# Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model

Anna Magdalena Kosek
Energy System Operation and Management
Department of Electrical Engineering
Technical University of Denmark
amko@elektro.dtu.dk

***Abstract*—This paper presents a contextual anomaly detection method and its use in the discovery of malicious voltage control actions in the low voltage distribution grid. The model-based anomaly detection uses an artificial neural network model to identify a distributed energy resource's behaviour under control. An intrusion detection system observes distributed energy resource's behaviour, control actions and the power system impact, and is tested together with an ongoing voltage control attack in a co-simulation set-up. The simulation results obtained with a real photovoltaic rooftop power plant data show that the contextual anomaly detection performs on average 55% better in the control detection and over 56% better in the malicious control detection over the point anomaly detection.**

***Keywords*—anomaly detection, intrusion detection system, smart grid, data analysis, cyber-physical security**

## I. Introduction

Cyber security is an increasing interest and worry in power systems. The main concerns consider new control paradigms, on-line access to a range of power system components and DERs (Distributed Energy Resources), and enormous data exchange and collection introduced by the so called Smart Grid. The power system security is mostly concerned with cyber security of AMI (Advanced Metering Infrastructure), [1], SCADA (Supervisory Control and Data Acquisition) security [2] and communication standards [3]. A new cyber-physical approach to the smart grid security was introduced in [4] and addresses a tight coupling between the physical power system and the ICT (Information and Communication Technology). Nine major research topics emerged from the combination of these two fields: vulnerability research, impact analysis, mitigation research, cyber-physical metrics, data and model developments, security validation, interoperability, cyber forensics and operator training [5]. A smart grid compatible IDS (Intrusion Detection System) needs to address both on-line and post-mortem analysis of the state of the observed cyber-physical system and detect anomalies in operation of both cyber and physical components. An anomaly detection method identifies rare data instances or events that do not match an expected pattern [6]. The development of models used for anomaly detection requires cyber-security and power system expertise, and additionally, if data driven models are required, data analysis knowledge. Once both cyber and physical anomaly detection analysis is performed, cyber-physical metrics need to be developed to combine the information from both domains to address the tight relations between the power system and the ICT domains. Anomaly detection with regression models has been used for discovering cyber-attacks on a SCADA system [7], a wind turbine fault detection [8], a PV (photovoltaic power plant) fault diagnostics [9]. A special case of a PV attack against voltage control in distribution power grids has been described in [10].

Two types of anomaly detection can be distinguished: point and contextual. The point anomaly detection takes the global view of the data [6]. The contextual or conditional anomalies were introduced in [11] and are defined as data points that are anomalous in a specific context and acceptable in another context. For example for spatial data, the location of a measurement is its context. For time series, time is the context for each measurement [6]. The advantage of the contextual over point anomaly detection is the detection accuracy. The disadvantage is that this method requires context data, which is not always available. Two methods for contextual anomaly detection exist: reduction to a point anomaly detection problem and utilizing the structure in data [6]. The reduction to point anomaly detection problem technique divides the data into contextual groups and analyses behaviour attributes for each context separately, reducing the problem to several point anomaly detections. Thos method produces a model for each context, as a consequence several models are used to represent a single system. In case of the time contextual data, models for every year, month, day of the month, minute and so on would have to be created. Contextual anomaly models utilising the structure of the data modify the structure the training data to include the date adding separately: year, month, day and so on as input variables, the modified input data is then used for training of a single contextual model.

In the energy domain the contextual anomaly detection have been previously used for recognising user behavior in a residential dwelling based on non-parametric belief propagation for energy efficiency [12]. In [12] a user behaviour is categorised as unusual equipment usage or bursty occupancy and is used to adjust the energy management schedule. Authors in [13] propose use of on-line contextual anomaly detection for fault diagnostics of power transformers. In this paper we propose to use contextual anomaly detection utilizing the structure in data for cyber-physical IDS. According to the author's knowledge, contextual anomaly detection have not been used to identify control actions.

978-1-5090-1164-3/16/$31.00 

## II. Anomaly based IDS

The proposed cyber-physical IDS architecture consists of two main parts: an analysis of the behaviour of the observed cyber-physical system and components, and a joint analysis of the cyber-physical system (figure 1). The behaviour analysis and characterisation of the physical power system is performed with two components: DER and power system analysis, the evaluation of the cyber vulnerabilities is performed in the cyber security analysis component. The joint cyber-physical analysis combines the information from both physical and cyber security components and presents the outcomes to the power system operator. In this work we consider the physical

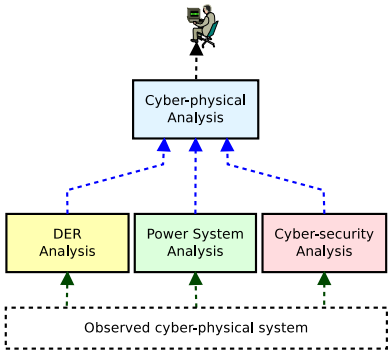


Fig. 1. Cyber-physical IDS architecture.

part of the proposed IDS and focus on DER and power system analysis. Additionally this paper introduces an on-line method to combine information produced by these components in the cyber physical analysis component. The proposed on-line anomaly based IDS architecture is presented in figure 2. The IDS consists of three parts: DER, power system and cyber-physical analysis.

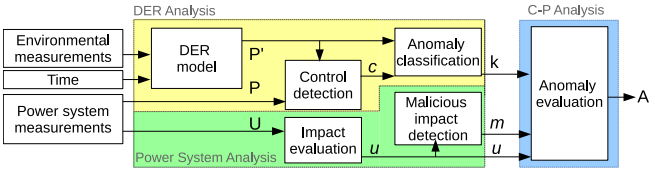


Fig. 2. IDS with anomaly detection and power system stability evaluation.

### A. DER analysis

The objective of the DER analysis is to identify a suspicious behaviour of a DER unit and associate it with a DER control action. The DER analysis consists of: a DER model, a control detection mechanism and an anomaly classification. In order to detect if a DER is being controlled, an anomaly in its behaviour need to be discovered. An anomaly based detection uses a normal behaviour model predicting a DER power production or consumption ($P'$) and compares it to the power measurement from the DER ($P$). The difference between these values is identified as anomaly $\alpha = P' - P$. Since the model introduces errors to anomaly detection, a threshold $\tau = 0.1$ was chosen to eliminate some of the model errors. Additionally this paper considers controllable power production (when $P$ is negative), where curtailment is the only possible control action, therefore all positive $\alpha > 0$ are treated as an error. The final anomaly $c$ associated with a curtailment action is as follows:

$$c = \begin{cases} 1 & \alpha > \tau \\ 0 & \alpha \leq \tau \end{cases} \tag{1}$$

The anomaly classification checks if the discovered anomaly is within the possible DER operation time $\beta$, therefore:

$$\beta = \begin{cases} 1 & P' < 0 \\ 0 & P' \geq 0 \end{cases} \tag{2}$$

The anomaly classification produces output $k = c\beta$ identifying all significant and possible curtailments of a DER, here classified as control anomalies $k$.

### B. Power system analysis

Power system analysis consists of two components: impact evaluation and malicious impact detection. The impact evaluation depends on the attack hypothesis, in this paper the considered attack influences the power stability by causing under- or over-voltage. The impact analysis takes under consideration the voltage limits and creates a piece-wise function $u$ evaluating measured voltages $U$. Let's consider $n$ as the nominal voltage value and $0.9n$ is considered under-voltage and $1.1n$ is over-voltage, the proposed function is as follows:

$$u(U) = \begin{cases} 1 & U \geq 0.9n \\ -20n(x - 0.9n) & 0.9n < U < 0.95n \\ 0 & 0.95n \leq U \leq 1.05n \\ 20n(x - 0.05n) & 1.05n < U < 1.1n \\ 1 & U \leq 1.1n \end{cases} \tag{3}$$

The impact evaluation function $u$ is presented in figure 3. The

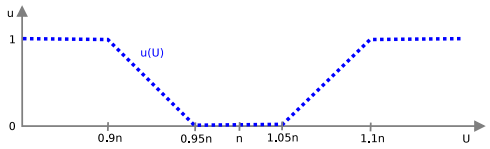


Fig. 3. Impact evacuation function.

output of the impact evaluation function is used in malicious impact detection component that evaluates the voltage difference $u_{diff}$ for each time $t$: $u_{diff} = u_{t-1} - u_t$. The output of the malicious impact detection component $u_{diff}$ is a measure of the state of the voltage from one point in time to another. If the $u_{diff}$ is positive, when $u_{t-1} > u_t$, the voltage have improved between time $t-1$ and $t$. If the $u_{diff}$ is negative, when $u_{t-1} < u_t$, the voltage have changed and is closer to under- or over-voltage between time $t-1$ and $t$. If the $u_{diff}$ is equal to zero, the voltage have not significantly changed, it might have changed inside of the $\pm 0.05n$ range or have not changed at all. The impact classification $m$ is as follows:

$$m = \begin{cases} 1 & u_{diff} < 0 \cup (u_{diff} = 0 \cap u = 1) \\ 0 & otherwise \end{cases} \tag{4}$$

The impact is classified as malicious if the voltage has changed towards under or over-voltage. Additionally, we assume that the malicious impact occurs in case the under or over-voltage is present and that this state didn't change between time $t-1$ and $t$.

### C. Cyber-physical analysis

Cyber-physical analysis evaluates the recognised anomalies. The DER analysis provides the control evaluation $k$, the power system analysis component brings the malicious impact evaluation $m$ and impact estimation $u$. In this work, we focus on the following three control anomaly cases: **normal control**, when $m = 0$, $u = 0$ and $k = 1$; **suspicious control**, when $m = 1, u > 0$ and $k = 1$; and **malicious control**, when $m = 1, u = 1$ and $k = 1$. The proposed anomaly based IDS and its three main analysis components have been tested in simulation, the implementation and results are presented in sections III, IV and V.

## III. DER MODEL

This paper proposes use of contextual anomaly detection for DER analysis and evaluates its use on an example DER: a residential rooftop PV panel. The time is used as a contextual attribute for PV production prediction as shown in figure 4. The anomalous behaviour is defined as PV's response to a control signal resulting in curtailment of its power production. The model input data is described in section III. Several modeling

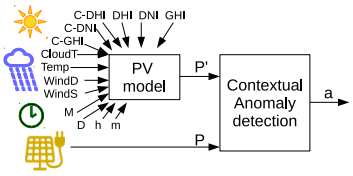


Fig. 4. Contextual anomaly detection with a PV mode.

approaches can be used to model a normal behaviour of a PV or any other DER. Three types of popular models are white, gray and black box models [14]. White box models use the known physical properties of the system. Gray box model and black box models both use the available system input and outputs to determine the system model. Gray box model combines a partial theoretical structure or partial physical system model and use model training methods to estimate parameters. In the black box model, only inputs and outputs of the system are know and the operation of the system is unknown. Machine learning methods are used to identify properties of the system by supervised model training. The black box model of a DER might be less accurate than a white box model, but can be adjusted to any unknown DER, that need to be observed and modelled. In this paper we investigate the use of machine learning technique, specifically artificial neural network (ANN), to model a DER. PV arrays have been previously modelled with use of ANN [15]. In the context of power system ANN was used together with anomaly detection in only in few cases: distribution feeder fault detection [16], detecting anomalies at substation level of abnormal measurements [17]. The design of the PV model presented in this paper is based on availability of input data for its training. Similar PV models have been proposed in numerous publications, for example a PV model using irradiation, ambient temperature, voltage, active power and current training set was proposed in [18]. According to author's knowledge no other contextual ANN PV models have been developed, where time is considered as a context.

### A. Model training data

*1) PV power production data:* The real PV production data was recorded by the Pecan Street Smart Grid Demonstration Program project that started in 2010. The objective was to implement an open platform Energy Internet Demonstration [19] with real residential consumers. The primary sight of the demonstration was at Austins Mueller community in Austin, Texas. One of the project outcome is a Dataport[1] database containing anonymized data of home electricity use, PV power, EV charging, and demand response data recorded while participating in the utility programs. The PV active power production was recorded by an energy monitoring system from eGauge. The considered solar power production used in this research is a rooftop PV produced by SunEdison, from a single-family home (referred in Dataport as house 774) in Austin, Texas. The data used in this research is 1 minute active power production in $kW$ from 1st January 2013 to 31st January 2014.

*2) Meteorological data:* The Meteorological data was acquired from National Solar Radiation Data Base (NSRDB)[2] developed by NREL (National Renewable Energy Laboratory). The used data comes from a meteorological station in Texas, Austin (latitude 30.29, longitude -97.7) from 1st January 2013 to 1st February 2014. The data is recorded every 30 minutes, the chosen data points, defined in the Glossary of Solar Radiation Resource Terms [3], are as follows. Diffuse Horizontal Irradiance (**DHI**) $[w/m^2]$ (diffuse sky radiation) - the radiation component that strikes a point from the sky, excluding circumsolar radiation. Direct Normal Irradiance (**DNI**) $[w/m^2]$ (beam radiation) - the amount of solar radiation from the direction of the sun. Global Horizontal Radiation (**GHI**) $[w/m^2]$ (global horizontal irradiance) total solar radiation. Three measures of clear sky irradiance: clear sky diffuse horizontal irradiance, direct normal radiance and global horizontal radiation (**C-DHI**, **C-DNI** and **C-GHI**) $[w/m^2]$ - measurement of DHI, DNI and GHI excluding the influence of clouds. Cloud type (**CloudT**) is another available meteorological data, NSRDB records 13 cloud types: clear, probably clear, fog, water, super-cooled water, mixed, opaque ice, cirrus, overlapping, overshooting, unknown, dust, smoke. Additional meteorological information are ambient temperature (**Temp**) $[c]$, wind direction (**WindD**) [Degrees], and wind speed (**WindS**) $[m/s]$.

*3) Contextual attributes:* The time stamp from each measurement was transformed into a vector $M, D, h, m$, where $M \in [1, 12]$ is a month, $D \in [1, 31]$ is a day, $h \in [0, 23]$ is an hour and $m \in [0, 59]$ is a minute. The relationship between contextual attributes (hour and month) and power production is presented in figure 5. For the purpose of this study, the training set was combined from the weather and PV production data together with the time information from 1st January 2013 to 31st December 2013. A total of 525540 data rows were divided into 80% training set (420660 data rows) and 20% validation set (104880 data rows). Before the 30 minute meteorological data was combined with 1 minute power production and time data, linear interpolation was performed on the weather data. This training set was used for the PV model training. The data from 1st January 2014 to 31st January 2014 was used in the simulation as on-line data. The PV production data used for

[1] https://dataport.pecanstreet.org/
[2] https://nsrdb.nrel.gov/
[3] http://rredc.nrel.gov/

simulation was modified in order to simulate PV control. In the simulation, an instantaneous and constant curtailment is assumed.

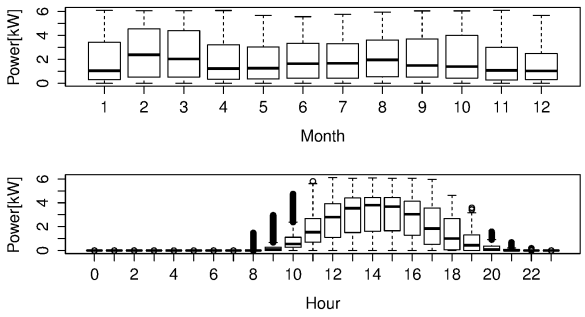


Fig. 5. Box plot of time of the day and month, and PV power production.

### B. ANN models

Let's consider a single layer feed-forward ANN with $n \in N_1$ inputs, one output, and a single set of model features $x = [x_0, x_1, x_2, ..., x_n]^\top$ and output variable $y \in R$ . The hidden layer consists of $h \in N_1$ neurons. In order to train the ANN, the forward propagation algorithm is used. The ANN model hypothesis is as follows:

$$H_w(x) = w_0 + \sum_h w_{1h}\phi(\alpha_h + \sum_k w_{kh}x_i) \quad (5)$$

Here, $w$ is model weights, $\phi_0$ is the output function and $\phi_1$ is the activation function. In this work the neural network is build to model a non-linear continuous function. According to Cyberenko theorem, sigmoid activation function of a single layer feed-forward ANN fulfills the universal approximation theorem, therefore a ANN with sigmoid activation function, as in equation (6), can approximate continuous functions.

$$\phi(z) = 1/(1 + e^{-z}) \quad (6)$$

The weights are chosen to minimise the cost function with least squares. In forward-feed ANN problem of over-fitting can be minimised with regularization [20], that is used to minimise the weights of the model, the cost function $J$ with regularization is as follows:

$$J(w) = \sum_i ||H_w(x^{(i)}) - y^{(i)}|| + \lambda \sum_h \sum_k w_{kh}^2 \quad (7)$$

Ripley [20] suggests to use $\lambda = 10^{-4} - 10^{-2}$ as a regularization parameter for least-squares fitting. Broyden-Fletcher-Goldfarb-Shanno (BFGS) algorithm [21] was used for solving unconstrained nonlinear optimization problem of minimising the the cost function $J(w)$.

The point ANN model (ANN-P) consists of 10 input neurons 15 hidden neurons and one output neuron. The regularization parameter $\lambda = 0.0006$. The contextual ANN model (ANN-P) consists of 14 input neurons 20 hidden neurons and one output neuron. The regularization parameter is $\lambda = 0.0006$. Both numbers of the hidden neurons and the regularization parameter for each model were chosen to minimise the root mean square error (RMSE) of the model prediction. As presented in table I the ANN-C model is more accurate than the ANN-P model based on RMSE.

TABLE I. COMPARISON OF THE DEVELOPED MODELS

| Model | | | | Residuals | | |
|---|---|---|---|---|---|---|
| Name | Prm | Ctxt prm | RMSE | Min | Median | Max |
| ANN-P | 10 | - | 0.88 | -3.82 | -0.14 | 4.25 |
| ANN-C | 14 | m, D, H, M | 0.43 | -3.11 | 0 | 3.81 |

## IV. SIMULATION

A co-simulation set-up was used to obtain results in this paper. The co-simulation [4] combines the PV, house and meteorological station emulators, power load flow solver PYPOWER part of the MATPOWER package for Python, implementation of monitors and attacker. Open source co-simulation orchestrator mosaik[5] synchronises the operation of all simulations and programs and exchanges data between them. Two scenarios

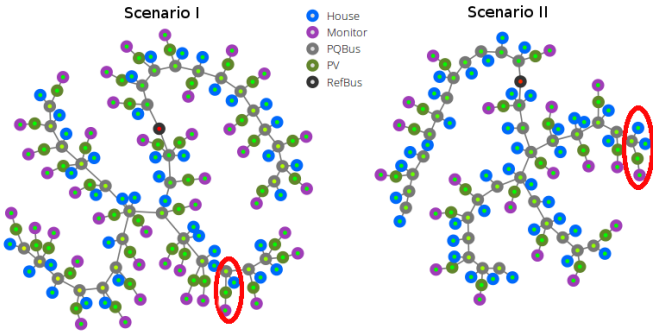


Fig. 6. System configuration for Scenario I and II.

were chosen to demonstrate the IDS system presented in section II. Both scenarios consider operation a LV distribution grid and consists of two feeders with houses and rooftop PVs. For each scenario two use cases are presented: normal operation and under attack. Use cases test hypothesis that an attacker controls PV operation in order to influence voltage on the line, leading to reduction of power quality. An autonomous monitor with IDS proposed in this paper observes each PV plant and tests the scenario hypothesis. The objective of the monitor in each use case is to determine if the PV control leads to over- or under-voltage on the line. According to EN50160 European standard the nominal value of voltage in LV grid is $230v$, over-voltage is defined as 10% increase of the nominal voltage ($253v$), under-voltage is 10% decrease of the nominal voltage ($207v$). In this section we present monitoring results from a single PV (refereed to PV number 744 in [19]). Two types of monitors: contextual and point anomaly detection have been implemented in the co-simulation set up.

Scenario I considers 100% residential PV penetration. The system configuration used for this scenario consists of 40 houses and PVs, divided into two feeders 12 sets of houses and PVs on feeder A and 28 sets of houses and PVs on feeder B (see figure 6). Ten houses and corresponding PVs have been created from real house data III-A1 and replicated to create 40 prosumers. The actors in the normal operation use case are: houses, PVs, monitors and an aggregator. The aggregator reads the voltage from each PQbus (connection point to the grid from both house and the PV) and curtails the PV in case the voltage is reaching over-voltage. The outcome

[4]https://pypi.python.org/pypi/PYPOWER
[5]http://mosaik.offis.de/

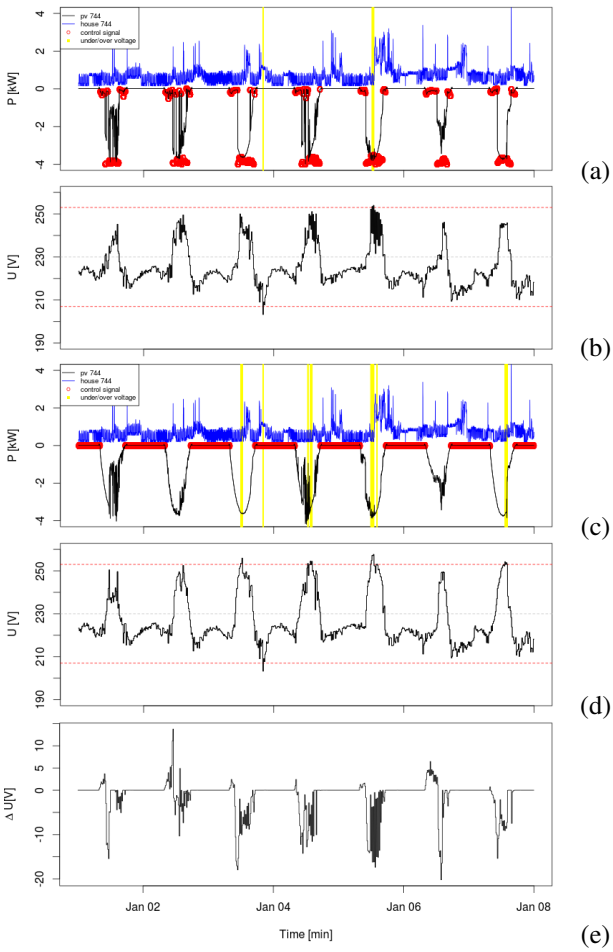


Fig. 7. Scenario I: house and PV load pattern (a) and voltage (b)- normal behaviour; house and PV load pattern (c) and voltage (d)- behaviour under attack; (e) voltage difference between the normal behaviour and the attack.

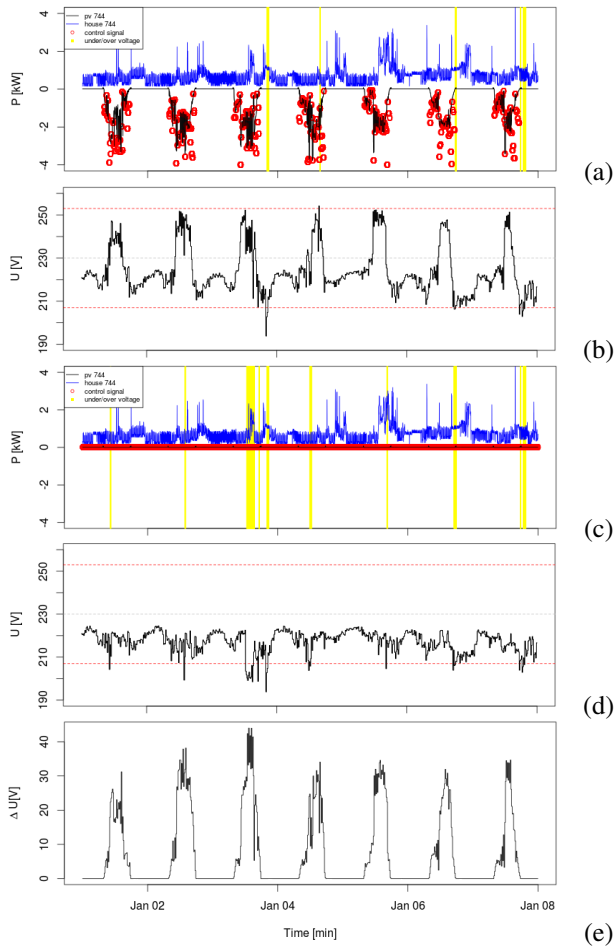


Fig. 8. Scenario II: house and PV load pattern (a) and voltage (b)- normal behaviour; house and PV load pattern (c) and voltage (d)- behaviour under attack; (e) voltage difference between the normal behaviour and the attack.

of the aggregator operation is presented in figure 7(a). In total 45 minutes of the operation voltage problems are visible (30 minutes over-voltage and 15 minutes under-voltage). In the use case under attack, the actors are as follows: houses, PVs, monitors and an attacker. The attacker gathers information about the active power production of each PV and voltage on each PQbus. The attacker sends control signals to each PV in order to reach either under or over-voltage. It is visible in figure 7(c) that the attacker's decision was not to curtail the PV operation and increase over-voltage, as presented in 7(d). The voltage problems increased to 240 minutes (where 225 minutes of over-voltage and 15 minutes of under-voltage). The difference between voltages for the normal operation and the attack use case is presented in figure 7(e), it is visible that the voltage is mostly decreased in this scenario.

In Scenario II 50% of the houses are equipped with rooftop PVs. The system configuration for this scenario is as follows: it consists of 40 houses and 20 PVs are divided into two feeders 12 houses and 5 PVs on feeder A and 28 houses and 15 PVs on feeder B (see figure 6). Similarly to the normal use cases from Scenario I, the aggregator is controlling the PV in order to meet the voltage limits, as presented in figures 8(a,b). There are several voltage problems: 15 minutes of over-voltage and 135 minutes of under-voltage. In the attack use case, the attacker is aiming at increasing the over- and under-voltage minutes by controlling the PV. It is visible in figure 8(c) that attacker decides to curtail the PV744 to $0kW$, which leads to a decrease in voltage. The total number of voltage problems is increased to 420 which all minutes are under-voltage. The voltage difference between use cases in the Scenario II is presented in figure 8(e). It is visible that voltage have been significantly decreased in this scenario.

## V. Results

Two presented models are tested for each use case in two scenarios. The results are divided into accuracy of the control detection and overall results of the malicious control detection. A confusion matrix and accuracy calculations are used to evaluate the control and attack results. The confusion matrix is a collection of occurrences of true positives (TP), true negatives (TN), false positives (FP), false negatives (FN) evaluated from a population of results. The accuracy is calculated as follows:

$$Acc = (TP + TN)/(TP + FP + FN + TN) \quad (8)$$

As seen in table II, the accuracy of the control action detection for point detection ranges between $0.39$ and $0.58$, where contextual anomaly accuracy is between $0.79$ and as much as $0.94$ for attack use case in Scenario II. Both methods

TABLE II. CONFUSION MATRIX OF CONTROL DETECTION

| Use case | TP | TN | FP | FN | Acc |
|---|---|---|---|---|---|
| contextual anomaly | | | | | |
| Scenario I: normal | 2033 | 5956 | 218 | 1873 | 0.79 |
| Scenario I: attack | 6 | 8863 | 1208 | 3 | 0.88 |
| Scenario II: normal | 2034 | 5956 | 218 | 1872 | 0.79 |
| Scenario II: attack | 3498 | 5953 | 213 | 416 | 0.94 |
| point anomaly | | | | | |
| Scenario I: normal | 1770 | 2194 | 3980 | 2136 | 0.39 |
| Scenario I: attack | 9 | 5498 | 4573 | 0 | 0.55 |
| Scenario II: normal | 1466 | 2194 | 3980 | 2440 | 0.36 |
| Scenario II: attack | 3693 | 2194 | 3972 | 221 | 0.58 |

TABLE III. CONFUSION MATRIX OF MALICIOUS CONTROL DETECTION

| Use case | TP | TN | FP | FN | Acc |
|---|---|---|---|---|---|
| contextual anomaly | | | | | |
| Scenario I: normal | 0 | 45 | 0 | 0 | 1 |
| Scenario I: attack | 44 | 15 | 0 | 181 | 0.25 |
| Scenario II: normal | 0 | 150 | 0 | 0 | 1 |
| Scenario II: attack | 249 | 141 | 0 | 30 | 0.93 |
| point anomaly | | | | | |
| Scenario I: normal | 0 | 45 | 0 | 0 | 1 |
| Scenario I: attack | 11 | 15 | 0 | 214 | 0.11 |
| Scenario II: normal | 0 | 149 | 1 | 0 | 0.99 |
| Scenario II: attack | 249 | 140 | 1 | 30 | 0.93 |

recognised less control actions during attack in Scenario I than in Scenario II. On average the accuracy of detection for the contextual method increases by $0.37$ over the point method that accounts to $55\%$ in the presented scenarios. As presented in table III, the discovery of malicious control is performed well by both point and contextual detection, scoring $0.99$ or $1$ accuracy. For the attack in Scenario II both methods have $0.93$ accuracy. However the attack case of the Scenario I is more problematic or both methods however, contextual anomaly recognised $4$ times more true positives than point anomaly detection, increasing the accuracy by $56\%$.

## VI. CONCLUSION

An on-line IDS detecting malicious DER control two attack on voltage scenarios in the LV grid is described and tested in this paper. The IDS consists of a DER analysis with a contextual anomaly detection and a power system analysis with an impact analysis. The simulation results obtained from the chosen scenarios confirm that a contextual anomaly detection is more accurate than point anomaly detection.

In the present implementation the IDS analysis in limited to a simple voltage use case. A more broad analysis modules need to be added for other power system malicious control. The presented DER model is calculated from the near past historical data, in the next implementation the model needs to be recalculated periodically or be based on a large set of data. The presented IDS is designed to a local produce the IDS only associated with a control of a single DER. If the underlying model is recalculated periodically the ANN training execution complexity should be considered. Additionally the presented co-simulation set-up allows implementation of different attack profiles, future work can include implementation of different attack profiles.

## ACKNOWLEDGEMENTS

This research has been conducted as part of the SALVAGE project (Cyber-physical security for low-voltage grids) funded via ERA-Net SmartGrids programme.

## REFERENCES

[1] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (ami)," in *PES GM - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*. IEEE, 2008, pp. 1–5.

[2] A. Creery and E. Byres, "Industrial cybersecurity for power system and scada networks," in *Petroleum and Chemical Ind. Conf., 2005. Industry Appl. Soc. 52nd Annual*. IEEE, 2005, pp. 303–309.

[3] G. N. Ericsson, "Cyber security and power system communication essential parts of a smart grid infrastructure," *Power Delivery, IEEE Trans.*, vol. 25, no. 3, pp. 1501–1507, 2010.

[4] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[5] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 847–855, 2013.

[6] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[7] D. Yang, A. Usynin, and J. W. Hines, "Anomaly-based intrusion detection for SCADA systems," in *5th intl. topical meeting on nuclear plant instrumentation, control and human machine interface technologies (npic&hmit 05)*. Citeseer, 2006, pp. 12–16.

[8] A. Zaher, S. McArthur, D. Infield, and Y. Patel, "Online wind turbine fault detection through automated SCADA data analysis," *Wind Energy*, vol. 12, no. 6, p. 574, 2009.

[9] M. Sanz-Bobi, A. M. San Roque, A. de Marcos, and M. Bada, "Intelligent system for a remote diagnosis of a photovoltaic solar power plant," in *Journal of Physics: Conference Series*, vol. 364, no. 1. IOP Publishing, 2012, p. 012119.

[10] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "On detection of cyber attacks against voltage control in distribution power grids," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*. IEEE, 2014, pp. 842–847.

[11] X. Song, M. Wu, C. Jermaine, and S. Ranka, "Conditional anomaly detection," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 19, no. 5, pp. 631–645, 2007.

[12] Z. Zhao, W. Xu, and D. Cheng, "User behavior detection framework based on nbp for energy efficiency," *Automation in Construction*, vol. 26, pp. 69–76, 2012.

[13] V. M. Catterson, S. D. McArthur, and G. Moss, "Online conditional anomaly detection in multivariate data for transformer monitoring," *Power Delivery, IEEE Transactions on*, vol. 25, no. 4, pp. 2556–2564, 2010.

[14] M. E. Khan and F. Khan, "A comparative study of white box, black box and grey box testing techniques," *Int. J. Adv. Comput. Sci. Appl*, vol. 3, no. 6, 2012.

[15] F. Almonacid, C. Rus, L. Hontoria, M. Fuentes, and G. Nofuentes, "Characterisation of si-crystalline pv modules by artificial neural networks," *Renewable Energy*, vol. 34, no. 4, pp. 941–949, 2009.

[16] S. Ebron, D. L. Lubkeman, and M. White, "A neural network approach to the detection of incipient faults on power distribution feeders," *Power Delivery, IEEE Transactions on*, vol. 5, no. 2, pp. 905–914, 1990.

[17] M. Martinelli, E. Tronci, G. Dipoppa, and C. Balducelli, "Electric power system anomaly detection using neural networks," in *Knowledge-Based Intelligent Information and Engineering Systems*. Springer, 2004, pp. 1242–1248.

[18] A. El Shahat, "Pv cell module modeling & ann simulation for smart grid applications," *Journal of Theoretical and Applied Information Technology*, vol. 16, no. 1, pp. 9–20, 2010.

[19] "Pecan Street Smart Grid Demonstration Program - Final Technology Performance Report," Pecan Street Inc., Tech. Rep., February 2015.

[20] B. D. Ripley, *Modern applied statistics with S*. Springer, 2002.

[21] J. D. Head and M. C. Zerner, "A BroydenFletcherGoldfarbShanno optimization procedure for molecular geometries," *Chemical physics letters*, vol. 122, no. 3, pp. 264–270, 1985.