Coherency-Based Detection Algorithm for Synchrophasor Cyberattacks

Philip Hart, Sowmya Acharya, Honggang Wang
GE Global Research
Niskayuna, New York, USA
philip.hart@ge.com

***Abstract*—The wide area monitoring system (WAMS) is critical for power system situational awareness, but represents a growing cybersecurity vulnerability. Malicious adversaries may seek to compromise one or more PMUs in order to effect control decisions that unnecessarily disrupt typical grid operations. One example of a particularly pernicious attack vector is the spoofing or replaying of a fault event using one or more compromised PMUs. This work documents the development and validation of a coherency-based cyberattack detection algorithm that integrates a sliding-window singular value decomposition (SVD) with physics-based partitioning analysis to achieve accurate classification of events. Special consideration is given to discerning a sophisticated fault-replay or fault spoofing attack from actual faults. A software-based cybersecurity testbed has been developed for rigorous testing of the algorithm. The algorithm is further validated using simulated synchrophasor datasets obtained from a MinniWECC 63-bus test system. Results show that the algorithm can successfully detect fault-replay attacks even when over half of the PMUs are compromised.**

***Index Terms*—Cyberattack, WAMS, synchrophasors, replay attack, detection algorithm, event classification, coherency, fault**

I. INTRODUCTION

Widespread deployment of phasor measurement units (PMUs) in the transmission system is leading to an increased level of situational awareness. However, since important control decisions may be executed based on input from this monitoring system, synchrophasor measurements represent a large and growing cybersecurity vulnerability. One example of a particularly pernicious attack vector is the spoofing or replaying of a fault event using one or more compromised PMUs. If such an attack displays a superficial consistency with typical fault behavior, it could potentially trick a human operator or an automated controller into implementing protective actions, potentially resulting in loss of load.

There has been considerable attention given in the literature to detection algorithms for anomalous WAMS data, particularly in the context of state estimation [1]. However, the detection of cyberattacks often warrants a dedicated approach, as they are hard to identify using the conventional

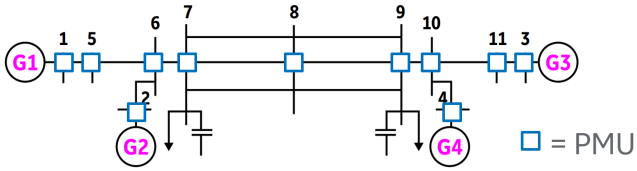


Fig. 1: WAMS network deployed in an example 2-area, 11-bus test system from [14].

methods for detecting bad data [2]. The survey in [3] lists different types of power systems cyberattacks and defenses against them. Cyberattack detection techniques can be classified using a dichotomy of model-based versus data-driven. For example, the model-based algorithms in [4], [5], and [6] depend on availability of an accurate system model, whereas in [7], a data-driven approach is employed.

Model-free, data-driven detection algorithms are appealing, as they can be more convenient to deploy than model-based methods. Ideally, data-driven approaches are also computationally-efficient and can be employed in real-time or near-real-time. The authors of [7] recognize the low-rank property of PMU data matrices and formulate a convex optimization problem for the detection of data substitution attacks. However, the matrix factorizations and optimization render this data-driven algorithm computationally expensive, therefore potentially not amenable to online attack detection.

While replay attacks can be particularly challenging to address, there has been work done on data-driven replay detection algorithms. The authors of [8] propose a detection algorithm which periodically injects a randomized signal to the measurements and use a linear time-invariant model of the system to detect replay attacks on smart-meter data. The data-driven approach presented in [9] introduces a metric called self-correlation coefficient for detection of replay attacks in power systems. The approach leverages the fact that the replay attack portions of the measurements show more periodicity than normal measurements. Reference [10] uses data mining techniques to detect cyberattacks including replay attack. The key concept used is called common path mining, which works by checking if a certain sequence of events has occurred in the prescribed manner. The detection system is first given a

This material is based upon work supported by the Department of Energy CEDS program under Award Number(s) DE-OE0000830.

representative set of paths which serve as signatures for normal operating scenarios. The actual measurements are then compared to these signatures to flag anomalies, if any. Reference [11] proposes a method which monitors the intra-PMU and inter-PMU correlations between different measurement quantities. Injection of spoofed data alters the normal values of these correlations and can be detected. The true-positive rate (TPR) obtained by the authors ranges between 77% and 86% for different scenarios.

In the aforementioned work, there is still a significant research gap associated with data-driven WAMS cyberattack detection algorithms that can (i) operate autonomously from the control center with minimal reliance upon the model or state; (ii) that can detect sophisticated fault-replay attacks or 'spoofed' fault signals with very high true-positive rate (TPR); and (iii) that can be rapidly trained and commissioned in the field. The objective of this work is to develop and validate a detection algorithm that has these properties.

In the proposed cyberattack detection algorithm, strong emphasis has been placed on the capability to discern actual physical fault events (e.g., short circuits, line faults, etc.) from spoofed synchrophasor waveforms that mimic fault-like behavior, including replay attacks. Whether implemented as a component of the phasor data concentrator (PDC) data quality reporting service or as a preconditioning step within WAMS applications at the control center, the algorithm in this work is intended to operate nearly autonomously from control center applications. Considering that fault events are relatively uncommon, and a large library of representative fault events may be difficult to accumulate, training and parameter tuning may best accomplished using data-driven methods that can exploit limited amounts of information about the physical model, if such information is available. Feature selection is made with consideration given to well-known physical properties of generic power networks, including spatiotemporal correlations and physics-based principles that broadly apply to most 3-phase, sparsely-connected, reactive power grids of arbitrary size and interconnection.

II. Detection Algorithm

To achieve fast and accurate event classification, rapid commissioning, and semi-autonomy from the control center, the developed cyberattack detection algorithm integrates a combination of data-driven and model-based methods. The following sections provide background regarding two techniques that are instrumental in the operation of the proposed cyberattack detection algorithm, including (i) the singular value decomposition (SVD); and (ii) an example model-based power system partitioning analysis tool.

A. Creation of Synthetic RSVs using Coherency Identification Algorithms

Since the SVD transformation serves as a core component of the algorithm, fundamental background on the SVD is now provided. Let $\mathbf{X}$ represent an $n \times m$ data matrix, wherein m represents the number of synchrophasor variables and n represent the number of synchrophasor data samples, or observations. The synchrophasor variables can comprise complex-valued phasor measurements or real-valued magnitudes and/or phase angles from one or multiple PMUs. The singular value decomposition (SVD) is a factorization of the centered data matrix $\mathbf{X}$. The SVD factorization is given by:

$$\mathbf{X} = \mathbf{U}\mathbf{\Delta}\mathbf{V}^T$$

where $\mathbf{\Delta}$ is a diagonal matrix containing singular values (positive numbers, ordered from largest to smallest) and $\mathbf{U}$ is an $n \times n$ matrix whose columns are the eigenvectors of $\mathbf{X}\mathbf{X}^T$. The matrix $\mathbf{V}$ contains the right singular vectors and is equivalent to the matrix of right eigenvectors of $\mathbf{X}^T\mathbf{X}$.

For a power system of arbitrary size and interconnection, vector-valued equation set (1) represents the well-known differential equations and algebraic constraints that dictate the angle (δ) and frequency (ω) dynamics of buses within the power system, in the electromechanical timescale [12].

$$\begin{aligned} \dot{\vec{\omega}} &= \mathbf{M}^{-1}(\mathbf{L_1}(\vec{P}_I - \vec{P}_N(\vec{\delta},\vec{V}))) \\ \mathbf{L_1}\dot{\vec{\delta}} &= \vec{\omega} \\ 0 &= \mathbf{L_2}(\vec{P}_I - \vec{P}_N(\vec{\delta},\vec{V})) \\ 0 &= \vec{Q}_L(\vec{V}) - \vec{Q}_{NL}(\vec{\delta},\vec{V}) \end{aligned} \quad (1)$$

In (1), $\mathbf{M}$ denotes a diagonal matrix with generator inertias along the entries, ordered by bus number, $\mathbf{L_1}$ denotes rows 1 through *m* of an *n*x*n* identity matrix, $\mathbf{L_2}$ denotes rows *m* through *n* of an *n*x*n* identity matrix; $\vec{P}_N :=$ a nonlinear, vector-valued function for the active power absorbed by the network, at each node; $\vec{P}_I :=$ vector of net active power injection at each node; $\vec{Q}_N :=$ a nonlinear, vector-valued function for reactive power absorbed by the network at load buses; $\vec{Q}_L :=$ vector of reactive power loads, at load buses. Functions $\vec{P}_N, \vec{P}_I, \vec{Q}_{N,L}, \vec{Q}_L$ are defined in [12].

Following a significant physical fault event within a given power system, a 'coherency signature' can usually be observed within the behavior of the network voltage angles. This coherency signature consistently depends more upon the particular structure and parameterization of the dynamic equation set (1) than it is upon the location, severity, or type of the fault. Over the past decades, partitioning strategies have been developed that use the physical model (1) to predict this coherency signature [12], [17]. The objective of such work is to utilize this signature to guide the aggregation of coherent nodes, and ultimately to develop a reduced-order dynamic model. Notably, as an alternative to using the physical model (1) to predict coherency, the SVD can be applied to a time window of synchrophasor data in which the dynamics of (1) are active [13].

The algorithm developed here leverages the link between the SVD and physics-based power system partitioning algorithms for purposes of detecting anomalous data, including bad data and sophisticated replay cyberattacks. More specifically, a physics-based partitioning method will

be used as a means to train or supplement the training of the cyberattack detection algorithm.

It is clear that within the network, PMUs may be placed at either generator nodes or 'PQ' nodes. 'Structure preserving' partitioning methods, such as the Generalized Eigenvalue Perturbation (GEP) algorithm [12], or Fiedler eigenvector analysis of the network admittance matrix, are especially relevant to this anomaly detection algorithm. Such methods can determine the existence of coherency (or lack thereof) at not only generator nodes, but also the PQ nodes at which PMUs will likely be placed.

As an example, the GEP partitioning algorithm [12] is reviewed below and linked to the SVD, with the ultimate goal of training a simple cyberattack detection algorithm described later. Notation is borrowed from [12]. The GEP approach can be implemented by following the step-by-step instructions described in Section IV of [12]. These instructions are summarized in steps 1 through 4, below. Step 5 connects the partitioning result to the detection algorithm.

1. $\mathbf{E}$ and $\mathbf{R}_S$, matrices defined in [12], are closely related to a linearized version of (1). As a first step, these two matrices are computed, assuming a particular equilibrium operating point of (1). For the differential-algebraic system comprised by $(\mathbf{E},\mathbf{R}_S)$, the smallest generalized eigenvalue and its associated eigenvector are identified, denoted by λ and v, respectively.

2. The gradient of the generalized eigenvalue λ with respect to the vector of network susceptances, $\vec{bl}$, is then computed. Under simplifying assumptions, index i of gradient $\vec{g}$ is given by a readily-identifiable analytical expression:

$$\vec{g}_i = \partial\lambda / \partial\vec{bl}_i = \frac{v^{\mathrm{T}} \frac{\partial \mathbf{R}_s}{\partial \vec{bl}_i} v}{v^{\mathrm{T}} \mathbf{E} v}$$

3. Gradient $\vec{g}_i$ is used to identify the element of the network chosen for deletion, by finding the smallest positive and real constant γ such that for some index r: $[\vec{bl} - \gamma\vec{g}]_r = 0$. Delete the entry at index r of the susceptance vector $\vec{bl}$.

4. Repeat Steps 1 - 3 for the new system with the missing branch, until a sufficient number of branches have been eliminated such that the nodes of the original network are fully partitioned into two disjoint subsets. A single iteration of the GEP algorithm has now been completed.

5. Once the network has been partitioned into two disjoint subsets of nodes (Subset 1 and Subset 2) using the GEP algorithm, a 'synthetic' right singular vector (RSV) is created. This synthetic RSV constitutes a prediction of a vector within the $\mathbf{V}$ matrix obtained from the SVD. This synthetic RSV is first instantiated as a zero vector with length equal to the number of PMUs associated with the synchrophasor angle data matrix, with the first element of the synthetic RSV corresponding to the first column of data (i.e., the first PMU), the second element of the synthetic RSV corresponding to the second PMU, and so on. The elements of this synthetic RSV are populated with a '1' or '-1' depending on whether the node that hosts each PMU is located in Subset 1 or Subset 2, respectively. If PMUs are not included within the boundaries of the portion of the network subject to the above GEP partitioning analysis, the element associated with that PMU remains zero. Once all elements are appropriately populated, the synthesized RSV is then normalized to have a magnitude of 1.

6. To generate additional synthetic RSVs for the network that correspond to faster inter-area system modes across smaller areas of the network, steps 1-5 can be iteratively repeated for the sub-networks of the power system associated with Subset 1 and Subset 2 determined in Step 4.

B. Event Classification

Fig. 2 shows a block diagram of the proposed cyberattack detection algorithm. The singular value decomposition (SVD) is applied to the pre-processed sliding window of synchrophasor data, and the resulting features are post-processed to create signatures of the system, which are subsequently utilized within both the event detection and classification subroutines. The event detection examines the SVD features for evidence of an event. Upon detection of an event, the event classification subroutine is invoked. To classify the event, the classification subroutine computes a measure of similarity between right singular vectors (RSVs) obtained from the SVD of the new time window of data either to (i) older SVD-derived signatures saved from historical fault events (a fully data-driven approach); or (ii) 'synthetic' RSVs

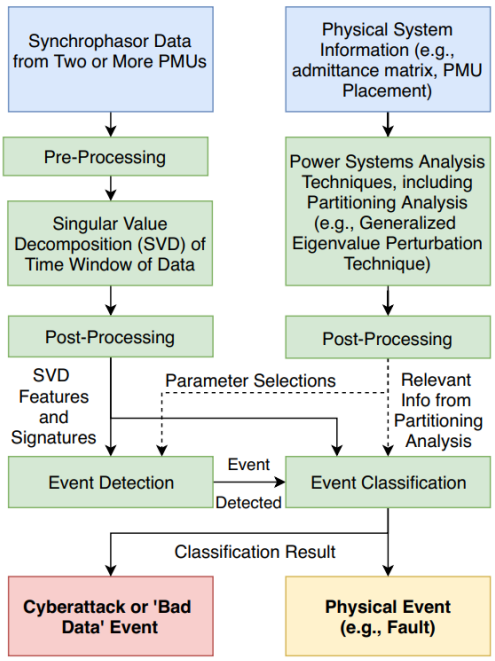


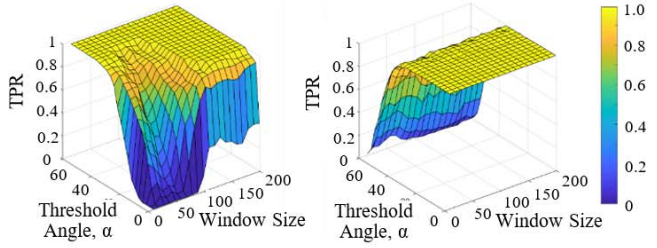
Fig. 2: Block diagram of synchrophasor cyberattack detection algorithm

developed using a partitioning analysis (a fully model-based approach); or both (i) and (ii). The measure of similarity is compared to a threshold value, termed 'Threshold Angle', α. If the similarity measure exceeds a certain threshold value, the synchrophasor data window is classified as anomalous (i.e., a cyberattack or bad data event). Additional model-based analyses besides the partitioning analysis can improve confidence in the selection of optimal algorithm parameters, such as certain decision thresholds and the size of the data window used for the SVD. While a partitioning analysis could be applied exclusively to the admittance matrix, the GEP method has been utilized as it more-accurately captures important electromechanical dynamics following a fault event.

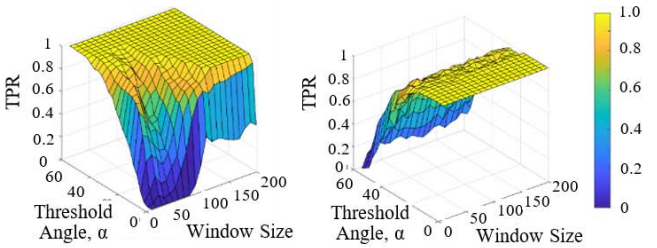
III. Validation of Algorithm Performance

A software-based testbed was realized in the MATLAB/Simulink platform to facilitate the development and rigorous evaluation of the WAMS cyberattack detection algorithm. Within this testbed environment, a first-principles, physics-based model of a standard 4-machine, 2-area power system (Fig. 1), as described in [14], is used to generate realistic trajectories of system states in response to fault or cyberattack events. The test environment is capable of automatically simulating a large number of randomized transient events using the two-area test system, including actual fault events and spoofed data injections from compromised PMU(s) that resemble fault events. Randomized parameters can include, but are not limited to: the nature of the fault (e.g., 3-phase short circuit or line fault), location of and severity of physical fault events, as well as the placement and total quantity of PMUs. To test the algorithm post-event performance, the classification subroutine was applied to windows of PMU data recorded using the 2-area, 11-bus simulation testbed. For the cyberattack simulations, waveforms at a fixed number of randomly-selected 'compromised' PMUs were recorded from the earlier fault simulations and replayed at those same nodes, while the remaining, uncompromised nodes displayed comparatively normal behavior associated with a random (small) load step disturbance. The difference in system frequency between fault and cyberattack simulations was not significant.

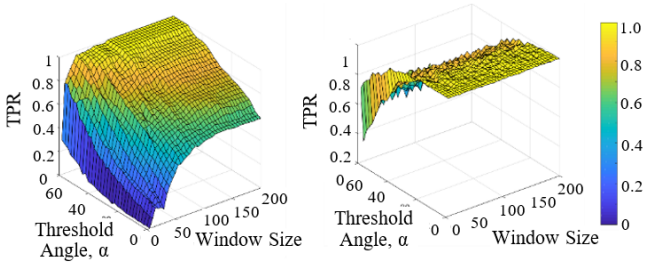
The results shown in Fig 3 demonstrate a thorough investigation of the 'true-positive rate' (TPR) for event classification—defined as the ratio of correct detections of an event divided by the number of events (e.g., the number of correct detections of a cyberattack divided by the number of



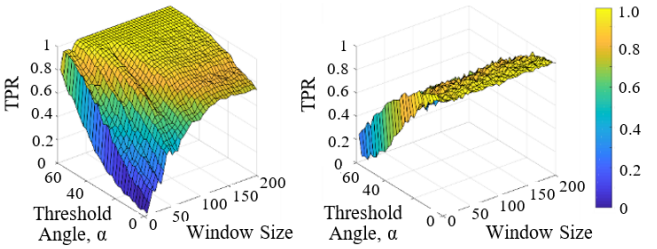
3(a) True positive rates for fault (*left*) and cyberattack (*right*) events; 11 PMUs; historical event signature used; nominal power system parameters.



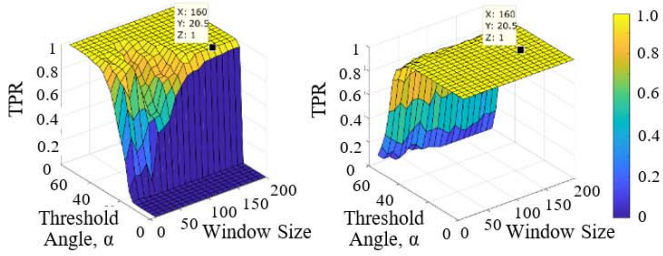
3(b) True positive rates for fault (*left*) and cyberattack (*right*) events; 7 PMUs; historical event signature used; nominal power system parameters.



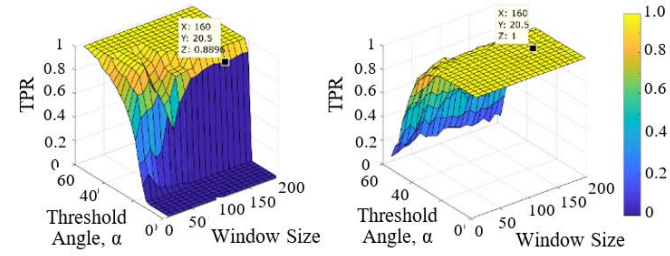
3(c) True positive rates for fault (*left*) and cyberattack (*right*) events; 11 PMUs; historical event signature used; augmented power system parameters.



3(d) True positive rates for fault (*left*) and cyberattack (*right*) events; 7 PMUs; historical event signature used; augmented power system parameters.



3(e) True positive rates for fault (*left*) and cyberattack (*right*) events; 11 PMUs; synthetic RSVs used; nominal power system parameters.



3(f) True positive rates for fault (*left*) and cyberattack (*right*) events; 7 PMUs; synthetic RSVs used; nominal power system parameters.

Fig. 3: Average true positive rate (TPR) as a function of decision threshold (α) and sliding window size, for various numbers of PMUs within the system. During cyberattack events, 5 PMUs are compromised.

TABLE I. SELECTIONS OF TPR RESULTS FROM FIG. 3 (FAULT TPR, CYBER TPR)

	Threshold	Window Size	11 PMU	7 PMU
Fig. 3(a)-3(b)	18 deg.	150 samples	Fig. 3(a): (1.0, 1.0)	Fig. 3(b): (1.0, 0.99)
Fig. 3(c)-3(d)	38 deg.	160 samples	Fig. 3(c): (0.91,0.87)	Fig. 3(d): (0.83,0.76)
Fig. 3(e)-3(f)	23 deg.	160 samples	Fig. 3(e): (1.0,1.0)	Fig. 3(f): (1.0,1.0)

cyberattacks). For every point on one of the 'fault event' TPR surface plots in Fig. 3, the fault event TPR value is calculated by: (i) applying the classification subroutine to PMU data (60 Hz sample rate) generated from 600 randomized fault simulations; then (ii) tallying the number of fault classifications; and (iii) dividing this number by the total number of detected events that were classified as either a fault or a cyberattack. Cyber event TPR (in the companion plot to the right of each fault TPR plot), is calculated in a similar manner, using 600 randomized cyberattack simulations for every point in the test matrix. The combined set of 1200 experiments are repeated across a test matrix of algorithm parameter combinations: two algorithm parameters are varied, including (1) the size of the sliding window used for the SVD; and (2) a particularly important decision threshold parameter ('Threshold Angle'). For all cyberattack events used for all subplots, five PMUs are compromised by the attacker.

In Fig. 3(a)-(d), a purely data-driven approach to algorithm training is pursued (GEP partitioning is not used). Features and signatures from only one historical event are used for signature comparison purposes, within the classification subroutine. For the nominal parameters of the Kundur test system, listed in [14], and for a large range of window size and decision threshold parameters, it can be observed that the algorithm has almost perfect performance (TPR near unity).

For a particular selection of parameters, Table 1 shows that algorithm had unity TPR for both fault and cyber classification when 11 PMUs were deployed, and near-unity TPR in the case that only 7 were deployed. Fig. 3(a) and 3(b) show that there is a clear dependency of the fault TPR on the data window size: at least 70 synchrophasor samples are needed in order for the SVD to properly capture the system signatures after a transient.

It should be acknowledged the system under consideration will not always contain two distinct areas separated by a long transmission corridor, as in the Kundur test system system [14]. In the results shown in Fig. 3(c) and 3(d), the length of the long transmission line corridor in the testbed's Simulink model is divided by 10. Subsequently, 1,200 randomized events are newly simulated. In the case of the augmented Fig. 3(c) and 3(d) and Table I show that the performance of the algorithm deteriorates significantly, especially in the case that only 7 PMUs are deployed. While results are not reported here due to space constraints, it was found through additional testing that the use of signatures from additional historical events can improve classification accuracy.

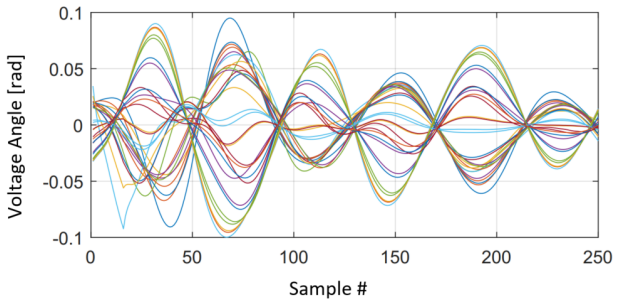


Fig. 4: Example voltage angle transient from post-processed, simulated synchrophasor data obtained from 30 buses of the MinniWECC system.

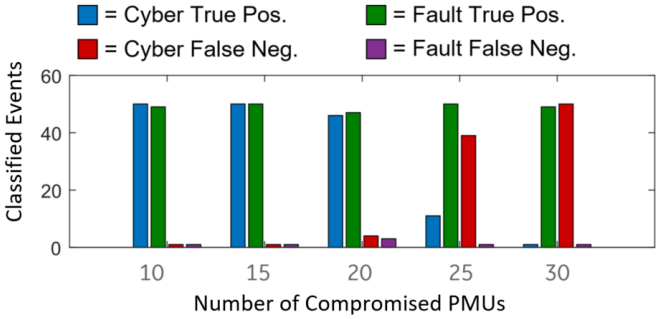


Fig. 5: Performance of detection algorithm when applied to MinniWECC simulation data: 30 PMUs are deployed.

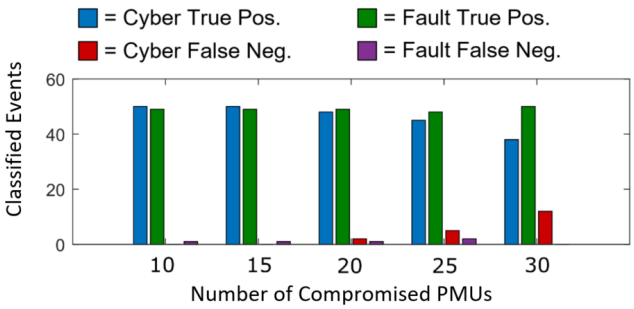


Fig. 6: Performance of detection algorithm when applied to MinniWECC simulation data: 40 PMUs are deployed.

To generate the surface plots in Fig. 3(e) and (f), a fully model-based approach to event classification was taken, using GEP partitioning analysis, and nominal parameters for the Kundur test system are again used. Knowledge of the network susceptances and the network incidence matrix, machine location and inertias, and PMU location is used to parameterize $\mathbf{E}$ and $\mathbf{R}_S$. To address the linearized equilibrium point implicit in the construction of $(\mathbf{E}, \mathbf{R}_S)$, conditions of zero load, zero power injection, uniform voltage magnitudes and 0 phase angle for all buses were assumed. Steps 1-4 of the GEP partitioning algorithm were applied. At the termination of the GEP algorithm, the parallel transmission lines defining the one half of the long transmission line corridor were identified as the optimal branch cutset separating two clusters of nodes. Under the tested conditions, the model-based approach was successful:

as shown in Fig. 3(e) and 3(f), a threshold angle of approximately 23-25 degrees would allow for perfect performance if either 11 or 7 PMUs are deployed.

The developed cyberattack detection algorithm was also validated using results from a MinniWECC model [15]. The MinniWECC model includes 115 ac transmission lines and 34 generators. PMU measurements are available from 63 buses. Fig. 4 shows post-disturbance voltage angle transients from 30 PMUs distributed throughout the MinniWECC system. To test the proposed algorithm, 5 realistic physical events were simulated. Fault-replay attacks were synthesized from these fault events. Five fault and cyberattack PMU datasets were collected for 10 random PMU deployment configurations, for a total of 100 tests (50 fault and 50 cyberattack). Finally, the 100 tests were repeated five times, by varying the number of compromised PMUs.

In the case that PMUs are deployed at 30 randomly-chosen buses in the system, Fig. 5 shows the relative amounts of correctly- and incorrectly-classified fault and cyberattack events for different quantities of compromised PMUs. The algorithm was found to perform satisfactorily: close to 50 of the fault events and close to 50 of the cyberattack events are classified properly even if 10 or 15 PMUs are compromised. If PMUs are deployed at 40 randomly chosen buses throughout the system, Fig. 6 shows that the performance of the algorithm improves significantly for the same numbers of compromised PMUs.

IV. Conclusions

Rigorous testing using software-based testbeds showed that the developed coherency-based WAMS cyberattack detection algorithm demonstrates either satisfactory or excellent performance under a broad range of conditions. However, performance of the algorithm was dependent upon the physical characteristics of the system included within the boundaries of the WAMS network, including the existence (or lack there-of) of dominant, inter-area swing modes within the WAMS network footprint. Under sub-optimal system conditions, the algorithm appears to require a larger number of PMUs and knowledge of more historical events to achieve satisfactory performance. The algorithm was shown to be able to function entirely in a purely data-driven manner, but also allow for training via one-time, expedient partitioning analysis of the power system if topological data is made available. In the case of both the original, unaltered Kundur 11-bus test system from [14] and in the more-realistic MinniWECC model, excellent performance was observed even under the circumstances in which features & signatures from only one historical event are available to the classification subroutine and a majority of the PMUs have been compromised in the cyberattack.

V. Acknowledgments

The authors acknowledge James Follum from Pacific Northwest National Laboratory (PNNL) for providing simulation data generated from the MinniWECC model.

References

[1] R. Deng, G. Xiao, R. Lu, H. Liang and A. V. Vasilakos, "False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey," *IEEE Transactions on Industrial Informatics,* vol. 13, no. 2, pp. 411-423, 2017.

[2] Y. Liu, P. Ning, Reiter and M. K., "False Data Injection Attacks Against State Estimation in Electric Power Grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security,* pp. 21-32, 2009.

[3] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications,* vol. 1, no. 1, pp. 13-27, 2016.

[4] S. G. Ghiocel *et al*, "Phasor-measurement-based state estimation for synchrophasor data quality," *IEEE Transactions on Power Systems,* vol. 29, no. 2, pp. 881-888, 2014.

[5] K. D. Jones, A. Pal and J. S. Thorp, "Methodology for Performing Synchrophasor Data Conditioning and Validation," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1121-1130, 2015.

[6] F. Pasqualetti, F. Dörfler and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," *IEEE Transactions on Automatic Control,* vol. 58, no. 11, 2013.

[7] M. Wang, "A Low-Rank Matrix Approach for the Analysis of Large Amounts of Power System Synchrophasor Data," in *48th Hawaii International Conference on System Sciences*, 2015.

[8] T. Tran, O. Shin and J. Lee, "Detection of replay attacks in smart grid systems," in *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*, 2013.

[9] M. Ma et al, "Detecting Replay Attacks in Power Systems: A Data-Driven Approach," in *Advanced Computational Methods in Energy, Power, Electric Vehicles, and Their Integration*, vol. 763, 2017.

[10] S. Pan, T. Morris and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems," *IEEE Transactions on Smart Grid,* vol. 6, no. 6, 2015.

[11] J. Landford, "Fast sequence component analysis for attack detection in smart grid," in *5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, 2016.

[12] C. DeMarco and J. Wassner, "A generalized eigenvalue perturbation approach to coherency," in Proceedings of the 4th IEEE Conference on Control Applications, Sep. 1995, pp. 611–617.

[13] K. K. Anaparthi, B. Chaudhuri, N. F. Thornhill and B. C. Pal, "Coherency identification in power systems through principal component analysis," in *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1658-1660, Aug. 2005.

[14] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. New York: McGraw-Hill, 1994, pp. 813-816.

[15] D. Trudnowski, D. Kosterev, and J. Undrill, "PDCI Damping Control Analysis for the western North American Power System," in *Power & Energy Society General Meeting*, 2013.

[16] J. D. Follum, "Electromechanical Mode Estimation in the Presence of Forced Oscillations," Ph.D. dissertation, University of Wyoming, 2014.

[17] J. Chow, *et al*, "Inertial and slow coherency aggregation algorithms for power system dynamic model reduction," *IEEE Transactions on Power Systems*, vol. 10, no. 2, pp.680–685, May 1995.