IPID4all Doctorate Research Exchange with OFFIS, Uni Oldenburg
Feedback report

Kaikai Pan, MSc.
IEPG, TU Delft
2600 GA, Delft, the Netherlands
Peter Palensky, Prof. Dr.
University of Oldenburg
OFFIS
26121 Oldenburg, Germany
Sebastian Lehnhoff, Prof. Dr.

March 28, 2016-April 8, 2016
Co-simulation of intelligent power grids and cyber-security test

Introduction

The intelligent power grids utilize enhanced information and communication technology (ICT). The interactions between electric power systems and ICT provide more flexibility and convenience but also increase the complexity. For instance, cyber security vulnerabilities within the ICT infrastructure may allow attackers to manipulate the physical system, communication network or software applications, impacting on power system reliability and even causing cascading outages. To understand the interdependency, co-simulation gives a solution to research on cyber security issues in intelligent power grids by integrating simulators in each domain. Within a co-simulation framework, security tests could be done by simulate certain kinds of attack scenarios.

Research Undertaken

During this research exchange, some work has been done based on the co-simulation framework MOSAIK developed in OFFIS. First, the co-simulation framework MOSAIK is studied and trained from several aspects, such as the MOSAIK API (how it communicates with a simulator), scenario definition (how to create specific scenario in pow grids), time scheduling (synchronization of simulators), and simulation master/manager (handing the simulator processes). With the learning process, some experiments are done following the training courses and tutorial given by OFFIS.

After having a better knowledge of MOSAIK, the scenario is built, i.e., studying adversarial actions/attacks on voltage control of interconnected micro-grids using the co-simulation framework MOSAIK. This scenario comes from the paper “Voltage control for interconnected micro-grids under adversarial actions” by André etc. In this scenario, each micro-grid is abstracted as a power inverter that can be controlled to regulate its voltage magnitude and phase-angle independently. Each power inverter is modelled as a single integrator, whose input is given by a voltage droop-control policy that is computed based on voltage magnitude and reactive power injection measurements. See Fig. 1 from this paper.

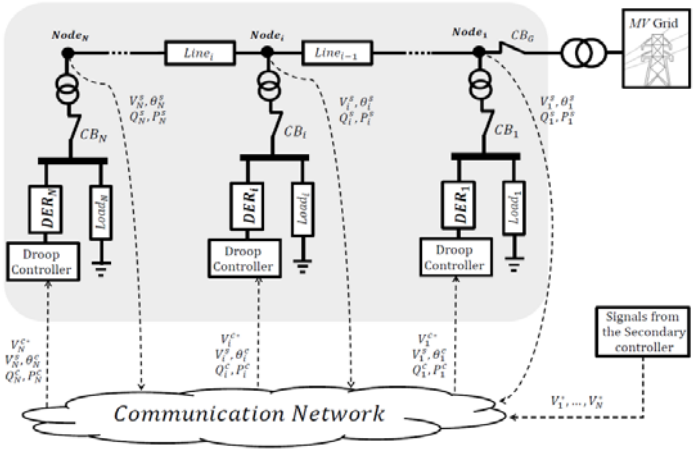

Fig. 1. Interconnected micro-grids model from the paper

With this interconnected micro-grids model, the attack scenario is defined, i.e., the adversary corrupts reference signals received by the voltage droop controllers. To study the potential impact of this scenario, MOSAIK is used to simulate the power grid, attack behaviour. This simulation can help to identify high risk attack scenario. For the simulation, each model of the micro-grid, controller, attacker is implemented in Python. Besides, the API for each model to connect with MOSAIK is built under the MOSAIK framework. It should be noted that this models can also be built in other tools or simulators, and now MOSAIK supports well with Python API and Java API.

In the simulation, the reference voltage for each micro-grid is corrupted by the adversary. There are four micro-grids in our scenario, and the reference voltage is injected with false data individually. Fig. 2 to Fig. 5 shows the results of voltage variation for each attack scenarios.

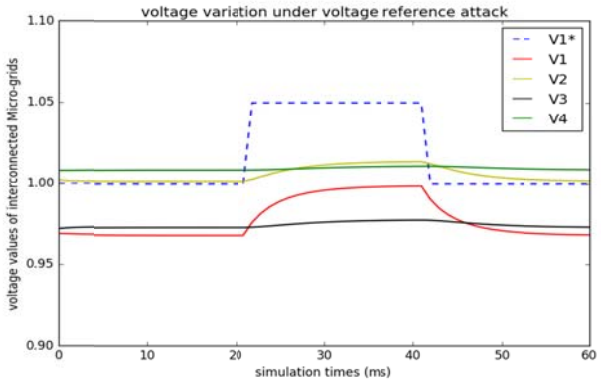

Fig. 2. Simulation results when attacker corrupts the reference voltage of micro-grid 1.

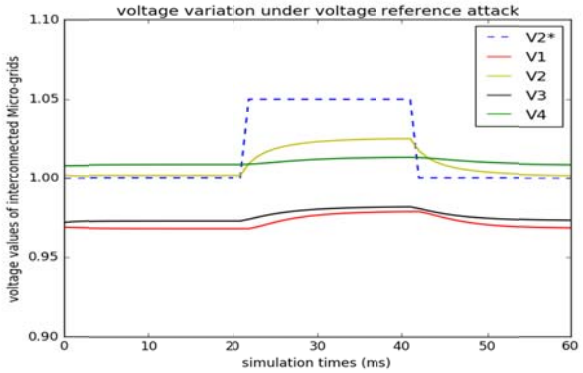

Fig. 3. Simulation results when attacker corrupts the reference voltage of micro-grid 2.

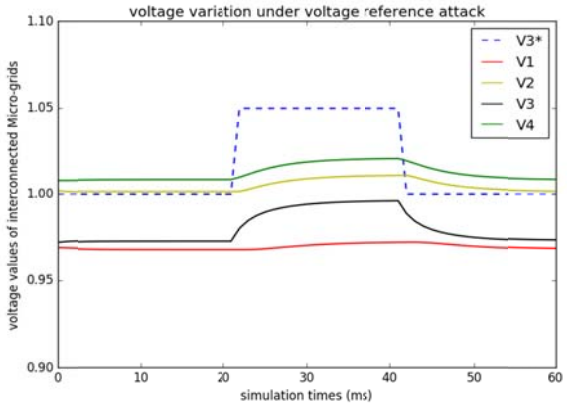

Fig. 4. Simulation results when attacker corrupts the reference voltage of micro-grid 3.

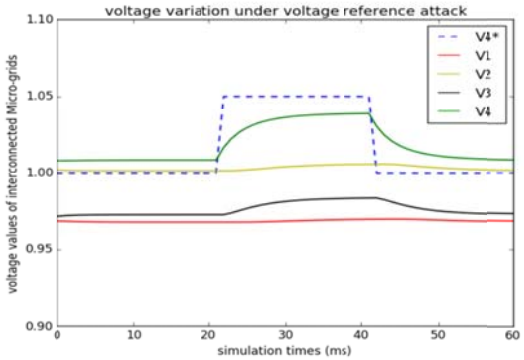

Fig. 5. Simulation results when attacker corrupts the reference voltage of micro-grid 3.

From the simulation, we can see that the corruption of reference voltage will lead to the variation in the voltage. This variation is big when the corresponding reference is corrupted for this micro-grid. The neighbouring micro-grid is impacted also due to the interconnectivity nature of the power grid.

Personal Experience

From the work with MOSAIK, this co-simulation platform suits for large scenario. The scalability is well satisfied. The scenario definition can be easily implemented in MOSAIK, which means that it supports the simulation of controls and applications in intelligent power grid. Now, MOSAIK has developed APIs for a certain number of simulators (e.g., Pypower, PowerFactory, OpalRT). APIs can be also customized for other simulators under MOSAIK framework. It would be better if the APIs for the network simulators in ICT domain will be provided in the future development.

Conclusions

Thanks to the support from DAAD, the exchange with OFFIS in University of Oldenburg works well. During the exchange, the co-simulation framework MOSAIK is studied. It turns out to be a good platform for large scale power system and different kinds of scenarios in intelligent power grids. Then the scenario is defined from a published paper. Each model in this scenario in built under MOSAIK framework. Finally the simulation results are obtained under the attack scenarios, proving the effectiveness of using co-simulation and advantages of MOSAIK

Outlook

- Possible further exchange for development and employment of MOSAIK in co-simulation of power system and ICT.
- Other possible research topic, e.g., real-time co-simulation using MOSAIK and RTDS, vulnerability assessment of power grids to attacks using simulation platform.