SAND2008-6099P

Secure and Reliable Wireless Networks for Critical Infrastructure Facilities

Wednesday, September 10th, 2008

SRI International, Washington D.C.

Bryan T. Richardson, Sandia National Laboratories

Denis Foo Kune, Honeywell International

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 Description

- Need:
  - Wireless network systems becoming more widely used in control systems due to lower cost and ease of implementation
  - Critical infrastructures need more security since they provide a means of controlling physical processes
  - Robustness is needed to provide 99.99999% availability demanded by control systems
  - Capability for emergency first responders to gain access to pertinent situational awareness data during emergencies
- Approach:
  - Leverage existing authentication and encryption technologies and techniques to provide pairwise link encryption between mesh devices
  - Research and implement robust multipath routing schemes tailored for control systems
  - Research and implement Quality of Service techniques that prioritize data for particular situations and from particular devices
  - Design and implement keying and triggering system for first responder devices
- Benefits:
  - Having a compromised link will no longer lead to the entire system being compromised
  - Losing an interior mesh node (i.e. DoS) no longer causes interruption of data acquisition
  - First responders no longer have to fumble with security yet communication is still secure
  - QoS keeps first responder devices from having to compete with normal control system devices for situational awareness data
- Competition:
  - Wireless mesh network systems exist at a basic level of security with no consideration for first responder access
  - Industrial standards bodies currently developing standards for industrial wireless mesh networks (want to help drive this)

Honeywell

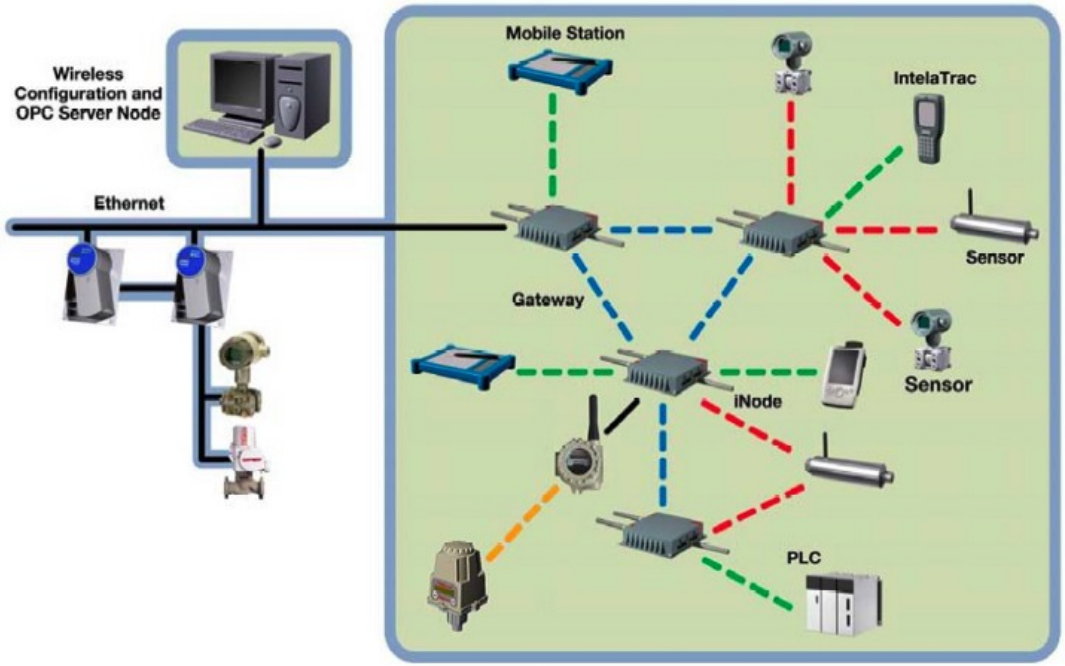
Sandia National Laboratories

Technical Accomplishments

- Enhanced Security
  - Cryptographic protocol for registration of mesh nodes with certificate authority (CA) and key exchange between pairs of nodes has been outlined
  - State diagram of states, events, and actions to represent the key management system is in development
  - Determination of all cryptographic functionality required (algorithms, random number generation, etc) is currently in process
  - Protocol descriptions for node registration, key exchange, and node removal are in development

Technical Accomplishments

- Multi-functional Plant Communication Network
  - Protocol description for first responder credentialing is in development
  - The accounting feature of RADIUS will be used to enforce the length of time a first responder can access the network



Honeywell

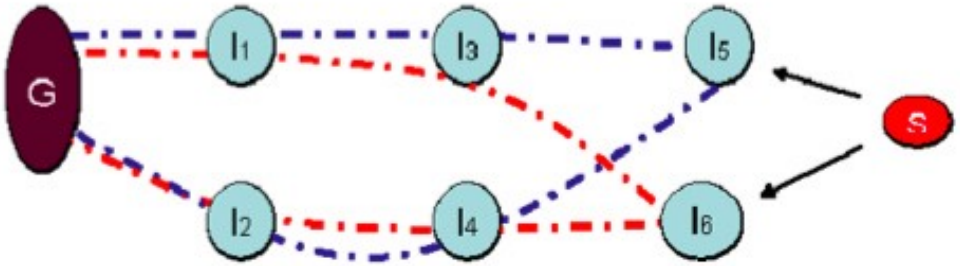
Sandia National Laboratories

Technical Accomplishments

- User Interaction and HMIs
  - Interacted with industry first responders to get a feel for the best approach to providing them with data in the event of an emergency.
  - Our initial approach assumed hand-held PDAs could be used by first responders to provide them with situational awareness data.
  - Our preliminary conversations suggest that, due to typical hazmat suits, in the short term a mobile command and control center should be given access to the wireless network, and in the long term head's-up displays (HUDs) should be considered.
  - CONOPS under consideration
    - Plant emergencies
    - Railcar derailment with HAZMAT cargo

Technical Accomplishments

- Robust and Reliable Communications
  - Leveraging emerging 802.11s standard to provide multiple node-disjoint paths between network nodes, which recommends AODV and OLSR
  - Considering enhancing AODV to support multi-path routing



Honeywell

Sandia National Laboratories

Milestones and Deliverables

- **Enhanced Security (end of Nov 08)**
  - Automatic node authentication
  - Unique cryptographic material per link
- **Multi-functional Plant Communication Network (end of Dec 08)**
  - Easy and fast deployment of time-limited credentials to emergency responders
- **User Interaction and HMIs (end of Dec 08)**
  - Access to data from the site
  - Condensed using predefined filters
  - Simple and easy to understand
- **Enhanced Robustness (end of March 09)**
  - Dual redundant non-overlapping routes
- **Quality of Service (end of March 09)**
  - Optimized message priority depending on current situation
- **Testing and Demonstration (Stage 1: mid Feb 09, Stage 2: mid May 09)**
  - OneWireless and generic (Linksys) mesh networks
  - Integration with Wonderware SCADA system
- **Final Report (end of June 09)**
  - Technical Performance Report
  - Commercialization Plan
  - Standardization Plan

Demonstrations

- **Stage 1: Mid Feb 09**
  - Enhanced Security
    - Show node registration via signing of public key by trusted third party
    - Contrast with current deployment
    - Show node revocation
  - Multi-functional Plant Communication Network
    - First responder credential is time dependent, but extensible
    - Credential deployment (under discussion)
  - User Interaction and HMIs
    - Mobile command unit has access to plant network and can securely obtain info on hazardous areas
- **Stage 2: Mid May 09**
  - Enhanced Robustness
    - Live mesh and killing nodes
    - Visualize with network route
  - Quality of Service
    - Show priority given to sensor data during normal operations
    - Switch to 802.11 data during emergency
    - Use UDP and VoIP to demonstrate

Public Relation Activities

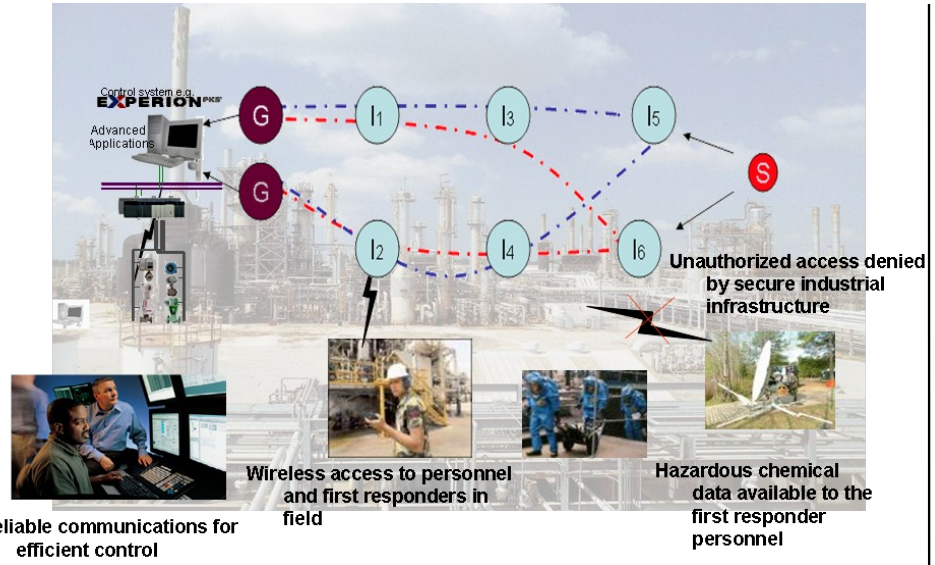
- **Recent:** None
- **Planned:** CATCH conference March 3-4 09
  - At least abstract and poster
  - Demonstration likely but not certain

Planned Transition

- **Commercialization**
  - Honeywell OneWireless is a success story with the U.S. DoE
    - www.honeywell.com/ps/wireless
  - Enhancements developed as part of this project will be proposed for the next generation of OneWireless products
- **Standards**
  - Applicable technologies will be offered to standardization bodies
    - IEEE 802.11, IEEE 802.15.4, ISA 100.11a

BAA Number: Cyber Security BAA07-09 **Offeror Name:** Sandia National Laboratories

Title: Secure and Reliable Wireless Networks for Critical Infrastructure Facilities



Operational Capability:

- Network to be robust to any single point of failure.
- Secure node registration and secure isolated pair-wise communication.
- Extensive safety and productivity improvements, as well as seamless bridging
- and inclusion of first responder devices.
- Quality of Service (QoS) provided for different data as well as for different situations.
- Useful, easy to read data displays available to mobile workers as well as situational awareness (SA) data available to first responders.
- Additional cost of ownership of a OneWireless system for our proposed reliability and security enhancements are expected to be negligible.
- Technical approaches outlined will provide rapid, secure, relevant SA data to first responders as they respond to emergency situations.
- OneWireless was developed as part of an 8 million dollar cost share with DoE and is a commercially available product for critical infrastructure systems.
- OneWireless is designed to be ISA100 compliant and can be integrated with other SCADA systems.

Technical Approach:

The Sandia-Honeywell team will deploy and test a hybrid mesh network for secure and reliable communications in industrial control systems with the following features:

- *Robust and reliable communication of field device data to the control system*
- *Enhanced security using single or multiple keys*
- *Multifunctional plant communication network that provides extensive safety and productivity improvements*
- *Quality of Service mechanisms for different types of data*
- *User interaction and human-machine interfaces available to mobile field workers and emergency first responders*

Milestones, Deliverables, and Contact Info:

Milestones:

- Use case scenario definition and requirement gathering
- Implementation and functional testing based on voice of customer inputs
- System integration, deployment, and testing utilizing Sandia's existing Honeywell Experion PKS system
- Enhanced system demonstration

Period of Performance: *12 Months (total)*

Deliverables: Network demonstration and final report describing reliability and cyber security enhancements, as well as a commercialization path and standardization path, related to hybrid wireless industrial process control system networks for critial infrastructure.

Offeror: Sandia National Laboratories, CA HSD Business Office, PO Box 969, MS9912, Livermore, CA 94551-0969

Contact Info: Bryan T. Richardson, (505) 845-2386, btricha@sandia.gov