TEXAS A&M UNIVERSITY

Distributed Internet-Based Load Altering Attacks Against Smart Power Grids

Authors: A.-H. Mohsenian-Rad and A. Leon-Garcia

Presenter: Harsha Patibandla

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Overview

- Introduction
- Types of Loads
- Defense mechanisms
- Cost efficient protection – System Model, Problem Formulation and Solution
- Numerical Example and Analysis
- Critical Assessment
- Future Work
- References

Introduction: Internet-based Load Altering Attacks

- Attack scenario addressed:
  - Vulnerability: Internet connected Loads
  - Threat: Attacker may alter load profile
  - Consequence: Cause circuit overflows and equipment damage
- Paper discusses the following:
  - Types of loads vulnerable
  - Applicable defense mechanisms
  - A new cost efficient load protection mechanism

Types of Loads

- Data Center and Computation Load
  - Can take up to 70 MW power
  - Power consumption almost doubled when busy
  - Threat: Overwhelm servers via bogus computation attacks
  - Extra power consumption will cause load fluctuations on the grid

Types of Loads

- Demand side management
  - Utility alters load curve shape of customers so as to minimize peak demand, improve system operation, quality-of-service, etc
  - Direct Load control
    - Control invisible to users
    - 2-way communication between utility and appliances
    - Threat: Attacker modifies command signals to turn on many loads simultaneously
    - Degradation of power quality, voltage problems, potential damage to utility and consumer equipment

Types of Loads

- Indirect Load control
  - Consumers control load according to price signals sent by utility via smart meters
  - Threat: Attacker injects false prices
  - Lower prices may cause major load spike

Defense Mechanisms

- Protection Of Smart meters and Data Centers
  - Vulnerable to attacks on CIA
  - reinforced metering infrastructure which protects the meter and the incoming signals
  - Use passwords, firewalls, and identity authentication

Defense Mechanisms

- Direct Load control protection
  - Communication is one on one (unicast)
  - Use private key encryption and message authentication code generation
- Indirect Load control protection
  - Messages are multicast
  - Use efficient group key management

Defense Mechanisms

- Attack Detection via Learning Demand Patterns
  - Learn the normal load trends
  - Identify anomalous behavior and take action (E.g. trip breaker)
- Load Shedding and Load Relocating
  - In case of suspected attack either shutdown the load or move it to different grid location

Cost Efficient Load Protection

- Protecting all vulnerable loads can be expensive
- Partial load protection can save costs
- Algorithm needed to choose critical loads which provides cost savings and gives sufficient protection

Cost efficient load protection – System Model

- System Model

The total active load power at bus i is given as

$$P_i = L_i + (1 - \alpha_i)\Delta_i - G_i \qquad (1)$$

Where,

- N – Set of all buses in the grid.
- For each bus $i \in N,\ G_i$ - The amount of active generation power at bus i.
- L_i- The amount of normal active load power at bus i, i.e. the load when no load altering attack is taking place.
- Δ_i- The maximum amount of extra active load power that can be added to bus i.
- Also, assume that the portion of the extra load at bus i which is being protected is denoted by α_i.
- Note that $0 \leq \alpha_i \leq 1$.
- If no protection is used at bus i, then the total altered load can be as high as Δ_i $\text{i.e. the whole vulnerable load.}$
- If α_i portion of vulnerable load at this bus is protected, then the total altered load will be $(1 - \alpha_i)\Delta_i$

Cost efficient load protection – System Model

- The dc power flow equation is given as,

$$G_i - L_i - (1-\alpha_i)\Delta_i = \sum_{j=1, j\neq i} B_{ij}(\theta_i - \theta_j), \forall_i \in N \quad (2)$$

$$P_{ij} = B_{ij}(\theta_i - \theta_j), \forall_i, j \in N \quad (3)$$

Where,

- If the active power generation is greater than the active load, then P_i will be a negative number.
- θ_i - Voltage phase angle at bus i.
- β_{ij} - The imaginary term in the complex value at row i and column j of the Y-bus matrix of the grid.
- P_{ij}- The power flow over each branch (i,j) in the electric grid where $i, j \in N$.

Cost efficient load protection – Problem formulation

- Problem formulation
- In order to avoid circuit overflow, it is required that,
- $P_{ij} \leq P_{ij}{}^{max}, \forall_i, j \in N$ (4)

$$\boxed{\begin{array}{l} \underset{\alpha}{minimize} \sum_{i \in N} C_i(\alpha_i) \qquad (5) \\ subject\ to\ Eqs.(2) - (4) \end{array}}$$

Problem Formulation

Ci → Cost of Protection for each load

Proposed Solution approach

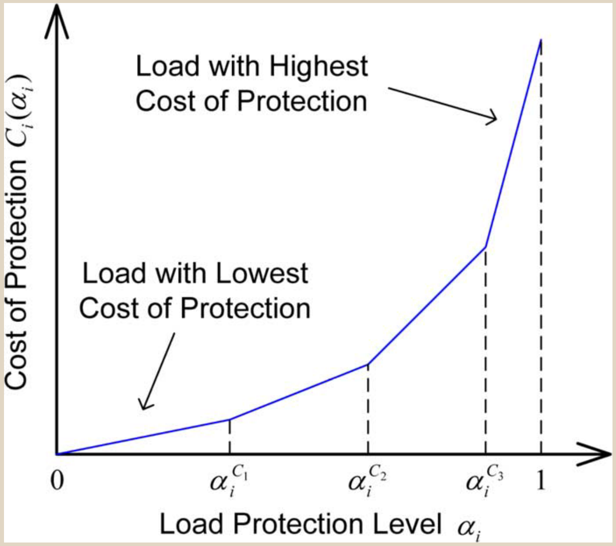


Figure from Ref. [1]

- Consider piecewise linear cost functions for the loads
- Consider Ki load classes with the below class cost indicators:

$$0 < {\alpha_i}^{C_1} < {\alpha_i}^{C_2} < \cdots << {\alpha_i}^{C_{K_i - 1}} < 1$$

- Protection: Start from lowest cost load and go to higher cost if necessary
- This problem can be formulated and solved using linear programming

Numerical example and analysis

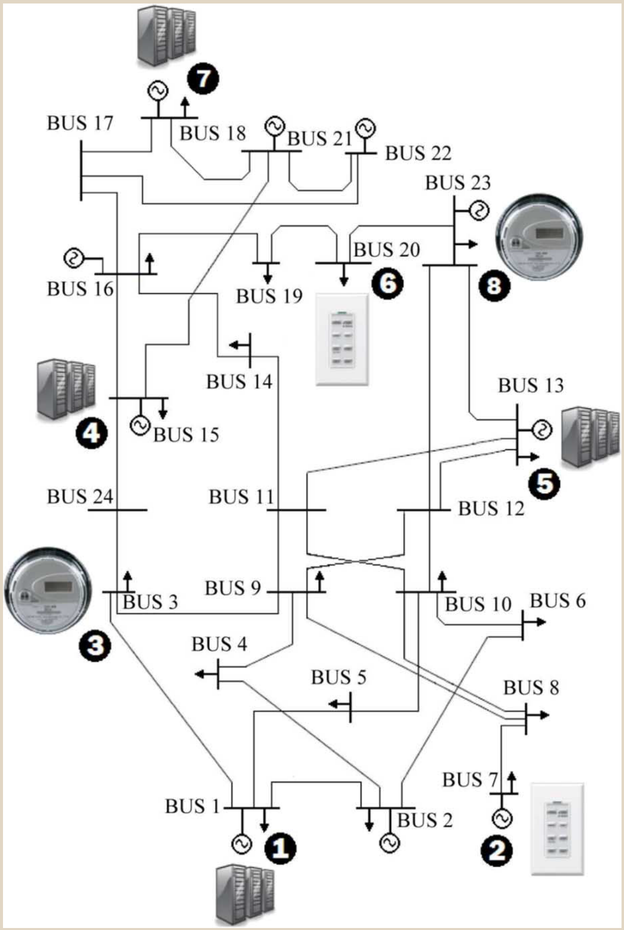


Figure from Ref. [1]

- modified version of the IEEE 24-bus reliability test system [3]
- 24 buses, 38 branches
- Generators at 10 buses: 1 spinning reserve
- Loads on 8 buses vulnerable
  - 4 data centers and 4 demand side management units
  - Each load: Normal – 50 MW; Peak – 100MW
- Piecewise linear cost function, $K_i = 2, \alpha_i = 0.5$
- Max P_{ij}=400 MW

Numerical example and analysis

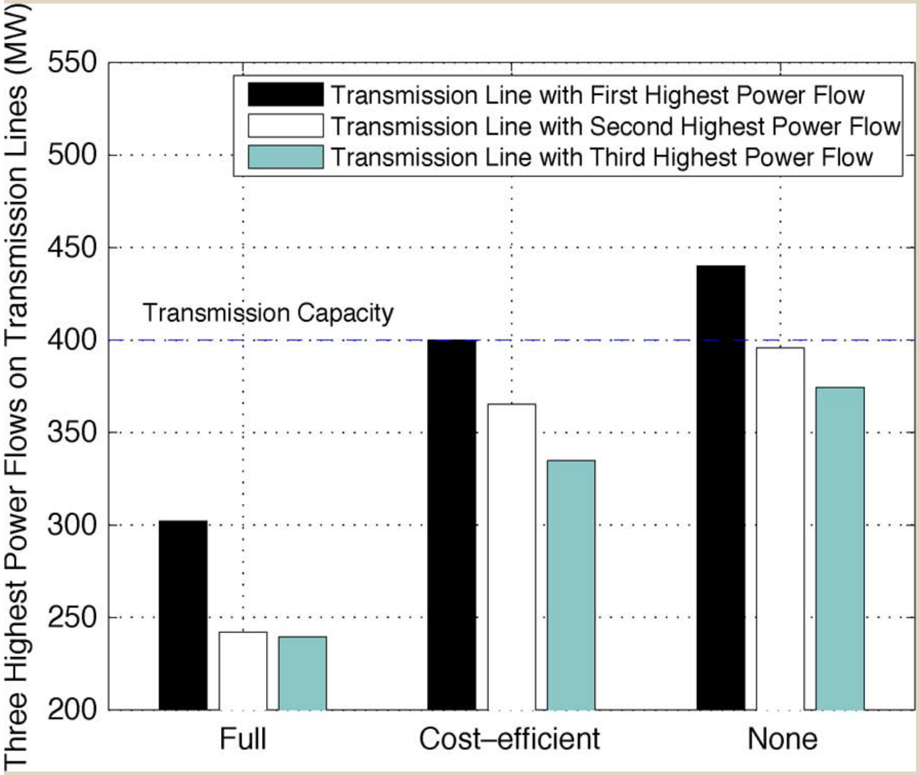


Figure from Ref. [1]

- No protection: Power flow >400 MW
- Full protection: Power flow 300 MW
- Partial Protection: Power flow 400 MW
  - Protect half of computation and directly controlled loads and quarter of indirectly controlled loads
  - Cost is 10.2% of full protection cost

Numerical example and analysis

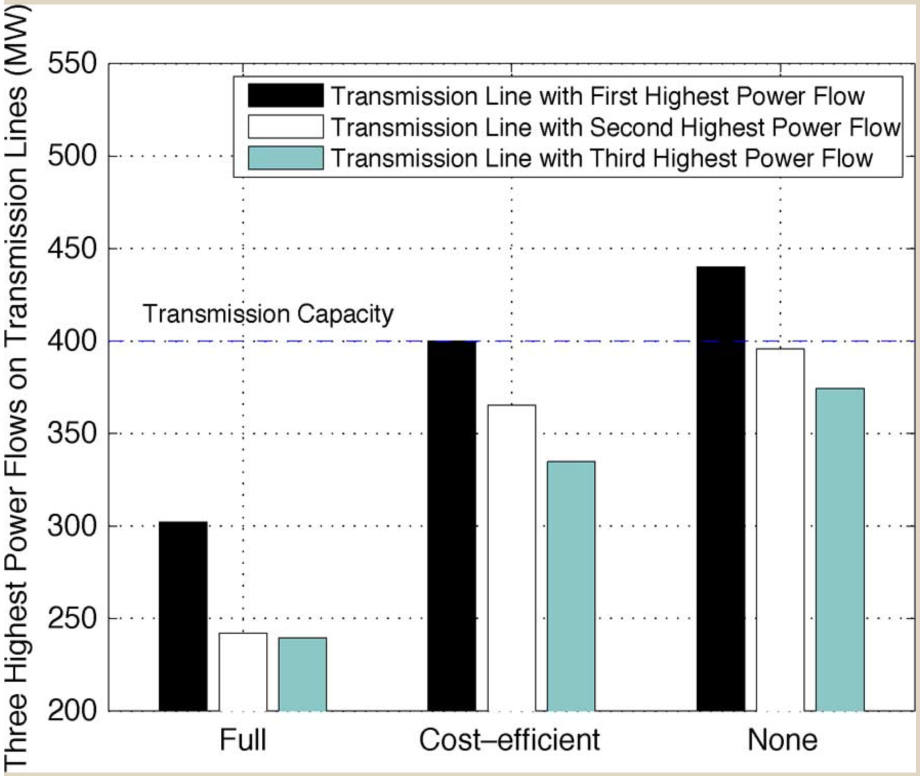
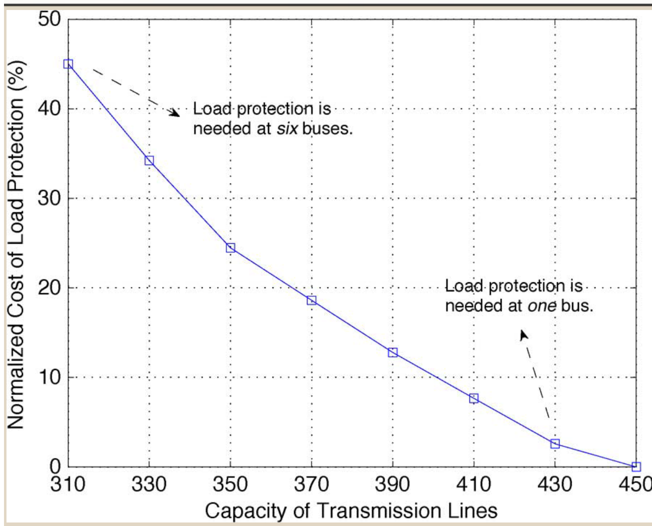
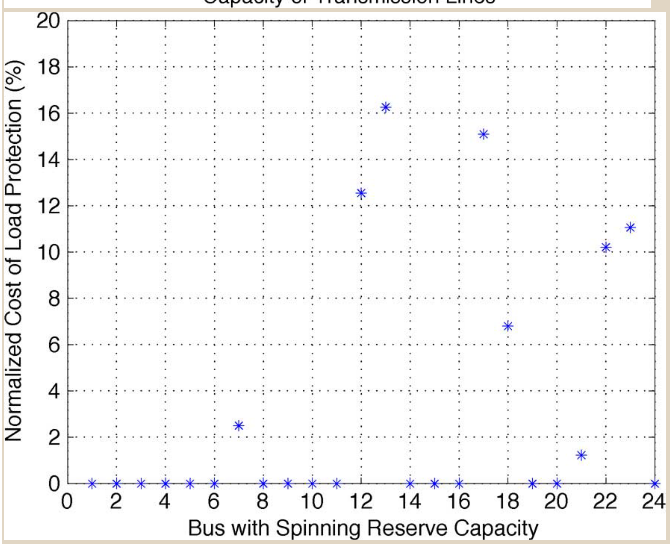


Figure from Ref. [1]

- No protection: Power flow >400 MW
- Full protection: Power flow 300 MW
- Partial Protection: Power flow 400 MW
  - Protect half of computation and directly controlled loads and quarter of indirectly controlled loads
  - Cost is 10.2% of full protection cost

Impact of Changes in Grid Parameters





Figures from Ref. [1]

- Load Protection cost drops as capacity of transmission lines increases
- The location of the spinning reserve affects the cost of protection.
- Grid topology and parameters need to be taken into account in the algorithm

Critical Assessment

- Paper identified a critical vulnerability
- Good overview of the different defense mechanisms
- Addresses cost efficiency – always an important concern
- Does not give numbers for the damage that might occur
- How large scale should an attack be to cause significant damage?
- The exact Cost optimization algorithm used is not mentioned
- Cost of protection: Loads will be protection for other purposes like privacy (for data center)
  - Will this cause reduction in cost?

Future work

- Investigate other types of vulnerable loads, e.g., industrial loads
- Protection scheme: Along with cost efficiency are there any concerns to be considered?

References

[1] - Distributed Internet-Based Load Altering Attacks Against Smart Power Grids

[2] - Reliability Test System Task Force, Application of Probability Methods Subcommittee, “The IEEE Reliability Test System—1996,” pp. 1010–1020, Aug. 1999

- Questions??