Machine Learning for Power System Disturbance and Cyber-attack Discrimination

Raymond C. Borges Hink, Justin M. Beaver,
Mark A. Buckner
Oak Ridge National Laboratory
Email: {borgesrc, beaverjm, bucknerma}@ornl.gov

Tommy Morris, Uttam Adhikari, Shengyi Pan
Critical Infrastructure Protection Center
Mississippi State Univeristy
Email: {morris, ua31, sp821}@msstate.edu

***Abstract*—Power system disturbances are inherently complex and can be attributed to a wide range of sources, including both natural and man-made events. Currently, the power system operators are heavily relied on to make decisions regarding the causes of experienced disturbances and the appropriate course of action as a response. In the case of cyber-attacks against a power system, human judgment is less certain since there is an overt attempt to disguise the attack and deceive the operators as to the true state of the system. To enable the human decision maker, we explore the viability of machine learning as a means for discriminating types of power system disturbances, and focus specifically on detecting cyber-attacks where deception is a core tenet of the event. We evaluate various machine learning methods as disturbance discriminators and discuss the practical implications for deploying machine learning systems as an enhancement to existing power system architectures.**

Keywords—machine learning, cyber-attack, SCADA, Smart grid

I. Introduction

The core mission of power systems is resilience - continued delivery of electricity to the customer. These systems have been designed with the redundancy and fault tolerance mechanisms to perform this mission, but at a time when computer security was not a design driver. As formerly physically isolated power systems were joined to the Internet for centralized control and management, it created a greater potential for unauthorized access and exposed these systems to the same vulnerabilities that plague traditional computer systems and networks.

Industrial control systems, such as those used in the Smart Electric Grid, are becoming more complex in their architecture and design. The Supervisory Control and Data Acquisition (SCADA) systems that are used are more interconnected and span multiple communication protocols and physical interfaces. The methods by which data are collected from remote locations, as well as commercially available SCADA software developed for physically isolated systems, lead to more potential flaws in the hardware and software and provide a much larger attack surface to threat agents [20]. Every asset of the Smart Grid, from home gateways to smart meters to substations to control rooms, is a potential target for a cyber-attack [21].

Modern power systems are now connected to the Internet and computer security is a new threat to resilience [18, 19]. Power companies must now engineer security into their systems in arrears of the system design, or rely exclusively on traditional computer network defenses to prevent unauthorized access. Power system operators who monitor, assess, and react to disturbances must now consider the new possibility that the system is under a cyber-attack. This question is particularly challenging for a human to answer because, unlike natural disturbances or faults, a cyber-attack is designed to deceive.

In this work, we explore the suitability of machine learning methods as a means of discriminating power system disturbances. We theorize that the machine learning algorithms will leverage non-linear complex relationships between power system measurements and that these will be sufficient to discriminate between malicious, non-malicious and natural disturbances. Cyber-attacks can have the same effects as natural events and so differentiating between malicious and non-malicious in a large and interconnected system can be overwhelming if not infeasible for a human. The intent of this work is to determine an optimal algorithm that is accurate in its classification such that it can provide reliable decision support to a power system operator, and thus relieve that operator of the burden of determining whether a disturbance is an intentional act. We evaluate the classification performance of various machine learning methods and discuss the implications for fielding machine learning systems and any associated operational constraints. The remainder of this paper is organized as follows. Section 2 presents related work. Section 3 discusses our methodology when applying our experiments and subsequent testing of machine learning methods. In Section 4 we describe our results. And finally, Section 5 presents conclusions.

II. Related Work

Machine learning has distinguished itself as a discriminator of malicious and anomalous events in intrusion detection for traditional cyber security networks [32] [33] [34]. These are systems that analyze the network transactions between computers and have been trained to characterize and recognize behavioral patterns in that traffic. Our approach is to extend this work and apply it to power systems, where networks are the means for communicating the state and operation of different power delivery components. This application focuses on the simultaneous assessment of dozens of variables associated with devices such as relays and generators as they are communicated within the power system network. The subsections below describe the vulnerabilities associated with modern power systems and the related work in intrusion detection systems (IDS) that domain.

A. Synchrophasor-based Smart Grid Cyber Security

The smart grid consists of two layers, cyber and physical systems. The two layers are coupled with each other and form the cyber-physical environment. The Synchrophasor or Phasor Measurement Unit (PMU) technology is built upon the cyber layer and provides real-time data to the energy management system (EMS) for the purpose of controlling the physical system. Such processes are presented as a sequence of execution events in the cyber-physical environment. The synchrophasor data includes not only the measurements such as voltage and current phasors but also the status of system devices including relays, breakers, switches, and transformers [1]. The extreme low latency offered by time-synchronized data provides a huge volume of data with extra information and enables various real-time power system control algorithms in order to increase smart grid reliability and stability [2] [3] [4]. The deployment of synchrophasor technology accelerates the use of communication networks within utilities and between neighboring utilities. The latest synchrophasor devices are vulnerable to cyber-attacks [7]; there are still large numbers of legacy devices in service with little or no protection against the attacks.

Contemporary attacks against a power system can be launched from a compromised personal computer (PC) through a network to control a breaker. For example, the Aurora event highlights the potential for an attacker to open and close a breaker at high speed from a remote connection to damage an electric generator [5]. Vulnerabilities can also be exploited against Intelligent Electronic Devices (IED) by uploading malicious settings. The Stuxnet worm [1] is an example of settings changes on a control device causing a physical system to malfunction. Moreover, most network protocols used in power systems are open standard protocols without any security features. Such protocols include IEEE C37.118 protocol, used for synchrophasor data streaming, MODBUS, used to remotely monitor and control IED, and DNP3, which is also used to remotely monitor and control IED. The penetration tests conducted in [6] and [7] have shown that cyber-attacks targeted against substation computers and devices can lead to Denial of Service (DoS) by making communication with a device impossible or causing devices to crash or reset and therefore prevent real time monitoring and controlling of the power system.

B. IDS for Smart Grid

In recent years, the emergence of Smart grid has motivated research into a variety of intrusion detection techniques. People with different backgrounds have created various intrusion detection systems (IDS) that focus on different intrusions against Smart grid. One type of IDS research focuses on IED security within Smart grid. For example, Chee-Wooi Ten et al. in [8] developed an anomaly-based detection technique for intrusions to IED. The Chee-Wooi Ten IDS is host-based thus only identifies attacks against a single IED in the substation using sequential events recorded in the log from that IED. Another IDS proposed by Chen et al. in [9] provides a protection mechanism for smart household appliances. Chen et al. created security rules for individual appliances by proposing homogeneous functions that models three factors of the appliance: device security, usability and electricity pricing. More advanced IDS of this type will consider behaviors of multiple devices within the system to obtain system level detection. In [10], Robert Mitchell et al. propose specification-based IDS for the electric grid by considering the behaviors of three types of physical devices in the electric grid: head-ends, distribution access points/data aggregation points and subscriber energy meters. They use readings from 22 sensors from the three types of devices as state components. By quantizing each of the 22 components into a limited number of ranges, they manually build three state machines with 3456, 1728, and 3456 states for the three devices respectively in the terms of conjunctive normal form. It's very expensive to build such IDS's due to the large state space. In addition, this IDS uses a limited number of sensors therefore it's able to detect a small number of attacks. And also the method is not scalable, since there are always new attacks and applications.

Another type of IDS for Smart grid leverages communication traffic in the information infrastructure to detect cyber-attacks. Yang et al. propose an IDS in [11] for synchrophasor systems that detects cyber-attacks by using access control white lists, protocol-based white lists and network behavior-based rules, each of which specify security rules in different layers of the synchrophasor system. The Yang et al. intrusion detection is limited to cyber-attacks including Man-in-the-Middle (MITM) and Denial of Service (DoS) against synchrophasor devices and IEEE C37.118 protocol. Similar to Yang's IDS, Zhang et al. in [12] propose a distributed IDS that analyzes communications traffic at different network levels of smart grid including home area networks, neighborhood area networks, and wide area networks. An intelligent module is deployed at each level to classify malicious data and possible cyber-attacks using data mining algorithms. These modules then communicate to get a system level view of the status of the whole communication network to improve the detection accuracy. Hadeli et al., in [13], propose an anomaly detection technique for industrial control systems that extracts behavior patterns of devices from protocols used in industrial control systems, for example, GOOSE messages, IEEE 61850, Manufacturing Message Specification, Modbus/TCP and redundant network routing protocols. The Hadeli et al. IDS uses a system description file to include a full description of the overall communication pattern in the industrial control system.

For the case of power system control applications, the system description file describes expected system behaviors from information carried by those protocols. Hadeli's method, along with [11] and [12] is efficient to detect malicious activities that cause changes in network traffic, but the IDS fails to detect malicious actions that result in invalid changes to the physical system. For example, Hadeli's method cannot detect a malicious trip command from a valid IP address that trips a relay, taking a transmission line out of service and causing a blackout. A specification-based IDS that can track sequential events in the system is reported in [14] for advanced metering infrastructure (AMI). The authors manually build the state machine by extracting specifications from two AMI protocols and they consider the devices status. To prove the correctness of the state machine, they use a model checking technique to verify their specifications. This IDS is also not applicable to transmission systems because transmission systems have far more control applications and disturbances than AMI. As such, manually building a state machine is very expensive.

While the two types of IDSs mentioned above were created from a computer science perspective, there has been work to create IDSs for Smart grid using power system theories. For instance, Valenzuela et al. [15] used optimal power flow programs to detect cyber-attacks, leveraging the notion that the bad data will cause the power flow to be dispatched erroneously. Talebi et al. in [16] proposed a mechanism for identification of bad data attacks in a power system using weighted state estimation. Zonouz et al. proposed an IDS that not only examines the measurement data using state estimation and power flow theory but also includes the results from network IDS to calculate the probability that the data is compromised [17]. Although these works all proved to be functional to detect false data, the limitation of this type of IDS is that it's limited to one type of attack and cannot be extended to detect other attacks against power systems.

In our previous work [36] we applied multiple learning algorithms to Modbus RTU data in order to show their viability as intrusion detection tools on a simple gas pipeline system. State-of-the-practice classification algorithms were applied in order to demonstrate an ability to discriminate command and data injection attacks for simple and small-scale SCADA systems. This was a foundation for the viability of machine learning in this domain.

In this work, we extend that approach in both complexity of the system under evaluation and in the sophistication of the classification methods applied. Our hypothesis is that the learning algorithms can detect disturbances and reliably classify them as a natural or malicious disturbance, despite any attempts at deception.

III. METHODOLGY

This section describes our approach to evaluating machine learning classification techniques for discriminating power system disturbances. The system used for evaluation is described as well as the different natural and man-made scenarios. We also discuss the machine learning methods used and the different approaches to classification.

A. Power System Description

In Figure I we show the power system framework used in this evaluation, a complex mix of supervisory control systems interacting with various smart electronic devices complemented by network monitoring devices such as SNORT and Syslog systems. The network is composed of 4 breakers controlled by intelligent electronic relays. These IEDs relay information back through a substation switch through a router back to the supervisory control and data acquisition systems. Attack scenarios were built and simulated with the assumption that an actor had already gained access to the substation network and poses an insider threat by issuing commands from the substation switch.

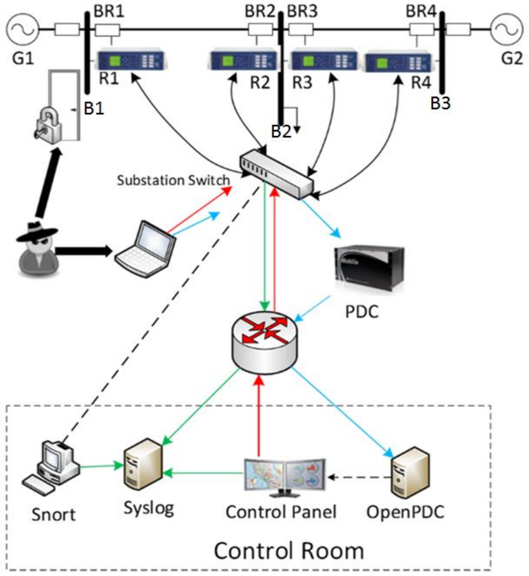

Fig. I. Experiment Network Diagram

In Figure I we have several components; firstly, G1 and G2 are power generators. R1 through R4 are IEDs that can switch the breakers on or off. These breakers are labeled BR1 through BR4. We also have two transmission lines. Line 1 spans from bus B1 to bus B2 and Line 2 spans from bus B2 to bus B3. Each IED automatically controls one breaker. R1 controls BR1, R2 controls BR2 and son on accordingly. The IEDs use a distance protection scheme which trips the breakers on detected faults whether actually valid or faked since they have no internal validation to detect the difference. Operators can also manually issue commands to the IEDs R1 through R4 to manually trip the breakers BR1 through BR4. The manual override is used when performing maintenance on the lines or other system components. In our analysis, we explicitly include examples from multiple operational scenarios in order to have confidence that any attack discrimination was valid during normal operations where the breakers were manipulated. The man-made disturbance scenarios are listed below.

Types of Scenarios:

1. *Short-circuit fault* – this is a short in a power line and can occur in various locations along the line, the location is indicated by the percentage range.
2. *Line maintenance* –one or more breakers are opened via the remote relay trip command for maintenance.
3. *Remote tripping command injection* (Attack) – this is an attack that sends a command to a relay which causes a breaker to open. It can only be done once an attacker has penetrated outside defenses.
4. *Relay setting change* (Attack) – relays are configured with a distance protection scheme and the attacker changes the setting to disable the relay function such that relay will not trip for a valid fault or a valid command.
5. *Data Injection* (Attack) – here we imitate a valid fault by changing values to parameters such as current, voltage, sequence components etc., in order to blind the operator and cause a black out.

B. Analytic Approach

To judge the viability of using machine learning for intrusion detection on smart grid electrical systems we tested various popular learners using Weka [22] as the machine learning framework and open-source simulated power system data provided by Mississippi State University [37]. The classification of events was performed using three different classification schemes:

- Multiclass - Each of the 37 event scenarios, which included attack events, natural events, and normal operations, was its own class and was predicted independently by the learners,
- Three-class – The 37 event scenarios were grouped into 3 classes: attack events (28 events), natural event (8 events) or “No events” (1 event).
- Binary – The 37 event scenarios were grouped as either an attack (28 events) or normal operations (9 events).

The data was drawn from 15 data sets which included thousands of individual samples of measurements throughout the power system for each event type. The datasets were randomly sampled at 1% to reduce the size and evaluate the effectiveness of small sample sizes. For this analysis, there was an average of 294 “No event” instances, 3,711 attack instances and 1,221 natural events instances used across the classification schemes. The date and time information were removed since scenarios were run sequentially and time and date would perfectly classify the data.

For each of the three schemes, Multiclass, Three-class and Binary, we tested 7 learners on 15 datasets. When running the experiments we chose to use the tenfold or 10x cross validation methodology. When testing using this method we partitioned the dataset into 10 sets randomly selecting instances from each category. The model was built on a ninety percent selection from the data and tested on the remaining ten percent of the data to evaluate the learner’s performance. We repeated this for each learner and each dataset then taking the average over the fifteen datasets to summarize the results.

The classification algorithms we tested were:

OneR – This is a learner with a very simplistic method that evaluates each feature’s optimum rule and chooses the best one [24] from all feature rule sets.

NNge – a nearest-neighbor-like algorithm that classifies examples by comparing to those already seen and comparing the new examples to its surrounding data points [27].

Random Forests – this is an ensemble of tree predictors where each tree casts a vote for the most popular class on input of a new instance [23]. The collection of decision trees are created from randomly pulled training data samples.

Naïve Bayes - is a probabilistic classifier based on the Bayes' theorem [25] that reflects the conditional probability distribution of a set of random variables, and was adopted into the field of machine learning in 1992 [26].

SVM – Support vector machines [28] trained using sequential minimal optimization [29]. An SVM model is a representation of the examples as points in a space, with classes divided by a mathematically determined set of hyperplanes that maximize the margin between the classes. New examples are then predicted to belong to a class based on their position in that space relative to the hyperplanes.

JRipper – Incremental Reduced Error Pruning algorithm that uses a separate-and-conquer methodology developed in [30] and modified by Cohen as shown in [31] to generate a sophisticated rule set.

Adaboost – short for Adaptive boosting, this is an algorithm use to improve the performance of other types of learning algorithms [35]. It is an ensemble learning method where each new model instance focuses on training examples that were misclassified in the previous models. By combining Adaboost with our strongest performer we achieve much better results. AdaBoost M1 method used in Weka can be used in conjunction with learners to improve their performance.

The classifiers we used can be grouped under these categories:

- Probabilistic classification (Naïve Bayes)
- Rule induction (OneR, NNge, JRipper)
- Decision tree learning (Random Forests)
- Non-probabilistic binary classification (SVM)
- Boosting, a meta-algorithm for learning (Adaboost)

IV. RESULTS

The results of our evaluation and analysis of the viability of machine learning as a method for power system disturbance discrimination are presented below. Initially, we evaluate the accuracy of various learners across all data sets in order to establish a pattern of consistency in the classification results. We follow with an evaluation of the various learning methods to the power system data to evaluate the power system disturbance classification. Next is an analysis of the most significant individual features that contribute to a decision. We conclude our analysis with a discussion on the operational viability of learning methods given the results of this research.

A. Analysis of Accuracy Results

The accuracy of a learner is defined as the percentage of correct classifications relative to the total number of classification decisions the learner made. When classes are balanced, accuracy provides a good general indicator of classifier performance. The machine learning method evaluation in Section III.B presents performance measures of the 10-fold cross validation averaged across all data sets. The goal of this is initial analysis step is to establish the consistency of learner performance across data sets so that any averaged performance values remain credible.

In Figures II, III and IV we show the classification accuracy average over the 15 datasets for multiclass, three-class and binary classification using 7 different algorithms. Note the consistency of the results regardless of the data set to which the learning method is applied. While minor variations exist for each learner, their individual performance remains steady regardless of the data set or classification scheme.

B. Machine Learning Method Evaluation

Having established that averaging the 10-fold cross validation results in a reasonable characterization of classifier performance over all data sets, we focus on the evaluation of the learners themselves using those averaged values. While accuracy provides a general indicator of classifier performance, recall, precision, and F-measure values give a more complete picture of how the classifier produces errors. Recall measures the true positive rate, precision measures the positive predictive value, and the F-measure is the harmonic mean of precision and recall. For these measures, values approaching 1.0 indicate strong classification performance.

Figure V shows the precision value of the various learners averaged over the 15 datasets where the 10-fold cross validation approach was used for each data set. Each line represents learner performance using the three different classification schemes. As the measure of positive prediction rate, precision provides a sense of the false positive values when predicting for specific class such as cyber-attack. For precision, Random Forests, JRipper and Adaboost+JRipper have the strongest performance over all classification schemes, with Adaboost+JRipper for the three-class scheme having the highest average precision value (0.991).

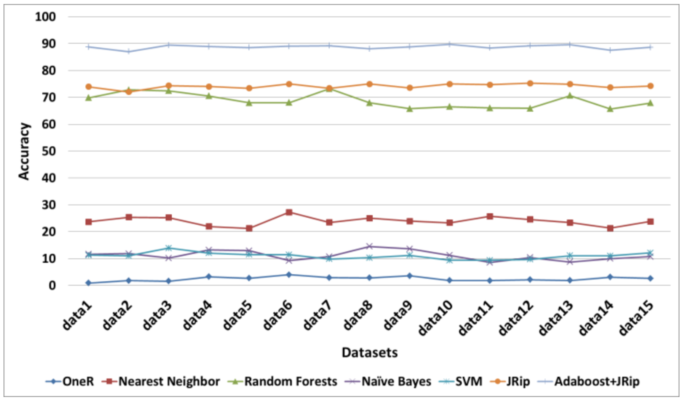

Fig. II. Multiclass Accuracy over Fifteen Datasets

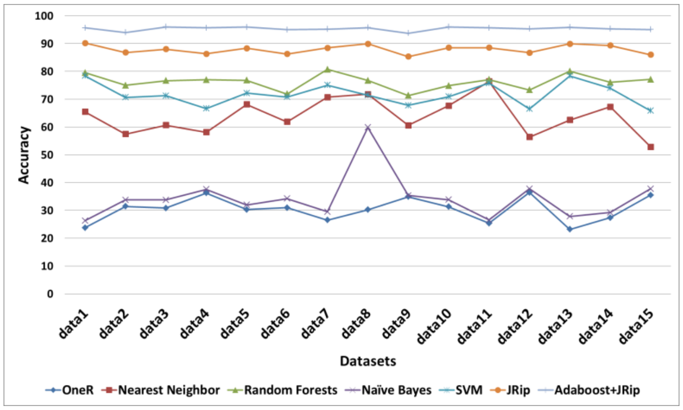

Fig. III. Three-class accuracy over Fifteen Datasets

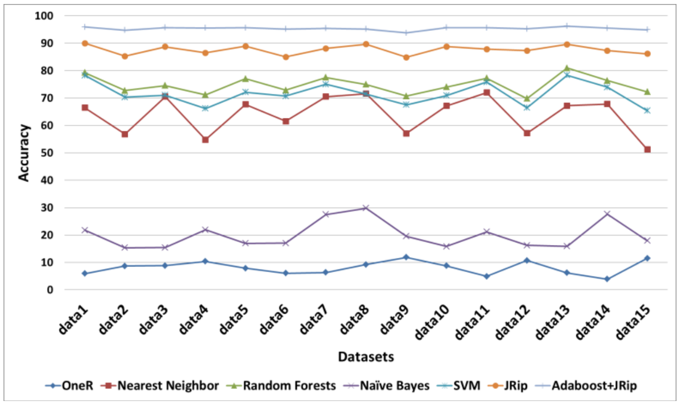

Fig. IV. Binary classification accuracy over Fifteen Datasets

Figure VI shows a similar set of results for averaged recall. As recall reflects true positive rate, this evaluation identifies the learning methods that detected cyber-attacks most successfully. Interestingly, a slightly different set of learners surface as high performers for this metric. For example, OneR and Naïve Bayes, two of the simplest methods, score very high (1.0 and 0.961, respectively) in terms of averaged recall whereas Random Forests performs significantly worse. JRipper and Adaboost+JRipper are consistently strong with recall values in the 08 to 0.9 range. The high recall values coupled with the low precision values for some learners indicate that learner's bias towards the positive (attack) class. That is, simple learners such as OneR and Naïve Bayes may correctly classify malicious power system disturbances, but at the cost of a disproportionate amount of false positive values. In a practical setting, the value that such a learner would bring to a decision would be low since its classification would not be reliable.

The F-measure, whose averaged values for all data sets are shown in Figure VII, intrinsically describes classification performance in terms of both precision and recall. As expected, those learners that performed well in terms of both precision and recall have the highest F-measure score, with JRipper+Adaboost having the highest overall value at 0.955 for the three-class classification scheme. Based on these results, the Adaboost+JRipper algorithm using a three-class classification scheme is the optimum approach to reliably classifying power system disturbances.

The variation in results based on classification scheme (multiclass, three-class, binary) is surprising. While the three-class produced the overall best performer, the results are inconclusive as to whether this is the optimum classification scheme across all learners. Different classification schemes coupled with different learners produce dramatically different results across all performance metrics. This implies an unexpected sensitivity to the classification scheme and suggests homogeneity in the data for all disturbance types. A future direction for this research is to explore classification schemes and learner configuration to more thoroughly address this issue, including the possibility of staging learners for optimum classification performance. Despite the inconsistencies in results across classification schemes, the JRipper+Adaboost algorithm as the optimum learner is still a valid result as that approach consistently outperformed the other learners across all classification schemes.

We attribute the strong performance of the JRipper+Adaboost approach to its tree-based approach to rule generation coupled with the learning ensemble. However, it was surprising that Random Forests, an ensemble method leveraging decision trees, performed poorly in comparison. We attribute this difference to the way in which the training data is prepared for each learning approach. Random Forests do no pruning of their underlying decision trees, and draw their training data samples randomly, thus providing a very basic approach to building the decision trees and combining them in an ensemble. JRipper applies a pruning algorithm to the sampled training data that minimizes errors. In addition, the boosting creates an ensemble that is focused on previously misclassified data, another intrinsic attempt to minimize error. Given the small number of training data examples relative to the number of features being evaluated, methods that explicitly attempt to minimize classification error should be expected to perform better.

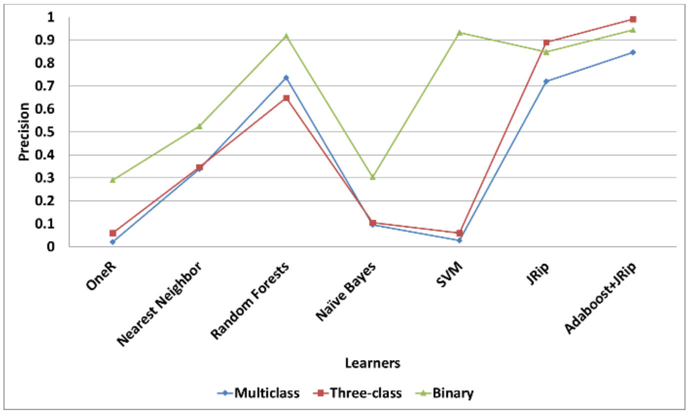

Fig. V. Average Precision over Classification Schemes

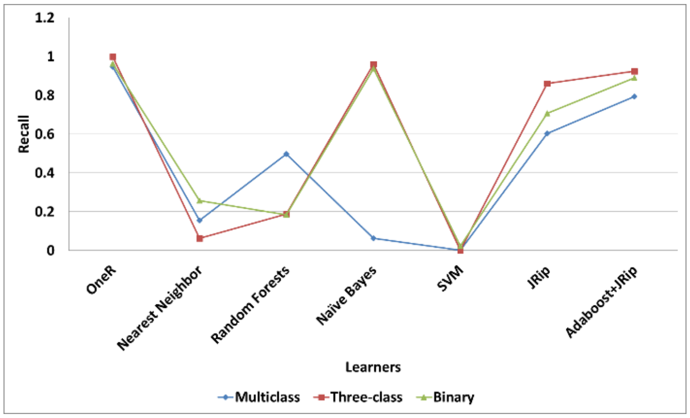

Fig. VI. Average Recall over Classification Schemes

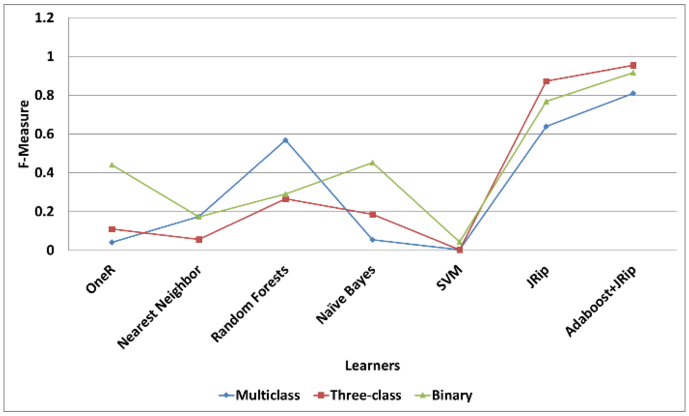

Fig. VII. Average F-Measure over Classification Schemes

C. Feature Analysis Discussion

In our framework there were 4 synchrophasors that measured 29 features each for a total of 116 PMU measurements. There are also three different log types: control panel logs, Snort logs and relay logs for each PMU for an additional 12 features and a total of 128 features. Table I shows the features extracted from each PMU and a short description for each. Note that numbers indicate a range of measurements.

TABLE I. FEATURE DESCRIPTIONS

Feature	Description
PA1:VH – PA3:VH	Phase A - C Voltage Phase Angle
PM1: V – PM3: V	Phase A - C Voltage Magnitude
PA4:IH – PA6:IH	Phase A - C Current Phase Angle
PM4: I – PM6: I	Phase A - C Current Magnitude
PA7:VH – PA9:VH	Pos. – Neg. – Zero Voltage Phase Angle
PM7: V – PM9: V	Pos. – Neg. – Zero Voltage Magnitude
PA10:VH - PA12:VH	Pos. – Neg. – Zero Current Phase Angle
PM10: V - PM12: V	Pos. – Neg. – Zero Current Magnitude
F	Frequency for relays
DF	Frequency Delta (dF/dt) for relays
PA:Z	Apparent Impedance seen by relays
PA:ZH	Apparent Impedance Angle seen by relays
S	Status Flag for relays

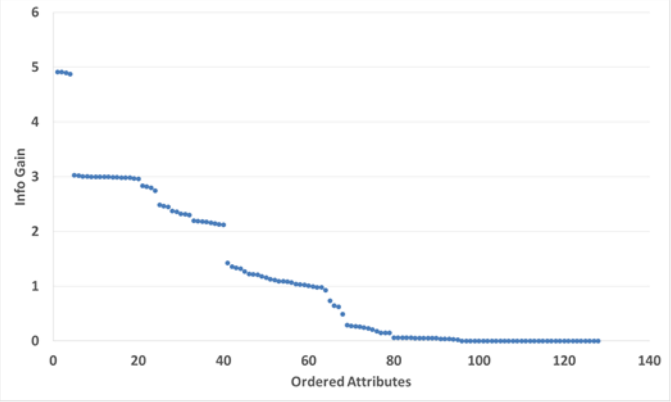

Fig. VIII. Information Gain Ranked Features

The information gain-ordered features are presented in Figure VIII. For our measurements, about 50% of the 128 features provide about 96% of the learning value. The four features with the highest information gain were Apparent Impedance measurements for each relay, having values in the 4.8 to 4.9 range. These were followed by Voltage Phase Angles, Current Phase Angles and Voltage and Current Magnitudes, which had values in the 3.0 range. Together, these account for the top 40 features. After these 36 additional features there is another comparatively large drop in information gain making up what appears to be three levels of information gain groupings.

We repeated the experiment using the JRipper algorithm and evaluated its classification performance using both the grouping of only the four best features and the grouping of top 40 features. Using only the top four features as training data yielded poor results, but using the top 40 features for training data resulted in the same classification performance for the as when using all of the available features. This identifies an opportunity for dimensionality reduction, but more importantly it reinforces the need for a algorithmic decision support component to power system disturbance classification. The simultaneous evaluation of the four most significant metrics (which in itself would be challenging for a human) is insufficient for reliable classification. It requires the simultaneous evaluation of dozens of power system metrics to detect power system disturbances for cyber-attack detection – a feat that is intractable for a human to perform.

D. Operational Viability Discussion

The classification approach to machine learning is still not widely used in industry as an intrusion detection system, mainly due to a poor understanding of the training data requirements that are necessary to construct a reliable learner. As the results indicate, a power system disturbance detector based that uses event classification to provide decision support to its operators would be reliable and effective in determining the nature of a disturbance and an appropriate associated course of action. However, an operational deployment of a classification system would also require the site-specific acquisition and maintenance of disturbance training data, since the classification models are not generally applicable, as rules from signature-based systems are. Both attack and normal operations data must be acquired in-situ, from the system that will be monitored, and then must be appropriately tuned to minimize false positives. The technical issue of the need for labeled training data could be abated by exploring alternative approaches that minimize or eliminate the amount of labeled data needed (e.g., unsupervised and semi-supervised methods) yet retain the classification performance. However, the operational processes for acquiring and maintaining in-situ training data and the support processes for learning system feedback and retraining criteria do not currently exist, and so are a both a barrier to operational viability and an opportunity for future research.

V. CONCLUSION

We have established initial benchmarks for applying machine learning approaches to power system disturbance classification on a smart power grid framework. Using the JRipper+Adaboost method over a three-class (Attack, Natural Disturbance, and No Event) classification scheme, we were able to reliably classify power system disturbances with low false positive rates. Therefore, based on the results of applying learning methods to this power system data, we conclude that machine learning is a viable approach to providing reliable decision support to power system operators on whether the system is under attack. Despite these results, we recognize that further work is required to make learning-based systems deployable in an operation environment. From a learning perspective, these results need to be validated on a broader set of power system data and with a wider variety of learning approaches, classification schemes, and amounts of labeled data. In addition, more work is required in understanding the concept of operations associated with these systems, such as methods for determining training and retraining needs, approaches for generating and managing labeled data, in-situ evaluation tools to select the optimum learner and tune the performance of that learner in that specific deployed environment. However, this work serves as an initial set of evidence for the application of machine learning in this domain and motivation for further research.

VI. ACKNOWLEDGEMENT

Research sponsored by the Laboratory Directed Research and Development Program of Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37831-6285; managed by UT Battelle, LLC, for the U.S. Department of Energy under contract DE-AC05-00OR2225. This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 for the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

VII. References

[1] N. Falliere, L. O'Murchu and E. Chien, "W32.Stuxnet Dossier", Online: http://goo.gl/kzVOSC, Nov. 2010.

[2] D. E. Bakken, A. Bose, C. H. Hauser, E. O. Schweitzer III, D. E. Whitehead, and G. C. Zweigle, "Smart Generation and Transmission with Coherent, Real-Time Data," Technical Report TR-GS-015. August, 2010.

[3] R. Moxley and D. Dolezilek, "Case studies: Synchophasors for wide-area monitoring, protection, and control," Proc. 2nd IEEE PES International Conf. and Exhibition on Innovative Smart Grid Technologies (ISGT Europe), pp.1-7, 5-7, Dec. 2011.

[4] S. Horowitz, D. Novosel, V. Madani, and M. Adamiak, "System-Wide Protection", IEEE Power & Energy Magazine, vol. 6, no. 6, pp. 34 – 42, Sep. 2008.

[5] SEL; "Mitigating the Aurora Vulnerability with Existing Technology." Online: http://goo.gl/9hkAJb, Oct. 2009

[6] M. Masera and I. Nai Fovino, "Effects of intentional threats to power substation control systems", Int. J. Critical Infrastructures, vol. 4, no. 1/2, pp.129–143, 2008.

[7] T. Morris, S. Pan, J. Lewis, J. Moorhead, B. Reaves, N. Younan, R. King, M. Freund, and V. Madani, "Cybersecurity Testing of Substation Phasor Measurement Units and Phasor Data Concentrators," (CSIIRW '11), pp. 12-14, Oct. 2011.

[8] Chee-Wooi Ten; Junho Hong; Chen-Ching Liu, "Anomaly Detection for Cybersecurity of the Substations," Smart Grid, IEEE Transactions on , vol.2, no.4, pp.865,873, Dec. 2011

[9] Y. Chen and B. Lou, "S2a: Secure smart household appliances," in Proc. 2nd ACM Conf. Data Application Security Privacy, San Antonio, TX, USA, pp. 217-228, Feb. 2012.

[10] Mitchell, R.; Ing-Ray Chen, "Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications," Smart Grid, IEEE Transactions, vol.4, no.3, pp.1254, 1263, Sept. 2013.

[11] Yang, Y.; McLaughlin, K.; Sezer, S.; Littler, T.; Pranggono, B.; Brogan, P.; Wang, H.F., "Intrusion Detection System for network security in synchrophasor systems," IET International Conf. , vol., no., pp.246,252, 27-29, April, 2013.

[12] Y. Zhang; L. Wang; W. Sun; Green, R.C.; Alam, M., "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids," Smart Grid, IEEE Transactions, vol.2, no.4, pp.796,808, Dec. 2011.

[13] Hadeli, H.; Schierholz, R.; Braendle, M.; Tuduce, C., "Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration," Emerging Technologies & Factory Automation, ETFA, vol., no., pp.1, 8, 22-25, Sept. 2009.

[14] Berthier, R.; Sanders, W.H., "Specification-Based Intrusion Detection for Advanced Metering Infrastructures," Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on , vol., no., pp.184,193, 12-14 Dec. 2011.

[15] Valenzuela, J.; Wang, J.; Bissinger, N., "Real-Time Intrusion Detection in Power System Operations," Power Systems, IEEE Transactions on , vol.28, no.2, pp.1052,1062, May, 2013.

[16] M. Talebi, J. Wang, Z. Qu, "Secure Power Systems Against Malicious Cyber-Physical Data Attacks: Protection and Identification," World Academy of Science, Engineering and Technology, vol. 66, 2012.

[17] Zonouz, S.; Rogers, K.M.; Berthier, R.; Bobba, R.B.; Sanders, W.H.; Overbye, T.J., "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures," Smart Grid, IEEE Transactions on , vol.3, no.4, pp.1790,1799, Dec. 2012.

[18] G. Weimann, "Cyberterrorism: How real is the threat?" United States Institute of Peace, Washington, United States, 2004.

[19] P. Anderson, "Analysis of Faulted Power Systems," IEEE Inc., 1995. Doug Westlund, "the Electric Grid Cyber-attack Surface Is Larger Than The Grid Itself", Online: http://goo.gl/MygNRz, 1995

[20] Doug Westlund, "The Electric Grid Cyber-attack Surface Is Larger Than The Grid Itself", Online: http://goo.gl/WGPzqW, last access 2014.

[21] Y. Aillerie; S. Kayal; J. Mennella; R. Samani; S. Sauty; L. Schmitt, "Smart Grid Deployment Requires A New End-to-end Security Approach", Online: http://goo.gl/UvliR4, June, 2013.

[22] M. Hall, E. Frank, Et Al., "The Weka Data Mining Software: An Update," Sigkdd Explorations, Vol. 11, No. 1, 2009.

[23] L. Breiman, "Random Forests," Machine Learning Vol. 45, No. 1, Pp. 5-32, 2001.

[24] R.C. Holte, "Very Simple Classification Rules Perform Well On Most Commonly Used Datasets," Machine Learning, Vol. 11, No. 1, Pp. 63-90, 1993.

[25] T. Bayes. Phil. "Trans. Of The Royal Soc. Of London", 1763.

[26] P. Langley, W. Iba, And K. Thompson, "An Analysis Of Bayesian Classifiers," Aaai, Vol. 90, 1992.

[27] B. Martin, "Instance-based Learning: Nearest Neighbor With Generalization" University Of Waikato, 1995.

[28] J. Platt, "Sequential Minimal Optimization: A Fast Algorithm for Training Support Vector Machines," Advances in Kernel Methods – Support Vector Learning", 1998.

[29] C. Cortes And V. Vapnik, "Support-Vector Networks," Machine Learning", Vol. 20, No. 3, Pp. 273–297, 1995.

[30] Fürnkranz J., Widmer G., "Incremental Reduced Error Pruning, Proc. 11th Intl. Conf. On Machine Learning", Ml-94, Pp. 70-77, Rutgers University, Nj, 1994.

[31] William W. Cohen, "Fast Effective Rule Induction", Proceedings of the Twelfth International Conf. On Machine Learning", Lake Tahoe, California, 1995.

[32] W. Hu, Y. Liao, and V. Vemuri. "Robust Support Vector Machines for Anomaly Detection in Computer Security". Proc. International Conf. On Machine Learning And Applications, Pages 23–24, 2003.

[33] C. Sinclair, L. Pierce, and S. Matzner. An Application of Machine Learning To Network Intrusion Detection. Proc. Computer Security Applications Conf., Page 371, 1999.

[34] R. Perdisci, G. Gu, and W. Lee., "Using an Ensemble of One-class SVM Classifiers to Harden Payload-based Anomaly Detection Systems", Proc. International Conf. on Data Mining, pages 488–498, 2006.

[35] Freund, Yoav, and Robert E. Schapire. "A decision-theoretic generalization of on-line learning and an application to boosting." Journal of computer and system sciences 55.1, 119-139. 1997.

[36] Justin Beaver, Raymond Borges, Mark Buckner, "An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications", 13th International Conf. on Machine Learning and Applications, 2013.

[37] Mississippi State University Critical Infrastructure Protection Center, "Industrial Control System Cyber Attack Data Set", Online: http://www.ece.msstate.edu/wiki/index.php/ICS_Attack_Dataset, Apr. 2014.