Energy Informatics

RESEARCH

Open Access

OpenDISCO – Open simulation framework for distributed smart grid control

Marius Stübs* and Kevin Köster

From The 7th DACH+ Conference on Energy Informatics
Oldenburg, Germany. 11-12 October 2018

* Correspondence: stuebs@informatik.uni-hamburg.de
Department of Computer Science, University of Hamburg, Hamburg, Germany

Abstract

OpenDISCO is an open-source framework for decentralized simulation and security assessment of distributed power grid control. By incorporating security assessment directly into the control algorithms' implementation process, the proposed framework aims to enable the rapid development of new control strategies. It provides a modular structure, enabling engineers and researchers to define own stress conditions and to simulate predefined cyber-attacks, thereby enabling continuous evaluation during the integration into existing power systems. A demo setup is presented, comprising a micro grid simulation and implementing a Controller-Hardware-in-the-Loop configuration.

Keywords: Smart grid, Demo, Security framework, Open-source

Introduction

The decentralization of Smart Grids is an ongoing transformation. For novel Smart Grid appliances, e.g. distributed control algorithms (DCAs), IT security is a core requirement and needs to be considered already in the development phase.

Prospectively, millions of new regenerative energy resources and electric cars need to be coordinating additionally to the existing power grid, to match supply and demand. The development of innovative DCAs is one possible contribution in the direction of a resilient Smart Grid. While decentralization of control algorithms can help avoiding single-point-of-failures and improve the system's resilience, as depicted in Fig. 1, its complexity increases. The OpenDISCO framework is a tool for assisting the development of resilient Smart Grid control despite these challenges.

Related work

Power grid functionality has traditionally been implemented in a centralized way. Current research shows alternative solutions based on DCAs for many of these applications, realized by so-called decentralized Virtual Power Plants (Stübs, 2018) and implementing grid functionality like Demand Response (Sakurama & Miura, 2017), Frequency-Load Control (Dong, 2016) and Power System State Estimation (Etemad & Lahouti, 2016).

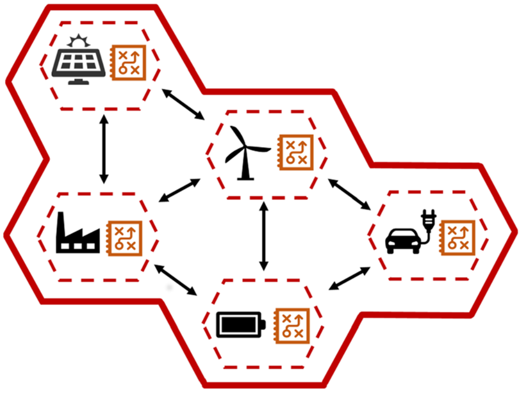

Fig. 1 Prospectively, distributed energy resources are connected via ICT infrastructures to form Smart Grids, enabling their self-organization as independent micro grids. Instead of introducing a central controller for all micro grids, the investigated approach makes use of a distributed control algorithm running on the different grid nodes

The integration of Controller-Hardware-in-the-Loop (CHIL) into a Smart Grid validation environment has been thoroughly tested (Andrén et al., 2013) and several Cyber-Physical Energy System (CPES) testbeds exist (Cintuglu et al., 2017). Verification of DCAs is a well-researched topic among wireless sensor networks (Wang & Bagrodia, 2011). However, a truly decentralized framework has not been developed and we aim to contribute to this development with a security assessment framework for the Smart Grid.

OpenDISCO framework

The proposed framework aims to accompany the development cycles of any DCA for CPES by describing an interface for an advanced resilience assessment. Three main properties, namely a modular structure, the distributed execution, stress condition simulation, build the core of the framework:

a) Modular Structure

Smart Grid engineers can independently develop modules to be executed by the OpenDISCO framework, that can implement the DCA's logical structure, as shown in Fig. 2. Thanks to the modularity of the framework, it is easy to introduce a new or different DCA in the code. Modules are required to implement an event-driven interface, thus granting interoperability with simulation tools. The modularity mechanism is built upon a message queue and an event-driven operation: When a message or event arrives at the control node, it is sent to the central message queue and is then available for processing by the framework's modules.

b) Distributed Execution

Each control node can be either simulated or executed in a distributed environment with a preconfigured topology. Message exchange between the control nodes is implemented using the publisher-subscribe concept. The communication network's topology is either

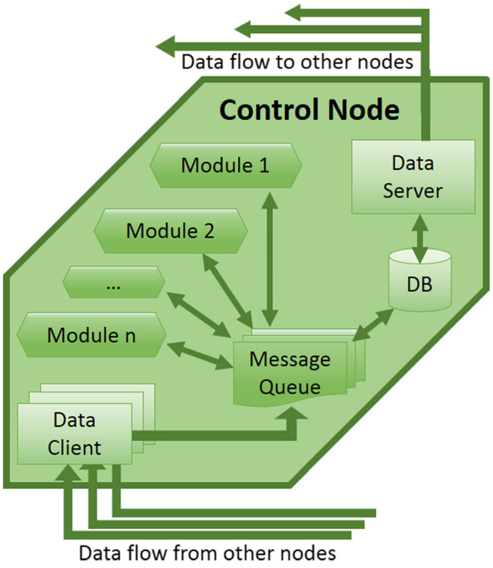

Fig. 2 Structure of a control node. Messages from the other nodes in the micro grid are delivered into the message queue to be processed by the control node's modules. Changes in a node's database values are then communicated as messages to connected control nodes

realized in hardware or simulated. Thereby different topologies can be used for evaluation, for example ring topology, fully meshed topology or an incomplete mesh.

c) Stress Condition Simulation

The framework includes an XML based attack description language, which allows to implement various attacker models. By creating designated attack simulation modules for the control nodes, it is possible to describe denial-of-service attacks and connectivity malfunctions, such as dropping or delaying messages, changing reported measurements and control commands, or even disconnecting from and re-connecting to the evaluated micro-grid. An additional feature is support for probabilistic and/or orchestrated attack behavior.

Case study

The presented case study shows a decentralized frequency-load control algorithm in an islanded micro grid (Nguyen et al., 2017). Each distributed energy resource (DER) is equipped with a control node, which implements a single node of the DCA and is responsible for commanding the DER. The power generating part of the DER is simulated in a digital real-time simulator, while the control nodes communicate in a communication network, shown in Fig. 3. The algorithm's task is to react to deviations in the micro grids electrical frequency from the nominal value of 50 Hz. The algorithm is realized as a distributed averaging consensus, requiring the control nodes to communicate and then act collectively. In the evaluated scenario, each control node can only communicate with its direct neighbors, implementing a locality-aware ICT topology.

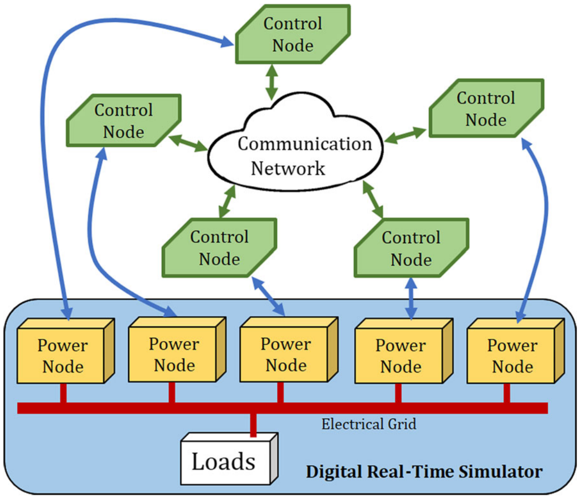

Fig. 3 Structure of the communication and power flow in the example micro grid

The evaluation of the connection between the digital real-time simulator and the control nodes was realized by implementing a cluster of Raspberry Pi embedded systems, as pictured in Fig. 4.

Demo setup

The demo setup uses a physical Raspberry Pi cluster as pictured in Fig. 4 and powered by a 230 V, 60 W power hub, providing low voltage DC via USB to the Ethernet switch and embedded devices, which are mounted on a rack. Implementing a CHIL configuration, each Raspberry Pi functions as the controller of a DER in the simulated CPES, in this case an islanded micro grid. The interconnection between the embedded devices utilizes Ethernet and TCP/IP. The connection from a displaying computer to the cluster is managed by a dedicated Raspberry Pi and realized via IEEE 802.11 wireless protocol with WPA2 password authentication. The managing Raspberry Pi then redirects incoming Wi-Fi connections via Ethernet, if requested, to any of the Raspberry Pi computers. When connected to the demo setup, the effect of DoS

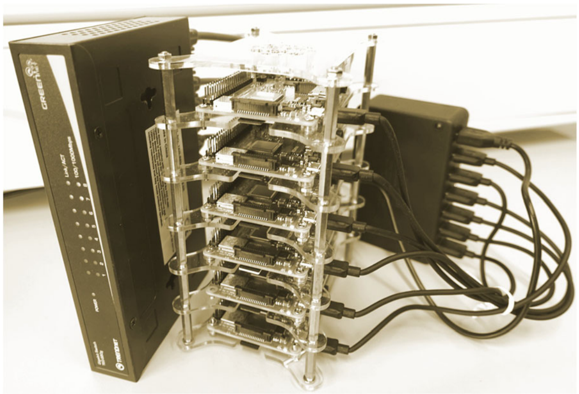

Fig. 4 The cluster of Raspberry Pi embedded systems realizing a decentralized CHIL configuration

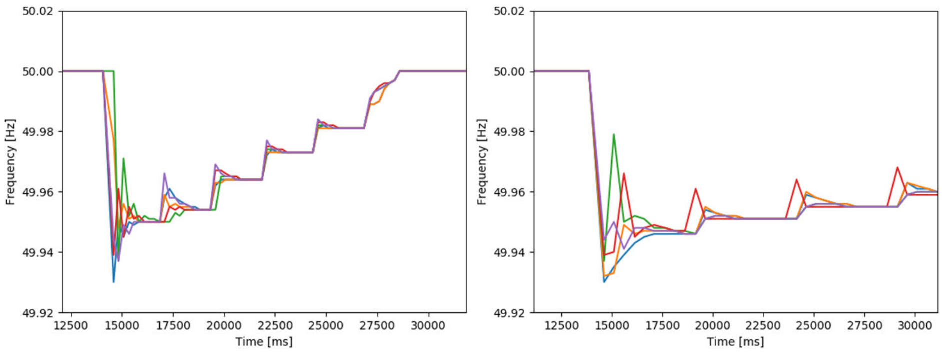

Fig. 5 Distributed consensus negotiation for frequency stabilization after a disturbance. Each color represents the proposed value of a single node. After each consensus iteration, that consensus value is used by each node to control the corresponding energy resource of the simulated micro grid. The left graph shows normal operation, whereas the right one shows the system during a DoS attack

attacks on the implemented control algorithm's performance can be displayed and evaluated on any connected device.

Results and discussion

For the current evaluation, we investigated only attacks against the availability of the test setup's communication. The attacker is assumed to be able to deliberately suppress or delay messages between control nodes. Figure 5a shows the default reaction of the evaluated system to a disturbance, where-as a simulated denial-of-service attack as depicted in Fig. 5b can be detected immediately.

In the context of the Smart Grid and DER, neither benevolence nor soundness of the communication partners can be generally assumed, although encrypted connections and public key management schemes can provide certainty of the identities and authorizations of other nodes. Nonetheless, contributing nodes can be malfunctioning or even malicious, whilst maintaining valid credentials.

Presented research indicates that decentralized detection and reaction strategies are a worthwhile contribution to improve robustness of distributed systems and might become a necessity in future, increasingly complex Smart Grid infrastructures.

Conclusion

The OpenDISCO framework is an easily extendable open-source tool for assessment of distributed control algorithms (DCAs). It enables Smart Grid researchers and engineers to simulate and continuously verify control strategies during development. The prototype implementation is freely available (Stübs et al., 2018) and includes example DCA, sample ICT topologies and a custom attack description language as well as various predefined attacker models.

Abbreviations

CHIL: Controller-Hardware-in-the-Loop; CPES: Cyber-Physical Energy System; DCA: Distributed Control Algorithm; DER: Distributed Energy Resource; DoS: Denial of Service; ICT: Information Communication Technology

Funding

This work was funded by Germany's Federal Ministry of Economics and Energy (BMWi). Publication costs for this article were sponsored by the Smart Energy Showcases - Digital Agenda for the Energy Transition (SINTEG) program.

Availability of data and materials

Source code and examples are freely available on the website of the Department of Computer Science at the University of Hamburg (Stübs et al., 2018).

About this supplement

This article has been published as part of *Energy Informatics* Volume 1 Supplement 1, 2018: Proceedings of the 7th DACH+ Conference on Energy Informatics. The full contents of the supplement are available online at https://energyinformatics.springeropen.com/articles/supplements/volume-1-supplement-1.

Authors' contributions

Abstract, introduction, related work and conclusion have been written by MS. The chapters OpenDISCO framework, case study, demo results as well as results and discussion have been collaboratively written by MS and KK. MS and KK have both contributed to the source-code and conducted said experiments together. The figures were created by MS. Both authors have read and approved the final manuscript.

Competing interests

No competing interests arise. The proposed solutions and software are free and open-source (Stübs et al., 2018). No commercial products are currently planned from this research.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Published: 10 October 2018

References

Andrén F, Lehfuß F, Strasser T (2013) A development and validation environment for real-time controller-hardware-in-the-loop experiments in smart grids. Int J Distributed Energy Resour Smart Grids 9(1):27–50

Cintuglu MH et al (2017) A survey on smart grid cyber-physical system testbeds. IEEE Commun Surv Tutorials 19(1):446–464

Dong L (2016) Decentralized load frequency control for an interconnected power system with nonlinearities, American Control Conference (ACC). IEEE, Boston

Etemad RH, Lahouti F (2016) Resilient decentralized consensus-based state estimation for smart grid in presence of false data, International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, Shanghai

Nguyen TL et al (2017) Agent based distributed control of islanded microgrid—real-time cyber-physical implementation, Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE PES, Torino

Sakurama K, Miura M (2017) Communication-based decentralized demand response for smart microgrids. IEEE Trans Ind Electron 64(6):5192–5202

Stübs M (2018) IT-security in self-organizing decentralized virtual power plants: student research abstract, Proceedings of the 33rd Annual ACM Symposium on Applied Computing. ACM, Pau

Stübs M, Kevin K, Laskow D (2018) OpenDISCO source code. https://git.informatik.uni-hamburg.de/OpenDISCO/OpenDISCO-framework. [Online; accessed 12-June-2018]

Wang Y-T, Bagrodia R (2011) Sensec: A scalable and accurate framework for wireless sensor network security evaluation, Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on. IEEE, Minneapolis