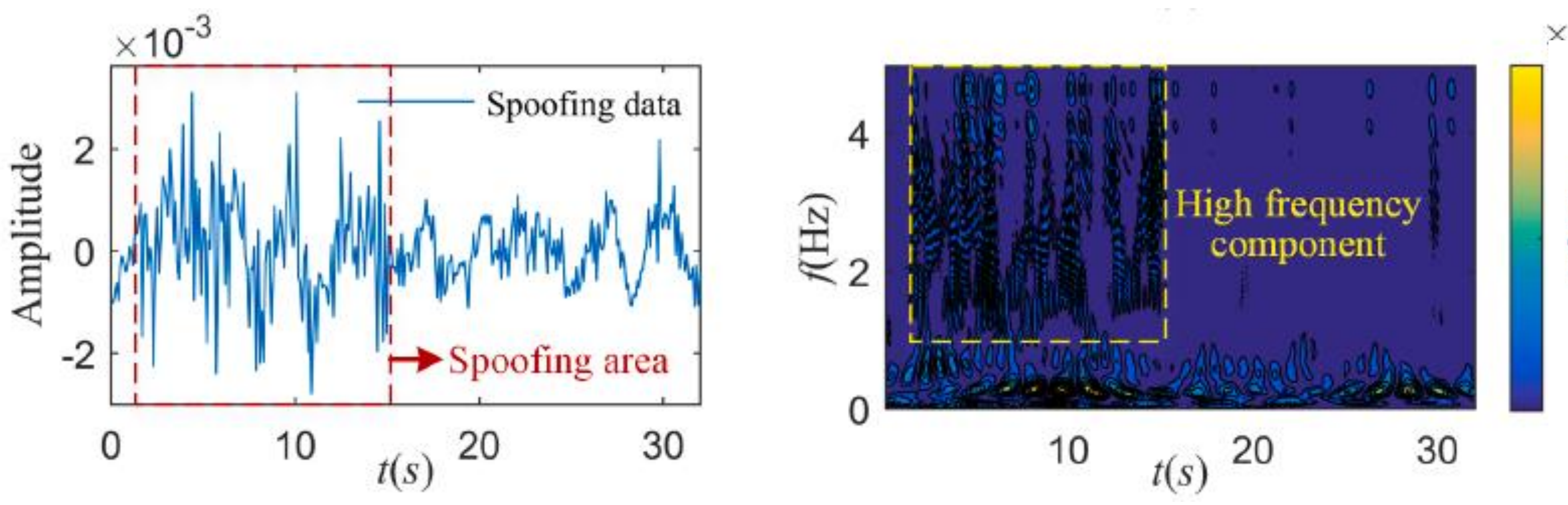
CPS: Small: Data-driven Real-time Data Authentication in Wide-Area Energy Infrastructure Sensor Networks

PI: Yilu Liu, University of Tennessee, Knoxville; Oak Ridge National Laboratory

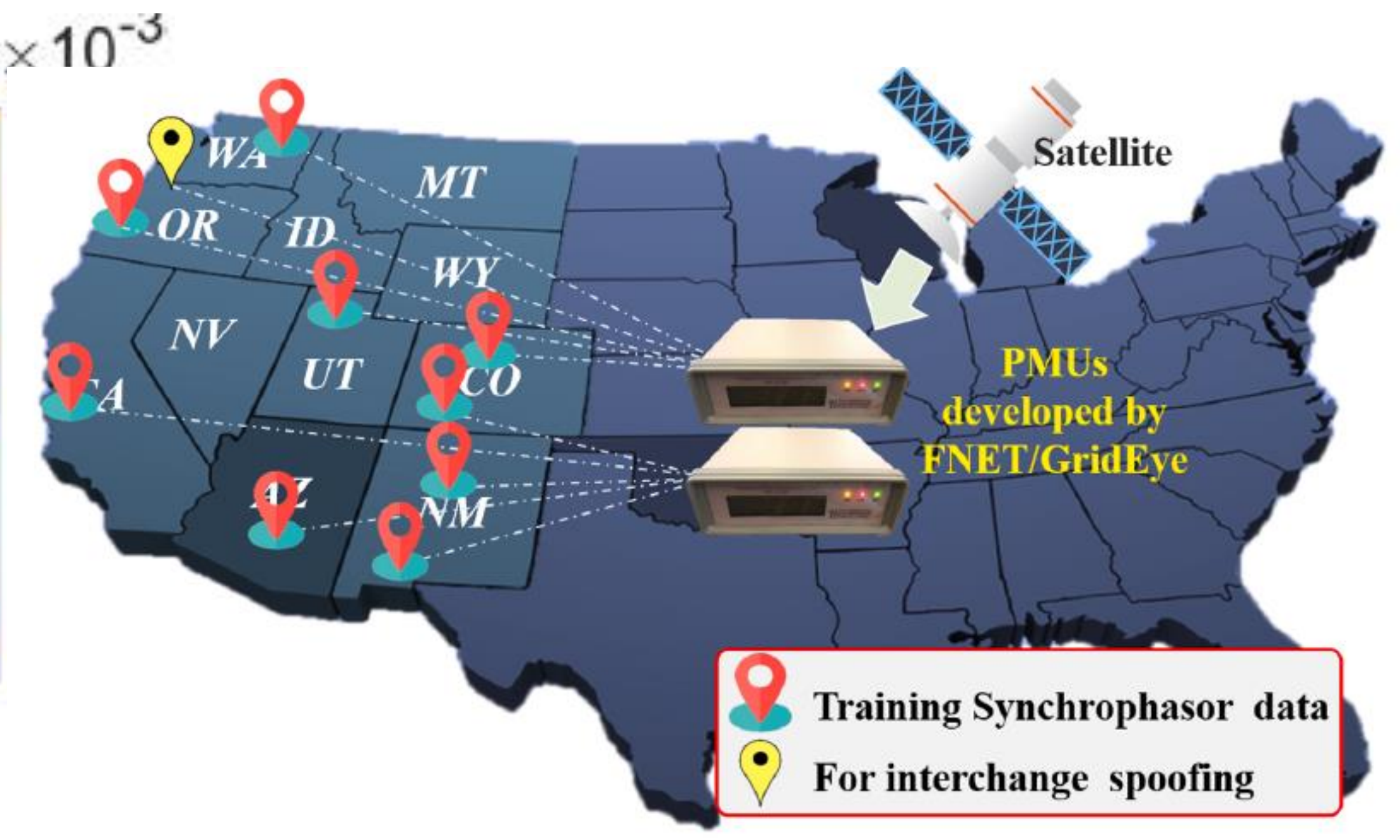
Co-PI: He Yin, University of Tennessee, Knoxville

Challenge:

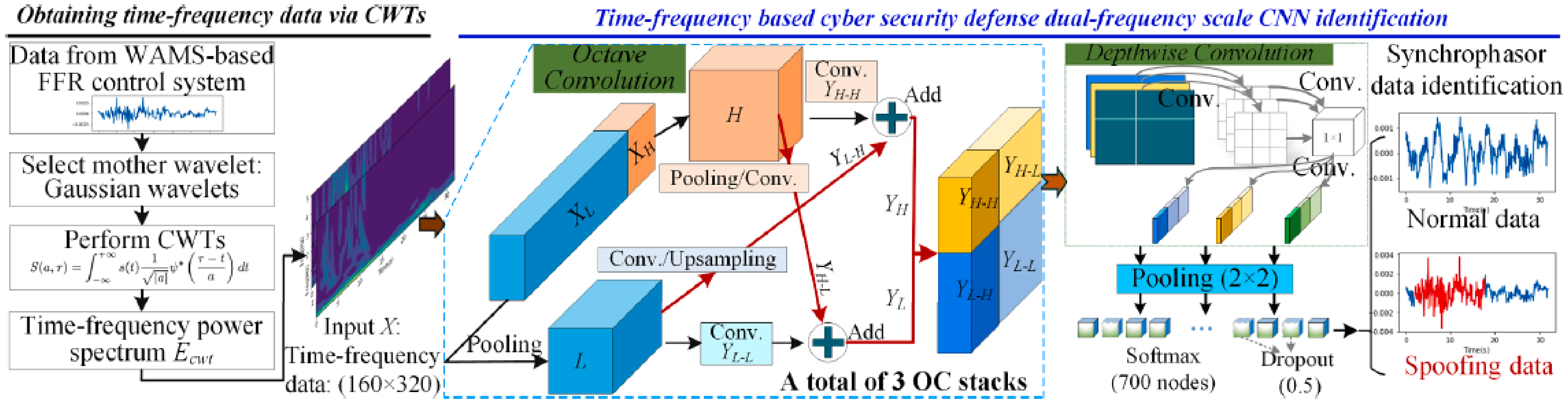
Measurements in wide-area energy infrastructure sensor networks are vulnerable to attacks from malicious cyber hackers.



Spoofing data and detection



Sensor deployment locations


Obtaining time-frequency data via CWTs
Data from WAMS-based FFR control system
Select mother wavelet: Gaussian wavelets
Perform CWTs
$S(a,\tau)=\int_{-\infty}^{+\infty} s(t)\frac{1}{\sqrt{|a|}}\psi^*\left(\frac{\tau-t}{a}\right)dt$
Time-frequency power spectrum E_{cwt}
Input X: Time-frequency data: (160×320)
Time-frequency based cyber security defense dual-frequency scale CNN identification
Octave Convolution
H
X_H
X_L
L
Pooling
Conv. $Y_{H\text{-}H}$
Add
Pooling/Conv.
$Y_{L\text{-}H}$
Y_H
$Y_{H\text{-}L}$
Conv./Upsampling
Conv. $Y_{L\text{-}L}$
Add
Y_L
$Y_{H\text{-}H}$
$Y_{H\text{-}L}$
$Y_{L\text{-}H}$
$Y_{L\text{-}L}$
A total of 3 OC stacks
Depthwise Convolution
Conv.
Conv.
1×1
Conv.
Pooling (2×2)
Softmax (700 nodes)
Dropout (0.5)
Synchrophasor data identification
Normal data
Spoofing data

Data acquisition

Data Convolution

Neural Network

Attack detection

Cyber security defense framework

Scientific Impact:

- A new spatial signature extraction method to authenticate sensor data sources.
- A time-frequency-based cyber security defense framework is proposed to detect the cyber spoofing of wide-area sensor data in fast frequency reserve control systems.
- These methods have been validated using actual sensor data collected by FNET/GridEye (link) in U.S. power grids.

Broader Impact:

Impact on society: Add an addition level of security beyond purely cyber or physical methods.

Education and outreach: Provide power grid and CPS security education and training resources, including seminars, course projects, lab tours, and demos to high-school, pre-college, REU, and graduate students.

Quantified potential impact: The detection rate for data spoofing attacks in CPS > 90%

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Award ID#: 1931975