Certicom Security for Sensor Networks

enabling **device mobility** in flexible, ad-hoc sensor networks

THE CHALLENGE

Wireless sensor networks present a powerful value proposition for many applications—everything from asset tracking and lighting control to security and fire alarm monitoring. Specifically, that value proposition includes rapid, flexible, cost-effective deployment and operation, as well as easy scalability.

Many of these advantages derive directly from the fact that the sensors involved are compact, battery-powered units—fairly simple and single-purposed. Yet this is exactly what produces one of the main challenges associated with these devices. It is difficult to preserve their economy and efficiency and at the same time give them enough intelligence to support some of the more sophisticated functions required. Those functions include enabling device mobility throughout the sensor network—and ensuring the security of the network, its nodes and the information they transmit.

Mobility in an 'Eccentric' Environment

In many situations, mobility is a key requirement for wireless sensor networks to be truly effective—technologically and as business tools. Devices must be able to move about freely, sending and retrieving data from wherever they happen to be. For them to do so without compromising the network requires that they remain authenticated and secure at all times. Typically, authentication and security in sensor networks 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.

Any node or authorized device can then authenticate itself to any other node as it moves around—or throughout—the network.

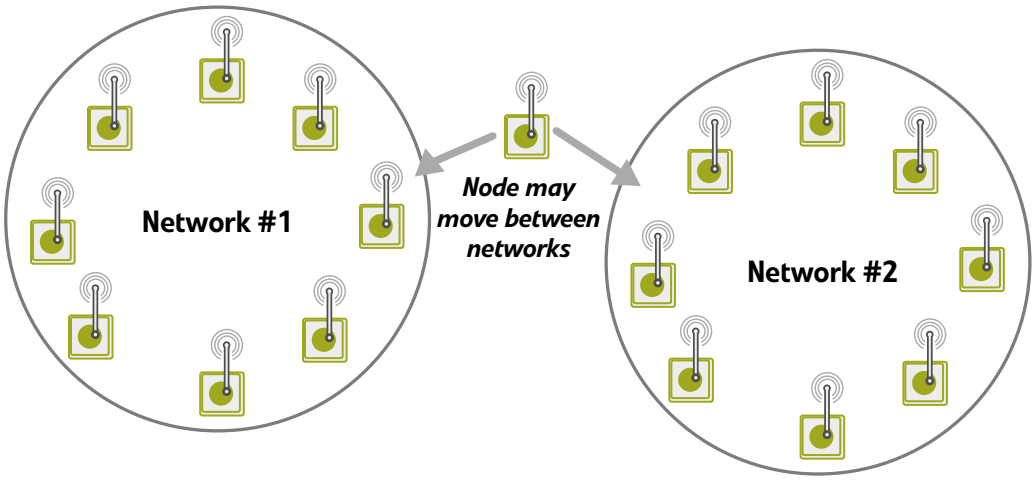

FIGURE 1: Public-key enables nodes to move between networks by authenticating other nodes.

REQUIREMENTS SCENARIOS

To appreciate how mobility comes into play in wireless sensor networks, consider the following real-world examples.

Goods on the Go

Warehouse or baggage-handling asset management systems offer the capability to track items—usually high-value items as well as operating equipment—through a warehouse to provide immediate data on the location of tracked items. As this occurs, nodes can move and re-configure network topology as necessary; each asset can be monitored for efficient movement and to avoid loss. Device policy may be used to define that only specific nodes can monitor or request data from other nodes.

In this case, the tracked asset must be able to identify itself to the various systems able to authenticate that identification—to confirm that the item is the right one. The asset is highly mobile, and the network must have the ability to keep up.

Vehicles on the Move

Fleet management is another area in which these kinds of flexible sensor networks have a role to play. In such cases, it is the vehicles themselves—rental cars, delivery vehicles or freight containers on transport trucks being three examples—that need to be tracked. In each case the vehicles may travel great distances and move in and out of multiple network areas; upon reentering, they must be able to identify and authenticate themselves to the network to ensure that accurate and valid data is exchanged.

People and Privacy

Another (very different) example of the importance of mobility in sensor networks has to do with hospital and home-patient monitoring systems in which security and reliability are critical. Protecting the integrity of data can literally be a matter of life and death if vital signs are being watched. Protecting patients' privacy is also critical—as HIPAA's privacy requirements make clear. Networks transmitting medical data are required to use strong security.

The applications using a sensor network inside a hospital or other medical facility must always 'know' that they're monitoring the right patient, and that the information they gather from the patient on the move is protected.

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 asset-management and medical applications, this kind of public-key infrastructure fosters user confidence and ensures regulatory compliance by installing irrefutable, provable identification into each device. If security policy so dictates, it allows the device to validate the identity of all monitoring equipment, ensuring that only properly credentialed monitors have access to patient or vehicle records. Finally, secure key exchange is enabled between a variety of nodes, meeting regulations for patient confidentiality of transmitted data.

The public-key model can also address 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 the physical network and communication between nodes. 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)

cryptographic software 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 perform to their full capabilities—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.

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 permit true, unimpeded mobility.

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 protects the value of your content, software and devices with government-approved security. Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the undisputed leader in ECC, Certicom security offerings are currently licensed to more than 300 customers including General Dynamics, Motorola, Oracle, Research In Motion and Unisys. Founded in 1985, Certicom's corporate offices are in Mississauga, ON, Canada with worldwide sales headquarters in Reston, VA and offices in the US, Canada and Europe.

North America 1.800.561.6100
EMEA +44.20.7484.5025
International +1.905.507.4220
E-mail info@certicom.com
www.certicom.com

certicom™