Recent Research in Smart Grid Communication Infrastructures and Cyber Security

Yi Qian

Department of Electrical and Computer Engineering
University of Nebraska, NE, USA

E-mail: yi.qian@unl.edu
Web: cns.unl.edu/yqian

October 18, 2016
Introduction to Smart Grid
Motivations & Objectives of Smart Grid

- Higher Penetration of Renewables
- Smart Charging of Electric Vehicles
- Consumers to Control Energy Bills
- Efficient Grid Operations & Reduced Losses
- Reduced Distribution Outages
- Improved System Reliability & Security

- Increased productivity
- Improved utilization
- Lower Greenhouse Gas Emission
- Facilitated renewable resource generation
- Enhanced customer experience
- Adherence to regulatory constraints
What is Smart Grid?

- An upgrade on upgrading generation, transmission, and distribution systems
- Incorporating advanced information and communications technologies (ICT) and control
- DoE defines Smart Grid in terms of key functions
  - Enabling active participation by consumers to adjust consumption based on price and overall demand
  - Better matching generation and demand
  - Integrating renewable (e.g., solar, hydro, wind, etc.) and distributed power generation sources
  - Providing more and better energy storage options
  - Improving power quality, reliability, and enhancing resiliency: wide area situational awareness (WASA)
The ICT Framework in Smart Grid
Proposed ICT Framework

(Big) Data Analytics

Information and Communication Technologies (ICT)
Two-way communications

RAW DATA

USEFUL INFO

- Smart devices
- Other information sources
- Weather forecast
- Social Network
- Stock Market
- Private Network
- Internet
- Local area network

Smart meters

Customers

Remote Control

Partial metering data

Metering data

Real-time DL

Real-time pricing

Pricing forecast

Service provider/Utility company

Local control center 1

Local control center 2

Authentication Center & PKG

Conventional energy sources

Renewable energy sources

Energy storage unit

Power Generators

Monitoring data

Real-time DLC

Pricing forecast

Energy forecast

Monitoring data

Real-time DL

Real-time pricing

Pricing forecast

Monitoring data

Real-time DLC

Pricing forecast

Energy forecast
Networks in the ICT Framework

• Private networks: deployed by utility companies
  • Networks in the advanced metering infrastructure (AMI)
    • Metering data gathering
    • Demand response control message distribution
  • Networks in the wide area monitoring systems (WAMS)
    • Monitoring data gathering
    • Controlling message distribution
  • Etc.

• Public networks: Internet based public network service
  • Remote monitoring and control from smart phones
    • E.g., smart appliances that have Wi-Fi connection to the Internet
  • Data transmission through cellular network service
    • E.g., transactional data from EVs
  • Applying public cloud computing service
    • For big data analytics
  • Etc.
Advanced Metering Infrastructure (AMI)

Advanced metering infrastructure (AMI) enables two-way communication between utilities and customers.
A PMU-based approach to operate ADNs

Monitoring infrastructure components:

- Phasor Measurement Unit (PMU)
- Feeder Monitoring, Control Unit (PDC+RTSE+control+protection)

Source: http://sine.ni.com/cs/app/doc/p/id/cs-16856#prettyPhoto
Smart Appliances

Security in the ICT Framework
Security Requirements

<table>
<thead>
<tr>
<th></th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Non-repudiation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Demand Response</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pricing forecast</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Energy forecast</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Metering data</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Wide Area Monitoring System</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring data</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Control message</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Cloud Computing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-processed data</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Raw energy forecast</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>External Sources</strong></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Other information</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Various types of data in smart grid communications have different security requirements as well as delay requirements.
Security Mechanisms

Initial authentication process
- A supplicant sends request to all of its active neighboring nodes
- The active neighboring nodes relay the request to the AS

Detailed process

- Authentication and key management process for private networks.
  - Illustrated with DAPs in AMI as communication nodes
Security Mechanisms (cont’d)

Security scheme for uplink transmission (single link).

Security scheme for uplink transmission (multi link aggregation).

• Security schemes in uplink and downlink transmissions.
Security Mechanisms (cont’d)

Security scheme based on zero-knowledge proof for the proposed distributed learning technique.

1: \( M_1 = H\left(y_k\right) \parallel tsp \)

4: \( M_4 = M_1 \parallel M_3 \parallel tsp' \)

2: \( M_2 = E(M_1; P_k^-) \)

3: \( M_3 = H(G) \)

5: \( M_5 = E(M_4; P_k^-) \)

6: Retrieve Dk’s pub key \( P_k^+ \)

7: \( D(M_5; P_k^+) \)

8: \( \begin{cases} Dk \rightarrow legitimate \\ Dk \rightarrow malicious \end{cases} \)
Security Mechanisms

• For internal data transmission over the Internet
  • Utility company does not have complete control
    – Huge amount of sensitive data goes through uncontrollable networks (by power companies)
  • How to protect such transmission?
    – We proposed to use identity-based security schemes to assist existing security schemes in the Internet and cloud computing servers
      – More efficient security parameter management
      – More control on the side of utility company

  • Anyone in the domain can generate public keys of other parties
  • Public keys are refreshed easily

• Private keys are generated by private key generator (PKG)
• Outdated private keys are easily revoked
### Proposed ID-Based Signcryption

#### Preliminaries

**Bilinear mapping:** \( \hat{\epsilon} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2 \)

- **Bilinearity:** \( \hat{\epsilon}(aP, bQ) = \hat{\epsilon}(P, Q)^{ab} \) for all \( P, Q \in \mathbb{G}_1 \) and \( a, b \in \mathbb{Z}_q^* \).
- **Non-degeneracy:** for any \( P \in \mathbb{G}_1 \), \( \hat{\epsilon}(P, Q) \neq 1 \) for all \( Q \in \mathbb{G}_1 \setminus \{0\} \).
- **Computability:** there is a polynomial time algorithm for computing \( \hat{\epsilon}(P, Q) \) for all \( P, Q \in \mathbb{G}_1 \).

#### Proposed ID-based signcryption scheme

**Setup:** The PKG chooses groups \((\mathbb{G}_1, \mathbb{G}_2)\) of prime order \( q\), a generator \( g \) of \( \mathbb{G}_1 \), a randomly chosen master key \( s \in \mathbb{Z}_q^* \), a domain secret \( g_1 = sg \in \mathbb{G}_1 \). The PKG also chooses three cryptographic hash functions, \( H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1 \), \( H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^* \) and \( H_3 : \{0,1\}^* \rightarrow \{0,1\}^n \). The domain public parameters are \( \text{params} = \langle \mathbb{G}_1, \mathbb{G}_2, g, q, g_1, H_1, H_2, H_3, n \rangle \). Public key of the AS is \( p_{AS} = H_1(AS||\text{time}) \). Secret key of the AS is \( d_{AS} = sp_{AS} \).

**Keygen:** For a given string \( ID \in \{0,1\}^* \), and an expiration time stamp \( \text{time} \), the algorithm builds a public key \( p_{ID} \) and a private key \( d_{ID} \) as follows.

- **Public key:** \( p_{ID} = H_1(ID||\text{time}) \).
- **Private key:** \( d_{ID} = sp_{ID} \).

Note that \( \text{time} \) is concatenated to \( ID \) without loss of generality. Other process can be taken for the same purpose, e.g., \( \text{time} \) can also be XORed to \( ID \).

**Signcrypt:** Sender A signcrypts message \( M \) in the steps as follows.

1. A picks a random value \( r \in \mathbb{Z}_q^* \), computes \( U = rg \in \mathbb{G}_1 \) and \( h_1 = H_2(M||A||U) \in \mathbb{Z}_q^* \).
2. sets \( V = d_A h_1 + rg_1 \in \mathbb{G}_1 \);
3. computes \( p_B = H_1(B||\text{time}) \), \( h_2 = H_2(A||B) \in \mathbb{Z}_q^* \) and \( X = h_2U \in \mathbb{G}_1 \);
4. computes \( h_3 = H_3(X||\hat{\epsilon}(rg_1, h_2p_B)) \);
5. sets \( W = M \oplus h_3 \);
6. final output is \( \langle U, V, W, X \rangle \).

Note that in the 4-tuple cipher text \( \langle U, V, X, W \rangle \), \( \sigma = \langle U, V \rangle \) is for digital signature and \( C = \langle W, X \rangle \) is for ciphertext.

**Decrypt:** Upon receiving \( \langle \sigma, C \rangle \), receiver B decrypts \( M \) in the steps as follows.

1. B computes \( h_3^* = H_3(X||\hat{\epsilon}(X, d_B)) \);
2. decrypts \( M = W \oplus h_3^* \).

**Verify:** After getting \( M \), B continues to verify the digital signature in the steps as follows.

1. computes \( p_A = H_1(A||\text{time}) \), and \( h_1 = H_2(M||A||U) \);
2. verifies if \( \hat{\epsilon}(g, V) = \hat{\epsilon}(g_1, p_A h_1 + U) \).
Analysis of the IBSC Scheme

Security analysis

The security of the proposed IBSC is based on the following computational problems

• **Computational Diffie-Hellman Problem:** given $P, aP, bP, cP \in G_1$, $\forall a, b, c \in Z_q^*$, there is no polynomial time algorithm to compute $abP \in G_1$

• **Bilinear Diffie-Hellman Problem:** given $P, aP, bP, cP \in G_1$, $\forall a, b, c \in Z_q^*$, there is no polynomial time algorithm to compute $\hat{e}(P, P)^{abc} \in G_2$

Performance analysis

Modified Weil pairing is adopted to apply performance analysis Weil pairing $\hat{e}(P, Q)$ over supersingular elliptic curve $E : \{y^2 = x^3 + 1 | x, y \in \mathbb{F}_p\}$

Modified Weil pairing: $\hat{e}(P, Q) = e(P, \phi(Q))$

where $\phi(x, y) = (\zeta x, y)$ and $\zeta$ is a primitive cube root of unity in $\mathbb{F}_p$.

$p \equiv 2 \mod 3$

$p = aq - 1$, for some prime $p$ and positive integer $a$

$k_p$ is the multiplier in $G_1$

<table>
<thead>
<tr>
<th></th>
<th>$q = 256$ b</th>
<th>$q = 256$ b</th>
<th>$q = 385$ b</th>
<th>$q = 385$ b</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$k_p = 256$ b</td>
<td>$k_p = 512$ b</td>
<td>$k_p = 256$ b</td>
<td>$k_p = 512$ b</td>
</tr>
<tr>
<td>Signcrypt</td>
<td>39.59 ms</td>
<td>68.89 ms</td>
<td>45.4 ms</td>
<td>74.7 ms</td>
</tr>
<tr>
<td>Decrypt</td>
<td>7.44 ms</td>
<td>7.44 ms</td>
<td>13.25 ms</td>
<td>13.25 ms</td>
</tr>
<tr>
<td>Sign</td>
<td>19.29 ms</td>
<td>36.87 ms</td>
<td>19.29 ms</td>
<td>36.87 ms</td>
</tr>
<tr>
<td>Verify</td>
<td>28.75 ms</td>
<td>34.61 ms</td>
<td>46.18 ms</td>
<td>52.04 ms</td>
</tr>
</tbody>
</table>

Intel Core i5 @ 3.1 GHz & 8G RAM
Possible Applications of the Proposed IBSC Scheme

• Short message encipherment
• Digital signature
• Session key distribution
• Signing right delegation

Signing right delegation
• When a local control center is under maintenance
• Not available due to cyber attack/natural disaster
• Etc.
Future Research Directions
Future Research Directions

• Optimization of renewable power source deployment and operation
  • To better accommodate the management of fossil fuel based power sources

• Fast and reliable learning techniques for big data analytics
  • Power consumption analysis
  • Smart pricing analysis
  • Real time anomaly detection (e.g., PMU data)

• Large scale graph modeling techniques
  • To better analyze the relationship among pieces of information

• Parallel computing and cloud computing
  • To speed up computation
  • To enhance scalability
Future Research Directions (cont’d)

• Better integration of EVs
  • Fast vehicular network for data exchange
  • (Near) real-time big data analytics for EVs

• Cyber security
  • Fast privacy protection
    • without traditional encryption algorithms
    • Or fast encryption algorithms
  • Real-time data integrity protection
    • Real-time anomaly detection, etc.
  • Cloud security

• Etc.
Conclusion
Conclusion

• Smart grid is a massive cyber physical system
• Advanced ICT are applied in smart grid communication infrastructures
• Smart grid generates big data
• Big data analytics is important to DR, monitoring system, and other applications in smart grid
• Many issues remain open in big data research of smart grid communications

Acknowledgement

This work was supported by the National Science Foundation under the grant CNS-1423408
References


