Sensei Partners

Securing the New Breed of Remote Wireless Sensor Networks

By Lee Hamilton, Associate – May 2003

Based on *Management of Wireless Monitoring and Control Networks* -
A presentation given by Lee Hamilton at the May 2003 United Telecom Council Annual Conference

A new breed of remote wireless sensor networks is emerging that is changing the fundamental infrastructure of remote wireless monitoring enterprises. With this change comes the challenge to define the security techniques and policies required by this more sophisticated and diverse enterprise.

The emerging remote monitoring enterprise is at the intersection of 4 key enabling technologies: very low cost wireless sensor nodes with integrated sensors; intelligent ad-hoc mesh network protocols; a vast increase in the availability of public wireless data services; and new security methods for authentication and encryption.

Many vendors such as Gaviton, Crossbow Technologies, Ember, Millenial Net and others are developing lost cost wireless sensor nodes that include the processor, memory RF hardware, sensor hardware, OS software and network protocol software all in form factors that can be as small or smaller then a cell phone, These nodes can be configured with just the processor and sensor hardware required for the required monitoring functionality. Competition and volume manufacturing will drive the price point for low-end nodes to below $50 in the next few years. In addition the nodes utilize a standards based RF link based on 802.11 or Bluetooth and some even allow interchangeable RF links depending on the application requirement. At the extreme small end of footprint size are the “smart dust” nodes which are tiny wireless microelectromechanical sensors (MEMS) approximately 5mm x 5mm in size.

Complementing these low cost integrated nodes is the development and commercialization of intelligent ad-hoc network protocols. What characterizes these software protocols is that the network intelligently configures itself with no human intervention as nodes are added or removed from the network. Also the nodes in the network are configured as a mesh that provides multiple possible paths for transmitting sensor data through the network. Most of these ad-hoc software protocols are hardware independent and can be integrated into a wide range of wireless node types and different types of RF data links. Several vendors offer intelligent ad-hoc sensor network protocols including MeshNetworks, Green Packet, Locust World and Ricochet.

The combination of very low cost per wireless sensor node combined with low cost of network deployment due to self-configuring ad-hoc networks will propagate large numbers of these sensor nodes out into many new parts of the remote monitoring enterprise that were previously considered too expensive to cover. This will result in large numbers of independent remote monitoring networks that will need to be logically connected together back to an operations center. The continuing increase in availability of public wireless data services can in some cases provide a solution to that problem

Over the past several years the six major wireless carrier companies in the U.S. have spent billions integrating higher speed, digital CDMA (1XRTT) and GSM technology into their networks. As a result about 80% of the U.S. population will be covered by relatively high speed digital cellular data services by the end of 2003. A much smaller percentage of actual geographic area is covered which limits the use of digital cellular for non-urban applications.

However there are a large number of alternative wireless data services that have much wider geographic coverage which complement digital cellular. These include analog cellular, high bandwidth VSAT and low bandwidth satellite data services. Public 802.11 wireless hotspots are beginning to be rolled out in some areas but it will be 2-5 years before 802.11 coverage matches digital cellular. Large remote monitoring enterprises will need to address security for a mix of data transport services that will backhaul sensor data from the field.

Several technologies currently, or will soon, provide new security techniques for authentication, encryption and authorization. The original standard for wireless security - WEP (Wired Equivalent Privacy) - is considered dead by virtually everyone. Many start-up companies are developing new wireless authentication and encryption solutions based on PEAP (Protected Extensible Authentication Protocol) and other emerging standards. Also the integrated software and hardware capabilities of new wireless sensor nodes allow additional levels of authentication beyond user name and password including biometric authentication at the node, client-server certificates extended to nodes and RF Tag interrogation in the physical proximity of nodes. New encryption algorithms for small nodes will include a key size and other encryption attributes that are dynamically scaled to the processing capacity of the specific node participating in the current session.

The bottom line is that there will be a proliferation of low cost wireless sensor nodes and Internet appliances into remote monitoring and control infrastructures over the next several years. Enterprise management solutions must administer complex multi-tiered security policies, proactively maintain high service levels, and identify threatening transaction patterns across the entire enterprise. This all needs to be done on much larger numbers and diverse types of wireless nodes, running over multiple data transport services. The complexity of the remote monitoring enterprise dictates that security is treated at an integral part of the overall functionality of the enterprise management solution.

The concept of integrating security in the context of overall enterprise management is often referred to as Total Service Delivery Management (Total SDM). Network security is a service whose functionality is defined by all the stakeholders in the remote monitoring enterprise such as network operations(security administration and threat detection), field operations(access and authorization), management(decision support) and even accounting(tracking guaranteed security levels).

A secure remote wireless monitoring enterprise in the context of Total SDM security must include the following components:

- A highly secure and fault tolerant operations facility including physical access control, power back-up, fire suppression and heating/cooling back-up.
- Secure communication gateways linking the operations facility to individual remote wireless sensor networks via high bandwidth wired, digital cellular or VSAT connections – and to corporate facilities via high bandwidth wired connections.
- A set of management applications that can administer multi-tiered security policies including authentication/encryption policy all the way down to the level of individual monitoring nodes.

- A set of analysis applications that track patterns of network traffic through the individual local sensor networks in the field and identify patterns that may constitute a security threat.
- Support for multiple logical enterprises where a single top-level security management facility may need to manage a logically divided enterprise or group of enterprises each with their own specific Total SDM requirements. This becomes especially important to support the increasing use of shared infrastructure, by completely different remote monitoring enterprises, to reduce operating cost and jointly develop leading edge security policies.

Many remote wireless monitoring enterprises are just beginning to incorporate new node technologies and wireless data services. They will need to take a transitional approach in migrating legacy security management systems and policies to the next level. Making a goal of supporting multi-tiered security policies in an integrated Total SDM operational model is a good long term strategy