Ensemble regression model-based anomaly detection for cyber-physical intrusion detection in smart grids - DTU Orbit (21/12/2018)

Ensemble regression model-based anomaly detection for cyber-physical intrusion detection in smart grids

The shift from centralised large production to distributed energy production has several consequences for current power system operation. The replacement of large power plants by growing numbers of distributed energy resources (DERs) increases the dependency of the power system on small scale, distributed production. Many of these DERs can be accessed and controlled remotely, posing a cybersecurity risk. This paper investigates an intrusion detection system which evaluates the DER operation in order to discover unauthorized control actions. The proposed anomaly detection method is based on an ensemble of non-linear artificial neural network DER models which detect and evaluate anomalies in DER operation. The proposed method is validated against measurement data which yields a precision of 0.947 and an accuracy of 0.976. This improves the precision and accuracy of a classic model-based anomaly detection by 75.7% and 9.2%, respectively.

General information
State: Published
Organisations: Center for Electric Power and Energy, Energy System Management, Risø National Laboratory for Sustainable Energy, Department of Electrical Engineering, Department of Informatics and Mathematical Modeling
Contributors: Kosek, A. M., Gehrke, O.
Number of pages: 7
Pages: 1-7
Publication date: 2016

Host publication information
Title of host publication: Proceedings of 2016 IEEE Electrical Power and Energy Conference
Publisher: IEEE
ISBN (Print): 978-1-5090-1919-9
(2016 ieee Electrical Power and Energy Conference (epec)).
Keywords: Data models, Density estimation robust algorithm, Training, Correlation, Power systems, Analytical models, Intrusion detection, power system, Data-driven modelling, machine learning, cyber-physical security, model-based anomaly detection, ensemble regression
DOIs:
10.1109/EPEC.2016.7771704
Source: FindIt
Source-ID: 2349602557
Research output: Research - peer-review › Article in proceedings – Annual report year: 2016