Vulnerability Analysis of Power Systems Based on Cyber-Attack and Defense Models

Saqib Hasan, **Amin Ghafouri, Abhishek Dubey, Gabor Karsai, Xenofon Koutsoukos**

Vanderbilt University

Outline

- Overview
- Challenges
- Contributions
- Power System model
- Attack Model and Algorithm
- Defense Model and Algorithm
- Contingency Simulator and Cascade Simulation Model
- Example System and Evaluation
- Conclusions and Future Work

Overview

- Smart grids are needed with the increasing demand for reliable energy.
- The technological advancements such as substation automation, PMUs, AMIs, etc., are deployed to improve the traditional power grid capabilities and improve reliability.
- They increases the attack surface due to the increase in cyber components.
- At present cyber-attacks are one of the major obstacles towards reliable system operations and give rise to new system vulnerabilities.

Overview

- Attackers take advantage of such vulnerabilities to cause severe system damage.
  - Example: Recent blackout of Dec 2015 Ukraine.
- Power systems consists of several substations.
- Substations have RTUs to control and monitor the field devices.
- They become the primary target for the attackers.
- Adversary can gain complete control of the RTUs and perform various types of attacks.

Challenges

- Time and effort to compromise an RTU limits the attacker.
- Attacker can access only a few RTUs before they get detected.

Challenges?

1. **To identify critical substations and protection assemblies to compromise in order to maximize system damage.**
2. **To identify critical substations to protect in order to minimize system damage.**

Contributions

- A game-theoretic approach to design an attacker/defender model is provided.
  - A formal attacker model is described.
  - An efficient polynomial-time algorithm for finding worst-case attack is developed.
  - A formal defender model is presented.
  - An efficient polynomial-time algorithm for identifying critical substations to protect is developed.
  - Evaluation results using standard IEEE-14, 39, and 57 bus systems are demonstrated to support the developed models.

Power System Model

- **System:**
  - G_P: power system, U: set of buses, G: set of generators, T: set of transformers, L: set of loads, *R*: set of transmission lines, *P*: set of protection assemblies (distance relays, over-current relays and circuit breakers).
- **Modeling substations**
  - Let $S = \{S^1, \ldots\ldots, S^m\}$ be the substations.
  - $S^i \subseteq P, \forall\, i \in \{1, \ldots, m\}$.
  - $F(S^i)$ returns the set of protection assemblies in S^i.
  - $\bigcup_{i=1}^{m} F(S^i) = P$
- **Load loss function**
  - Loads are defined by L_j, where $j = 1\ to\ n,\ \ n \in \mathbb{N}$
  - Current flowing through each load is defined by:

    I_j, where $j = 1\ to\ n,\ n \in \mathbb{N}$
  - Load loss is calculated as:

    $J(A_{P'}) = \sum_{j=1}^{n} L_j, \forall\, I_j = 0$

Attacker Model

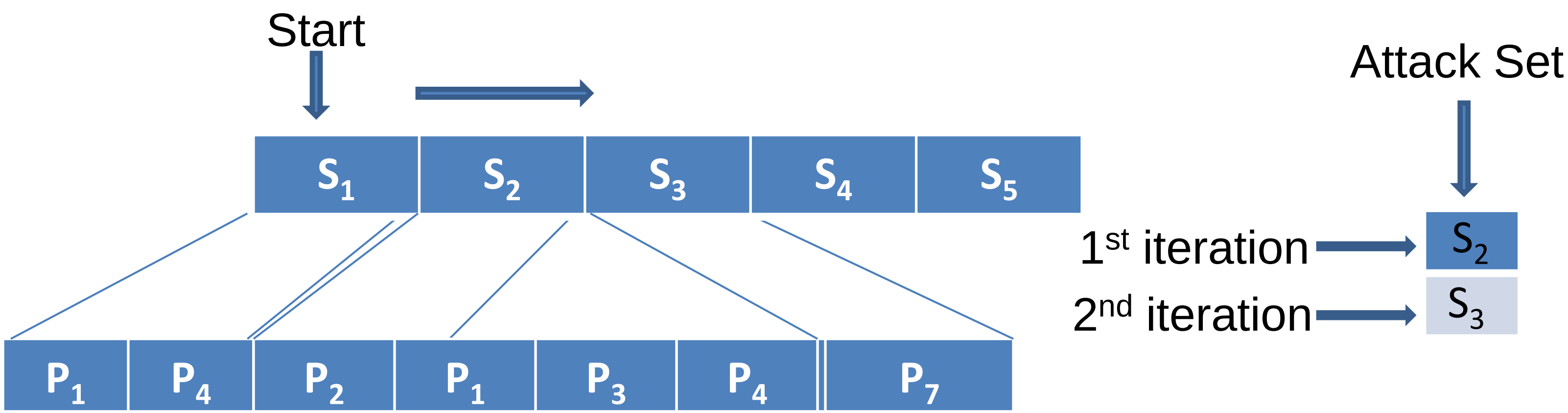
- **Attack Model:**
  - First, attacker identifies substations $S' \subseteq S$ to attack.
  - Attacker has budget B_S where $|S'| \leq B_{S.}$
  - Then, the attacker identifies protection assemblies $P' \subseteq \mathrm{F}(S')$ to manipulate.
  - Attacker has budget B_P where $|P'| \leq B_{P.}$
  - Finally, attacker launches a cyber-attack $A_{P'}$ on protection assemblies $P' \subseteq F(S')$.
  - Uniform, unit cost for attacking a substation.
- **Attacker's Goal:**
  - Goal of the attacker is to maximize the load loss

$$\max_{S'} \max_{P' \subseteq F(S')} J(A_{P'})$$
$$\text{s.t.} \quad |S'| \leq B_S, \quad |P'| \leq B_P$$

Attack Algorithm

- Consider a set of substations $S = \{S_1, S_2, S_3, S_4, S_5\}$.
- Consider a set of protection assemblies $P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8\}$.
- Attack budget is restricted to 2.

Select a substation	Select the protection assemblies with the substations	Identify and record Loss	Select Next Substation



Defender Model

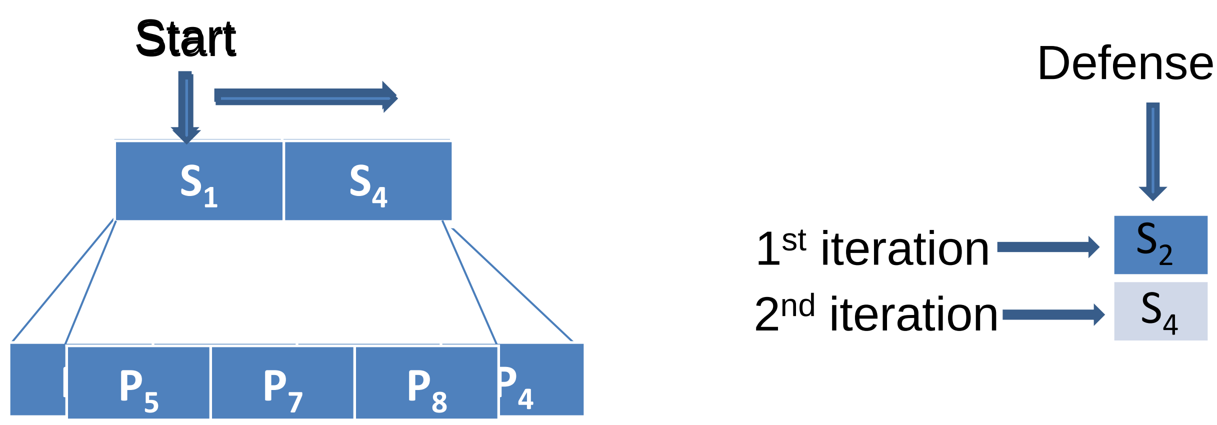
- **Defense Model:**
  - Defender can protect the substations D_S from cyber-attacks.
  - Defender has a budget B_D , where $|D_S| \leq B_{D\,.}$
- **Defender's Goal:**
  - Goal of the defender is to minimize the load loss

$$\min_{D_S} \max_{S' \subseteq S - D_S} \max_{P' \subseteq F(S')} J(A_{P'})$$
$$\text{s.t.} \quad |D_S| \leq B_D, \quad |S^{'}| \leq B_S, \quad |P^{'}| \leq B_P$$

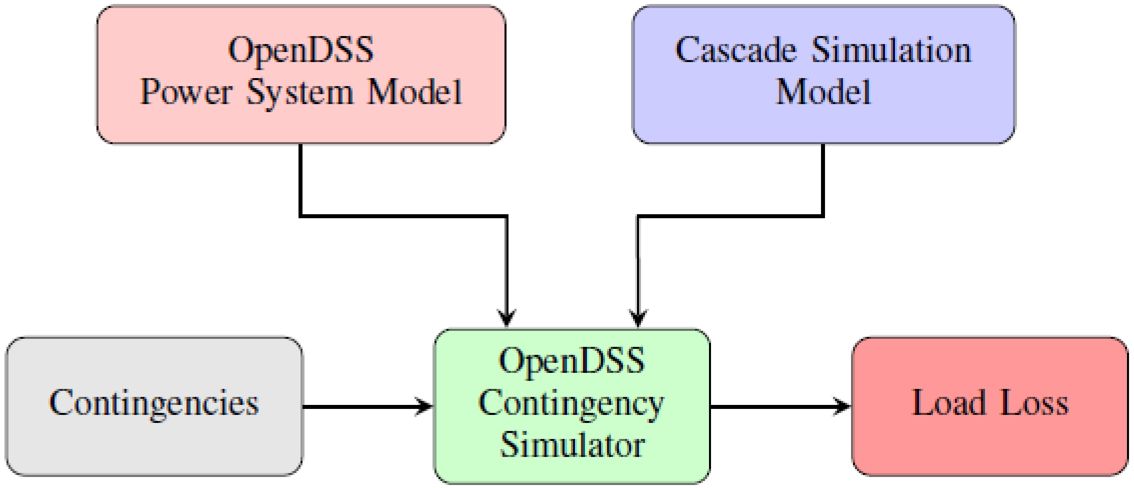
Defender Algorithm

- Consider a set of substations $S = \{S_1, S_2, S_3, S_4, S_5\}$.
- Consider a set of protection assemblies $P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8\}$.
- Defense budget is restricted to 2.

Run Attack Sequence based on the attack budget	Select a substation to protect and remove it from rest of the attack set.	Identify and record Losses	Select next Substation

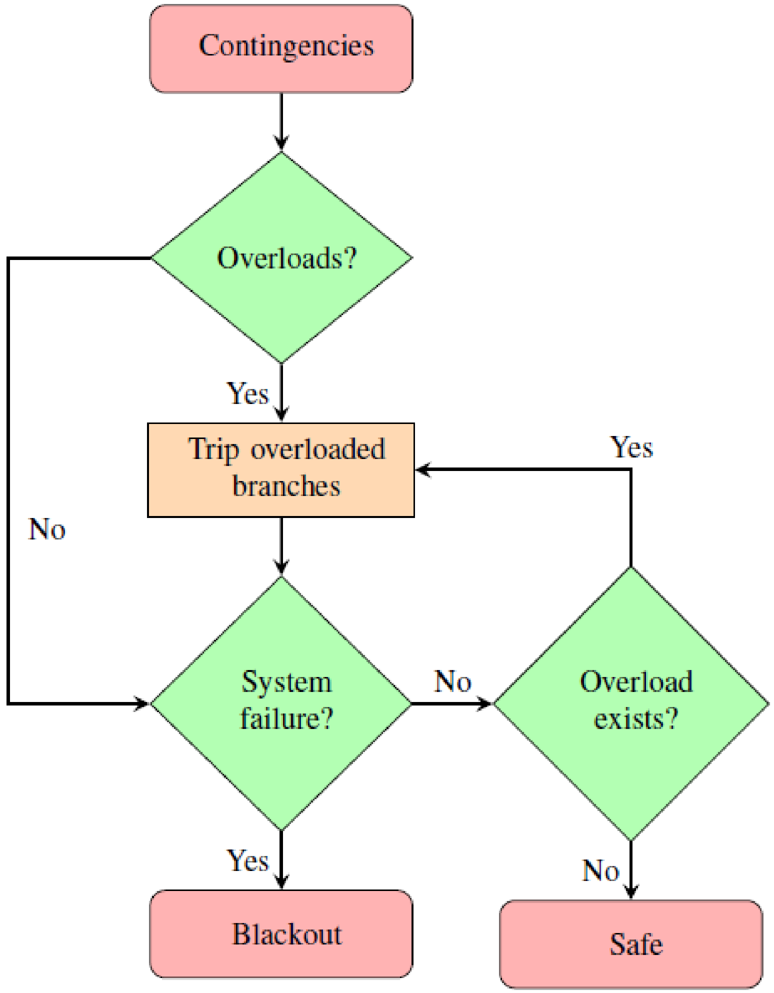


Contingency Simulator



Contingency simulator Framework

Cascade Simulation Model



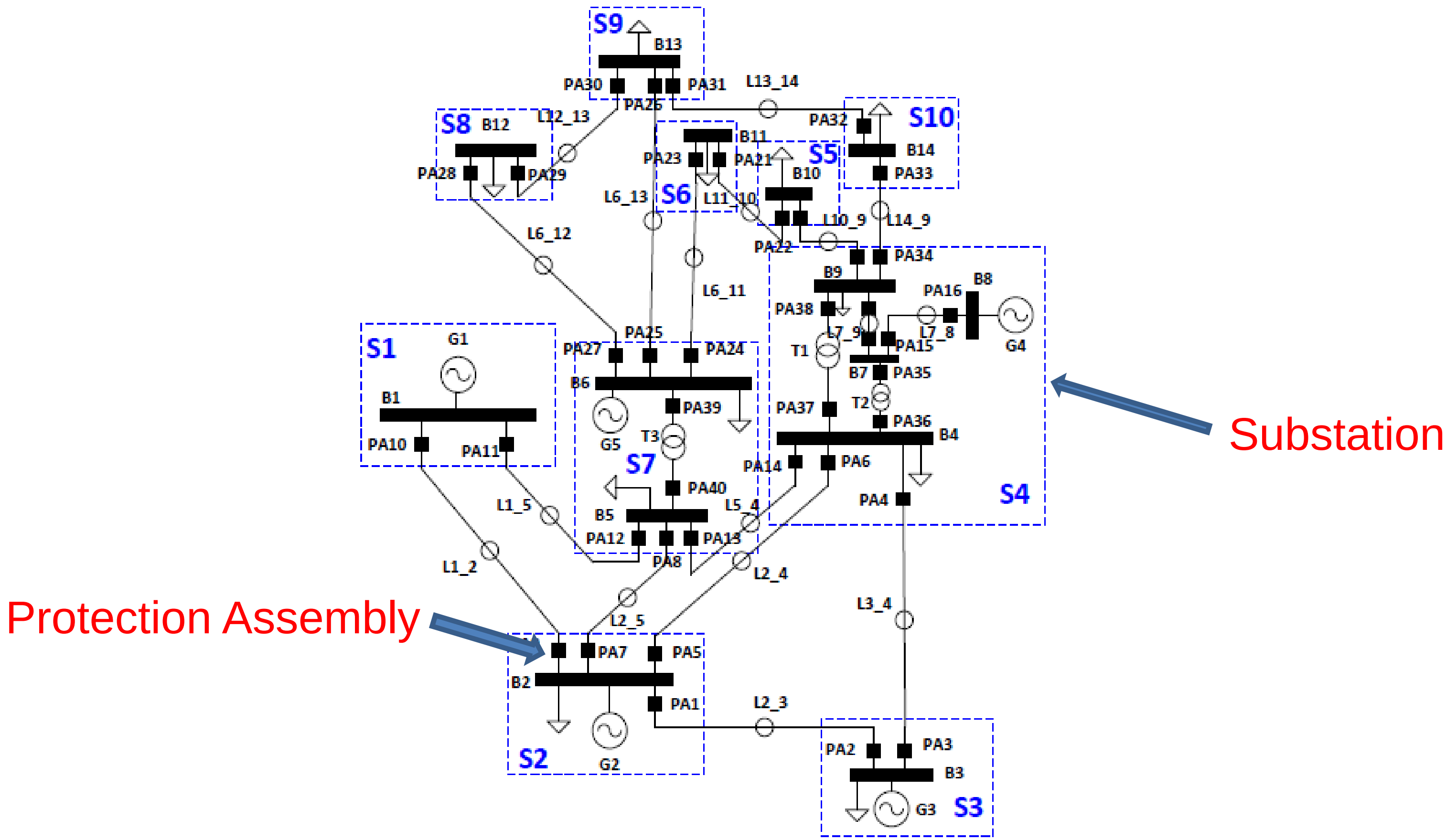
Cascade Simulation Model

IEEE PES Power & Energy Society®

IEEE

Example System

- Blue colored dotted boxes represent the substations.



IEEE-14 Bus System

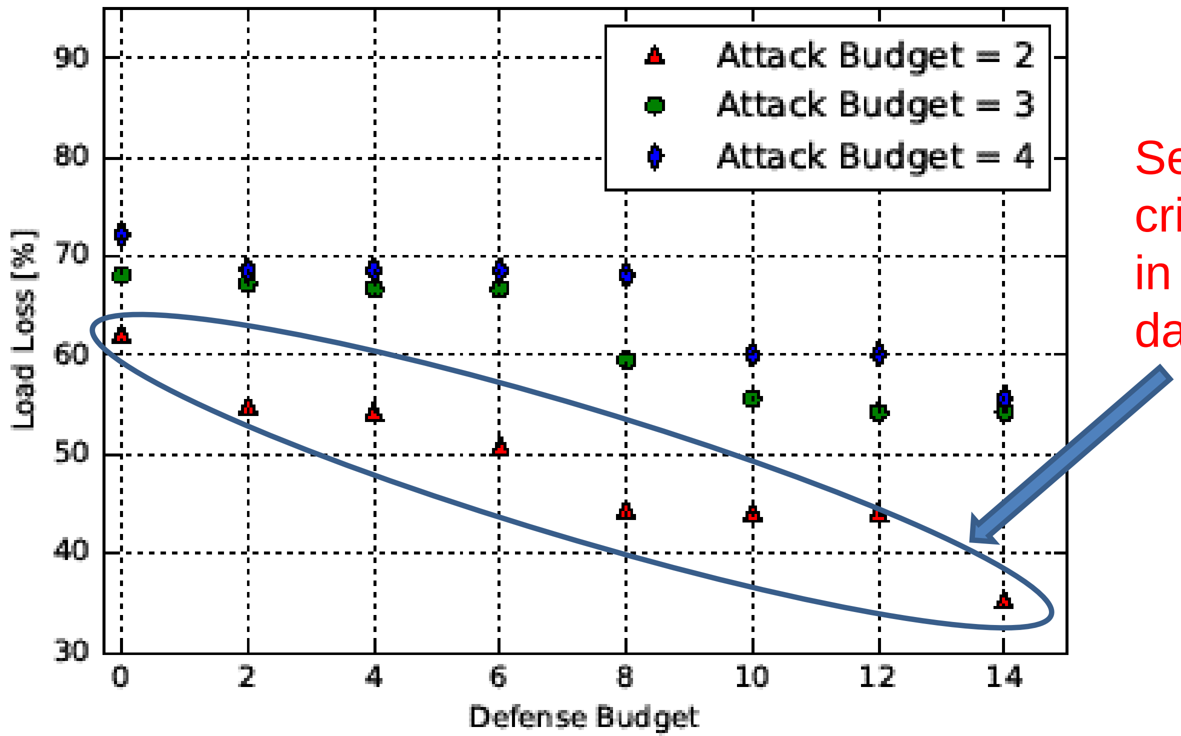
Evaluation

- Attack-Defense Scenario
- With only half the number of substation protection budget the load loss is minimized by 57.31%.

TABLE I: IEEE-14 Bus System Attack-Defense Scenario

Attack Budget (B_S)	B_P	Defense Budget (B_D)	Pre-Defense Load Loss	Post-Defense Load Loss	Substations Attacked	Substations Defended	Improvement (%)
2	2	3	51.17	48.30	S7	S4, S3, S2	5.61
2	2	4	51.17	43.46	S1, S6	S4, S3, S2, S7	15.07
2	2	5	51.17	29.55	S8, S9	S4, S3, S2, S7, S6	42.25
2	2	6	51.17	21.84	S5, S10	S4, S3, S2, S7, S6, S9	57.31

Evaluation

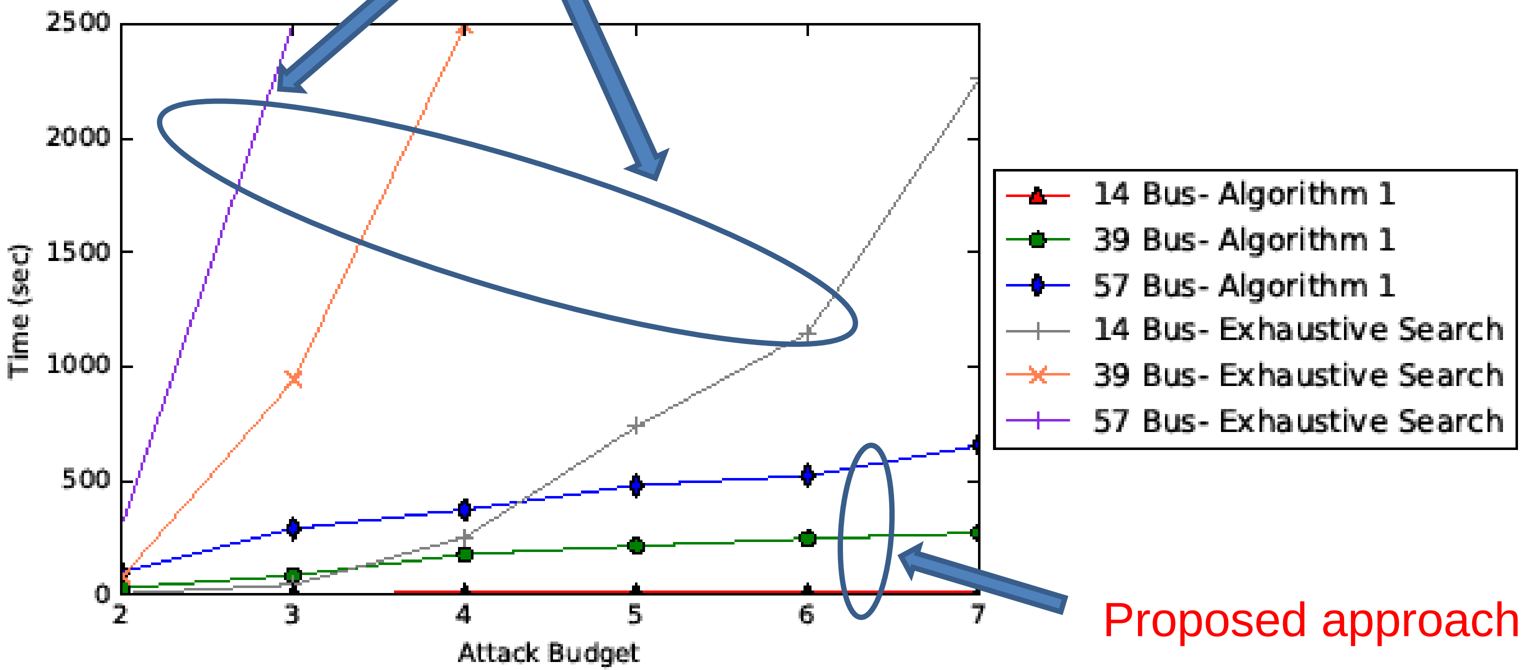


Selecting and protecting critical substations results in minimizing system damage

IEEE-39 Bus System

Evaluation: Attack Execution Time

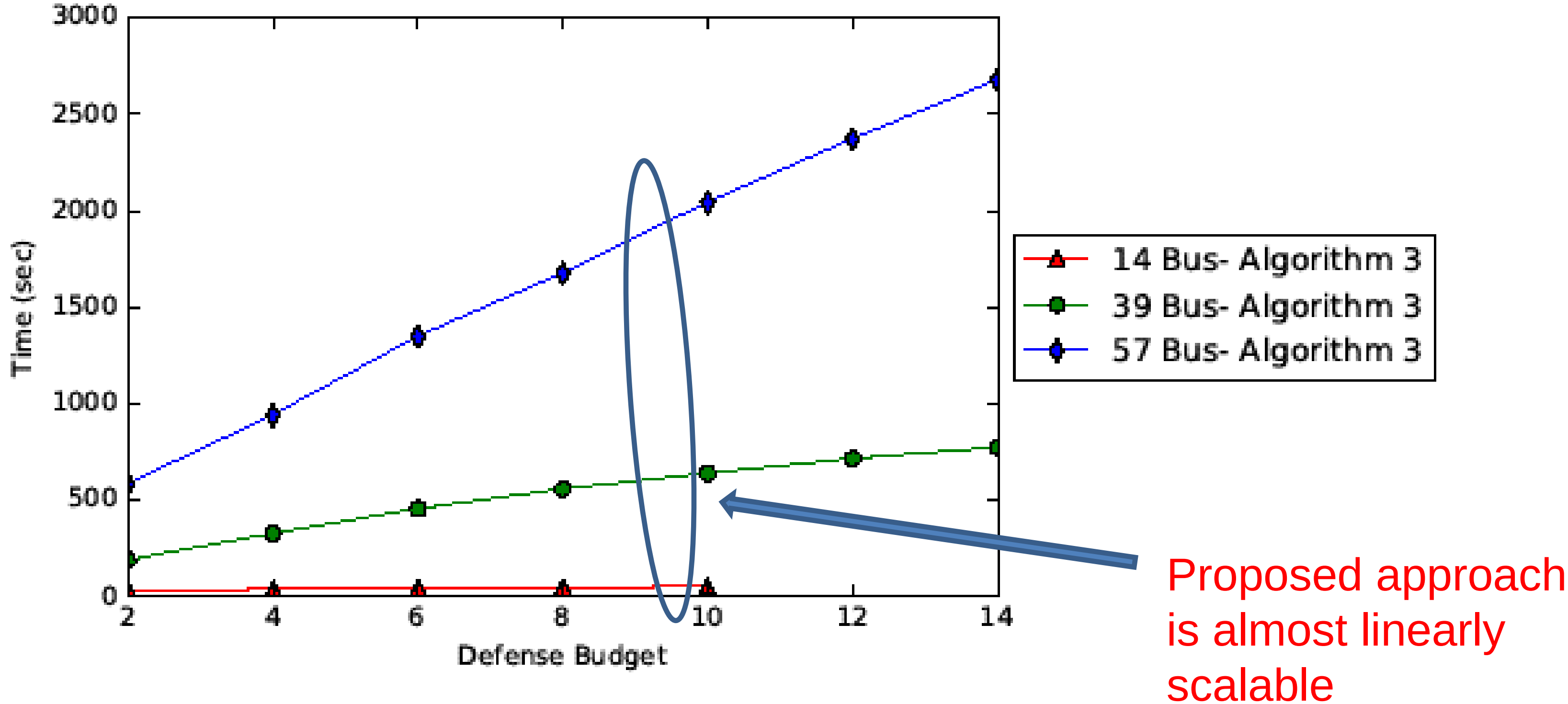
Exhaustive search takes much longer than the proposed approach



Proposed approach

Attack Execution Time

Evaluation: Defense Execution Time

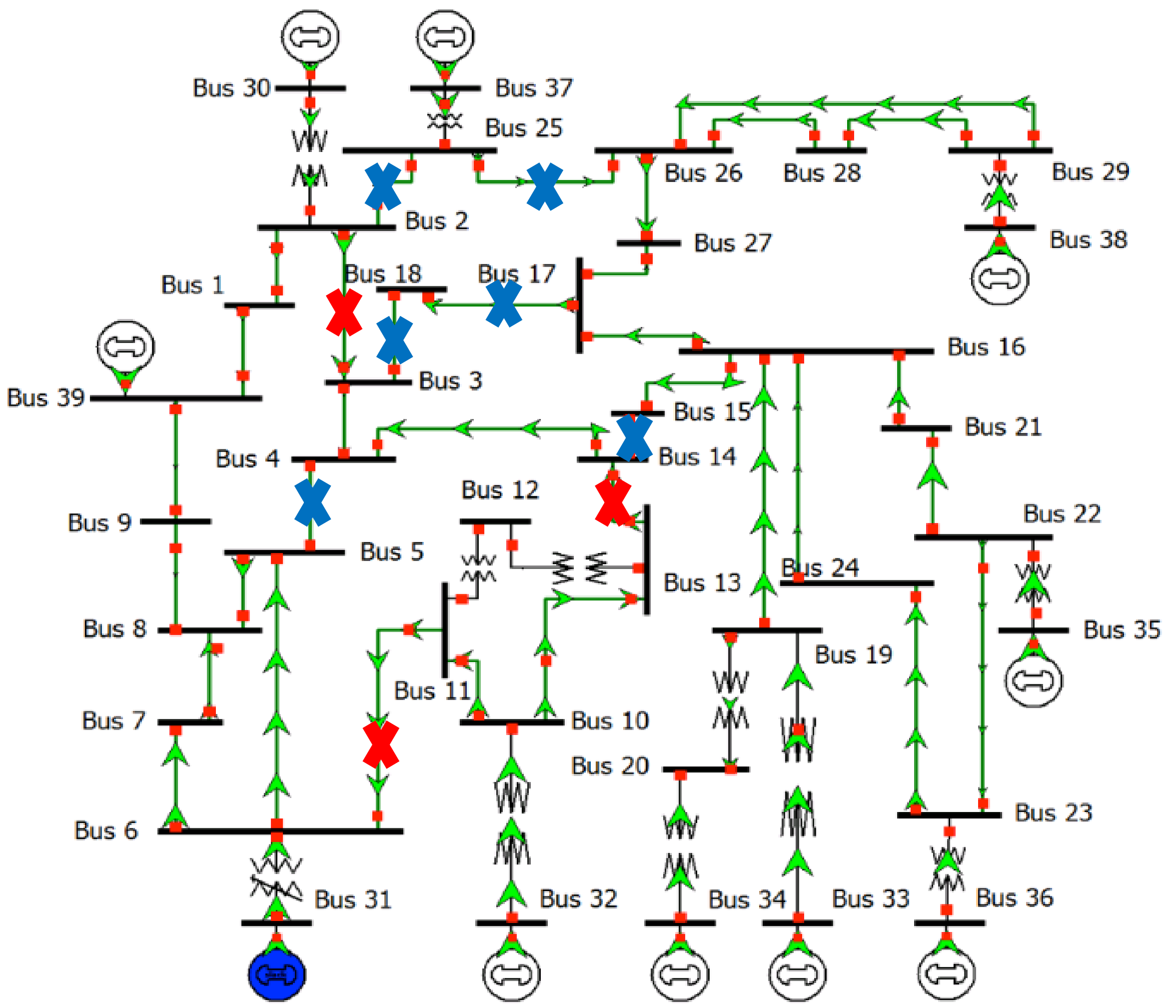


Defense Execution Time

Conclusion and Future Work

- A game theoretic approach for attacker/defender modeling is proposed.
- The models are formally described and developed.
- The algorithms presented are able to identify critical substations to attack and protect given the budget constraints in order to improve power system resilience.
- The algorithms presented perform significantly better than the exhaustive search.
- As part of the future work, we will look at the dynamic attacker/defender modeling in power systems.

Static Attack Scenario



- Initial attacks

↓ delay

- Stage1 Line Outages

15.86%

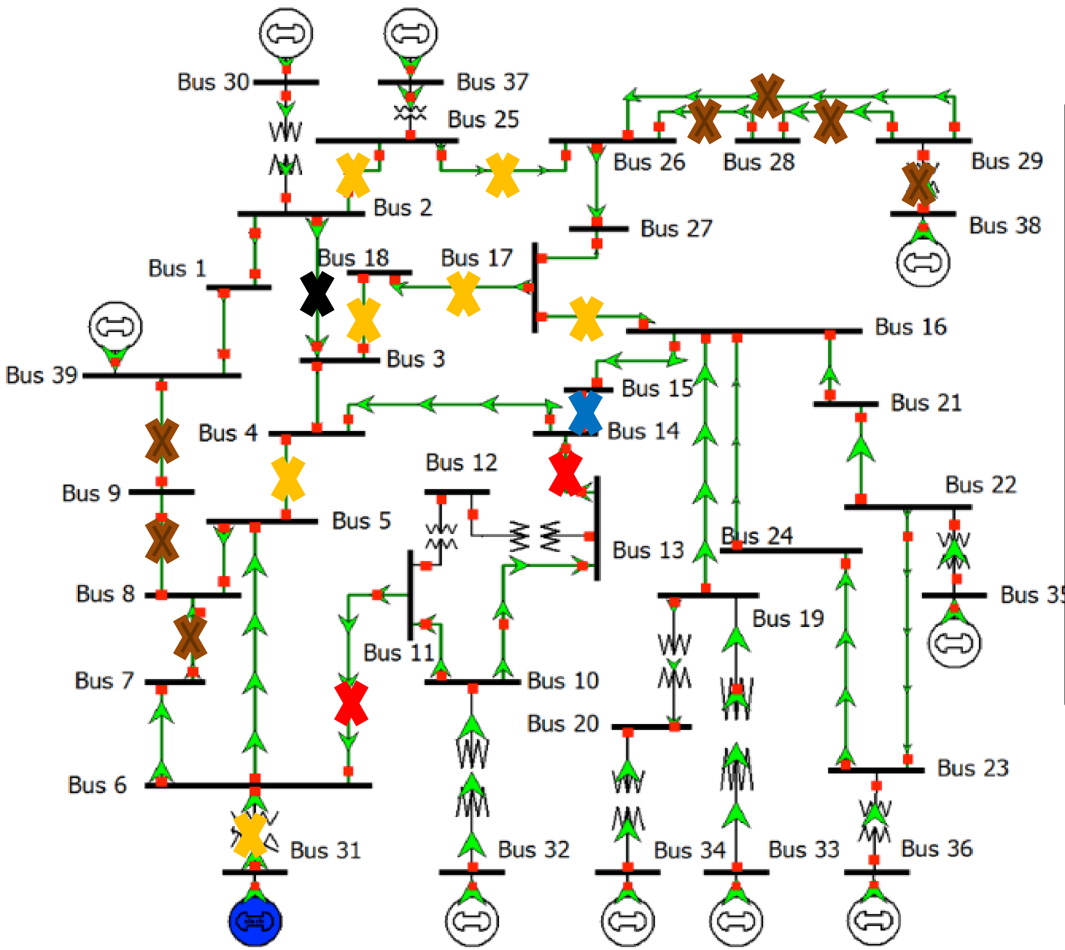
Ultimate Load Loss: 15.86%

http://icseg.iti.illinois.edu/ieee-39-bus-system/

IEEE PES Power & Energy Society®

IEEE

Dynamic Attack Scenario



- Initial attacks
delay
-Stage1 Line Outages + **Stage1 attack**
delay
- Stage2 Line Outages
delay 15.86%
- Stage3 Line Outages
42.78%

Ultimate Load Loss: 42.78%

http://icseg.iti.illinois.edu/ieee-39-bus-system/

Acknowledgements

- National Science Foundation (NSF), CNS-1329803.
- Foundations of Resilient Cyber-Physical Systems (FORCES), CNS-1238959.

THANK YOU!