Sep 30th, 9:00 AM

A Clustering Approach to Industrial Network Intrusion Detection

Leary Tomlin Jr.
Mississippi State University, lt648@msstate.edu

Marsella R. Farnam
Mississippi State University, mrj1@msstate.edu

Shengyi Pan
Mississippi State University, sp821@msstate.edu

A Clustering Approach to Industrial Network Intrusion Detection

Leary Tomlin Jr.
Mississippi State University
479-2 Hardy Rd
Mississippi, MS
lt648@msstate.edu

Marsella R. Farnam
Mississippi State University
479-2 Hardy Rd
Mississippi, MS
mrj1@msstate.edu

Shengyi Pan
Mississippi State University
479-2 Hardy Rd
Mississippi, MS
sp821@msstate.edu

ABSTRACT

Industrial control system (ICS) networks and supervisory control and data acquisition (SCADA) system networks are less likely to be within a strict closed network environment, which increases the likelihood of cyber-attacks. Over the last decade, intrusion detection has become an additional security measure for ICS and SCADA system networks to help prevent and minimize loss that may be sustained from cyber-attacks. ICS and SCADA network communication is typically repetitive and deterministic, which allows normal activity to be more easily modeled on the behavior of system specific events. Given this deterministic behavior, an unsupervised anomaly-based intrusion detection system may provide increased performance over the more typical misuse detection method. We propose an unsupervised machine learning approach for the implementation of a network IDS in power system applications. The approach would supplement a more complex IDS by quantifying the degree by which an event is an attack, given network data states, to improve intrusion detection and minimize false alarm rates. The clustering approach contains four key processes: data preprocessing, unsupervised learning (cluster analysis), generating features from clusters, and classifying states using the Mamdani fuzzy inference system. Data sets from a simulated power distribution system are used to illustrate the impact of the proposed approach.

Keywords

cluster analysis, cluster tendency, feature selection, FIS, IDS, ICS, machine learning, SCADA, smart grid

1. INTRODUCTION

SCADA systems are industrial control systems (ICS) that manage the behavior of large distributed systems which exist in critical infrastructure sections [16]. SCADA systems rely upon confidentiality, integrity, and availability of data to ensure continuity of operations [16]. In the event of an cyber-attack, incidents such as blocked information flow, unauthorized changes to commands, inaccurate transfer of information to system operators, or endangerment of human life due to interference of safety system operations could occur [16]. In 2010, Stuxnet specifically attacked SCADA systems, resisted anti-virus detection, maintained stealth, and avoided detection all while utilizing multiple methods to infect systems by way of network shares and thumb drives [16].

The overall model for this work involves unsupervised learning through the use of different techniques to identify threats in an environment where the data is not labeled or classified. This task must be completed to ensure the systems operate as designed with no manipulation of functionality while also ensuring no disclosure of data to unauthorized individuals and continuous operation of data availability to those who are authorized [16].

As power systems increasingly depend on communication infrastructures to provide the wide-area monitoring and control, power systems are exposed to the threat of cyber-attacks. Cyber-attacks are another form of power system contingency. Attacks that target power systems can exploit vulnerabilities in control devices and communication links to corrupt control and measurement signals [10][13], and compromise monitoring algorithms [23]. Cyber-attacks that corrupt control and measurement signals can be disguised as power system disturbances or control actions. Situational awareness technologies are needed to distinguish between actual power system disturbances related to natural events, and cyber-attacks.

A single classifier which identifies all types of power system contingencies is needed as an input to automated event response algorithms such as autonomic management frameworks, system integrity protection schemes (SIPS) [18], and wide area protection systems (WAPS) [1]. Wide area measurement systems (WAMS) couple time synchronized voltage, current, and frequency measurements with high speed networks to allow improved power system situational awareness [9]. Compared to traditional SCADA systems that poll field sensors once per several seconds; synchrophasor systems allow measurement of up to 120 samples per second. However, using synchrophasor data alone is not enough to detect cyber-attacks. Such example can be a cyber-attack that mimics a real fault by first infecting false measurements then tripping the relay. The status of other power system components such as relays and breakers is also available as time-synchronized data via synchrophasor systems [2]. Combining synchrophasor data with other system logs such as relay status logs and network event monitor logs

DOI: 10.1145/1235

can extend the situational awareness capabilities provided by a synchrophasor system to detect cyber-attacks. But, this creates the challenge of how heterogeneous data sources can be merged to train and use such a classifier. This paper provides a clustering approach that leverages the data to discern its underlying structure and classify states as normal behavior or cyber-attacks.

In this work, a pattern for a scenario is presented as a sequence of system samples/states in temporal order. A system state in a common path is made up of multiple instantaneous readings from available sensors from the system. Attacks may originate from a compromised node in the control center, sending control commands or measurement packets covered by legitimate source IP addresses and legal packet formats. As such, it is assumed the masquerading packets cannot be detected by traditional network intrusion detection systems. Validation of the proposed algorithm is based on simulated data because actual synchrophasor data is not available for researchers due to the proprietary nature of data, confidentiality issues, and lack of proper sharing mechanism among researchers and institutes. Additionally, data sets captured from utilities contain a limited number of scenarios. This limits diversity in the data set. Some power system scenarios are rare, especially cyber-attacks, hardware-in-the-loop (HIL) simulation allows targeted data set creation realistic scenarios captured from the same commercial devices found in utilities. The same data used in this work has also been used in [5] for synchrophasor data mining research.

Intrusion detection systems (IDS) [22] are network security appliances designed to quickly intercept attacks, potentially overlooked by security measures such as firewalls, to protect data confidentiality, integrity, and availability by preventing or minimizing the impact of attacks. Network intrusion detection systems typically utilize misuse detection methods to identify normal states given historical knowledge of attacks and vulnerabilities. New attacks may be overlooked by misuse detection methods if there is no prior record of an attack. Anomaly detection is the opposite of misuse detection, which identifies attacks given historical knowledge of normal states. Supervised learning techniques are most commonly used for anomaly detection [7]. These techniques rely heavily on training data set(s) made up of normal states [31]. For supervised learning anomaly detection techniques to be effective in real-world applications the training data would need to contain an assortment of all possible normal states found within each observation and be free of any outliers that would compromise the algorithm. Obtaining a training data set of this caliber may not be practical or necessary for each IDS application. Unsupervised anomaly detection provides benefits over misuse detection and supervised anomaly detection. Unsupervised methods do not require prior knowledge of states or training data; thus, potentially detecting new attacks without any record of attacks or normal states. However, assumptions must be made on the data given the clustering model to distinguish attack states from normal states.

Rule-based methods are commonly combined with misuse detection for intrusion detection. The rules are built on known vulnerabilities and attack vectors. The drawback to this approach is there dependency on prior knowledge of threats and how those threats appear on the network. To improve the detection of unknown threats statistical methods may be supplemented. This can be accomplished by monitoring the occurrence of some specific event over time with a choice statistical metric. If the quantity exceeds a specified bounds then one can assume intrusion. A similar method will be used with our approach to intrusion detection. Supplementing methods such as cluster validity and fuzzy inference system may be necessary to more easily quantify the cluster result.

Partition-based clustering methods such as the fuzzy c-means (FCM) algorithm [3], groups data on the assumption that groups are tight well-separated clusters of data. Therefore, similar assumptions may be inferred to detect outliers using this type of algorithm: 1) if anomalies (cyber-attacks) are present, then the number of normal states greatly exceeds the number of anomalous states; 2) the anomalous states are measurably different than normal states. These assumptions may not always be true. For instance, if attack states greatly exceed normal states, then the algorithm would classify cyber-attacks as normal behavior, and vice versa. This would lead to a significant false classification rate. Also, cyber-attacks disguised as typical power system disturbances may not be measurably different than normal activity, if the disturbances are common. In this case, the second assumption would prevent the algorithm from identifying cyber-attacks. Alternatively, if the power system disturbance is uncommon, then the associated system states may be incorrectly classified as cyber-attacks.

The proposed approach takes an alternative method by using the cluster prototypes from a data set of normal states, similar to supervised learning, and compares the cluster prototypes from each observed sample, which is coupled with power system logs to improve detection.

The following work presents several contributions. First, our primary contribution, which distinguishes our work from existing unsupervised learning IDS methods is an unsupervised machine learning approach that provides increased detection rates by minimizing the constraints associated with typical unsupervised learning IDS. We also present a methodological approach and usage model applied to industrial power system networks. In order to intelligently quantify the presence of cyber-attacks and relax the assumptions required to detect anomalies using cluster analysis the FCM is combined with the fuzzy inference system (FIS). The FCM and FIS are the main fundamental methods utilized in the proposed clustering approach to industrial network intrusion detection.

The remainder of this paper is organized as follows: In section 2, we present related works and their relevance to the motivation of this work. Section 3, we describe the proposed clustering approach and respective mathematical models. We provide explicit results comparing the FCM IDS, K-means IDS, and proposed IDS in Section 4. Section 5 describes electrical transmission substation protection and concludes the paper.

2. RELATED WORK

Various traditional data mining algorithms were used to classify power system faults and cyber-attacks in [5]. These algorithms were able to differentiate between three broad categories; power system disturbance, control actions, and cyber-attacks. Current research on applying data mining to synchrophasor data for power system fault and disturbance classification can be found in [25] and [8]. The K-nearest neighbor algorithm was used to classify three phase faults, voltage oscillation, and voltage sag scenarios in [25]. Hoefding Trees based stream data mining is used in [8]. This approach was able to classify three phase faults and single line to ground faults grouped for binary classification with greater than 90 percent accuracy using simulated power system data.

In the recent past, many literary works were contributed presenting unsupervised anomaly-based intrusion detection methods implementing algorithms such as the K-means [19] and FCM. As mentioned earlier, clustering anomaly detection typically identifies attack states without learning from training data. For example, an unsupervised IDS using FK-prototype clustering was presented in [29]. The system did not perform as well as misuse and supervised anomaly detection methods applied to the same data set. This resulted from the inability to identify attacks when attack states were measurably similar to normal states. The authors recognized that the drawback may have been linked to not utilizing training data.

A network IDS using the FCM was presented in [26]. The algorithm is applied more generally where data is classified given abnormal or normal clusters; therefore, making the assumption that abnormal and normal states strictly belong to their respective clusters. This approach assumes no other relationship exists between clusters and anomalies, and a crisp decision is made based on an observation belonging to a particular cluster. However it is not clear how the clusters are labeled, and the aforementioned assumptions were used to classify each observed state. The FCM IDS performance was similar to the FK-prototype clustering.

The work presented [14] is a similar method using the K-means algorithm. Again, this algorithm was confined to the aforementioned set of assumptions in order to detect attacks. The K-means algorithm outperformed the FK-prototype using the same data set in [29].

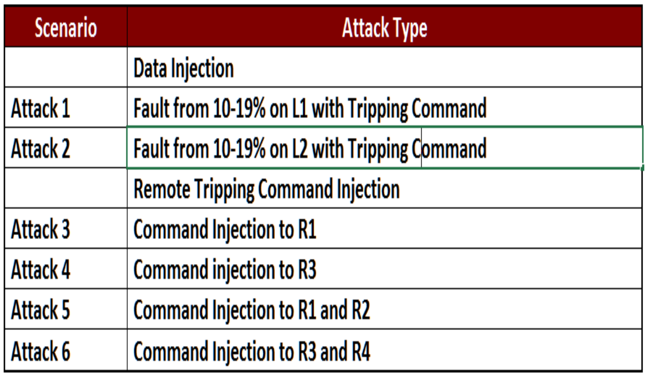
The research presented in [4] combined anomaly detection algorithm with a clustering algorithm. This technique is used to identify anomalies related to clusters by finding the cluster membership, multiple cluster membership, and the degree of which each state is an anomaly. In contrast to the work presented in [26], this approach attempts to distinguish the relationship between anomalies and clusters.

Each algorithm successfully demonstrates the application of unsupervised machine learning for anomaly-based intrusion detection; however, they all share a common set of assumptions. Applying clustering with these assumptions alone is not enough. The ideal IDS should quantify the degree of an attack or normal state regardless of whether the feature space has more or less cyber-attack activity versus normal activity, and should be capable of identifying cyber-attacks that mimic normal behavior.

3. METHODOLOGY

The following subsections describe the proposed unsupervised anomaly-based IDS approach (Fig. 1). The power system data discussed in [5] was used to evaluate the proposed method. The data set is described in more detail in the following section. We will discuss the techniques used and analyze the proposed IDS results against the K-means IDS, and FCM IDS.

3.1 IDS Algorithm



Scenario	Attack Type
	Data Injection
Attack 1	Fault from 10-19% on L1 with Tripping Command
Attack 2	Fault from 10-19% on L2 with Tripping Command
	Remote Tripping Command Injection
Attack 3	Command Injection to R1
Attack 4	Command injection to R3
Attack 5	Command Injection to R1 and R2
Attack 6	Command Injection to R3 and R4

Table 1: Attack Scenarios Selected from the Power System Data Set to Evaluate the Proposed IDS.

Our approach to evaluating clustering for IDS in ICS and SCADA systems consists of four processes. 1) A pre-processing step is applied to the data sets as an attempt to improve the clustering efficiency and outcome. This step also includes feature reduction and a process to estimate the number of clusters. The subtractive clustering technique was used to estimate the underlying number of clusters. 2) Clustering analysis is conducted to find underlying structures present in the data sets. 3) Features are generated from the cluster result considering cluster intra-distances and inter-distances and their associated elements. 4) States are classified given the index generated by the fuzzy inference system.

3.2 Data Set Description

The power system data used in this analysis is a subset of data sets created by Mississippi State University [5]. The initial data set consisted of 15 sets with 37 power system event scenarios within each data set. The different scenarios are divided into Natural Events (8), No Events (1), and Attack Events (28). We used the power system data to generate more complex data sets (Table 1). There are multiple types of scenarios that are found within the data sets (see enumeration below).

1. Short-circuit fault which represents a short in a power line that can occur in various locations along the line.

2. Line Maintenance which represents when one or more relays that are disabled on a line requiring maintenance.

3. Remote tripping command injection which represents an attack that results in a command being sent to a relay which causes a breaker to open.

4. Relay setting change which represents an attack where the attacker changes the setting of relays that are configured with a distance protection and causes the relay function to become disabled and not trip for an actual fault or command.

5. Data injection which represents an attack that imitates an actual fault by changing current, voltage, sequence, components values to parameters which ultimately result in a blackout.

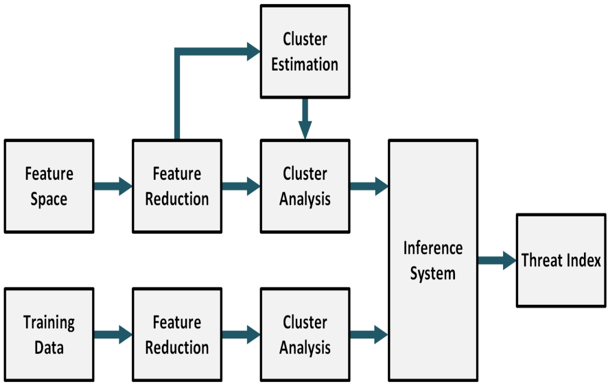


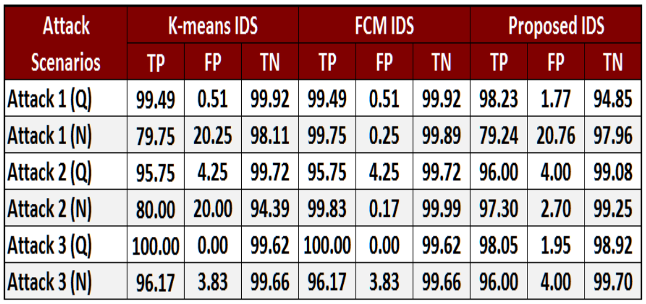
Figure 1: Flow Diagram of Proposed Clustering Approach to Industrial Network Intrusion Detection

3.3 Feature Selection

Initially, the feature space was reduced by applying principal component analysis (PCA) a popular feature reduction technique also used in [4][27]. The PCA is used to reduce the M-dimensional feature space by projecting the data on lines (principal components) in an N-dimensional space such that the most variance is achieved. The principal components ($\boldsymbol{y}$) follow three properties [27]: 1) $E[y(i)y(j)] = 0, i \neq j$, therefore uncorrelated; 2) $y_1 \geq y_2 \geq, ..., \geq y_n$; and 3) the total variation in $y_1, y_2, ..., y_n$ is equal to the total variation in the original features $x_1, x_2, ..., x_m$. The principal components can be found easily using eigenanalysis of the covariance (correlation) matrix of $\boldsymbol{x}$ [15]. The eigenvectors represent the direction of the principal components. The eigenvalues give a measure for the amount of variance on features for each direction. The highest eigenvalue is the first principal component, the second highest is the second principal component, and so on. The feature space is reduced by only using the principal components with the most significant values.

The features below were selected from four features plus logs shown to have the most information in prior work [5]. Only a few features out of the 128 dimension feature space were needed to classify data in the power system data set. These features were utilized in place of the features generated using the PCA approach to evaluate and compare the IDS methods as it increased computational efficiency.

1. Phase A Current Phase Angle
2. Phase A Current Phase Magnitude
3. Control Logs
4. Relay Logs
5. Snort Logs



Attack Scenarios	K-means IDS			FCM IDS			Proposed IDS		
	TP	FP	TN	TP	FP	TN	TP	FP	TN
Attack 1 (Q)	99.49	0.51	99.92	99.49	0.51	99.92	98.23	1.77	94.85
Attack 1 (N)	79.75	20.25	98.11	99.75	0.25	99.89	79.24	20.76	97.96
Attack 2 (Q)	95.75	4.25	99.72	95.75	4.25	99.72	96.00	4.00	99.08
Attack 2 (N)	80.00	20.00	94.39	99.83	0.17	99.99	97.30	2.70	99.25
Attack 3 (Q)	100.00	0.00	99.62	100.00	0.00	99.62	98.05	1.95	98.92
Attack 3 (N)	96.17	3.83	99.66	96.17	3.83	99.66	96.00	4.00	99.70

Table 2: K-means, FCM, and Proposed IDS Algorithm Results for Quantization versus Normalization Comparison.

3.4 Standardize Data

The features presented in the power system data set are within numerous ranges. Features with much larger values or much smaller values may bias the clustering algorithm as the features have more influence on the optimization task. Standardizing the feature space so that the feature values are within the same range is a way to improve clustering results. We used unity based normalization. The features are normalized by calculating:

$$\hat{x}_n = \frac{x_n - min(x)}{max(x) - min(x)} \tag{1}$$

where $\boldsymbol{x} = (x_1, \cdots, x_n)$ is the feature space and $\hat{x}_n$ is the n^{th} normalized feature.

An additional step was added in the normalization function to better handle large variance in the distance vectors computed as inputs to the inference system. During analysis it was noted that large variance in the distance vector was caused by very few states having greater value than the average vector value. Using unity based normalization was not enough to resolve this issue alone. The problem was mitigated by establishing a simple threshold for the upper bound of each distance vector. We used the following piecewise function:

$$D(i) = \begin{cases} 2\frac{\sum_{i=1}^{n} D(i)}{N}, D(i) > 2\frac{\sum_{i=1}^{n} D(i)}{N} \\ D(i), D(i) < 2\frac{\sum_{i=1}^{n} D(i)}{N} \end{cases} \tag{2}$$

Quantization was applied to the data sets as another alternative to reduce large variance in data facilitated by only a few outliers. The quantized feature sets and normalized feature sets were compared using the K-means, FCM, and proposed IDS results. As illustrated in Table 2, the K-means performance is reduced using normalized data versus quantized data; however, the FCM and proposed IDS perform slightly better (overall) given the normalized results. The quantization method was selected over the normalization method as it is less computationally complex. The algorithms are compared using true positive (TP) detection rate, false positive (FP) detection rate, and true negative (TN) detection rate.

3.5 Cluster Tendency

A cluster tendency technique was used to help alleviate any doubt that the power system data structure could be accurately modeled by clustering. The Hopkins Test which calculates a numerical index that represents whether features in a data set differ significantly from the assumption that the features are uniformly distributed [17][12]. The index is computed by comparing the distance (d_i) between features and their nearest neighbors to the distance (s_i) between uniformly generated random features and their real nearest neighbors. The Hopkins index is:

$$\boldsymbol{h} = \frac{\sum_{i=1}^{n} s_i}{\sum_{i=1}^{n} s_i + \sum_{i=1}^{n} d_i} \tag{3}$$

If clusters are present in the underlying structure, then the distance s_i will be greater than distance d_i, because the distances from random sampled data to their real neighbors should be greater than the distances from real data to their real neighbors who may be clustered together. In this case the index is high. If features are equally probable (uniformly distributed), then d_i and s_i are similar and the index will approach 0.5 [17]. The Hopkins index was applied to the data sets selected for the evaluation prior to synthesizing the data sets to increase complexity. For the most part, values greater than 0.9 were found for each data set, which were the average of ten iterations of the Hopkins index algorithm.

3.6 Cluster Analysis

The FCM is a widely accepted clustering model and was presented as an improvement to the hard K-means clustering algorithm [3][24]. The FCM adopts concepts from fuzzy set theory by assigning membership to each data point representing the degree to which the data belongs to a cluster. This membership value is inversely proportional to the distance between data point x_i and cluster centroid (prototype) c_j. The prototypes are the cluster centers determined by the FCM. The key difference between the K-means is the fuzzy partitioning. The fuzzy membership assignment is constructed using the membership matrix U whose values are between $[0, 1]$. The assigned membership matrix values for each cluster must sum to 1:

$$\sum_{i=1}^{c} U_{ij} = 1, \forall j = 1, ..., n \tag{4}$$

The FCM clustering algorithm seeks to minimize the cost function

$$J_{FCM} = \sum_{i=1}^{N} \sum_{j=1}^{C} u_{ij}^{m} ||x_i - c_j||^2 \tag{5}$$

Where m, commonly referred to as the fuzzifier parameter (set to 2.0 in [3]). The fuzzifier is determined by the degree of fuzziness in the clusters. The vector u_{ij} is the degree of membership of x_i in the cluster c_j and $||x_i - c_j||^2$ is the Euclidean distance from the states x_i to the cluster prototypes c_j. We may minimize J_{FCM} only if

$$U_{ik} = (\sum_{j=1}^{c} (\frac{||x_i - c_k||^2}{||x_j - c_k||^2})^{\frac{2}{m-1}})^{-1}, 1 \leq i \leq c; 1 \leq k \leq n; and \tag{6}$$

$$\boldsymbol{v}_i = \frac{\sum_{k=1}^{n} u_{ik}^{m} x_k}{\sum_{k=1}^{n} u_{ik}^{m}}, 1 \leq i \leq c. \tag{7}$$

The FCM can be summarized in two steps: 1) search for the cluster prototypes; and 2) assign the data (states) membership to the prototypes using a distance metric such as the Euclidean distance. This is an iterative process conducted until the algorithm converges, i.e., the prototypes are relatively fixed with respect to prior iterations.

3.7 Fuzzy Inference System

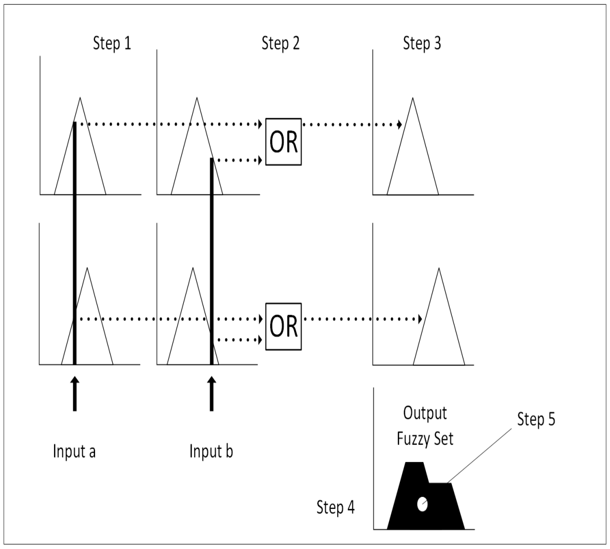


Figure 2: Example Mamdani Fuzzy Inference System

Fuzzy inference system (FIS) is a process based on fuzzy set theory [30] that maps inputs (e.g., features generated from FCM membership values, prototypes, etc.) to outputs. When used as a fuzzy classifier these outputs are classes such as attack or normal for this application. The Mamdani fuzzy inference system [20] process can be described by the following five steps shown in Fig. 2: 1) Fuzzify inputs by applying input membership functions (antecedents) - this step finds the degree to which the input belongs to the respective fuzzy sets. 2) Use fuzzy set operators (e.g., fuzzy and, fuzzy or, etc.) - this combines the fuzzy set inputs given the fuzzy rules to determine each ruleâĂŹs truth value. 3) Determine the consequence (fuzzy set) of each rule by combining the ruleâĂŹs truth value with the output membership function. 4) Aggregate the consequence to find the output distribution. 5) Finally, find the crisp result by defuzzifying the output distribution. This may be accomplished by computing centroid.

The fuzzy rules describe how the FIS makes a decision given input features. The input features utilized for the proposed method were derived from the FCM result and a training set (data set of only normal states). The features are: a) distance between cluster prototypes and sample space centroid; b) distance between each state and training data centroid; c) distance-density ratio. Fuzzy rules were developed similar to [6] relating the input variables to an output variable for the purpose of generating an index between $[0, 1]$; thus, quantifying the degree by which each state is an attack. A simple threshold of 0.7 was used to classify states. States were classified as attack if the attack index was greater than or equal to 0.7, otherwise the states were classified as normal.

4. SUMMARY OF EXPERIMENTS AND RESULTS

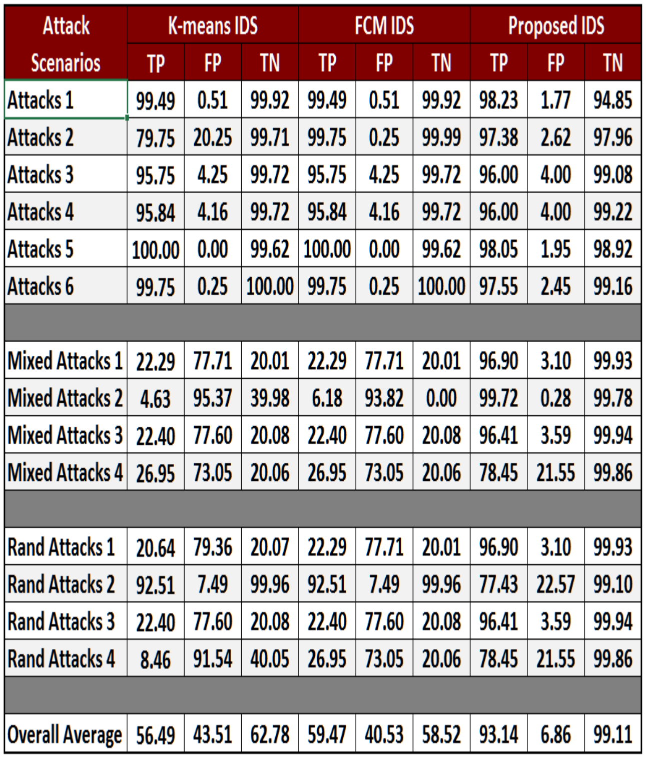
To validate the proposed anomaly-based IDS for electrical transmission substation protection we tested the clustering algorithms by writing software using MATLAB [21] and the power system data set. Each data set was binary (two class) including sensor measurements of cyber-attack events and normal activity. The data sets included several thousand samples for each cyber-attack scenario selected.

The FCM, K-means, and proposed IDS algorithms were evaluated using three groups of attack scenarios. Five different data sets of the same attack type were used for each attack scenario in the experiment. Three groups were created from this data. The first group maintained each data set in its original form. This group, denoted simply by Attacks, contained six attack scenarios (See Table 3). The data sets represent attack scenarios 1 to 6. The second group was created by combining data samples collected during numerous cyber-attack events with an attack scenario data set. The attack samples were combined in this way to make the number of attack states much greater than the number of normal states. This was required because each data set was primarily made up of normal states, containing approximately 10-20 percent attack states. The second group, denoted by Mixed Attacks, contained four attack scenarios. The third group was created by randomizing the states in each data set from group two, as an attempt to remove large collections of similar states in the data; thus, increasing the problem complexity. The third group is denoted by Random (Rand) Attacks. As mentioned previously, the first group was not modified. This data was selected to provide a structure adhering to the constraints placed by the K-means and FCM IDS where they would achieve the best performance. The mixed data sets add complexity by increasing the attack states versus normal states while adding attacks from various attack scenarios. The random attack group adds even more complexity by randomly reordering the states in the mixed data sets.

Table 3 illustrates the performance of the algorithms given each attack scenario. The performance was determined by applying the IDS algorithms to five data sets from each attack scenario. The values presented are the average over all five data sets. The K-means and FCM IDS algorithms perform exceptionally well given attack scenarios from group one. These algorithms outperform the proposed IDS, achieving perfect detection of cyber-attacks given some scenarios; however, the results are expected since the first attack group provides ideal system behavior. The performance of these algorithms greatly diminishes when applied to the mixed attack and random attack group scenarios. The proposed method overcomes the added complexity by utilizing FIS, which allows for more information to be drawn from the cluster results and when combined with system logs the algorithm performance is improved significantly. The K-means and FCM IDS algorithms simply find underlying structures in data, so although control logs, relay logs, and snort logs were contained in each data set the algorithms failed to distinguish cyber-attacks from normal activity.

Randomly reordering samples within the data set increased complexity for some scenarios, for others the results of the Rand Attack scenarios mirrored the Mixed Attack scenarios. The possibility of duplicated results between these scenarios was expected as reordering samples should not change the underlying data structure as long as the features remain the same for each sample.

Our approach utilizes threshold-based classification to draw the line between cyber-attacks and normal activity. Using this procedure the algorithm may inaccurately classify states as it attempts to apply a linear classifier to a non-linear threshold vector. To the best of our knowledge, this step prevented the algorithm from outperforming the K-means and FCM IDS algorithms when applied to the first attack group.



Attack Scenarios	K-means IDS			FCM IDS			Proposed IDS		
	TP	FP	TN	TP	FP	TN	TP	FP	TN
Attacks 1	99.49	0.51	99.92	99.49	0.51	99.92	98.23	1.77	94.85
Attacks 2	79.75	20.25	99.71	99.75	0.25	99.99	97.38	2.62	97.96
Attacks 3	95.75	4.25	99.72	95.75	4.25	99.72	96.00	4.00	99.08
Attacks 4	95.84	4.16	99.72	95.84	4.16	99.72	96.00	4.00	99.22
Attacks 5	100.00	0.00	99.62	100.00	0.00	99.62	98.05	1.95	98.92
Attacks 6	99.75	0.25	100.00	99.75	0.25	100.00	97.55	2.45	99.16
Mixed Attacks 1	22.29	77.71	20.01	22.29	77.71	20.01	96.90	3.10	99.93
Mixed Attacks 2	4.63	95.37	39.98	6.18	93.82	0.00	99.72	0.28	99.78
Mixed Attacks 3	22.40	77.60	20.08	22.40	77.60	20.08	96.41	3.59	99.94
Mixed Attacks 4	26.95	73.05	20.06	26.95	73.05	20.06	78.45	21.55	99.86
Rand Attacks 1	20.64	79.36	20.07	22.29	77.71	20.01	96.90	3.10	99.93
Rand Attacks 2	92.51	7.49	99.96	92.51	7.49	99.96	77.43	22.57	99.10
Rand Attacks 3	22.40	77.60	20.08	22.40	77.60	20.08	96.41	3.59	99.94
Rand Attacks 4	8.46	91.54	40.05	26.95	73.05	20.06	78.45	21.55	99.86
Overall Average	56.49	43.51	62.78	59.47	40.53	58.52	93.14	6.86	99.11

Table 3: K-means, FCM, and Proposed IDS Algorithm Results.

The overall results illustrate a vast improvement with using the proposed IDS approach over the simple FCM and K-means IDS algorithms. The significant difference in performance demonstrates the limitations of the K-means and FCM IDS algorithms. Furthermore, the results of the proposed IDS shows the benefits of adding intelligent techniques such as the FIS to provide a mechanism that can be used to improve detection.

5. CONCLUSION

Electrical transmission substation protection systems must address cyber-attacks along with many other contingencies such as natural events, system faults, accidents, and operator error [11]. Sensor measurements are normally monitored by control centers housed at substations incorporating ICS/SCADA systems. The proposed IDS can support transmission substation protection systems by alerting system operators of potential cyber-attacks. However, the IDS should be supplemented with other cyber-attack detection procedures to determine if potential attacks are genuine. For instance, erroneous sensor readings may lead to true outliers or anomalies. This behavior would be classified as a cyber-attack using anomalous-based IDS techniques discussed thus far, as most unsupervised machine learning methods used to distinguish network states utilize similarity metrics and rely on system models derived from normal activity; therefore, additional methods may be necessary to waive this behavior as a cyber-attack.

The proposed algorithm would suffice as a host-based network IDS [28] given its utilization of substation control logs, relay logs, and snort logs. The IDS would be best placed in electrical transmission substations. Each substation would run its own separate IDS instance, which would be configured to monitor behavior of systems (e.g., sensors, synchrophasors, and PMUs) contained in its network. This usage model could be extended from one substation to thousands of substations, and would have a minuscule footprint on system bandwidth and hardware, as opposed to using a single IDS instance for multiple substations. Utilizing a single IDS instance for multiple substations presents certain issues, such as a single point of failure, which could leave all associated substations without a cyber-attack detection mechanism if the IDS fails. Another, concern utilizing a single IDS instance for multiple substations is bandwidth and hardware requirements. For example, network traffic and logs from each sensor and substation would be transmitted to the IDS system; thus increasing network bandwidth requirements between these systems. Also, the computational complexity and resources such as memory and CPU utilization would be increased with each substation, which may lead to increased hardware requirements and costs.

In this paper, we propose a clustering approach to industrial network intrusion detection for power system applications. The approach supplemented a more complex IDS by quantifying the degree by which an event is an attack, given network data sets, to improve intrusion detection and minimize false alarm rates. The study shows practical value when applied to a synthetic power system data set, and presents a usage model showing how the IDS may be implemented in a real application.

Our experimental results highlight the issues associated with using cluster analysis as a singular tool for anomaly-based intrusion detection as the performance is degraded if system network states do not meet certain criteria during a cyber-attack event. Instead, clustering analysis should be paired with techniques that allow for more intelligent results given cluster features determined from the analysis.

Although we recommend that clustering not be used as a singular tool for IDS, our results did find that there was a vast improvement with using the proposed IDS over the simple FCM and K-means IDS algorithms. In the end, if clustering alone is used, then detection performance can be improved by adding intelligent techniques such as FIS.

6. REFERENCES

[1] M. Adamiak, A. Apostolov, M. Begovic, C. Henville, K. Martin, G. Michel, A. Phadke, and J. Thorp. Wide area protection 8212;technology and infrastructures. *Power Delivery, IEEE Transactions on*, 21(2):601–609, April 2006.

[2] D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle. Smart generation and transmission with coherent, real-time data. *Proceedings of the IEEE*, 99(6):928–951, 2011.

[3] J. C. Bezdek. *Pattern recognition with fuzzy objective function algorithms.* Kluwer Academic Publishers, 1981.

[4] A. bin Haji Ismail, A. Abdullah, K. bin Abu Bak, M. bin Ngadi, D. Dahlan, and W. Chimphlee. A novel method for unsupervised anomaly detection using unlabelled data. In *Computational Sciences and Its Applications, 2008. ICCSA '08. International Conference on*, pages 252–260, June 2008.

[5] R. Borges Hink, J. Beaver, M. Buckner, T. Morris, U. Adhikari, and S. Pan. Machine learning for power system disturbance and cyber-attack discrimination. In *Resilient Control Systems (ISRCS), 2014 7th International Symposium on*, pages 1–8, Aug 2014.

[6] S. Cateni, V. Colla, and M. Vannucci. A fuzzy logic-based method for outliers detection. In *Artificial Intelligence and Applications*, pages 605–610, 2007.

[7] Y. Chen, X. Dang, H. Peng, H. Bart, and H. Bart. Outlier detection with the kernelized spatial depth function. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 31(2):288–305, Feb 2009.

[8] N. Dahal. Synchrophasor data mining for situational awareness in power systems. Technical report, Ph.D. dissertation, Mississippi State University, 2012.

[9] J. De La Ree, V. Centeno, J. Thorp, and A. Phadke. Synchronized phasor measurement applications in power systems. *Smart Grid, IEEE Transactions on*, 1(1):20–27, June 2010.

[10] N. Falliere, L. O. Murchu, and E. Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 2011.

[11] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid; the new and improved power grid: A survey. *Communications Surveys Tutorials, IEEE*, 14(4):944–980, Fourth 2012.

[12] B. Hopkins and J. Skellam. A new method for determining the type of distribution of plant individuals. *Annals of Botany*, 18(2):213–227, 1954.

[13] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry. Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection*, 2(3):73–83, 2009.

[14] M. Jianliang, S. Haikun, and B. Ling. The application on intrusion detection based on k-means cluster algorithm. In *Information Technology and Applications, 2009. IFITA '09. International Forum on*, volume 1, pages 150–152, May 2009.

[15] I. Jolliffe. *Principal component analysis.* Wiley Online Library, 2005.

[16] R. D. Larkin, J. Lopez, Jr., J. W. Butts, and M. R. Grimaila. Evaluation of security solutions in the scada environment. *SIGMIS Database*, 45(1):38–53, Mar. 2014.

[17] R. G. Lawson and P. C. Jurs. New index for clustering tendency and its application to chemical problems. *Journal of chemical information and computer sciences*, 30(1):36–41, 1990.

[18] V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson, S. Imai, and A. Apostolov. Ieee psrc report on global industry experiences with system integrity protection schemes (sips). *Power Delivery, IEEE Transactions on*, 25(4):2143–2155, Oct 2010.

[19] L. Maglaras, J. Jiang, and T. Cruz. Integrated ocsvm mechanism for intrusion detection in scada systems. *Electronics Letters*, 50(25):1935–1936, 2014.

[20] E. H. Mamdani and S. Assilian. An experiment in linguistic synthesis with a fuzzy logic controller. *International journal of man-machine studies*, 7(1):1–13, 1975.

[21] MATLAB. *version 8.3.0.532 (R2014a)*. The MathWorks Inc., Natick, Massachusetts, 2014.

[22] J. McHugh, A. Christie, and J. Allen. Defending yourself: The role of intrusion detection systems. *Software, IEEE*, 17(5):42–51, Sept 2000.

[23] S. Mousavian, J. Valenzuela, and J. Wang. A probabilistic risk mitigation model for cyber-attacks to pmu networks. *Power Systems, IEEE Transactions on*, 30(1):156–165, Jan 2015.

[24] N. Pal and J. Bezdek. On cluster validity for the fuzzy c-means model. *Fuzzy Systems, IEEE Transactions on*, 3(3):370–379, Aug 1995.

[25] Y. Pires, J. Morais, C. Cardoso, and A. Klautau. Data mining applied to the electric power industry: Classification of short-circuit faults in transmission lines. In *Innovative Applications in Data Mining*, pages 107–122. Springer, 2009.

[26] W. Ren, J. Cao, and X. Wu. Application of network intrusion detection based on fuzzy c-means clustering algorithm. In *Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on*, volume 3, pages 19–22, Nov 2009.

[27] M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L. Chang. A novel anomaly detection scheme based on principal component classifier. Technical report, DTIC Document, 2003.

[28] C.-W. Ten, J. Hong, and C.-C. Liu. Anomaly detection for cybersecurity of the substations. *Smart Grid, IEEE Transactions on*, 2(4):865–873, Dec 2011.

[29] G. Xiang, W. Min, and Z. Rongchun. Applying fuzzy data mining to network unsupervised anomaly detection. In *Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium on*, volume 2, pages 1296–1300, Oct 2005.

[30] L. A. Zadeh. Fuzzy sets. *Information and control*, 8(3):338–353, 1965.

[31] J. Zhang, M. Zulkernine, and A. Haque. Random-forests-based network intrusion detection systems. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 38(5):649–659, Sept 2008.