

# Anomaly Detection Based on Regularized Vector Auto Regression in Thermal Power Plant

Yi-Ming Wei<sup>1</sup>, Hao Yu<sup>2,3</sup>, Wen-Jun Wang<sup>2,3</sup>,  
Yue-Heng Sun<sup>2,3,a</sup>, Jian Wang<sup>1</sup> and Zhan-Jie Song<sup>4</sup>

<sup>1</sup> School of Electronic Information Engineering, Tianjin University, Tianjin, 300072, China

<sup>2</sup> Tianjin Key Laboratory of Cognitive Computing and Application

<sup>3</sup> School of Computer Science and Technology, Tianjin University, Tianjin, 300072, China

<sup>4</sup> School of Science and Institute of TV and Image Information, Tianjin University, Tianjin, 300072, China

**Abstract.** Anomaly detection has gained widespread interest especially in the industrial conditions. Contextual anomalies means that sensors of industrial equipment are interrelated and a sensor data instance called anomalous should be in a specific context. In this paper we propose a scheme for temporal sensor data monitor and anomaly detection in thermal power plant. The scheme is based on Regularized Vector Auto Regression, which is used to capture the linear interdependencies among multiple time series. The advantage is that the RVAR model does not require too much knowledge about the forces influencing a variable. The only prior knowledge needed is a list of variables which can be hypothesized to affect each other. Experimental results show that the proposed scheme is efficient compared with other methods such as SVM, BPNN and PCA.

## 1 Introduction

In China, most of the electricity is generated by thermal power plants. Coal miller, Coal feeder, Fans and so on are the main equipment of the power plant and they are crucial for stable power supply. For monitoring the status of such equipment real time, thousands of sensors are installed (such as: temperature sensors, pressure sensors, speed sensors), from which we can acquire temporal series data all the time. Thus, in order to monitor the working situation of systems in the thermal power plants, it is very crucial to detect anomalies based on real-time data of the anomaly condition for further diagnoses and proceeding. And with the development of technology and reduction of cost, the requirements of the industry are continually increasing and, apart from advanced process control techniques, system availability, reliability and safety are becoming attributes of primary importance. So anomaly detection is one of the first and most important steps needed to ensure operational continuity of the thermal plant safety, as well as high production quality standards.

Anomaly detection (also called outlier detection, novelty detection, or fault detection) refers to the problem of finding patterns in data that do not conform to expected behavior [1], which involved Intrusion Detection, Fraud Detection, Industrial Safety Detection (which we are focus on), Image and Text Processing fields etc. Anomaly detection basically intends to recognize abnormal conditions in the operation of a monitored system. The primary task of anomaly detection

is to recognize abnormal conditions while minimizing both probability of false alarms and detection time, which is defined as time between the happening of an anomaly and its detection. In recent years, intensive research efforts have been made in the field of process supervision, fault detection and diagnosis to enhance the reliability and availability of control systems in industrial. A variety of techniques have been proposed. (Details refer to the reviews [1-6]).

In thermal power plants, sensors installed on the equipment are not isolated, rather they are interrelated. Generally, judging a sensor normal or abnormal should be considering the other sensors or history data itself as reference, in other words, a sensor data instance is anomalous must be in a specific context (but not otherwise), so it is termed as a contextual anomaly [1]. So, a reasonable idea is that first we can estimate theoretical values of all sensors should return and then compare them to the real data returned by the sensors, if the differences exceed some thresholds predetermined, the corresponding sensor should be abnormal. In this paper, a scheme based on Regularized Vector Auto Regression was proposed, which modeled the relationship among sensors. This model can be acquired by training history data offline, and be used in anomaly detection process real time. The propose scheme is efficient for the data of the thermal power plants compared with other method.

The paper is organized as follows. In section II, we discuss related work and in section III, we describe the details of our proposed regularized vector auto regression algorithm. Then, experimental results will be displayed in

<sup>a</sup> Corresponding author: yhs@tju.edu.cn

section IV, Finally, section V concludes the paper and presents directions for future work.

## 2 Related Work

Anomaly detection is a very important and well-studied problem in data mining and analyzing. So far, there are many surveys about the anomaly detection methods in various fields. Hodge and Austin [2] provided an extensive survey of anomaly detection techniques developed in machine learning and statistical domains. An extensive review of novelty detection techniques using neural networks and statistical approaches and has been presented in [3, 4]; Patcha and Park [5] presented a survey of anomaly detection techniques used specifically for cyber-intrusion detection; Gupta, et al. [6] provided a structured overview of anomalies definitions for various forms of temporal data.

Sensors as data acquisition sources are installed on a fixed equipment. Every sensor data could be a symptom (also called feature) of the state of the equipment, which returns a numerical value per second (continuous or binary value). For example, sensor  $X_i$  in time  $T_j$ , the returned data denoted as  $Y_{ij}$ . In time  $T_j$ , all sensors data can constitute a feature vector  $(Y_{1j}, Y_{2j}, \dots, Y_{nj})$ , and  $n$  is the number of the sensors installed on the equipment. In actual situation, the number of the sensor is very large, and the speed of the data acquisition is high, so it is must to develop a fast and efficient scheme. To handling with high dimensional data, some schemes proposed [7-10]. Most of these methods share the common view: dimensional reduction. They suppose that the original data space is sparse, which can be processed in a succinct subspace. Usually, the population of anomalies is small, compared to the number of regular objects, limiting the subspace learning capability of the most algorithms [11]. Especially in thermal power plant, failure of equipment is very rare. In most cases, failures are related to different sensors. Due to lack of anomaly instances, dimension of some sensors should not be excluded from the model. So, subspace analysis is not suitable for our dataset.

## 3 Regularized Vector Auto Regression Method

In this section, the proposed anomaly detection method will be detailed. Firstly, data preprocessing is performed; secondly, the regression model is setup; and in the end, anomaly determining is presented.

### 3.1. Data Preprocess

When the data is acquired, the first step is to preprocess the data. In the paper the preprocessing can be divided into three steps: data interpolation, noise data removal and data normalization.

Due to the hardware faults, some sensor data may be missing during the process of transmission. For example,

if  $Y_{ij}$  which is the data of the sensor  $X_i$  in time  $Y'_{ij}$  is missing, then it can be linear interpolated as:

$$Y'_{ij} = 2 * Y_{ij-1} - Y_{ij-2} \quad (1)$$

where  $Y'_{ij}$  is substitute for  $Y_{ij}$ .

After solve the problem of data missing, then is to clean data and filter data. The sensor data always tend to incomplete, noisy, and inconsistent, it is necessary to remove and filter such data. This step is used to smooth signals and filter noises. Because the validity of many models is ensured only under steady-state conditions, it is important to identify and select the steady state data.

In order to avoid bias due to the different magnitudes in the measured data eliminate the effect of index dimension and quantity of data, it is crucial to normalize all attribute values into the same scale to avoid the influence of scale. There are various normalizations methods in the literature, in this paper we adopt the most common used one, min-max normalization equation:

$$X' = \frac{X + X_{\min}}{X_{\max} - X_{\min}} \quad (2)$$

In summary, data pre-processing techniques not only can improve the quality of the data, helping to improve the accuracy and efficiency of data mining process, but also can ensure the data is under steady-state conditions.

### 3.2 Model Setup

VAR model describes a linear regression function of  $k$  endogenous variables, and a  $p$ -th-order VAR is expressed formally as follows:

$$Y_t = c + A_1 Y_{t-1} + A_2 Y_{t-2} + \dots + A_p Y_{t-p} + e_t \quad (3)$$

where  $Y_{t-l}$  is called the  $l$ -th lag of  $Y$ ,  $c$  is  $k \times 1$  vector of constants, and  $k$  is dimension of model (i.e. numbers of sensors).  $A_i$  is time-invariant  $k \times k$  matrix (regression coefficients), and  $e_t$  is  $k \times 1$  vector of error terms.

Rewriting VAR( $p$ ) concisely with  $k$  variables in a general way which includes  $T+1$  observations  $Y_0$  through  $Y_T$ , we can stack the vectors and then denote it by a matrix notation.

$$Y = AZ + \quad (4)$$

From the concise matrix notation, the regression parameters can be estimated by the multivariate least squares (MLS), i.e.

$$\text{Min} \|Y - AZ\|_2 \quad (5)$$

As the curse of dimensionality, it needs some techniques to prevent over-fit in solving (5). So, an effective scheme is that: detecting the sensors relationships firstly, then constructing a series VAR models. Since the interrelationships of all sensors are complicated, it is hard to detect the relationships accurately. Regularization is an alternative scheme, which is widely used in the process of model selection (such as: LASSO [12], Ridge Regression [13], Elastic Net [14], etc.).

So, we can rewrite (6) as:

$$\text{Min} \|Y - AZ\|_2 + \lambda_1 \|A\|_1 + \lambda_2 \|A\|_2 \quad (6)$$

$\lambda_1$  and  $\lambda_2$  are punish coefficients. Obviously, elastic net is a generalized method of lasso and ridge regression.

### 3.3 Anomaly Determining

As described in last section, given a newly observed vector  $X'$ , and a learned regression coefficients, we can calculate the error means of the observed value  $X'$  between the predicted value. In this paper, we assume that the learned regression coefficients should represent all of normal output state of the sensors. Therefore, for a normal data sample, the error of predicted value and observed value will be small. In contrary, the larger error means, the predicted value is not reconstructed well by normal regression coefficients, then, it should be deemed as anomaly data. So the greater the error value, the higher probability of failure occurrence of the equipment being monitored.  $X'$  is detected as an unusual if the error is greater than a predefined threshold  $\varepsilon$ , which is a tradeoff between False Positive and False Negative and control the sensitivity of the algorithm.

## 4 Experimental Results

In this section, to experimentally validate effectiveness of the RVAR method, we describe experiments carried out to assess performance on real-world data. In order to compare with the different methods, we evaluate the quality of the anomaly detection results using the area under the AUC and the F1-score.

### 4.1 Dataset

The datasets used to evaluate our RVAR algorithm are shown in Table 1. It provides a brief explanation about the data background, including data size, number of attribute, and class distribution. The anomaly detection datasets were collected from the thermal power plant. These samples were acquired at a synchronous sampling rate and represented all modes of operation. Totally, 10,000 samples are collected for further analysis. There are 34 attributes (the number of the sensors) with continuous values and 1 target attribute with two-class labels (normal and abnormal). Approximately 10% of the normal training data was randomly selected and set aside from each mode group to serve as quarantine testing set.

### 4.2 Anomaly Detection Algorithms

For anomaly detection, we use RVAR method which is trained on only normal data. For each data point, the classifier produces a decision value that represents its confidence in that point being an anomaly. We apply a threshold on the decision value as a cutoff point for decision making. A data point is flagged as an anomaly if the decision value exceeds a threshold. Varying the threshold varies the number of correctly classified outliers (true positives) and incorrectly classified normal data (false positives). The quality of classification is built from a confusion matrix which records correctly and

incorrectly recognized examples for each class. Using this information, we plot a curve of the true positive rate versus the false positive rate, known as the Receiver Operating Characteristic (ROC) curve.

The ROC curve is a graphical plot that illustrates the model performance for multiple threshold values. The curve is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings. TPR (also known as called Recall or Sensitivity) measures the proportion of actual positives (abnormal) which are correctly identified. FPR (also known as the fall-out) refers to the probability that the incorrect positive results occur among all negative samples available during the test. These measures are given by formulas in following equation:

$$TPR = \frac{TP}{TP + FN},$$

$$FPR = \frac{FP}{FP + TN},$$

For the training phase of the anomaly detection algorithms, we take a one-class (or semi-supervised) learning approach and train only on normal data points. During testing, both normal and anomaly data points are used to see how well the model is able to detect anomaly. Since no anomaly are used during the training phase, we use all anomaly during testing phases of the cross validation.

The results of our experiments are present in figure 1. From the figure, it is not difficult to find that presented method can identify anomaly with a high detection rate and few false positives, as reflected in the high average AUC. Anomaly is just relative concept, it is sensitive to threshold. In thermal power plant, threshold can be set according to practical demands of users.

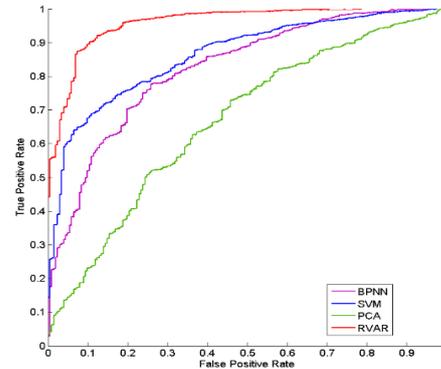


Figure 1. Comparison of ROC curves.

For evaluating the performance of the algorithms and produce, we also adopt measure of the F1-score on the different equipment (primary air fan, induced draft fan and air fan). The measures of choice calculated on positive class:

$$\text{precision} = \frac{TP}{TP + FP},$$

$$\text{recall} = TPR,$$

$$F1\_score = \frac{2 * \text{precision} * \text{recall}}{\text{precision} + \text{recall}}$$

All three measures distinguish the correct classification of labels within different classes. They concentrate on one class (positive examples). The experimental results of different methods about the F1-

score are presented in figure 2. As can be seen, the results of our method are much better than SVM, BPNN and PCA. By looking at the figure, it is easy to find that the results of SVM and BP perform better than PCA. The reason may be the different parameter settings (such as: the number of basis in PCA method, the setting of node and layer in BP etc.). Therefore the performance of methods varies slightly.

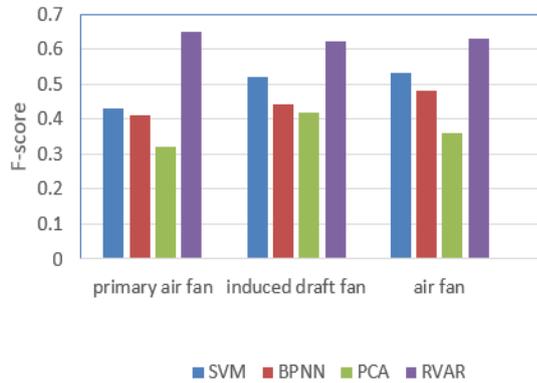


Figure 2. F1-score of different methods.

## 5 Conclusions

This paper focuses on the industrial domain, and proposed a Regularized Vector Auto Regression based method for contextual anomaly detection in Thermal Power Plant. Actual fields test proved that the proposed method is fast and efficient compared with SVM, BPNN and PCA methods. The result shows that the method can successfully detect anomalies in the real-time data underlying the normal behavior model. The result also demonstrates the feasibility of this method practically. The proposed method builds a model for anomalies detection directly from archived data, rather than building it based on human expertise. There is no universal anomaly detection method suitable for any application domains. The proposed method still has the following application constraints: there is a certain class of processes where it is not possible to achieve proper identification, and there are highly complex processes where a simplified linear model would not carry enough information for efficient fault detection and isolation. However, this approach has considerably increased the reliability and safety of a thermal power plant unit.

## Acknowledgments

The work was jointly supported by the Major Project of National Social Science Fund (14ZDB153), the major research plan of the National Natural Science Foundation (91224009, 51438009), the National Science and Technology Pillar Program (2013BAK02B00, 2013BAK02B06, 2015BAL05B00 and 2015BAL05B02), Science and Technology Pillar Program of Tianjin Municipal Science and Technology Commission (12CZDSF07200, 13ZCZDGX01099, 13ZCDZSF02700), the Ocean Public Welfare Scientific Research Project

under Grant No. 201305033, National Science and Technology Program for Public Well-being (2012GS120302), National Natural Science Foundation of China (61303110), Tianjin Research Program of Application Foundation and Advanced Technology (14JCTPJC00517).

## References

1. V. Chandola, A. Banerjee, V. Kumar, ACM computing surveys (CSUR), **41**, 15 (2009)
2. V. J. Hodge, J. Austin, Artificial Intelligence Review, **22**, 85-126 (2004)
3. M. Markou, S. Singh, Signal processing, **83**, 2481-2497 (2003)
4. M. Markou, S. Singh, Signal processing, **83**, 2499-2521 (2003)
5. A. Patcha, J. M. Park, Computer networks, **51**, 3448-3470 (2007)
6. M. Gupta, J. Gao, C. Aggarwal, J. Han, Synthesis Lectures on Data Mining and Knowledge Discovery, **5**, 1-129 (2014)
7. F. Angiulli, C. Pizzuti, Knowledge and Data Engineering, IEEE Transactions on, **17**, 203-215 (2005)
8. F. Angiulli, F. Fassetto, ACM Transactions on Knowledge Discovery from Data (TKDD), **3**, 4 (2009)
9. F. Angiulli, S. Basta, S. Lodi, C. Sartori, Knowledge and Data Engineering, IEEE Transactions on, **25**, 1520-1532 (2013)
10. T. de Vries, S. Chawla, M. E. Houle, Knowledge and information systems, **32**, 25-52 (2012)
11. X. H. Dang, I. Assent, R. T. Ng, A. Zimek, E. Schubert, Data Engineering (ICDE), 2014 IEEE 30th International Conference on. IEEE, 88-99 (2014)
12. R. Tibshirani, Statistics in medicine, **16**, 385-395 (1997)
13. R. Tibshirani, Journal of the Royal Statistical Society. Series B (Methodological), 267-288 (1996)
14. H. Zou, T. Hastie, Journal of the Royal Statistical Society: Series B (Statistical Methodology), **67**, 301-320 (2005)