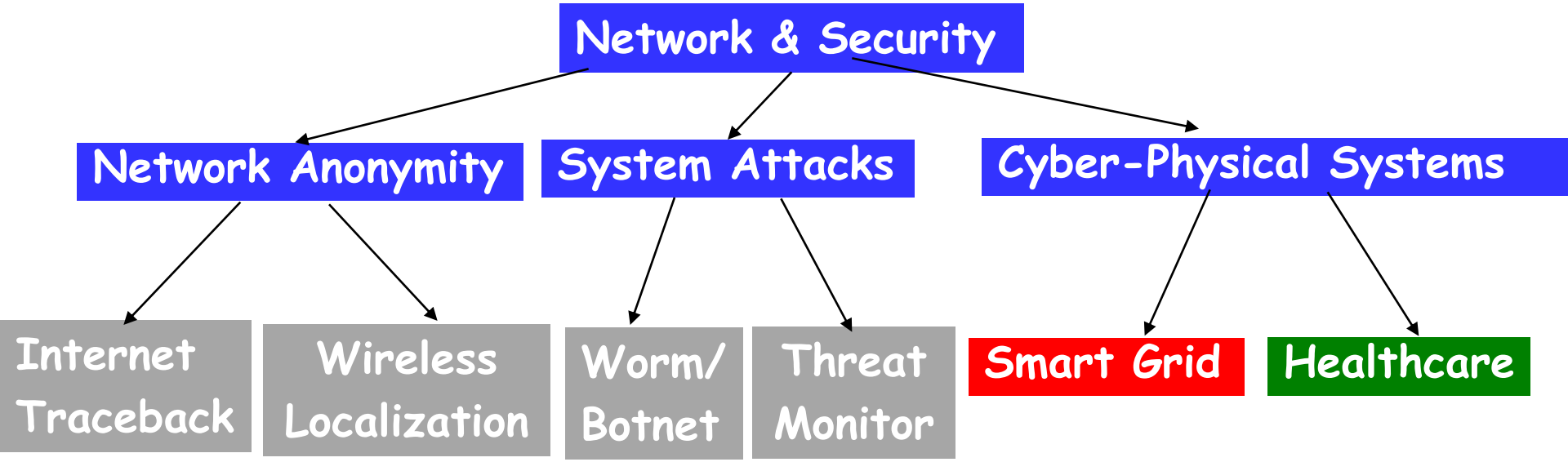
False Data Injection Attacks in Smart Grid: Challenges and Solutions

Dr. Wei Yu
Assistant Professor
Department of Computer & Information Sciences
Towson University
http://www.towson.edu/~wyu
Email: wyu@towson.edu

Research Projects



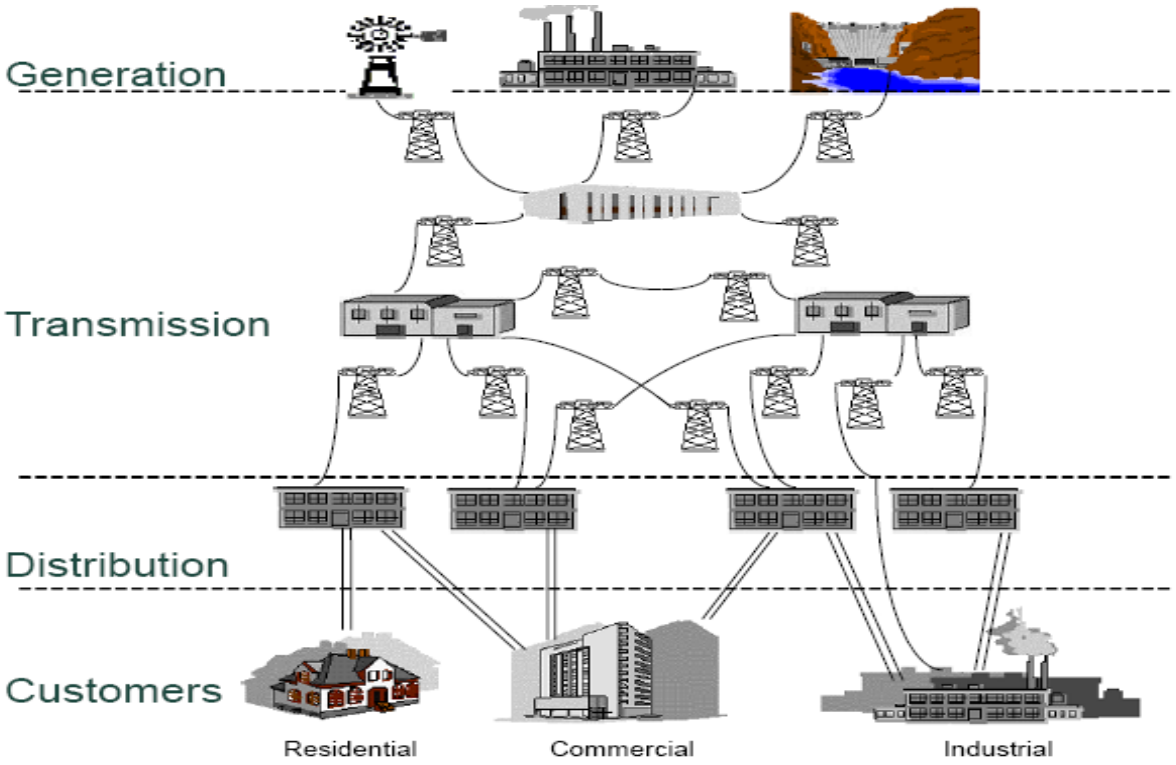
1. Qinyu Yang, Jie Yang, Wei Yu, Nan Zhang, and Wei Zhao, "False Data Injection Attack Against Power System State Estimation: Modeling and Defense", in Proceedings of IEEE Globecom 2011 (journal version is under submission to IEEE TPDS)
2 Jie Lin, Wei Yu, Guobin Xu, Xinyu Yang and Wei Zhao, "On False Data Injection Attacks against Distributed Energy Routing in Smart Grid," in Proceedings of IEEE/ACM International Conference on Cyber Physical System (ICCPS), 2012.
3. Xinyu Yang, Jin Lin, Paul Moulema, Wei Yu, Xinwen Fu, and Wei Zhao, "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems," in Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS), 2012.

http://www.towson.edu/~wyu

Outline

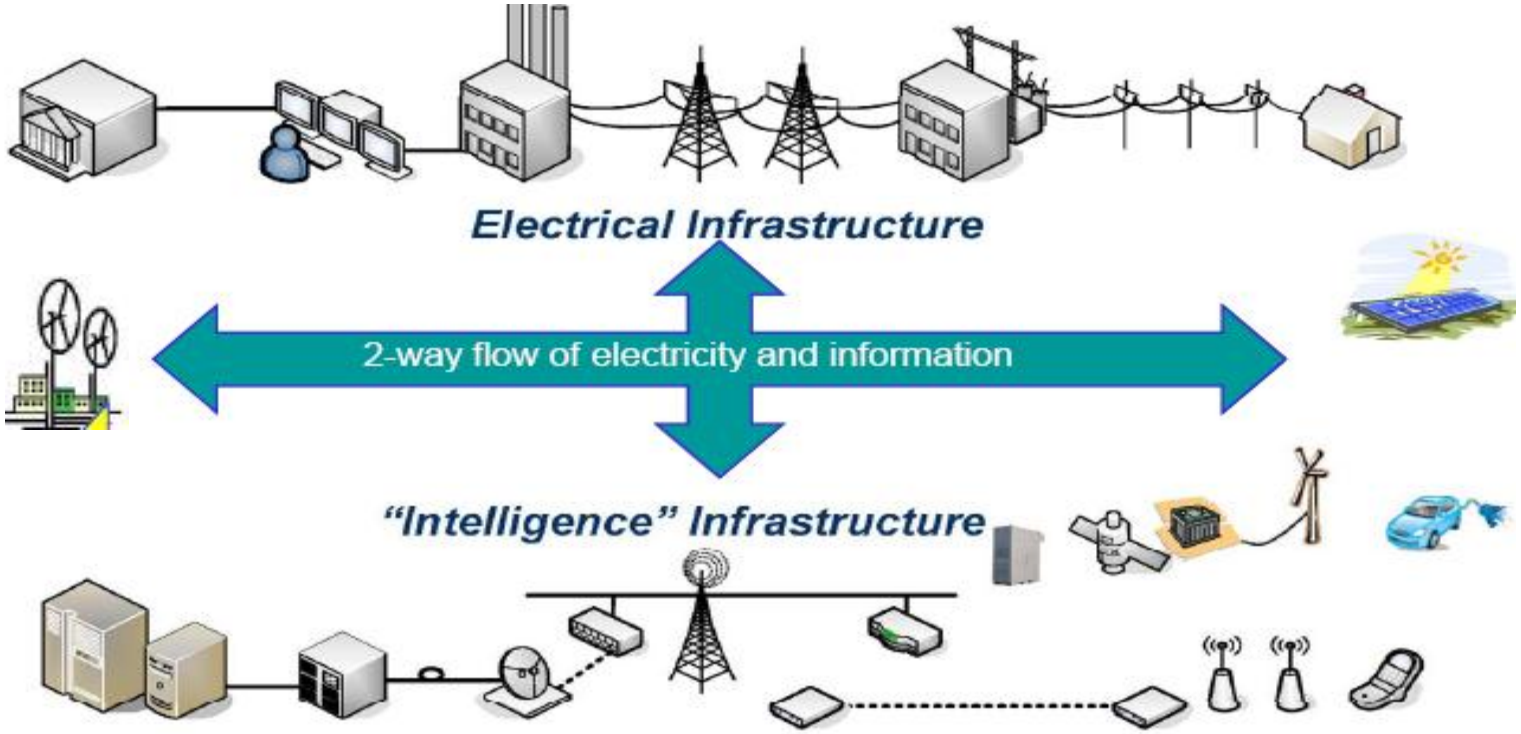
- Overview
- False Data Injection Attack against Grid System State Estimation
- False Data Injection Attack against Energy Distribution
- Final Remarks

Traditional Grid



- Centralized one way electricity delivery from generation to end-users
- Over-provision energy generation and load control
- Limited automation and situational awareness
- Lack of customer-side management

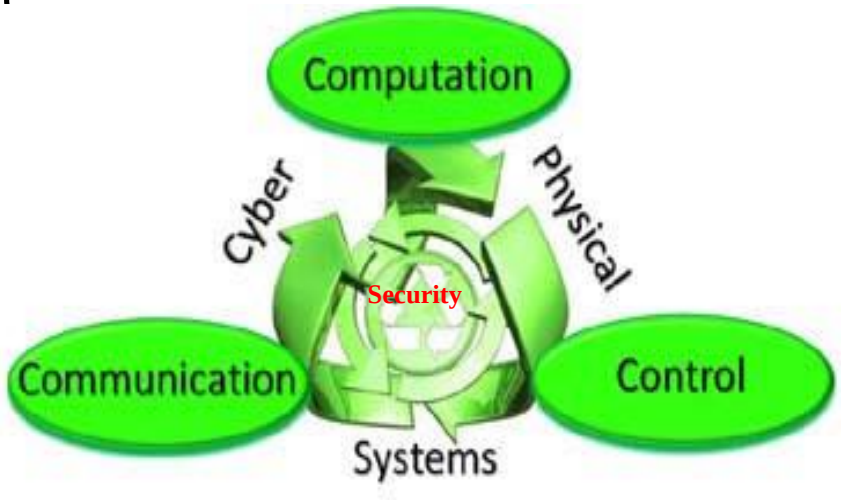
Smart Grid: An Energy-based Internet



- Smart Grid will comprise a vast array of devices and systems with two-way communication and control capabilities
- An energy-based Internet

Smart Grid as an Energy-based Cyber-Physical System (CPS)

- Cyber – computation, communication, and control that are discrete, logical, and switched
- Physical – natural and human-made systems governed by the laws of physics and operating in continuous time
- Cyber-Physical Systems – systems in which the cyber and physical systems are tightly integrated at all scales and levels
- **Smart grid is a typical CPS**, which integrates a physical power transmission system with the cyber process of network computing and communication



Key Services in Smart Grid (NIST)

- **Energy distribution management:** Making the energy distribution system more intelligent, reliable, self-repairing, and self-optimizing
- **Distributed renewable energy integration:** Integrating distributed renewable-energy generation facilities, including the use of renewable resources (i.e., wind, solar, thermal power, and others)
- **Distributed energy storage**: Enabling new storage capabilities of energy in a distributed fashion, and mechanisms for feeding energy back into the energy distribution system
- **Electric vehicles-to-grid**: Enabling large-scale integration of plug-in electric vehicles (PEVs) into the transportation system
- **Grid monitoring and management**: Enabling the demand response and consumer energy efficiency
- **Smart metering infrastructure**: Providing customers real-time (or near real-time) pricing of electricity and can help utilities achieve necessary load reductions

Real-World Cyber Attacks in Smart Grid

- Cybercriminals compromise computers anywhere they can find them (even in smart grid systems)
  - January 2003, computers infected by the Slammer worm shut down safety display systems at power plant in Ohio
- Disgruntled employees can be the major source of targeted computer attacks against systems
  - Contractor launches an attack on a sewage control system in Queensland in 2000
  - More than 750,000 gallons of untreated sewage released into parks, rivers, and hotel grounds
- Terrorists, activists, and organized criminal groups
  - In 2008, there was evidence of computer intrusions into some European power utilities
  - In 2010, Stuxnet worm provides a blueprint for aggressive attacks on control systems

False Data Injection Attacks

- Smart grid may operate in hostile environments
- Meters and sensors lacking tamper-resistance hardware increases the possibility to be compromised
- The adversary may inject false measurement reports to the disrupt the smart grid operation through the compromised meters and sensors
- Those attacks denoted as **false data injection attacks**
  - It can disrupt the grid system state estimation
  - It can disrupt the energy distribution

Outline

- Overview
- False Data Injection Attack against Grid System State Estimation
- False Data Injection Attack against Energy Distribution
- Final Remarks

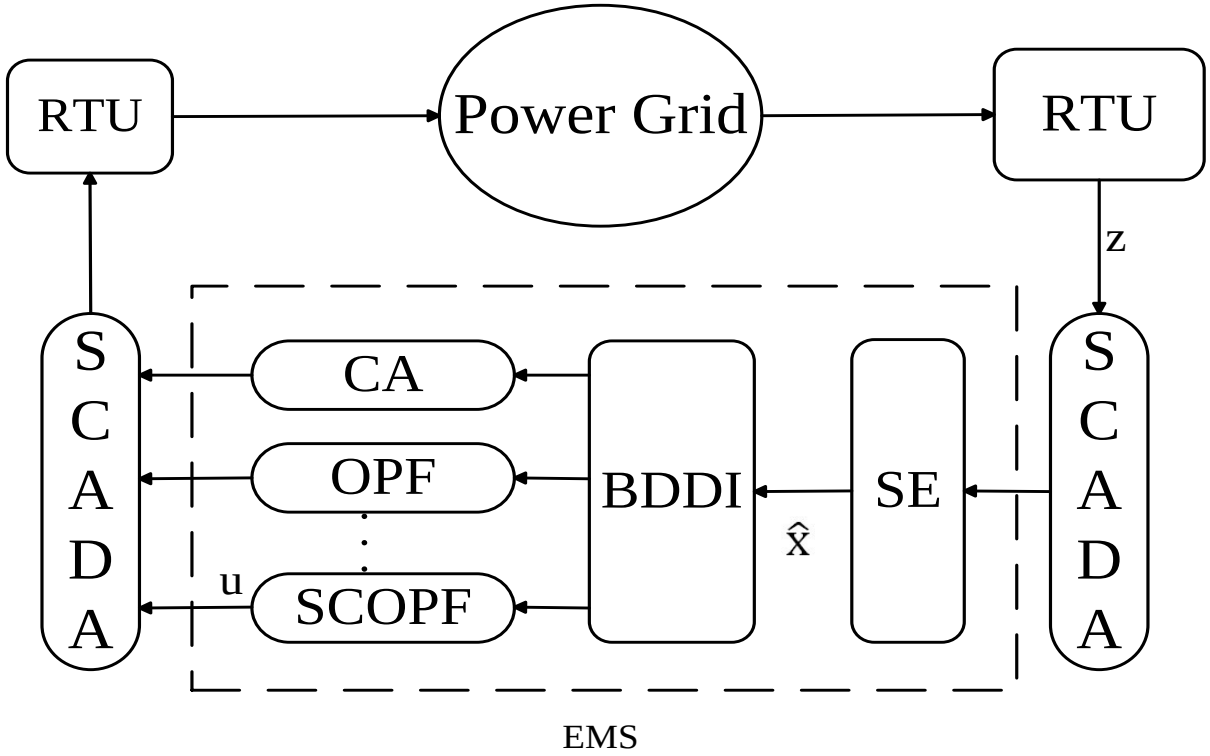
Objectives

- Smart grid shall provide reliable, secure, and efficient energy transmission and distribution
- State estimation is a very critical component in power grid system operation
  - Used by Energy Management Systems (EMS) at the control center to ensure that the power grid is in the desired operation states
- Objectives of this research
  - Modeling the false data injection attacks against power system state estimation
  - Studying countermeasures against such attacks

Power System Operation

- The operation condition of a power grid over time can be determined if the network model and voltages at every system bus are known.
- State estimator (SE) uses Supervisory Control and Data Acquisition (SCADA) data and system model to estimate the system states (e.g., voltages at all system buses) in real time.

State Estimation Process



EMS: Energy management system
RTU: Remote terminal unit
BDDI: Bad data detection and identification
CA: Contingency analysis
OPF: Optimal power flow
SCOPF: Security constrained OPF

Algorithm for State Estimation

- The state estimation can be formalized by

$$\mathbf{z} = h(\mathbf{x}) + \mathbf{e}$$

z: Measurement vector (bus voltages, bus active an reactive power flows, and branch active and reactive power flows)

x: State vector (bus voltage magnitudes & phase angles)

h(x): Nonlinear vector function determined by the system topology

e: Error vector, cov(e)=R

- Most existing state estimators use a weighted least squares (WLS) method to minimize the objective error function

$$\min_{\mathbf{x}}: \ J(\mathbf{x}) = [\mathbf{z}\text{-}h(\hat{\mathbf{x}})]^T \mathbf{R}^{-1} [\mathbf{z}\text{-}h(\hat{\mathbf{x}})]$$

Bad Data Detection and Identification

- What is bad data?
  - Random errors can be filtered by the state estimator
  - Large measurement errors occur when meters have biases, drifts or wrong connections

- How to deal with bad data?
  - Detection and identification of bad data are done only after the estimation process by processing the measurement residuals
  - Largest normalized residual (LNR) test: the presence of bad data is determined by a hypothesis test if

$$\mathbf{J}(\mathbf{x}) = \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|^2_{\mathbf{R}^{-1}} \geq \tau.$$

False data Injection Attacks

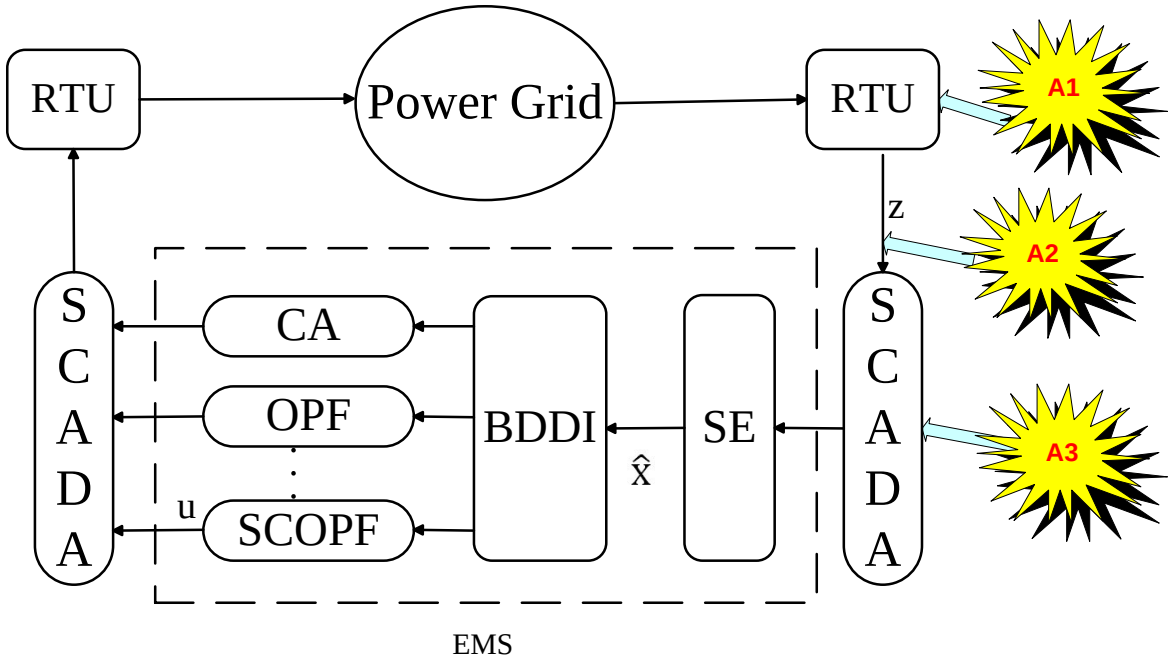
- Liu et al., "False data injection attacks against state estimation in electric power grids," in Proceedings of ACM Computer Communication Security (CCS), November 2009
- By taking advantage of the configuration information of a power system, the adversary can inject malicious measurements
  - Mislead the state estimation process without being detected by existing bad data detection techniques.

$$\mathbf{z}_a = \mathbf{z} + \mathbf{a}, \hat{\mathbf{x}}_{bad} = \hat{\mathbf{x}} + \mathbf{c}$$

$$\begin{aligned} \left\| \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_{bad} \right\| &= \left\| \mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c}) \right\| \\ &= \left\| \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{H}\mathbf{c}) \right\| \\ &= \left\| \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \right\| \end{aligned}$$

$$\textit{when} \quad \mathbf{a} = \mathbf{H}\mathbf{c}$$

False data Injection Attacks



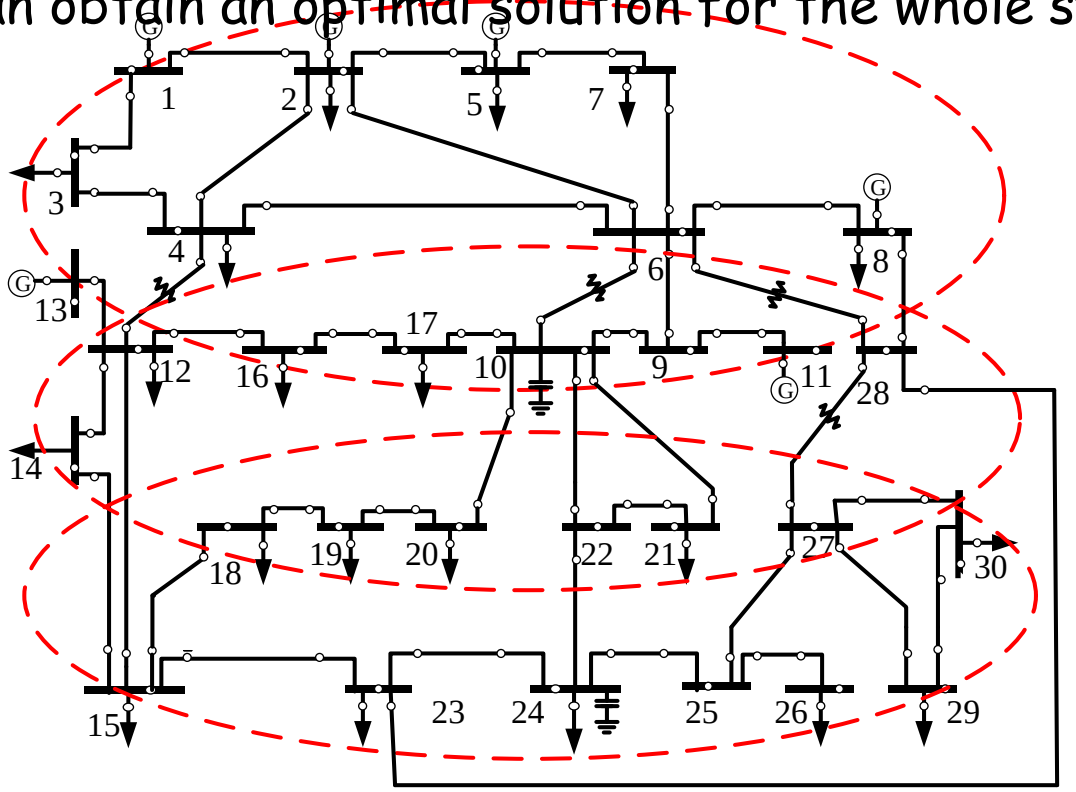
- Assumptions
  - The adversary has an accurate model of the power system
  - The adversary knows the state estimation and bad data detection methods
  - The adversary will compromise as few meters as possible

Our Contributions

- When the attackers are constrained to inject false data into specific number of state variables, what is the least number of meters should they compromise?
  - We develop a least-effort attack model to identify the optimal set of meters to launch false data injection attacks.
  - We show that the problem can be reduced to a NP-hard problem - minimum subadditive join problem.
  - We develop a heuristic algorithm to derive the results efficiently.
  - We develop countermeasures to defend against such attacks.

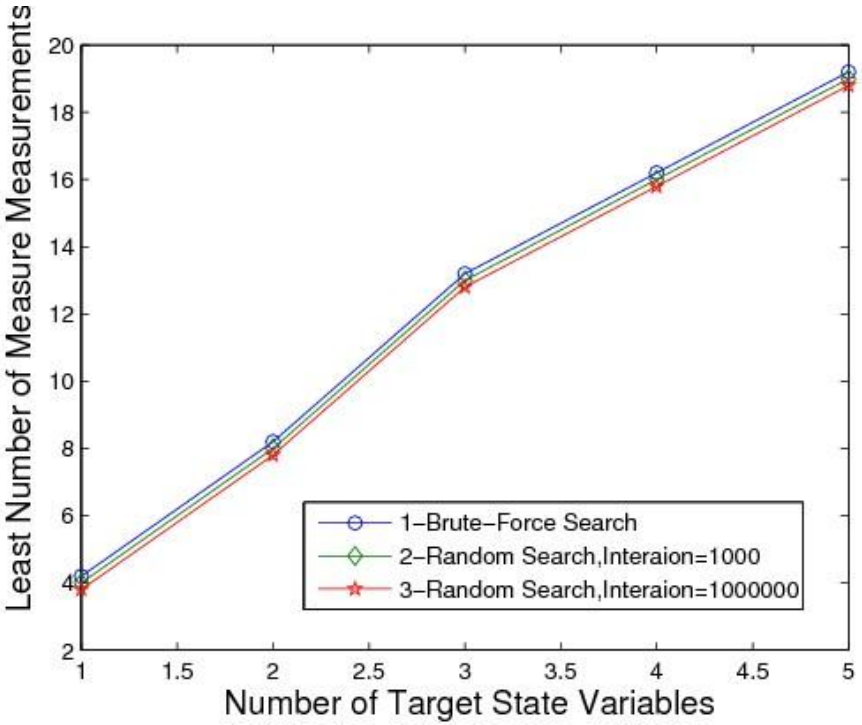
Hierarchical Approach

- We first divide the large-scale power system into N overlapping areas, find the suboptimal sets of sensor measurements in each area.
- We then can obtain an optimal solution for the whole system.

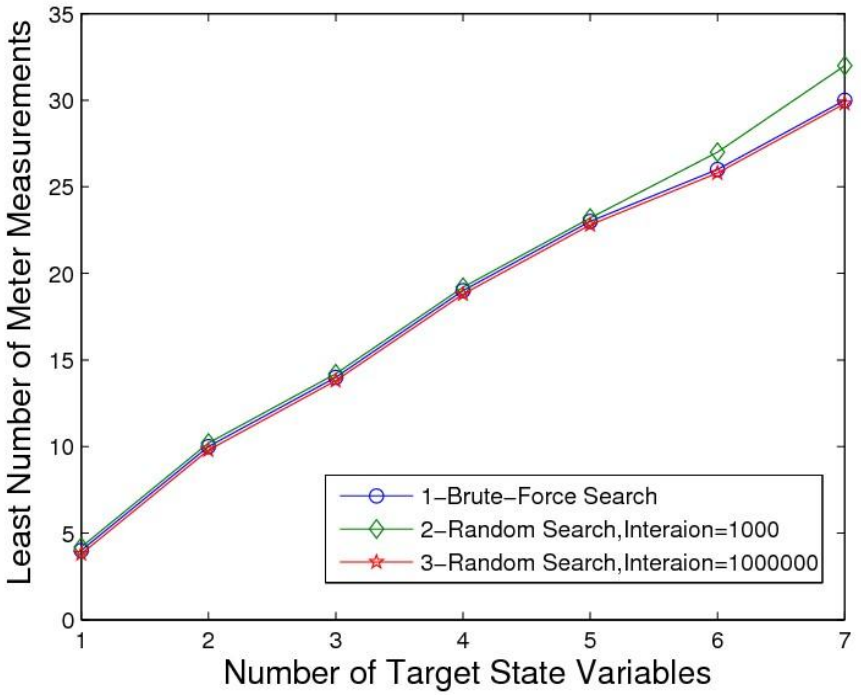


Example of IEEE 30-bus with Measurements

Performance of Brute-force Search

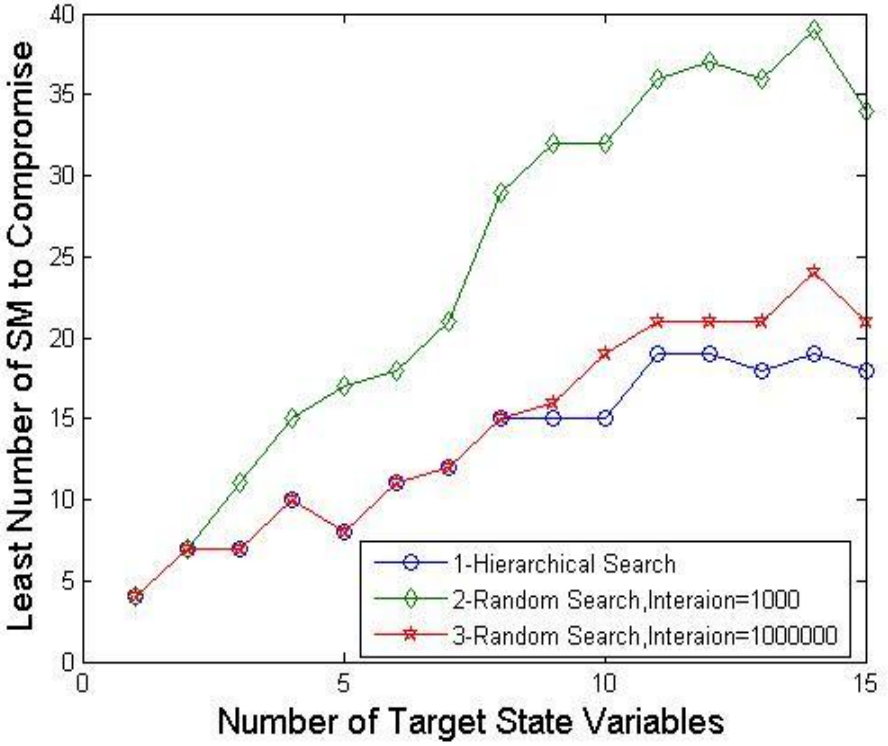


Brute-force Search for IEEE 9-bus

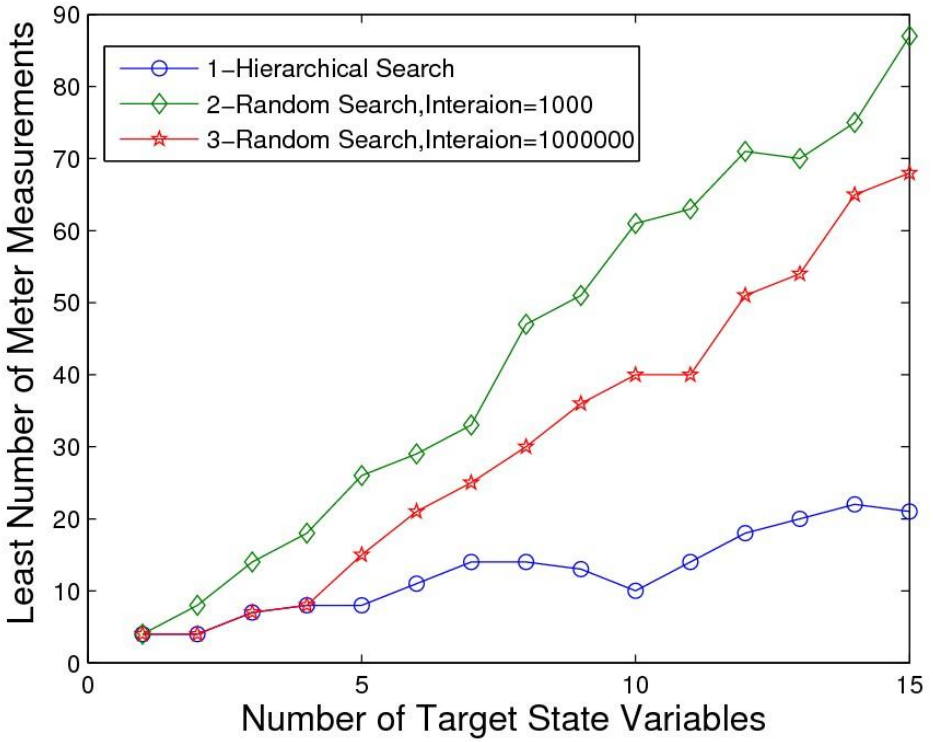


Brute-force Search for IEEE 14-bus

Performance of Hierarchical Search

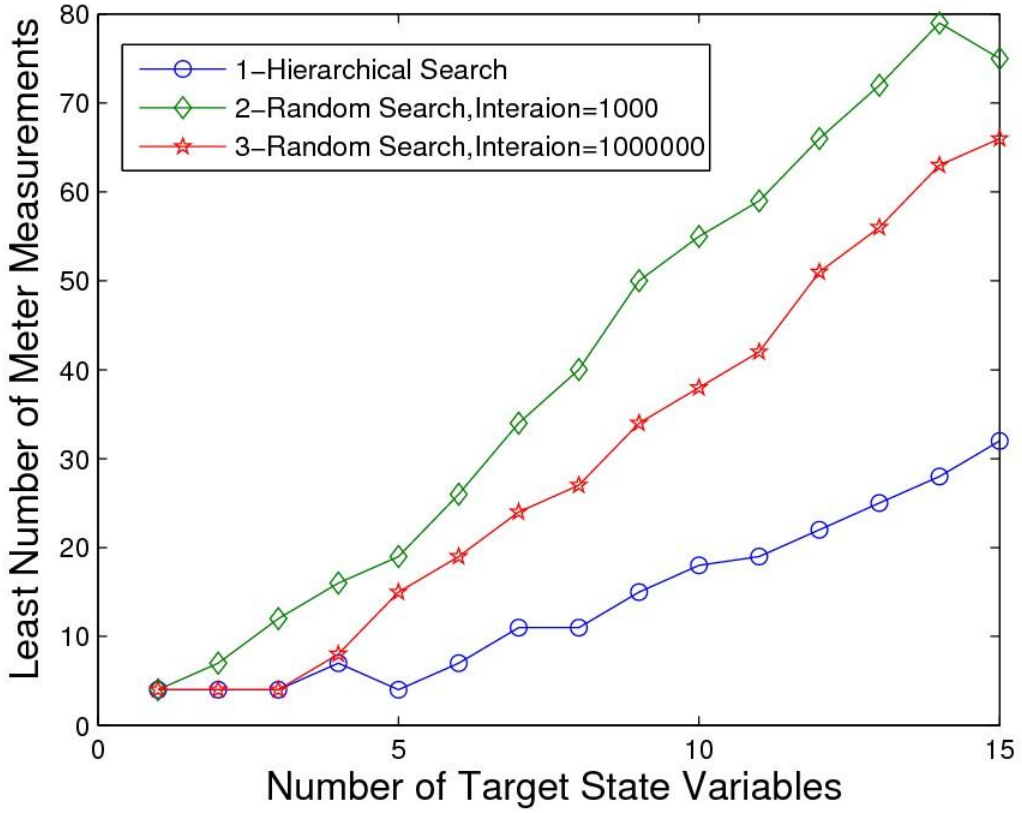


Hierarchical Search for IEEE 30-bus



Hierarchical Search for IEEE 118-bus

Performance of Hierarchical Search

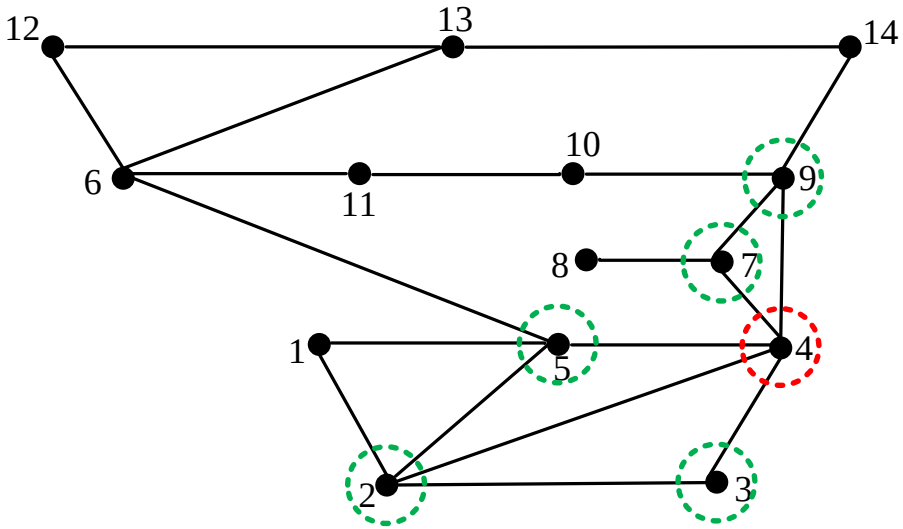


Hierarchical Search for IEEE 300-bus

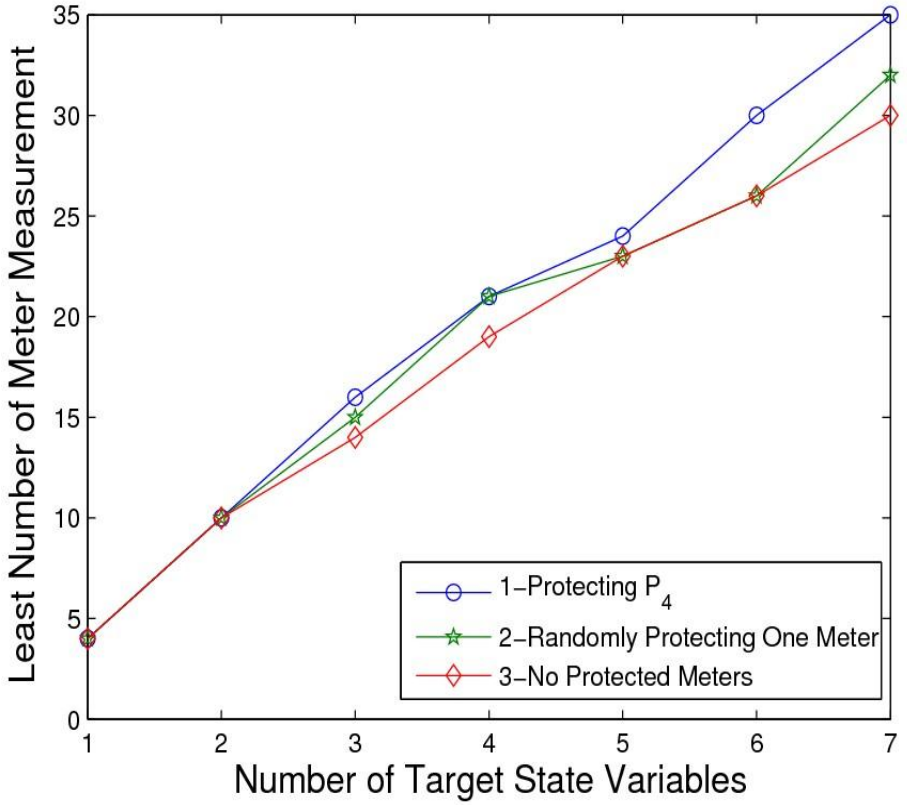
Countermeasures

- System Protection
  - Some of the measurement play a critical role in determining a specific state variable, while others are redundant to improve the accuracy of state estimation.
  - How to select a set of sensors to protect and make attacks difficult to deploy.
- Anomaly Detection
  - Spatial-based detection
    - Treat all the measurements received at a certain time as a unity and the accumulated deviation of all compromised measurements will be significant.
  - Temporal-based detection
    - Consider the fact that the adversary needs to manipulate sensor measurements over time
    - Develop the nonparametric cumulative sum (cusum) change detection technique.

Preliminary Evaluation Results



Topology of IEEE 14-bus System



Ongoing Research

- Attacks in dynamic state estimation
  - The dynamic state estimation can obtain complete, coherent, and real-time dynamic states.
  - We investigate attack schemes against dynamic state estimation and countermeasures.

- Attacks against control algorithms
  - Applications such as contingency analysis, optimal power flow, and economic dispatch can be the target.
  - Attacks will make the control center generate false control signals.

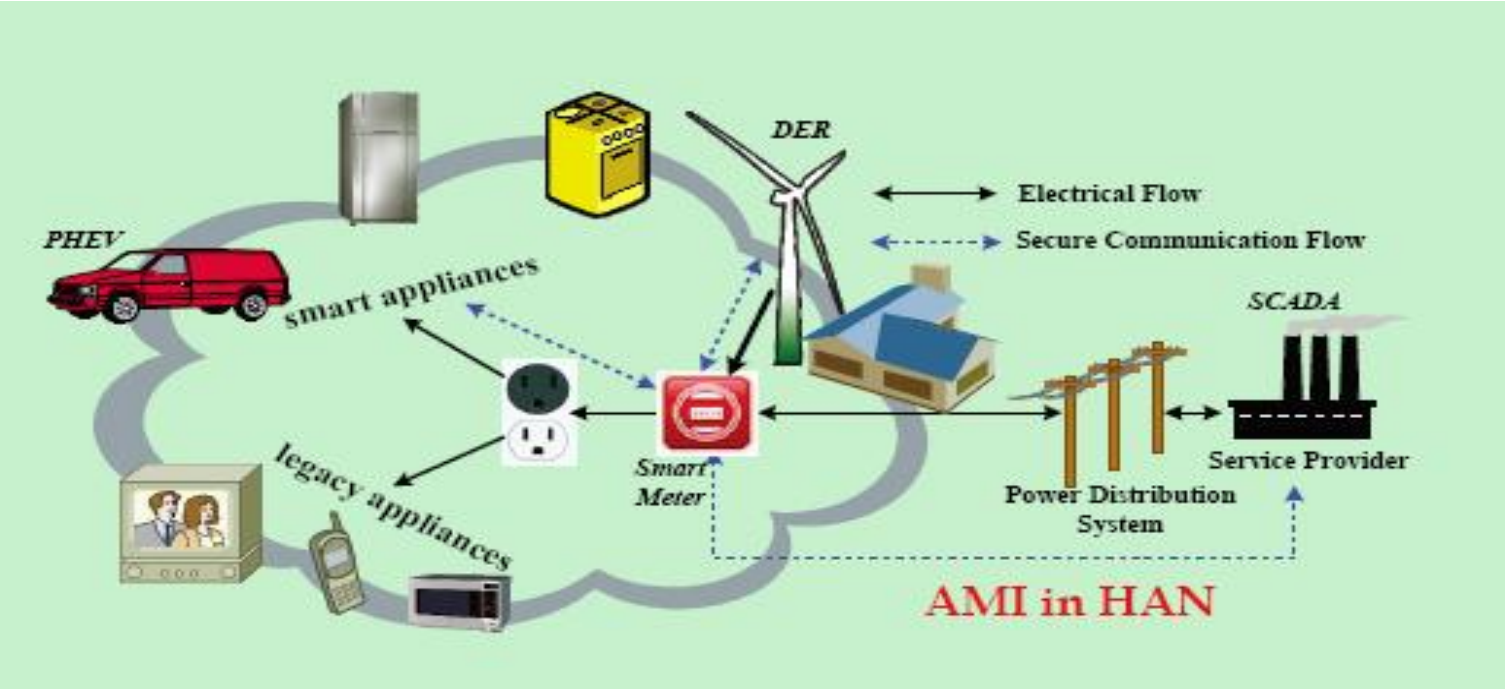
Outline

- Overview
- False Data Injection Attack against Grid System State Estimation
- False Data Injection Attack against Energy Distribution
- Final Remarks

Objectives

- Smart grid shall provide reliable, secure, and efficient energy transmission and distribution
  - Efficiently utilize the distributed energy resources
  - Minimize the energy transmission overhead
- Objectives of this research
  - Study the vulnerability of distributed energy routing process
  - Investigate false data injection attacks against the energy routing process

Smart Meters



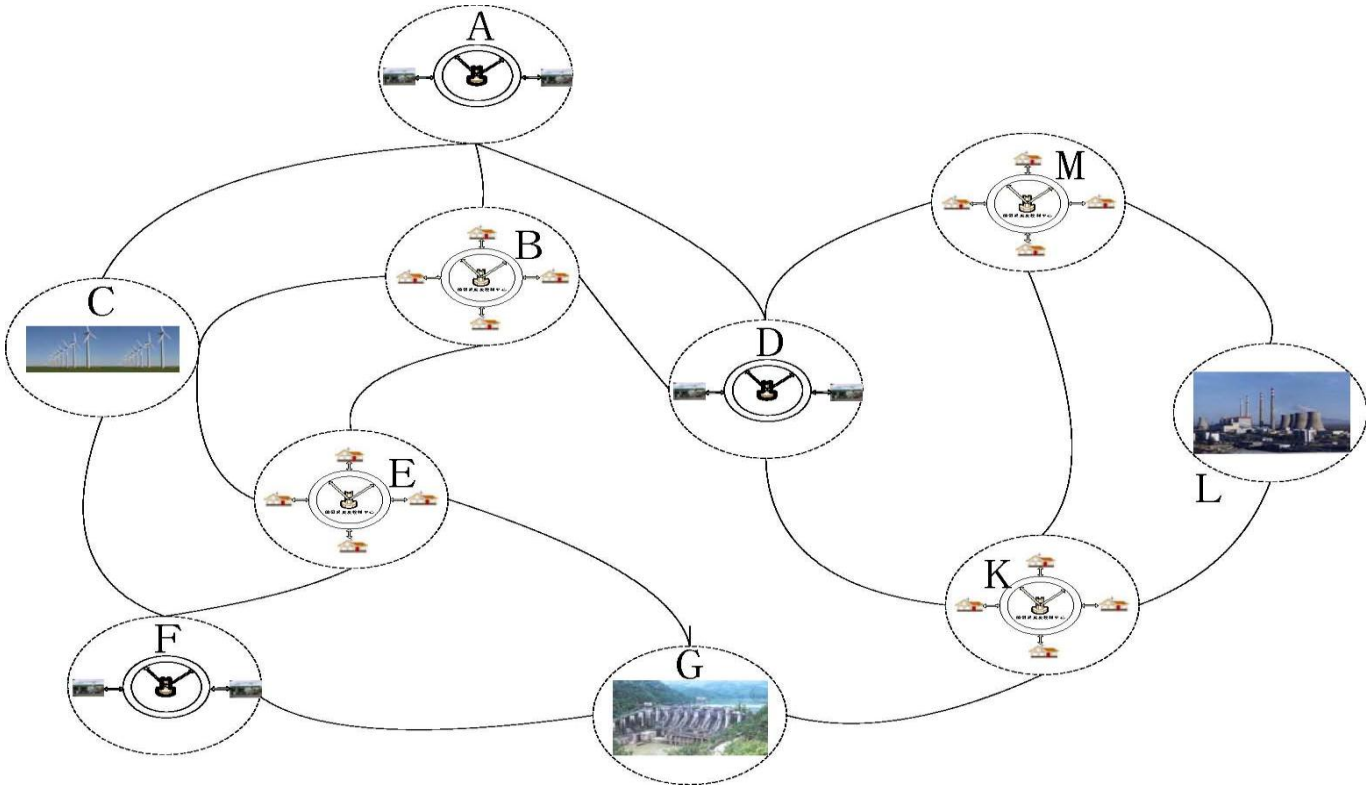
- Smart meter computes consumption and sends the information to utility for monitoring and billing purpose.
- Smart meter has the ability to disconnect-reconnect remotely and control the user appliances and device to manage load and demands.
  - Examples: reduce bill for customer & optimize power flow for utility

Attacks against Smart Meters

- Smart meter is "computer" and all cyber attacks can be applied
- Widespread use of smart meters
- A potentially large number of opportunities for the adversary
  - Forging the demand request of a smart meter (e.g., requesting a large amount of energy).
  - Misleading the electric utility into making incorrect decision about local or regional usage and capacity.
  - Nightmare scenario: deployed millions of smart meters and controlled by adversary
    - Interrupt the supply/demand process and cause disastrous consequences

Network Model

- The input energy of demand-nodes should be equal to their demanded energy.
- The output energy of supply-nodes should be less than energy that they could provide to the grid.
- The energy transmitted on a link should be less than the link capacity.



Distributed Energy Management

- The formalization of distributed energy management is

$$\textit{Objective.} \quad Min\left(Cost = \frac{1}{2}\sum_{l_{ij}\in L} Cost_{ij}\cdot E_{ij} \right)$$

$$S.t.\begin{cases} \forall v \in N_P & \sum_{i\in N_v} E_{vi} \le P_v \\ \forall u \in N_D & \sum_{j\in N_u} E_{uj} = -D_u \\ \forall l_{ij} \in L & E_{ij} = -E_{ji} \\ \forall l_{ij} \in L & \left|E_{ij}\right| \le Load_{ij} \end{cases}$$

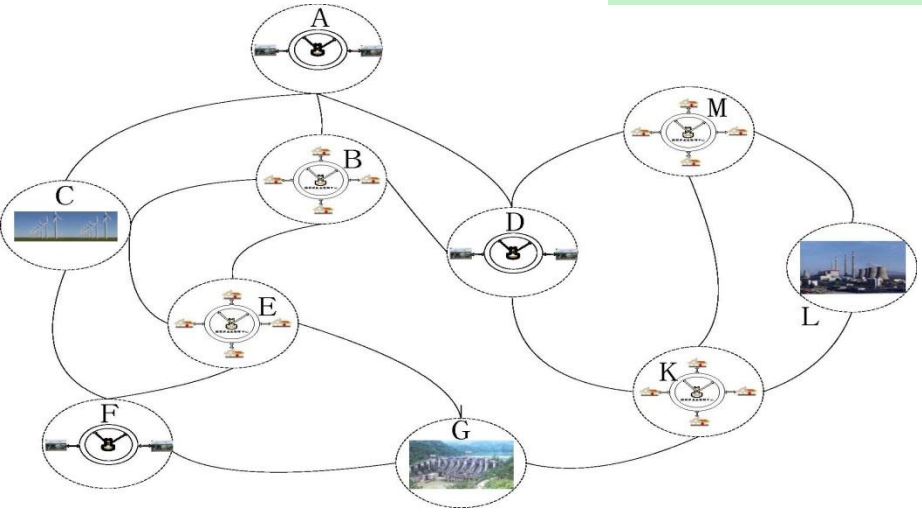
E_{ij} is the energy transmitted on link L_{ij};
N_P is the supply-nodes set;
N_D is the demand-nodes set;
P_v is the residual energy of node v;
D_u is demanded energy of node u.
$Load_{ij}$ is the link capacity of link L_{ij}

Example

$$\textit{Objective.} \quad \textit{Min}\left\{\textit{Cost}\left(\frac{1}{2}\cdot\sum_{E_{IJ}}\left(|E_{IJ}|\cdot Cost_{IJ}\right)\right)\right\}$$

$$\textit{S.t.}$$

$$\begin{cases}
E_{AC}+E_{AB}+E_{AD}=-D_A \\
E_{DA}+E_{DB}+E_{DK}+E_{DM}=-D_D \\
E_{FC}+E_{FE}+E_{FG}=-D_F \\
E_{CE}+E_{CA}+E_{CF}+E_{CB}\le P_C \\
E_{BC}+E_{BA}+E_{BE}+E_{BD}\le P_B \\
E_{EC}+E_{EB}+E_{EF}+E_{EG}\le P_E \\
E_{MD}+E_{ML}+E_{MK}\le P_M \\
E_{LM}+E_{LK}\le P_L \\
E_{KM}+E_{KD}+E_{KL}+E_{KG}\le P_K \\
\forall E_{IJ}, \quad E_{IJ}+E_{JI}=0 \\
\forall E_{IJ}, \quad 0\le|E_{IJ}|\le Load_{IJ}
\end{cases}$$



A, D, and F are demand nodes

Others are supply nodes

False data Injection Attacks

- **Injecting False Energy Data**
  - Energy-request Deceiving Attack
    - The adversary compromises demand-nodes and injects forged quantity of demanded energy.
  - Energy-supply Deceiving Attack
    - The adversary compromises supply-nodes and injects forged quantity of energy that the supply-nodes could provide to the grid.
- **Injecting False Link-state Data**
  - Claiming invalid energy links as valid
  - Claiming valid energy links as invalid

Metrics

- Supplied energy loss
  - Energy loss due to forged energy data from energy supply perspective
- Energy transmission cost
  - The increased total energy transmission cost caused by forged energy data
- The number of outage users
  - Some users could be outage due to the unbalance energy distribution caused by attacks

Energy-request Deceiving Attack

- In this scenario, the formalization of compromised distributed energy management is

$$Objective. \quad Min\left(Cost^{*} = \frac{1}{2}\sum_{l_{ij}\in L} Cost_{ij}\cdot E_{ij} \right)$$

$$S.t.$$

$$\begin{cases} \forall v \in N_P \quad \sum_{i\in N_v} E_{vi} \le P_v \\ \forall u \in N_D \quad \sum_{j\in N_u} E_{uj} = -D_u \\ \forall u^{*} \in N_{D^{*}} \quad \sum_{j\in N_{u^{*}}} E_{u^{*}j} = -D^{*}_{u^{*}} \le T_E \\ \forall l_{ij} \in L \quad E_{ij} = -E_{ji} \\ \forall l_{ij} \in L \quad \left|E_{ij}\right| \le Load_{ij} \end{cases}$$

u* is the compromised demand-nodes;
$D^{*}_{u^{*}}$ is the forged demanded energy;
T_E is the threshold

Energy-request Deceiving Attack (cont.)

- **Supplied Energy Loss:**

$$\Delta D^n = \sum_{u_i \in N_{D^*}} D^*_{u_i} - D_{u_i}$$

When the grid has enough energy, the forged demanded energy will be provided by supply-nodes, and then the supplied energy loss would occur.

Energy-request Deceiving Attack (cont.)

- **Energy Transmission Cost**:

$$\Delta Cost_n = Min(Cost_n^*) - Min\left(Cost\right)$$

As the analysis in our paper, with the increase of forged demanded energy $D_{u^*}^*$, the energy transmitted on links would be increase, and we can always have $\Delta Cost_n > 0$. Hence, energy-request deceiving attack can certainly increase the energy transmission cost.

Energy-request Deceiving Attack (cont.)

- **The number of outage users:**

  With the objective of minimize the number of outage demand-nodes, the problem can be represented by

$$Objective. \qquad s = Min\left(\| N_D^{'} \|\right)$$

$$S.t.$$

$$\sum_{u \in N_D^{'}} D_u \geq \sum_{u \in N_D} D_u - \sum_{v \in N_P} P_v$$

$N_D^{'}$ is the set of outage users.

Energy-supply Deceiving Attack

- In this scenarios, the formalization of compromised distributed energy management is

$$Objective. \quad Min\left(Cost^{*} = \frac{1}{2}\sum_{l_{ij}\in L} Cost_{ij}\cdot E_{ij} \right)$$

$$S.t.$$

$$\begin{cases} \forall v \in N_P \quad \sum_{i\in N_v} E_{vi} \le P_v \\ \forall v^* \in N_{P^*} \quad \sum_{i\in N_{v^*}} E_{v^*i} \le P^*_{v^*} \\ \forall u \in N_D \quad \sum_{j\in N_D} E_{uj} = -D_u \\ \forall l_{ij} \in L \quad E_{ij} = -E_{ji} \\ \forall l_{ij} \in L \quad \left|E_{ij}\right| \le Load_{ij} \end{cases}$$

v* is the compromised supply-nodes;

$P^*_{v^*}$ is the forged energy that supply-node could provide to the grid.

Energy-supply Deceiving Attack

- Claiming more energy than supply-node can provide
  - Demand-node cannot obtain expected energy
- Claiming less energy than supply-node can provide
  - Increase energy transmission cost
  - Increase number of outage users

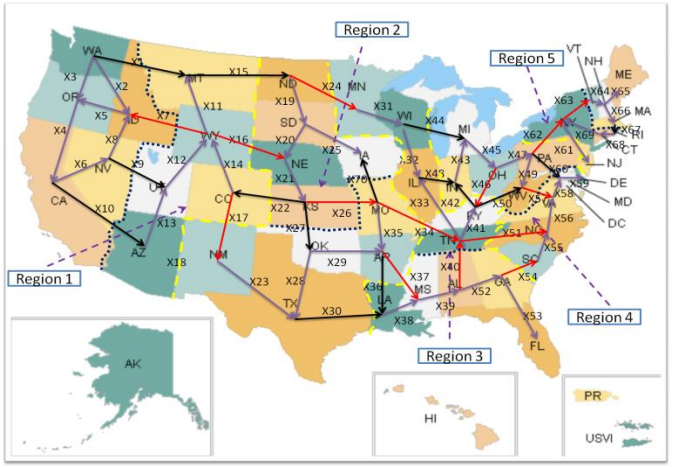
Injecting False Link-state Data

- Claiming invalid energy links as valid
  - Demand node cannot obtain enough requested energy
  - Disrupt energy transmission in the grid

- Claiming valid energy links as invalid
  - Small number of links compromised—total transmission cost increase
  - Large number of links compromised—total transmission cost decrease

Performance Evaluation

- **Topology**: The simplified version of the US smart grid.
- **Data set**: 2009 US Energy Information Administration State Electricity Profiles.
- **Length of the energy links**: Computed using Google map.
- **Metrics**: Increased transmission cost, User outage rate, and Supplied energy loss.



Performance Evaluation (cont.)

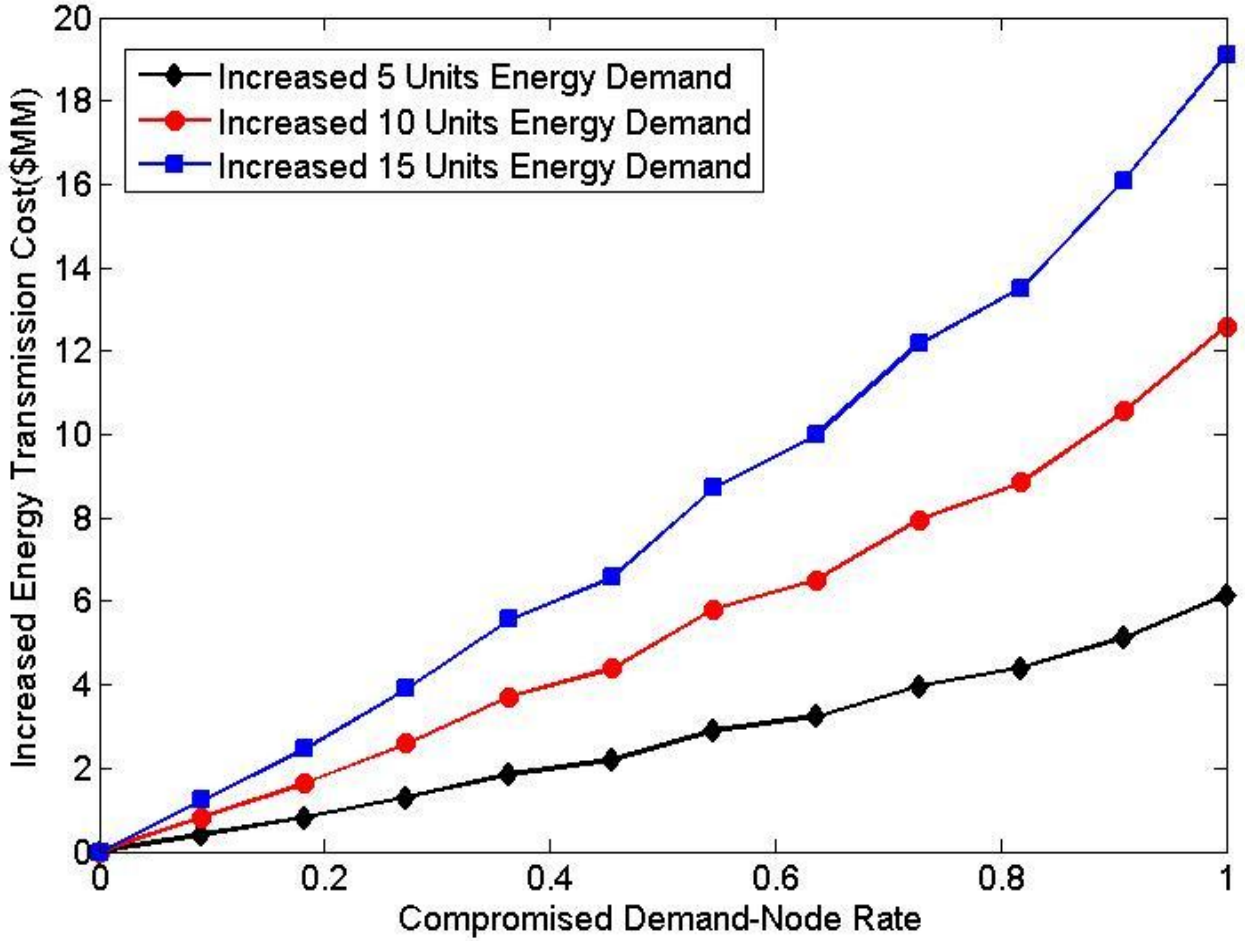


Fig. 3 Increased Energy Cost vs. Compromised Demand-Node Rate

Performance Evaluation (cont.)

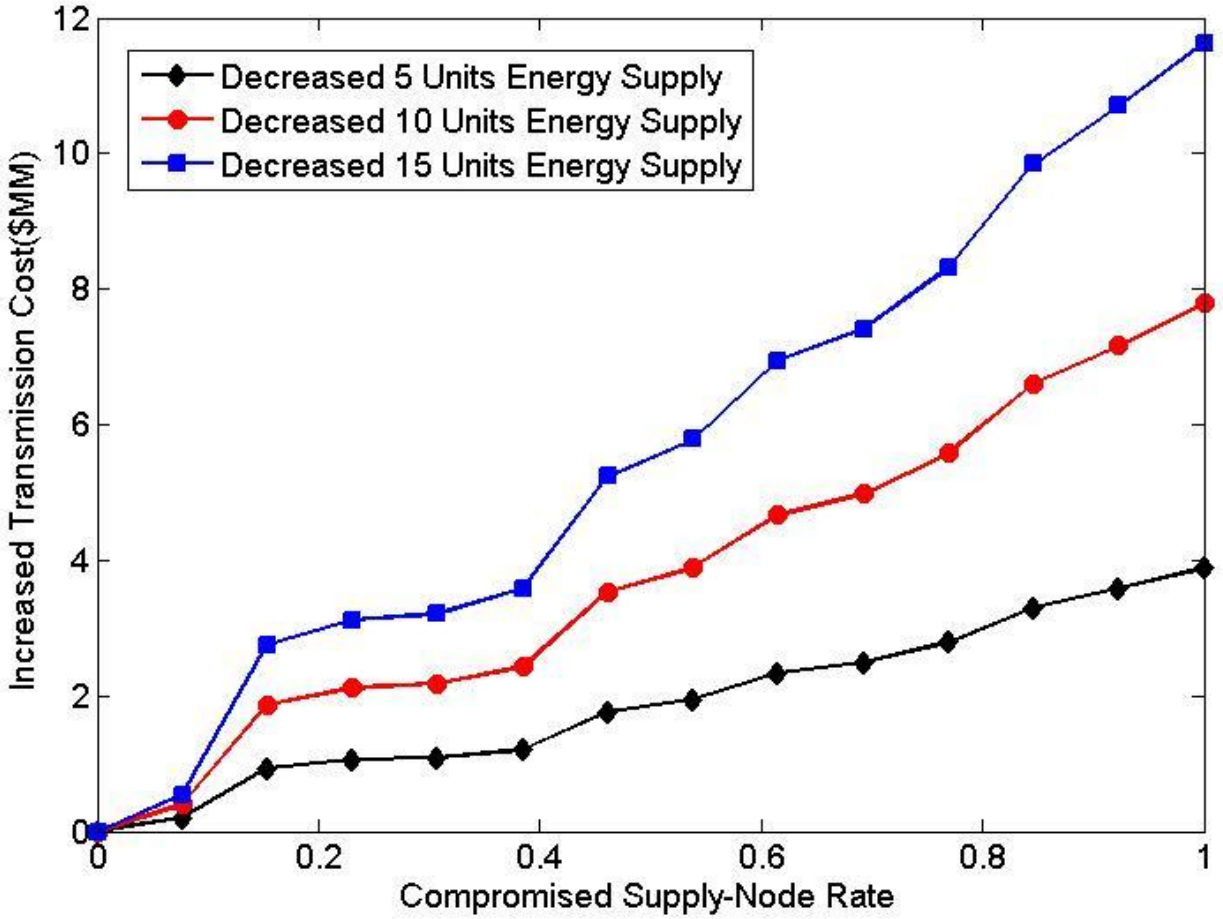


Fig. 4 Increased Energy Transmission Cost vs. Compromised Supply-Node Rate

Performance Evaluation (cont.)

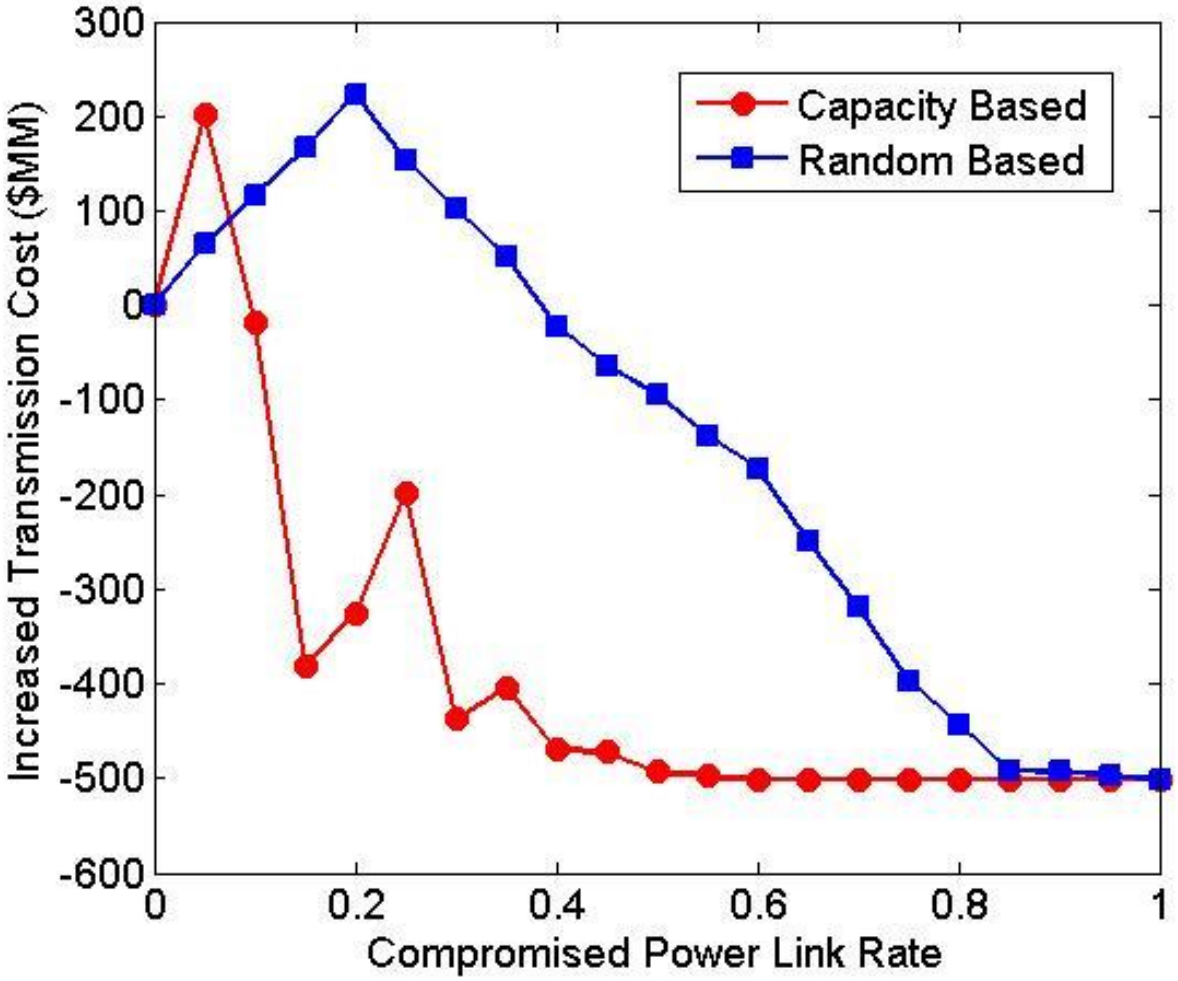


Fig. 5 Energy Transmission Cost vs. Compromised Energy Link Rate

Performance Evaluation (cont.)

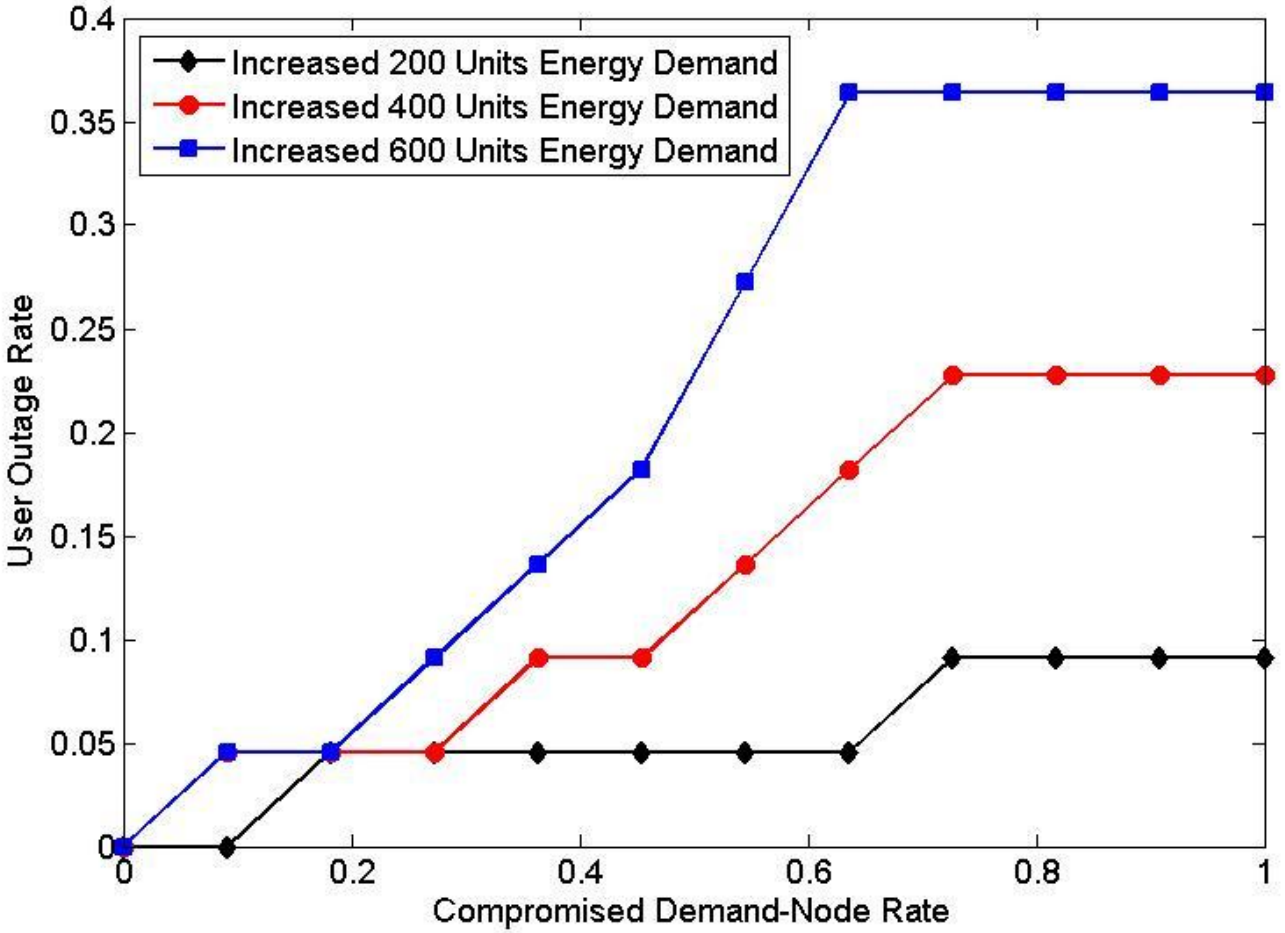


Fig. 6 User Outage Ratio vs. Compromised Demand-Node Rate

Performance Evaluation (cont.)

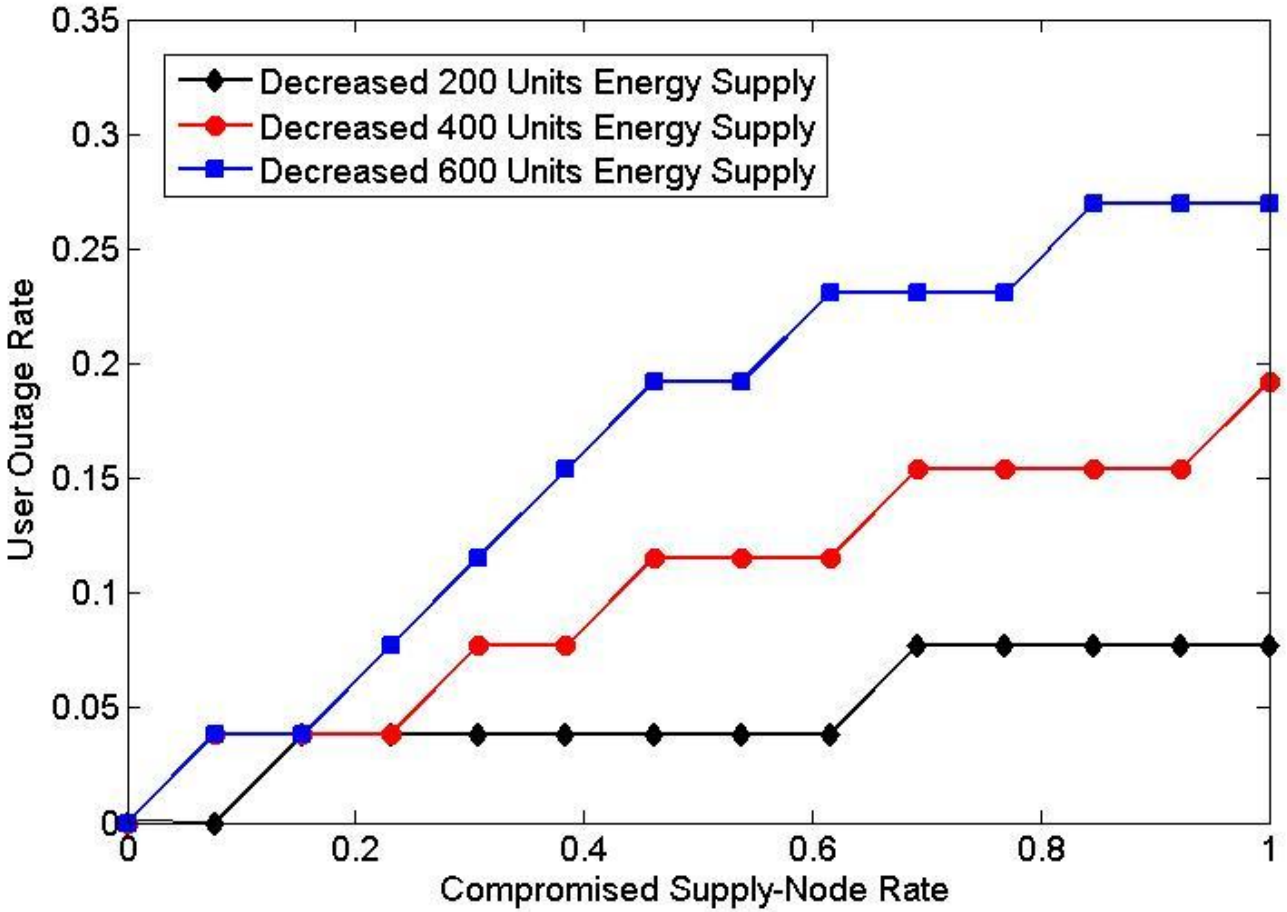


Fig. 7 User Outage Rate vs. Compromised Supply-Node Rate

Performance Evaluation (cont.)

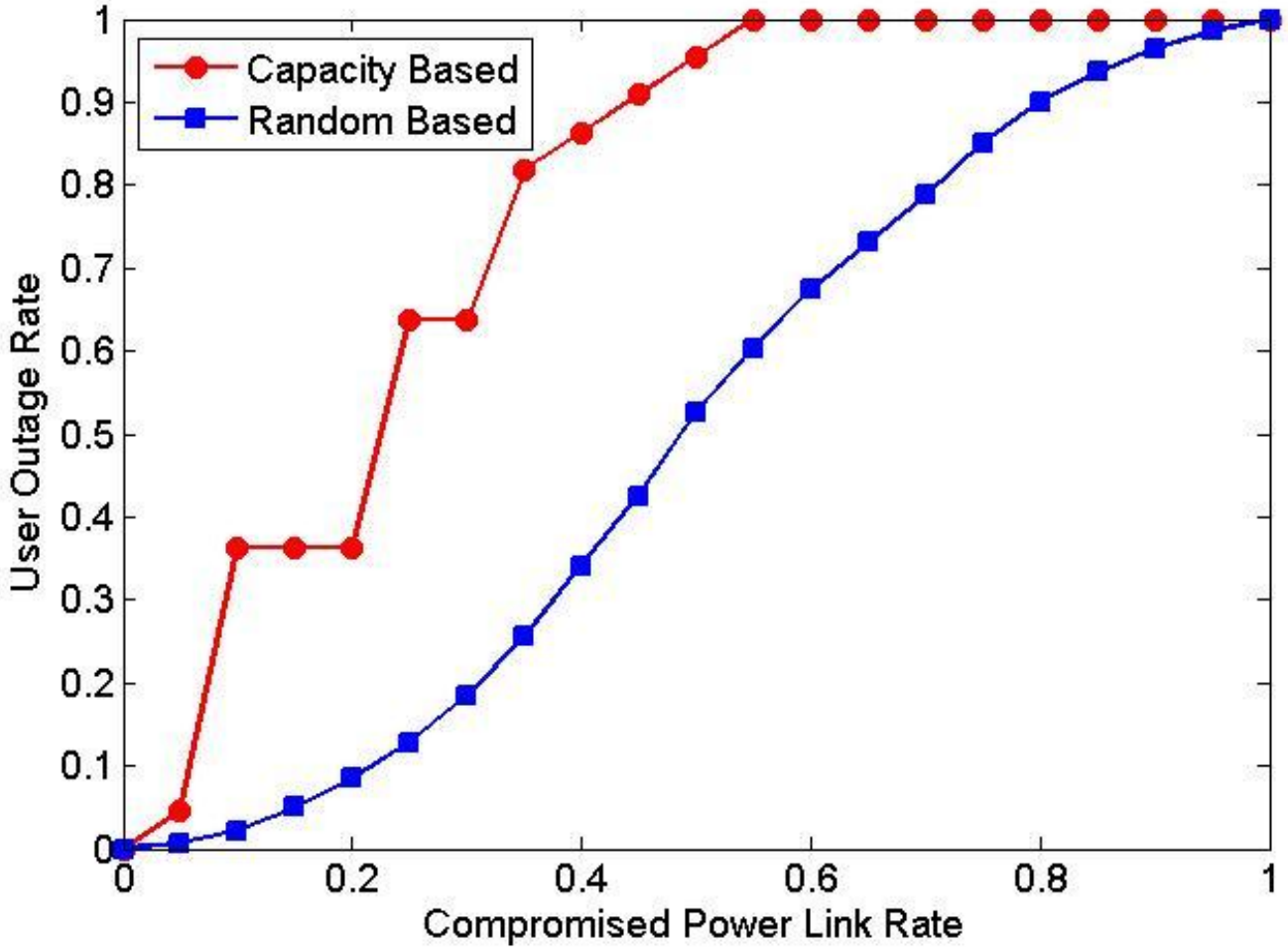


Fig. 8 User Outage Rate vs. Compromised Energy Link Rate

Performance Evaluation (cont.)

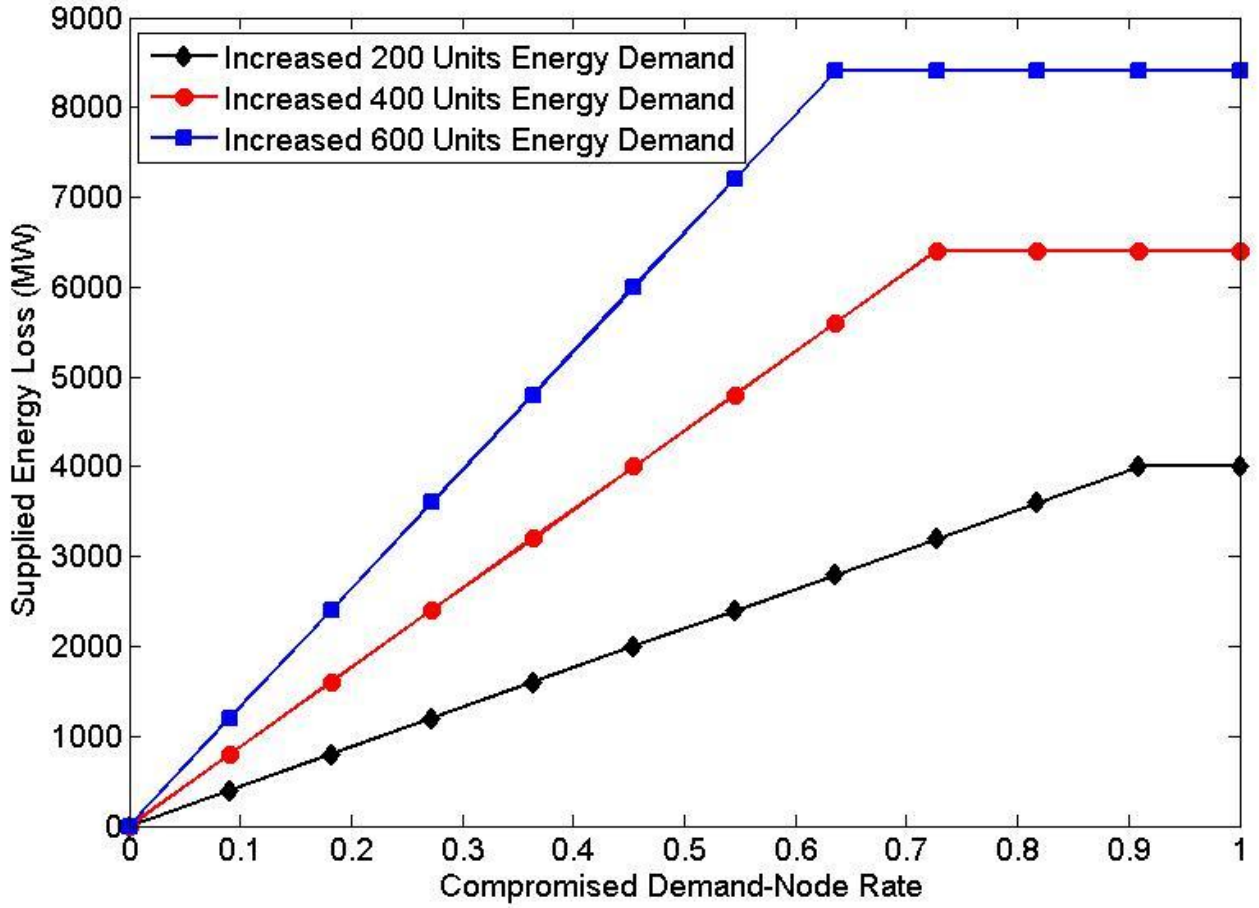


Fig. 9 Supplied Energy Loss vs. Compromised Demand-Node Rate

Final Remarks

- False data injection attacks against power system state estimation
  - Modeling attacks
  - Developing countermeasures
- False data injection attacks against energy routing process
  - Exploring the space of attack strategies
  - Modeling and analysis
- Ongoing research
  - Explore other attacks (data integrity, timing, and others)
  - Defend against those attacks
    - Prevention, detection and response

Thank You!

Questions?