# Vulnerability Analysis Based on Cyber-Attack and Defense Models in Power Transmission Systems

*Saqib Hasan*
*Department of Electrical Engineering and Computer Science*
*Vanderbilt University*

# Introduction

- Smart grids are a result of advancement in technology.
- Potentially increases the surface for cyber-attacks.
- Dec. 2015 Ukraine blackout is an example of recent cyber-attack.
- Power systems consists of several substations.
- Substations have their own RTUs (Remote Terminal Units).
- Components in power systems can be remotely controlled through these RTUs.
- Attackers take advantage of technology advancements and compromise the RTUs to destabilize the system.
- Compromising all the substations is difficult because of the time and effort required by the attacker.
- Challenge is to identify the critical substations to attack and defend based on attacker and defender budgets.

# Power System Model

- **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 assembly components (distance relays, over-current relays and circuit breakers).
- **Modeling substations**
  - Let $\mathrm{S} = \{S_1, \ldots\ldots\ldots, Sm\}$ be the substations.
  - $S_i \subseteq \mathrm{P}, \forall\ \mathrm{i} \in \{1, \ldots\ldots, \mathrm{m}\}$
  - $\bigcup_{i=1}^{m} S_i = \mathrm{P}$
- **Load loss function**
  - Loads are defined by $L_i$, $where\ i = 1\ to\ n,\ \ n \in \mathbb{N}$
  - Current flowing through each load is defined by:

$$I_l, where\ l = 1\ to\ n,\ n \in \mathbb{N}$$

  - Load loss is calculated as:

$$J(A_P) = \sum_{i=1}^{n} L_i, \forall\ I_l = 0$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Static Attack Model

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

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

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Static Defense 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

$$argmin_{D_S} max_{S' \subseteq S - D_S} max_{P' \subseteq S'} J(A_P)$$
$$\text{s.t.} \quad |D_S| \leq B_D$$
$$|S'| \leq B_S$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Simulator and Approach

- OpenDSS, a steady state simulator is used to compute the results.
- Algorithms used for attack and defense.

**Algorithm 1** Algorithm for Finding Worst-Case Attack

**Input:** $G_p, B_S, B_P$
**Initialize:** $L_w \leftarrow 0, T_w \leftarrow \emptyset, S_w \leftarrow \emptyset, L_g \leftarrow 0$
**for** $p = 1, \ldots, B_S$ **do**
  **if** $S_w == \emptyset$ **then**
    $S_d \leftarrow \texttt{Substation\_comps}(\emptyset)$
  **end if**
  **else:**
    $S_d \leftarrow \texttt{Substation\_comps}(S_w)$
  **for all** $i \in S_d$ **do**
    $S_t \leftarrow S_d(i)$
    $T_o, L_m \leftarrow \texttt{Worst\_Case\_Attack}(G_p, S_t, B_P)$
    **if** $L_m > L_w$ **then**
      $L_w \leftarrow L_m$
      $T_w \leftarrow T_o$
      $S_w \leftarrow i$
      **if** $(L_g - L_w) == 0$ **then**
        **break**
      **end if**
      **else:**
        $L_g \leftarrow L_w$
    **end if**
  **end for**
**end for**
**return** $S_w, T_w, L_w$

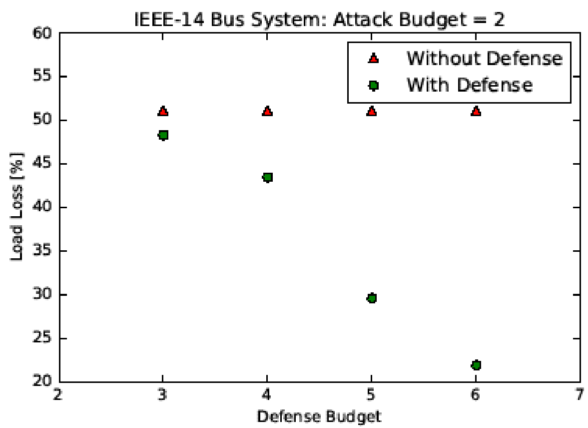
**Algorithm 2** Algorithm for Finding the Defense

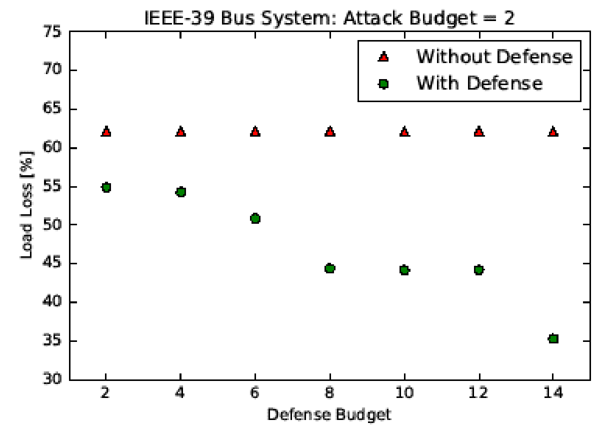
**Input:** $G_p, B_S, B_P, D_S$
**Initialize:** $S_d^{'} \leftarrow \emptyset, S_D \leftarrow \emptyset, L_w \leftarrow 100$
$S_{wo}, S_{wl}, S_{ws} \leftarrow \texttt{Get\_Attack}(G_p, B_S, B_P, \emptyset, \emptyset)$
**for** $i = 1, \ldots, D_S$ **do**
  $L_w \leftarrow 100$
  **if** $S_D! = \emptyset$ **then**
    $S_{ws} \leftarrow \texttt{Get\_Attack}(G_p, B_S, B_P, S_D, \emptyset)$
  **end if**
  **for all** $p \in S_{ws}$ **do**
    $S_{wo}, S_{wl}, S_{sub} \leftarrow \texttt{Get\_Attack}(G_p, B_S, B_P, S_D, p)$
    **if** $S_{wl} < L_w$ **then**
      $L_w \leftarrow S_{wl}$
      $S_d^{'} \leftarrow p$
    **end if**
  **end for**
  $S_D \leftarrow S_D \cup S_d^{'}$
**end for**
**return** $S_D$

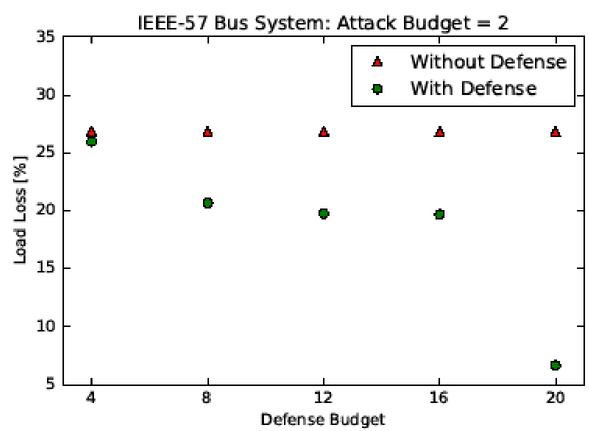
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Results for Static Attack and Defense

* **Defense** vs. **Attack**

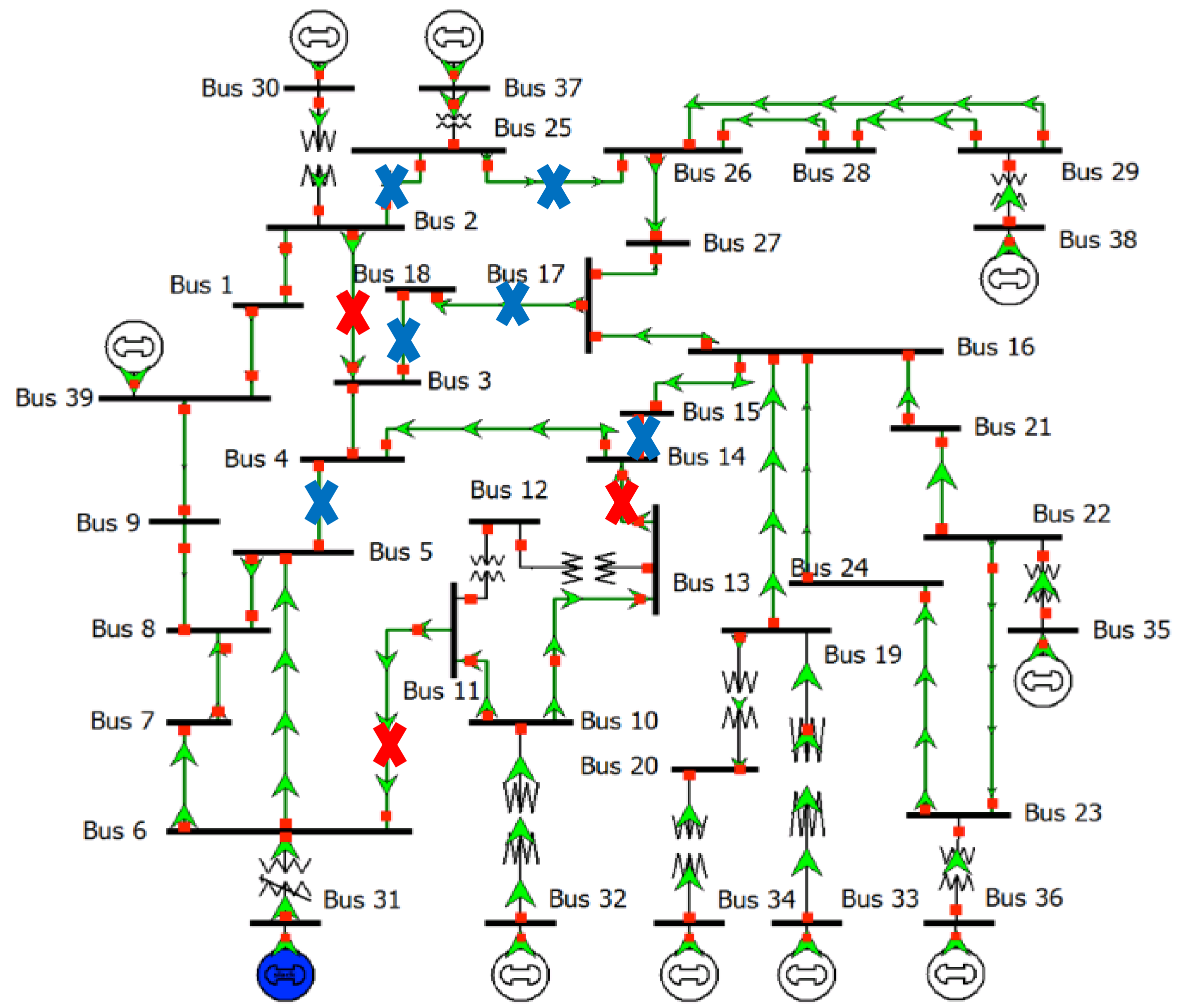



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Static Attack Scenario




- **Initial attacks**

↓ **delay**

- Stage1 Line Outages

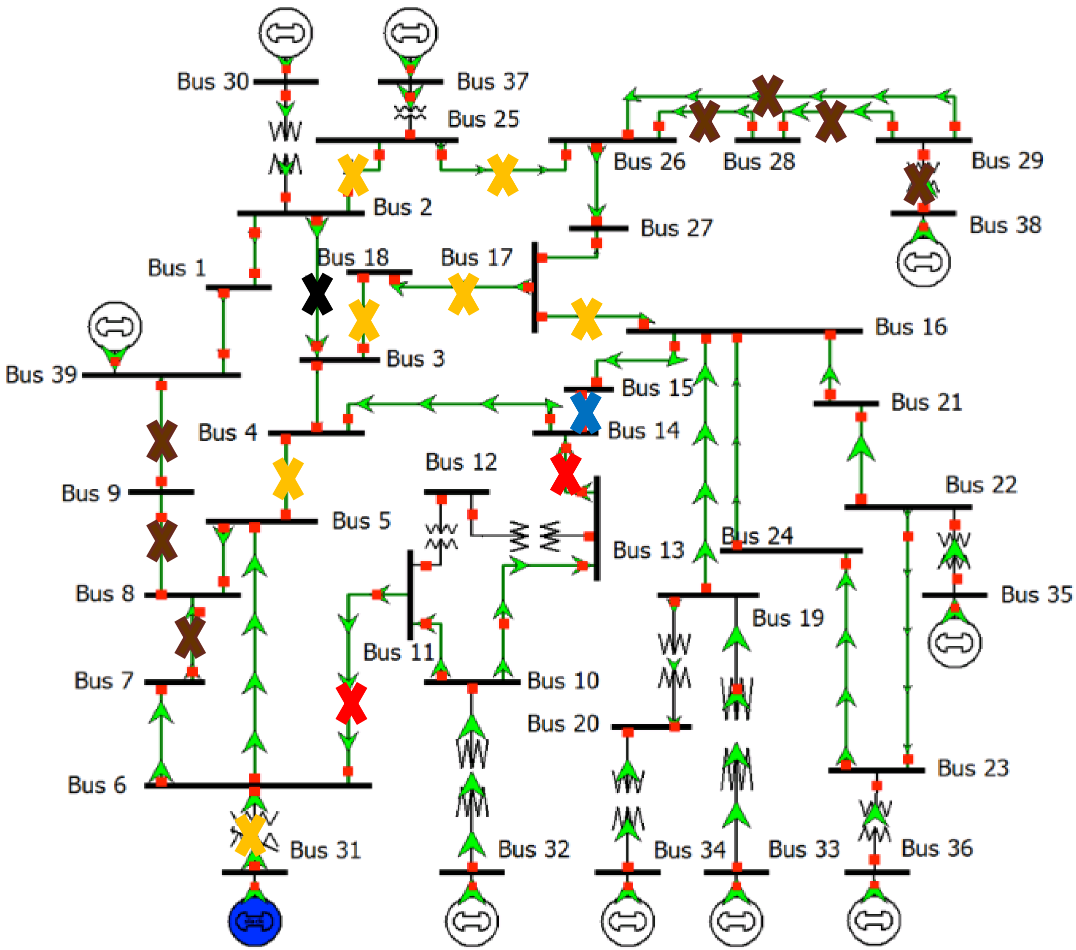
15.86%

**Ultimate Load Loss: 15.86%**

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

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# 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/

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Dynamic Attack Model

* Attack $A(k)$ is launched at timestep $k$
* Define attack history as $H(k) = \{A(i)\}_{i=1}^{k-1}$
* $F(H(k))$ provides system state $x(k)$, where $F(H(k))$ is the network config
* **Worst-case attack:**

$$\max_{A(1),\ldots,A(T)} \sum_{k=1}^{T} J(A(k), x(k))$$

$$\text{s.t. } x(k) = F(H(k))$$

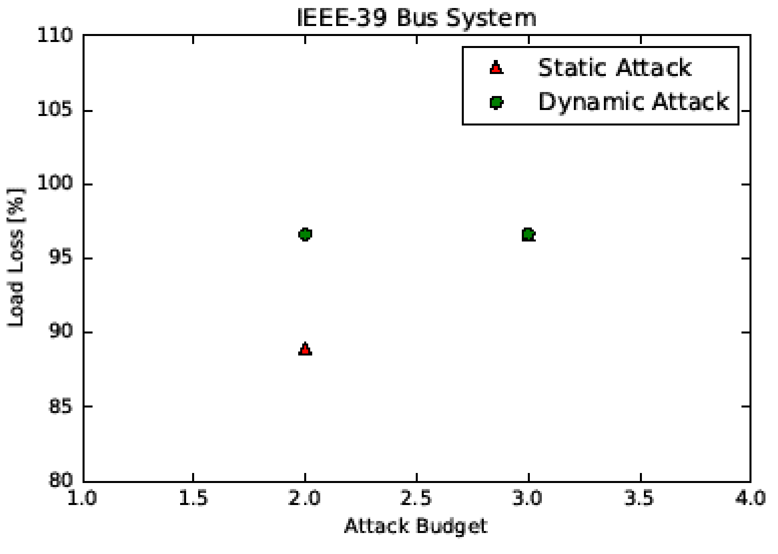
$$\sum_{k=1}^{T} |A(k)| \leq B$$

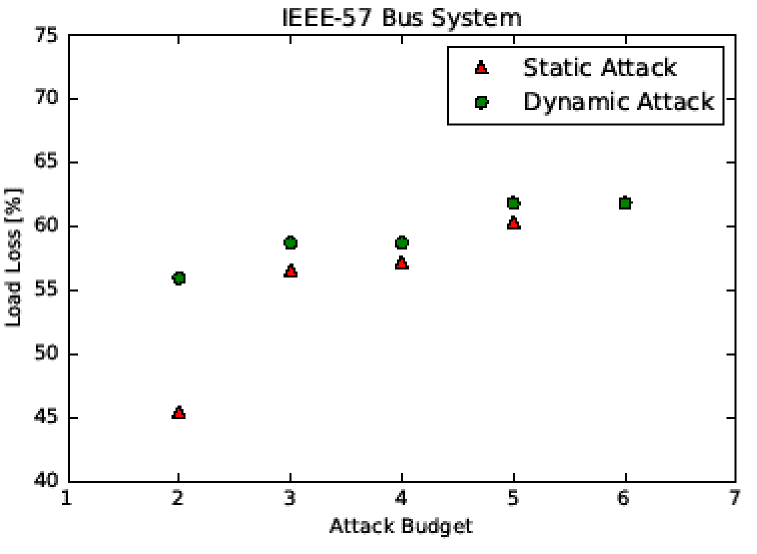
$$\forall k, k' \in \{1, \ldots, T\} : A(k) \cap A(k') = \emptyset$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Dynamic vs Static Attack Results

- Dynamic vs Static
- **Dynamic attack results in more load loss**



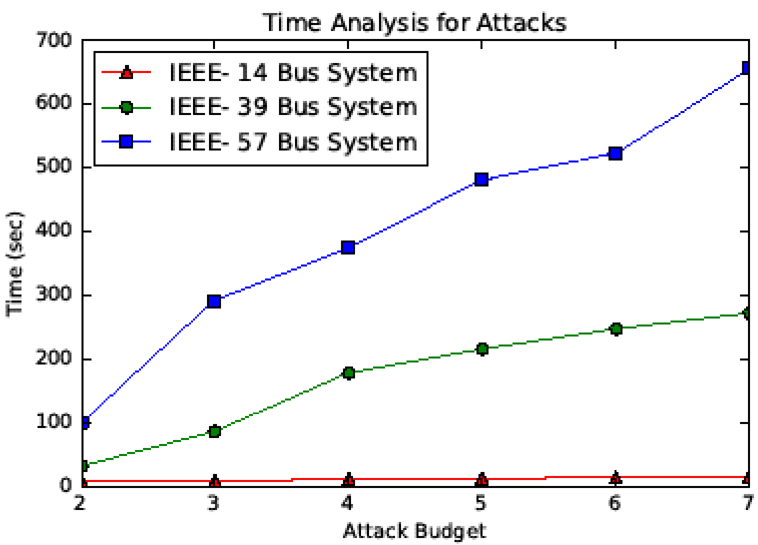



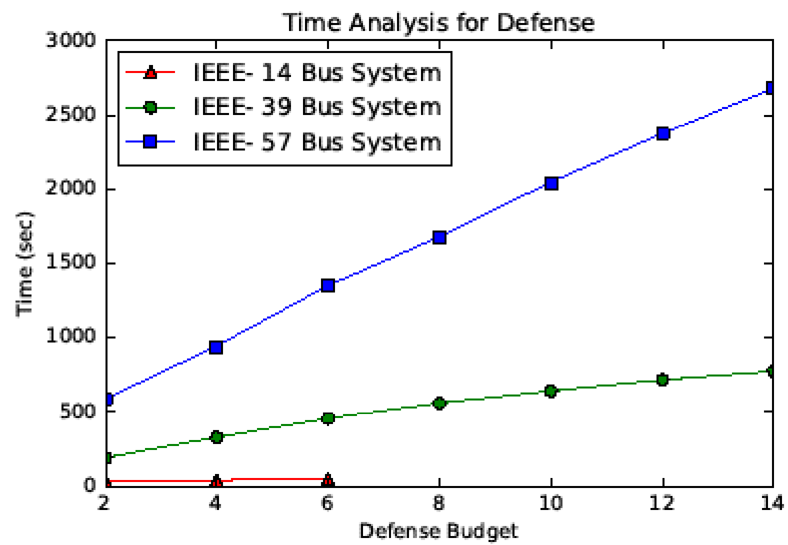

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# THANK YOU

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

# Static Attack and Defense Run Time




FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS