State-Aware Decentralized Database Systems for the Smart Grid

Overview and Problem Statement

The modernization of power grid industrial control systems (ICSes) is likely to lead to the adoption of modern cloud services for data historians and to derivation of "big data" analytics. The data destined for that cloud service consist of either PMU measurements cached in several data-concentrators and part of the new wide-area measurement systems, or power injection and flow measurements accrued by SCADA servers. Those data today are processed separately, because current power system state estimation (PSSE) lacks support for heterogeneous sampling and sensing modalities. The data are forwarded from the data concentrators to the PSSE servers, which then compute the state. For nonlinear SCADA measurement, the PSSE is solved iteratively using the Gauss-Newton method. Several authors have proposed methods to perform a hierarchical aggregation as a more efficient and scalable technique to determine the state. More recently, our previous work has improved the PSSE algorithms such that they become adaptive to changing network conditions, e.g., in the worst case with completely randomized cooperation with neighboring sensors.

An implicit assumption made in the previous studies on PSSE is that the time and frequency at which PMU/SCADA measurements are taken are consistent across all the distributed sensing sites. In reality, the times of measurement often lack consistency and integrity, which is an intrinsic vulnerability of wide area sensor systems. Data logs coming from different analog to digital converters are not in phase and may also differ in the frequency of sampling, in some cases because of heterogeneity in the sensors, and in others because the data are simply not refreshed in the data historians with the same frequency. Lack of good synchronization in sensing may be the result of a malfunction or due to intentional delay attacks or spoofing attacks on the GPS signals.

That premise motivated our recent work, in which we advanced the area of decentralized signal processing and explicitly considered timing errors and non-homogenous sampling rates in linear and nonlinear least squares estimation problems with distributed sensing. For linear observation models, we provided a necessary and sufficient condition for identifiability of the sampling offsets. We propose a general algorithm for joint regression on latent vectors and on sampling offsets; in it, we exploit asynchrony and redundancy in the spatial sampling to attain sub-Nyquist sampling resolution of the slow sensor feeds. The efficacy of the proposed decentralized algorithm has been shown by numerical simulations.

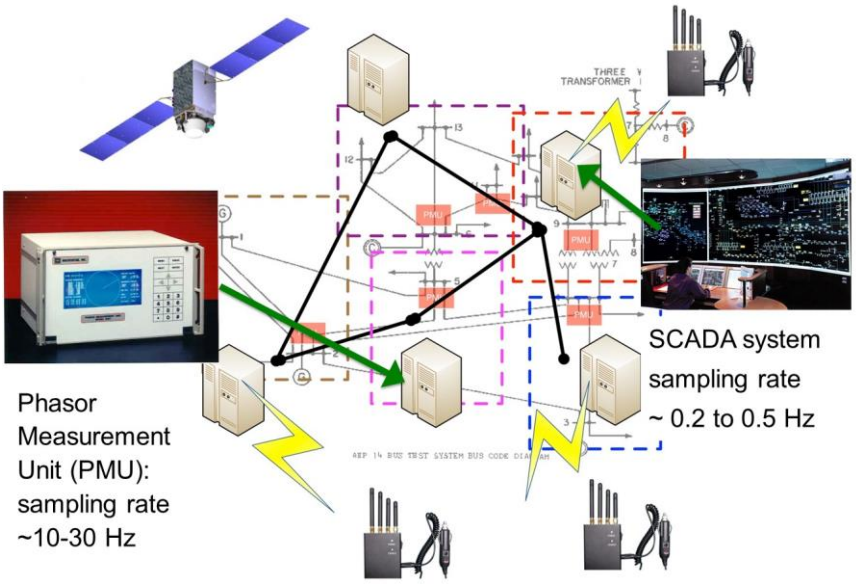


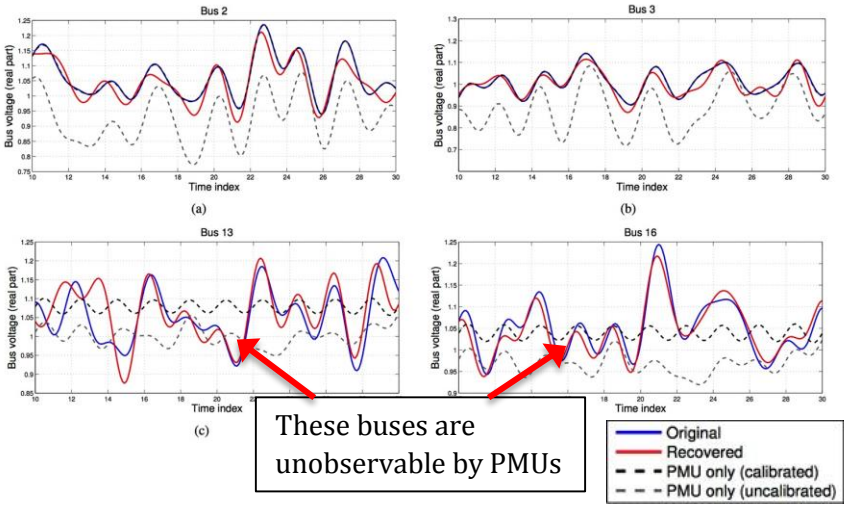
Fig. 1. A hybrid PSSE system in which the sampling rate & measurement mechanisms are allowed to be heterogeneous across sensors.

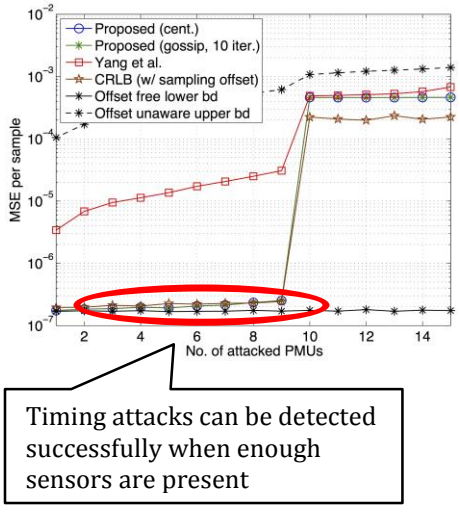
Research Objectives

- Study how to infer the power system's state from measurements collected at heterogeneous sensors, i.e., sampled at different rates and with unknown sampling offsets.
- (For the PMU-only case:) Study the conditions under which a GPS spoofing attack can be detected and corrected.
- Study the possibility of "super-resolution" recovery through use of a massive amount of sensors with low sampling rates, e.g., SCADA.
- **Smart Grid Application Area:** The SCADA system for the electrical transmission network and the AMI network in a distribution network.

Technical Description and Solution Approach

- Using a frequency domain representation, we have formulated the joint state and timing error estimation problem as a weighted least squares problem similar to conventional PSSE, with the exception that the timing error now appears as a nonlinear distortion in terms of the phase.
- The joint estimation problem is being tackled using a gossip-based alternating optimization approach, which has been demonstrated to yield good estimation performance.
- We have studied the conditions required for successful detection of timing attacks under the PMU-only model. Roughly speaking, the condition states that we will need to deploy more sensors than are needed in the absence of a timing attack.
- We have performed simulation to demonstrate that the power system state can be recovered even if it was sampled by the slower, sub-Nyquist SCADA sensors.





Results and Benefits

- We have studied the formulation of the PSSE problem with asynchronous sampling.
- We have studied how signal processing techniques can be applied to prevent/correct timing attacks, such as GPS spoofing.
- **Technology Readiness Level:** Basic research.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Hoi-To Wai, htwai@ucdavis.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security