Обнаружение аномалий в технологических процессах

Опушнев Степан, 2022 г.

Аномалия или неисправность?

Аномалия – событие или период в данных, который очень редко встречается и значительно отличается от большинства данных.

Неисправность - недопустимое отклонение по меньшей мере одной характеристики или переменной системы.

Будем говорить о аномалии, но подразумевать неисправности.

Технологический процесс

- Многомерный временной ряд
- Равные интервалы времени
- Измеряемые значения (датчики) и управляющие воздействия (актуаторы)
- Непрерывные и дискретные признаки
- Неизвестная, нелинейная связь между признаками
- Как правило, доступно только «нормальное» состояние процесса

Какие именно процессы

- Относительно небольшие, но многочисленные:
  - теплообменники нагрева и охлаждения
  - регулирующие узлы (давления, температуры и т.д.)
  - вентиляционные установки
  - процессы подготовки (воды, сжатого воздуха и т.д.)
- Недостаточно важны, чтобы выделять много времени
- Достаточно важны, чтобы исправность была важна
- Не требуется мгновенная реакция, но задержка играет роль

Выбор метрики

- Задача несбалансированной бинарной классификации:
  - точность (precision) – доля правильных предсказаний среди всех предсказаний
  - полнота (recall) – доля правильных предсказаний среди всех аномалий
  - f-мера – среднее гармоническое точности и полноты
- Основная метрика будет F1-мера: наибольшая область определения, усредненная, можно сместить баланс

$$F_1 = \frac{2 \times TP}{2 \times TP + FP + TN}$$

Особенности подсчёта метрики

- Данные делятся на интервалы (15 минут по умолчанию)
- Значение TP, FP, TN определяется на интервале в целом
- Метрика считается для временного ряда
- Метрика усредняется по набору временных рядов

Данные

	GHL (Gasoil Heating Loop)	TEP (Tennessee Eastman Process)		SWaT (Secure Water Treatment)
Источник данных	Kaspersky Lab	Harvard Dataverse	Kaspersky Lab	iTrust CRCS
Тип	Моделирование	Моделирование	Моделирование	Реальный процесс
Признаки	12	51	52	51
Обучение	1 x 400+ часов	500 x 25 часов 10000 x 25 часов	200 x 120 часов 336 x 120 часов	1 x 140 часов
Тест	48 x 50+ часов	500 x 48 часов 10000 x 48 часов	142 x 120 часов	1 x 150 часов
Типов аномалий	2	20	4	36

Как выглядят процессы?

Здесь будет несколько картинок

Критерии выбора алгоритмов

- Быстродействие (алгоритма, доступной имплементации)
- Нетребовательность к ресурсам (CPU, RAM, HDD)
- Обучение по нескольким файлам (partial_fit, warm_start и т.п.)
- Возможность дообучения
- Хорошая работа с параметрами по умолчанию
- Интерпретируемость

Классификация алгоритмов

- Ошибка представления:
  - запоминание границ
  - метод главных компонент (PCA)
  - решающие деревья (Isolation Forest, Robust Random Cut Forest)
- Ошибка предсказания:
  - линейные
  - нелинейные

Стратегия исследования

На GHL и TEP:

- Проверить работоспособность алгоритмов
- Подобрать хорошо работающие параметры по-умолчанию
- Проверить ансамблирование
- Подобрать параметры ансамблирования

На GHL, TEP, SWaT:

- Провести финальную проверку

DirectLimitWatchman

Идея:

- Запоминает граничные значения признаков
- Считает неисправностью значения, выходящие за границы

Результат:

- Предсказание по каждому признаку

PcaLimitWatchman

Идея:

- Преобразует данные в пространство главных компонент
- Запоминает граничные значения
- Считает квадратичную ошибку представления (PMSE)
- Считает неисправностью значения главных компонент и PMSE, выходящие за границы
- Предсказание по каждой компоненте и PMSE

IsoForestWatchman

Идея:

- Данные случайно разбиваются по случайным признакам
- Строится лес разбивающих деревьев
- Чем проще отделить наблюдение, тем больше вероятность, что это аномалия

Результат:

- Предсказание аномалии общее

LinearPredictWatchman

Идея:

- Значение признака предсказывается, как линейная комбинация признаков на предыдущем наблюдении
- Предсказываются только непрерывные признаки
- Предсказатель по каждому признаку обучается независимо по алгоритму линейной регрессии
- Запоминает границы ошибки предсказания и PMSE
- Считает аномалией значения, выходящие за границы

Результат:

- Предсказание по каждому непрерывному признаку и PMSE

DeepPredictWatchman

Идея:

- Значение текущего наблюдения предсказывается по нескольким предыдущим наблюдениям
- Предсказатель строится по принципу рекуррентной нейронной сети (LSTM)
- Запоминает границы ошибки предсказания и PMSE
- Считает аномалией значения, выходящие за границы

Результат:

- Предсказание по каждому признаку и PMSE

Этапы обучения

1. По всем обучающим файлам проводим предобучение (изучение данных, подстройка параметров алгоритма, обучение скейлера)
2. По всем обучающим файлам проводим обучение (обучение основного алгоритма детекции/предсказания)
3. По всем обучающим файлам проводим постобучение (запоминание границ признаков, границ ошибок представления/предсказания)

Ансамблирование, роль отсечки

Отдельный сторож может хорошо работать на одних процессах и плохо на других. Мы хотим объединить предсказания, чтобы получать стабильно хороший результат.

Ансамбль:

- Предсказывает каждым сторожем
- Считает по каждому семплу количество предсказаний аномалии
- Считает семпл аномалией, начиная от некоторого количества

Отсечка может выступать в качестве параметра уверенности:

- Чем больше отсечка, тем больше мы уверены в положительном предсказании, но тем больше пропускаем аномалии
- Чем меньше отсечка, тем меньше мы уверены в положительном предсказании, но тем меньше пропускаем аномалии

Отсечка может быть подстроена, при добавлении новых методов в ансамбль.

Результаты (F1-мера)

	GHL	TEP Harvard	TEP Kaspersky	SWaT
DirectLimitWatchman	0.3792	0.6821	0.4154	0.3257
PcaLimitWatchman	0.3882	0.6007	0.2570	0.1611
IsoForestWatchman	0.0508	0.5252	0.0689	0.2679
LinearPredictWatchman	0.0289	0.8120	0.4438	0.2134
DeepPredictWatchman	0.3224	0.7167	0.3917	0.3094
WatchSquad(threshold=4)	0.4950	0.7271	0.4104	0.3479

Выводы

- Подготовил датасеты для обучения детекции аномалий
- Сформулировал метрику
- Выбрал и проверил методы обнаружения аномалий
- Собрал ансамбль методов, который можно использовать в реальной задаче

Пути улучшения

Общие:

- Считать ошибки более высокого порядка $|e|^n, n > 2$
- Сглаживать ошибки (например EWMA)
- Ансамблировать предсказания с некоторыми весами в зависимости от степени доверия к методу
- Предсказывать на несколько шагов
- Добавлять новые методы в ансамбль (автоэнкодеры, прочие изолирующие деревья, one-class-SVM, модификации PCA, FDA, PLC, CVA и т.д.)

Зависимые от процесса:

- Добавлять в датасет значения уставок процесса
- Генерировать признаки по физическому смыслу
- Генерировать признаки по статистической значимости, если есть примеры аномалий
- Ансамблировать предсказания с некоторыми весами, автоматически подбирая веса (классификатор линейный, на деревьях), если есть примеры аномалий
- Оценивать ошибки предсказания/представления с помощью моделей, учитывающих физический смысл процесса