CPS: Small: Fusion of Sensory Data and Expansivity of System Dynamics for Detection and Separation of Signature Anomaly in Energy CPS Wide-Area Monitoring and Control

Kaveri Mahapatra (KZM221@psu.edu), PI: Nilanjan Ray Chaudhuri (nuc88@engr.psu.edu)
The Pennsylvania State University, University Park, PA

PROBLEM/CONTEXT

1. Spurious or maliciously injected sensor data originating from cyber-attacks can have similar appearance as system's dynamic response.
2. They can seriously jeopardize the monitoring and stabilization controls of power grids. This can lead to system-wide blackouts and cost our economy billions of dollars.

OVERARCHING GOAL

Can we leverage the physical system's expansive dynamic behavior to distinguish disturbances from data anomalies? To that end, the aim is to bridge the gap between developments in the area of singular value perturbation theory and Principal Component Analysis (PCA) – traditionally focused on the 'signals' side of the CPS, with the intrinsic properties from the 'systems' side of the CPS.

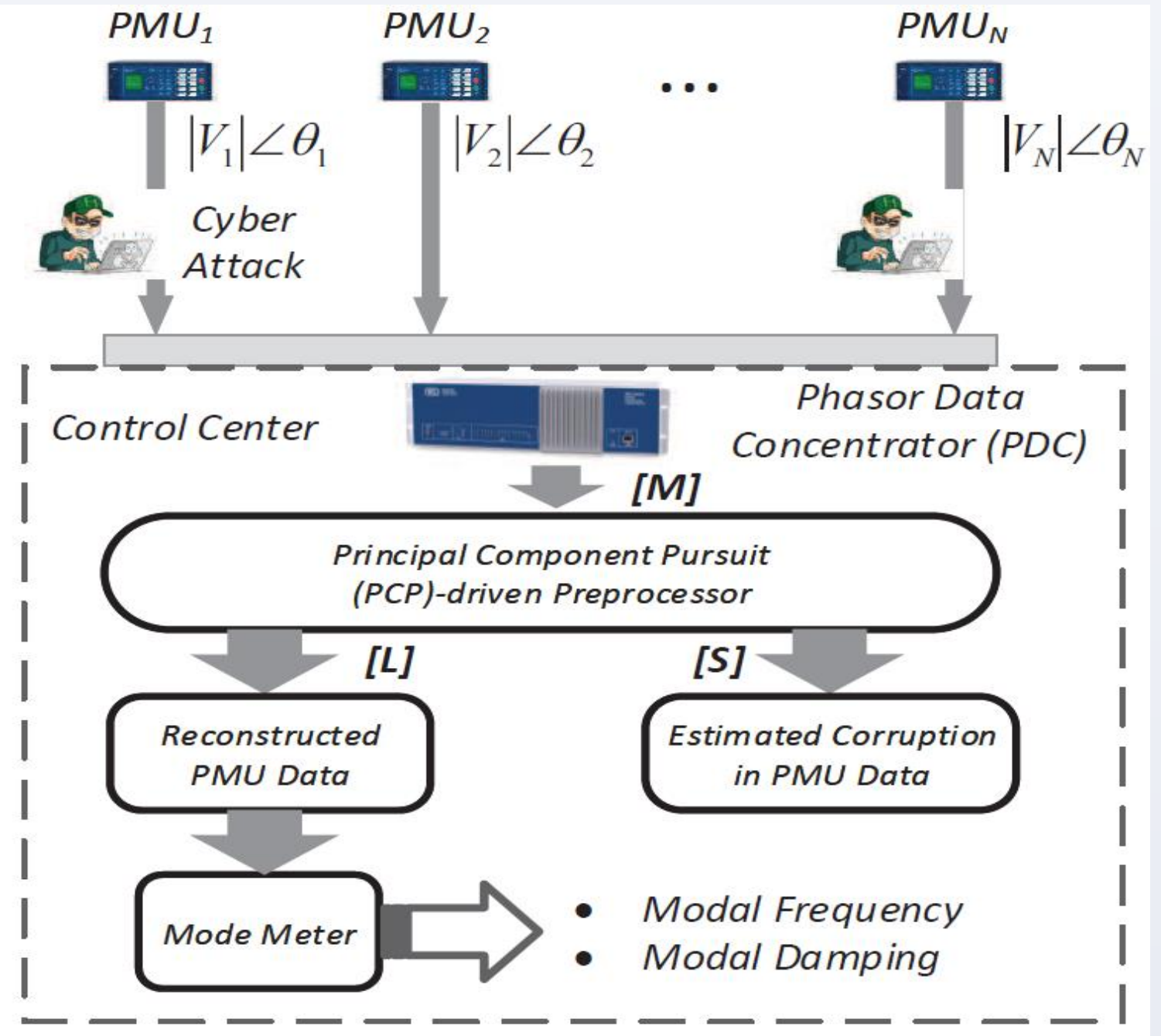
KEY IDEAS

1. Establish bounds on deviations in the Principal Component (PC) scores in terms of the system state matrices.
2. Bounds explicitly show the effect of the system matrices associated with the nominal and disturbance states on PC score deviations.
3. Apply emerging concepts of Principal Component Pursuit and Robust PCA to separate the anomalous signatures and correct the data for real-time applications.

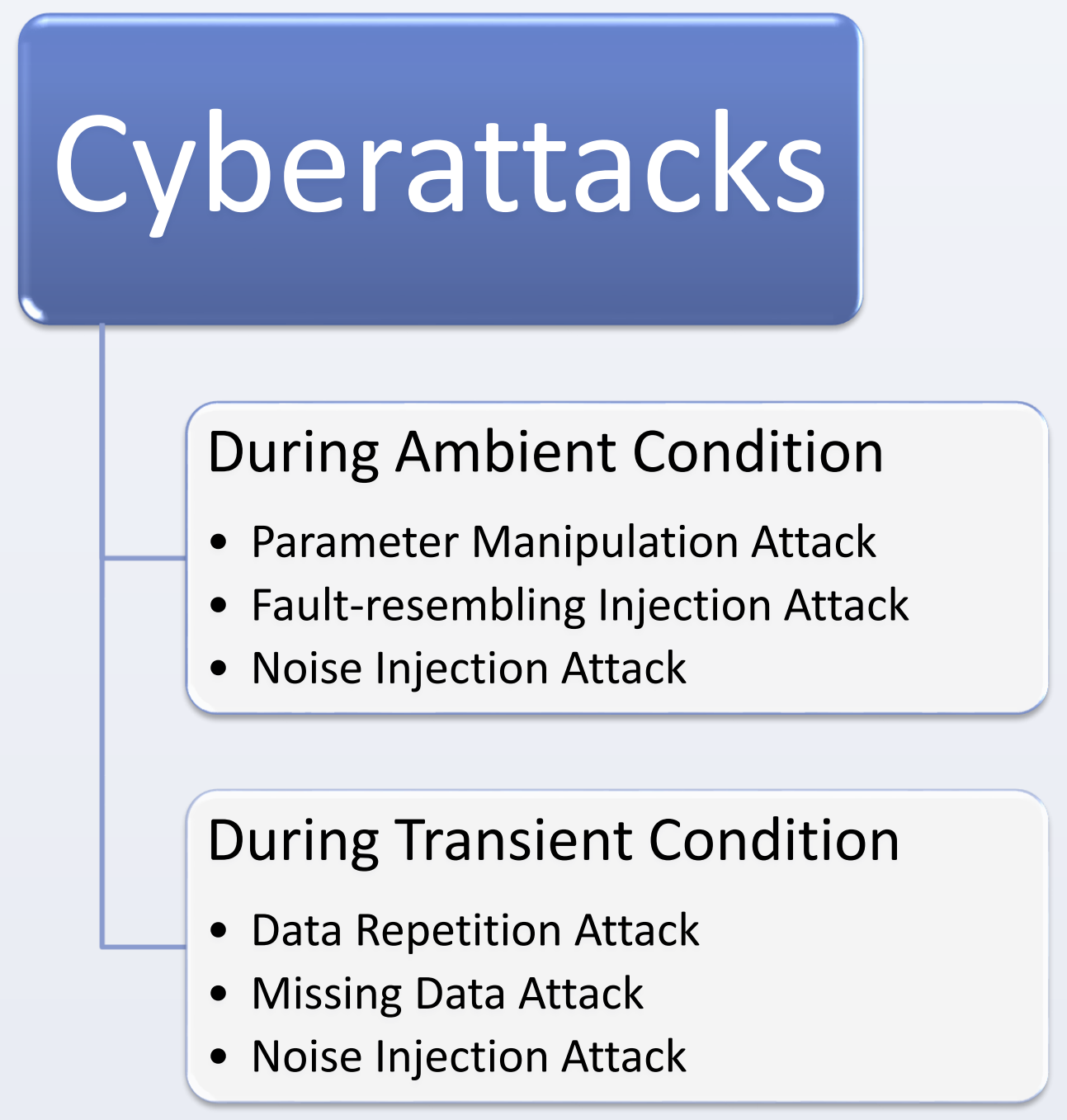
MAIN DEVELOPMENTS

1. A Robust PCA algorithm using Principal component pursuit (PCP) technique is proposed for an overlapping window framework of PMU measurements.
2. Any malicious data injections in PMU measurements is formulated as a PCP problem and is solved using an alternating direction-based optimization algorithm.
3. PCP aims to recover a low rank matrix (Original, L) from highly corrupted measurements (Corrupted, M = L+S) by solving a convex program.
4. The input to PCP is the corrupted measurement matrix, M which consists of time series voltage phasor data obtained from PMUs. The outputs are the matrices corresponding to the reconstructed signals, (L) and estimated corruption (S) in PMU data. Reconstruction of the PMU signals is further analyzed by the mode metering algorithms.

1. Proposed architecture for malicious corruption-resilient wide-area oscillation monitoring algorithm



Brief Summary of Results

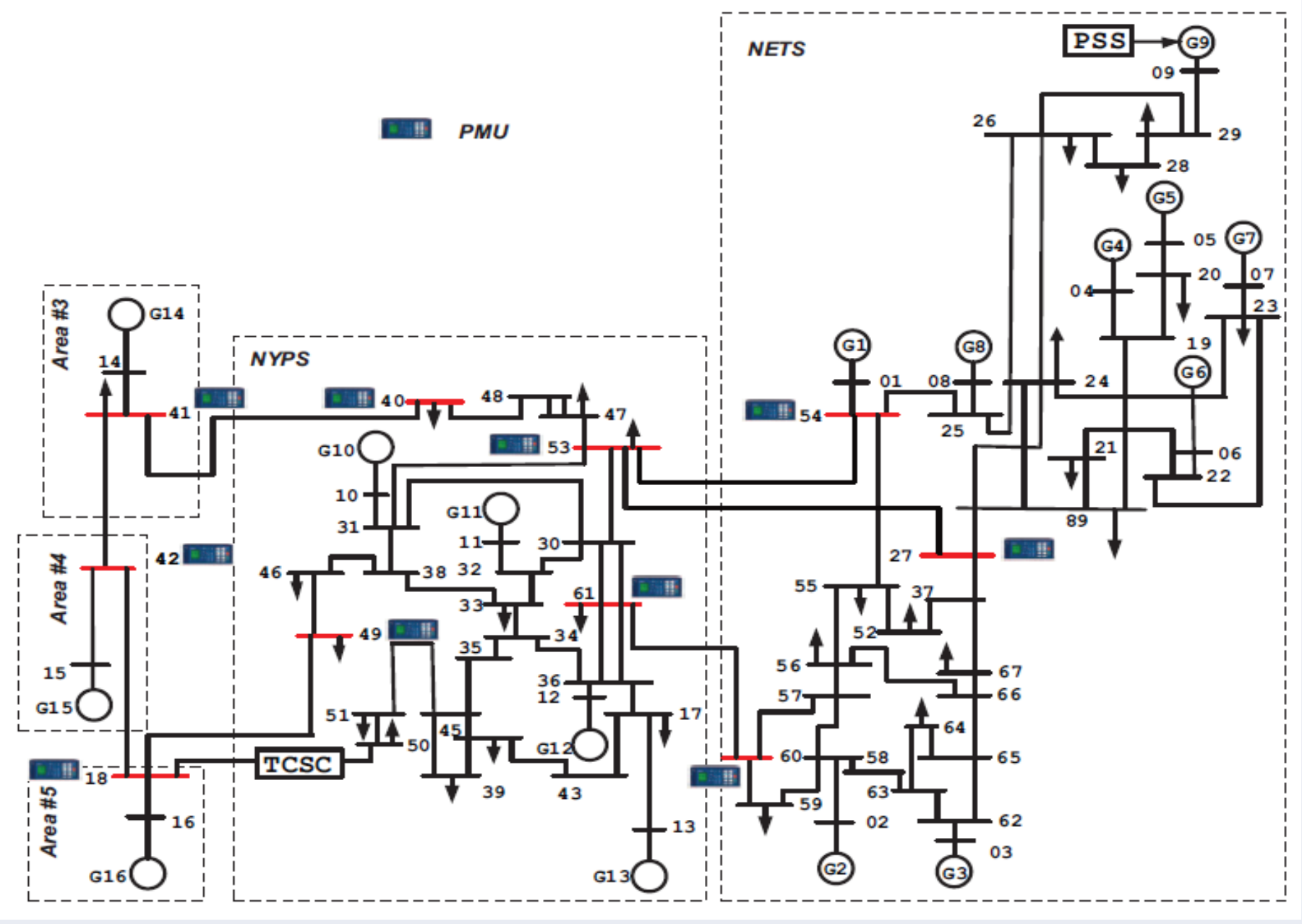


Cyberattacks

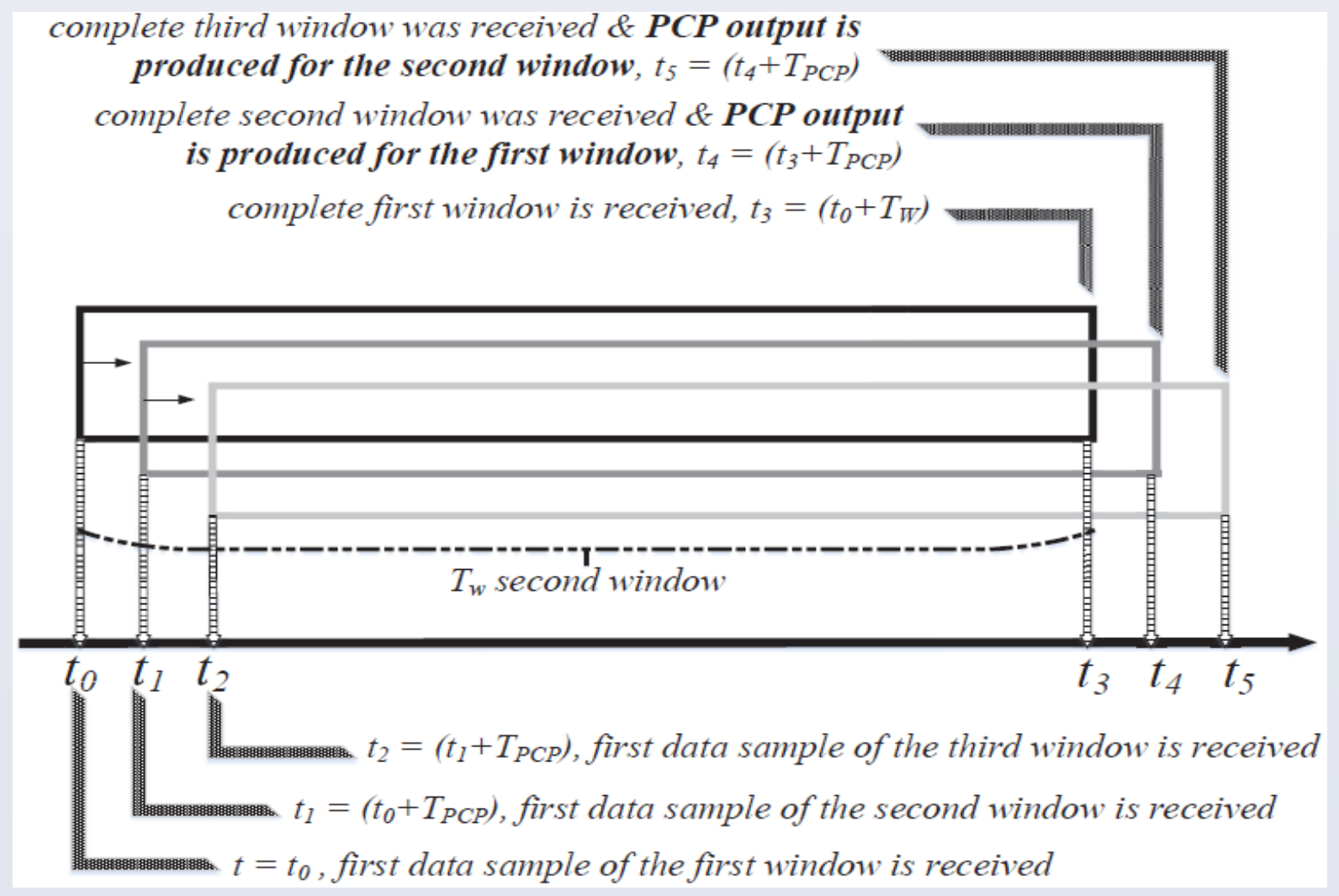
During Ambient Condition
- Parameter Manipulation Attack
- Fault-resembling Injection Attack
- Noise Injection Attack

During Transient Condition
- Data Repetition Attack
- Missing Data Attack
- Noise Injection Attack

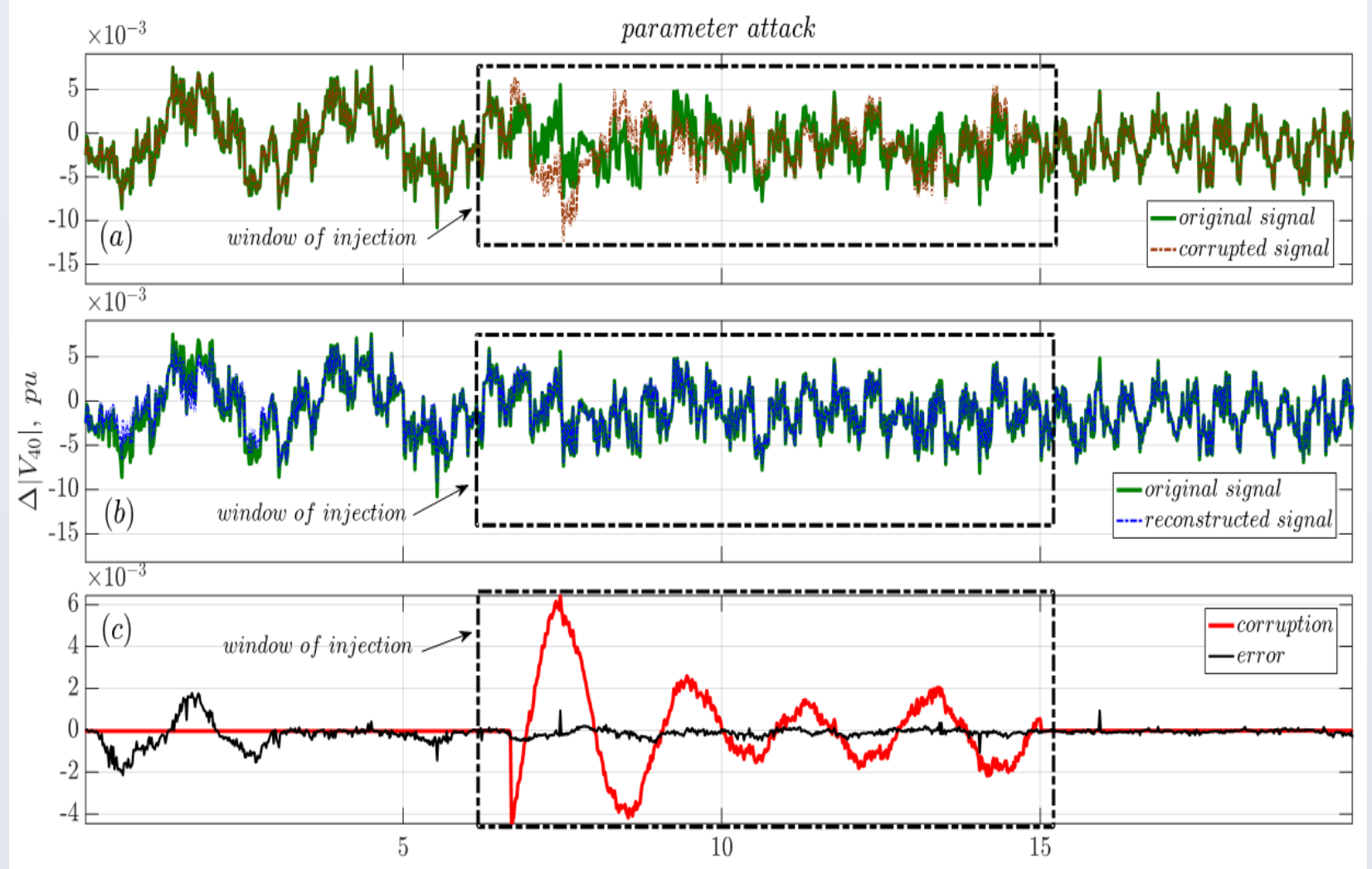
2. Test System: 16-machine, 5-area New England-New York system with PMU buses highlighted in red



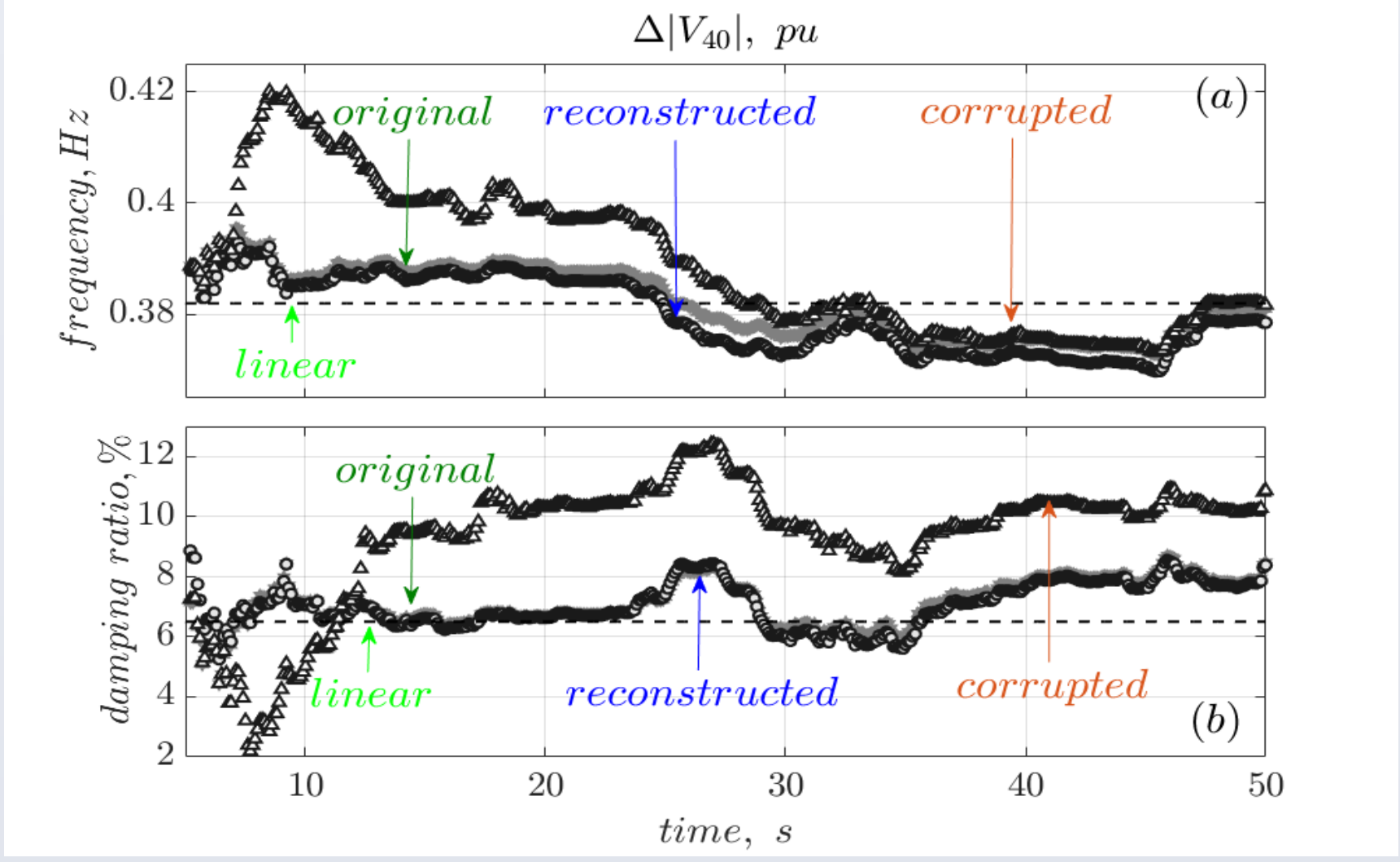
3. Proposed 'Overlapping Window' framework


complete third window was received & PCP output is produced for the second window, $t_5 = (t_4+T_{PCP})$
complete second window was received & PCP output is produced for the first window, $t_4 = (t_3+T_{PCP})$
complete first window is received, $t_3 = (t_0+T_W)$
T_w second window
t_0 t_1 t_2 t_3 t_4 t_5
$t_2 = (t_1+T_{PCP})$, first data sample of the third window is received
$t_1 = (t_0+T_{PCP})$, first data sample of the second window is received
$t = t_0$, first data sample of the first window is received

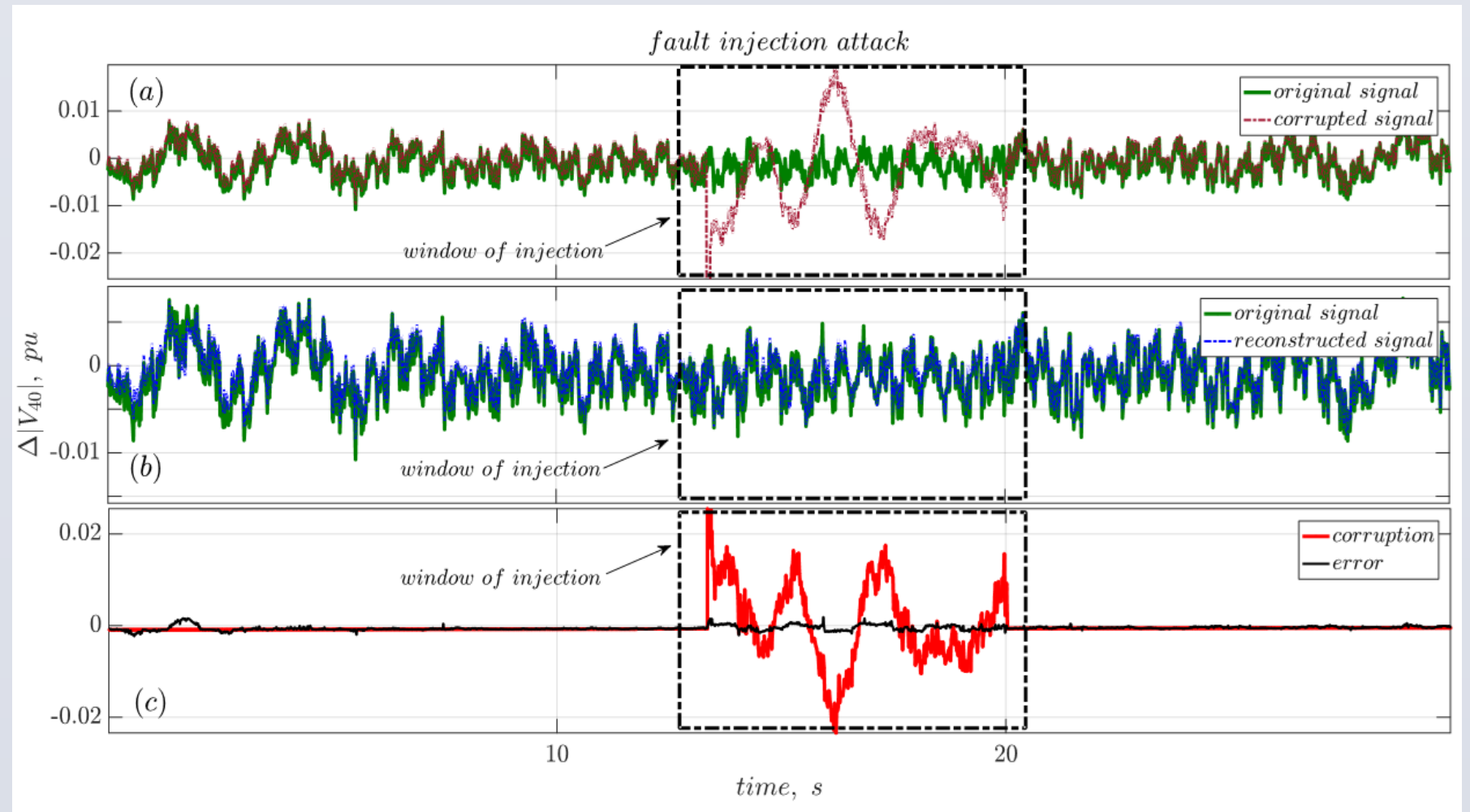
4. Parameter manipulation attack in a signal



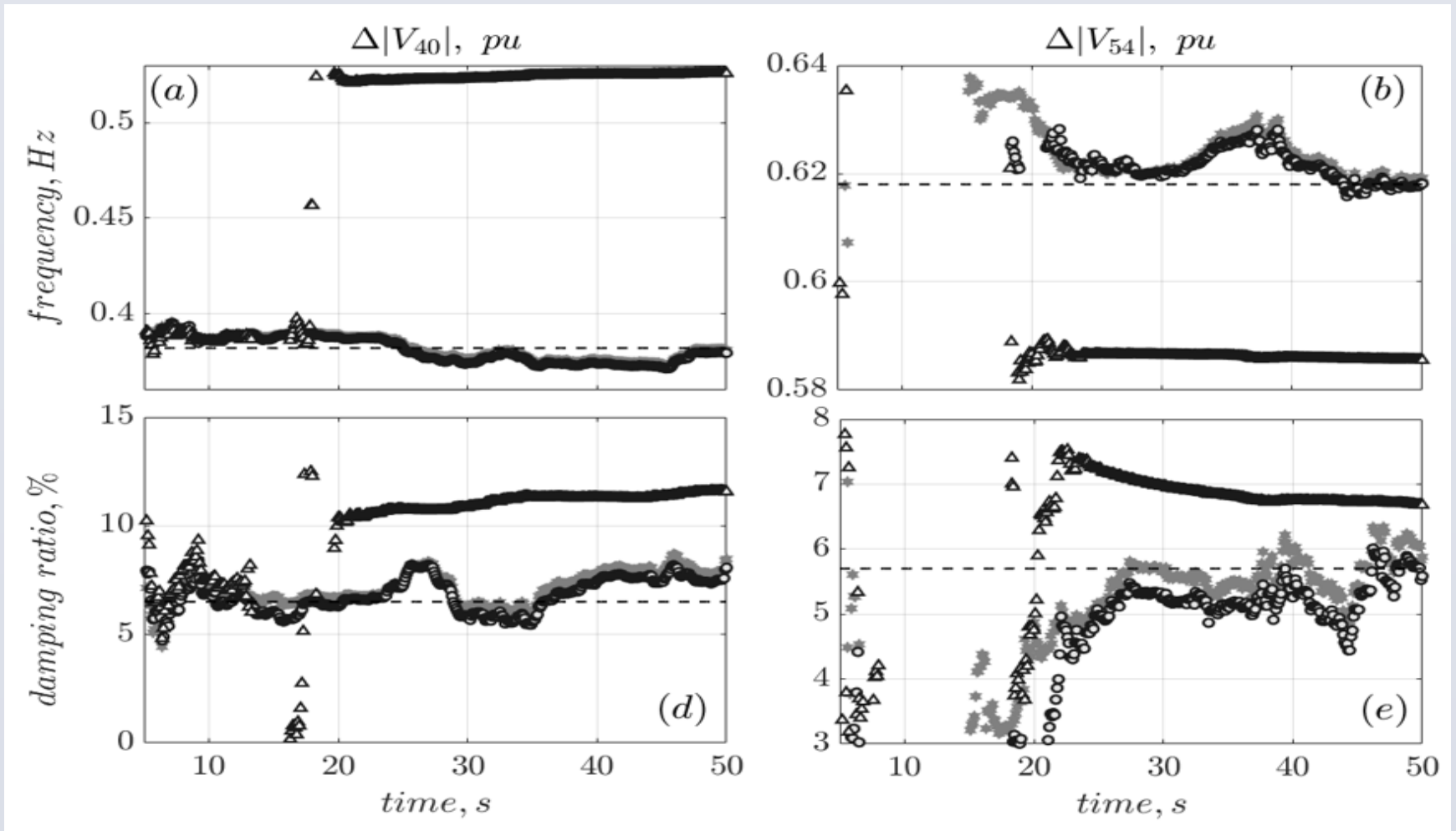
5. Corresponding estimated Frequency and Damping ratio



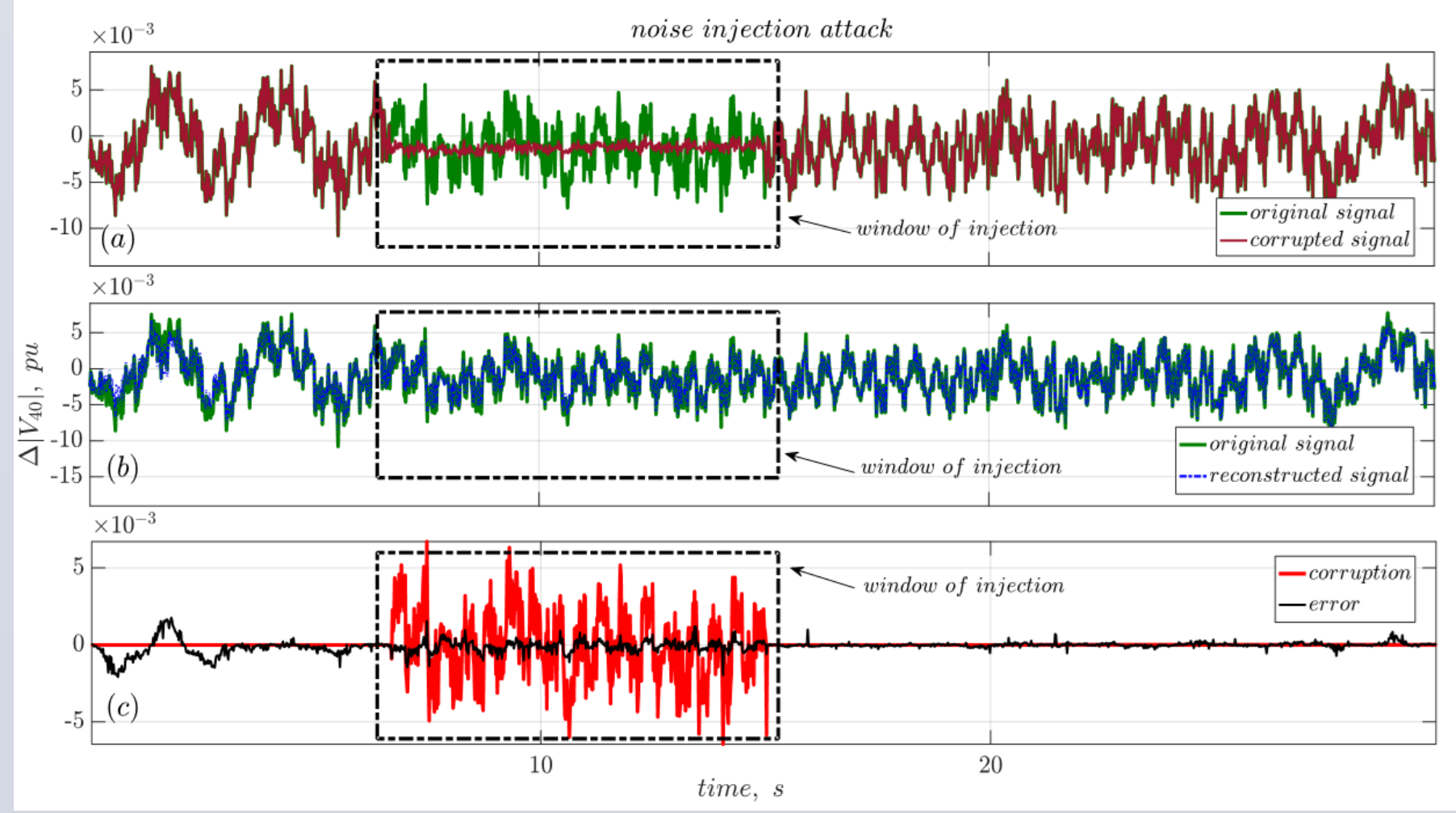
6. Fault injection attack during ambient condition



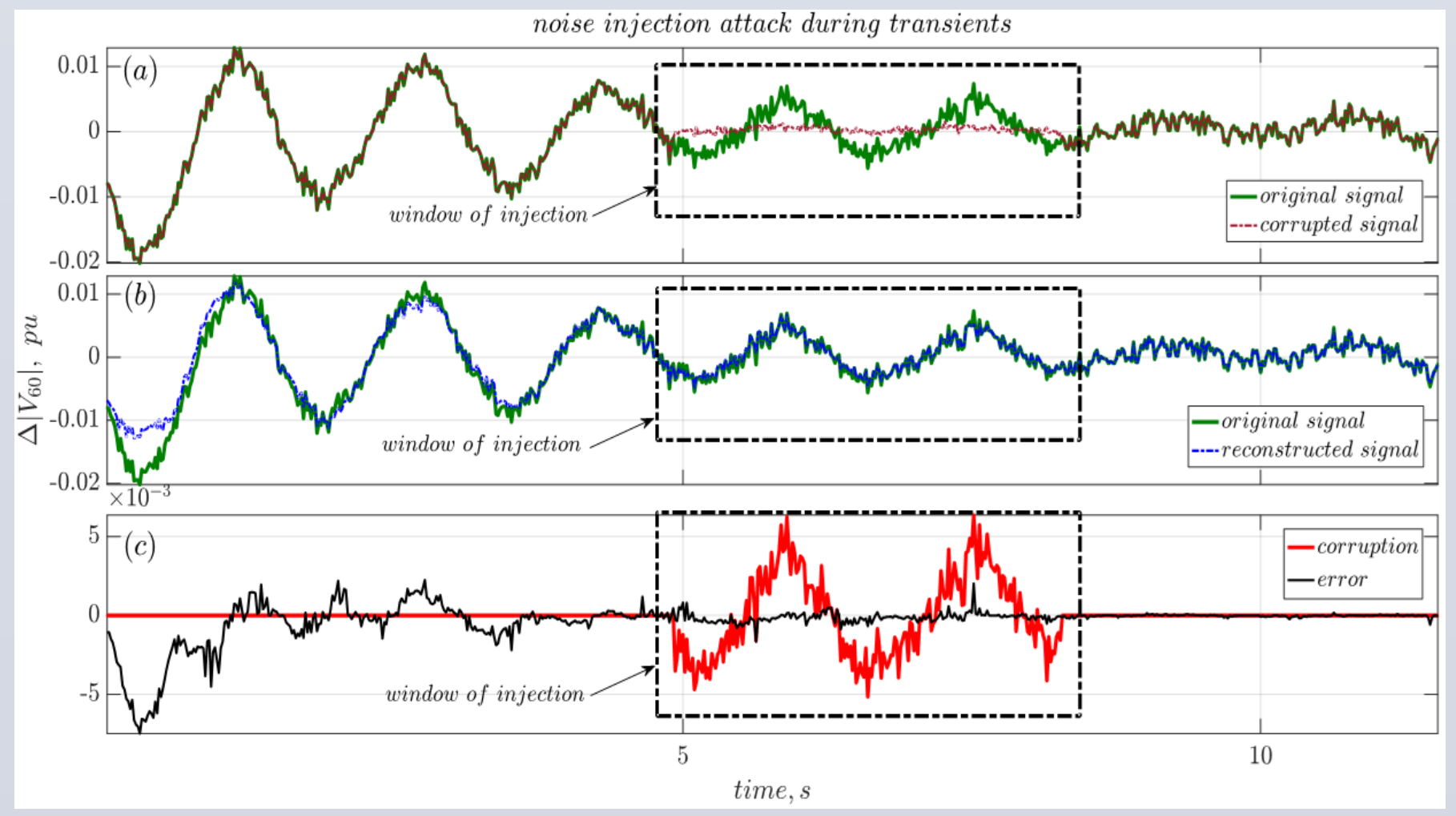
7. Corresponding estimated Frequency and Damping ratios



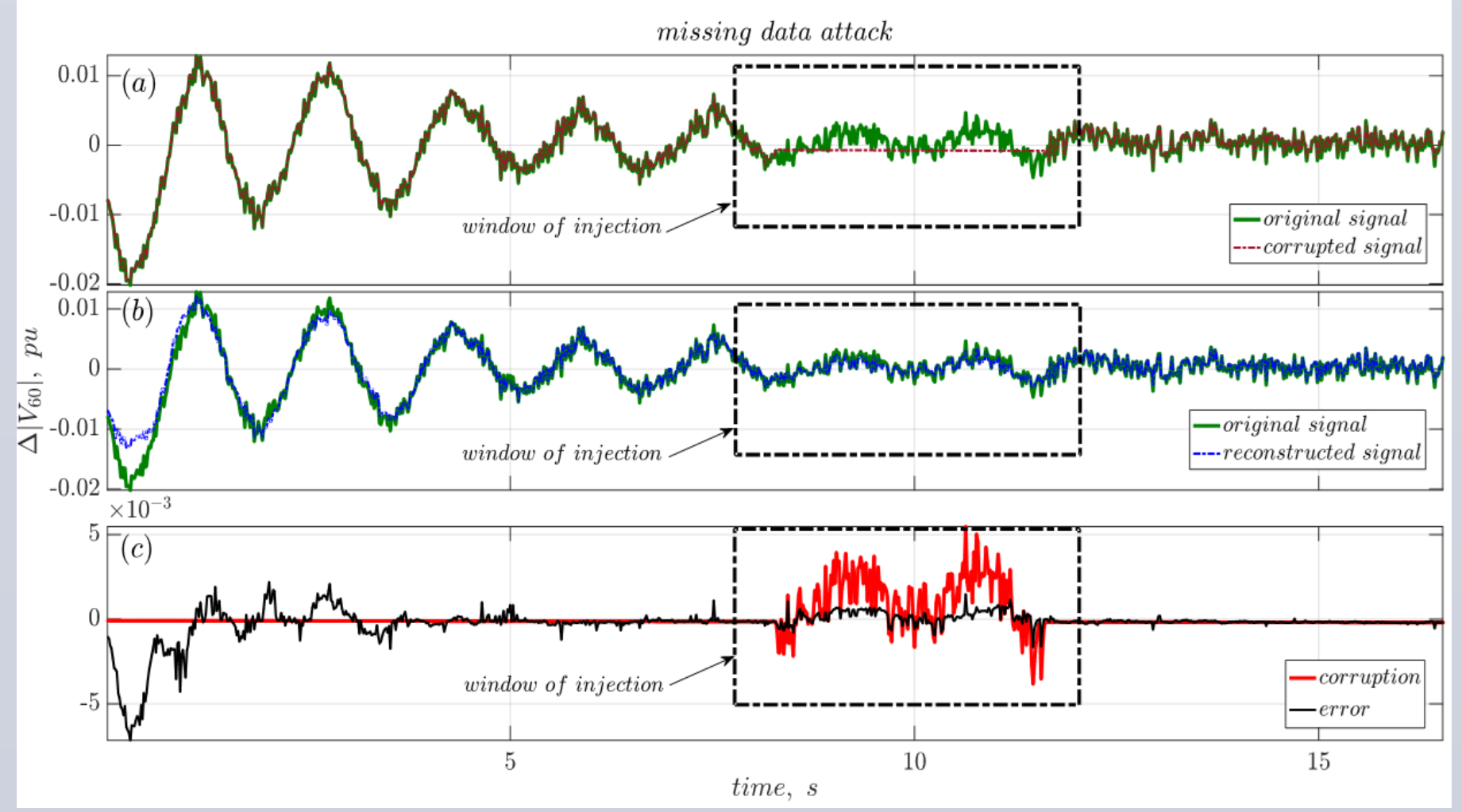
8. Noise injection attack during ambient condition



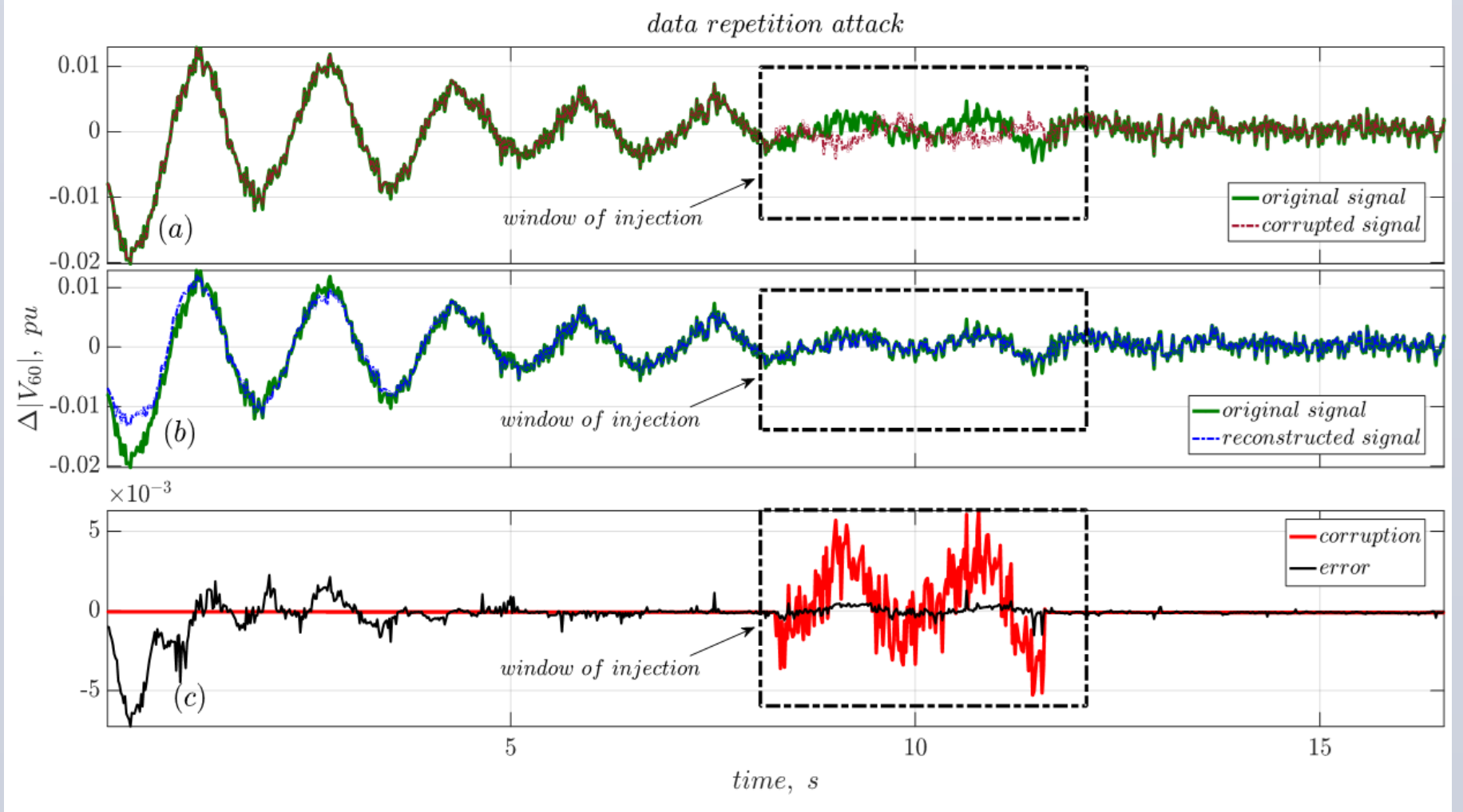
9. Noise injection attack during transient condition



10. Missing data attack during transient condition



11. Data repetition attack during transient condition



Key Takeaways

From work [1]:

1. A PCP-based interface is proposed between raw PMU data and the algorithms used for wide-area monitoring application to provide resilience against different malicious data corruptions originating from cyber attacks.
2. PCP, as a block processing technique recovers the original matrix from (i) data repetition, (ii) missing data, (iii) noise injection, (iv) parameter manipulation, and (v) fault resembling injection attacks. The results suggest that the reconstructed data set can be post-processed by wide-area monitoring algorithms like mode meters.

From work [2]:

1. A recursive projected compressed sensing (Reprocs)-based technique is proposed for online sample-by-sample detection and correction of malicious injections in PMU measurements. The proposed method manages to recover a time sequence of sparse vectors containing corrupted elements and a time sequence of dense vectors containing true measurements from their sum.
2. Results suggest that the proposed method is able to recover the original data vector faster than the memory-intensive block-processing-based algorithms. The proposed method works when corruption is present only in a limited number of signals among a set of measurements.

Ongoing Work

- Develop an online detection algorithm to detect simultaneous corruptions in multiple signals instead of using a memory-intensive block processing algorithm.
- Determine relationship between the deviations reflected in estimated modes and corresponding damping ratios of the system due to any corruption present in the synchrophasor measurements, which are used for modal estimation.
- Developing different attack models with malicious data injections with false data injection at strategic places and determine the effect of these attacks on system operation, control, and protection.

Products

1. K. Mahapatra, N. R. Chaudhuri, "Malicious Corruption Resilient Wide-Area Oscillation Monitoring using Principal Component Pursuit," under review in *IEEE Transactions on Smart Grid.*
2. K. Mahapatra, N. R. Chaudhuri, "A projected compressed sensing based technique for online detection and clearance of malicious injections in PMU measurements," under review in *IEEE PES GM conference 2017.*

Financial support from NSF under grant award #1739206 is gratefully acknowledged