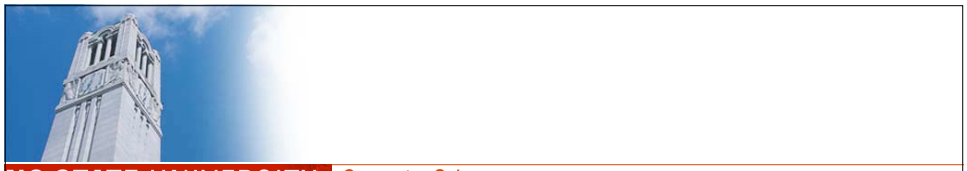


NC STATE UNIVERSITY Computer Science

CSC 774 Network Security

Topic 9.1 Key Predistribution in Wireless Sensor Networks (1)

Outline

- Wireless sensor networks
- Security in sensor networks
- Probabilistic key predistribution for sensor networks

Wireless Sensor Networks

- Composed of
  - Low cost, low power, and multifunctional nodes
  - Wireless communication in short distances
- Sensor node
  - Sensing
  - Data processing
  - Communication
  - Unattended

Security in Sensor Networks

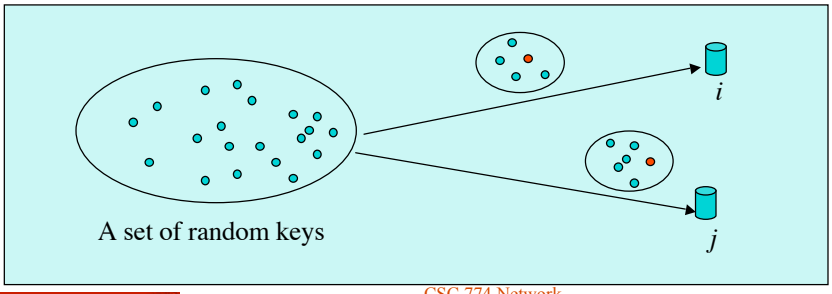
- Sensor networks
  - Resource constraints
    - Limited energy, low computational power, low communication capability
  - Subject to node compromises
- Sensor network security
  - Point-to-point authentication
  - Broadcast authentication
  - Encryption
  - Key management is a fundamental security service.

Establishing Pairwise Keys in Sensor Networks

- Traditional techniques are not practical in sensor networks
  - Public cryptography: not feasible
  - Key distribution centers (KDC): not feasible

Probabilistic Key Predistribution

- Basic idea
  - Assign a random subset of keys of a key pool to each node
  - Two nodes can establish secure communication if they have at least one common key



Probabilistic Key Predistribution (Cont'd)

- Key distribution (three phases)
  - Key pre-distribution
  - Shared-key discovery
  - Path-key establishment

Probabilistic Key Predistribution (Cont'd)

- Key pre-distribution
  - Generate a large pool of *P* keys and their ids
  - For each sensor, random draw *k* keys out of *P* without replacement
    - This forms the key ring of the sensor
  - Load the key ring into the memory of the sensor
  - Save the key ids of each key ring and the sensor id on a trusted controller
  - For each node, load the *i*-th controller node with the key shared with that node.

Probabilistic Key Predistribution (Cont'd)

- Key pre-distribution (Cont'd)
  - Parameters *k* and *P* are critical
    - Only a small number of keys need to be placed on each node's key ring
    - Any two nodes share at least a key with a chosen probability

Probabilistic Key Predistribution (Cont'd)

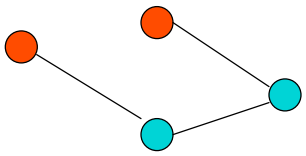
- Shared-key discovery
  - Each node discovers its neighbors in wireless communication range with which it shares keys
  - Method 1:
    - Each node broadcasts the list of key ids on its key ring
    - Give an adversary additional knowledge of key distribution
    - No direct ways to comprise keys

Probabilistic Key Predistribution (Cont'd)

- Shared-key discovery (Cont'd)
  - Method 2 (private shared-key discovery)
    - For each key on a key ring, each node broadcasts a list
      - α, $E_{Ki}(\alpha)$, i= 1, …, k, where α is a challenge
    - If a node receives this list, it tries to decrypt each cipher-text with every key it has
    - The node establishes a shared key if it can successfully decrypt a cipher-text

Probabilistic Key Predistribution (Cont'd)

- Path-key establishment
  - Assign a path-key to selected pairs of nodes that
    - Are in wireless communication range
    - Do not share a common key
    - But are connected by two or more links at the end of shared-key discovery
  - Established through those links



Probabilistic Key Predistribution (Cont'd)

- Revocation
  - Revoke the entire key ring of a compromised node
  - A controller node broadcasts a single revocation message containing a signed list of key ids for the revoked key ring
    - The controller generates a signature key K_e, and unicasts it to each node by encrypting it with the key they share.
  - Each node verifies the signed list of key ids, and removes those key from its key ring

Probabilistic Key Predistribution (Cont'd)

- Re-keying
  - Restart shared-key discovery and path-key discovery

Analysis

- Model a sensor network as a random graph
  - All the sensor nodes are the vertices in the graph
  - There is an edge between two vertices if the corresponding nodes share a common key
- Analysis questions
  - What should be the expected degree (*d*) of a node so that a sensor network with *n* nodes is connected?
  - Given *d* and the size of a neighborhood (*n'*), what should be the key ring size (*k*) and key pool size (*P*) for a network with *n* nodes?

Analysis (Cont'd)

- What should be the expected degree (*d*) of a node so that a sensor network with *n* nodes is connected?
  - Answered by random graph theory
  - G(*n*, *p*): a graph of *n* nodes for which the probability that a link exists between two nodes is *p*.
  - d = p * (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:

$$P_c = \lim_{n \to \infty} \Pr[\text{G(n,p) is connect}] = e^{-e^{-c}}$$

  - where

$$p = \frac{\ln(n)}{n} + \frac{c}{n} \text{ and } c \text{ is any real constant.}$$

Analysis (Cont'd)

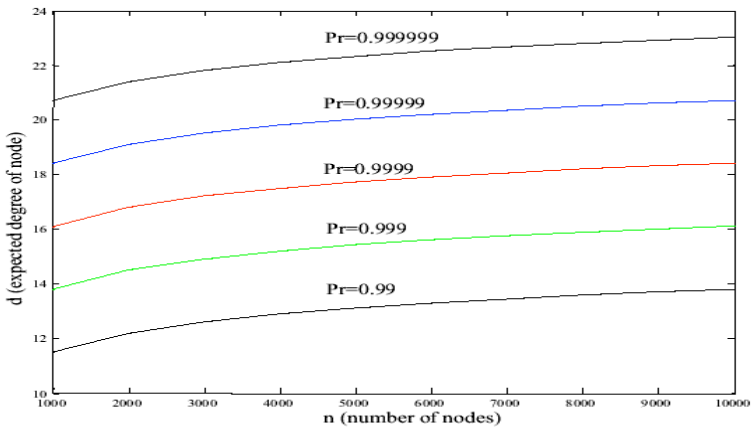


Figure 1: Expected degree of node vs. number of nodes, where $P_c = Pr[G(n,p)$ is connected$]$

Analysis (Cont'd)

- Given *d* and the size of a neighborhood (*n'*), what should be the key ring size (*k*) and key pool size (*P*) for a network with *n* nodes?
  - *p'*: probability of sharing a key between any two nodes in a neighborhood (*p'=d/(n'-1)*)
  - *p'* = 1 – Pr[two nodes do not share any key]

$$p' = 1 - \frac{((P-k)!)^2}{(P-2k)!P!}$$

- Simplify with Stirling's approximation $n! \approx \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n}$

$$p' = 1 - \frac{(1-k/p)^{2(P-k+\frac{1}{2})}}{(1-2k/p)^{(P-2k+\frac{1}{2})}}$$

Analysis (Cont'd)