Обнаружение аномалий в технологических процессах

https://github.com/sau114/skillfactory_rds/tree/main/module_final

Опушнев Степан, 2022 г.

Аномалия или неисправность?

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

Неисправность – неожиданное и недопустимое отклонение по меньшей мере одной характеристики или переменной системы.

Мы говорим аномалия, подразумеваем – неисправность.

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
  - вентиляционные установки
  - процессы подготовки
- Недостаточно важны, чтобы выделять много времени
- Достаточно важны, чтобы следить за исправностью
- Не требуется мгновенная реакция, но задержка имеет значение

Выбор метрики

- Задача несбалансированной бинарной классификации:
  - точность (precision)
  - полнота (recall)
  - f-мера – среднее гармоническое точности и полноты
- Основная метрика будет F1-мера:
  - наибольшая область определения
  - среднее, но не среднеарифметическое
  - можно сместить баланс (Fβ-мера)

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

Особенности подсчёта метрики

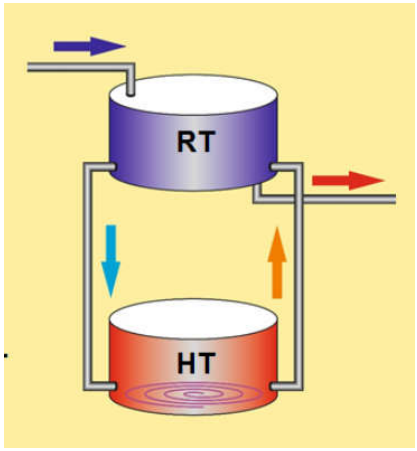
Чтобы учесть влияние задержки обнаружения и приблизить к возможному применению:

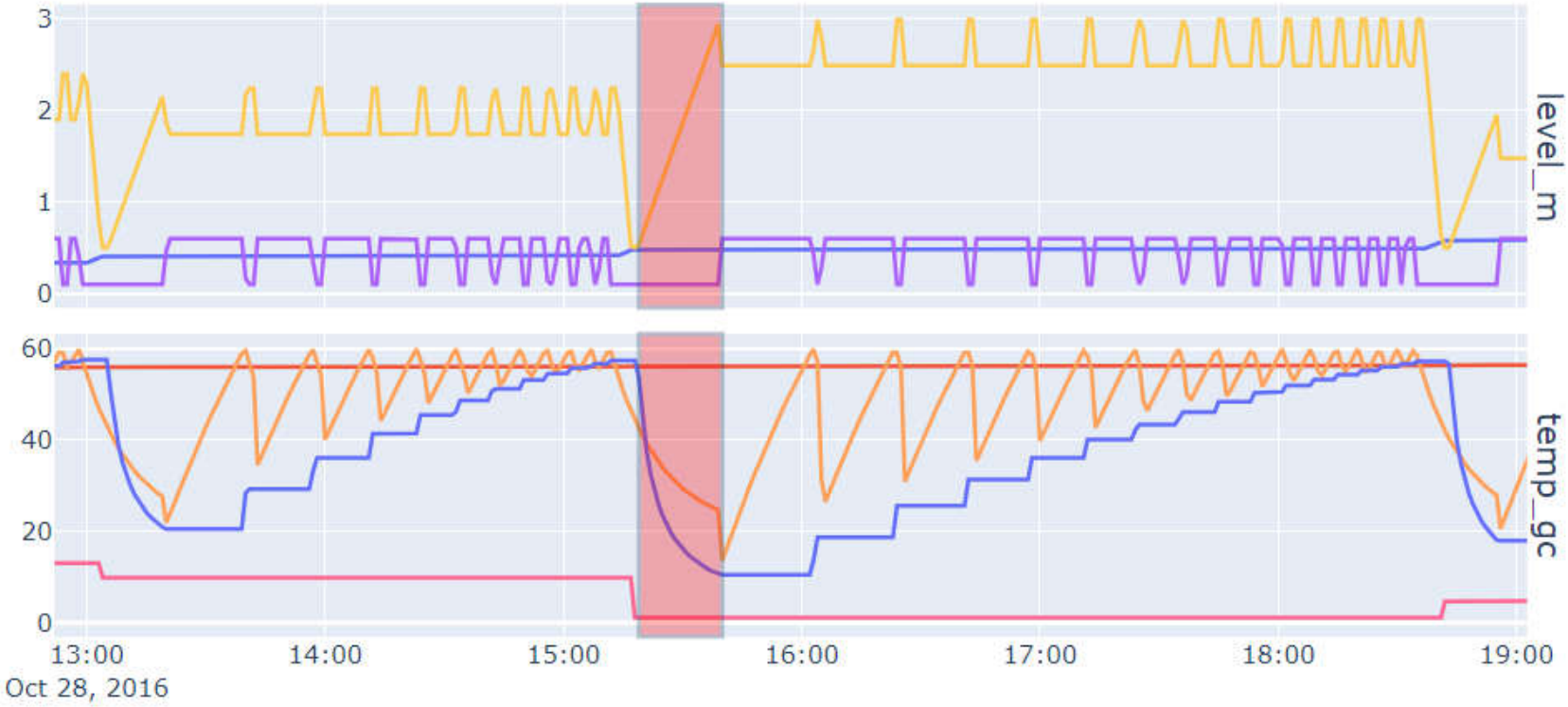
- Временной ряд делится на интервалы (по 15 минут)
- Значение TP, FP, TN определяется на интервале в целом
- Метрика считается для всего временного ряда
- Метрика усредняется по всем временным рядам

Данные после обработки

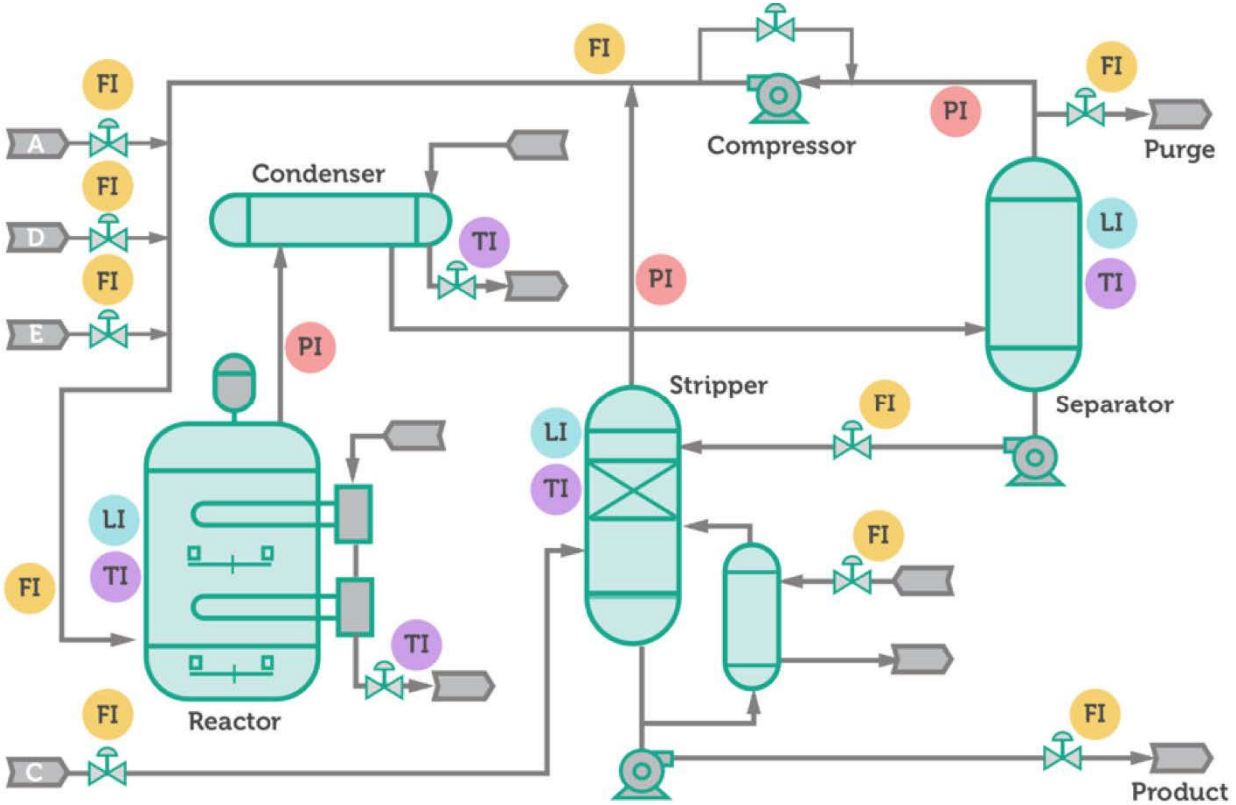
	GHL (Gasoil Heating Loop)	TEP (Tennessee Eastman Process)		SWaT (Secure Water Treatment)
Источник данных	Kaspersky Lab	Harvard Dataverse	Kaspersky Lab	iTrust CRCS
Тип	Симуляция	Симуляция	Симуляция	Реальный процесс
Переменные	12	52	53	51
Период	1 минута	3 минуты	1 минута	1 минута
Обучение	1 x 400+ часов	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	6 x 25 часов
Типов аномалий	2	20	4	36

Посмотрим на GHL

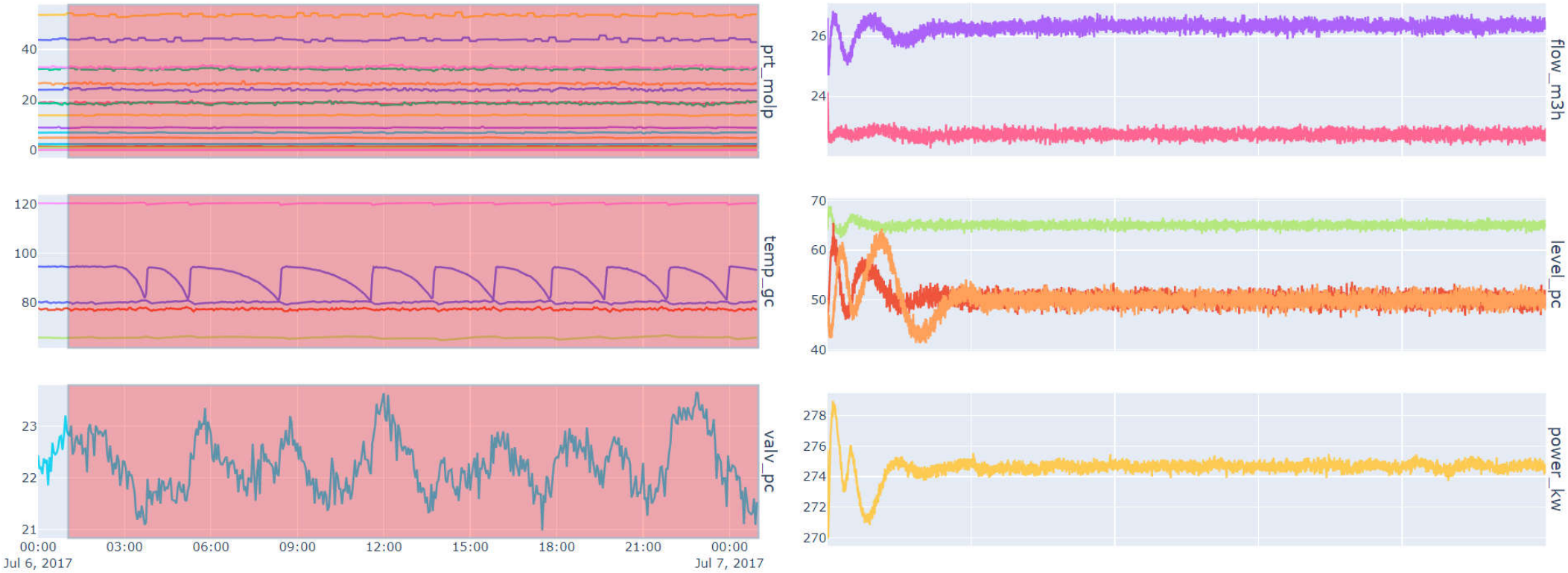




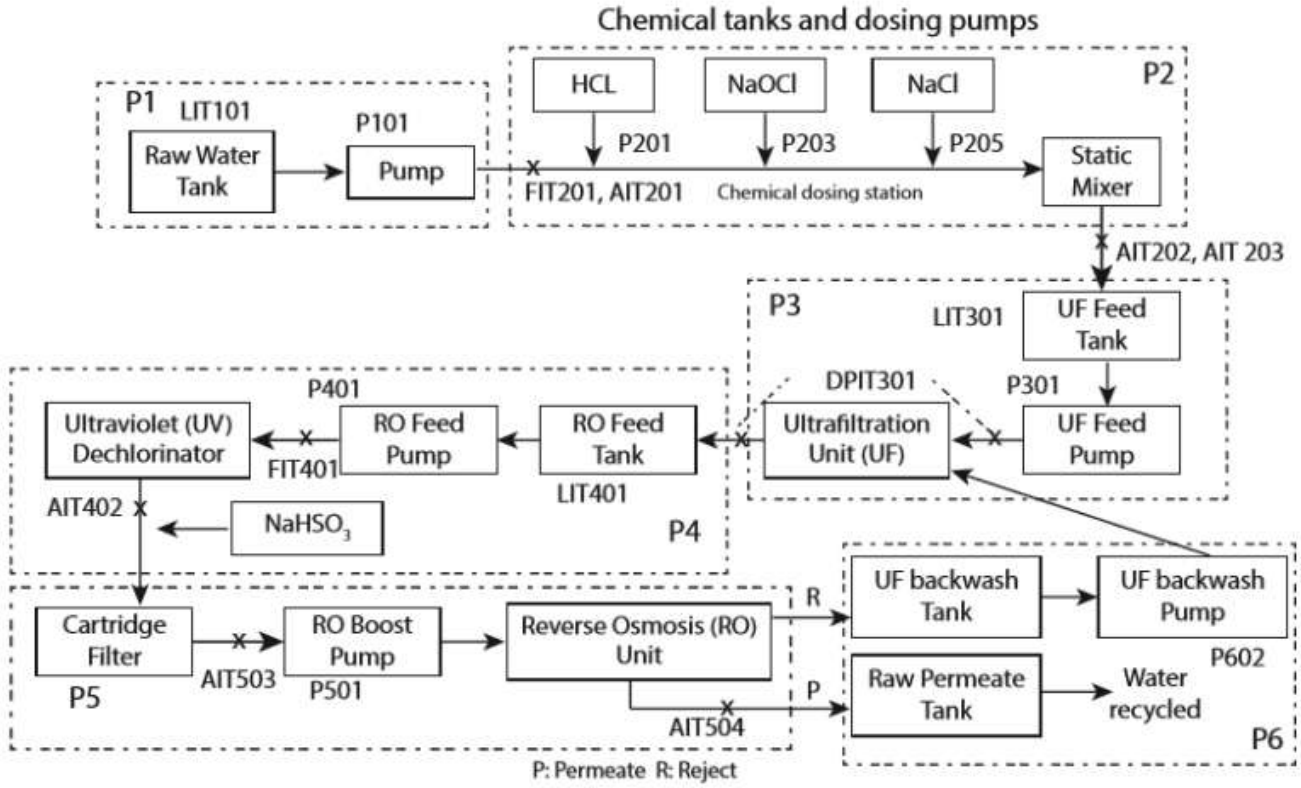
Посмотрим на TEP



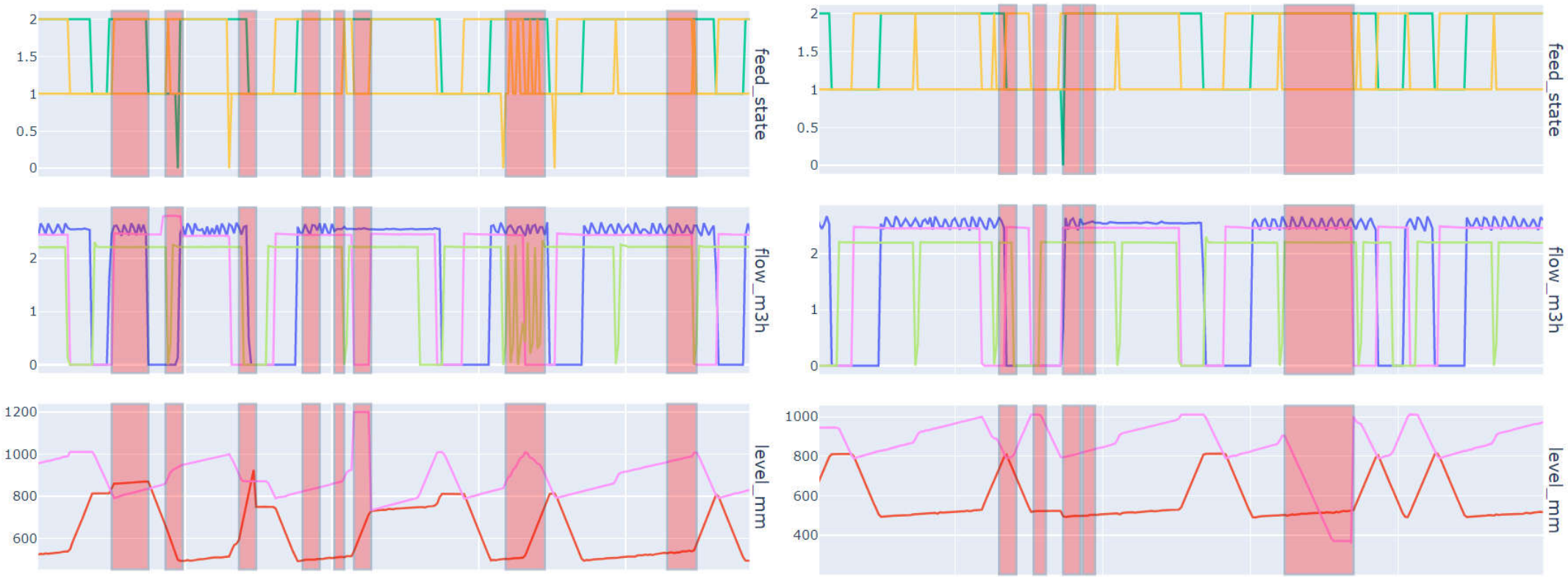
Посмотрим на TEP



Посмотрим на SWaT



Посмотрим на SWaT



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
- Перспективы интерпретации результата

Классификация алгоритмов

- Ошибка представления – обучение без учителя:
  - запоминание границ «как есть»
  - метод главных компонент (PCA)
  - решающие деревья (Isolation Forest)
- Ошибка предсказания – обучение с учителем:
  - линейные методы
  - нелинейные методы

Стратегия исследования

На симуляциях (GHL и TEP):

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

На всех (GHL, TEP, SWaT):

- Провести финальную проверку

DirectLimitWatchman

Идея:

- Использует переменные процесса «как есть»
- Запоминает граничные значения
- Считает неисправностью значения, выходящие за границы

Результат:

- Предсказание по каждому признаку

PcaLimitWatchman

Идея:

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

Результат:

- Предсказание по каждой главной компоненте и PMSE

IsoForestWatchman

Идея:

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

Результат:

- Предсказание аномалии по каждому семплу

LinearPredictWatchman

Идея:

- Значение признака сейчас - линейная комбинация признаков в прошлый раз
- 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:

- Текущее семпл предсказывается по нескольким предыдущим
- Предсказатель строится на базе 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. Предобучение по всем обучающим файлам: изучение данных, подстройка параметров алгоритма под количество файлов, обучение скейлера
2. Обучение по всем обучающим файлам: обучение основного алгоритма представления/предсказания
3. Постобучение по всем обучающим файлам: запоминание границ ошибок представления/предсказания

Сколько мы можем предсказать?

	GHL	TEP	SWaT
DirectLimitWatchman	12	52	52
PcaLimitWatchman	4	4	4
IsoForestWatchman	1	1	1
LinearPredictWatchman	8	53	26
DeepPredictWatchman	13	53	53
Итого	**38**	**163**	**136**

Ансамблирование

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

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

WatchSquad(threshold=4)	GHL	TEP Harvard	TEP Kaspersky	SWaT
Precision	0.4932	0.9983	0.7705	0.2689
Recall	0.6027	0.6895	0.4384	0.8569

Выводы

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

Пути улучшения, общие

- Считать ошибки более высокого порядка $|e|^n, n > 2$
- Сглаживать ошибки (например EWMA)
- Ансамблировать предсказания с некоторыми весами в зависимости от 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.)

Пути улучшения, зависимые от процесса

- Добавлять в признаки значения уставок и режимов
- Генерировать новые признаки по физическому смыслу
- Генерировать новые признаки по статистической значимости, если есть примеры аномалий
- Ансамблировать предсказания с автоматически подбираемыми весами (линейный классификатор), если есть примеры аномалий

Спасибо за внимание