, security, scalability, resiliency, the ability to self-form, and self-healing operation. The ability to reconfigure the system easily is particularly useful to museum curators, who change their collections and displays frequently. A similar system can easily be configured for asset security in non-museum settings.

CONCLUSION

Wireless sensor networks offer numerous benefits over previous networking solutions for many applications, including lowered costs, the ability to leverage infrastructure for multiple applications, and the capacity to restructure the network quickly and easily, as well as security, scalability, and ease of administration. The technology is developing rapidly, with numerous vendors offering WSN components and hundreds of millions of nodes expected to be deployed by the decade’s end. However, companies that seek to take advantage of the growing market must offer more integrated and field-proven “plug-and-play” offerings for the numerous applications that are arising for WSN technology.

