Incremental anomaly detection using contextual bandit and decision tree

Youngin Kwon
Artificial Intelligence of Graduate School
Ulsan National Institute of Science and Technology
Ulsan, 44919
Republic of Korea
younginkwon@unist.ac.kr

Abstract

The developments of processing units and storing data make advances in existing learning methods based on analysis to machine learning(ML) and deep learning(DL)-based methods. Specifically, the need to utilize these approaches keep increasing for reducing production cost and enhancing product quality in the real industrial area. Among the research area for industry field, anomaly detection also has improved techniques by ML and DL algorithms. Most existing detection algorithms however are operated as batch-based algorithm, which runs using gathered data under fixed period and regularly by several minutes. In real industrial data, there are sudden drift that does not previously occur and real-time data for an interval before updating. We apply an incremental anomaly detection approach using incremental decision regression tree(FIMT-DD) and contextual multi-armed bandit(CMAB). It will be compared with existing methods like support vector machine and DNN under injection molding dataset for real industrial problem.

1 Introduction

The developments of processing units and storing data make advances in existing learning methods based on analysis to machine learning(ML) and deep learning(DL)-based methods. Specifically, the need to utilize these approaches keep increasing for reducing production cost and enhancing product quality in the real industrial area. Among the research area for industry field, anomaly detection also has improved techniques by ML and DL algorithms. Most existing detection algorithms however are operated as batch-based algorithm, which runs using gathered data under fixed period and regularly by several minutes. In real industrial data, there are sudden drift that does not previously occur and real-time data for an interval before updating. Ding, Li, and Liu implies that the environment where new type of anomalies arises overtime is not capable for batch setting [1].

To handle unexpected drift of anomalies, we apply an incremental detection algorithm, which combines two adaptive methods, incremental regression tree learner and contextual multi-armed bandit algorithm(CMAB) by Soemers et al. in real industrial dataset [2]. It is designed for semi-supervised learning and uses fast incremental model trees with drift detection(FIMT-DD) as incremental tree model by Ikonomovska [3]. FIMT-DD is the regression tree model to capture concept drift sequentially, and multi-armed bandit algorithm is a method which interacts with defined environment by reward as one of the sequential decision making algorithm. The main advantage of combined method is real-time learning by assigning pseudo-label and updating tree iteratively compared with representative algorithms for semi-supervised learning. Furthermore, our CMAB uses doubly robust estimator as its reward for the problem that has small amount of labeled data of semi-supervised learning [4]. Injection molding dataset is used for measuring performance of proposed method and baseline algorithms as real industry dataset.

36th Conference on Neural Information Processing Systems (NeurIPS 2022).

2 Related Work

2.1 Anomaly Detection

Anomaly detection is a research area for identification of rare items, events or observations which deviate significantly from the majority of the data and do not conform to a well defined notion of normal behaviour [5]. It recently spreads many applications such as cyber-security intrusion detection, fraud detection, and fault detection [6]. There are three broad types of anomaly detection as supervised, semi-supervised, and unsupervised approaches. As the solution of those problem, there are ML-based algorithms like support vector machine, random forest, and principal component analysis(PCA) and DL-based algorithms such as deep neural network(DNN) and autoencoder(AE).

2.2 Decision Tree

Decision Tree is the algorithm easily explainable by splitting observations into decision nodes of tree. Basic tree model is classification and regression tree(CART) model which uses a partitioning criteria to compose two children nodes with as uniform amounts of data as possible by entropy or gini index [7]. It has advantages as intuitive and common algorithm for classification and regression simultaneously, but it suffers overfitting problem. To resolve overfitting, ensemble methods are proposed to generate result by concatenating different trees as bagging, boosting, and stacking. Random forest is bagging-based method to combine all independent trees in equal, and there are many boosting based tree learned by weak learner such as Adaboost, gradient boosting tree(XGBoost and LightGBM).

Basic tree models are also batch-based algorithms that use static data until executing model like general prediction model. However, they are not adequate for the situation where real-time drifts occurs, because batch algorithms will spend a lot of time to update by increasing amount of data. So, there are incremental decision tree models to handle concept drift that means target variable changes in adversarial manner over time. We use fast incremental model trees with drift detection(FIMT-DD) as incremental tree model by Ikonomovska [3]. It formulates the tree model which gets individual data sequentially and updates sub-trees when criteria is satisfied.

2.3 Multi-Armed Bandit(MAB)

Multi-armed bandit algorithm(MAB) is a method which interacts with defined environment by reward as one of the sequential decision making algorithm. It is designed by Lai and Robbins as adaptive decision making problem [8, 9]. The agent of bandit chooses one arm by its criteria and observes reward of the arm under the situation where there are fixed candidates for individual timesteps. In every timestep, the reward can be only obtained selected arm called as partial feedback, and learning occurs adaptively by monitored feedback. The objective of bandit problem is to maximize cumulative sum of rewards during whole the time. To accomplish this objective, algorithm needs to overcome exploitation and exploration trade-off occurred by uncertainty of expected values. Moreover, we assume that rewards of defined arms follow certain distribution with unknown expected value as stochastic MAB problem. Recently, MAB uses many real life applications in healthcare, finance, recommender system [10].

The basic MAB problem has limitation to utilize partial feedback only, although there are contextual information of news article in newspaper recommender problem [11]. The problem with contextual information for MAB problem is called contextual MAB(CMAB). As contexutal stochastic MAB problem, Li et al. adopts LinUCB algorithm which considers expected value of each arm is linear combination between context vectors of actions and unknown parameter by Chu et al. [12]. LinUCB algorithm is a variant of UCB algorithm for stochastic MAB problem, and UCB algorithm is developed under optimism-in-the-face-of-uncertainty(OFU) principle to select arm based on upper confidence bound(UCB) that composes the estimate of expected value and exploration bonus. UCB is proper algorithm to consider trade-off simultaneously, because the estimates represent exploitation of arm and exploration bonus decreases to pull specific arm more. LinUCB is an algorithm to modify exploitation and exploration to linear payoff function. We select LinUCB algorithm as contexutal stochastic MAB problem for incremental anomaly detection algorithm.

3 Problem Setting

Our agent observes $T(T_{train} + T_{unlabel})$ data composed by T_{train} number of data for train from labeled observations and $T_{unlabel}$ number of data from unlabeled observations, and there are T_{test} data to evaluate performance from labeled data with train data. Each observation has d-dimensional contextual information $\mathbf{x}_t$ whose there are characteristics about process each timestep t, and there is label $l_t \in \{0, 1\}$ which means anomaly. Furthermore, there is q_t as the quantity of defective product to indicate the degree of anomaly in time t. The reward $r(t)$ for regression tree and CMAB algorithm is $q_t * l_t$, where it has non-negative value to indicate the level of anomaly. We use random forest regressor to fill error quantity for labeled data and define rewards to use estimated quantity, because the all q_t value of labeled data is missing.

4 Method

Our proposed method is based on Seomers et al using credit card transaction dataset [2]. They formulate the fraud detection problem as CMAB with decision tree where leaves are the arms of bandit and reward is a degree of fraud transaction by reflecting the amount of transaction. Furthermore, we apply doubly robust estimator as its pseudo-reward to deal with a problem that has small amount of labeled data for semi-supervised learning [4]. It makes that CMAB can fully learn all observations when chosen arms are not the corresponding arm of each timestep as well. We apply the defective product quantity to express a degree of out-of-control process for injection molding dataset.

The pseudo code of our approach is Algorithm 1. Before executing learning process, the regression tree must be trained from labeled data, and CMAB is trained while there is true label l_t of each timestep. In semi-supervised phase, pseudo-label is assigned by CMAB, and tree and bandit models are trained simultaneously. Allocating pseudo-label is to compare clustering result by CMAB with maximum averaging reward node of trained tree, because observations are grouped as one of leaf nodes by the average of components in regression tree model. The CMAB algorithm needs to re-train when incremental tree splits, because MAB assumes fixed number of arms. The iterative train and re-train procedure is repeated until whole time T. CMAB has hyperparameter K as $[3, 4, 5, 6]$ that restrict maximum number of leaf to prune regression tree. Moreover, it takes 5 bootstrap iterations, because there is randomness within CMAB model. The result of detected anomaly is generated by hard voting method of bootstrapped CMABs and can be changed to adjusting threshold within 1 to 5.

5 Experiment

5.1 Dataset

Injection molding is one of the methods for plastic molding by injecting the heated thermoplastic into cavity of molds. It prefers to molding process, because there are several advantages compared with other molding methods. It consists of three phases as filling, pressurisation, and compensating phase. In detail, there are 8 procedures as a cycle of process. This dataset represents real industry data about wind shield side molding of Hyundai Avante(Elantra) CN7 as CN7 and Genesis G80 as RG3. There are quality characteristics during a cycle of process such as time, position, and temperature of production component, and it has a label whether the cycle is anomaly. There are 1425 and 52547 observations for labeled and unlabeled data for CN7. There are 1182 and 37477 observations for labeled and unlabeled data for RG3. The labeled data for CN7 and RG3 are separated as train and test set as (997, 428) for CN7 and (827, 355) for RG3 to evaluate models.

5.2 Result

Proposed algorithm is evaluated with baselines for semi-supervised learning such as support vector machine(SVM) and deep neural network(DNN). Our method figures out anomalies compared with other baseline algorithms, but baselines have chances to improve by tuning their hyperparameters. However, there is limitation where CMAB cannot have consistent result despite of several bootstrapping. So, we adjust the level of hard voting by m within 1 to 5. Our combined approach does not perform better than DNN about CN7 data, but it finds 7 of 8 anomalies with 33% less time than DNN. Proposed method could be suitable at real-time detection as long as it overcomes the problem at performance.

Algorithm 1 LinUCB-based anomaly detection with incremental regression tree

Learn incremental regression tree $\mathcal{T}$ having $\mathcal{T}_{leaf} \geq 2$ by $(X_{train}, r(t))$
Set $\delta > 0, K > 0, k = \mathcal{T}_{leaf} > 2, A = I_{k \times d}, f = \mathbf{0}_{k \times d}, l = l_{train}$
while $t < T$ **do**
    $\mathcal{M}_{UCB} = LinUCB(k, d, \delta)$
    for $t = 1, \ldots, T$ **do**
        $\hat{\theta}_t = A^{-1}b$
        Observe observation $\mathbf{x}_t \in \mathbb{R}^d$, $l_t \in \{\text{None}, 0, 1\}$ at t
        for $a = 1, \ldots, k$ **do**
            $UCB_a(t) = \hat{\theta}_t^T \mathbf{x}_{t,a} + \alpha \sqrt{\mathbf{x}_{t,a}^T A^{-1} \mathbf{x}_{t,a}}$
        end for
        Choose action $a_t = argmax_a UCB_a(t)$
        if l_t is not None **then**
            Observe reward $r_{a_t}(t)$ with true label l_t
        else
            Observe reward $r_{a_t}(t)$ with true pseudo-label l'_t

$$\begin{cases} l'_t = 1 & \text{if } a_t = argmax_{leaf} \mathcal{T}_{leaf} \\ l'_t = 0 & \text{if } a_t \neq argmax_{leaf} \mathcal{T}_{leaf} \end{cases}$$

        end if
        Observe pseudo-reward $r_{a_t}(t)' = \left\{1 - \frac{\mathbb{I}(i=a_t)}{\pi_i(t)}\right\} \mathbf{x}_{t,i}^T \hat{\theta}_t + \frac{\mathbb{I}(i=a_t)}{\pi_i(t)} r_{a_t}(t)$
        Append pseudo-label at $l' \leftarrow l'_t$
        if $k < \mathcal{T}_{leaf} < K$ **then**
            Update tree $\mathcal{T}$ by $(\mathbf{x}_t, r(t))$
            $l \leftarrow l + l'$
            break
        end if
        Update $\mathcal{M}_{UCB}$ by $(\mathbf{x}_t, r(t))$
    end for
end while

Table 1: Overall result of proposed and baseline algorithms

Metric	CN7			RG3		
	SVM	DNN	CMAB ($K = 4, m = 2$)	SVM	DNN	CMAB ($K = 3, m = 4$)
Accuracy	0.98	0.98	0.80	0.98	0.98	0.98
Precision	0.0	0.60	0.08	0.0	0.0	0.0
Recall	0.0	0.38	0.88	0.0	0.0	0.0
Elapsed time(s)	0.01	542	144	0.01	632	141

6 Conclusion

In our paper, we refer the importance of incremental anomaly detection method for real industrial field where concept drift occurs by testing injection molding dataset. So, we propose LinUCB-based anomaly detection with incremental regression tree model. The proposed model implies suitable approach as real-time detection algorithm which spends much less time, although it does not stable by serveral iterations. There are further ways to develop this model by adding policy to swap leaf node when new node is generated at maximum amount of leaf nodes replace FIMT-DD tree learner with other tree models.

References

[1] Kaize Ding, Jundong Li, and Huan Liu. Interactive anomaly detection on attributed networks. In *Proceedings of the twelfth ACM international conference on web search and data mining*, pages 357–365, 2019.

[2] Dennis Soemers, Tim Brys, Kurt Driessens, Mark Winands, and Ann Nowé. Adapting to concept drift in credit card transaction data streams using contextual bandits and decision trees. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 32, 2018.

[3] Elena Ikonomovska, Joao Gama, and Sašo Džeroski. Learning model trees from evolving data streams. *Data mining and knowledge discovery*, 23(1):128–168, 2011.

[4] Wonyoung Kim, Gi-soo Kim, and Myunghee Cho Paik. Doubly robust thompson sampling with linear payoffs. *Advances in Neural Information Processing Systems*, 34:15830–15840, 2021.

[5] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):1–58, 2009.

[6] Charu C Aggarwal. An introduction to outlier analysis. In *Outlier analysis*, pages 1–34. Springer, 2017.

[7] Leo Breiman, Jerome H Friedman, Richard A Olshen, and Charles J Stone. *Classification and regression trees*. Routledge, 2017.

[8] Herbert Robbins. Some aspects of the sequential design of experiments. *Bulletin of the American Mathematical Society*, 58(5):527–535, 1952.

[9] Tze Leung Lai, Herbert Robbins, et al. Asymptotically efficient adaptive allocation rules. *Advances in applied mathematics*, 6(1):4–22, 1985.

[10] Djallel Bouneffouf, Irina Rish, and Charu Aggarwal. Survey on applications of multi-armed and contextual bandits. In *2020 IEEE Congress on Evolutionary Computation (CEC)*, pages 1–8. IEEE, 2020.

[11] Lihong Li, Wei Chu, John Langford, and Robert E Schapire. A contextual-bandit approach to personalized news article recommendation. In *Proceedings of the 19th international conference on World wide web*, pages 661–670, 2010.

[12] Wei Chu, Lihong Li, Lev Reyzin, and Robert Schapire. Contextual bandits with linear payoff functions. In *Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics*, pages 208–214. JMLR Workshop and Conference Proceedings, 2011.