Protecting Power System Operations Against Cyber Attacks in the Presence of Renewables

Jasper Chumba, Kostas Hatalis, Dawon A. Jeong, Shalinee Kishore, Tianheng Sun, Chengbo Zhao, Lehigh University Department of Electrical and Computer Engineering

Background

- **Renewable generation** brings uncertainty while communication network opens up new avenues for cyber attacks in modern power grid.
- An **intelligent attacker**, using unsecured communication channels, could exploit uncertain nature of the renewable power to hide manipulative acts.
- No intrusion detection mechanisms available to protect power system operations against such attacks.
- The **proposed work** here aims to study and counter a new class of intelligent and dynamic attacks that mimic renewable generation patterns to interfere with the system stability.

Objective

- Develop and simulate attack models for renewable generations and be aware of their uncertainty.
- Develop the forecasting models for renewable generations.

Simulation and Result

As the wind generation is inherently intermittent and unstable due to the varying speed and direction, the load frequency model maintains the frequency deviation near to zero. Figure. 1 shows the load frequency control for two-interconnected control area and Figure. 2 is the simulation result of this model. From the result, the frequency deviation recedes to zero in the end. Additionally, in the two interconnected areas, the two control areas will assist each other.

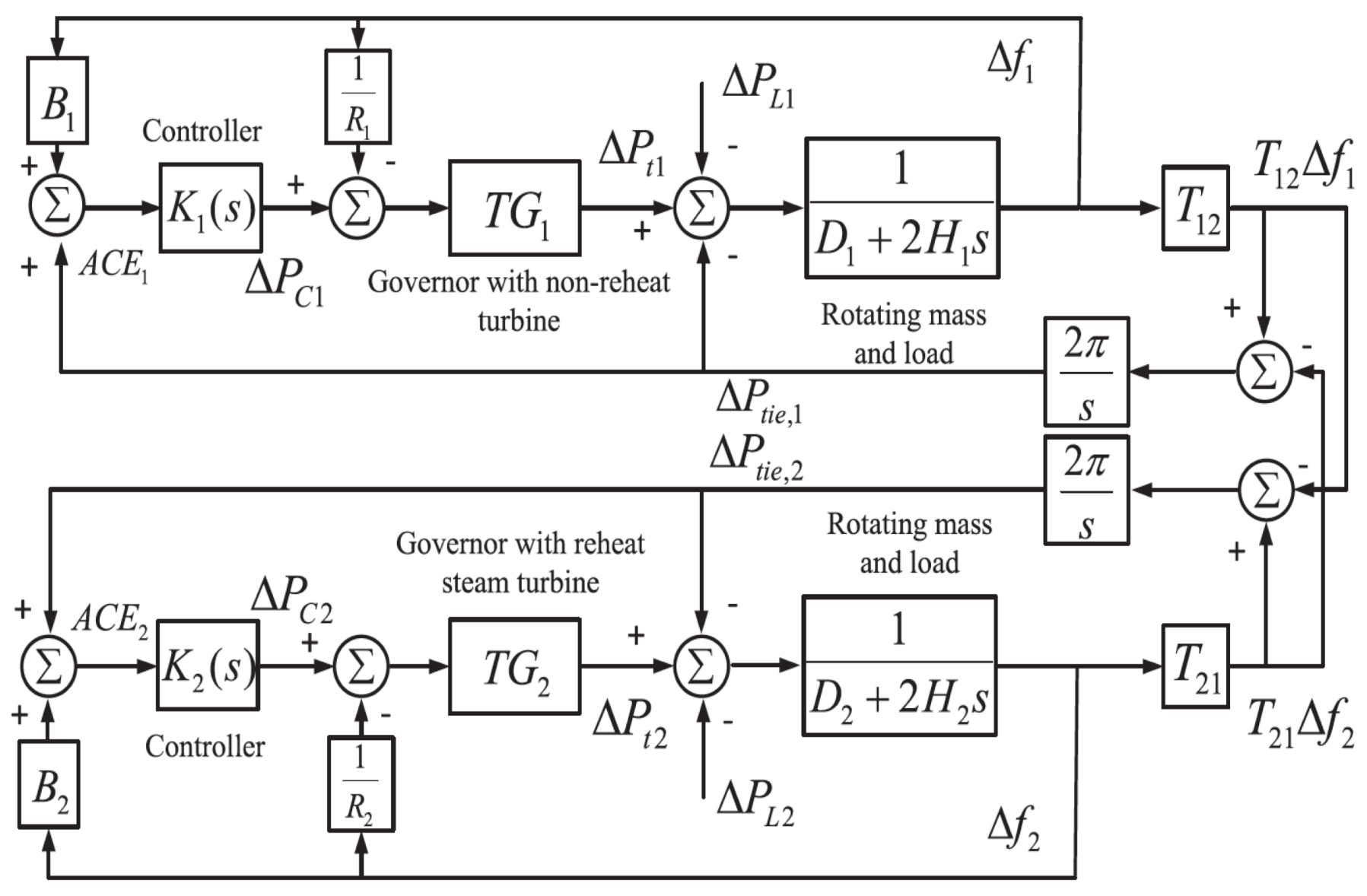

Figure. 1 Two-interconnected Area Model

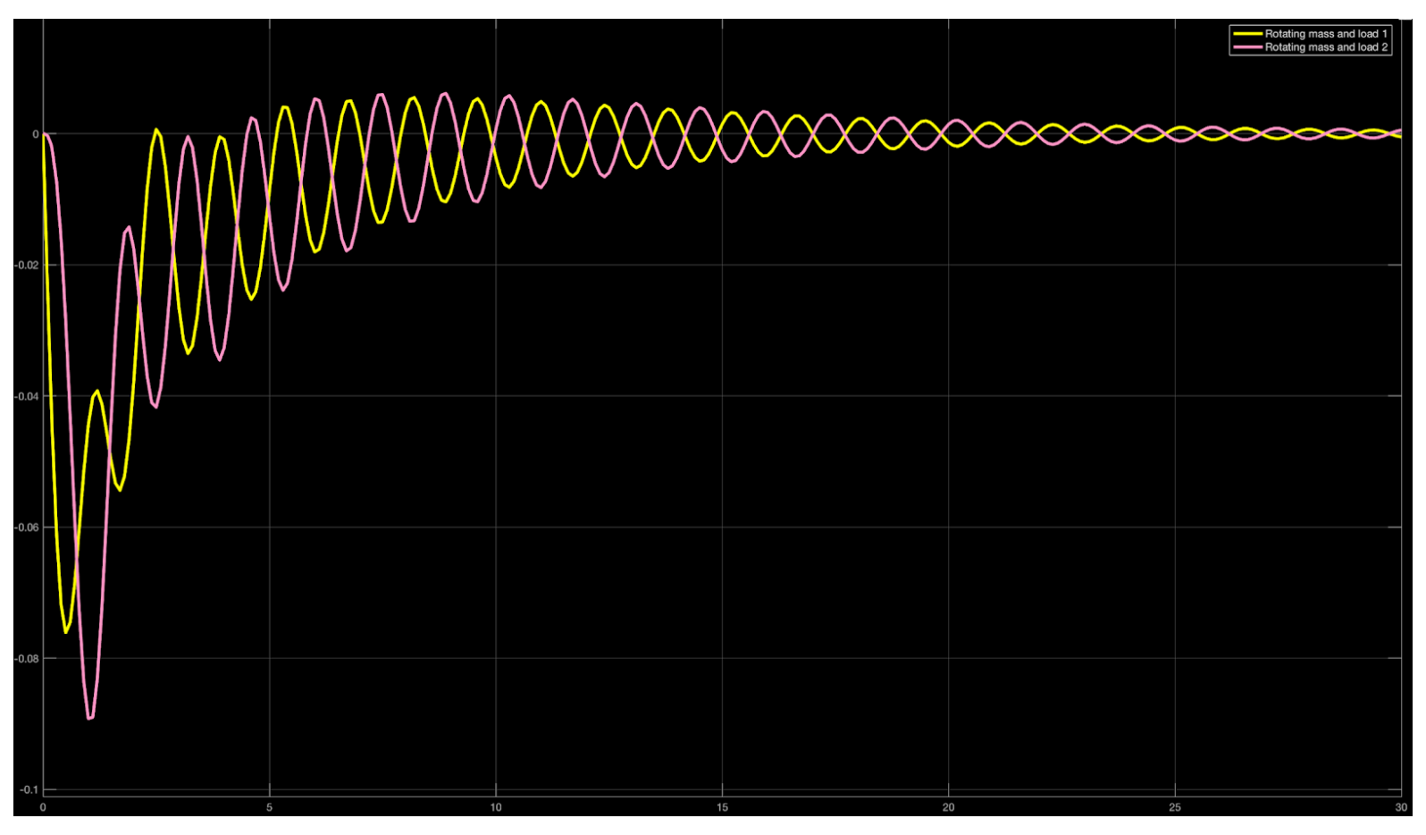

Figure. 2 Two-interconnected Area Simulation

Attack Models

- **Attack Constraints**
  - Frequency sensors are heavily monitored, hence we resolve to power sensors for implementing attacks.
  - FDI attack on power flow measurements must bypass Bad Data Detection(BDD) i.e there should be an attack vector
  - Attack must be stealthy and happen in the shortest Time To Emergency(TTE). TTE is the time from onset of attack to the first time of unsafe frequency deviation.

$$\Delta\omega(k+h)=\begin{bmatrix}\mathbf{u}_{H-1}\\ \vdots\\ \mathbf{u}_{h+k-l+1}\\ \mathbf{u}_{h+k-l}\\ \vdots\\ \mathbf{u}_{h}\\ \mathbf{u}_{h-1}\\ \vdots\\ \mathbf{u}_{0}\end{bmatrix}^{\intercal}\begin{bmatrix}\Delta\mathbf{p}_{k-H+h+1}\\ \vdots\\ \Delta\mathbf{p}_{l-1}\\ \Delta\mathbf{p}_{l}\\ \vdots\\ \Delta\mathbf{p}_{k}\\ \Delta\hat{\mathbf{p}}_{k+1}\\ \vdots\\ \Delta\hat{\mathbf{p}}_{k+h}\end{bmatrix}+\begin{bmatrix}\mathbf{v}_{H-1}\\ \vdots\\ \mathbf{v}_{h+k-l+1}\\ \mathbf{v}_{h+k-l}\\ \vdots\\ \mathbf{v}_{h}\\ \mathbf{v}_{h-1}\\ \vdots\\ \mathbf{v}_{0}\end{bmatrix}^{\intercal}\begin{bmatrix}\mathbf{0}\\ \vdots\\ \mathbf{0}\\ \mathbf{Ta}_{l}\\ \vdots\\ \mathbf{Ta}_{k}\\ \mathbf{Ta}_{k+1}\\ \vdots\\ \mathbf{Ta}_{k+h}\end{bmatrix}$$

H=Horizon window
ΔP=Load change
U&V=Coefficients based on generator constants
h=Attack iterator
k=Current AGC cycle
l=Onset of attack
W=number of sensors that an attacker has write access.

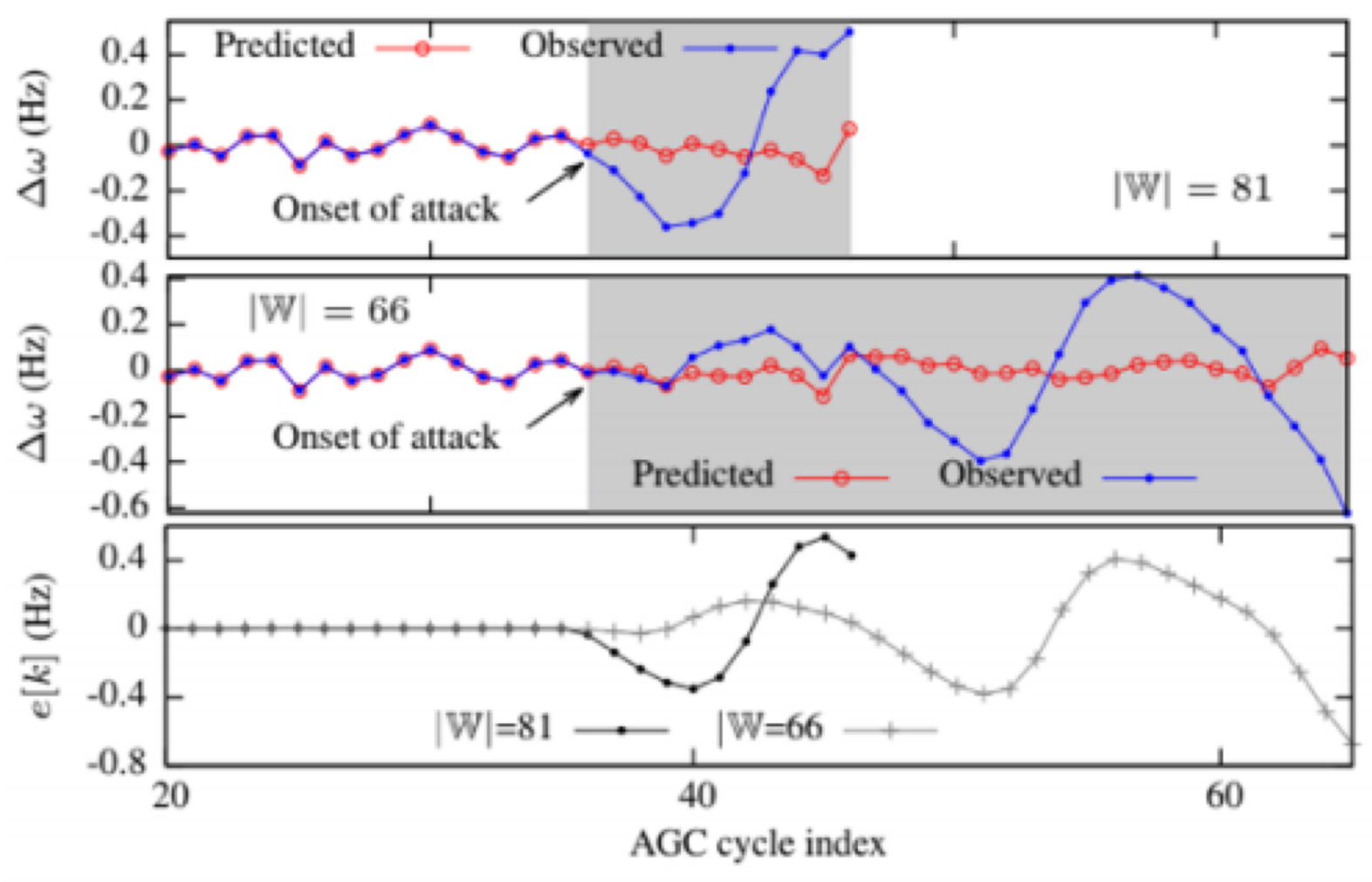

Figure. 3 Attack Sequence Simulation Results

Mathematical Model

- **Time Series Decomposition**

Check for stationarity. If not, keep applying time series decomposition until it becomes stationary. Then check if stationarity series is white noise. If not, select an ARMA model then subtract the ARMA model from the stationary series to get the residual series.

- **Test for Stationarity**

No trend, seasonality, or major shifts. Flat simple moving average and rolling variance. Zero or fast decay to zero autocorrelation

Time series patterns: Trend(T), Seasonality(S), Cycles(C), irregular fluctuations (I)

Additive model: $y_t = S_t + T_t + C_t + I_t$

- **SARIMA Model**

Seasonal autoregressive integrated moving average (SARIMA) model is used to trend the seasonality:

SARIMA(p,d,q)(P,D,Q)[S]

- **Hypothesis Test**
  - Generalized Likelihood Ratio Test (GLRT)

First set the null hypothesis to find the distribution of attacks. Then, calculate the p-value for each hypothesis. Last, find threshold value from the equity.

$$\mathcal{H}_0 : x_t \overset{\text{iid}}{\sim} \mathcal{N}(0,\sigma^2), t = 1, ..., N$$

$$\mathcal{H}_1 : x_t \overset{\text{iid}}{\sim} \mathcal{N}(A,\sigma^2), A > 0, t = 1, ..., N$$

$$\frac{p(\mathbf{x}; A, \mathcal{H}_1)}{p(\mathbf{x}; \mathcal{H}_0)} = \frac{\frac{1}{\sqrt{2\pi\sigma^2}} \exp^{-\frac{1}{2\sigma^2}\sum_{t=1}^{N}(x_t-A)^2}}{\frac{1}{\sqrt{2\pi\sigma^2}} \exp^{-\frac{1}{2\sigma^2}\sum_{t=1}^{N}x_t^2}} \underset{H_0}{\overset{H_1}{\gtrless}} \gamma$$

$$P_{FA} = P(T(\mathbf{x}) > \gamma'; \mathcal{H}_0) = Q\left(\frac{\gamma'}{\sqrt{\sigma^2/N}}\right) \Rightarrow \gamma' = \sqrt{\frac{\sigma^2}{N}}Q^{-1}(P_{FA})$$

- K Nearest Neighbors (KNN)

The KNN has two different outputs:
Classification: the output is a class membership
Regression: the output is a property value

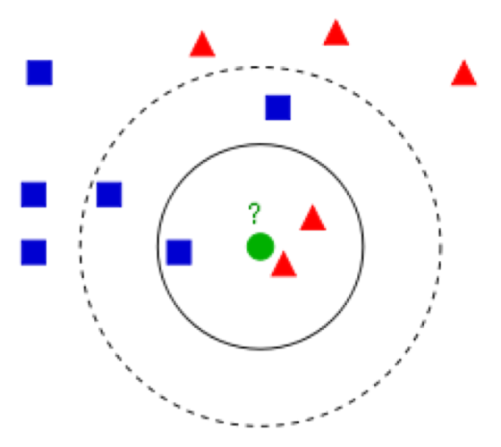

Figure. 4 K Nearest Neighbors Example

- **Accuracy**

Mean squared error	$\text{MSE} = \frac{1}{n}\sum_{t=1}^{n} e_t^2$
Root mean squared error	$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{t=1}^{n} e_t^2}$
Mean absolute error	$\text{MAE} = \frac{1}{n}\sum_{t=1}^{n} \lvert e_t \rvert$
Mean absolute percentage error	$\text{MAPE} = \frac{100\%}{n}\sum_{t=1}^{n} \left\lvert \frac{e_t}{y_t} \right\rvert$

Summary

Attacks on the grid power sensors is feasible and can be done stealthy in the presence of renewable energy. More accurate future-prediction of renewable energy will help detect and eliminate attacks in the grid system. Our proposed models for accurately predicting renewable energy as discussed above are important steps towards protecting power grids against cyber attacks in the presence of renewables.

Acknowledgement(s):

David and Lorraine Freed Undergraduate Research Symposium, Lehigh University

LEHIGH UNIVERSITY | P.C. ROSSIN COLLEGE OF ENGINEERING AND APPLIED SCIENCE