Műszaki Tudományos Közlemények vol. 18. (2023) 63–69.
DOI: Hungarian: https://doi.org/10.33895/mtk-2023.18.12
English: https://doi.org/10.33894/mtk-2023.18.12

ANOMALY DETECTION WITH ARTIFICIAL INTELLIGENCE METHODS – AN OVERVIEW

Sebestyén Pál György,[1] Hangan Lia-Anca,[2] Czakó Zoltán[3]

[1] *Technical University of Cluj-Napoca, Faculty of Automation and Computers, Department of Computers. Cluj-Napoca, Romania, gheorghe.sebestyen@cs.utcluj.ro*

[2] *Technical University of Cluj-Napoca, anca.hangan@cs.utcluj.ro*

[3] *Technical University of Cluj-Napoca, zoltan.czako@cs.utcluj.ro*

Abstract

Nowadays, more and more human activities depend on computer-based automated systems. Fully automated (robotized) production lines, energy distribution infrastructures and other urban services or environmental surveillance systems are just some examples of cyber-physical systems that depend entirely on automated control systems. In these cases a significant challenge is to identify abnormal behaviors of the supervised or controlled systems, in order to avoid malfunction or sometimes catastrophic events. Our main research goal was to evaluate the potential of adapting and using AI techniques in the field of anomaly detection. We also developed a platform, called AutomaticAI, which can help specialists in different domains to identify the best approaches to solve a given anomaly detection problem. The platform can select the best AI algorithm and parameter configuration for a given set of data containing normal and abnormal data. The tool was used successfully in a variety of domains, from cyber-physical systems to the medical domain.

Keywords*: anomaly detection, artificial intelligence, outlier detection.*

1. Introduction

1.1. Context and motivation

In the times of the forth industrial revolution (Industry 4.0) we are surrounded by different kinds of cyber-physical systems, such as robotized industrial processes, energy and other urban service distribution infrastructures, autonomous transportation, remote healthcare systems, intelligent buildings and cities. All these systems are supervised and controlled by computers, computer programs or computer-based devices. Sometimes services and functionalities critical for the safety of our lives (e.g. autonomous cars) are totally dependent on such autonomous systems. But what happens when something goes wrong, for instance a sensor is not providing the correct measured value, a control device responsible for a critical functionality is broken, or the behaviour of the controlled system is changing in a manner not foreseen in the designing phase? How does an automated (e.g. computer-based) supervising system detect and then react to such an anomaly?

In the past when supervision tasks were performed by humans (e.g. process operators, or simple beneficiaries of some services or devices) a basic training was enough to detect and react to such cases. In an automated system the anomaly detection should be part of the control system. Therefore, in recent years anomaly detection has become an important research subject, and a number of solutions have been proposed and tested.

Anomalies may come in different shapes and forms, from very simple ones (e.g. a value that exceeds an allowed interval) that can be solved with simple thresholding or filtering methods towards complex ones that are hard to define and detect even by a human observer (e.g. climate change effects). In this last case artificial intelligence methods can be used to model and recognize abnormal behaviour.

1.2. Anomaly types

A simple definition for “anomaly” would be a data or a (system) behavior that is very different

from other: data or detected behaviour. A more elaborate definition was given by Hawkins in 1980: “anomaly is an observation that differs so much from other observations that raises suspicion that it was produced by a different mechanism” (e.g. a malfunction in the system or an artificial intervention in a financial process).

There are some other words that have similar or close meaning with the anomaly word: abnormal (behaviour), outlier or deviant.

There are a number of issues regarding the recognition of an anomaly:

- how big the deviation should be in order to classify it as an anomaly?
- natural noise present in some data should not be confused with anomaly
- an anomaly may be a question of viewpoint, or might depend on the context in which it was produced (e.g. a European in an Asian population may be considered an anomaly)
- humans, based on education and experience have a natural ability to recognize an anomaly, even there is no rational explanation for it; computers do not have this “natural” ability.

Regarding the types of possible anomalies we could mention some of them:

- a data/value in the evolution of a signal that exceeds some interval considered normal;
- a change in the linear evolution of a signal;
- some stochastic values that don’t follow a known probability distribution (e.g. Gaussian distribution);
- some multi-parameter observations/objects that don’t fit in some pre-defined classes considered normal cases;
- some deviations in the periodicity of a signal (e.g. arithmias in an ECG signal).

1.3. Domains for automated anomaly detection

Automated recognition of anomalies is an important task [1–4] in the context of new trends such as: IoT, IioT, and Industry 4.0. It is important for safety critical cyber-physical systems where the system must contain fault tolerant and self healing solutions.

In healthcare, different diseases and their symptoms may be considered anomalies of the human body. Early detection of such changes in the physiological parameters of a patient may prevent later evolution of more serious diseases.

Anomaly detection is also useful in any application which deals with huge amounts of data, catalogued as „big data”. In this case manual analyses are not feasible, but some outlier data may influence the outcome of the automated analysis. Therefore, anomaly detection is used in order to eliminate erroneous data.

Automated anomaly detection is needed also in cases when changes are so subtle that the human senses don’t detect them. For instance, in industry early detection of future defects is the bases for preventive maintenance.

Examples of domains where anomaly detection may play a significant role:

- in economic and financial applications, for the detection of frauds or economical tendency changes;
- in industrial processes, for detection of malfunctioning devices or infrastructures, preventive maintenance, alarms generation;
- in medicine for the detection of diseases and symptoms or for abnormal behaviour detection in case of psychologically impaired persons;
- in environment monitoring for detection of parameter changes, contaminations, air pollution;
- in informatics systems for the detection of cybernetic attacks on computing devices, networks of software.

The paradox is that the same anomaly detection technique may be applied for a wide variety of domains and application types. Therefore, we consider that there should be a general anomaly detection tool that may be adapted for different particular domains.

2. Taxonomy of anomaly detection techniques

Because there are many types of anomalies and anomaly detection techniques we considered that it would be useful to define a kind of classification or a taxonomy [5]. Analysing the literature in the field we identified a number of criteria that can be used for classification:

- based on the nature of the anomaly;
- based on the nature of the analysed data;
- based on the evaluation methods;
- based on the nature of the applications.

According to the first criterion the following types of anomalies can be identified:

- single point anomalies or outliers – a value that significantly differ from the rest of the values; examples are: wrong measurements, erroneous data transmission; [1]

– contextual anomaly – where a value/data is very different from a closer context – a more complex anomaly that take into consideration a value's neighborhood; examples are: deviations on the stock market, pixels in an image affected by noise; [2]
– anomalies in time series – where the anomaly is detected as a deviation form a normal trend; e.g. artefacts in an ECG signal. [4]

Based on the nature of analysed data we can take into consideration the number of attributes contained in an observation and the type of correlation existing between observations. From the first point of view we have single variable observations (e.g. temperature variations) and multivariable observations (e.g. EEG signals). Based on the second view there may be:

– data with statistical correlations between observations (e.g. the marks for a discipline follow a Gauss distribution);
– time-based correlation – where the values sampled in time have some kind of correlation (e.g. process parameters);
– spatial correlation – where data measured in neighbouring nodes are somehow correlated (e.g. temperature measurements made by a number of sensors spread in a given region);
– functional correlation – where the physical and chemical law determine some rigorous correlation between measured values (e.g. electrical parameters such as voltage, current and power in an electrical infrastructure).

The anomaly detection methods applied for a given case should take into consideration these types of correlations present in the input dataset.

We can also define different informatics approaches for solving the anomaly detection problem. Some of them are based on system analysis and signal processing methods such as min-max, thresholding, interpolation, system identification, Fourier or Laplace transforms. Other methods are inspired from artificial intelligence such as classification and clustering (e.g. KNN, K means, SVM, random forest, etc.) or neural networks. In this case through a process of training a given classifier may distinguish between normal and abnormal observations.

And finally, based on the type of the applications we may distinguish between techniques that may be applied in off-line mode, where there are no real-time restrictions and any complex method can be applied and techniques for on-line mode, where strict time restrictions limit the use of complex methods that are time consuming.

3. A software platform for anomaly detection

In order to offer a generic tool for anomaly detection we developed a platform which is a collection of procedures useful in the process of data analysis and anomaly detection [6, 7].

The motivations for such an approach were:

– there are many detection techniques and it is difficult to decide from the start which will be the best one for a given dataset;
– beside anomaly detection usually we need other data preprocessing and visualization tools which should be part of a platform;
– specialists from different domains (physics, chemistry, biology, environmental or earth sciences) may not have enough knowledge in artificial intelligence or signal processing domains but they need anomaly detection tools.

The platform is a configurable tool in which a user can define a data processing pipeline containing different preprocessing, classification and visualization procedures that are adapted for a given dataset or application. The platform was initially developed for anomaly detection but it can be useful for other purposes where datasets must be classified.

3.1 AutomaticAI – a tool for selection of best classifier algorithm

If we consider just the artificial intelligence methods and their variations , there is a huge variety of choices and unfortunately there is no unique best solution for all possible applications. In a classic research approach, a limited number of methods are tested and compared and from that set the best performing one is selected. But there may be other methods (untested) which may perform even better.

There is also the problem of setting the optimal parameters for a given method; the obtain results may vary drastically with the values of the setting parameters. The researcher should select the best method form a multidimensional search space, which may be a very time consuming process. [8].

In order to solve this selection and parameters' setting problem we proposed and implemented an automatic method that try to find the best performing method from a wide variety of possibilities. [9]

Our solution is based on an optimization technique built upon particle swarm optimization and simulated annealing methods. [10, 11]

In principle the method works as follows:

– in the first step a number of particles are defined, that represent different classification techniques in different settings;
– in the next repeating step, through a number of epochs the best algorithm and its best setting is selected using the particle swarm optimization technique; each algorithm is trained on the given dataset and a performance function determines which has the best quality parameters. In the next epoch the best performing algorithm set is preserved and through mutations (e.g. parameter changes) new particles are created. Through simulated annealing the mutation degree (e.g. parameter changes) is reduced as the simulation epochs pass;
– finally the method presents the best performing algorithm and their settings together with their quality measures (e.g. accuracy, precision, recall, F1, confusion matrices.

The experiments made on different datasets from different domains showed the efficiency of the proposed method; in each case the automated method found a solution in a reasonable time that gave quality parameters comparable with methods proposed by other research groups. The experiments also showed that there is no unique best solution for all the studied cases. Therefore, the process of finding the best solution is a necessary step.

4. Experiments with the AutomaticAI platform

In this chapter we present a number of experiments in different domains performed in order to validate the efficiency of the proposed AutomaticAI tool.

4.1. Anomaly detection in water infrastructures

In this experiment the goal was to find a method for determining the quality of the water in a distribution infrastructure and generate alerts in case of contamination.

In this experiment we used a dataset called GECCO 2017 [12], that contains approximately 100.000 observations/probes, and each probe include 9 parameter values, that are relevant for the quality of the water (e.g. temperature, pH, conductivity, chlorine content, turbidity).

After applying the AutomaticAI procedure we obtained the best performing algorithms with their best setup. Table 1 shows the results for the first 10 classification algorithms. It seems that in this experiment the Random forest offer very high rate of anomaly (contamination) recognition and the Ridge classifier showed the poorest results.

Table 1. *Algorithms selected for water quality classification. (set parameters: class_weight= 'balanced', max_depth=42, n_estimators=130)*

Algorithm	F1-Measure
RANDOM FOREST	99.92%
EXTRA TREES CLASSIFIER	99.81%
DECISION TREE	99.19%
MLP	99.49%
KNN	99.47%
One-Class SVM	81.46%
SGD CLASSIFIER	50.36%
LOGISTIC REGRESSION	49.66%
PASSIVE AGRESSIVE CLASSIFIER	45.36%
RIDGE CLASSIFIER	37.34%

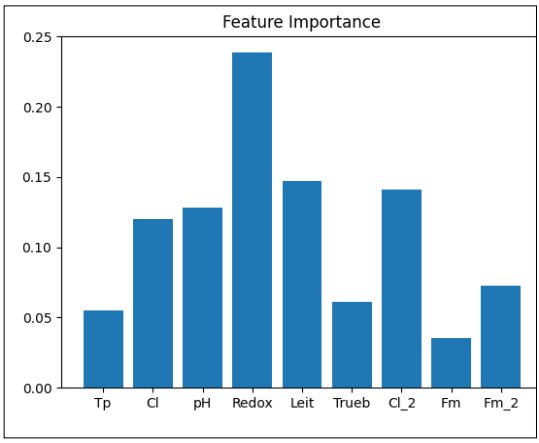

Fig. 1. *Feature importance in the classification of water probes.*

Through other methods included in the platform it could be calculated which parameter had the highest influence in the decision. Figure 1 show this dependence.

4.2. Corona virus infection as anomaly detection

In this experiment our goal was to detect corona virus infection from usual blood analysis without the need for specialized tests (e.g. PCR tests). The need for such an approach was evident in the first phase of the pandemic when PCR tests were rare [13].

In this experiment our goal was to detect corona virus infection from usual blood analysis without

the need for specialized tests (e.g. PCR tests). The need for such an approach was evident in the first phase of the pandemic when PCR tests were rare.

4.3. Cancer detection from colorectal images

In this experiment the goal was to classify colorectal images as containing cancer polyps or not. Traditionally through colonoscopy a trained medical person can distinguish between images with and without cancer formations (polyps). **Figure 2** shows the difficulty of separating normal colon images from those with cancer.

In this experiment we used a pre-trained convolution neural network called ResNet50 in order to extract relevant features from images. Then, using AutomaticAI we determined which classifying algorithm performs best in distinguishing between images containing cancer formations of not. In this experiment the Ridge classifier proved to be the best one with Accuracy=98.33%, Precision=100% and Recall=76.64%.

It is interesting to mention that in the first presented experiment the Ridge Classifier had the poorest results.

Fig. 2. *Colonoscopy images; first two with cancer and the last without.*

4.4. Anomaly detection in esophageal measurements

In this experiment **[14, 15]** we analysed acoustic 2D images from a device called High Resolution Manometry (HRM). (**Figure 3**). This device is used for the detection of abnormal functioning of esophagus in the process of swallowing.

The goal in this case was twofold:

– to identify wrong positioning of the probe in the esophagus;
– classify diseases related with the swallowing process.

In each case a set of images obtained from a HRM device were labelled by trained specialists as good of wrong (bed positioning) images and images representing different diseases.

The difficulty in this case was the relatively small number of labelled images available for training and that sometimes, even for the human observer, it was difficult to discriminate between wrong positioning of the probe and a given disease. Because of this the quality parameters are not as good as in the previous experiments, but still very good in this context. In the case of probe positioning error detection, the precision obtained was 90,67% and the F1 parameter was 84.21%. For classification of diseases we used a classical algorithm present in the medical literature.

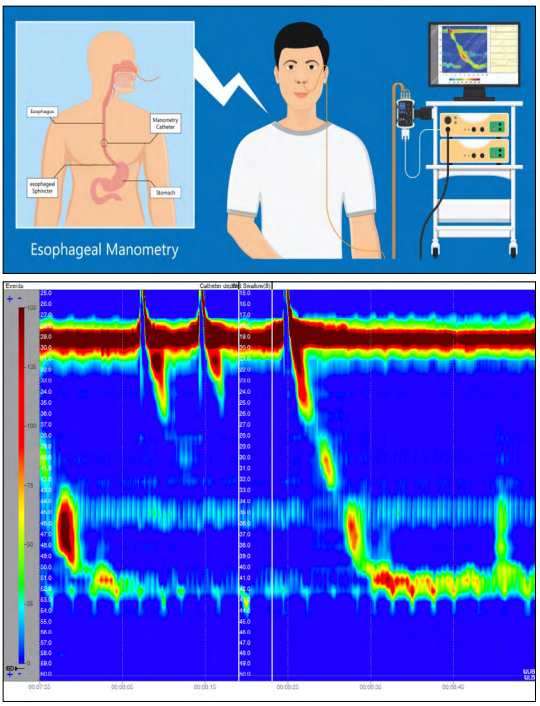

Fig. 3. *HRM measurement- device and obtained 2D image.*

5. Future work

In order to provide access to our anomaly detection platform for a wider category of specialists from different domains we intend to deploy the platform on a cloud infrastructure. A first version was successfully deployed on a private cloud, but for open access services a public cloud is needed. The cloud deployment can benefit from higher computing resources, that may contribute to the reduction of time needed for the automatic selection and training of anomaly detection algorithm.

We also intend to diversify the domains in which anomaly detection and our platform is used. We also intend to add to the platform new artificial intelligence algorithms as well as signal processing detection methods.

6. Conclusions

As showed in this paper, anomalies play an important role in the lifetime of an application. Automatic anomaly detection is more and more a mandatory functionality of a system, mainly for those cases when systems have an autonomous life. It is also important for safety-critical, fault-tolerant and self –healing systems. Anomaly detection techniques can be used also in different medical areas in order to identify diseases as deviations from the normal physiological behaviour of human body.

A specialist in a given domain needs an efficient tool in order to identify and separate or eliminate anomalies for datasets. For this purpose, we developed a configurable platform that contains multiple procedures necessary in the process of data analysis and anomaly detection.

The most important part of the platform is the AutomaticAI tool that automatically selects the best performing classification algorithm for a given dataset. The efficiency and versatility of this automatic method was proved through a number of experiments performed in a variety of domains: water infrastructures, medical imagery, covid detection, etc.

References

[1] Chandola V. , Banerjee A., Kumar V.: *Anomaly Detection: A Survey.* ACM Computing Surveys, 41/3. (2009) 1–58. https://dl.acm.org/doi/10.1145/1541880.1541882

[2] Agrawal S., Agrawal J.: *Survey on Anomaly Detection using Data Mining Techniques.* Procedia Computer Science, 60/1. (2015) 708–713. https://doi.org/10.1016/j.procs.2015.08.220

[3] Gupta M., Gao J., AggarwalC. C. , Han J.: *Outlier Detection for Temporal Data: A Survey*. IEEE Transactions on Knowledge and Data Engineering, 26/9. (2014) 2250–2267. https://doi.org/10.1109/TKDE.2013.184

[4] Hodge V. J., Austin J.: *A Survey of Outlier Detection Methods.* Kluwer Academic Publishers, 2004.

[5] Czako Z., Sebestyén Gy., Hangan A.: *Colorectal image classification with transfer learning and auto-adaptive artificial intelligence platform*. In: Trends and Innovations in Information Systems and Technologies 28. Springer International Publishing, 2020. 534–543.

[6] Czako Z., Sebestyén Gy., Hangan A.: *AutomaticAI–A hybrid approach for automatic artificial intelligence algorithm selection and hyperparameter tuning.* Expert Systems with Applications, 182. 2021. https://doi.org/10.1016/j.eswa.2021.115225

[7] Czako Z., Sebestyén Gy., Hangan A.: *Artificial Intelligence Algorithms Selection and Tuning for Anomaly Detection.* Computational Intelligence: International Joint Conference, IJCCI 2018 Sevilla, Spain. Revised Selected Papers, 2021.

[8] Adankon M. M., Cherirt M.: *Model Selection for LS-SVM: Application to Handwriting Recognition.* Pattern Recognition, 42/12. (2009) 3264–3270. https://doi.org/10.1016/j.patcog.2008.10.023

[9] Sebestyén Gy., Hangan A., Czako Z., Kovács Gy.: *A taxonomy and platform for anomaly detection.* 2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 2018. https://doi.org/10.1109/AQTR.2018.8402710

[10] Pradeepmon T., Panicker V., Sridharan R..: *Parameter selection of discrete particle swarm optimization algorithm for the quadratic assignment problems.* Procedia Technology, 25. (2016) 998–1005. https://doi.org/10.1016/j.protcy.2016.08.199

[11] Simsek A., Kara R.: *Using Swarm Intelligence Algorithms to Detect Influential Individuals for Influence Maximization in Social Networks*. Expert Systems with Applications, 114. (2018) 224–236. https://doi.org/10.1016/j.eswa.2018.07.038

[12] Sebestyén Gy., Hangan A., Czako Z.: *Anomaly detection in water supply infrastructure systems.* 23rd International Conference on Control Systems and Computer Science (CSCS), 2021. https://doi.org/10.1109/CSCS52396.2021.00064

[13] Czako Z., Sebestyén Gy., Hangan A.: *COVID-19 Preliminary Patient Filtering based on Regular Blood Tests using Auto-Adaptive Artificial Intelligence Platform.* IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), 2020. https://doi.org/10.1109/ICCP51029.2020.9266277

[14] Popa Ș. L., Surdea-Blaga T., Dumitrașcu D. L., Sebestyén Gy., et al.: *Automatic Diagnosis of High-Resolution Esophageal Manometry Using*

Artificial Intelligence. Journal of Gastrointestinal & Liver Diseases, 31/4. (2022) 383–389. https://doi.org/10.15403/jgld-4525

[15] Surdea-Blaga T., Sebestyén Gy., Czako Z., Hangan A., et al.: *Automated Chicago Classification for Esophageal Motility Disorder Diagnosis Using Machine Learning.* Sensors, 22/14. (2022). https://doi.org/10.3390/s22145227