Certicom Security for Sensor Networks

Ensuring Security in Wireless Sensor Networks

THE CHALLENGE

The list of applications for wireless sensor networks is constantly growing. Companies and government organizations are recognizing the potential of these networks to enable everything from asset tracking in warehouses to temperature control in office buildings. Their advantages are many: they deploy rapidly and re-deploy with great flexibility due to their wireless nature. They're cost-effective to maintain and to operate, and they scale easily.

Most sensors in such networks are conveniently compact: often single-purposed battery-powered units and are usually fairly simple.

Yet that compactness and simplicity can be problematic where security is concerned. It is difficult to preserve economy and efficiency and at the same time give sensor nodes enough intelligence to support some of the more sophisticated functions required to ensure the security of the network and the information it transmits.

Why Security Is Essential

The entire value proposition for sensor networks hinges on the expectation that they will function as designed. Failures—whether produced by error or attack—can have exactly the opposite effect of what was intended, creating downtime, interfering with efficiencies and increasing costs.

The prospect of such failures is unpleasant both for network vendors and for their customers. Vendors, particularly, stand to lose reputation and business if their networks can't hold up their end of the bargain.

To prevent calamities, the sensor network must be secured against unauthorized use—again, whether accidental or malicious. This requires authentication and access control.

Most often today, these are established through centrally managed key exchanges: a central controller verifies node identities and distributes the keys for nodes to establish secure connections. This works for small and self-contained networks, but does not permit easy growth. An apt analogy for the central controller is the traffic cop: he or she may be able to manage a busy intersection, but any increase in lanes, streets or traffic could quickly get out of hand.

There are several practical challenges associated with this model:

- **establishing connections between networks—because nodes don't have the intelligence to know which controller to take direction from;**
- **requiring nodes to request direction from a controller can introduce delays and increase network complexity;** and
- **centralized control creates a central point of failure for a secured network.**

So what's the alternative?

Flexible, decentralized mesh architectures allow sensor networks to grow and interoperate easily. Within such an architecture, public-key-based authentication and security allows nodes to operate independently and collaboratively. Each device is issued its own keys and security policy. Identities and policies can be created centrally, then distributed to nodes to enable network operation.

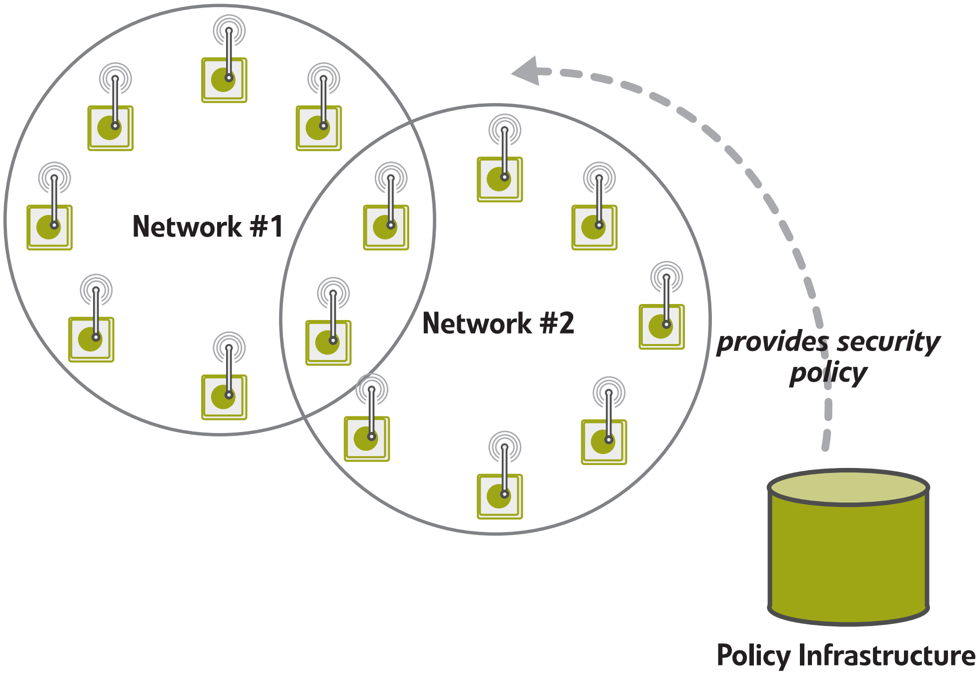

FIGURE 1: With public-key nodes operate independently and create secure connections by authenticating other nodes.

REQUIREMENTS SCENARIOS

To appreciate how security is required—and must be enabled—in wireless sensor networks, consider the following real-world examples.

Keeping It Under Control

Increasingly, wireless sensor networks are being deployed to assist with commercial building controls such as those for lighting and energy-management systems. In such cases, network operators promise their clients that the systems will help reduce lighting, heating and other costs through superior control of building conditions. With lighting costs alone making up 20 to 30 percent of operating expenses, this is an enormously appealing proposition.

To deliver the full benefits, operators must be sure their networks are protected against rogue nodes, active attacks and even user error—by securing every sensor node individually and by ensuring that access to the system is restricted to authorized nodes only. It's a business imperative, because the operator's reputation depends on the performance of the network.

Safety-first Systems

Perhaps even more business-critical are alarm-monitoring networks involving motion sensors or smoke and fire detectors. In these cases, the monitoring is provided as a commercial service—and failure to perform could result in the loss of or damage to property and information. People's safety may even be at risk.

In both this and the previous example, some measure of flexibility is also required. Client organizations must be able to grow or reconfigure their physical space and have their sensor networks keep up with the changes as effortlessly as possible.

The Public-key Advantage

Public key-based networking enables nodes to operate independently and collaboratively. Each device is issued its own keys and security policy. Identities and policies can be created centrally, then distributed to nodes to enable network operation. For building systems control and alarm monitoring applications, this kind of public-key infrastructure allows each node to operate with some autonomy, protecting the network in an unencumbered and easily reconfigurable way. It enables validation of all monitoring equipment. And the secure key exchange between a variety of nodes protects the data being monitored and shared.

The public-key model also addresses the complexities that arise from the interactions of proprietary, open-source and consortium-driven sensor networking technologies. A provable identity based on public-key can be used by the same back-end systems, independent of the type of network that is in use. In other words, public-key identification is technologically 'portable'.

THE SOLUTION

Certicom Security for Sensor Networks allows developers of low-power sensor devices to build secure, reliable operation into networks from the very beginning of the process, rather than having to add it on later. Its public-key-based operation eliminates the need for centralized control of node identities. Instead, Certicom distributes security functions throughout the network to each of the individual sensor nodes. This supports the establishment and maintenance of sensor networks that are scalable, fluid and easily reconfigurable—providing capabilities for an array of new and innovative applications.

The Components

Security Builder MCE (Microcontroller Edition)

CryptographicSoftware Module for Low-power Devices

Security Builder MCE provides the cryptographic primitives required to create a trusted platform for low-power devices. In addition to symmetric encryption, it allows you to integrate key exchange and digital signatures based on elliptic curve cryptography (ECC): the only public-key scheme capable of meeting the footprint and power limitations of these constrained environments. Security Builder MCE provides an API to the device networking stack, and can deliver even stronger performance when combined with the Certicom f(2^m) IP Core.

Certicom IP Core

Hardware IP Core for the Acceleration of ECC on Low-power Devices

The Certicom f(2^m) IP Core accelerates processor-intensive finite-field ECC operations, which are otherwise prohibitively slow for many embedded applications, enabling low-power devices to benefit from the improved security of public-key cryptography. The f(2^m) hardware core accelerates public-key operations over elliptic curves of characteristic 2. It operates in concert with Security Builder MCE to interface with the device networking stack.

OUTCOMES

Certicom Security for Sensor Networks provides the missing link that allows sensor networks to fulfill their true potential—flexibly and securely.

Specifically, it gives the network a decentralized way to validate the identity of participating nodes; to establish communication between nodes; to encrypt data for information security; and to enable integrity checking that ensures messages have not been altered or corrupted.

Using public-key technology spreads operational capability and intelligence among the network nodes—while still allowing for centralized administration of the network's security policies. It is simply that each of the nodes has the ability to enforce those policies independently.

Certainly, permitting device mobility and ensuring standards-level security is not required for every sensor network. In home controls, for example, the requirements for authentication and protection are minimal, and symmetric-key security is likely to be acceptable. For higher-value systems, however, public-key security enabled by the Certicom solution provides a better way to manage device identities and deliver strong security.

Certicom works with application vendors to ensure that the capabilities offered through public-key operations are extended from the device up to sensor network applications.

About Certicom

Certicom, a wholly owned subsidiary of Research In Motion Limited (RIM) (Nasdaq: RIMM; TSX: RIM), manages and protects the value of content, applications and devices with government-approved security. Adopted by the National Security Agency (NSA) for government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the global leader in ECC, Certicom's security offerings are currently licensed to hundreds of multinational technology companies, including IBM, General Dynamics, Motorola and Oracle. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada with worldwide sales offices in USA and Asia. Visit www.certicom.com.

certicom™

USA
3600 Glen Canyon Rd., Suite 1
Scotts Valley, CA 95066
USA
Tel: 1.831.438.4100
Fax: 1.831.438.4111
Sales: 1.800.561.6100
sales@certicom.com

Corporate Headquarters
5520 Explorer Drive, 4th Floor
Mississauga, ON L4W 5L1
Canada
Tel: 1.905.507.4220
Toll Free: 1.800.561.6100
(NA only)
info@certicom.com

Japan
Research In Motion Japan Ltd.
Nippon Brunswick, Building 7F
5-27-7 Sendagaya,Shibuya-ku,
Tokyo 151-0051, Japan
Tel: 03 6367 3567
sales@certicom.com

A Subsidiary of Research In Motion Limited RIM®