A Key-Management Scheme for Distributed Sensor Networks

Stratimir Doichev
April 23, 2003
CSC 774 Network Security

Paper Overview

• Presents a key-management scheme designed to satisfy operational and security requirements of DSNs by selectively distributing and removing keys from sensor nodes as well as re-keying nodes without substantial computations or bandwidth usage.
Outline

- Background
  - Distributed Sensor Networks
  - Key Management in Distributed Sensor Networks
- Related Work
- Proposed Key-Management Scheme
  - Key Distribution
  - Key Revocation
  - Re-Keying
- Analysis
- Simulation Results and Scenario
- Conclusion and Future Work

Background: Distributed Sensor Networks

- Collection of battery powered sensor nodes
- Types of nodes:
  - Data-collection nodes: cache data and make it available for processing to application components within the network
  - Control-nodes: monitor the status of and broadcast simple commands to sensor nodes
- Dynamic in nature
- Communication/Computation constraints
  - Limited power and communication range
  - Typical asymmetric (public-key) cryptography too expensive
- Key-Management Issues
Background: Key-Management in DSN

- Traditional Internet style key distribution
  - Impractical due to unknown topology prior to deployment, communication range limitations, etc.

- Current key-management techniques:
  - Rely on key-predistribution
  - Single mission key
    - Inadequate due to security risks
  - Pair-wise privately shared keys
    - Requires the storage of (n-1) keys in each sensor, n(n-1)/2 per DSN
    - Addition, deletion, or re-keying of sensor nodes becomes very complex
    - Sensor nodes have on-chip memory limitations

Outline

- Background
  - Distributed Sensor Networks
  - Key Management in Distributed Sensor Networks
- Related Work
- Proposed Key Management Scheme
  - Key Distribution
  - Key Revocation
  - Re-Keying
- Analysis
- Simulation Results and Scenario
- Conclusion and Future Work
Related Work

• In the last decade key-management research has been primarily focused on broadcast and group communication.

• Group communication related work:

• Broadcast communication related work:

Outline

• Background
  – Distributed Sensor Networks
  – Key Management in Distributed Sensor Networks

• Related Work

• Proposed Key Management Scheme
  – Key Distribution
  – Key Revocation
  – Re-Keying

• Analysis

• Simulation Scenario and Results

• Conclusion and Future Work
Proposed Key-Management Scheme

- Relies on probabilistic key sharing among the nodes of a random graph and uses a simple shared-key discovery protocol
- Each sensor node has a key ring consisting of randomly chosen k keys from a large pool of P keys.
- Key Distribution
  - Key pre-distribution phase
  - Shared-key discovery phase
  - Path-key establishment phase
- Key Revocation
- Re-Keying

Key Distribution

- Phase 1: Key Pre-Distribution
  - Consists of 5 off-line steps:
    - Generate a large pool of P keys (2^17 – 2^20 keys)
    - Randomly choose (n times) k keys out of P without replacement
    - Load each set of keys (key ring) into each sensor node
    - Save key identifiers and associated sensor identifiers on the controller nodes
    - Load the identity and shared key (K_ci) of a controller node responsible for a particular sensor node into that node’s memory (shared key can be derived)
- Phase 2: Shared-Key Discovery
  - “Public” method → Each node broadcasts in clear text the key identifiers of the keys on their key ring
  - “Private” method → Each node broadcasts a list of challenges encrypted with each key (e.g. E_Ki(,), i=1,…,k)
Key Distribution cont’d

- **Phase 3: Path-Key Establishment**
  - Assigns a path key to selected pairs of sensor nodes that do not share a key but are connected by two or more links
  - Path keys need not be generated since after the second phase is finished a number of keys on a key ring are left unassigned.

Key Revocation

- Necessary when a node is compromised
- The controller node performs the following steps in order to revoke a key(s):
  - Creates a list of k key identifiers that has to be revoked
  - Generates a signature key, $K_e$, and unicasts it to each affected node by encrypting it with $K_{ci}$ (the key shared with each node during the pre-distribution phase)
  - Signs the list of k key identifiers with $K_e$ and broadcasts it
- Once the keys are removed from the designated key rings, some links may disappear and the affected nodes need to repeat the shared-key discovery phase and possibly the path-key establishment.
Re-Keying

- Sometimes keys expire and re-keying must take place.
- It doesn’t involve any broadcast messages from a controller node.
- After expired-key removal, the affected nodes restart the shared-key discovery and possibly path-key establishment phase.

Outline

- Background
  - Distributed Sensor Networks
  - Key Management in Distributed Sensor Networks
- Related Work
- Proposed Key Management Scheme
  - Key Distribution
  - Key Revocation
  - Re-Keying
- Analysis
- Simulation Scenario and Results
- Conclusion and Future Work
Analysis

- DSN Connectivity with Random Graphs
  - \( P \) → total number of available keys.
  - \( G(n, p) \) → a graph of \( n \) nodes for which the probability that a link exists between two nodes is \( p \).
  - \( d = p \times (n - 1) \) → expected degree of a node (i.e. the average number of edges connecting that node with its neighbors).

- Erdos and Rényi’s Equation:
  - Given a desired probability \( P_c \) for graph connectivity and number of nodes, \( n \), the threshold function \( p \) is defined by:
    \[
    P_c = \lim_{n \to \infty} \Pr[G(n, p) \text{ is connected}] = e^{\pi - c}
    \]
  - where
    \[
    p = \frac{\ln(n)}{n} + \frac{c}{n} \quad \text{and} \quad c \text{ is any real constant}.
    \]

Analysis cont’d

Figure 1: Expected degree of node vs. number of nodes, where \( P_c = \Pr[G(n, p) \text{ is connected}] \)
Analysis cont’d

- Given a neighborhood connectivity constraint requirement $n_-$ and $d$, the probability of sharing a key between any two nodes in a neighborhood becomes:
  - $p_\_ = d/(n_-1)$
  - The following equation represents the relationship between $P$, $p_\_$ and $k$:

$$p' = 1 - \frac{\left(1 - \frac{k}{P}\right)^2(P-k+\frac{1}{2})}{\left(1 - \frac{2k}{P}\right)(P-2k+\frac{1}{2})}$$
Analysis cont’d

• Example 1:
  – Assume a DSN has 10,000 nodes and the resulting network should be connected
    with probability $P_c = 0.99999$. What is the average number of neighbors that
    each node is connecting with?
  – Answer:
    • Using Erdos and Rényi formula we get that $c = 11.5$
    • $p = \frac{\ln(n)}{n} + \frac{c}{n}$, we get $p = 0.002$
    • $d = p \times (n - 1)$, we get $d = 20.7 \approx 20$ nodes.

• Example 2:
  – Given that 75 keys are distributed out of 10,000 to every sensor node in a DSN,
    what is the probability that any two nodes share a key in their ring?
  – Answer:
    • $p_\_ = 0.4326 \approx 43.26\%$

Outline

• Background
  – Distributed Sensor Networks
  – Key Management in Distributed Sensor Networks

• Related Work

• Proposed Key Management Scheme
  – Key Distribution
  – Key Revocation
  – Re-Keying

• Analysis

• Simulation Scenario and Results

• Conclusion and Future Work
Simulation Scenario and Results

- **Purpose**
  - To evaluate the efficiency and scalability of the key distribution scheme

- **Setup**
  - Pool of 10,000 keys
  - A Distributed Sensor Network with 1000 nodes
  - Average density of 40 sensor nodes in a neighborhood
  - Each simulation is run 10 times

Simulation Scenario and Results

- **Effect on the network topology**

![Average path length graph](image)

*Figure 3: Average path length at the network layer*
Simulation Scenario and Results

![Graph showing the ratio of nodes reachable vs number of hops.]

**Figure 4: Path length to neighbors**

Simulation Scenario Results

- Effect of an attack against unshielded sensor nodes

![Graph showing the number of keys vs number of links where a key is used.]

NC State University  Computer Science  CSC 774 Network Security  23
Outline

• Background
  – Distributed Sensor Networks
  – Key Management in Distributed Sensor Networks

• Related Work

• Proposed Key Management Scheme
  – Key Distribution
  – Key Revocation
  – Re-Keying

• Analysis

• Simulation Scenario and Results

• Conclusion and Future Work

Conclusion and Future Work

• Conclusion
  – The results show that the proposed scheme is superior to the traditional key management techniques.
  – It is scalable and flexible with possible trade-offs between sensor-memory size and connectivity.
  – Provides better overall security given that a sensor node is compromised (i.e. attacker has a k/P chance of successfully attacking a link).

• Future Work
  – More detailed analyzes and simulations can be performed to further refine the relationships between k, the connectivity of the network and the overall pool of keys, P.
  – This scheme can be incorporated in the development of a LHAP for Distributed Sensor Networks.
Questions?