Industrial-strength security for ZigBee: The case for public-key cryptography

By Mitch Blaser

While the popular image of wireless networking usually features cell phones, PDAs, and laptop computers, there are all manner of other devices for which wireless networking presents great advantages. These devices are programmed to perform specific tasks or provide specific information accurately and reliably.

They range from managing automated lighting and heating systems in large buildings, to controlling and monitoring business-critical manufacturing processes. These industrial and commercial environments have demanding requirements in terms of network architecture, power consumption, operating cost, and perhaps most importantly, security. In this article, Mitch makes the case for public-key cryptography for ZigBee wireless networks.

Industrial and consumer security
Work performed by the ZigBee Alliance and the complementary work of the IEEE 802.15.4 standards group, promises to meet security requirements for industrial environments. Designed specifically for low-bandwidth, high-reliability applications – and with security as one of its core elements – ZigBee promises to deliver the benefits of wireless networking for industrial settings.

It also has wide applicability in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys and games.

Node determination
These networks may have a few, hundreds, or even thousands of nodes. As the networks grow, security and management will present a crucial requirement: to identify which node is responsible for what activity.

For instance, when a switch has the job of turning a machine off in case of emergency, it is critical that the command, issued over the network, is received by the correct device and then followed. Alternatively, when a device such as a temperature gauge or a light sensor fails or sends incorrect data, operators will want to know what happened and how to fix it. To do this, operators will need to know quickly and without doubt, which device is causing the problem, and how to prevent it from happening again.
System downtime
For these emerging wireless networks, any system downtime, whether from network failure, an unresponsive device, or an active network attack is a failure to secure the network. In large-scale networks and critical applications built with ZigBee technology, it is essential to implement public-key cryptography that can be used to uniquely identify a node on a network, and then be able to securely send or retrieve data from that node.

With public-key cryptography, one key that only the device knows binds the device to its identity on the network; and a second key, mathematically related to first, is used by the network to verify that identity. This enables device identification to be performed rapidly, surely, and in a cryptographically strong manner.

ZigBee networks can use public-key methods to exchange keys and uniquely identify nodes. This identity can be used to manage the network device life-cycle and decrease management costs, while improving the security of the network and giving the network owner better control over the devices.

Why wireless?
As companies seek ways to reduce operational and support costs and capital investments in today’s competitive global markets, production equipment must deliver reliability, availability, and maintainability. To do this, industry must improve production performance and safety while minimizing costs and extending the operational life of equipment.

Networked wireless sensors and manufacturing devices can enable real-time data sharing throughout a facility while adjusting to changing conditions to limit major failures. A 1997 study by a Presidential advisory board in the US indicated that wireless sensors could improve efficiency by 10 percent and reduce pollution emissions by over 25 percent.

In fact, the physical characteristics of some industrial environments make wireless the only viable networking option. In such cases, the notion of rolling out and maintaining a hardwire network is not only impractical but also prohibitively expensive. For example, some environments consist of an enormous number of devices or sometimes devices are not always easily accessible. Some applications are emerging because of this wireless connectivity; for example, vibration sensors on packing crates to limit breakage – an idea that would have been impossible using a wired sensor.

Ad hoc networks
ZigBee networks are built to operate in an ad hoc manner; that is, the nodes themselves establish communication paths, by communicating with nodes that are nearby. Routed networks like the Internet support multiple communications paths and reconfigure to let the network degrade gracefully if a node fails or an attack is executed on the network. This provides impressive robustness and stability. Ad hoc networks take this feature a step further, with each node able to provide routing rather than using central routers as the Internet.

Unlike other wireless networks, where multiple devices tend to connect independently to a single hub, without contact with other nearby nodes, ZigBee nodes can be interconnected to build a mesh architecture in which all nodes in close proximity can communicate. Popular wireless standards such as 802.11 and Bluetooth have less flexible topologies, making them less than ideal for industrial applications. Both are designed for hub-and-spoke environments, and are consequently unable to effectively support flexible configuration and mesh connectivity. An ad hoc network is shown in Figure 1.

Many of the conditions that make it difficult to hardwire a network in this type of scenario also make it difficult to provide devices with a hardwired power supply – which is precisely what an 802.11 network would require. Bluetooth permits battery operation, but only for short periods of time. By its very nature, ZigBee overcomes these obstacles: devices are built to deliver years of operation from a single battery.

ZigBee power savings
ZigBee differs from other wireless networking protocols because it spreads an encoded signal across a broad spectrum. ZigBee uses Ultra-Wideband (UWB), a wireless transmission method that needs no carrier and means that data is encoded as a pulse train of low power Radio Frequency (RF) energy over many frequencies. This pulsing is much more efficient because it demands considerably less power than broadcasting a single, conspicuous power spike like 802.11 and Bluetooth.

ZigBee conserves further energy by powering down network elements when they are inactive. This significantly extends battery life, allowing devices to operate without the need of a hardwired power supply. As shown in Table 1, the advantages of ZigBee are clear for low-speed networks.

Other ZigBee benefits
As mentioned previously, ZigBee is designed to support low-bandwidth data exchanges – which describe most industrial control and monitoring applications. The design enables fast, flexible, and inexpensive implementation. At the same time, these applications are mission-critical; consequently, expectations of reliability are exceptionally high. ZigBee provides that reliability and these other benefits:

- Cost savings – Installation without physical wiring will avoid the $50 to $100 cost per foot of wire (includes labor costs). In addition, robust, self-configuring mesh networks will save on maintenance costs.
- Rapid commissioning – Installation and provisioning of devices can occur rapidly and without significant costs or physical construction.
- Flexibility – Placement of sensors in optimal locations allows a network to be adaptable and reconfigurable. In addition, placing sensors on all parts of an operation will allow applications never before considered for manufacturing, warehouses, and operational facilities.
- Reliability – Monitoring a large number of inexpensive sensors will offer improved control information, and capabilities to prevent failure and avoid system downtime.

In part due to these inherent benefits, a ZigBee network could be vulnerable to downtime or an attack if not properly secured. Security techniques built into the ZigBee design can ensure that a network is working properly, that only authorized
devices are contributing data to an operation and that control information is sent to and from the correct devices.

**Security features**
ZigBee was created with security as a primary objective, using three main security-design principles.

- Every layer originating a frame is responsible for securing it. This simplifies the overall security solution, because multiple layers are not responsible for securing the same frame.
- Only one key is exchanged between a source and destination device, irrespective of the layer in which the message originates.
- An end-to-end security model is applied throughout; messages are routed independently of trust considerations because only the source and destination devices in any given exchange have access to the shared key. Data can therefore proceed across multiple hops without having to be decrypted and re-encrypted at each hop.

**Advanced Encryption Standard**
ZigBee uses the Advanced Encryption Standard (AES) for symmetric encryption because not only is it stronger than other options, it is faster and can be inexpensively implemented in hardware. The AES hard-ware implementation is much faster than a software implementation. In a short period of time, the cost of designing it into the hardware can be recouped as AES is small enough to fit into small sections of unused space within a device. Additionally, AES is specified as a standard for US government use by the National Institute for Standards and Technology (NIST) under the Federal Information Processing Standard (FIPS) 197.

By definition, a symmetric algorithm means communicating parties use the same key to encrypt and decrypt the messages; but the two communicating parties must find a way to agree on a symmetric key. Therefore, although AES is the symmetric algorithm of choice for ZigBee, it is only part of the security equation.

**Elliptic Curve Cryptography**
Currently, ZigBee uses Symmetric-Key Key Exchange (SKKE), based on AES, to establish keys between communicating nodes. However, the best approach is to dynamically establish keys between communicating nodes as necessary, through the use of using public-key algorithms based on Elliptic Curve Cryptography (ECC). This offers distinct advantages for key exchange including scalability and non-repudiation.

ECC is ideal for ZigBee because it is offers the most security per bit of any public key scheme. Traditional public-key systems, such as RSA, DSA, and Diffie-Hellman (DH) have been widely used for over 20 years. While they have served us well, they are too big and slow to include in constrained environments without severely impacting design choices and profit margins. ECC corrects this problem. Based on the elliptic curve discrete logarithm problem, these public-key algorithms have the benefit of faster computations and smaller key sizes for comparable security.

**Key establishment**
An elliptic curve version of the Menezes-Qu-Vanstone (MQV) scheme is proposed...
as the key establishment mechanism for ZigBee. MQV is an efficient public-key agreement scheme that offers key authentication and key establishment in one calculation. NIST currently has a draft Special Publication, referred to as SP 800-56, which specifies an Elliptic Curve version of MQV (ECMQV) as the key agreement mechanism for US Government use (Figure 2).

The well-known Diffie-Hellman was not used because it requires two sets of calculations and exchanges, one for key agreement and one for authentication, to set up a secure channel. Like AES, ECMQV is fast, strong, and can be inexpensively implemented in hardware. In addition, by using elliptic curve methods, key sizes will be kept small even as security needs increase.

ZigBee also includes numerous key transport services that contribute to the reliability of the overall system. Key re-establishment and refresh capabilities are all built in, enabling ZigBee to offer flexible and robust security policy management capability. By verifying endpoints through its public-key exchange mechanism, ZigBee can provide strong authentication mechanisms, building on a secure foundation.

**Building for strength**

In addition to using proven, efficient algorithms such as AES and ECC, there are a number of elements that can make the low-power wireless networks robust and secure:

- **Key management** – Distribution of keys is one of the functions that maintains the integrity of the network. You need to ensure that the key exchange protocols used do not compromise the system by using weak keys or impact the performance of the device.
- **Reliability** – Improved system up time can result if protocols are engineered to be sure that the wireless network is always networking; this could include a heartbeat function and management polling.
- **Configuration management** – Fast enrollment of devices, two-way identity exchange, and rapid decisions as to trust relationships will be critical in making devices work together.
- **Policy management** – Segmentation of the network and determination of what objects can provide what functions are important in a wireless world.
- **System integrity** – Security protocols can ensure that the network and the sensors themselves are working properly.

**ZigBee applied**

To appreciate the advantages of ZigBee as a wireless standard – and its security capabilities in particular – it is helpful to consider a real-world example: a manufacturing operation with assembly, packaging, and shipping functions. Each has its own control and monitoring requirements, and each depends on the others for the operation as a whole to achieve optimum output (Figure 3).

Data communications in such an environment take advantage of ZigBee’s ad hoc capability. As sensors on machinery and packages move past control nodes on manufacturing equipment, the network reconfigures as the topology changes. ZigBee allows for efficient point-to-point communications. As parts of the manufacturing and shipping operations move or act in relation to each other and share data, the identity of each node must be clearly identified, and the authenticity of communications – the knowledge that a particular communication is from a particular node – must be certain.

**The ZigBee solution**

Versatile and reliable, ZigBee presents a simple, low-cost solution for wireless networking in industrial monitoring.
and control environments. In addition, it is relevant outside of the exclusively industrial arena as well, with applications in consumer electronics, computing, and personal health care.

Network implementations often struggle to reach an acceptable compromise among considerations of performance, security, and cost. ZigBee delivers all three, making it the standard for many kinds of applications.

In ad hoc networks, where nodes may be mobile or transient, the identity of a node is essential to its participation in a network. Public key-based identities deliver stronger security within the constraints of process and control networks – meeting the real-world demands of applications from smart badges and building-systems automation to industrial and medical devices.

“...a symmetric algorithm means communicating parties use the same key to encrypt and decrypt the messages; but the two communicating parties must find a way to agree on a symmetric key.”

ZigBee is an excellent standard for industrial and commercial wireless networking environments. Moreover, public key security based on ECC reinforces ZigBee’s strengths, making possible truly robust wireless networks.

Mitch Blaser specializes in the application of cryptographic protocols and elliptic-curve cryptography to real-world problems at Certicom Corporation. Prior to Certicom, Mitch held market development and product management positions with Alcatel, Newbridge Networks, and TimeStep specializing in network security and cryptographic applications. Mitch holds a MSc in Telecommunications from Southern Methodist University in Dallas.

For more information, contact Mitch at:

Certicom Corporation
5520 Explorer Drive
Mississauga, ON L4W 5L1
Tel: 905-507-4220
Fax: 905-507-4230
E-mail: mblaser@certicom.com
Website: www.certicom.com