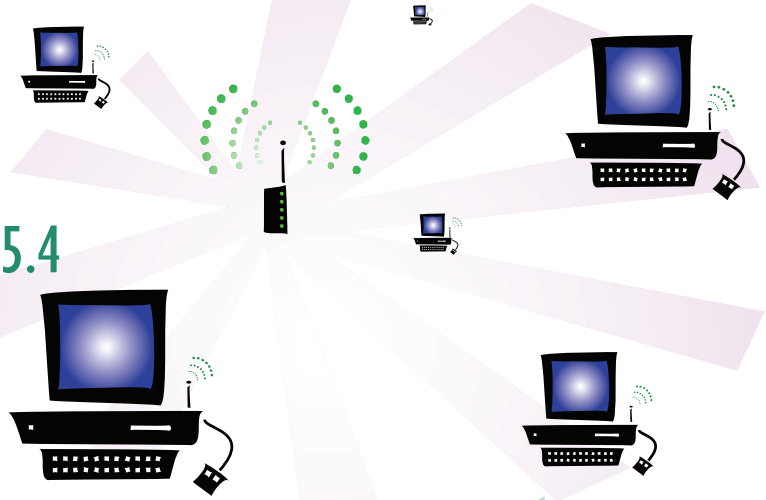
Secure, low-power, IP-based connectivity with IEEE 802.15.4 wireless networks



By David Culler, PhD

IEEE 802.15.4 radios have gained in popularity, and various protocols are used over these radios for wireless connections. IP connectivity is desired for many of these wireless links, but it must be secure and low power. David explores the case for 6LoWPAN in wireless sensor networks.

Industrial instrumentation makers have repeatedly grappled with questions of how and when to utilize IP-based interconnects – which have in their favor widespread commercial adoption, rapid development cycles, and broad interoperability – in place of their more traditional, often proprietary industrial counterparts. Ethernet led the way as an alternative to RS-485 and other multidrop buses, and many industrial standards, including BACNet, LonTalk, Common Industrial Protocol (CIP), and Supervisory Control And Data Acquisition (SCADA), introduced an *IP option* utilizing either TCP/IP or UDP/IP over Ethernet. However, IP's ease of integration and broad interoperability raised some fears about reduced barriers to attack.

Meanwhile, the abundant benefits of operating above IP rather than directly on the particular link became apparent as the broad commercialization of Ethernet yielded 10, 100, and 1,000 Mbps in short order and at low cost. In addition, Wi-Fi (IEEE 802.11) emerged as the dominant wireless link for computers, laptops, and PDAs. Once link-level security was in place with Wi-Fi Protected Access (WPA), this became widespread in industrial environments as well – just another link under IP. Given its high power consumption, Wi-Fi has been most widely adopted on handheld client devices and embedded PCs, which are recharged on a daily basis or mains powered.

But until very recently, the IP approach was thought to be closed to wireless embedded networks because IP protocols could not be scaled down sufficiently to operate on microcontrollers and low-power links, notably the IEEE 802.15.4 radio link. IEEE 802.15.4 packets are quite small, and the entire stack must fit in a very small memory footprint.

The IETF 6LoWPAN draft standard for IPv6 communication over 802.15.4 released in March changes all this. 6LoWPAN's potential for low-power operation makes it attractive for use not just in handhelds, but also in a wide range of instruments. Its built-in support for AES-128 encryption offers the basis for robust authentication and security. To be competitive with more limited link-specific protocols, 6LoWPAN utilizes a *pay only for what you use* header-compression scheme. Through direct integration with IP routers, it can take advantage of the most advanced network security schemes rather than depend on those provided by *ad hoc* gateways. The availability of a low-power wireless IP option offers a new suite of longevity, security, and ease-of-integration trade-offs that is valuable to understand when comparing 6LoWPAN with traditional industrial options.

IP – connecting what you want the way you want to

The Internet is now so familiar that most people seldom think about how it is constructed, much less about what it means to add a new communication link to the Internet family. The Internet architecture is defined in layers, with IP being the middle layer that forms a "narrow waist," allowing diverse applications above to utilize a variety of communication links below in a common, link-independent fashion. It allows different kinds of links to be connected as a single network, with routers steering each message to its desired

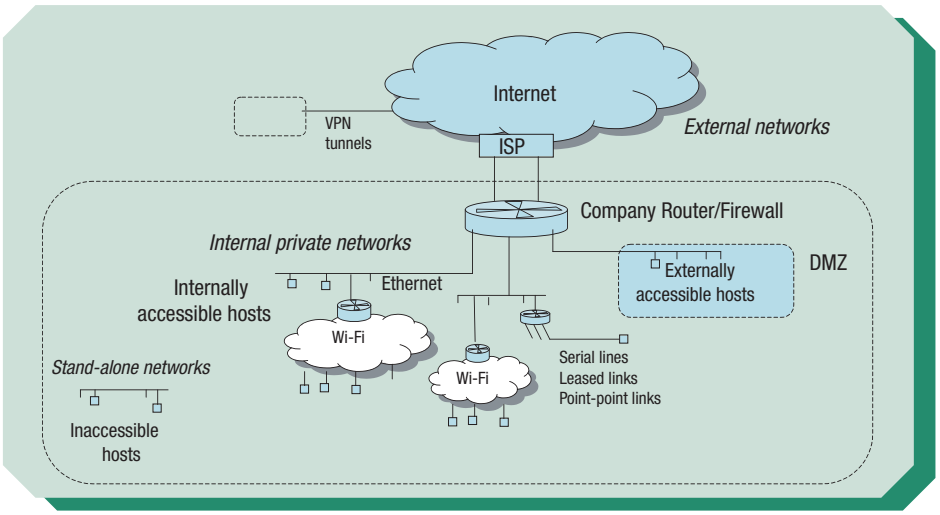


Figure 1

destination, crossing different kinds of links along the way. Software is highly leveraged because it is built on TCP/IP or UDP/IP data transports, regardless of the particular physical devices underneath.

The industrial or corporate network is typically a *small Internet* composed of Ethernet and Wi-Fi subnetworks (see Figure 1). It is connected to the public Internet through specialized firewall routers, which typically allow only certain machines or hosts to be accessible from outside while permitting most internal machines to access hosts outside. Each host has an IP address, such as 192.168.2.33, and a host name, such as devel.acme.com. The address may be public (accessible externally) or private (accessible only internally). Internet protocols locate and route information to and from accessible hosts, transparently crossing multiple links in order to get there.

IP separates new technology concerns, interoperability, and incorporation by masking the underlying physical links' details, such as their packet size and format and how they are interconnected. Applications interact with other applications and services by transferring application-level information directly, regardless of the physical interconnections. A laptop client machine may access a corporate server, networked printer, and network control unit in the same fashion, even though one may be wireless, one on the manufacturing floor Ethernet, and the other in the back office. If any of these devices or networks is upgraded, they all can still function and interact in the same logical manner.

Security is addressed at several levels: physical protection of the wires and devices, encryption of the data transferred over wired and wireless links, and control of the ability to name or route messages to hosts and services.

IEEE 802.15.4 – a new, standard, low-power, wireless link

Each communication link conforms to specific lower-level standards, including a packet's coding scheme and the basic structure, so that the physical devices can talk to each other. IEEE 802.15.4, the latest wireless link standardized by IEEE in 2004, is designed to enable the development of compact, low-power, relatively inexpensive embedded devices that can run on batteries for extended periods (one to five years). It is used in numerous home and industrial automation proprietary offerings and industry-specific standardization efforts, including ZigBee, SP100.11a, and WirelessHART. IEEE 802.15.4 carries information on radio transceivers at 2.4 GHz, roughly the same unregulated band as Wi-Fi and Bluetooth, and transmits at a maximum power of 1 mW, about 1 percent of the power of Wi-Fi or cellular phones. This low-transmit power limits transmission range, so collections of these devices must work together to route information hop by hop over longer distances and around obstacles, much like in the Internet.

The IEEE 802.15.4 coding scheme spreads information over a spectrum of frequencies with built-in redundancy to make it more robust in harsh environments (for example, around heavy machinery) than the many prior proprietary low-power radios. Multihop routing protocols can further enhance reliability by routing around obstacles, detecting losses, retransmitting packets, and even utilizing multiple next-hop candidates.

IEEE 802.15.4 packets are small and formatted as shown in Figure 2. Each packet begins with several bytes of preamble so the receiver can lock on and tell what is coming. The header contains source and destination address fields that specify where it came from and who should receive it. Much like Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11), each device has a unique, relatively large identifier (EUID 64) associated with it at the time of manufacturing. Because 802.15.4 packets are so small, a 16-bit short address can be assigned dynamically to devices and used for communication instead. Furthermore, collections of devices can be partitioned into distinct logical networks by assigning a 16-bit PAN-ID to each collection, much like the service set identifier in Wi-Fi networks.

All network protocols that are built on IEEE 802.15.4 use this same basic frame format and link-level header. The additional information they must exchange for correct operation is placed within the data payload section as a network-level header. For example, when data is communicated over multiple hops, the network header specifies where it starts, where it ends, and how to get from one to the other. Unfortunately, each of the current proprietary protocols and industrial protocols performs this network-level operation differently. Moreover, none of the protocols address how such packets are transferred out of or into the 802.15.4 network to and from existing computers, controllers, and devices on other networks in the plant, factory, or enterprise.

LoWPAN – making IP work over a low-power link

The IETF 6LoWPAN working group was specifically chartered to tackle the problem of defining how to carry IP-based communication over IEEE 802.15.4 links in a manner that conforms to open standards and provides interoperability with other IP links and devices, as well as among 802.15.4 (LoWPAN) devices.

Such a solution has many advantages. Not only does it allow many different companies to manufacture LoWPAN devices that can work together in a network, but these devices also can work with the many networked computers and devices that already exist. This eliminates the need for an array of complex gateways

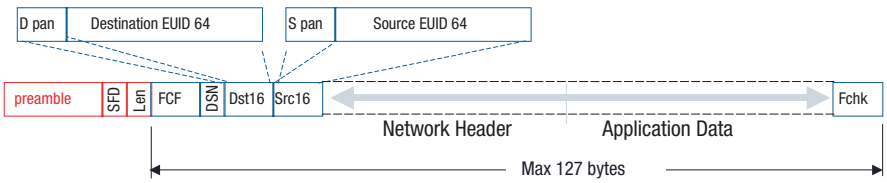


Figure 2

(namely, one for each different local 802.15.4 protocol), the many adapters required for existing applications to communicate through these gateways, and the many gateway-specific security and management procedures. Familiar interfaces can be used in existing machines and applications. The vast body of IP-based standards that has been hardened through the years to provide security, authentication, translation, look-up, configuration, and management can be adopted directly rather than reinvented. The wealth of established IP-based tools, techniques, and practices can be utilized immediately to incorporate and manage these new devices.

Indeed, most industrial communication standards, which were originally developed to provide interoperability over particular industry-specific buses and links, already support an IP option. For example, BACNet evolved from RS-232 and RS-485 and LonWorks evolved from dedicated twisted pairs and power line to IP over Ethernet. CIP evolved from CAN and DeviceNet to EtherNet/IP with the explicit recognition that EtherNet was a placeholder from many additional physical links under IP. Wi-Fi has enjoyed that path of entry. Even SCADA and Foundation FieldBus have IP options. Although these networks are deployed, utilized, and managed very differently in the industrial setting than in the IT enterprise, the value lies in leveraging broad commercial developments and incorporating new technology without replacing all the old.

Unfortunately, IP's utility does not come for free. Addresses and headers are large, and data transfers may be much larger than what fits in a little 802.15.4 packet. The 6LoWPAN group addressed this technical challenge by devising a means to squeeze IP into small packets, carrying only the bare essentials. The 6LoWPAN format is a *pay as you go* plan. The extremely compact basic header expands as broader IP capabilities are utilized. Figure 3 shows a typical example. The entire 40-byte IPv6 header plus the 8-byte UDP transport header are compressed down into just 7 bytes, even smaller than a typical ZigBee header.

When an 802.15.4 device communicates with a nearby 802.15.4 device, the source and destination IP addresses can be compressed to almost nothing. A single header-compression byte communicates that the IP addresses should be inferred from the link addresses in the basic 802.15.4 packet. When communication occurs with other devices outside the embedded network, the larger IP address is included. When the amount of data exchanged is small enough to fit in a basic packet, it can be included with no overhead. For large transfers, a fragmentation header is added to keep track of how the message is broken into fragments. If a single 802.15.4 can get the packet to its destination, it can be transmitted with no overhead; if multiple hops are required, a mesh routing header is included. Or, IP routing can be used within the embedded network.

Thus, the simplest, most frequent case is handled efficiently, and additional information is included in the header as the task becomes more complex. 6LoWPAN is just as efficient as current link-level protocols for the limited cases they address, but extends gracefully into much broader usage.

Security and wireless instrumentation

Once various devices and networks can be connected, it is important to assess the security implications of doing so. For starters, wireless communication raises the possibility of devices "overhearing." Physical security alone cannot be relied on to protect the information transfer. Encryption provides this basic level of protection. IEEE 802.15.4 specifies a very strong form of encryption, AES-128, and essentially all chips that implement the standard perform encryption in hardware. The device contains a protected key typically established during commissioning that encrypts packets as they are transferred to the radio and decrypts packets as they are received. These keys also authenticate the device to the infrastructure so that rogue devices cannot pretend to provide useful information.

Additional security measures, outlined in Figure 4, focus on how the embedded wireless network is connected to other networks. In some sense, the most secure network is stand-alone, disconnected from all other computing devices. The level of protection here is the same, whether the network is IP-based or a proprietary nonroutable protocol because there is no physical way to route into or out of the network. Access can be obtained only from within.

Of course, embedded networks are often connected to other networks so that information can be transferred in and out easily. For nonroutable embedded networks such as ZigBee, Highway Addressable Remote Transducer (HART), SCADA, and RS-485, this connection can be made with a gateway – typically a computer with an IP connection, say over Ethernet, and an interface to the embedded network. Security tends to be only as good as the weakest link, which in this case is the gateway. If the gateway is compromised, all the embedded devices that connect through it are equally compromised. Such gateways are often general-purpose computers running conventional Operating Systems (OSs) with known vulnerabilities that can be exploited. To reduce these vulnerabilities, gateways are typically put behind firewalls and the scope of the networks that can communicate with them is restricted.

When the embedded network is IP-based, the gateway is reduced to a simple router between the conventional network and the embedded network. This is a specialized device that does not need to run general-purpose OSs or applications. It can be configured and managed like the other routers and firewalls that protect the conventional network and can provide additional firewall, access control, and authentication levels for the embedded network. The router can provide basic translation services, such as the network address translation and firewall rules typically used in home and commercial networks, and selectively expose

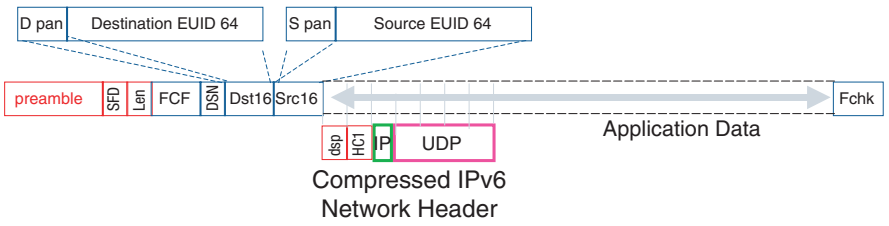


Figure 3

embedded devices to the internal corporate network, much like the demilitarized zone hosts on a conventional network.

As instruments and sensors become connected with low-power wireless links, they essentially become wireless physical information servers, in contrast to the cell phone and PDA, which are wireless clients. In enabling an extremely efficient implementation of IP over 802.15.4 radios, such monitoring points can be protected in much the same way that critical servers containing sensitive information or hosting critical business processes are protected.

Going forward

Metcalfe's Law states that the value of a network grows as the square of the number of devices because each potential connection has value. Historically, instrumentation has been sparsely connected, often with humans transporting the information. The dramatic advance of highly integrated microcontrollers, sensors, and now low-power, cost-effective, high-quality CMOS radios means that instruments, meters, and gauges can be treated as networked devices serving physical information for monitoring, analysis, and control. Standards that allow these devices to interoperate and simplify utilizing the information they provide are essential.

IP provides a set of widely used, long-standing, open standards that manage diverse and evolving suites of devices and networks with well-established mechanisms for protecting critical network resources. With the advent of 6LoWPAN, these protocols have been scaled down sufficiently to be useful in wireless embedded networks. The 6LoWPAN breakthrough is to leverage the shared context typical of the use cases for this technology to obtain a very compact and efficient IP implementation, removing the factors that have given rise to a plethora of *ad hoc* standards and proprietary protocols. Now, low-power wireless devices on IEEE 802.15.4 can simply join the IP family, along with Wi-Fi, Ethernet, and a host of other devices. IES

David Culler *is the cofounder and CTO of Arch Rock Corporation and has been a University of California, Berkeley, computer science professor since 1989. David has conducted seminal work in wireless sensor network technologies, serving as principal investigator of the DARPA Network Embedded Systems Technology project, which created the open platform for wireless sensor networks based on TinyOS, and as founding director of Intel Research, Berkeley. He is a National Academy of Engineering member, ACM Fellow, and IEEE Fellow, and was named one of* Scientific American*'s Top 50 Researchers. He holds a BA in Mathematics from UC Berkeley and MS and PhD degrees in Computer Science from MIT.*

Arch Rock Corporation
657 Mission Street, Suite 600
San Francisco, CA 94105-4120
415-692-0828
dculler@archrock.com
www.archrock.com

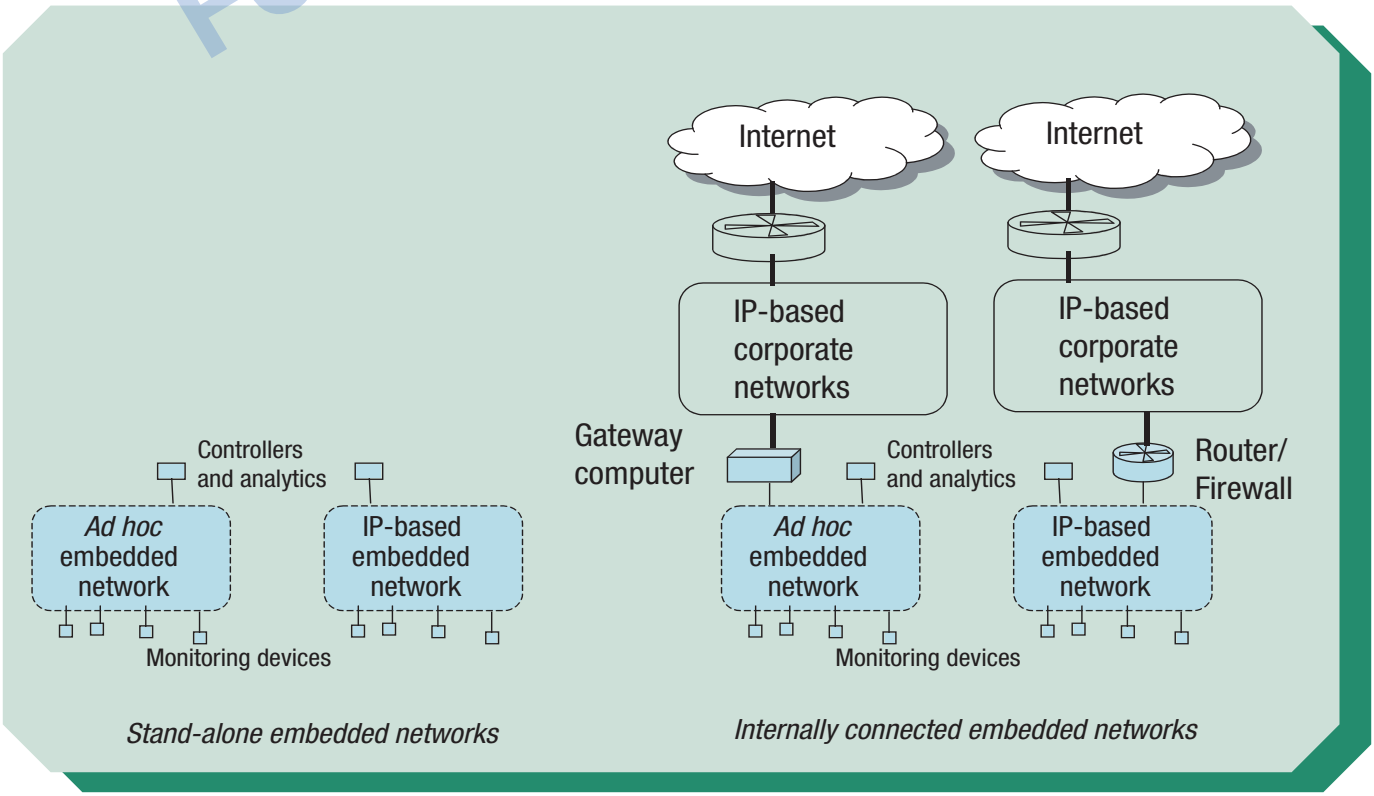


Figure 4