Secure and Reliable Wireless Networks for Critical Infrastructure Facilities

SANS SCADA Summit 2009
Orlando, Florida

Bryan T. Richardson
Senior Member of Technical Staff
Sandia National Laboratories

February 3rd, 2009

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Project Overview

- *Teaming*
  - *Sandia National Laboratories*
  - *Honeywell International*
  - *Funded by DHS S&T via BAA 07-09 (1 year)*
- *Wireless Mesh Network Improvements*
  - *Industrial wireless mesh networks are becoming a reality*
    - *Honeywell OneWireless*
    - *Emerson/Cisco solution*
  - *Security and robustness improvements*
  - *Fast, easy integration of emergency first responders*
  - *Development*
    - *Commercially available OneWireless mesh network*
    - *COTS 802.11 wireless routers*

What is the Problem?

- Attacks against link-layer communication
  - Routing information modification
    - Source routing
    - Distance vector routing
  - Network/Transport layer header modification
  - Fragmentation
  - Rogue nodes
- One key used by all nodes
  - Single point of failure/compromise
- First Responder situational awareness
  - Easy access to mesh network – insecure
  - Secure access to mesh network – too hard to use

Key Management Options

- **Single network key with manual rekey**
  - Simplest, easiest approach
  - Compromise of single node can be catastrophic
- **Single network key with electronic rekey**
  - Two communication layers: data, rekey message
  - No attribution of nodes
- **Unique network identity and multiple network keys**
  - Public key management: *increased complexity*
  - Each node has a unique key
    - Supports distinct link encryption and authentication

Our Solution

- **Distinct link encryption authentication**
  - Cryptographic protocol for registration of mesh nodes with certificate authority (CA) and key exchange between pairs of nodes
    - CA establishment
    - Node registration
    - Node removal/Certificate revocation
    - Symmetric key exchange
- **First Responder**
  - Pre-emergency first responder credentialing
  - Use of flash memory cards for authentication
  - Time-limited mesh network access

Benefits

- **Distinct Link encryption/authentication**
  - Having a compromised node will no longer lead to the entire system being compromised
- **Secure mesh routing**
  - Losing an interior mesh node (i.e. DoS) no longer causes interruption of data acquisition

Benefits

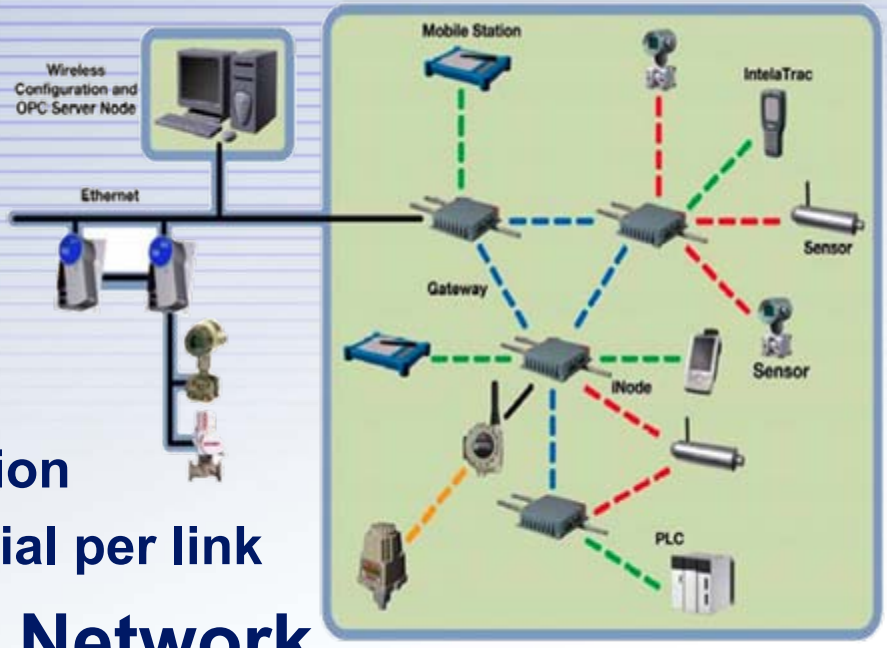
- First responders get access to the wireless network for intra-group communication and situation awareness.
  - Recommend best practices of read-only data
- First responders no longer have to fumble with security, yet communication is still secure

Transition Plan

- **Commercialization**
  - **Enhancements developed as part of this project will be proposed to Honeywell for the next version of the OneWireless product offering**
- **Standards**
  - **Relevant technologies will be offered to the appropriate standards bodies**
    - IEEE 802.11, 802.15.4, ISA 100.11a

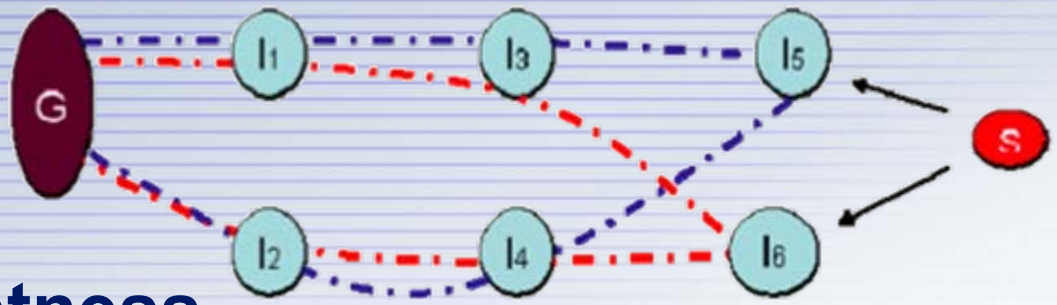
Backup Slides

Technical Activities



- **Enhanced Security**
  - Automatic node authentication
  - Unique cryptographic material per link
- **Multi-functional Mesh Network**
  - Fast, easy deployment of time-limited security credentials to emergency responders
- **Quality of Service (QoS)**
  - Specific QoS for emergency situations

Technical Activities



- **Enhanced Robustness**
  - Dual redundant, non-overlapping routes
- **User Interface**
  - First responder access to data from the site
  - Data condensed using predefined filters
  - Simple and easy to understand interfaces
- **Testing and Demonstration**
  - OneWireless and COTS mesh networks
  - Integration with Honeywell Experion PKS System

Milestones and Deliverables

- **Milestones**
  - Use case scenario definition and requirement gathering for enhanced system demonstration
  - Implementation and functional testing based on voice of customer inputs
  - System integration, deployment, and testing utilizing Sandia's Honeywell Experion PKS System
  - Enhanced system demonstration
- **Deliverables**
  - Technical Performance Report
  - Commercialization Plan
  - Relevant technology will be made available to standards bodies, such as IEEE and ISA