Deep Learning-based Approach to Smart Factory: Methods and Applications

Van Quan Nguyen*, Linh Van Ma*, and Jinsul Kim**

요 약

스마트 제조는 수집, 분석, 시각화 및 의사 결정에서의 시스템 성능 향상을 의미합니다. 우리는 장치 기반 및 네트워크 기반 기술뿐만 아니라 센서 데이터 조작에 있어 고급 프로세스를 시작하기 위해 기계 학습을 널리 사용하는 것을 목격 해 왔습니다. 이 글에서는 산업용 시스템의 센서 데이터를 분석하기위한 LSTM 아키텍처 기반의 반복적 인 신경망을 제시합니다. 시계열 데이터는 타임 라인에 따라 개체의 상태에 반영되기 때문에 많은 시스템에서 중요한 부분이 되었습니다. 왜 우리가 반복적 인 신경망을 데이터의 순서를 탐색하는 솔루션으로 사용하는지에 대한 주된 이유. LSTM 신경 회로망의 응용을 증명하기 위해 이상 검출 알고리즘을 제안하고 여러 데이터 집합에서 수행한다.

Abstract

Smart manufacturing refers to using advanced techniques in collecting, analyzing, visualization and decision making in management to improve system’s performance. We have been witnessing the widespread of machine learning to launch advanced process in the manipulation of sensor data as well as managing devices and productions based on network technologies. This article presents recurrent neural network with LSTM architecture-based approach to analyzing sensor data for the industrial system. Using time series data has become a critical part of many systems because this explored information reflect the state of objects according to the timeline. This is the major reason why we use Recurrent Neural Networks as a solution to explore the sequence of data. In order to prove the application of LSTM neural network, anomaly detection algorithm is proposed and perform on time series datasets.

Key words

Deep Learning, Long Short-Term Memory (LSTM), Time series Data, Anomaly detection, SCADA

Ⅰ. Introduction

In the real-world, mechanical devices such as engines, vehicles, even body part of human are typically instrumented by the various physical sensor to recorded the behavior and health of objectives. For monitoring status during operation, we would like to be able to discriminate between the normal and abnormal state of a considered system [1]. For example, we analyze the signal from sensor built-in smart factory to recognize that what is going wrong, need to be repaired.

* School of Electronics and Computer Engineering, Chonnam National Univ., Yongbong-ro, Buk-gu, Gwangju 500-757

** Corresponding author

This study discussed a machine learning based approach to explore sensor data. Since the objective is time series data, LSTM-RNN based model [2] is the best solution. Such a model play an essential role in anomaly detection applications. Generally, the usage anomaly detection is very helpful in behavior analysis or support for other kinds of analysis like detection, identification, and prediction of the occurrence of these anomalies.

The rest of the paper is constructed as follows: Section 2 is the review of data-driven intelligence. Section 3 introduction general framework and application of anomaly detection using deep learning. Next, the visualization and performance are presented. Finally, Section 5 is the conclusion.

II. Deep learning based approach

Machine learning is a technique in which programs iteratively learn from data instead of being static. It is used to build an input-based model that can be used to make predictions or decisions. These system learn from the data and can adjust themselves accordingly through learning feature to make better performance.

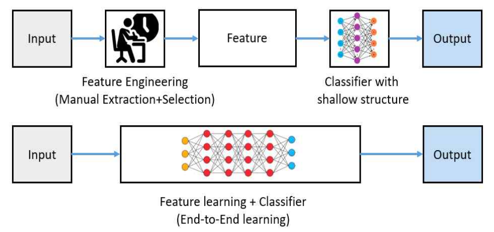


Figure 1: a) Traditional machine learning b) deep learning based approaches

As shown in Figure 1, the deep architecture includes feature learning and classification stage, it seems more advantaged than traditional machine learning based method since we do not need design the feature extraction engineering. In conventional machine learning, the system requires feature engineering to transform raw input data into appropriate domains or suitable form to extract handcrafted feature [3]. Generally, the feature selection stage will spend the most time in the process of development of machine learning system. These extracted features are fed into classification phase. Overall, deep learning is an end-to-end learning structure with the minimum human inference, and the parameters of deep learning model are trained jointly [3].

III - Applications of deep learning in Smart Factory

3.1. Overview framework

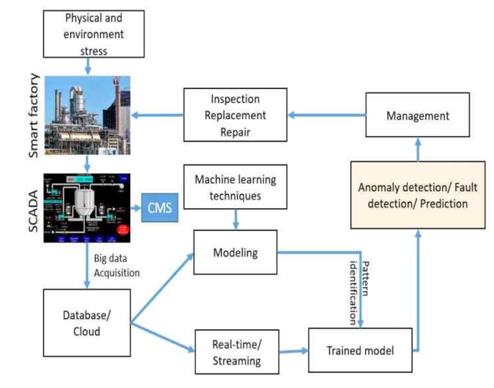


Figure 2: A general framework with machined learning based applications

Figure 2 is proposed general framework for anomaly detection integrated into the smart industrial factory. As you known, the industrial equipment always is installed in environmental stress, the anomaly event can happen during operation. In order to maintain manufacture system efficiency, process data for smarter decisions and mitigate downtime SCADA [4] systems have become crucial for the industrial organization. They help to control industrial processes both local and remote location. As shown in the diagram, SCADA block directly interacts with devices such as sensors, valves, pumps, motors to monitor, gather, record event into a database as well as support for processing real-time data. Interaction can perform through human-machine interface (HMI) software. In the experiment, we use a solution for visualization event from the database. This framework also has machine learning based anomaly detection on time series data from a smart factory.

3.2 Anomaly detection architecture

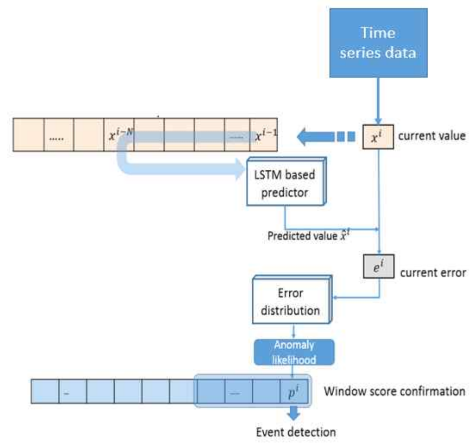


Figure 3: Flowchart of Anomaly detection

Figure 3 illustrates the flowchart of anomaly detection [5] based on two models namely LSTM based prediction model and error-distribution model. LSTM network has memory blocks that are connected through layers {64, 256, 100}. Then, it was pre-trained on normally dataset. The LSTM based prediction model refers to observed history data to estimate incoming data point in the time-series. The prediction errors are modeled to fit parameters (mean, standard deviation) of a Gaussian error distribution using maximum likelihood estimation. Event detection will be verified via confirmation stage based on the number of event candidates in the sliding window.

IV. Visualization and Performance

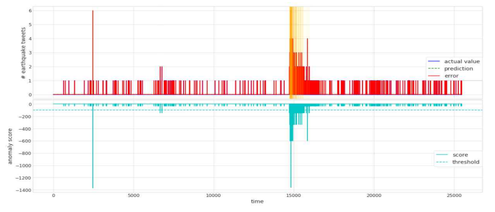
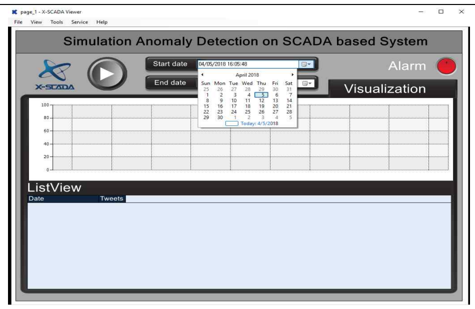
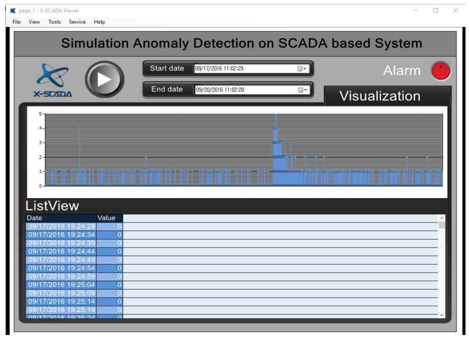


Figure 4: Illustration of anomaly detection on time series data

Figure 4 is the performance of anomaly event detection algorithm using LSTM recurrent neural network on social sensor data. Yellow-color maker denoted the occurrence of an event on the timeline.



a- Query data from database using GUI



b- Visualization data in time line and table form (list view)

Figure 5: Visualization using X-SCADA solution [6]

Ⅴ. Conclusions

We introduction the machine learning in industrial system and explore LSTM based predictor operation on time series data to learn temporal signal feature for detecting anomaly pattern. Apparently, without feature engineering, deep learning provide advanced analytics and offer great potential in real applications especially as smart manufacturing. In the future, we implement our approach to big data framework to process the large volume of data from multiple sensor sources.

Acknowledgement

This work (Grants No. C0513295) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2017. Also, this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (MEST)(Grant No. NRF-2017R1D1A1B03034429).

References

[1] V. Chandola, A. Banerjee and V. Kumar, Anomaly detection: A survey. ACM computing surveys (CSUR), (2009), Vol.41, No.3, pp.15.

[2] S. Hochreiter and J. Urgen Schmidhuber, Long Short-Term Memory. Neural Computation, (1997), Vol. 9, No. 8, pp. 1735-1780.

[3] J. Wang, Y. Ma, L. Zhang, R. X. Gao, & D. Wu, Deep learning for smart manufacturing: Methods and applications, Journal of Manufacturing Systems, (2018).

[4] S. D. Antón, D. Fraunholz, C. Lipps, F. Pohl, M. Zimmermann and H. D. Schotten, Two decades of SCADA exploitation: A brief history. In Application, Information and Network Security (AINS), 2017 IEEE Conference, (2017), IEEE, pp. 98-104.

[5] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, Long short term memory networks for anomaly detection in time series. Proceedings (2015), pp. 89.

[6] Home website: http://www.xisom.com