УДК 00.004.89

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ГИБРИДНОЙ СЕТИ КОХОНЕНА ДЛЯ ЗАДАЧИ КЛАСТЕРИЗАЦИИ СЕТЕВОГО ТРАФИКА

К.А. Петова[1], О.П. Солдатова[1]

[1] Самарский университет, г. Самара
e-mail: 2024-03086@students.ssau.ru

Аннотация

Целью данной работы является исследование эффективности применения гибридной сети Кохонена для задачи кластеризации сетевого трафика. Слой карты Кохонена выступает в роли инструмента для кластеризации данных, а многослойный персептрон – в роли классификатора, уточняющего полученные результаты. Для проведения исследований был использован набор данных CSE-CIC-IDS 2018.

Ключевые слова: гибридная сеть Кохонена, многослойный персептрон, кластеризация, классификация, алгоритмы обучения.

Введение

В современном мире увеличение объема IP-трафика способствует появлению новых видов сетевых атак, нацеленных на нарушение работы удаленных серверов, компьютеров и сетей. В последнее время внимание исследователей все чаще смещается в сторону применения моделей машинного обучения и нейронных сетей для детекции кибератак [1, 2].

Рассматриваемый в данной работе способ обнаружения аномалий включает в себя два этапа обработки данных: кластеризацию и классификацию трафика с помощью гибридной сети Кохонена. Поскольку обучение многослойного персептрона (MLP) производится на размеченных данных, он может давать неточные предсказания в случае появления новых угроз. При этом полученный для каждого нового неизвестного примера вектор расстояний до карты Кохонена (SOM) может использоваться для анализа ошибок MLP: если объект далёк от всех известных типов трафика, это может указывать на его нетипичный характер.

1. Анализ и предобработка данных

Для проведения исследований был выбран набор данных CSE-CIC-IDS 2018 [3]. Исходные данные представлены в виде отдельных файлов, соответствующих различным дням сбора сетевого трафика. Суммарное число записей, разделенных на 25 классов, в объединенном файле составило 63 195 145. Было решено укрупнить категории до общих типов и отбросить наименее представленные классы для повышения стабильности обучения сети. Получилось 5 классов: Benign – класс легитимного сетевого трафика; DoS и DDoS – классы атак, направленных на отказ в обслуживании; Bot – атаки, связанные с ботнетами (сетями зараженных устройств); Brute Force – вредоносная активность, характеризующаяся перебором комбинаций паролей, логинов или ключей шифрования. В ходе предобработки были удалены дубликаты, константные и мета-признаки. Итоговое число признаков составило 78.

Из полученных данных с помощью случайного разбиения было сформировано три набора – для обучения, валидации и тестирования. Такой подход был использован для оценки качества модели в условиях статистически однородных выборок.

Также проводилось разбиение данных по дням, при котором большинство подтипов укрупненных категорий попадали либо в обучающую, либо в тестовую выборку. Помимо базовых наборов, были сформированы три вспомогательные выборки тестирования: с данными, близкими к обучающему распределению; с подтипами, отличными от обучающего набора;

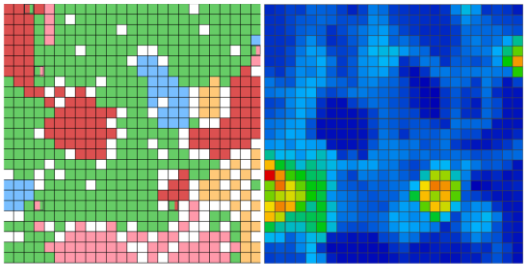
с объектами новых типов атак. В последнюю были включены записи классов Infiltration и Web Attacks, характеризующиеся скрытым проникновением в систему и эксплуатацией веб-уязвимостей. Данные выборки использовались для оценки вклада характеристик самоорганизующейся карты в интерпретацию типичности объектов и её согласованности с уверенностью классификатора, в то время как основной тестовый набор применялся для оценки обобщающей способности гибридной сети на подтипах данных, отличающихся от обучающего распределения. Для избежания утечки данных параметры нормализации вычислялись только на обучающих образцах, после чего применялись к выборкам для валидации и тестирования.

2. Проведение исследований

Для проведения первого этапа исследований были выбраны наборы данных, сформированные с помощью случайного разбиения. Обучение сети Кохонена проводилось в две фазы, отличающиеся величинами радиуса соседства и коэффициента обучения. В первой фазе (грубая настройка) для обеспечения глобальной организации карты данные параметры задавались большими значениями. Во второй фазе (тонкая настройка) для достижения локальной точности – малыми значениями [4].

Из-за дисбаланса классов в выборке для обучения использовалась циклическая сбалансированная подача данных на вход сети Кохонена для формирования устойчивости к неравномерному распределению образцов. Начальные значения весов карты задавались случайно в диапазоне минимальных и максимальных величин каждого признака. Определение меры близости входного образца до узлов двумерной решетки производилось с помощью евклидовой меры. При обучении обновлялись веса нейрона победителя и его соседей [5]. Вектор признаков, подаваемый на вход MLP, формировался из координат нейрона-победителя и расстояний до k ближайших нейронов на карте. Для проведения анализа влияния алгоритма обучения на точность классификации персептрона были выбраны два алгоритма: SGD с моментом и Adam.

В первой серии экспериментов был определен оптимальный размер карты Кохонена. Исследуемые размеры: 15 на 15, 20 на 20, 25 на 25. Для каждого из них было проведено по три эксперимента, в каждом из которых итерации двухфазного обучения масштабировались пропорционально количеству нейронов. Были установлены наилучшие параметры сети Кохонена: размер карты 25 на 25, количество итераций обучения первой и второй фазы – 320000 и 1280000. Вторая серия экспериментов была проведена при оптимальных параметрах сети Кохонена для определения наилучшего числа k, влияющего на состав признакового вектора для классификатора. Было выбрано пять значений k: 25, 31, 38, 43, 50. Оптимальное значение k составило 38. Для обеспечения сопоставимости результатов во всех описанных выше экспериментах были зафиксированы единые параметры обучения и архитектуры MLP: 10 эпох обучения, коэффициент обучения 0,001, алгоритм SGD с моментом 0,9, два скрытых слоя (128 и 64 нейрона соответственно). В третьей серии экспериментов был проведен сравнительный анализ результатов работы гибридной сети Кохонена при оптимальных параметрах и разных алгоритмах обучения: SGD с моментом и Adam. Критериями качества на тестовых данных в каждой серии являлись результаты классификации, в частности метрики: Macro Precision, Macro Recall и Macro F1-score. На рисунке 1 (а, б) представлены результаты обучения карты с оптимальными параметрами.



а б

Рисунок 1 – Результаты обучения сети Кохонена: а – карта распределения классов; б – U-matrix

На карте классов видны четко сформированные кластеры разного цвета (зеленый – класс Benign, красный – DDoS, розовый – DoS, голубой – Bot, желтый – Brute Force). Белым цветом обозначены мертвые нейроны, число которых составило 98. U-matrix, демонстрирующая расстояния между узлами решетки в пространстве весов, подтвердила сформированную структуру: плотные темно-синие области соответствуют зонам с минимальным расстоянием, а более светлые – переходам между кластерами. Самые яркие области (зеленого, оранжевого и красного цвета) указывают на наличие резкого разделения между группами.

Наилучшие результаты классификации были достигнуты при формировании вектора признаков из 40 компонентов (координаты нейрона-победителя и расстояния до 38 ближайших нейронов) и обучении персептрона с алгоритмом Adam в течение 5 эпох. Анализ отчета о классификации подтвердил стабильность модели: величина Macro F1-score оказалась равной 0,9971, Macro Precision – 0,9964, Macro Recall – 0,9979. Матрица ошибок продемонстрировала незначительное взаимное спутывание объектов класса нормального сетевого трафика Benign с объектами классов DoS и DDoS. Лучше всего сетью были распознаны классы Brute Force и Bot.

Дополнительно была проведена оценка MLP, обученного на исходных признаках. При случайном разбиении были получены сопоставимые значения метрик классификации (Macro F1-score составила 0,9989), что указывает на ограниченный вклад SOM в условиях статистически однородных данных и высокую информативность исходного признакового пространства. Следует отметить, что полученные результаты могут быть связаны с выбранной стратегией разбиения, при которой обучающая и тестовая выборки имеют близкие статистические характеристики.

В связи с этим было проведено исследование с разбиением данных по дням для оценки способности модели классифицировать ранее не наблюдавшиеся подтипы атак. Для этого были использованы оптимальные параметры и архитектура гибридной сети, определенные ранее.

При данном подходе было выявлено существенное снижение качества классификации, при этом для типа DDoS показатели резко ухудшились (F1-score = 0,0034), тогда как для классов Benign и DoS метрики остались высокими (около 0,9). Такие результаты указывают на зависимость обобщающей способности модели от типа трафика. Рост ошибки квантования SOM подтвердил наличие сдвига в данных: значение QE увеличилось с 0,607 на обучающей выборке до 2,118 на тестовой. Это свидетельствует о значительных различиях между обучающими и тестовыми данными и появлении новых типов данных.

Для оценки вклада SOM в интерпретацию результатов классификации был введён дополнительный слой принятия решений, основанный на классификации MLP и наборе метрик, описывающих положение и свойства объекта в пространстве слоя SOM. С помощью данной комбинации рассчитывалась оценка, по которой объект относился к одной из категорий: надежный, сомнительный или атипичный. Установлено, что при использовании слоя принятия решений для выборки, близкой к обучающему распределению, доля сомнительных и атипичных объектов оказалась низкой (около 7%), тогда как для ранее неизвестных типов сетевого трафика она возросла до 44,27%. В частности, для класса Web_XSS большинство объектов было отнесено к сомнительным и атипичным, что отражает их существенное отличие от обучающих примеров. Несмотря на ухудшение качества классификации, для выборки, содержащей подтипы известных атак, не использованных при обучении, доля объектов, отнесённых к сомнительным и атипичным, оказалась достаточно низкой (4,31%). Большинству образцов класса DDoS, ошибочно отнесенных MLP к классу Benign, был присвоен статус надежных из-за того, что вычисленные характеристики SOM (расстояние до нейрона победителя, чистота нейрона, частота активации и т. д.) не зафиксировали отклонений от обучающего распределения.

Таким образом, слой принятия решений демонстрирует способность SOM к частичному выявлению атипичных объектов. Даже при высокой уверенности MLP анализ самоорганизующейся карты позволяет обнаруживать структурно отличающиеся примеры.

Тем не менее, эффективность подхода ограничена случаями, когда ошибочно классифицированные объекты попадают в плотные области, ассоциированные с другими классами: в таких ситуациях признаки атипичности отсутствуют, и ошибки не выявляются, что указывает на необходимость дальнейшего развития метода.

Заключение

В ходе исследования было проведено обучение и тестирование гибридной сети Кохонена. Применение SOM позволило снизить размерность признакового пространства (с 78 до 40 признаков) и сформировать основные кластеры сетевого трафика. Такой подход обеспечил высокую эффективность последующей классификации при случайном разбиении данных, что было подтверждено при анализе результатов тестирования сети. При разбиении данных по дням было показано снижение обобщающей способности модели, при этом введенный слой принятия решений позволил частично выявлять нетипичные и ранее не наблюдавшиеся объекты. Таким образом, использование SOM обеспечивает анализ структуры данных и выявление отклонений от обучающего распределения, тогда как MLP отвечает за точность классификации. Такое сочетание делает гибридный подход более устойчивым к изменениям входных данных и расширяет его возможности по обнаружению аномалий.

Список использованных источников

1. Баклашов, А. С. Статистические и плотностные методы кластеризации в задачах обнаружения аномалий сетевых систем: сравнительный анализ / А. С. Баклашов, Д. С. Кулябов // Discrete and Continuous Models and Applied Computational Science. – 2025. – Т. 33, № 1. – С. 27–45.

2. Селиверстов, Д. Е. Применение искусственного интеллекта в задачах обнаружения деструктивных воздействий на информационные и технические системы / Д. Е. Селиверстов, К. Д. Русаков // Известия Юго-Западного Государственного университета. – 2025. – Т. 29, № 4. – С. 125–139.

3. DistriNet Research Unit. – URL: https://intrusion-detection.distrinet-research.be/CNS2022/CSECICIDS2018.html (дата обращения: 02.03.2026).

4. Kohonen, T. Self-Organizing Maps / T. Kohonen. – Berlin; Heidelberg: Springer, 2001. – 501 p.

5. Осовский, С. Нейронные сети для обработки информации / С. Осовский. – М. : Финансы и статистика, 2002. – 344 с.

STUDY OF THE EFFECTIVENESS OF USING A KOHONEN HYBRID NETWORK FOR THE NETWORK TRAFFIC CLUSTERING TASK

K.A. Petova[1], O.P. Soldatova[1]

[1]Samara University, Samara
e-mail: 2024-03086@students.ssau.ru

Abstract

The aim of this work is to investigate the effectiveness of applying a hybrid Kohonen network to the task of network traffic clustering. The Kohonen map layer serves as a tool for data clustering, while the multilayer perceptron acts as a classifier refining the obtained results. The CSE-CIC-IDS 2018 dataset was used for the study.

Keywords: hybrid Kohonen network, multilayer perceptron, clustering, classification, learning algorithms.