Karlsruhe Institute of Technology

Earliest start: Now!

KASTEL

Master's Thesis

Power outages through targeting time synchronization of protection relays

Scientific Title: Analysis of GNSS spoofing impacts on differential protection schemes in a digital substation

Welcome to KASTEL Security Lab Energy! KASTEL Security Research Labs focuses on secure and trustworthy complex networked systems through interdisciplinary work, from basic to applied research, while combining teaching and innovation. KASTEL Security Lab Energy addresses the cyber-physical security of energy systems, covering a broad range of topics from hardware to communication structures in Smart Grids (SGs). New concerns about risks of security threats have emerged with the implementation of SGs infrastructure: In a digital substation analogue data (voltages and currents) is digitized in so-called Merging Units (MUs). This data is required for the relays to decide if to open a circuit breaker (i.e. to disconnect a section of the grid from the main electricity grid). During the process of digitization, the data is equipped with a time stamp such that further processing can align measurement taken by different devices. This data is then processed in relays which analyze the received data and send commands to the circuit breakers if a pre-defined threshold is surpassed.

Using time synchronization attacks the protection relay receives data which is not consistent in time. We investigate if this can lead to a circuit breaker opening in realistic scenarios. This thesis aims to evaluate the feasibility of GNSS spoofing attacks by introducing controlled time offsets and analyzing their impact on protection relay behavior, i.e., through experimentally assessing incorrect relay operation under time synchronization attacks.

Tasks - The proposed thesis consists of the following **main tasks**

- Familiarization: configuration of a Relay to enable transformer differential protection
- Test Cases: setting up framework, running experiments with different scenarios of time manipulation.
- Analysis and Evaluation: assess attack feasibility, including the effect of NTP and PTP update intervals

We offer:

- Opportunity to work with realistic lab environment with industrial hardware
- Hands-on tasks with the opportunity to contribute to scientific publications
- Close supervision

Requirements:

- Student in Computer Science or electrical engineering
- Motivated to frequently configure relays
- Good Python programming skills
- Preferably: completed Energy Informatics lecture/seminar

We are happy to answer any questions you might have. If you are interested, contact us via email to sine.canbolat@kit.edu and clemens.fruboese@kit.edu preferable including informative documents about you.
A prior HiWi time can be arranged to get more familiarization with the topic.

Contact Data

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

Name Surname: Sine Canbolat, Clemens Fruböse
Secure Energy Systems (SES)
Phone: +49 721 608-22913/45764
E-mail: sine.canbolat@kit.edu and clemens.fruboese@kit.edu