Выявление аномалий в киберфизических системах на основе рекуррентных графиков

Н. А. Ширяев

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

n.shiryaev.work@gmail.com

Е. С. Новикова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)

esnovikova@etu.ru

Я. Чен

Китайский горнотехнологический университет

Сюйчжоу, Китай

Дж. Чжао

Исследовательский институт; Государственная электроэнергетическая компания Цзянсу

Цзянсу, Китай

fedora.cy@gmail.com

***Аннотация*. В данной работе предложен подход к выявлению аномалий в многомерных временных рядах киберфизических систем, основанный на преобразовании ряда в рекуррентный график и последующем анализе с помощью свёрточного автокодировщика. Эксперименты на наборах данных SWaT показали, что метод обеспечивает полноту обнаружения аномалий до 100% при F1-мере 0.97 на наборе SWaT. Преобразование многомерного временного ряда в рекуррентный график позволяет эффективно использовать лёгкие свёрточные сети и снижает число ложноотрицательных срабатываний.**

Ключевые слова: многомерные временные ряды; обнаружение аномалий; рекуррентный график, точечная диаграмма, сверточный автокодировщик

I. Введение

Анализ временных рядов играет важную роль во многих отраслях экономики, таких как здравоохранение, производство, финансы, сельское хозяйство, энергетика и т. д. К актуальным задачам их анализа относится выявление аномалий в многомерных временных рядах. Аномальные события могут свидетельствовать о сбоях или изменениях в поведении системы, возникающих в том числе в результате преднамеренного вредоносного воздействия на неё.

В последнее время предложены методы на основе графовых нейронных сетей, которые выявляют аномалии за счет анализа изменения структурных связей между параметрами многомерных рядов [1, 2]. Например, в [2] представлена модель выявления аномалий в многомерных нерегулярных временных рядах на основе графовой нейронной сети, которая оценивает изменения в плотности данных во времени. Также активно исследуются методы поиска аномальных последовательностей без учителя [3, 4], например, в [4] в основе решения данной задачи лежит концепция диссонанса временного ряда, который выявляется с помощью сиамских нейросетей.

В настоящей работе решается задача выявления аномалий в многомерных временных рядах путем их преобразования в рекуррентные графики, позволяющие учитывать динамику функционирования системы.

II. Анализ релевантных работ

В [5, 6] представлена систематизация подходов на основе глубокого обучения с учетом используемых архитектур глубоких нейронных сетей, исследованы наиболее часто используемые наборы данных в задачах выявления аномалий как в одномерных, так и многомерных временных рядах. В [5] авторы представили общие рекомендации по выбору метрик оценки качества выявления аномалий в многомерных временных рядах. Авторы работы [7] отмечают, что на текущий момент не существует универсального алгоритма обнаружения аномалий, применимого во всех ситуациях, учет специфики прикладной области может значительно повысить качество обнаружения аномалий. Кроме того, более простые архитектуры, такие как сверточные нейронные сети (CNN) и сети с длительной краткосрочной памятью (LSTM), «обычно превосходят по качеству более сложные модели, включая усовершенствованные архитектуры трансформеров» [7].

В последнее время для выявления аномалий во временных рядах предложен ряд подходов, в основе которых лежит преобразование исходного временного ряда в графическое представление, что позволяет адаптировать для их анализа методы, изначально разработанные для исследования изображений, в т.ч. на основе предобученных глубоких нейронных сетей.

К методам визуализации состояния системы в фазовом пространстве относятся рекуррентные диаграммы и диаграммы расстояний (distance plot), которые используются для анализа поведения динамической системы [11]. С их помощью возможен анализ структуры временных рядов, включая исследование таких характеристик, как периодичность, стационарность, хаотичность, нелинейность и т.д. Чаще всего рекуррентные диаграммы применяются для классификации одномерных временных рядов [13]. В [13] было показано, что применение рекуррентных

диаграмм в сочетании с полями Грамиана позволяет достичь точности классификации аномального трафика в Интернете вещей в среднем до 99,8% в различных тестовых сценариях с высокой вычислительной эффективностью.

Таким образом, применение преобразования временных рядов в изображения позволяет разрабатывать эффективные методы обнаружения аномалий на основе легковесных моделей машинного обучения, которые учитывают, как пространственные, так и временные зависимости в анализируемых данных. Однако многие методы построения изображений применимы только для одномерных временных рядов, что делает актуальным задачу их адаптации для анализа многомерных временных рядов, описывающих функционирование одной системы. В настоящей работе исследуется применимость рекуррентных графиков в задачах выявления аномалий в многомерных временных рядах на примере данных от киберфизических систем.

III. Подход к выявлению аномалий на основе рекуррентных графиков

A. *Определения и формальная постановка задачи*

Многомерный временной ряд $X = \{\boldsymbol{x}_t\}$, где $t = 1 \ldots T$ определяется как упорядоченное множество k-мерных векторов, каждый из которых записан в определённый момент времени t и состоит из k вещественных наблюдений, т.е. $\boldsymbol{x}_t = (x_t^1, \ldots, x_t^k)$. Таким образом, каждая точка данных $\boldsymbol{x}_t$ представлена k-мерным вещественным вектором, а последовательность многомерного временного ряда S_t^n длины $n \leq T$ представляет собой упорядоченное множество точек $S_t^n = \{\boldsymbol{x}_t, \boldsymbol{x}_{t+1}, \ldots, \boldsymbol{x}_{t+n-1}\}$, где $t \leq |T| - n + 1$. Каждый компонент многомерного временного ряда X^j является одномерным временным рядом, т.е. $X^j = \{x_t^j\}$, где $t = 1 \ldots T$.

В данной работе решается задача обнаружения аномальных последовательностей в многомерном временном ряде, то постановка задачи может быть сформулирована следующим образом. Пусть $X = \{\boldsymbol{x}_t\}$, многомерный временной ряд, а S_t^n – его последовательность длины $n \leq T$, где $t = 1 \ldots T$, необходимо найти такое отображение A, которое для элемента S_t^n сопоставляет оценку аномалии A: $S_t^n \rightarrow s_t$. Если оценка аномалии превышает некоторые порог $\delta_{anomaly}$, то последовательность $\boldsymbol{x}_t$ считается аномальной.

B. *Построение рекуррентной диаграммы для многомерного временного ряда*

Рекуррентный график строится на основе матрицы $\mathbf{R}_{i,j}$, столбцы и строки которой обозначают моменты времени, а ее элемент r_{ij} отражает повторение i-го состояния системы в j-ый момент времени: $\mathbf{R}_{ij} = \Theta(\varepsilon - \|X_i - X_j\|)$, где X_i – фазовая траектория исследуемой динамической системы, $i, j = 1, \ldots, k$ и $k << N$, пороговый параметр ε задает окрестность подобия точек в пространстве, $\| \cdot \|$ — выбранная метрика расстояния, а Θ — функция Хевисайда: $\Theta(a) = 1$ при $a \geq 0$, иначе 0. Фазовое пространства системы может быть построено на основе вектора наблюдаемых значений параметров данный системы с помощью с помощью метода временных задержек на основе теоремы Такенса [11]. В работе для каждого признака строится вложение с параметрами (d, τ), где $d = 3$ – размерность вложения, $\tau = 1$ – величина временной задержки.

В качестве метрики расстояния между векторами x_i и x_j чаще всего используется евклидово расстояние или косинусное сходство.

Рекуррентные графики могут быть пороговыми бинарными и непрерывными. По аналогии с ними в работе определяются бинарные и непрерывные точечные диаграммы.

Бинарные точечные диаграммы определяются матрицей, элементы которой равны 1, если нормализованное расстояние между векторами не превышает порога ε, и 0 в противном случае. Порог ε может быть задан некоторым фиксированным значением либо вычисляться динамически с учетом требуемой доли ненулевых рекуррентных точек (recurrence rate, RR). Под долей ненулевых рекуррентных точек RR понимается отношение числа ненулевых рекуррентных точек (исключая диагональные) к общему числу возможных пар состояний. В последнем случае все внедиагональные элементы матрицы расстояний сортируются, и порог устанавливается таким образом, чтобы доля элементов, не превышающих порог, равнялась заданному значению RR. Такой адаптивный выбор порога позволяет получать графики с одинаковой плотностью точек для различных временных интервалов и сравнивать их между собой.

Пороговые непрерывные диаграммы вычисляются аналогично бинарным, однако элемент матрицы вычисляется как минимальное из 1 и отношения нормализованного расстояния к порогу ε. Непрерывные точечные диаграммы сохраняют исходные значения расстояний между парой векторов. Они содержат больше информации о поведении системы, что полезнее при извлечении признаков с помощью сверточных нейронных сетей.

Выбор порога ε является нетривиальной задачей, он определяет вид точечной диаграммы, и, если он неправильно выбран, матрица может $\mathbf{R}_{i,j}$ может состоять в основном или из одних нулей или единиц, что затруднит выявление характерных признаков поведения системы, поэтому в настоящей работе значение порога определяется автоматически по целевому значению доли ненулевых рекуррентных точек. На рис. 1 представлен пример бинарного рекуррентного графика со значением параметра ε и непрерывного рекуррентного графика для одного и того же временного ряда длиной 120 отсчетов.

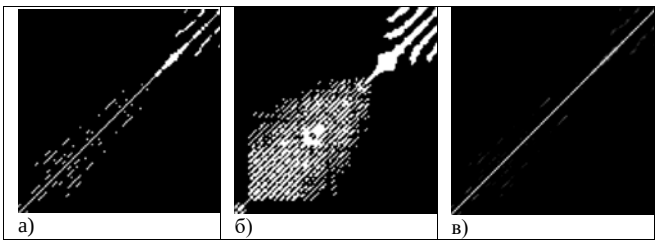

Рис. 1. Точечные диаграммы, построенные при разных настройках для одного и того же временного ряда длиной 120 отсчетов: а) бинарная диаграмма с порогом $\varepsilon = 0.5$; б) бинарная диаграмма с целевым значением параметра RR = 15%; с) непрерывный точечная диаграмма с порогом $\varepsilon = 0.5$.

C. *Классификация точечной диаграммы многомерного временного ряда*

Перед построением точечных диаграмм исходные многомерные временные ряды проходят этап

предварительной обработки, целью которого является разделение переменных на две группы:

- числовые (непрерывные) признаки, обычно представленные значениями датчиков и используемые для расчёта попарных расстояний и формирования RP;
- категориальные переменные, описывающие дискретные состояния исполнительных механизмов (например, положение клапанов, режимы работы насосов).

Такое разбиение связано с тем, что категориальные параметры, меняясь скачкообразно, сильно влияли на структуру рекуррентных графиков. Для сохранения информации о состоянии дискретных компонентов системы, они преобразуются с помощью one-hot кодирования и формируют отдельный вектор, который подается на вход разработанной нейронной сети.

Для анализа точечных диаграмм временных рядов была реализована модель сверточного автокодировщика (CNN-AE). В разработанной модели для обучения используется комбинированная функция потерь, учитывающая не только качество реконструкции точечной диаграммы, но и сохранение признаков, извлечённых из неё, а также точность восстановления one-hot вектора, характеризующего метку класса. Функция потерь формируется как взвешенная сумма трёх компонент:

- среднеквадратичная ошибка между реконструированным изображением и исходным;
- ошибка реконструкции признаков, вычисляемая как среднеквадратичная ошибка между вектором признаков, полученным после свёрточного экстрактора, и вектором, восстановленным декодером;
- среднеквадратичная ошибка восстановления категориальных признаков, закодированных one-hot представлением.

D. Экспериментальная оценка разработанного подхода

В ходе экспериментальной оценки исследовалось влияние следующих параметров на точность обнаружения аномалий во временных рядах с

- длина анализируемого временного ряда *n*;
- режим формирования точечного графика – бинарный,
- значение порогового параметра RR (Reccurence rate).

В качестве тестового набора данных был выбран набор данных SWaT (Secure Water Treatment) версии 2015 года [15], который представляет собой набор логов, собранных со стенда, моделирующего функционирование водоочистных сооружений.

Обучение модели осуществлялось на рекуррентных диаграммах, необходимо было преобразовать исходные данные в обучающую выборку, состоящую из изображений. Для ее формирования данные размечались следующим образом: график R_n^t считался аномальным, если процент аномальных значений в текущем временном окне *n* был больше заданного порогового значения. В ходе эксперимента данный параметр был выставлен в 10%. Шаг генерации точечных диаграмм составил 1 секунду, т.е. сдвиг составил 1 запись. Исходные данные предварительно были нормированы, а затем преобразованы в точечную диаграмму. Разделение исходного набора на обучающую и тестовую выборки производилось случайным образом в соотношении 80 на 20.

Величина окна *n* в работе определялась экспериментально, были выбраны следующие значения: 30, 60, 90, 120, что соответствует 30 секундам, 1 минуте, 1 минуте и 30 секундам и 2 минутам функционирования анализируемой системы. Эксперименты показали, что ошибка обучения оказалась минимальной для окна Δt, равному 120.

Сверточный автокодировщик обучался 10 эпох, оценка эффективности обнаружения аномалий во временных рядах осуществлялась при помощи классических метрик, таких как точность (precision), полнота (recall) и F1-мера,

В табл. 1 (SWaT) представлены полученные результаты при разных значениях выбранных параметров. Самые высокие показатели точности и F1-меры для набора SWaT достигнуты при пороге recurrence rate = 0.15 (15%); при RR > 20% качество падает. В целом, для SWaT точность обнаружения аномалий (precision) составила ≈0.95, F1-мера — 0.97, а полнота (recall) во всех экспериментах равнялась 1.0, то есть все аномалии были обнаружены.

ТАБЛИЦА I. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТОВ ДЛЯ РАЗНЫХ НАСТРОЕК ГЕНЕРАЦИИ ТОЧЕЧНОЙ ДИАГРАММЫ ДЛЯ ДАТАСЕТА SWAT

Тип точечной диаграммы	**Размер окна**	**Точность (Precision)**	**Полнота (Recall)**	**F1-мера**	**ROC-AUC**
Бинарный	120	0.80	0.78	0.79	0.73
Бинарный	90	0.81	0.76	0.78	0.74
Бинарный	60	0.77	0.72	0.74	0.73
Бинарный	30	0.71	0.60	0.65	0.70

Было также выполнено сравнение эффективности разработанного подхода с другими предложенными в научной литературе путем оценки метрик точности, полноты и F1-меры, полученных на наборе SWaT. В табл. 2 представлены краткое описание подходов, используемых в сравнительном анализе, и полученные результаты. В ней жирным шрифтом выделены максимальные значения в столбце. Из нее следует, что предложенный в данной работе метод характеризуется более высоким значением полноты обнаружения аномалий, и незначительно уступает по точности методам ocSVM, DeepSVDD и MTS –DVGAN.

ТАБЛИЦА II. РЕЗУЛЬТАТЫ СРАВНЕНИЯ ПРЕДЛОЖЕННОГО МЕТОДА С МЕТОДАМИ ОБНАРУЖЕНИЯ АНОМАЛИЙ, ПРЕДСТАВЛЕННЫМИ В НАУЧНОЙ ЛИТЕРАТУРЕ

Подход	**Точность (Precition)**	**Полнота (Recall)**	**F1-мера**
Предложенный подход	0.80	0.79	**0.79**
Подход на основе графовой нейронной сети [17]	0.64	**0.89**	0.74

Подход	Точность (Precition)	Полнота (Recall)	F1-мера
Одноклассовый метод опорных векторов ocSVM [18]	**0.99**	0.59	0.74
Одноклассовый автокодировщик DeepSVDD SVDD [18]	**0.99**	0.65	0.78
Вариационный автоэнкодер на основе двух сетей долгой краткосрочной памяти MTS – DVGAN [19]	**0.99**	0.67	**0,79**

IV. Заключение

В настоящей работе предложен подход к выявлению аномалий в многомерных временных рядах, отличающийся методом преобразования исходных данных в точечную диаграмму и последующим применением сверточного автоэнкодера для их анализа. Выполненные эксперименты позволили определить параметры генерации точечной диаграммы, для которых тестовая точность, полнота и F1-мера достигает максимальных значений. Следует отметить, что предложенный подход обладает высокой точностью обнаружения аномалий, в частности полнота их выявления достигает 100%. Таким образом, преобразование многомерного временного ряда к точечной диаграмме позволяет значительно снизить число ложноотрицательных срабатываний.

Список литературы

[1] Д.Н. Карпухин, В.Л. Бурковский. Алгоритмизация пространственно-временного процесса построения графических моделей анализа потенциальных неисправностей в многомерных временных рядах с пропущенными значениями // Вестник Воронежского института высоких технологий, 2024.

[2] Mlyahilu N. J., Novikova E., Graph Construction Approaches for Graph Neural Networks-Based Anomaly Detection in Time Series // In Proc. of XXVIII International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russian Federation, 2025, pp. 144-147. DOI: 10.1109/SCM66446.2025.11060448

[3] Tafazoli et al. Matrix Profile XXVIII: Discovering Multi-Dimensional Time Series Anomalies with K of N Anomaly Detection.

[4] Я.А. Краева, Нейросетевой метод обнаружения аномалий в многомерных потоковых временных рядах. DOI: http://dx.doi.org/10.14529/cmse240403

[5] Wang, F., Jiang, Y., Zhang, R., Wei, A., Xie, J., & Pang, X. A Survey of Deep Anomaly Detection in Multivariate Time Series: Taxonomy, Applications, and Directions // Sensors, 2025. 25(1), 190.

[6] Paparrizos J., Boniol P., Liu Q., Palpanas T. Advances in Time-Series Anomaly Detection: Algorithms, Benchmarks, and Evaluation Measures // Proc. of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.2 (KDD '25). 2025. ACM, New York, NY, USA, pp. 6151–6161.

[7] Darban Z. Z., Webb G.I., Pan S., Aggarwal C., Salehi M. Deep Learning for Time Series Anomaly Detection: A Survey // ACM Comput. Surv. 2024, 57, 1, Article 15 (January 2025), 42 pages.

[8] Park H., Jang H. Enhancing Time Series Anomaly Detection: A Knowledge Distillation Approach with Image Transformation // Sensors. 2024, no. 24: 8169.

[9] Bazgir O., Zhang R., Dhruba S.R. et al. Representation of features as images with neighborhood dependencies for compatibility with convolutional neural networks // Nature Communications. 2020. Vol. 11. No 4391.

[10] Park J., Seong S., Lee J., Hong C. Vortex Feature Positioning: Bridging Tabular IIoT Data and Image-Based Deep Learning // Internet of Things, 2025. Vol. 31, no. 101533.

[11] Marwan N., Romano M. C., Thiel M., Kurths J, Recurrence plots for the analysis of complex systems // Physics Reports, 2007. Vol. 438, is. 5–6, pp. 237-329.

[12] Jin D., Hu Y., Chen B., He G., Chen Y., Shen Z. TIAN: A time series Imaging Association Network for human abnormal behavior detection // Information Fusion, Volume 118, 2025, 102906, ISSN 1566-2535.

[13] Z. Xia, K. Long, Y. Yu, L. Huang, W. Hao, and J. Tan, “A lightweight intrusion detection system for connected autonomous vehicles based on ECANet and image encoding,” Journal of Information Security and Applications, vol. 92, p. 104082, Jul. 2025.

[14] Aldrich C. A Comparative Analysis of Image Encoding of Time Series for Anomaly Detection’, Time Series Analysis - Recent Advances, New Perspectives and Applications // IntechOpen, Dec. 15, 2023.

[15] Goh J., Adepu S., Junejo K. N., and Mathur A. A dataset to support research in the design of secure water treatment systems // Critical Information Infrastructures Security. Cham: Springer International Publishing, 2017, pp. 88–99.

[16] Paparrizos J., Boniol P., Palpanas T., Tsay R., Elmore A., and Franklin M. Volume Under the Surface: A New Accuracy Evaluation Measure for Time-Series Anomaly Detection // Proc. of the VLDB Endowment Journal, 2022. Vol. 15, pages 2774-2787.

[17] L(y)u S., Wang K., Wei Y., Liu H., Fan Q., Wang B. GNN-based Advanced Feature Integration for ICS Anomaly Detection // ACM Trans. Intell. Syst. Technol. 2023.14, 6, Article 106 (December 2023), 32 pages.

[18] Tushkanova, O.; Levshun, D.; Branitskiy, A.; Fedorchenko, E.; Novikova, E.; Kotenko, I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. Algorithms 2023, 16, 85.

[19] Haili Sun, Yan Huang, Lansheng Han et al. MTS-DVGAN: Anomaly detection in cyber-physical systems using a dual variational generative adversarial network // Computers & Security. 2024. Vol. 139. No 103570.

.