Пулеко І.В., к.т.н., доцент,
Свінцицька О.М., к.е.н., доцент,
Державний університет «Житомирська політехніка»
Чумакевич В.О., к.т.н., доцент
Національний університет «Львівська політехніка»

ПОКАЗНИКИ ЯКОСТІ ДЕТЕКТОРІВ АНОМАЛІЙ, ЩО ВИКОРИСТОВУЮТЬ МЕТОДИ МАШИННОГО НАВЧАННЯ

Виділення в даних нетипових, аномальних представників є особливим завданням у машинному навчанні. Крім низки практичних застосувань (виявлення збоїв у показаннях датчиків, хакерських атак, незвичайних результатів діагностик), це завдання вважається етапом побудови будь-якого алгоритму машинного навчання, у якому дані перевіряються на консистентність та очищаються від викидів і шуму.

Існують три широкі категорії методів виявлення аномалій. Для контрольованих методів машинного навчання для виявлення аномалій потрібен «розмічений» набір даних, у якому кожен екземпляр був позначений як "нормальний" чи "аномальний", на якому і здійснюється навчання класифікатора. Однак цей підхід досить рідко використовується при виявленні аномалій через загальну недоступність розмічених даних та часту незбалансованість класів. Методи напівконтрольованого виявлення аномалій припускають, що деяку частину даних позначено. Це може бути будь-яка комбінація нормальних або аномальних даних, але найчастіше методи створюють модель, що представляє нормальну поведінку із заданого набору даних для нормального навчання, а потім перевіряють ймовірність того, що тестовий екземпляр буде згенерований моделлю. Неконтрольовані методи виявлення аномалій припускають, що дані не мають маркування, і на сьогоднішній день вони найчастіше використовуються через їх ширше та актуальніше застосування.

Результати роботи алгоритмів машинного навчання в задачах виявлення аномалій можуть мати такі види:

- Мітки – кожен екземпляр тестової вибірки отримує мітку нормальний або аномальний. Цей вид особливо притаманний системам, що базуються на моделях класифікації.

- Оцінки – кожному екземпляру тестової вибірки ставиться у відповідність оцінка аномальності. Це дозволяє ранжувати вихідні дані, проте потребує додаткового порогового параметру.

Оскільки випадки аномальної поведінки системи за визначенням є рідкими, задача оцінки результатів роботи алгоритмів машинного навчання є особливо складною. В загальному випадку більш кращий алгоритм визначається такою базовою оцінкою:

$$Base\ Rate = argmax \frac{1}{l} \sum_{i=1}^{l} [y_0 = y_i]$$

l – кількість членів тестової вибірки; y_i – результат передбачення;

y_0 – значення елемента даних визначене експертом.

Для оцінки результатів роботи окремих алгоритмів машинного навчання використовують різні підходи. Більшість з них базується на побудові матриці помилок (Confusion Matrix). Можливі два загальні види помилок: а) нормальна поведінка системи або користувача помилково приймається за аномальну (False Positives); б) спроба зловмисного проникнення в систему приймається за нормальну активність (False Negatives). Хоча жодна з цих ситуацій небажана, друга — більш небезпечна, і тому однією з основних задач побудови систем виявлення є чітке визначення умов, за яких ситуація сприймається як аномальна, так, щоб жодна з перелічених ситуацій не виникала занадто часто.

Для оцінки якості виявлення при контрольованому навчанні застосовують ряд метрик на основі Confusion Matrix: Overall Accuracy, Receiver operating characteristics (ROC) curve, Precision, Recall, F-score, Area under the curve (AUC), Precision-recall (PR) curve та інші.

Досить часто при використанні різних алгоритмів детектування аномалій виходять схожі показники якості і користувачеві важко вибрати один з них. Вибір найкращого класифікатора можна розглядати як задачу багатокритеріальної оптимізації. Тут автори пропонують застосувати метод розв’язування багатокритеріальних задач на основі нелінійної схеми компромісів, представлений у роботах Вороніна А. М. Після адаптації до задачі показник буде мати вигляд:

$$NSC=arg\ i=1nImiImi-Iix-1\ ,$$

де Imi – максимальне значення часткового показника;

Ii – отримане поточне значення часткового показника (наприклад, Acc - accuracy; Pr - precision; Rec - recall; F1 – F1-score).

Переваги методу нелінійної схеми компромісів полягають у тому, що цей метод досить простий за обчислювальними витратами і дозволяє отримувати розв’язки з множини Парето з урахуванням обмежень за принципом «наскільки від обмежень, наскільки це можливо». По-друге, скалярна згортка при опуклості часткових критеріїв має властивість унімодальності (тобто задача стає однозначно вирішеною).