The securing of ad-hoc wireless networks
A case for public-key cryptography

Mitch Blaser describes how networks based on Zigbee and RFID need security built-in to ensure they are working correctly and data is sent to and from the correct devices.

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 do specific tasks or provide specific information, accurately and reliably. They range from managing automated lighting and heating systems in large buildings to monitoring business-critical manufacturing processes or tracking inventory of goods.

These industrial and commercial environments have demanding requirements in terms of network architecture, power consumption, operating cost and, perhaps most importantly, security. Popular wireless networking options may not provide the flexibility required for these applications.

Unlike wireless networks, where multiple devices tend to connect independently to a single hub, ad-hoc wireless networks can change their topology with some frequency. This means that nodes can interconnect to build a mesh architecture in which all nodes in close proximity can communicate. When each node within the network can communicate with all nearby nodes, the network can quickly and easily route communications to the next available node resulting in impressive robustness, stability and flexibility.

ZigBee and the complementary IEEE 802.15.4 standard were designed specifically for low-bandwidth data exchanges, such as ad hoc networks and have wide applicability in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys and games.

Active radio frequency identification (RFID) is a wireless form of automated identification technology that can be used for ad-hoc networks. It allows for non-contact reading of data, which makes it effective for manufacturing and other hostile environments where bar code labels may not perform well.

Both of these technologies enable fast, flexible and inexpensive implementations of ad hoc networks. At the same time, most applications are essential to business operations; consequently, expectations of reliability are exceptionally high. ZigBee and RFID provide that reliability along the ability to realize cost savings through rapid installation and provisioning of devices.

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

The need for scalable security
The fact that these ad hoc networks may have a few, hundreds, or even thousands of nodes means that security and management are 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. 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. Or when tracking sensitive materials as they are transported across the country, the agency will want to know immediately if something goes missing. To do this, opera-
hub-and-spoke environments, and are con-
for ad hoc networks. Both are designed for
topologies, making them less than ideal
as 802.11 and Bluetooth have less flexible
over 25 percent.

percent and reduce pollution emissions by
less sensors could improve efficiency by 10
to operate in an ad-hoc manner; that is,
ZigBee or active RFID networks are built
ible configuration and mesh connectivity.

These networks can use public-key meth-
ods 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 net-
work owner better control over the devices. But before we get into the security require-
ments in more details, let’s first look at the technologies behind these ad-hoc wireless
networks.

Technologies for ad-hoc wireless networks
Networked wireless sensors and manufact-
uring devices can enable real-time data sharing throughout a facility while adjust-
ing to changing conditions to limit major failures. A 1997 study by a Presidential ad-
visory board in the U.S. indicated that wire-
less sensors could improve efficiency by 10 percent and reduce pollution emissions by
over 25 percent.

However, popular wireless standards such as 802.11 and Bluetooth have less flexible
ologies, making them less than ideal for ad hoc networks. Both are designed for
ub-and-spoke environments, and are con-
sequently unable to effectively support flex-
ible configuration and mesh connectivity.
ZigBee or active RFID networks are built
to operate in an ad-hoc manner; that is,
communication paths are established by
the nodes themselves, by communicating with nodes that are nearby.

ZigBee differs from other wireless net-
working protocols because it spreads an
code 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 be-
cause it demands considerably less power
than broadcasting a single, conspicuous
power spike, as 802.11 and Bluetooth do. And 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.

RFID is a generic term for technologies
that use radio waves to automatically iden-
ify people or objects. Typically, a reader
communicates with a tag, which holds digi-
tal information in a microchip. The RF
tag includes a chip and the antenna which
enables the chip to transmit the informa-
tion to the back-end system through a
reader.

An active RFID tag has a transmitter to
send back information, rather than reflect-
ing back a signal from the reader, as a pas-
sive tag does.

Most active tags use a battery to transmit
a signal to a reader. They’re used for track-
ing expensive items over long ranges. For
instance, the U.S. military uses active tags
to track containers of supplies arriving in
ports. Access control and transportation
systems are also widely implemented ap-
lications for RFID technology.

Regardless of the technology being used,
security is essential due to the very nature
of the applications for these ad-hoc wireless
networks.

Security designed in
For the security to be effective, an end-to-
end security model must be applied; mes-
ages are handled independent of trust
considerations because only the source
and destination devices in any given ex-
change have access to the shared key. Data
can therefore proceed across multiple hops
or between a device and backend system
without having to be decrypted and re-en-
rypted at each node.

The Advanced Encryption Standard
(AES) should be used for symmetric en-
cryption because not only is it stronger than
other options, it is faster and can be imple-
mented in hardware inexpensively. Once in
hardware, AES becomes much faster than
in software and over a short period of time,
the cost of adding it into the hardware can
be recouped as AES is small enough to fit
into small sections of unused space within
chips. Additionally, AES is specified as a
standard for U.S. government use by the
National Institute for Standards and Tech-
nology (NIST) under the Federal Informa-
tion 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. So
although AES is the symmetric algorithm
of choice, it’s only part of the security equa-
tion.

While you can use symmetric-keys be-
tween communicating nodes, the best
approach is to dynamically establish keys
using public-key algorithms based on el-
liptic-curve cryptography (ECC). This of-
fers distinct advantages for key exchange
including scalability and non-repudiation.

ECC is ideal as the public-key algorithm
because it 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 mar-
gins. ECC corrects this problem. Based on
the elliptic curve discrete logarithm prob-
needs increase. Key sizes will be kept small even as security increases. And by using elliptic curve methods, these public-key algorithms have the benefit of faster computations and smaller key sizes for comparable security.

An elliptic curve version of the Menezes-Qu-Vanstone (MQV) scheme is ideal for the key establishment mechanism in ad-hoc wireless networks. MQV is an efficient public-key agreement scheme that offers key authentication and key establishment in one calculation. NIST currently has a draft standard, referred to as SP 800-56, that specifies an elliptic curve version of MQV as the key agreement mechanism for U.S. Government use. The well-known Diffie-Hellman (DH) 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 implemented inexpensively in hardware. And by using elliptic curve methods, key sizes will be kept small even as security needs increase.

A robust and secure network

In addition to using proven, efficient algorithms such as AES and ECC, there are a number of elements that can make 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 be realized if protocols are engineered to ensure that the wireless network is always networking; this could include a heartbeat function and management polling.
- Configuration management: fast enrolment 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 is important in a wireless world.
- System integrity: security protocols can ensure that the network — and the sensors themselves are working properly.

A real-world example

To appreciate the advantages of active RFID or ZigBee as a wireless standard for ad hoc networks, 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; each depends on the others for the operation as a whole to achieve optimum output.

As each device is installed, the media access control (MAC) address or serial number is recorded manually or annotated as it makes contact with the network manager, and annotated with a human-readable name.

As assets move past control nodes on manufacturing equipment, nodes reconfigure network topology as necessary. Secure device groups can be used such that only specific nodes can monitor or request data from nodes.

Data communications in such an environment take advantage of ZigBee or RFID’s ad-hoc capabilities. 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 result is that each piece can be monitored for efficient movement and to avoid loss.

In the example above, the degree of protection required depends on the situation. A warehouse full of weapons will attract more adversaries than a warehouse full of office supplies. Similarly, the value of information about the contents of the next truck out the gate differs according to whether the truck is carrying rubber tires or medicinal narcotics. Analysis of these factors leads to a valuation of the assets, how hard the adversary is willing to work, and how much security is required.

Network implementations often struggle to reach an acceptable compromise among considerations of performance, security and cost; ZigBee and active RFID can deliver all three, making them ideal for the kinds of applications discussed here.

ZigBee and active RFID present simple, low-cost solutions for wireless networking in a variety of environments. Their architectural flexibility permits rapid deployment and support of large numbers of devices. And with the appropriate level of security built into its design they can offer the security required for even the most sensitive 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 security, based on ECC, deliver stronger security within the constraints of ad hoc networks — meeting the real-world demands of applications from smart badges and building-systems automation to industrial and medical devices.

Mitch Blaser is Product Manager at Certicom.

Accelerating Verification of Elliptic Curve Digital Signatures

For almost a decade, mathematicians have been researching faster ways to verify the elliptic curve digital signatures algorithm (ECDSA). A team of researchers at Certicom has developed a new implementation for ECDSA that reduces the time needed to verify a digital signature by 40 per cent, making it more efficient than open source and other legacy systems.

Referred to as Fast ECDSA Verify, this new implementation is especially relevant for applications such as Check 21 and epassports that need to process large quantities of information efficiently. This new implementation will also have positive implications for those organizations that are using the ECC-based technology recommended by the National Security Agency to protect national security information.