THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 2 Article 5

6-30-2017

A Power Grid Incident Identification Based on Physically Derived Cyber-Event Detection

Travis Atkison
University of Alabama, atkison@cs.ua.edu

Nathan Wallace
Cybirical, nwallace@cybirical.com

Recommended Citation

Atkison, Travis and Wallace, Nathan (2017) "A Power Grid Incident Identification Based on Physically Derived Cyber-Event Detection," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 2 , Article 5.
DOI: https://doi.org/10.15394/jdfsl.2017.1480
Available at: https://commons.erau.edu/jdfsl/vol12/iss2/5

A POWER GRID INCIDENT IDENTIFICATION BASED ON PHYSICALLY DERIVED CYBER-EVENT DETECTION

Travis Atkison[1], Nathan Wallace[2]
University of Alabama[1]
Tuscaloosa, AL, USA
atkison@cs.ua.edu (Corresponding Author)

Cybirical[2]
Mandeville, LA, USA
nwallace@cybirical.com

ABSTRACT

This article proposes a cyber-event detection framework to aid in incident identification and digital forensics cases aimed at investigating cyber crime committed against the critical infrastructure power grid. However, unlike other similar investigative techniques, the proposed approach examines only the physical information to derive a cyber conclusion. The developed framework extracts information from the physical parameters stored in historical databases of SCADA systems. The framework uses a pseudo-trusted model derived from randomly selected power system observations found in the historical databases. Afterwards, a technique known as Bayesian Model Averaging is used to average the models and create a more trusted model. Results indicate a successful classification of on average 89% for the simulated cyber events of varying magnitudes.

Keywords: event detection, infrastructure protection, industrial control system, cyber security

1. INTRODUCTION

Industrial Control Systems (ICSs) can be found across many industries ranging from transportation to utilities (Macaulay, Tyson (2012)). An ICS is comprised of multiple controllers, each functioning as logic engines using conditional processing. One of the most prevalent ICSs is the critical infrastructure power grid. This meshed network of geographically distributed control systems (DCSs) has recently seen an influx of solid-state devices with Internet/intranet networking capabilities. Benefits of this influx include the command and control ability granted to the governing ICS. This governing ICS contains the supervisory control and data acquisition (SCADA) system. However, with this influx of smart network capable devices, the potential for various cyber threats arises (Miller and Rowe (2012)). Several works have been published on the difficulties and possible solutions associated with the live detection of cyber-incidents targeting the critical infrastructure power grid (Lo, Zeng, Marchand, and Pinkerton (1992); Nian-de, Shi-ying, and Er-keng (1982); Gu, Liu, Wang, Guan, and Xu (2013); L. Liu, Esmalifalak, and Han (2013); Yano, de Abreu, Gustavsson, and Åhlfeldt (2015)).

The solutions provided for live detection of cyber-incidents may work in theory and in practice for certain circumstances; however, it is not feasible for these methods to be installed across all utilities and co-ops at once. The resources required for such installations decrease the probability that such innovative methods will be implemented in the near future. However, in the mean time it is still desired, for the systems lacking extensive live detection capabilities, to be able to identify if and when a cyber-incident occurred. Furthermore, the live detection of data-injection attacks detects these attacks via bad data filters in the state estimation calculation. These solutions do not address possible post measurement attacks that seek to compromise the historical databases of SCADA systems. Such databases provide extensive operational information including purchasing, selling, billing, and other business intelligence metrics.

This paper proposes an incident response identification framework capable of detecting cyber-incidents targeting the historical databases of the power grid. The proposed approach seeks to identify attacks against power system applications by utilizing physical data stored in the historical databases of SCADA systems. The approach uses a "pseudo-trusted" model derived from a set of power system observations located in the database to investigate a region of the database that is believed to contain an event. Principal Component Analysis (PCA) is used to represent the pseudo-trusted observations in a new space where a classification feature is extracted. Multiple models are averaged together using a technique known as Bayesian Model Averaging to create a "trusted" model. Using the classification feature, each instance in the suspected region is tested and classified accordingly.

This article is organized into the following sections. First, the background in Section 2 provides information describing the SCADA infrastructure of power systems including an examination of the amount of information that is provided by the smart grid. Section 3 explains the 14-Bus power system used during the testing of the developed approach. The attack model or cyber-incident model is described in Section 4. The approach is outlined in Section 5 followed by a section outlining how the approach is evaluated. Section 6 provides the evalutation approach overview. The next section, Section 7, provides details on the experimental setup and results of the developed approach followed by conclusion.

2. BACKGROUND

The power grid, like other industrial control system applications, is becoming more and more governed by a cyber infrastructure. Cyber attacks that take advantage of the interconnected nature of these systems are on the rise. Figure 1 shows a graphic representing the typical communication infrastructure used in a SCADA environment. These environments are distributed across large geographic distances and offer several entry points an attacker may exploit to gain access to the SCADA network. Every node and every link of the communication infrastructure, theoretically, is an entry point. Here, a cyber infrastructure is used to control a physical application. For instance, in the case of the critical infrastructure power grid, packets traverse the cyber infrastructure to either monitor or control the generation, transmission, or distribution of power to paying customers. Such systems are called cyber-physical systems (CPS) and can range from an oil refinery to a nuclear power plant.

The energy management system (EMS) manages the generation of electrical power while efficiently delivering that power to customers. This management is made possible via the commands and measurements sent via the infrastructure outlined in Figure 1. Once new measurements are received by the infrastructure, the SCADA system performs a state estimation calculation to determine the best representation of the system and filters out any bad data that may be the result of noise or failing equipment. Afterwards, the derived state of the system along with a corresponding timestamp is stored in the historical database known as The Historian. Information is retrieved from these databases for the purposes of billing, purchasing, and other business

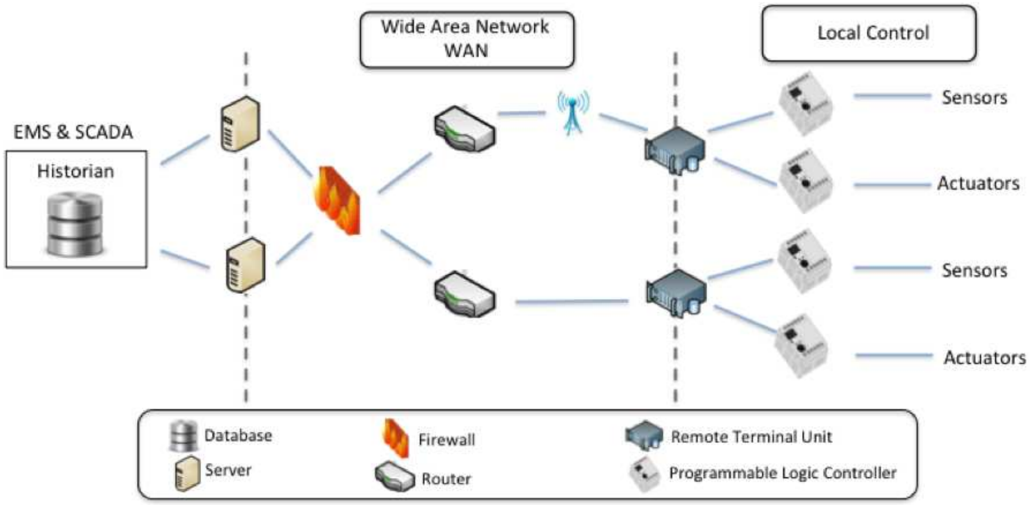

Figure 1. SCADA Communication Infrastructure for Distributed Control System

related intelligence metrics.

Traditional approaches to intrusion detection in these systems are based on bad data detection via the state estimation calculation. Some of these techniques and statistical measures for securing the power grid focus on examining reported state parameters and the resulting state estimation. Such techniques include the bad data detection schemes presented in (Lo et al. (1992); Nian-de et al. (1982); Gu et al. (2013); L. Liu et al. (2013)) and analysis of variance techniques as those presented in (Wehenkel (1998)). These approaches examine reported state parameters on an instance by instance basis and utilize circuit theory equations for the detection of anomalies in the resulting power system state estimation calculation. Data anomalies are then labeled as bad data resulting from measurement errors or faulty equipment.

Early implementation knowledge discovery approaches to bad data detection include the works of (Abbasy and El-Hassawy (1996); Shyh-Jier and Jeu-Min (2002); Teeuwsen and Erlich (2006); Huang, Lee, Shih, and Wang (2010); Gastoni, Granelli, and Montagna (2003)), wherein neurons are created that use patterns formulated based on historical or training datasets. Artificial intelligence is used in some of these approaches; however, these approaches do not utilize historical state parameters to reach conclusions, rather these techniques use neurons for faster convergence of the state estimation process. Bad data detection in power systems can be accomplished alongside the state estimation process. Throughout most of the literature, the objective function to be minimized in the state estimation process is considered to be related to a Chi square distribution.

An extensive survey of data mining approaches for power system security was conducted in (Hatziargyriou, Papathanassiou, and Papadopoulos (1995); Mori (2006); Fozdar, Arora, and Gottipati (2007)) with a full text on the subject presented in (Wehenkel (1998)) and (Momoh and El-Hawary (2000)). Most of the classification approaches use decision trees. However, the actual objects being analyzed range from transient stability to steady state power flows. Though not specific to the context of intrusion detection, the works of (Van Cutsem, Wehenkel, Pavella, Heilbronn, and Goubin (1993); Hatziargyriou, Contaxis, and Sideris (1994); Yang and Hsu (1994); Hatziargyriou et al. (1995)) demonstrate successful implementations of machine learning algorithms for power system security focusing on control reliability. Using decision trees, actual (Yang and Hsu (1994); C. Liu, Rather, Chen, and

Bak (2013)) and modeled (Hatziargyriou et al. (1994)), power system data is used to build models for the purpose of establishing preventive measures for stabilization in instances of required contingencies. In (Yang and Hsu (1994)), decision trees are also used for contingency analysis; however, the technique utilized is the Iterative Dichotomizer 3 (ID3) process and is based on the entropy of the dataset being analyzed. This ID3 algorithm is similar to the one utilized for power flow contingency analysis in (Yang and Hsu (1994)).

2.1 Power Grid Data

The growing source of data is a result of two relatively new intelligent electronic devices; the Phasor Measurement Unit (PMU) and the smart meter. The smart meter is the base element of the advanced metering infrastructure (AMI). This is in part a result of the establishment of the Smart Grid Investment Grant (SGIG) program by the Energy Independence and Security Act of 2007 (*Energy Independence and Security Act of 2007.* (2007)), Section 1306, and amended under the American Recovery and Reinvestment Act of 2009 (*The American Recovery and Reinvestment Act of 2009* (2009)). In July of 2012, the Department of Energy (DOE) published a progress report of the SGIG program stating that PMUs offer the essential wide-area visibility needed in the power grid due to its sampling rate of 30 to 120 times per second. The report then goes on to state that there are currently over 950 networked PMUs installed in North America funded by the SGIG program. The SGIG AMI projects support the installation of smart meters capable of transmitting data at 15-, 30-, or 60- minute intervals for customer billing information, interval load data, system voltage levels, and power quality. There are currently a total of 65 SGIG AMI projects, with an end goal of installing a total of 15.5 million smart meters (U.S. Department of Energy (2012)). As of mid 2014, the total number of AMI meter installations reported to the *Smart-Grid Integrated Project Reporting Information System* (SIPRIS) (U.S. Department of Energy (2014b)) was 16.2 million, well past the end goal (U.S. Department of Energy (2014a)).

As of 2015 there were an estimated 65 million smart meters installed nationwide. The RF meshed AMI network is operated predominately on the unlicensed Industrial, Scientific, and Medical (ISM) band between 902 to 928 MHz and is defined in Part 15 of the FCC regulations. A proprietary protocol that is optimized for AMI meshed network communication is described in (Geelen, van Kempen, van Hoogstraten, and Liotta (2012)). When in initiation mode, each packet is 32 bytes in length with a header of 15 bytes that is capable of containing the packet's route. Metering nodes are capable of caching the previously established packet routes for future communication. The security of packet transmission can be based on key pairs (Lichtensteiger, Bjelajac, Mu andller, and Wietfeld (2010)). However, this protocol and others have been found to contain vulnerabilities as demonstrated by Brinkhaus et al. (Brinkhaus and Carluccio (2011)).

At the distribution level, the electrical loads are determined by the power consumption of the customers. This example of interdependence, amongst others, allows for a unique opportunity for the development of an analytical framework that, in the event of a cyber incident, will detect a certain number of inconsistencies in the reported power system state variables. Database and historical data can be analyzed for its trending information and will contain information that can be used to detect high-level periodic malware similar to the Stuxnet worm.

3. POWER SYSTEM MODEL

The example power system utilized is the IEEE 14-bus standard test case, operating at 135 kV with a base power of 100 MVA. This particular system has been used extensively in the literature (Yuma and Kusakana (2012); Moghbel, Mokui, Masoum, and Mohseni (2012); Fitiwi and Rao (2009); Hashim, Hamzah, Latip, and Sallehhudin (2012)) for the purposes of simula-

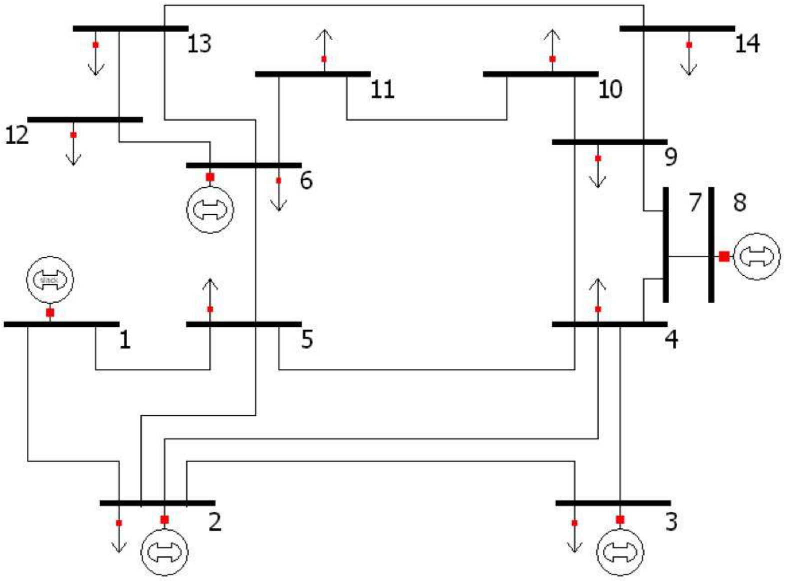

Figure 2. IEEE 14-Bus Power System

tion and development of power control applications. The system, shown in Figure 2, is comprised of 11 load busses and 2 generation busses. The generation busses are located on Bus 1 and 2 while busses 3, 6, and 8 supply a purely reactive power. The developed approach for the detection of database attacks is based on a set of models to simulate power system dynamics and to produce a set of possible state estimation attacks. The attack models include the changing of an observed power system instance in a manner that targets power system state variables. It is considered, as described in Section 4, that this change can take on many forms.

3.1 Modeling Power Systems

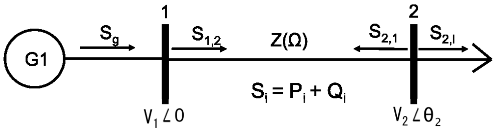

Figure 3. Power System Notation

The following describes the simulation approach taken to best recreate the physical parameters associated with the critical infrastructure power grid. In an attempt to mirror live power systems for the development process, power flow simulations include such factors as line impedances along with shunt capacitance for transmission lines greater than 50 miles. This approach is often utilized in both academia and industry and is considered the standard approach for power flow studies (Glover (2012)). An illustration of a power system model is shown in Figure 3, where `G1` is a generator (load), V_i is the voltage at bus i, and $Z(\Omega)$ is the impedance. The apparent power $S_{i,j}$ is made up of the real and reactive powers $P_{i,j}$ and $Q_{i,j}$, respectively.

4. CYBER-INCIDENT MODEL

The cyber-incident model seeks to recreate two possible power system cyber attacks. The first includes a data injection attack and is when an individual injects falsified measurements into the communication infrastructure of the SCADA system. The detectability of such data injection attacks depends on the approach taken by the bad data detection filters performed during the state estimation process. This type of attack involves spoofing the identity of the source so the destination believes the information is coming from the trusted source. These types of attacks can have a devastating impact on the system if the received state measurement is used to make control decisions. In the event the data injection attack goes unnoticed, the malicious reading will still be stored in the historical database of the SCADA system.

The second type of attack is considered a post–state estimation attack and involves the direct manipulation of state variable values in the historical SCADA databases. Not only are the measured state variables used for the control and monitoring of the power system, they are also used for business intelligence. Such business intelligence includes the selling and purchasing of power to and from neighboring utilities and more recently to and from residential and commercial customers. The purchasing of power from residential and commercial customers is the product of the micro-grid initiatives. These micro-grids allow the standard consumers to sell power they have generated back to the utility providers. Motivated by profits, any one of these actors may be motivated to change values in the historical databases to make it appear as though they have purchased less or sold more power.

The cyber-incident model developed by this paper seeks to recreate these potential attacks by manipulating different state parameters at varying factors. Each attack type is mathematically based on the Hadamard product, $\overrightarrow{X_i}' = \overrightarrow{X_i} \circ I'_{System}$. For instance, a single variate attack type, which is a random instance, $\overrightarrow{X_r}$, from data matrix $\mathbf{X}$, was selected according to a random index i such that $\overrightarrow{X_r}|_{r=i}$ and $\{i \, \epsilon \, \mathbb{Z}| \leq M\}$ where $M\text{x}n$ is the size of $\mathbf{X}$. Next, an initialization vector, $I_{System} = [a_1 \cdots a_n] = [1 \cdots 1]$, of all ones and of length n was created. To determine which variable will simulate the attack, a random index l is selected such that $\{l \, \epsilon \, \mathbb{Z}|1 \leq l < 15\}$, where $1 \leq l < 15$ is the voltage state variables attacked. The element of I_{System} defined by random index l is then changed to the factor f to simulate the attack. For this assessment, a total of 5 different attack factors are simulated and include $f = 0.99, 0.95, 0.90, 0.85,$ and 0. Each attack factor represents a possible alteration on that state variable as defined by the Hadamand product.

5. APPROACH

The fostered approach is designed to aid in an incident response investigation with the developed method determining attack occurrences. This approach uses power system state variables stored in a SCADA Historian server to identify when a system intrusion has occurred. Iterating through each suspected power system observation, the approach then compares the observation to a pseudo-trusted model. The pseudo-trusted model is derived by randomly selecting power system observations from the entire database. These random instances may or may not include observations between the suspecting region. Once determined, a dimensional transformation technique known as principal component analysis (PCA) is used to transform the power system data to a reduced dimensional space. From here a distance metric is used as a detection feature and is based on Hotelling's T^2 value associated with each power system observation. When a suspect instance has been labeled as containing a cyber-incident, the instance can be set aside for further investigation.

5.1 Principal Component Analysis

PCA serves in the creation of the pseudo-trusted model by converting each power system instance, including suspect instances, into a new dimensional space for comparison. PCA is a quantitative process for achieving a system simplification by converting each multivariate observation into a lower dimensional space. This simplification is made possible through a transformation where all basis vectors are orthogonal. Each orthogonal vector is referred to as a principal component (PC) (Cios, Pedrycz, Swiniarski, and Kurgan (2010)). PCA is based on the statistics of a training set to linearly transform the set in such a way that the new primary basis are independent of each other. PCA finds a linear transformation such that

$$\mathbf{Y} = \mathbf{XW} \tag{1}$$

where $\mathbf{X}$ and $\mathbf{Y}$ are mxn matrices related by a transformation $\mathbf{W}$ of size pxp. Based on Equation (1), the following variables can be defined: $\mathbf{w_i}$ are the rows of $\mathbf{W}$, $\mathbf{x_i}$ are the columns of $\mathbf{X}$, and $\mathbf{y_i}$ are the columns of $\mathbf{Y}$. The row vectors of $\mathbf{W}$ $\{w_1, ..., w_m\}$ are called the principal components of $\mathbf{X}$.

Before PCA can be applied to a data set, it is customary to first perform sanitization on the data. This sanitization guarantees there is no unintended biasing of the new components. After sanitizing, the normalized covariance, $\mathbf{S_X}$, was determined using the unbiased estimator for normalization.

$$\mathbf{S_X} = \frac{1}{n-1}\mathbf{X}\mathbf{X}^T \tag{2}$$

This produced a covariance matrix with dimensions mxm with the diagonal terms representing the variances and off-diagonal terms representing the covariances of data matrix $\mathbf{X}$. The closer the off-diagonal terms are to zero the closer the variables, represented by the indices of $\mathbf{S_X}$, are to being completely uncorrelated. Conversely, the higher these off-diagonal terms are the more correlated the two variables are. Also the higher the off-diagonal terms are the higher the redundancy is in the data matrix $\mathbf{X}$.

The linear transformation produced by PCA selects a transformation $\mathbf{W}$ such that the principal components or basis vectors w_i produced are completely orthonormal. Orthonormality is ensured due to the fact that the dot product of each basis vector with another produces the Kronecker delta function, $w_i \cdot w_j = \delta_{ij}$. In addition to being orthonormal, the basis vectors are ordered based on the amount of variance that is being accounted for by that basis vector or principal component. This corresponds to the fact that PCA will produce a transformation matrix $\mathbf{W}$ such that the variance of data matrix $\mathbf{X}$ is mostly accounted for by principal component w_1. The lower the diagonal terms of the covariance matrix are the lower the redundancy is in the data. Therefore, the solution to PCA seeks a covariance matrix $\mathbf{S_Y}$ such that the off-diagonal terms are zero where,

$$\mathbf{S_Y} = \frac{1}{n-1}\mathbf{Y}\mathbf{Y}^T \tag{3}$$

Plugging Eq. (1) into Eq. (3), we have

$$\mathbf{S_Y} = \frac{1}{n-1}\mathbf{W}(\mathbf{X}\mathbf{X}^T)\mathbf{W}^T \tag{4}$$

With this solution to PCA, it can be shown that the principal components of data matrix $\mathbf{X}$ are the eigenvectors of $\mathbf{X}\mathbf{X}^T$ or are the rows of $\mathbf{W}$. Also, the i^{th} diagonal term of $\mathbf{S_Y}$ is the variance of $\mathbf{X}$ projected onto the i^{th} principal component, $\mathbf{p_i}$.

5.1.1 Hotelling's $\mathbf{T^2}$

The Hotelling's T^2 value, Eq. (5), is an extension of the t-test, a test to determine the difference between means of two independent variables. This extension of the t-test allows for a statistical measure of the multivariate distance of each instance from the center of a data set. The result allows for the detection of instances that occur at far distances from the data center as defined by data matrix $\mathbf{X}$.

$$T^2 = n(\mathbf{X} - \mu)'\mathbf{S}^{-1}(\mathbf{X} - \mu) \tag{5}$$

The identification approach presented in this article is a probabilistic approach in describing how likely an instance is to occur. Instances that fit to the dynamics of the data matrix $\mathbf{X}$, or control set, have a high likelihood of occurring while instances that lie on the boundaries are less likely to occur.

It can also be shown that the Hotelling's T^2 value follows the $\mathcal{F}$ distribution as defined by Eq. (6) (Härdle and Simar (2012)),

$$T^2 \sim \frac{(n-1)p}{(n-p)}\mathcal{F}_{p,n-p}(x) \tag{6}$$

where p is the number of principal components retained and n is the number of instances in the sample space. The $\mathcal{F}$ cumulative probability distribution function returns the cumulative probability of obtaining a value x for given parameters p and n. By rearranging Eq. (6) we can calculate that the probability of observing at least T^2 is

$$P(\geq T^2) = 1 - F_{p,n-p}(z) \tag{7}$$

where,

$$z = T^2\frac{(n-p)}{p(n-1)}$$

This allows for a probabilistic metric to determine whether or not an instance is in-control. If the instance is in-control, then it follows the dynamics as defined by the data matrix **X**. A low probability for observing T^2, as defined by Eq. (7), corresponds to a high T^2 value. This means that the instance is far away from the multivariate center and therefore is least likely to occur. Conversely, a high probability corresponds to a low T^2 value and is therefore closer to the center of the data.

Any in-control instance can be considered an instance whose variables follow the dynamics of the system. These instances can be considered instances that would occur under normal operation. An out-of-control instance would be an instance whose dynamics do not fit uniformly in with the dynamics of the in-control instances. Out-of-control instances are not considered normal operation, and therefore, any operation that exists outside of normal operation can be classified as an out-of-control instance.

The Hotelling's T^2 value and the probabilistic metric aided in the classification of the instances into either an in-control set or an out-of-control set. An in-control instance would have a low T^2 value and high probability of occurring. While an out-of-control instance would have a low probability and a high T^2 value. This statistical metric classification of instances can be made such that instances that are not in-control are classified as a cyber-event.

Detection using the Hotelling's T^2 value is based on creating a quantile threshold. By transforming the trusted model into the new dimensional space, where redundancy is reduced, and plotting the Hotelling's T^2 value of each power system instance of the trusted model, a threshold value, T_{th}^2, can be created. By letting $T_{th} = Q_\alpha = inf\{q : P[T^2 < q] \geq \alpha\}$, where α is the quantile value, a maximum threshold is determined. If any newly observed power system instance's Hotelling's T^2 value is found to be greater than T_{th}^2, then it can be classified as an out-of-control instance. To limit the number of false positive classifications a quantile threshold value of $\alpha = 0.99$ was used for detection.

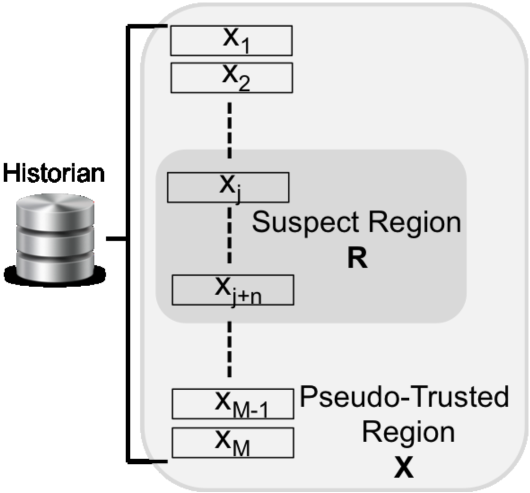

Figure 4. Experimental Setup

5.2 Implementation

The approach of this work involves first choosing a total of m random observations to develop a single pseudo-trusted model of size m. This is repeated a total of ten times. Looking at Figure 4, there are a total of M possible instances that can be used to construct the trusted models. PCA is then used to transform each model into the new dimensional space where the threshold value of each model is extracted and is based on the Hotelling's T^2 value described in Section 5.1.1. Once extracted for each model, the T^2 values are averaged together resulting in the threshold value, $\bar{T}_{th}$. Next the Hotelling's T^2 value of the i^{th} suspect power system observation, T_i', is determined and compared against the threshold value. If $T_i' > \bar{T}_{th}$, then the i^{th} observation is flagged as containing a possible event. This process is then repeated for each suspect observation x_i. The overall implementation algorithm is described in Algorithm 1 shown below. Here the threshold value T_{th} is determined for this model and is based on the 99% quantile Hotelling's T^2 value associated with the model. This is repeated a total of ten times with the resulting T_{th}^i averaged together to get $\bar{T}_{th}$.

Algorithm 1 Detection/Identification Approach

```
Input: Data Matrix X, Suspect Region R
Output: Malicious Instance $x_i$
for $r_i$ in R do
    for n=1 to 10 do
        I=rand(m,size(X))    ▷ m random indices
        $X' = X(I)$    ▷ Pseudo-Trusted Model
        $Y' = X'W$    ▷ Perform PCA
        $T_n^2 = T^2(Y')$
    end for
    $\bar{T}_{th}^2 = avg(T_1^2 \dots T_{10}^2)$
    if $T_{ri}^2 \geq \bar{T}_{th}^2$ then
        $r_i$ contains cyber-incident
    else
        No observed attack
    end if
end for
```

6. EVALUATING IDENTIFICATION APPROACH

		Prediction Class [P]		
		$\mathbf{c_1}$	$\mathbf{c_2}$	**total**
Actual Class[A]	$\mathbf{c_1}'$	True Negative	False Positive	C_1'
	$\mathbf{c_2}'$	False Negative	True Positive	C_2'
	total	C_1	C_2	

Figure 5. Classification Matrix

The following methods described are some of the most common evaluation methods for assessing the success of a classifier (Cios et al. (2010)). Figure 5 shows the classification matrix (contingency table) used to keep track of successes and failures for each attack type considered. In the case of this analysis, positive logic is used corresponding to the classification of instance **x** into class c_2, the malicious class. Using positive logic the following terms can be defined.

- *Sensitivity*- or recall is the measure of how often we find what we are looking for. It is the measure of how often we classify **x** into c_2.

$$Recall(R) = \text{TP Rate} = \frac{\text{TP}}{(\text{TP}+\text{FN})} \tag{8}$$

- *Precision*- used often in text analysis

$$Precision(P) = \frac{\text{TP}}{(\text{TP}+\text{FP})} \tag{9}$$

- *F-Measure*- harmonic mean of precision (P) and recall (R).

$$F = \frac{2*\text{P}*\text{R}}{(\text{P}+\text{R})} \tag{10}$$

7. EXPERIMENTAL SETUP AND RESULTS

The suspect region, **R**, is comprised of 1000 observations while the pseudo-trusted region, **X**, is comprised of a total of 90,000 power system observations. An attack is performed only on the voltage values of the power system topology. Simulation of the detection tool is performed for different attack factors f and includes $f = 0.99, 0.95, 0.90, 0.80,$ and 0. In addition to changing the attack factor, the training model size is changed in an effort to determine the optimal training size. The different sizes of the training models include $m = 100, 500, 1000, 2500,$ and 5000. In each case, a total of 100 power system observations are randomly selected from the region **R**. Next, a random voltage state variable is selected and multiplied by the attack factor f. This produces a suspect region **R** with a total of 100 malicious power system instances and 900 non-malicious instances for a total of 1000 observations. To test the developed approach, each instance in the suspect region **R** is tested according to the approach presented in Algorithm 1. For each simulation, the True Negative, False Negative,

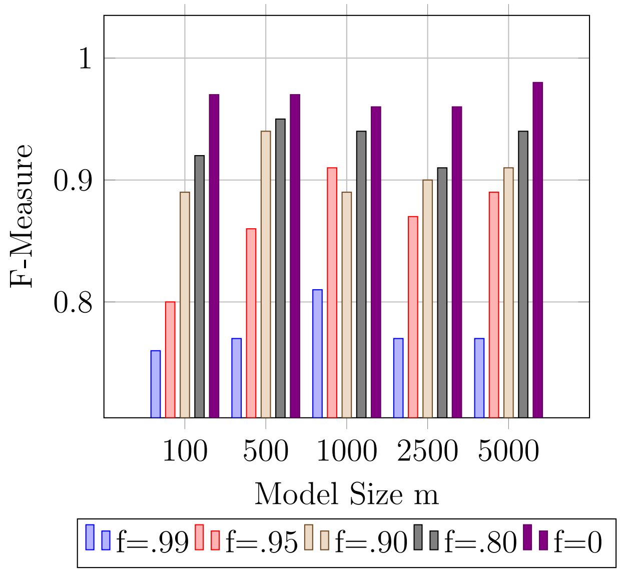

Figure 6. F-Measure of Detection Approach for Model Size M

False Positive, and True Positive counts are recorded. Afterwards, the F-Measure is calculated according to Eq. (10).

The results of the detection approach include the detection classification matrices outlined in Table 1 and the F-measure results shown in Figure 6. It was determined that the hardest attack factor to detect was one where the original value was multiplied by 0.99, $f = 0.99$. This attack factor produces a value that has been altered by only 1% of its original value. Nonetheless, the developed approach was able to return on average 68.2% true positive classification with a false positive classification of 4.1%. As expected, the greatest success for detection occurred when the attack factor was zero, $f = 0$. For this attack type, the average true positive classification was found to be 99% while the false positive was 3.8%.

8. CONCLUSION

Currently, little literature exists on evaluating the data integrity of historical SCADA databases after the power system state estimation calculations have been performed. These databases are used for the purposes of billing, purchasing, and other business related intelligence metrics. Given the value of the information held in these databases, it may be advantageous for malicious actors to alter the values stored within them. Motivation may include price manipulation in the energy markets or adjusting power consumption. This research suggests using the physical power system state variables stored within these databases to detect alterations of these values. Such alterations are the result of possible cyber-intrusions into the critical control local area network and therefore are labeled as a cyber-incident. Using the approach developed by this paper, results show that depending on the magnitude of the alteration it is possible to detect such system breaches.

A technique known as principal component analysis (PCA) is used to represent the power system state variables in a new space. Here, information is extracted allowing for the creation of a detection feature and is based on the distances between each observation plotted in the new space. The output of the framework reveals the target time of the attack. Because the attack could happen live with the database storing the injected values or after the fact, the framework does not distinguish between the two scenarios. Bayesian Model Averaging is used to average extracted features in an effort to decrease any negative biasing a malicious instance may have on the developed pseudo-trusted model. Results show the highest average classification accuracy for a model size of 1000 to be 89.2%. This includes the detection of an attack that changes a state variable by only 1%. For attacks that altered the historical value to zero, the framework was able to classify with an average accuracy of 99.9% true positive classification.

Table 1. Classification Matrix for Varying Model Size m

		Attack Factor f									
		0.99		0.95		0.90		0.85		0	
m	A\P	c_1	c_2	c_1	c_2	c_1	c_2	c_1	c_2	c_1	c_2
100	c_1’	**890**	10	**885**	15	**887**	13	**896**	4	**894**	6
	c_2’	33	**67**	23	**77**	9	**91**	12	**88**	1	**99**
500	c_1’	**895**	5	**893**	7	**893**	7	**896**	4	**893**	7
	c_2’	34	**66**	20	**80**	6	**94**	6	**94**	0	**100**
1000	c_1’	**894**	6	**894**	6	**888**	12	**890**	10	**892**	8
	c_2’	28	**72**	12	**88**	11	**89**	3	**97**	0	**100**
2500	c_1’	**890**	10	**892**	8	**892**	8	**890**	10	**893**	7
	c_2’	31	**69**	17	**83**	11	**89**	8	**92**	1	**99**
5000	c_1’	**894**	6	**894**	6	**895**	5	**894**	6	**895**	5
	c_2’	33	**67**	15	**85**	12	**88**	6	**94**	0	**100**

REFERENCES

Abbasy, N. H., & El-Hassawy, W. (1996). Power system state estimation: Ann application to bad data detection and identification. In *Proc. africon* (Vol. 2, p. 611-615).

The american recovery and reinvestment act of 2009. (2009). [Washington, D.C. : U.S. G.P.O.].

Brinkhaus, S., & Carluccio, D. (2011). Smart hacking for privacy. In *Proc. 28th chaos comm. congr.*

Cios, K., Pedrycz, W., Swiniarski, R., & Kurgan, L. (2010). *Data mining: a knowledge discovery approach.* New York London: Springer.

Energy independence and security act of 2007. (2007). [Washington, D.C. :U.S. G.P.O.: Supt. of Docs., U.S. G.P.O., distributor].

Fitiwi, D., & Rao, K. S. R. (2009, Januarary). Assessment of ann-based auto-reclosing scheme developed on single machine-infinite bus model with ieee 14-bus system model data. In *Proc. tencon.*

Fozdar, M., Arora, C., & Gottipati, V. (2007). Recent trends in intelligent techniques to power systems. In *Universities power engineering conference, 2007. upec 2007. 42nd international* (pp. 580–591).

Gastoni, S., Granelli, G., & Montagna, M. (2003). Multiple bad data processing by genetic algorithms. In *Power tech conference proceedings, 2003 ieee bologna* (Vol. 1, pp. 6–pp).

Geelen, D., van Kempen, G., van Hoogstraten, F., & Liotta, A. (2012, January). A wireless mesh communication protocol for smart-metering. In *Proc. icnc* (p. 343 -349).

Glover, J. (2012). *Power System Analysis and Design* (5th ed.). Stamford, CT: Cengage Learning.

Gu, Y., Liu, T., Wang, D., Guan, X., & Xu, Z. (2013). Bad data detection method for smart grids based on distributed state estimation. In *Proc. icc* (p. 4483-4487).

Härdle, W., & Simar, L. (2012). *Applied multivariate statistical analysis.* Heidelberg New York: Springer.

Hashim, N., Hamzah, N., Latip, M., & Sallehhudin, A. A. (2012, Feburary). Transient stability analysis of the ieee 14-bus test system using dynamic computation for power systems (dcps). In *Proc. isms* (p. 481-486).

Hatziargyriou, N., Contaxis, G., & Sideris, N. C. (1994). A decision tree method for on-line steady state security assessment. *IEEE Transactions on Power Systems*, *9*(2), 1052-1061.

Hatziargyriou, N., Papathanassiou, S., & Papadopoulos, M. (1995). Decision trees for fast security assessment of autonomous power systems with a large penetration from renewables. *IEEE Transactions on Energy Conversion*, *10*(2), 315-325.

Huang, C.-H., Lee, C.-H., Shih, K.-R., & Wang, Y.-J. (2010). Bad data analysis in power system measurement estimation using complex artificial neural network based on the extended complex kalman filter. *European Transactions on Electrical Power*, *20*(8), 1082–1100.

Lichtensteiger, B., Bjelajac, B., Mu andller, C., & Wietfeld, C. (2010, October). Rf mesh systems for smart metering: System architecture and performance. In *Proc. smartgridcomm* (p. 379 -384).

Liu, C., Rather, Z. H., Chen, Z., & Bak, C. L. (2013). An overview of decision tree applied to power systems. *International Journal of Smart Grid and Clean Energy*, *2*(3).

Liu, L., Esmalifalak, M., & Han, Z. (2013). Detection of false data injection in power grid exploiting low rank and sparsity. In *Proc. icc* (p. 4461-4465).

Lo, K., Zeng, P., Marchand, E., & Pinkerton, A. (1992). New bad-data detection and identification technique based on rotation of measurement order for sequential state estimation [for power systems]. *IEEE Proceedings of Generation, Transmission* *and Distribution*, *139*(5), 387-401.

Macaulay, Tyson. (2012). *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.* Boca Raton, FL: CRC Press.

Miller, B., & Rowe, D. (2012). A survey of SCADA and critical infrastructure incidents. In *Proc. of acm conference on research in information technology* (pp. 51–56).

Moghbel, M., Mokui, H., Masoum, M., & Mohseni, M. (2012, September). Reactive power control of dfig wind power system connected to ieee 14 bus distribution network. In *Proc. aupec* (p. 1-7).

Momoh, J., & El-Hawary, M. (2000). *Electric systems, dynamics, and stability with artificial intelligence applications.* New York, NY: M. Dekker.

Mori, H. (2006). State-of-the-art overview on data mining in power systems. In *Proc. psce* (p. 33-34).

Nian-de, X., Shi-ying, W., & Er-keng, Y. (1982). A new approach for detection and identification of multiple bad data in power system state estimation. *IEEE Transactions on Power Apparatus and Systems*, *101*(2), 454-462.

Shyh-Jier, H., & Jeu-Min, L. (2002). Artificial neural network enhanced by gap statistic algorithm applied for bad data detection of a power system. In *Proc. t&d-ap* (Vol. 2, p. 764-768).

Teeuwsen, S. P., & Erlich, I. (2006). Neural network based multi-dimensional feature forecasting for bad data detection and feature restoration in power systems. In *Proc. pes-gm* (p. 6).

U.S. Department of Energy. (2012, July). *The american recovery and reinvestment act of 2009 smart grid investment grant program progress report.*

U.S. Department of Energy. (2014a, June). *Advanced metering infrastructure and customer systems smart meters deployed.* Report.

U.S. Department of Energy. (2014b, June). *Smartgrid integrated project reporting information system.* (`www.sipris.energy.gov`)

Van Cutsem, T., Wehenkel, L., Pavella, M., Heilbronn, B., & Goubin, M. (1993). Decision tree approaches to voltage security assessment. *IEEE Proceedings of Generation, Transmission and Distribution*, *140*(3), 189-198.

Wehenkel, L. (1998). *Automatic learning techniques in power systems.* Boston, MA: Kluwer Academic.

Yang, C.-C., & Hsu, Y.-Y. (1994). Estimation of line flows and bus voltages using decision trees. *IEEE Transactions on Power Systems*, *9*(3), 1569-1574.

Yano, E. T., de Abreu, W., Gustavsson, P. M., & Åhlfeldt, R.-M. (2015). A framework to support the development of cyber resiliency with situational awareness capability. In *20th international command and control research and technology symposium, june 16-19, annapolis, maryland, usa.*

Yuma, G., & Kusakana, K. (2012, May). Damping of oscillations of the ieee 14 bus power system by svc with statcom. In *Proc. eeeic* (p. 502-507).