АНАЛИЗ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ КЛАССИФИКАЦИИ ИНТЕРНЕТ ТРАФИКА

Латыпов Родион Дамирович

студент, Московский государственный технический университет имени Н.Э. Баумана, РФ, г. Москва

Гудков Олег Владимирович

научный руководитель, старший преподаватель, Московский государственный технический университет имени Н.Э. Баумана, РФ, г. Москва

Введение

Первые системы классификации трафика основывались на извлечении из пакетов номеров портов и сопоставлении их со списком, например, под протокол HTTP выделен порт 80. Информацию о протоколе можно уже использовать для примерного определения типа деятельности пользователя. Этот метод классификации работает очень быстро и не требует хранения данных о потоке, вычислительно прост. Однако, номер порта определён не для всех протоколов, а некоторые протоколы выбирают порты для обмена данными в ходе своей работы случайным образом (как FTP). Вдобавок, некоторые протоколы могут использовать известные номера портов других протоколов, чтобы замаскироваться под них, если другой протокол является более предпочтительным с точки зрения интернет-провайдера. Следующим шагом развития классификаторов интернет трафика стало использование технологии DPI (Deep Packet Inspection, глубокий анализ пакетов). Фильтрация сетевых пакетов в этом случае проводится по их полному содержимому, то есть проводится анализ не только заголовков, но и всего трафика на уровнях модели OSI со второго и выше. Этот метод показывает высокую точность работы, а полученная с его помощью разметка зачастую принимается как эталонная для данных с неизвестными классами. Для классификации с помощью DPI создаётся библиотека сигнатур и шаблонов пакетов, и для каждого пакета производится поиск соответствий в этой библиотеке. При всех своих достоинствах метод DPI сталкивается с существенными проблемами в своей работе. Среди главных – невозможность работы с зашифрованным трафиком, доля которого в Интернете растёт с каждым годом, и высокие требования к ресурсам. Для хранения данных пакетов и библиотеки сигнатур требуется достаточно большой объём памяти, а при росте количества известных классов растёт размер этой библиотеки и, соответственно, время на поиск соответствий в ней. Поэтому, этот метод плохо подходит для работы в высокоскоростных сетях в режиме реального времени. Кроме того, определённую сложность представляет создание и поддержание в актуальном состоянии библиотеки сигнатур при всё увеличивающемся количестве протоколов и приложений в Сети. Тенденции изменения сетевого трафика, широкое распространение шифрования, рост скорости передачи данных, а соответственно и необходимой скорости их обработки, постоянное появление новых классов трафика - всё это потребовало появления новых способов его классификации. Для этого были предложены методы машинного обучения, которые позволяют во многом упростить работу с созданием наборов различающих характеристик классов, автоматизируя этот процесс на основе анализа большого количества примеров этих классов (собрать который значительно проще, чем проанализировать вручную). Кроме того, многие из предложенных методов работают с общими признаками потоков, а не с полезной нагрузкой пакетов, что решает проблемы, связанные с шифрованием и с защитой данных пользователей. Это же даёт преимущество в скорости классификации и уменьшает необходимый для принятия решения объём памяти [1].

Латыпов Р.Д. АНАЛИЗ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ КЛАССИФИКАЦИИ ИНТЕРНЕТ ТРАФИКА // Студенческий форум: электрон. научн. журн. 2022. № 20(199). URL: https://nauchforum.ru/journal/stud/199/113013 (дата обращения: 02.09.2025).

Подготовка данных для анализа

Для анализа пакетов методами машинного обучения необходимо выделить признаки на основе которых будет приниматься решение. При классификации сетевого трафика можно выделить следующие виды признаков:

- статистические признаки – выделенные экспертом характеристики потока, такие как средняя длина пакетов или максимальное время отклика;
- данные пакета – содержимое полезной нагрузки или все байты пакета вместе с заголовками;
- метаинформация о пакете – информация о пакете, такая как размер пакета, используемый протокол или размер его полезной нагрузки.

В данной работе было принято использовать все байты пакетов, так как это позволяет построить наиболее точный классификатор, устойчивый к намеренным попыткам замаскировать поступающий пакет под другой класс.

Так как для работы нейронных сетей необходимо фиксированное количество входных признаков, было принято решение использовать только первые 256 байтов пакета. Для представления данных в необходимом для работы нейронной сети виде поделим значение каждого байта на максимальное значение: 255. Таким образом каждый байт данных пакета будет представлять собой значение (0,1). В случае если длина исходного пакета данных будет меньше 256 байт, недостающие значения будут заполнены 0.

Классификация отдельно взятых пакетов может быть неточной так как в пределах одного взятого потока могут находиться пакеты существенно различающиеся по структуре и набору данных. В связи с чем было принято решение классифицировать не отдельные пакеты трафика, а потоки. Потоки формируются на основе значений адресов, портов и типов транспортного протокола пакетов. Как показано в работе [2] для классификации достаточно взять значения байтов первых 6 пакетов каждого потока, которые склеиваются вместе и подаются на вход нейронной сети.

Многослойная нейронная сеть

Искусственные нейронные сети состоят из нескольких слоёв искусственных нейронов, каждый из которых получает на вход несколько числовых значений и преобразует их в выходное значение в соответствии со своими внутренними правилами (заранее заданной функцией активации и вычисляемыми весами входных параметров). Слой сети может состоять из произвольного числа нейронов, каждый из которых может быть соединён с любыми нейронами из предыдущего и последующего слоёв.

Для решения задач классификации хорошо подходят многослойные нейронные сети прямого распространения (рисунок 1). Первый слой является входным, на его нейроны поступают данные пакетов. Последний слой нейронной сети является выходным. С него считывается информация о принадлежности пакета классу, за который отвечает эта сеть. Для определения класса поступающих пакетов строится несколько подобных нейронных сетей, каждая их которых обучается определять свой тип входящих пакетов.

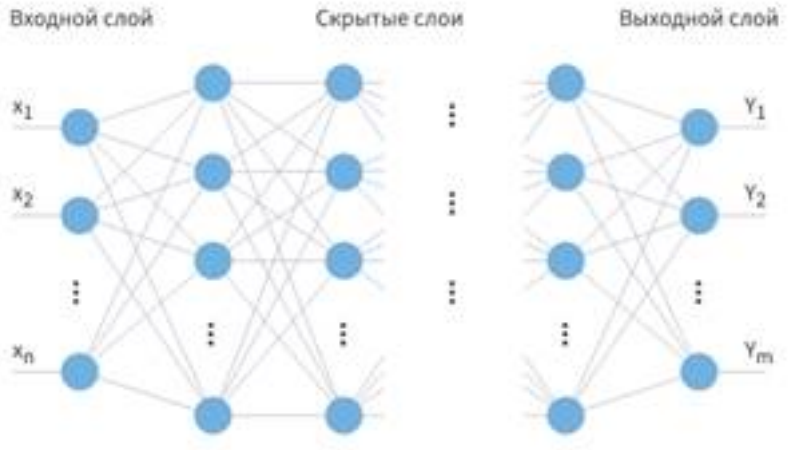

Рисунок 1. Схема многослойной нейронной сети

Между входным и выходным слоем располагаются один или несколько промежуточных, или скрытых слоёв. Скрытыми они называются по тому, что их входы и выходы неизвестны для внешних по отношению к нейронной сети программам и пользователю [3].

Свёрточная нейронная сеть

Свёрточная нейронная сеть (представлена на рисунке 2) – является одним из видов искусственных нейронных сетей. В отличие от полносвязной нейронной сети, где каждый нейрон предыдущего слоя связан с каждым нейроном следующего слоя, в свёрточной нейронной сети используется лишь ограниченная матрица весов, которая двигается по всему обрабатываемому слою. Принцип работы основан на поэтапной свёртке входных параметров исследуемого пакета. Архитектура сети представляет собой череду свёрточных слоёв и слоёв подвыборки, после которых идёт полносвязная нейронная сеть.

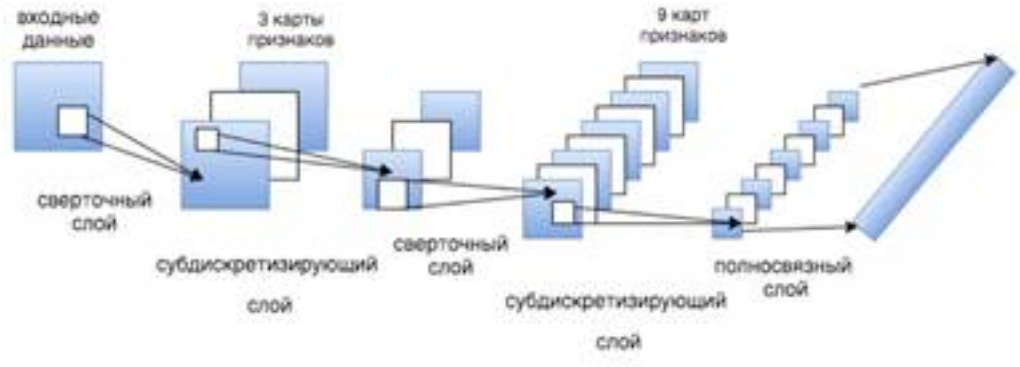

Рисунок 2. Схема свёрточной нейронной сети

Обучение нейронной сети производится методом обратного распространения ошибки. Выходное значение нейронной сети сравнивается с ожидаемым, и в зависимости от разницы производится перенастройка весов нейронов полносвязной сети и матриц весов свёрточной сети.

Свёрточная нейронная сеть позволяет находить зависимости между соседними байтами в сетевых пакетах, что позволяет находить собственные шаблоны для каждого класса

протоколов/приложений и, следовательно, повышает точность классификации трафика [4].

Автокодировщик

Автокодировщик – особый тип нейронных сетей, обучающийся методом обратного распространения ошибки без учителя. Архитектура автокодировщика не отличается от архитектуры полносвязной нейронной сети, за исключением того, что входной и выходной слои автокодировщика обязательно должны иметь равную длину. Схема автокодировщика представлена на рисунке 3.

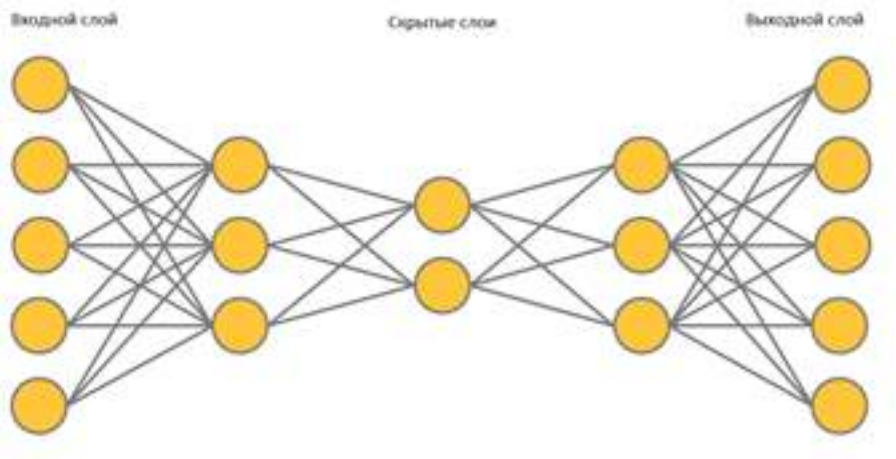

Рисунок 3. Схема автокодировщика

Основной принцип работы автокодировщика заключается в том, что на выходном слое необходимо получить отклик наиболее близкий к входному сигналу. Для того, чтобы нейронная сеть не принимала каждый поступающий пакет за свой, между входным и выходным слоями располагают скрытые слои. Количество нейронов скрытых слоёв должно быть меньше количества нейронов на входном слое. Таким образом в процессе работы данные поступающие на вход сначала сжимаются, а потом восстанавливаются обратно. В процессе обучения автокодировщик учится сжимать и восстанавливать пакеты одного типа, выделяя из данных общие признаки. Обученная нейронная сеть хорошо справляется с восстановлением пакетов того типа на котором производилось обучение, и некорректно востанавливает пакеты других типов, благодаря чему можно сделать вывод о принадлежности исследуемого пакета к классу, на котором производилось обучение, на основе разницы между входным и выходным слоями.

Рекуррентная нейронная сеть

В рекурентных нейронных сетях на результат работы нейронной сети влияет не только текущий исследуемый пакет, но и отклик на предыдущие исследованные пакеты. Таким образом можно анализировать цепочку связанных пакетов, например, несколько подряд идущих пакетов потока.

Для реализации возможности «запоминать» информацию об уже проанализированных пакетах, необходимо помимо выходного вектора сети, сохранять вектор, описывающий внутреннее состояние сети. То есть вектор в котором будут содержать воспоминания об уже проанализированных пакетах.

Существует много разновидностей рекуррентных, но для нашей задачи наиболее подходящей является сеть с долгой краткосрочной памятью. Помимо сохранения внутреннего состояния сети в архитектуру данной сети добавлены входные м выходные вентили, влияют на то, какие из входных данных окажут влияние на внутреннее состояние ячейки, и что из внутреннего

состояния окажет влияние на выход сети. Схема блока сети представлена на рисунке 4. «Входной вентиль» контролирует меру вхождения нового значения в память, а «вентиль забывания» контролирует меру сохранения значения в памяти. «Выходной вентиль» контролирует меру того, в какой степени значение, находящееся в памяти, используется при расчёте выходной функции активации для блока.

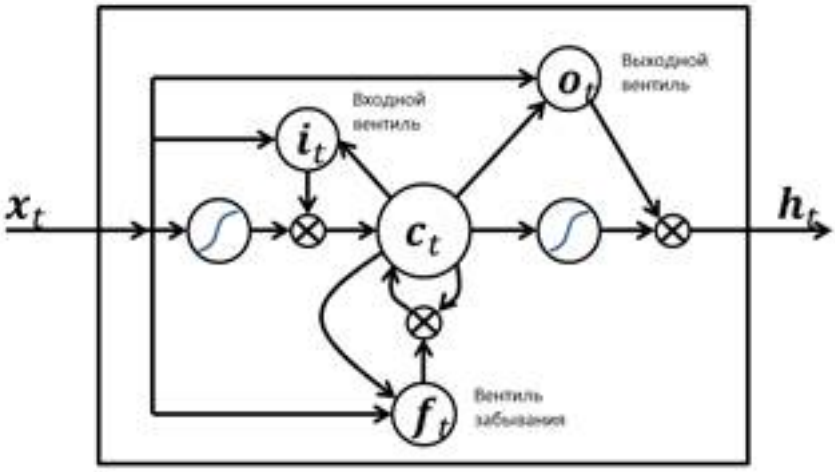

Рисунок 4. Схема блока сети с долгой краткосрочной памятью

Так как данная разновидность нейронных сетей сохраняет информацию о предыдущих пакетов исследуемого потока, она может с высокой точностью классифицировать поток. Благодаря тому, что пакеты анализируются раздельно, при создании нового потока данная сеть может предположить класс потока, ещё до того, как наберётся достаточное количество пакетов для классификации другими методами, и корректировать своё решение с увеличением количества входных данных.

Результаты исследования

Для каждого класса данных было сформировано по одной нейросети каждого типа: многослойноя нейронная сеть, свёрточная нейронная сеть, автокодировщик, рекурентная нейронная сеть. Подготовленные данные были поделены: 1000 потоков каждого из классов были переданы на обучение, а 100 потоков – на тестирование.

После обучения на вход каждого классификатора были переданы все тестовые потоки для определения точности классификации. На основе полученных данных были вычислены следующие метрики

Точность (precision) – показывает какую долю из объектов, названных классификатором положительными – на самом деле являются положительными.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

Полнота (recall) – показывает какую долю из объектов положительного класса нашёл классификатор.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

F-мера – среднее гармоническое precision и recall.

$$F_1 = \frac{2 * \text{precision} * \text{recall}}{\text{precision} + \text{recall}}$$

Метрики рассчитывались отдельно для каждого класса, после чего были вычислены их средние значения для каждого из классификаторов. Средние значения метрик precision, recall и F_1 представленны в таблице 1.

Таблица 1.

Показатели работы классификаторов интернет трафика

Классификатор	Precision	Recall	F_1
Многослойноя нейронная сеть	0,830	0,837	0,82
Свёрточная нейронная сеть	0,923	0,932	0,91
Автокодировщик	0,924	0,913	0,90
Рекурентная нейронная сеть	0,886	0,879	0,86

Как видно из таблицы самым точным оказался алгоритм свёрточной нейронной сети, однако автокодировщик несущественно отстаёт от свёрточной нейронной сети в точности, и обладает существенным преимуществом в виде возможности обучаться без учителя.

Наименее точным оказался алгоритм полносвязной многослойной нейронной сети. Алгоритм является наиболее простым из представленных, в связи с чем результат эксперимента ожидаем.

Список литературы:

1. Гетьман А.И., Иконникова М.К. Обзор методов классификации сетевого трафика с использованием машинного обучения. Труды Института системного программирования РАН. 2020;32(6):137-154.

2. S. Rezaei, B. Kroencke and X. Liu, "Large-Scale Mobile App Identification Using Deep Learning," in IEEE Access, vol. 8, pp. 348-362, 2020.

3. Аналитическая платформа Loginom [Электронный ресурс] – Режим доступа - https://wiki.loginom.ru/articles/multilayer-neural-net.html (Дата обращения 11.10.2021)

4. Lotfollahi M., Jafari Siavoshani M., Shirali Hossein Zade R. Deep packet: a novel approach for encrypted traffic classification using deep learning. Soft Computing, vol. 24, issue 3, 2020, pp. 1999-2012.