Построение классов сетевой активности устройств интернета вещей

О. С. Исаева

Институт вычислительного моделирования СО РАН

isaeva@icm.krasn.ru

Аннотация. **Одним из ключевых направлений обеспечения безопасности сетей является классификация сетевого трафика с целью выявления аномалий и потенциальных угроз. В рамках исследования решалась задача построения устойчивых классов сетевой активности устройств интернета вещей, которые могут быть использованы для разметки данных и последующей классификации. Предложен метод сокращения размерности признакового пространства на основе анализа стабильности и веса признаков. Выполнена семантическая интерпретация полученных кластеров, продемонстрировавшая эффективность предложенного подхода. Результаты будут использованы при построении системы обнаружения аномалий в среде интернета вещей.**

Ключевые слова: интернет вещей; данные сетевых журналов; методы кластеризации; сокращение признакового пространства

I. Введение

В условиях стремительного роста числа устройств, подключённых к сетям связи в рамках глобальной структуры Интернета вещей (IoT), неуклонно возрастает потребность в обеспечении кибербезопасности и надёжности подобных систем. Одним из важных инструментов в этой области является классификация сетевого трафика по типам активности [1]. Общая цель классификации заключается в выявлении значимых характеристик сетевого поведения и отнесении его к определённым категориям. Классификация позволяет разделять нормальный трафик, фоновую активность, потенциальные угрозы и тем самым формирует основу инструментов обнаружения вторжений.

Актуальность решения задачи классификации определяется её влиянием на повышение эффективности использования существующих каналов связи и качества управления трафиком, открывающим возможности для прогнозирования нагрузки сети [2]. Обнаружение аномалий в сетевой активности IoT-устройств позволяет выявлять отклонения от типового поведения, при этом сами устройства, из-за ограниченных вычислительных ресурсов, гетерогенности протоколов и разнообразия внешних угроз, не способны применять традиционные методы обеспечения безопасности.

Сетевой трафик можно представить как многомерный динамический процесс, возникающий в результате взаимодействия и наложения множества отдельных информационных потоков, каждый из которых обладает собственным набором характеристик и порождается соответствующими сетевыми протоколами [3]. Для его корректной классификации необходимы качественные и репрезентативные наборы данных. В большинстве случаев такие данные представлены в виде размеченных сетевых сессий, собранных с использованием инструментов мониторинга трафика, либо сгенерированных в контролируемой среде. Получение таких данных требует либо использования собственных инструментов сбора и подготовки информации, либо обращения к публичным источникам [4]. Современные исследования демонстрируют широкое применение открытых наборов данных, которые активно используются в научном сообществе [5]. Однако они обладают рядом особенностей, влияющих на их применимость в реальных условиях. Среди ключевых ограничений выделяются: неоднородность состава трафика, различия в подходах к моделированию сетевой активности, вариации в методах сбора и предварительной обработки данных. Большинство публичных наборов данных собирается в искусственной имитационной среде или в изолированных тестовых окружениях с имитацией устройств. Эти факторы оказывают существенное влияние на эффективность систем обнаружения аномалий при переносе моделей из имитационной среды в реальные условия. Некоторые наборы данных содержат ошибки в сегментации сетевых сессий или расчёте значений признаков, что снижает точность построенных на их основе моделей машинного обучения [6]. Кроме того, такие данные зачастую охватывают широкий спектр типов угроз, ориентированных на различные информационные системы, что потенциально приводит к избыточному усложнению моделей и снижению их специфичности. Ещё одной важной характеристикой является эволюция свойств сетевого трафика во времени. Изменения в характере активности, вызванные как развитием атакующих и предотвращающих техник, требуют регулярного обновления и переобучения моделей классификации, что, в свою очередь, предполагает наличие актуальных данных для повторной настройки систем анализа.

На данный момент отсутствует универсальный эталонный набор данных, который мог бы быть принят в качестве стандарта для задач классификации сетевого трафика. Исследовательские группы выбирают данные, исходя из целей и специфики решаемых задач, чтобы обеспечить адекватность построенных моделей и их применимость в реальных сетевых условиях. Выбор информативных признаков, используемых для классификации, остаётся одной из ключевых задач [7]. Эффективность модели напрямую зависит от способности выделять такие признаки и анализировать их влияние на точность классификации. В зависимости от содержания, все признаки могут быть разделены на следующие категории [8]:

- данные пакета – содержимое полезной нагрузки или байты пакета без разделения на заголовок и данные;

Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ в рамках мероприятий по созданию и развитию региональных НОМЦ (Соглашение 075-02-2025-1606)

- метаинформация – размер пакета, длина полезной нагрузки, направление передачи, тип сервиса, флаги протоколов;
- временные характеристики – интервалы между пакетами, длительность сессии, начало и окончание потока;
- информация о потоке – агрегированные параметры, характеризующие поведение всего сетевого соединения или группы связанных потоков.

Различные комбинации этих признаков используются во многих работах [9]. Для автоматизации извлечения информативных признаков из неструктурированных сетевых журналов разработан ряд специализированных инструментов: Tranalyzer [10], CICFlowMeter [11], NTLFlowLyzer [12], NFStream [13] и другие. Использование одного из этих инструментов к собственным данным позволяет формировать набор метрик, характеризующих функционирование сети безопасность которой необходимо обеспечить. Полученные признаки могут быть использованы в качестве эталонной системы характеристик, обеспечивающей возможность сравнения результатов собственных исследований с опубликованными данными в научной литературе. Анализ временных характеристик и пространства признаков позволил выбрать NTLFlowLyzer как наиболее полно отражающий особенности сессий интернета вещей [14].

Для классификации трафика в наборах данных применяются методы ручной или автоматической разметки. Ручная разметка является трудозатратной и недостаточно эффективной, поскольку не позволяет выявлять сложные механизмы поведения устройств или новые типы атак. В современных подходах к автоматизированной классификации сетевого трафика широко применяются статистические характеристики, строятся математические модели сетевых сессий, проводятся исследования законов распределения ключевых параметров трафика, таких как длительность соединения и скорость передачи, с целью формирования профилей сетевой активности устройств [15]. Особое внимание уделяется применению моделей машинного обучения, включая различные конфигурации нейронных сетей, способных выявлять скрытые паттерны в больших объёмах данных. Для анализа последовательностей и временных зависимостей используются рекуррентные нейронные сети [16], а для обработки структурированной информации – свёрточные нейронные сети, позволяющие эффективно извлекать признаки из полезной нагрузки пакетов [17].

Однако, в условиях высокой размерности признакового пространства (в наборах данных, получаемых при анализе трафика устройств Интернета вещей, число признаков может превышать 300), использование указанных методов ограничивается сложностью интерпретации результатов и анализа взаимосвязей между характеристиками. Для преодоления этих трудностей применяются комбинированные двухэтапные подходы, в которых первый этап направлен на снижение размерности входного пространства признаков, а второй – на классификацию и анализ поведения устройств [18].

Для исследования безопасности сети интернета вещей в Красноярском научном центра создана инфраструктура сбора данных и имитации угроз [19]. В данной работе представлен подход к анализу собираемых в этой инфраструктуре данных.

Целью данного исследования является построение классов сетевой активности устройств интернета вещей, предназначенных для обеспечения корректной разметки данных и последующего применения в задачах классификации сетевого трафика. Для достижения поставленной цели предполагается реализовать следующие этапы:

- проведение кластеризации данных для оценки применимости методов в условиях отсутствия заранее заданных меток классов;
- уменьшение размерности признакового пространства на основе анализа стабильности и информативности признаков с целью улучшения классификационных свойств данных, таких как локальная связность и согласованность;
- проведение кластеризации данных на сокращённом признаковом пространстве;
- экспертная оценка и содержательная интерпретация полученных кластеров специалистами предметной области.

II. Кластеризация полного признакового пространства

Рассмотрим множество данных X размерности $n \times m$, где n – количество объектов наблюдения, m – количество признаков, $x_{i\,j}$ – значение j-го признака для i-го объекта наблюдения, $X_i=(\,x_{i\,1}, \ldots, x_{im})$ – значения всех признаков для i-го объекта, а $P_i=(\,x_{1j}, \ldots, x_{nj})$ – значения j-го признака для всех объектов.

Анализ множества данных требует их предобработки, расчёта статистических характеристик, выбора метода кластеризации, разбиения выборки на кластеры и семантической интерпретации полученных результатов. В качестве примера в табл. 1 представлены основные свойства фрагмента данных, собранных в штатном режиме работы от четырёх датчиков интернета вещей в течение одного месяца без имитации атак или угроз безопасности.

ТАБЛИЦА I. Свойства данных

Показатель	Значение
Размерность данных	(2221, 347)
Количество значений	770687
Пропущенных значений (nan, inf)	20623
Количество записей в день (макс)	73
Количество записей в день (мин)	4
Уникальных значений с столбце (макс)	2135
Уникальных значений с столбце (мин)	1
Кол-во коррелирующих пар признаков	878
Кол-во мультиколлинеарных признаков	359
Кол-во взаимозависимых пар признаков	136

Для выделения классов сетевой активности, по которым будут размечаться сессии, были рассмотрены различные методы кластеризации, представляющие разные подходы к группировке данных. В качестве базового и наиболее распространённого метода использовался алгоритм k-средних, позволяющий эффективно разделять данные на компактные кластеры при заданном числе групп. Также применялся метод Affinity Propagation, не требующий предварительного задания количества кластеров, однако отличающийся

высокой вычислительной сложностью и чувствительностью к изменению параметров. В качестве альтернативного подхода была использована агломеративная иерархическая кластеризация, основанная на восходящей стратегии объединения элементов и учитывающая взаимосвязи между кластерами на различных уровнях иерархии.

Определение оптимального числа кластеров осуществлялось с помощью эвристического метода локтя, который позволяет выявить такое значение *k*, при котором дальнейшее увеличение числа кластеров перестаёт приводить к существенному уменьшению суммы внутрикластерных расстояний. Пример визуализации выбора числа кластеров для алгоритма *k*-средних представлен на рис. 1.

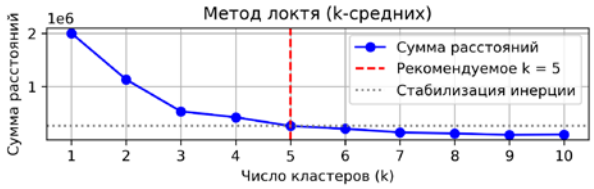

Рис. 1. Выбор оптимального числа кластеров

По каждому подмножеству признаков выполнялась несколькими методами кластеризация. Построенные группы подвергались сравнительному анализу и исследованию с целью интерпретации полученных классов. Рассматривались следующие подходы к кластеризации:

1. Использование признаков, определённых экспертами как наиболее значимые. Пример визуализации кластеров, построенных по двум исходным признакам, представлен на рис. 2.

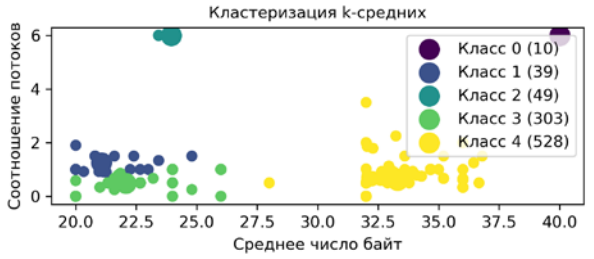

Рис. 2. Пример кластеризации по заданным признакам

2. Уменьшение размерности признакового пространства методом главных компонент. Построена система обобщённых признаков – линейных комбинации исходных переменных, объясняющих заданную долю дисперсии данных. Выполнена кластеризация (рис. 3).

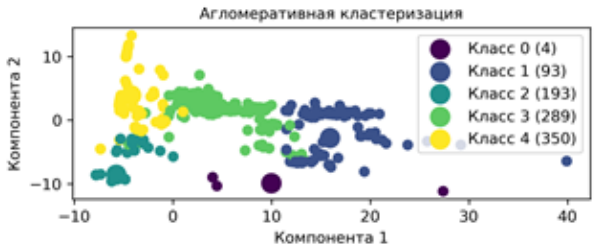

Рис. 3. Пример кластеризации для главных компонент

3. Отображение построенных кластеров в базовые координаты и интерпретация экспертами выделенных групп.

Проведённые исследования не позволяют выбрать предпочтительное разбиение: с точки зрения предметной области схожие сессии могли быть отнесены к разным кластерам, а отличающиеся – к одному. Одной из причин такого эффекта является наличие большого числа зависимых признаков – коррелирующих, мультиколлинеарных и взаимозависимых. Эти признаки вносят избыточную информацию и увеличивают вес определённых направлений в пространстве, что может искажать реальную структуру данных и формировать артефактные кластеры. Для решения этой проблемы был предложен подход к удалению зависимых признаков на основе расчёта их стабильности и веса.

III. Сокращение признакового пространства

Признак $P \in X$ исключается из X при условии:

$$\forall Q \in X^P \setminus P: [S(P) < S(Q)] \wedge [W(P) < W(Q)],$$

где X^P – множество зависимых с P признаков, $S(P)$ – коэффициент стабильности, $W(P)$ – агрегированный вес признака. Коэффициент стабильности вычисляется:

$$S(P) = \frac{1}{T-1} \sum_{t=1}^{T-1} M\left(P^{(t)}, P^{(t+1)}\right),$$

где T – количество случайных выборок, полученных из X, $M(P^{(t)}, P^{(t+1)})$ – показатель взаимной информации между признаком P на t-ой и $(t+1)$-ой выборках.

$$M = \frac{2}{m(m-1)} \sum_{j=1}^{m} \sum_{k=j+1}^{m} M_{jk},$$

$$M_{jk} = \sum_{x_{ij} \in P_j} \sum_{x_{ik} \in P_k} \frac{p(x_{ij}, x_{ik})}{n} \cdot \ln \frac{n \cdot p(x_{ij}, x_{ik})}{p(x_{ij}) \cdot p(x_{ik})}$$

где M_{jk} определяет величину взаимной информации между P_j и P_k [20], $p(x_{ij}, x_{ik})$ – частота совместного появления значений признаков P_j и P_k, $p(x_{ij})$ и $p(x_{ik})$ – частота появления каждого значения признака в отдельности.

Агрегированный вес признака определятся как:

$$W(P) = \sum_{i=1}^{c} |v_i(P)| \cdot \frac{\lambda_i}{\sum_{m=1}^{c} \lambda_m},$$

где $c = \min\{j \mid \sum_{i=1}^{j} \lambda_i \Big/ \sum_{i=1}^{m} \lambda_j \geq \varsigma\}$ – количество признаков, содержащих ς дисперсии исходного набора данных, λ_i – собственное значение, $v_i(P)$ – компонента собственного вектора v_i, соответствующая признаку P.

Применение данного подхода позволило сформировать признаковое пространство, состоящее из 17 исходных компонент. Анализ этого пространства показал улучшение структуры кластеров: они стали более компактными и лучше разделёнными. Для оценки качества кластеризации использовался силуэтный коэффициент, его график для сокращённого признакового пространства приведён на рис. 4, до сокращения его среднее значение составляло 0.57.

Кластеризация полученного набора данных показала слабую зависимость от выбора конкретного алгоритма и высокую степень интерпретируемости результатов.

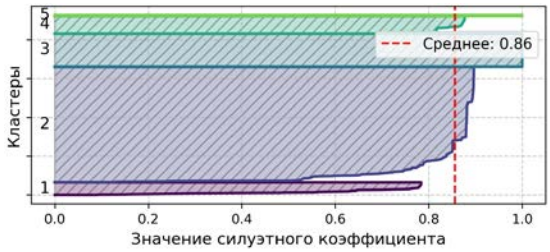

Рис. 4. Силуэтный коэффикиент кластеров

Эксперты предложили семантическую интерпретацию выделенных групп следующим образом: кластер 1 объединяет неудачные установки соединений, кластер 2 составляют легитимные сессии, сопровождаемые передачей данных между клиентом и сервером, кластер 3 также содержит легитимные сессии, однако характеризуется большей продолжительностью и свидетельствует об активном взаимодействии с устройствами интернета вещей, кластер 4 состоит из кратковременных сессий, соответствующих сканированию сети на транспортном уровне, кластер 5 включает сканирование на уровне прикладных протоколов.

IV. Заключение

В ходе исследования была решена задача построения классов сетевой активности устройств Интернета вещей, предназначенных для корректной разметки данных и последующего применения в системах классификации и анализа сетевого трафика. Были рассмотрены методы, представляющие разные подходы к группировке данных, такие как *k*-средних, Affinity Propagation и иерархическая кластеризация. Было показано негативное влияние большого числа зависимых признаков на качество кластеризации.

Для повышения устойчивости и интерпретируемости моделей предложен метод сокращения размерности признакового пространства на основе оценки стабильности и веса признаков. Применение предложенных оценок для выбора и исключения признаков позволило улучшить компактность и разделенность кластеров.

Экспертная интерпретация выделенных кластеров позволила определить их семантическую принадлежность и использовать полученные классы для формирования системы разметки данных. Полученные результаты могут быть применены в задачах обнаружения аномалий и построения систем кибербезопасности для сетей интернета вещей.

Список литературы

[1] Dosunmu M.M., Ayo F., Ogundele L.A., Taiwo A.I. Deep packet inspection model based on support vector machine for anomaly detection in local area networks // Iraqi journal for computers and informatics, 2024, № 50, pp. 8-21.

[2] Гетьман А.И., Маркин Ю.В., Евстропов Е.Ф., Обыденков Д.О. Обзор задач и методов их решения в области классификации сетевого трафика // Труды ИСП РАН, 2017, № 29(3), С. 117-150.

[3] Шыхалиев Р.Г. Анализ и классификация сетевого трафика компьютерных сетей // İnformasiya texnologiyaları problemləri, 2010, №2, С. 15–23.

[4] AL-Akhrasa M., Alshunaybirb A.,. Omarc H, Alhazmib S. Botnet attacks detection in IoT environment using machine learning techniques // International journal of data and network science, 2023, V. 7, pp. 1683–1706.

[5] Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A. A survey of network-based intrusion detection data sets // Computers & Security, 2019, V. 86, pp. 147-167.

[6] Moustafa N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society, 2021, Vol. 72, pp. 102994.

[7] Исаева О.С., Кулясов Н.В., Исаев С.В. Создание инструментов сбора данных для анализа аспектов безопасности Интернета вещей // Информационные и математические технологии в науке и управлении, 2022, № 3(27), С.113-125.

[8] Гетьман А.И., Иконникова М.К. Обзор методов классификации сетевого трафика с использованием машинного обучения // Труды ИСП РАН, 2020, № 32(6), С. 137–154.

[9] Oudah H., Ghita B., Bakhshi T. A Novel Features set for internet traffic classification using burstiness // Proc. of the 5th International conference on information systems security and privacy, 2019, V. 1, pp. 397-404.

[10] Burschka S., Dupasquier B. Tranalyzer: Versatile high performance network traffic analyser // IEEE Symposium series on computational intelligence, 2016, pp. 1–8.

[11] Nilesh P., Rama C., Krishan S. SSK-DDoS: distributed stream processing framework based classification system for DDoS attacks // Cluster computing, 2022, № 25, pp. 1355-1372.

[12] Shafi M.M., Lashkari A.H., Roudsari A.H. NTLFlowLyzer: Towards generating an intrusion detection dataset and intruders behavior profiling through network and transport layers traffic analysis and pattern extraction // Computers & Security, 2025, V. 148, pp. 104160.

[13] Aouini Z., Pekar A. NFStream: A flexible network data analysis framework // Computer networks, 2022, V. 204, pp. 108719.

[14] Исаева О. С., Кулясов Н. В., Исаев С. В. Инфраструктура сбора данных и имитации угроз безопасности сети интернета вещей // Сибирский аэрокосмический журнал, 2025, Т. 26, № 1, С. 8–20.

[15] Киреева Н.В., Чупахина Л.Р. Частный случай исследования параметров сетевого трафика для определения законов распределения времени передачи пакетов // Международный журнал прикладных и фундаментальных исследований, 2015, № 5–3, С. 395–398.

[16] D'Angelo G., Palmieri F. Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial – temporal features extraction // Journal of network and computer applications, 2021, V. 173, pp. 102890.

[17] Денисенко В.В., Ященко А.С. Применение искусственного интеллекта для анализа сетевого трафика // Международный журнал гуманитарных и естественных наук, 2023, № 1-1(76), С. 19-22.

[18] Ермаков Р.Н. Детектирование сетевых протоколов с применением методов машинного обучения и алгоритмов нечёткой логики в системах анализа трафика // Информация и космос, 2020, №1, С. 97–109.

[19] Isaeva O.S., Kulyasov N.V., Isaev S.V. Creation of a simulation stand for studying of the internet of things' technologies // AIP Conference Proceedings, 2022, № 2647, pp. 040030.

[20] Цурко В.В., Михальский А.И. Оценка статистической связи случайных величин через взаимную информацию // Автоматика и телемеханика, 2022, В. 5, С. 76–86.