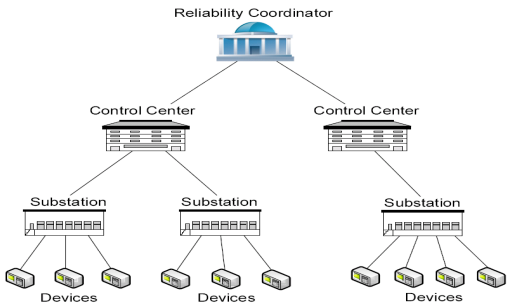
Non-Interactive Multi-Level Key Establishment Scheme for Hierarchical Electric Power Grids

Qiyan Wang, Himanshu Khurana, and Klara Nahrstedt
qwang26@cs.uiuc.edu hkhurana@uiuc.edu klara@cs.uiuc.edu

Hierarchical Electric Power Grids



Goals

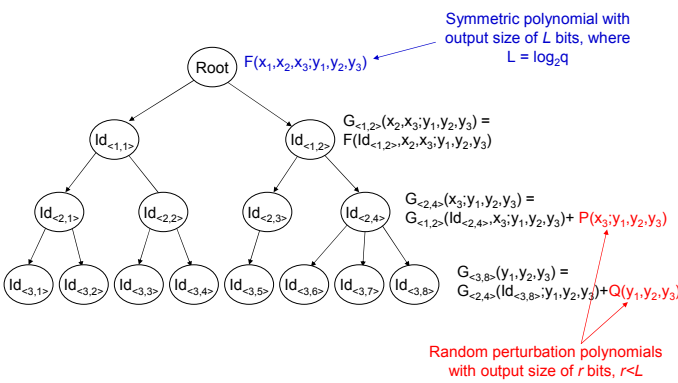
- **Flexible key establishment**: *Any two* entities in the hierarchy can establish a shared key without interaction.
- **Efficient key distribution:** Each key distributor *only* distributes keys to its direct children in the hierarchy.
- **Strong security resistance**: The scheme should be able to resist a large number of node compromises.
- **Small storage and computational overhead**: The scheme should introduce small storage overhead and computational overhead at each node.
- **Scalability:** The scheme should be able to scale to a potentially large number of nodes.

Approach Overview

- Use **symmetric multivariate polynomial** to enable flexible multi-layer key establishment. For example, for 4-level hierarchy, we need a six-variable symmetric polynomial as below.

  $F(x_1,x_2,x_3;y_1,y_2,y_3)=F(y_1,y_2,y_3;x_1,x_2,x_3)$
- Propose a new construction **for multivariate perturbation polynomials** to provide strong collusion resistance.
- Assign each node a **unique ID vector**.
- Derive and distribute a **unique secret polynomial share** for each node according to its ID vector.
- **Compute the shared key locally** using the other node's ID vector.

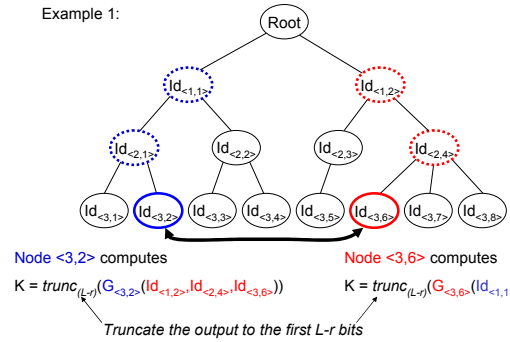
Key Pre-distribution



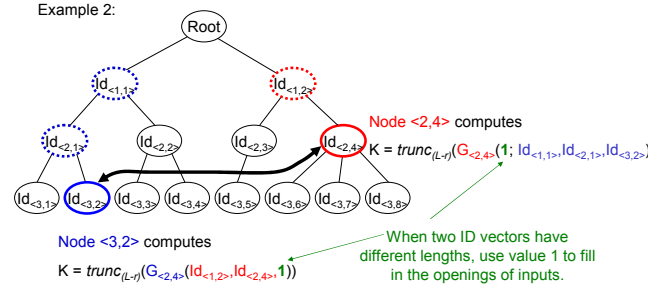
Key Establishment

- Each of the two participating nodes locally computes the shared key by evaluating its polynomial share with the other node's ID vector (which includes IDs along the path from the root to this node).

Example 1:

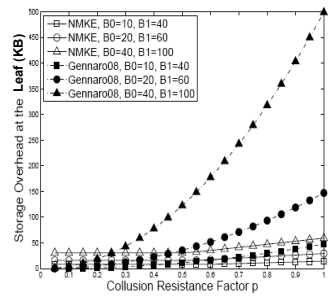


Example 2:

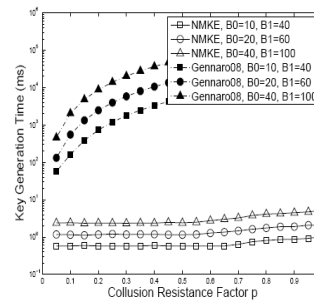


Evaluation

- Comparison of efficiency between our scheme (NMKE) and the related work of Gennaro et al. (Gennaro08).



(a) Storage overhead at each leaf node. B_0 (or B_1) is the number of Children of the root node (or each second-level node).



(b) Computational times to generate a key at each node.

Future Efforts

- Develop complete security proof of the scheme
- Implement a prototype of the scheme on a real testbed.

Trustworthy Cyber Infrastructure for the Power Grid

University of Illinois at Urbana-Champaign