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

Qiyan Wang
Computer Science Department
University of Illinois at Urbana-Champaign
qwang26@cs.uiuc.edu

Himanshu Khurana
Information Trust Institute
University of Illinois at Urbana-Champaign
hkhurana@uiuc.edu

Klara Nahrstedt
Computer Science Department
University of Illinois at Urbana-Champaign
klara@cs.uiuc.edu

ABSTRACT

Reliable data transmission is an important aspect to ensure safety of the electric power grid. In this paper, we propose a non-interactive multi-level key establishment scheme to protect data transmission in hierarchical power grids. Our scheme enables higher-level nodes to hierarchically distribute key materials to lower-level nodes. With the key material, each node is able to locally generate a secret key shared with any other node in the hierarchy (either at the same level or at a different level). Our scheme has strong resistance to collusion attacks. Analysis and experimental results show that our scheme possesses high efficiency in terms of both computational costs and storage overhead.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Cryptographic controls; C.2.0 [**Computer-Communication Networks**]: General security and protection

General Terms

Security, Algorithm, Design

Keywords

Key establishment, Electric power grids, Security protocol

1. INTRODUCTION

The electric power grid is a large distributed system connecting electric power generators, power devices, and monitoring and control stations through power transmission and distribution networks across a large geographical area. Although the power grid is crucial to national security, increasing demand for electricity and an aging infrastructure put increasing pressure on the reliability and safety of the power grid as witnessed in the electric blackout in August 14, 2003 [1].

Reliable data transmission is an important aspect to ensure safety of the power grid. In the power grid, measurement devices (e.g., meters, and phasor measurement units) transmit measurement data (e.g., voltage angles) to substations or control centers which estimate the system state with the received measurement results. Based on the system state, substations and control centers may transmit control signals to control devices (e.g., breakers or relays) to perform operations (e.g., to shut down an electric bus) to maintain the system state in a normal range. Communication between control centers/substations is also necessary to accommodate coordinations (e.g., balancing power load between two areas). These communicating entities (referred to as *nodes*) in the power grid are typically managed in a hierarchical fashion (see Fig. 1) according to their geographic locations. One design goal of the next-generation power grid is to enable any two nodes in the hierarchy to directly communicate with each other to maximize the flexibility of information sharing, thereby improving reliability of the power grid.

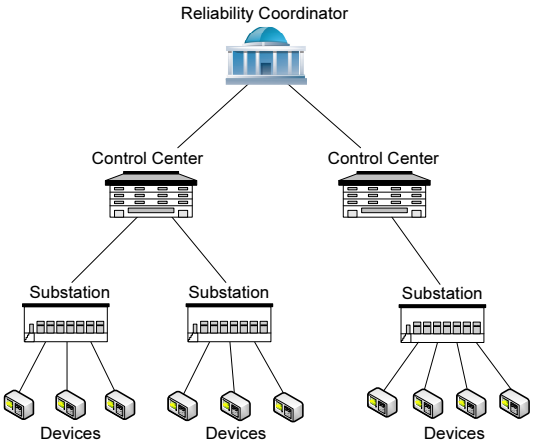

Figure 1: The electric-power-grid hierarchy

To ensure safety of the power grid, it is necessary to consider the potential attacks in which malicious adversaries eavesdrop, modify transmitted data or inject false data to screw up the system. The primal approach to securing data transmission is to use key-based security primitives, such as HMAC (keyed-Hash Message Authentication Code) and symmetric-key encryption, which require a key-establishment mechanism to ensure that any two nodes can share a secret key. As we known, PKI (Public Key Infrastructure) or IBE (Identity Based Encryption) can enable two parties to se-

curely establish a secret key. However, these approaches may have a high management cost considering that the power grid may involve a great number of devices, and besides the central key servers may easily become the attacking target (e.g., denial-of-service attacks).

We design a Non-interactive Multi-level Key Establishment (NMKE) scheme for hierarchical power grids. In NMKE, each non-leaf node in the hierarchy produces and distributes key materials to its children nodes, and with the key materials each node X can locally compute a secret key $K_{X,Y}$ shared with an arbitrary node Y (either at the same level or at a different level) in the hierarchy using the public identification information of Y. We focus on four-level hierarchies (e.g., Fig. 1), although it is feasible to extend NMKE to more than four levels. NMKE is perfectly resistent to collusion of any number of compromised nodes at the third and fourth levels, and is partially resistant to a threshold number of nodes at the second level. NMKE can scale to very large power grids and achieve high computational efficiency and small storage overhead.

2. THE NMKE SCHEME

NMKE is based on multi-variate symmetric polynomials, which was first proposed by Blunto et al. in [3] for group key agreement. In particular, at the initialization stage of NMKE, the root node of the hierarchy generates a random six-variate polynomial $\mathcal{F}(x_1, x_2, x_3; y_1, y_2, y_3)$ (referred to as the *master polynomial*) in the finite field F_q, s.t., $\mathcal{F}(, x_i, ; , y_i,) = \mathcal{F}(, y_i, ; , x_i,)$, $i = 1, 2, 3$. For each node A at the second level, the root node assigns a public identifier ID_A to A and gives A a five-variate polynomial share $\mathcal{G}_A(x_2, x_3; y_1, y_2, y_3) = \mathcal{F}(ID_A, x_2, x_3; y_1, y_2, y_3)$. Then A further distributes four-variate polynomial shares to its children nodes (say B), $\mathcal{H}_B(x_3; y_1, y_2, y_3) = \mathcal{G}_A(ID_B, x_3; y_1, y_2, y_3)$. Finally, a leaf node C that is a child of B obtains a three-variate polynomial share $\mathcal{U}_C(y_1, y_2, y_3) = \mathcal{H}_B(ID_C; y_1, y_2, y_3)$.

In NMKE, each node has an unique *identification vector (IV)*, which consists of three elements and is used for key establishment. The root node's IV is $(null, null, null)$, where the value of *null* is equal to 1. The IV of a second-level node A is $(ID_A, null, null)$, and a third-level node B whose parent is A has the IV $(ID_A, ID_B, null)$. (ID_A, ID_B, ID_C) is the IV of C, which is a child of B. To compute a secret key, each node evaluates its polynomial share by fixing all x's (if any) to be *null* and setting all y's as the elements of the other node's IV. For example, when C attempts to establish a shared key with a second-level node D, C computes $K_{C,D} = \mathcal{U}_C(ID_D, null, null) = \mathcal{F}(ID_A, ID_B, ID_C; ID_D, null, null)$, while D computes $K_{D,C} = \mathcal{G}_D(null, null; ID_A, ID_B, ID_C) = \mathcal{F}(ID_D, null, null; ID_A, ID_B, ID_C)$. Due to the symmetry property of $\mathcal{F}(x_1, x_2, x_3; y_1, y_2, y_3)$, $K_{C,D} = K_{D,C}$.

The above construction can only achieve partial resistance to collusion attacks at each level. To address this problem, we add Random Perturbation Polynomials (RPPs) to the polynomial shares that are distributed to third-level nodes and leaf nodes. The purpose of this is to prevent the attacker from getting the original polynomial shares, which are the essences of breaking the master polynomial. In particular, A generates (for its child B) a four-variate perturbed polynomial share $\mathcal{H}'_B(x_3; y_1, y_2, y_3) = \mathcal{H}_B(x_3; y_1, y_2, y_3) + h_B(x_3; y_1, y_2, y_3)$, where $h_B(x_3; y_1, y_2, y_3)$ is a RPP with r-bit outputs, $r < l = \lceil \log_2 q \rceil$, and $\mathcal{H}_B(x_3; y_1, y_2, y_3) = \mathcal{G}_A(ID_B, x_3; y_1, y_2, y_3)$. Similarly, C obtains $\mathcal{U}'_C(y_1, y_2, y_3) = \mathcal{U}_C(y_1, y_2, y_3) + u_C(y_1, y_2, y_3)$. Due to the existence of RPPs, the least significant r bits of the outputs of polynomial evaluations are perturbed. Hence, the most significant $l - r$ bits of the outputs are used as the key. If the $(l - r)$-bit key segment is not long enough to resist brute-force-based attacks, multiple master polynomials can be used simultaneously and concatenating these key segments can form a strong cryptographic key.

Our design of RPPs is combining Lagrange interpolation and the construction algorithm for univariate perturbation polynomials in [5]. We let $\mathcal{I}_1, \mathcal{I}_2, \mathcal{I}_3$ denote the domains of x_1, x_2, x_3 (or y_1, y_2, y_3), respectively. In other words, $\mathcal{I}_i$ is the set of identifiers of the nodes at the $(i+1)$-th level. We let $\mathcal{J}_X$ denote the set of identifiers of X's children. In NMKE, the RPP for a four-variate polynomial share (of node B) is constructed as

$$h_B(x_3; y_1, y_2, y_3) = \sum_{i=1}^{\lambda} \alpha_{B,i}(x_3) \cdot \beta_{B,i}(y_1) \cdot \psi_i(y_2, y_3)$$

where,

- $\alpha_{B,i}(x_3)$, $i \in [1, \lambda]$, is a r_1-bit RPP constructed on the fly using Lagrange interpolation with randomly picked data points $\{(c_j, d_j) : c_j \in \mathcal{J}_B, d_j \in_R [0, 2^{r_1} - 1]\}$.
- $\beta_{B,i}(y_1)$, $i \in [1, \lambda]$, is a r_2-bit RPP constructed on the fly using Lagrange interpolation with randomly picked data points $\{(e_j, f_j) : e_j \in \mathcal{I}_1, f_j \in_R [0, 2^{r_2} - 1]\}$.
- $\psi_i(y_2, y_3)$, $i \in [1, \lambda]$, is a r_3-bit RPP pre-computed using the algorithm in [5].

Note that the degrees of $\alpha_{B,i}(x_3)$ and $\beta_{B,i}(y_1)$ are $|\mathcal{J}_B|$ and $|\mathcal{I}_1|$, respectively, which are fairly small since there are limited number of nodes (resp. children) at the first level (resp. of B). Furthermore, the construction algorithm in [5] ensures that $\psi_i(y_2, y_3)$ can have a small degree and scale to potentially large domains (i.e., $\mathcal{I}_2 \times \mathcal{I}_3$). The perturbation length of $h_B(x_3; y_1, y_2, y_3)$ is $r = r_1 + r_2 + r_3$. Similarly, the construction of three-variate RPP for leaf node C is

$$u_C(y_1, y_2, y_3) = \sum_{i=1}^{\lambda} \beta_{C,i}(y_1) \cdot \psi_i(y_2, y_3)$$

3. SECURITY ANALYSIS

The Perturbation Polynomial (PP) proposed by Zhang et al. in [5] was recently broken in [2]. The main reason is that there are a very limited number of PPs that are used in their scheme and are pre-constructed. Hence the more nodes are compromised, the more knowledge the attacker can obtain about the master polynomials and these PPs. After enough nodes are compromised, the attacker can gain sufficient knowledge to break the polynomial share of any non-compromised node. On the contrary, there are a large number of RPPs available in NMKE, due to Lagrange interpolation with randomly picked data points. These RPPs are randomly created on the fly. Once a node gets compromised, a new RPP that is unknown to the attacker is introduced. When λ is not smaller than $t_2 \cdot t_3$, where t_2 (or t_3) is the degree of x_2, y_2 (or x_3, y_3), the knowledge (about

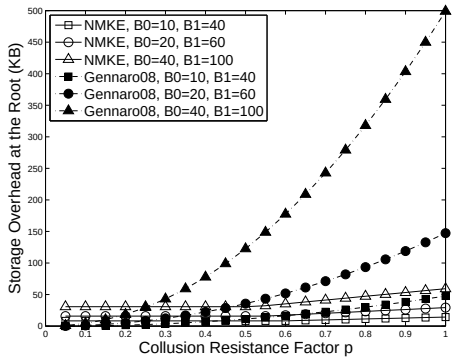

Figure 2: Storage overhead at each leaf node. B_0 (resp. B_1) denotes the number of children of the root node (resp. a second-level node).

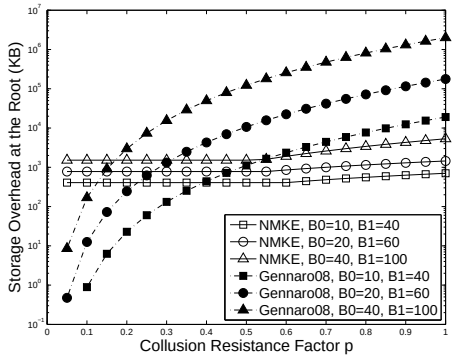

Figure 3: Maximum storage overhead at any non-leaf node (including the root node)

the master polynomials and involved RPPs) gained by the attacker after compromising a node is less than the unknown information introduced by the RPP. Since the resistance to collusion attacks at the third and fourth levels is independent of t_2, t_3, we can choose small values for t_2, t_3 to make λ small. A systematic proof on the security of NMKE is the focus of our future work.

4. EVALUATION

We evaluate NMKE in terms of the storage overhead at each node and the computational time to generate a key. We compare NMKE against a hierarchical key establishment scheme proposed by Gennaro et al. in [4] (referred to as Gennaro08), which combines IBE and polynomial-based key establishment scheme [3]. Gennaro08 supports hierarchical key distribution, but only enables leaf nodes to establish shared keys with each other (whereas NMKE enables any two nodes in the hierarchy to share a secret key).

To measure the resistance to collusion attacks, we introduce the metric of *(collusion) resistance factor* ρ_l, which represents what fraction of children of X at level l ($l = 2, 3, 4$) that the attacker needs to compromise in order to break the polynomial share of X. In NMKE, the third and fourth levels in the hierarchy are perfectly resistent to collusion attacks, and hence $\rho_l = 1$, $l = 3, 4$. We let $\rho = min\{\rho_l : l = 2, 3, 4\}$.

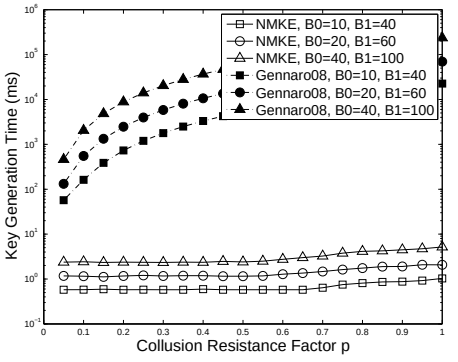

Figure 4: Computational times to generate a key

We set $t_2 = t_3 = 1$ and $l = 48$ (recall that $l = \lceil \log_2 q \rceil$). The perturbation lengths of $\alpha_{B,i}(x_3)$ and $\beta_{C,i}(y_1)$ constructed by Lagrange interpolation are $r_1 = r_2 = 4$, and the perturbation length of $\psi_i(y_2, y_3)$ is $r_3 = 40$ with $\lambda = 4$. This configuration can support up to about $64,000$ nodes at each level. To generate 128-bit keys, we use 32 master polynomials. The storage overheads are shown in Fig. 2 and Fig. 3. We implement NMKE using Miracl on a Windows XP machine with dual 2.26 GHz CPUs and 2 GB RAM. Fig. 4 gives the computational time to generate a secret key. The results are averaged over $1,000$ independent runs.

We see that the storage overhead introduced by NMKE is considerably smaller than that of Gennaro08 when the hierarchy is large and the resistance to collusion attacks is high. In addition, NMKE does not require any expensive modular exponentiation computations, and thus has significantly higher computational efficiency than Gennaro08. In NMKE, it only takes less than $7ms$ to generate a secret key, which is $10,000$ to $100,000$ times faster than Gennaro08. These salient benefits ensure that NMKE can be gracefully applied to the power grid, where power devices may have limited memory and computational resources.

5. REFERENCES

[1] Final report on the august 14, 2003 blockout in the united states and canada. 2004. *http://reports.energy.gov/B-F-Web-Part1.pdf*.

[2] M. Albrecht, C. Gentry, S. Halevi, and J. Katz. Attacking cryptographic schemes based on "perturbation polynomials". *The 16th ACM Conference on Computer and Communication Security (CCS'09)*.

[3] C. Blundo, A.D.Santis, A. Herzberg, S.Kutten, U. Vaccard, and M. Yung. Perfectly secure key distribution for dynamic conference. *In Advances in Cryptology (CRYPTO'92)*, 1992.

[4] R. Gennaro, S. Halevi, H. Krawczyk, T. Rabin, S. Reidt, and S.D.Wolthusen. Strongly resistant and non-interactive hierarchical key-agreement in manets. *The 13th European Symposium on Research in Computer Security (ESORICS'08))*, 2008.

[5] W. Zhang, M. Tran, S. Zhu, and G. Cao. A random perturbation-based scheme for pairwise key establishment in sensor networks. *The 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc'07)*, 2007.