SAND2009-0482C

Secure Wireless Key Management for MAC-Layer Security and First Responder Credentialing

SCADA Security Scientific Symposium

January 22, 2009

Miami, Florida

Tim Draelos, Sandia National Laboratories

Honeywell

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.

Sandia National Laboratories

Research Team

Tim Draelos

Bryan Richardson

Mark Torgerson

Pete Sholander

Honeywell

Soumitri Kolavennu

Henrik Holmes

Denis Foo Kune

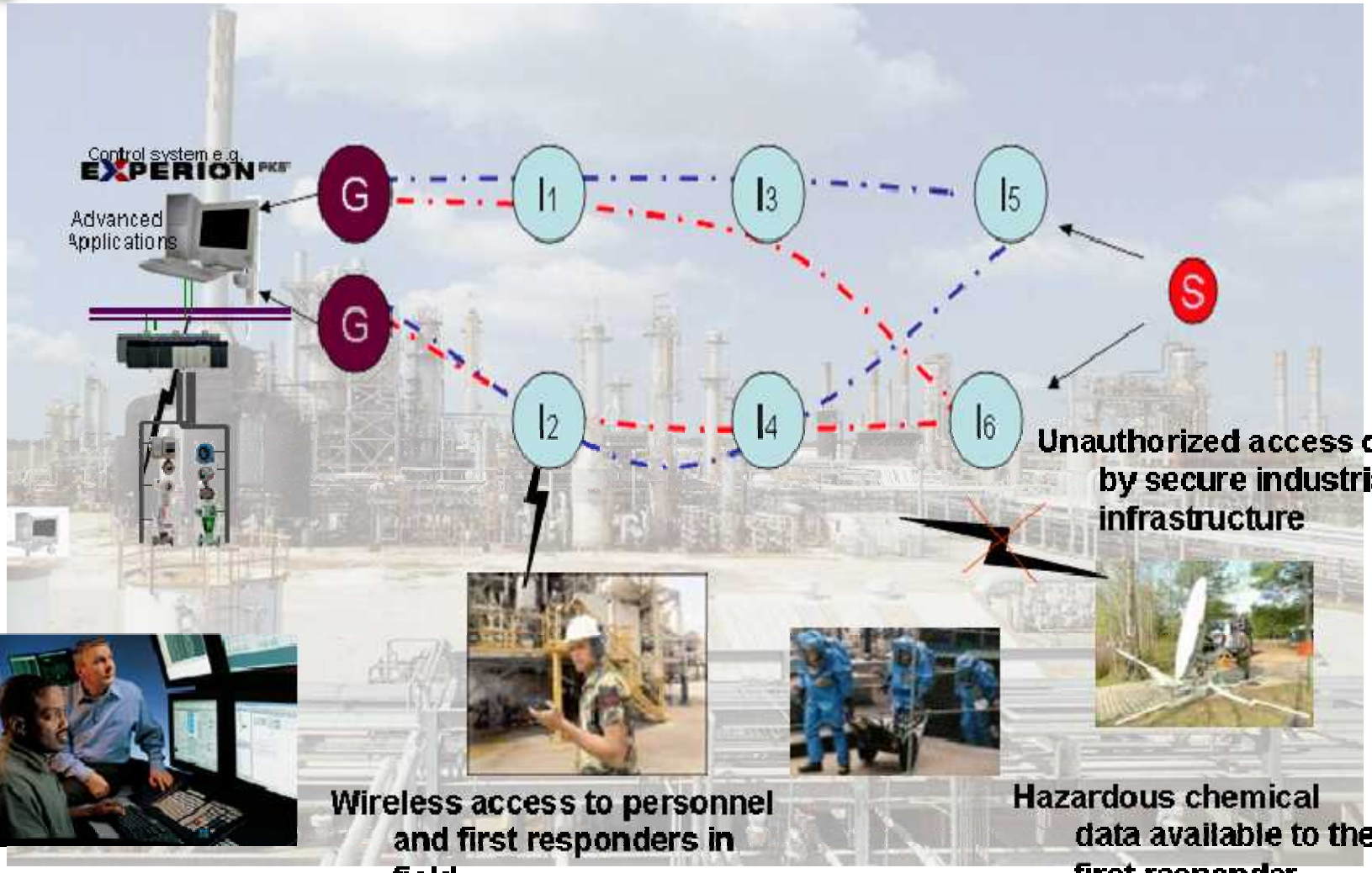
Andrew Johnson

This work was supported under Award Number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate.

Honeywell

Sandia National Laboratories

Application Space



Unauthorized access denied by secure industrial infrastructure

Reliable communications for efficient control

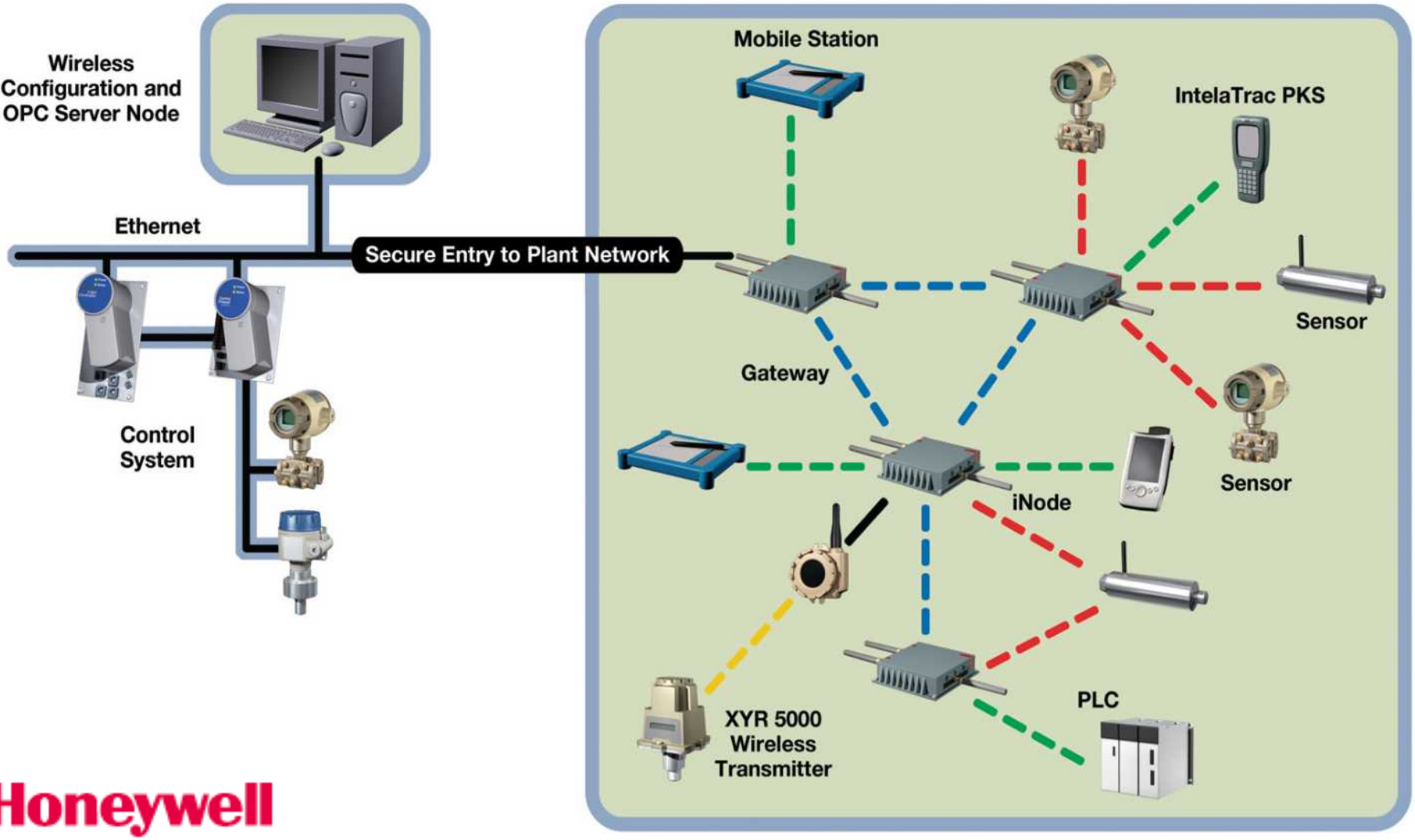
Wireless access to personnel and first responders in field

Hazardous chemical data available to the first responder personnel

Honeywell

Sandia National Laboratories

Application Network



Honeywell

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 situation awareness**

Honeywell

Sandia National Laboratories

Network Communication Threats

Threat / Concern
Compromised nodes in the PCS wireless network
Introduction of unauthorized nodes into PCS network
Man-in-the-Middle Attack on Integrity
Man-in-the-Middle Attack on Confidentiality
Lack of Attribution
Emergency responders lack situation awareness (SA) during plant emergencies.

NOTE: It is impossible to ensure or measure security completely

Honeywell

Sandia National Laboratories

Security Metrics

- **Weakness-based metrics are the metrics of choice**
  - Weaknesses or lack thereof embody the security of the system
  - One cannot know all of the unmitigated weaknesses
  - No nontrivial metric of unknown weaknesses exists

No metric exists that can tell you how secure your system is in an absolute sense

- **This doesn't mean that you cannot secure your system**
  - One may create a system so that the set of exploitable weaknesses is empty and is thus secure against all real adversaries
    - You will just never know when you have done that
  - Not all security related metrics are trivial
    - Value can be had from measuring known aspects of the system

Key Exchange Solution Space

- **IPSEC**
  - Internet Key Exchange (IKE)
    - Diffie-Hellman Key Exchange
- **RFC 4432**
  - RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol
    - Requires RSA Digital Signature Generation
- **Custom Protocol**

Current State-of-the-Art

Threat / Concern	Current Solutions
Compromised nodes in the PCS wireless network	All nodes must be re-keyed with new network-wide key
Introduction of unauthorized nodes into network	Group key must be sent via out-of-band channel to new node
MM Attack on Integrity	Single network key - allows masquerading & traffic injection
MM Attack on Confidentiality	Adversary can eavesdrop on existing links
Lack of Attribution	None
Emergency responders lack SA during plant emergencies	None

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 messages
  - 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 and 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**
  - Time-limited mesh network access

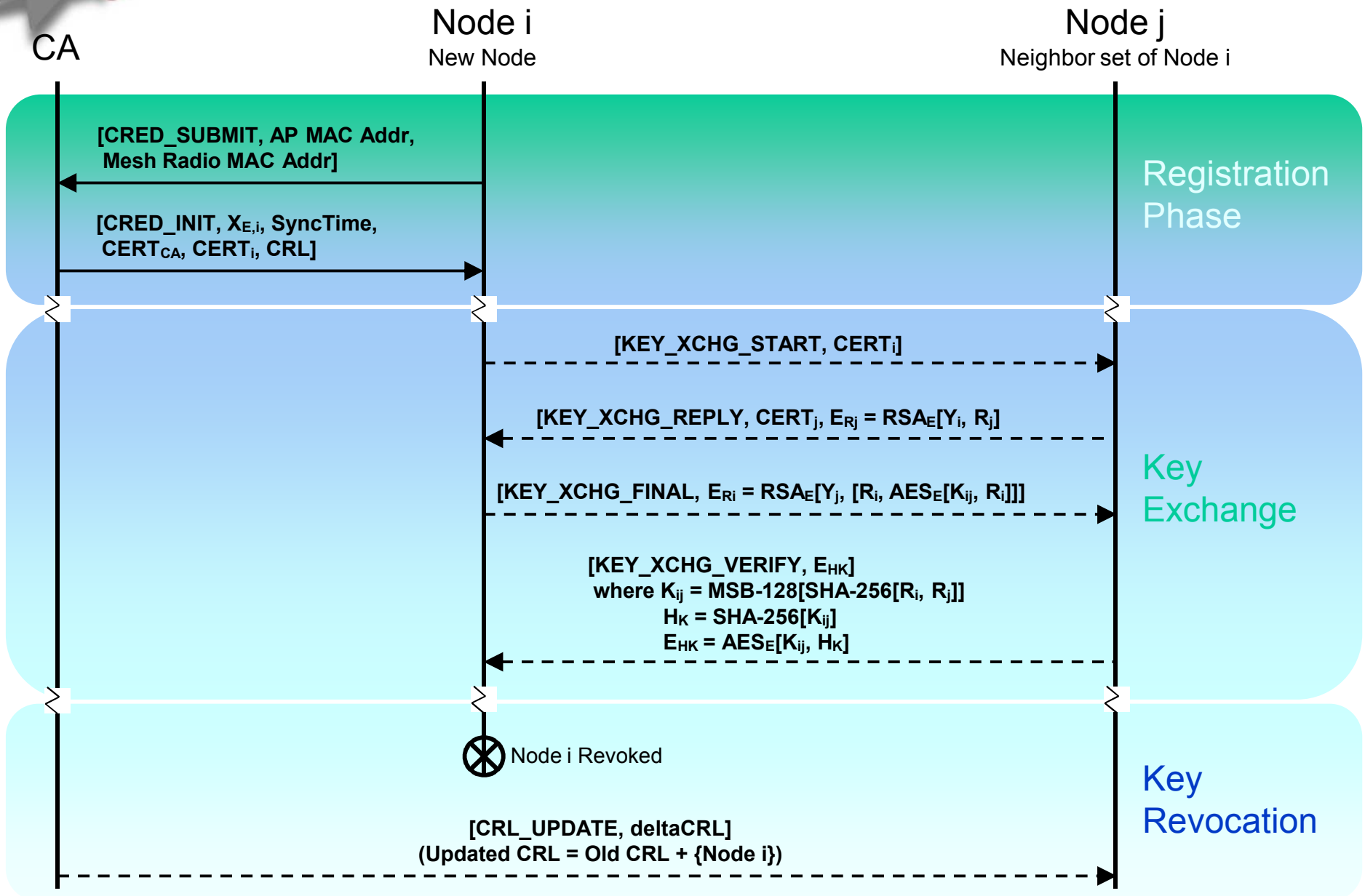
Honeywell

Sandia National Laboratories

Enhancements to State-of-the-Art

Threat / Concern	Our Solution
Compromised nodes in the PCS wireless network	Exclude unicast traffic from bad node; Update group keys
Introduction of unauthorized nodes into network	Certificate-based technique allow secure add/drop of nodes
MM Attack on Integrity	Stop malicious data insertion via strong source identification
MM Attack on Confidentiality	Unique keys protect information between pairs of routing nodes
Lack of Attribution	Distinct per-link keys makes attribution possible
Emergency responders lack SA during plant emergencies	Allow access to mesh network during emergencies

Key Management Protocols



CA Establishment

- CA creates its own RSA digital signature parameters, including its private/public RSA key pair, [$X_{S,CA}$, $Y_{S,CA}$].
- CA creates its own self-signed certificate, $CERT_{CA}$.
- CA establishes a Certificate Database, D_{CERT}, based on Certificate Serial Number (CSN).
- CA establishes a CRL of all revoked node's certificates.

Node i Registration

- Node connects to the Certificate Registration port of the CA.
- Node sends to the CA:

  [CRED_SUBMIT, Node's MAC addresses].
- CA generates RSA encryption/decryption parameters for node, including an encryption private/public key pair, [$X_{E,i}$, $Y_{E,i}$].
- CA creates an X.509v3 certificate, $CERT_i$, for node.
- CA stores $CERT_i$ in the Certificate Database.
- CA sends to node i:

  [CRED_INIT, $X_{E,i}$, SyncTime, $CERT_{CA}$, $CERT_i$, CRL].
- Node i stores $X_{E,i}$, SyncTime, $CERT_{CA}$, $CERT_i$, and CRL.

Honeywell

Sandia National Laboratories

Node Removal / Certificate Revocation

- CA adds removed/revoked node's CSN information to CRL.
- CA digitally signs a CRL update message (deltaCRL).
- CA broadcasts a CRL update to all remaining nodes

  [CRL_UPDATE, deltaCRL].
- Remaining nodes verify the deltaCRL and updates its CRL.

Symmetric Key Exchange

- Node i sends to Node j: [KEY_XCHG_START, $CERT_i$].
- Node j checks validity of $CERT_i$.
- If $CERT_i$ is invalid, exit protocol, send to Node i: [KEY_XCHG_ERROR].
- Node j generates a 128-bit random key, R_j.
- Node j encrypts R_j with Node i's public key, $E_{Rj} = RSA_E[Y_i, R_j]$.
- Node j sends to Node i: [KEY_XCHG_REPLY, $CERT_j$, E_{Rj}].
- Node i checks validity of $CERT_j$.
- If $CERT_j$ is invalid, exit protocol, send to Node j: [KEY_XCHG_ERROR].
- Node i decrypts $R_j = RSA_D[X_i, E_{Rj}]$.
- Node i generates a 128-bit random number, R_i.
- Node i computes the shared key,K_{ij} = MSB-128[SHA-256[R_i, R_j]].

Symmetric Key Exchange (cont)

- Node i encrypts R_i and authenticates the shared key,
  $E_{Ri} = RSA_E[Y_j, [R_i, AES_E[K_{ij}, R_i]]]$.
- Node i sends to Node j: [KEY_XCHG_FINAL, E_{Ri}].
- Node j decrypts $[R_i, AES_E[K_{ij}, R_i]] = RSA_D[X_j, E_{Ri}]$
- Node j computes the shared key, $K_{ij} = MSB\text{-}128[SHA\text{-}256[R_i, R_j]]$.
- If $R_i \oplus AES_D[K_{ij}, R_i]$, exit protocol, send to Node j: [KEY_XCHG_ERROR].
- Node j hashes K_{ij}, $H_K = MSB\text{-}128[SHA\text{-}256[K_{ij}]]$.
- Node j encrypts H_K with AES-128 and K_{ij}, $E_{HK} = AES_E[K_{ij}, H_K]$.
- Node j sends to Node i: [KEY_XCHG_VERIFY, E_{HK}].
- Node i decrypts $H_K = AES_D[K_{ij}, E_{HK}]$.
- If $H_K \oplus MSB\text{-}128[SHA\text{-}256[K_{ij}]]$, exit and send Node j: [KEY_XCHG_ERROR].

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

Time-Limited First Responder Credentialing: Preparation

- **The Plant Manager (PM)**
  - Establishes and maintain a First Responder (FR) Database (FRD)
    - List of approved FRs registered with proper credentials.
      - Proper credentials decided upon by PM
- **The Radius Server (RS)**
  - Associates access privileges with each FR in the database.
- **FRs register with PM before accessing the network.**
- **The PM shall issue a Storage Device (SD) to each registered FR upon request during an emergency.**
  - SDs hold a username and password for access to wireless network
- **The PM (or delegate) manages the privileges of FRs regarding access to the wireless mesh network.**
  - No Access – DEFAULT setting
  - Full Access

Honeywell

Sandia National Laboratories

Time-Limited First Responder Credentialing: Emergency Op

- As soon as possible after the beginning of an emergency,
  - Each FR SD shall be loaded with a unique username and password.
    - The permissions for all approved FRs shall be set to Full Access.
  - The RS sets a count-down timer, T, to 72 hours and begins counting down.
    - The PM can extend the duration of the FR privileges (increase T) at any time.
- Once on site in response to an emergency, the FR is
  - Given a SD to install in his own computing device or
  - Given a computing device (with 3-digit login PIN) with a SD already installed.
- Information must be added to the FR Database
  - FR credential, Computing device ID, SD ID, Username, Password
- Test the equipment issued for access to the wireless mesh network.
- Each iNode in the wireless mesh network will operate as a wireless access point and Network Access Server (NAS) and interact with FR clients.

Time-Limited First Responder Credentialing: Emerg. Op (cont)

- When a FR attempts to connect to the network
  - Username and Password communicated automatically to the wireless access point with the highest signal strength.
  - The NAS will submit an Access-Request message to the RS.
- RS checks credentials information in the FRD
  - The RS sends an Access-Reject response if
    - The count-down timer is zero OR
    - All conditions of the Access-Request are not met OR
    - The privilege setting for the FR is No Access.
  - The RS sends an Access-Accept response if
    - The count-down timer is greater than zero AND
    - All conditions of the Access-Request are met AND
    - The privilege setting for the FR is Full Access.
- When T = 0, the RS terminates each FR session via Packet of Disconnect.
  - The NAS (access point for FR) will terminate its session with that FR.
- PM can set FR privileges to No Access at any time.
- PM sets all FR privileges to No Access at the end of the emergency
- PM can terminate all FR sessions at any time

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

Honeywell

Sandia National Laboratories

Planned Demonstrations

- **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

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**
  - In regular contact with the principal architect for OneWireless
- **Standards**
- **Applicable technologies will be offered to standardization bodies**
  - IEEE 802.11, IEEE 802.15.4, ISA 100.11a