

Bachelor Thesis

TSA (Time Synchronization Attack) on Phasor measurement unit - KASTEL Security Lab Energy

Scientific Title: Evaluation of microPMU with respect to time spoofing vulnerability and applicability for control schemes

Welcome to the Secure Energy Systems (SES) Research Group! The highlighted objective of “Secure Energy Systems (SES)” working group is about the cyber-physical security of energy systems. The working topics cover a broad range from hardware to the communication structure in Smart Grids (SGs).

New concerns about risks of security threats have emerged with the implementation of SGs infrastructure. Phasor Measurement Units (PMUs) measure the time shift between voltages (so-called phase angles) at different positions in the grid. To make use of these measurements, time accuracy of few micro seconds is required which is normally provided by GNSS synchronized receiver clocks. GNSS receivers are often prone to GNSS spoofing attacks. The goal of the thesis is to investigate both the GNSS spoofing vulnerability and the resolution required to monitor fast dynamics.

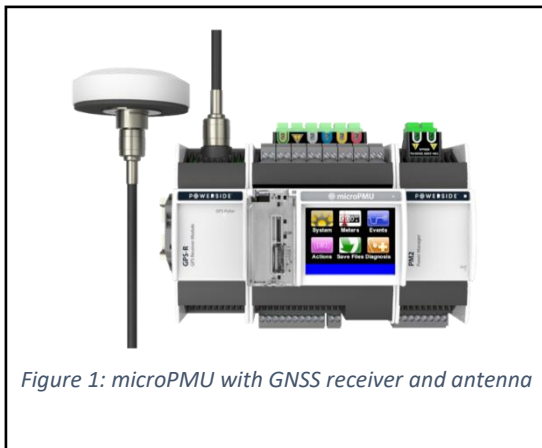


Figure 1: microPMU with GNSS receiver and antenna

We offer

- Interesting tasks with the possibility of contributing to scientific publications
- Hands-on experiment
- Close supervision

Requirements

- Bachelor's student in Computer Science or electrical engineering
- Familiar with data analysis (in our case: IEEE C37.118)
- Familiarity with analog signal processing / amplification
- Motivated to work on GNSS spoofing

Tasks - The proposed thesis consists of the following main tasks

- Familiarization: Phasor measurement units, GNSS time synchronization, measurement resolution
- Test Cases: Conduct Time Synchronization Attacks (TSAs) using GNSS spoofing, create test cases with rich frequency spectrum and investigate the reproducibility of the signal using the PMU's recordings
- Evaluate both PMU's physical constraints on fast control schemes as well as the limitations by the PMU data exchange standard IEEE C37.118

We are happy to answer any questions you might have. If you are interested, contact us via email to eva.hetzel@kit.edu and clemens.fruboese@kit.edu including current transcript of records and a resume/CV.

Contact Data

Karlsruher Institut für Technologie (KIT)
Automation and Applied Informatics (IAI)
Standort: Campus North

Name Surname: Eva Hetzel, Clemens Fruböse
Secure Energy Systems (SES)
Phone: +49 721 608-45764
E-mail: eva.hetzel@kit.edu and clemens.fruboese@kit.edu