ния равновесной формы нити, он пишет: «Формы равновесия в плоскости орбиты задаются графиками однопараметрического семейства эллиптического синуса».

СПИСОК ЛИТЕРАТУРЫ

1. Math24.ru / Уравнение-цепной-линии. html.
2. Меркин Д.Р. Введение в механику гибкой нити. / Д.Р. Меркин. – М.: Наука. – 1980.
3. Аппель П. Теоретическая механика. / П. Аппель. – М.: ГИФМЛ. – 1960. Т. I.
4. Белецкий В.В. Динамика космических тросовых систем. / В.В. Белецкий, Е.М. Левин. – М.: Наука. – 1990.
5. Адлай С. Ф. Исследование устойчивости равновесных форм нити в окрестности спутника на круговой орбите // Вестник Нижегородского университета им. Н.И. Лобачевского, том 1, № 4 (2), 2011. С. 27-28.
6. Минаков А.П. Основы механики нити. / А.П. Минаков. // Научно-исследовательские труды Московского текстильного института. – 1941. – т. 9. – вып. 1.
7. Щедров В.С. Основы механики гибкой нити. / В.С. Щедров. – М.: Машгиз. – 1961.

УДК 004.032.26 : 004.85

Черниговский Александр Валерьевич,
аспирант кафедры «Вычислительные машины, комплексы, системы и сети», ФГБОУ ВО «Ангарский государственный технический университет», тел. 89041112385, e-mail: chernigovsky.alex@gmail.com
Кривов Максим Викторович,
к.т.н., доцент, зав. кафедрой «Вычислительные машины, комплексы, системы и сети», ФГБОУ ВО «Ангарский государственный технический университет», тел. 89025614935, e-mail: vmk@angtu.ru

НЕЙРОННЫЕ СЕТИ КАК ИНСТРУМЕНТ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Chernigovskiy A.V., Krivov M.V.

NEURAL NETWORKS AS AN INSTRUMENT OF ANALYSIS OF NETWORK TRAFFIC

Аннотация. *В статье рассмотрены основные способы классификации сетевого трафика. Показано, что в настоящее время особый интерес в данной области представляют системы машинного обучения, основанные на применении нейронных сетей. Сравнение основных типов искусственных нейронных сетей показало, что для регулирования трафика в условиях ограниченной производительности могут быть использованы рекуррентные нейронные сети.*

Ключевые слова: *сетевой трафик, классификация, искусственные нейронные сети, сверточные нейронные сети, рекуррентные нейронные сети.*

Abstract. *In this paper basic methods of network traffic classification were considered. It was shown that at present, machine learning systems based on neural networks are of particular interest in this area. Comparison of the main types of artificial neural networks showed that to regulate traffic in conditions of limited performance RNN can be used.*

Keywords: *network traffic, classification, artificial neural networks, convolutional neural networks, recurrent neural networks.*

Важность сетевых коммуникаций в современном мире сложно переоценить. При этом не менее серьезной задачей является правильная классификация и регулирование сетевого трафика. Данная потребность обусловлена:

- возрастающими сетевыми нагрузками;
- ограниченной пропускной способностью существующих каналов связи;
- возрастающими требованиями к улучшению сетевых сервисов;
- растущими потребностями в качестве и скорости передачи и обработки данных.

Точная идентификация трафика важна для мониторинга безопасности, повышения

качества обслуживания и прогнозирования сетевых нагрузок. Кроме того, она находит свое применение в сетевой безопасности и для QoS, как инструмент оптимизации и управления системой [1].

Классификация сетевого трафика может основываться на различных параметрах передаваемых данных, таких, как IP-адрес, тип данных, приложение, номер порта, время между пакетами, задержка и т.д. Поэтому, цель данной работы – изучить существующие способы классификации сетевого трафика, а также рассмотреть возможность применения алгоритмов, основанных на нейронных сетях, для анализа трафика.

Любой поступающий пакет данных состоит из заголовка различных уровней (рисунок 1) и, собственно, передаваемой информации. Поэтому, первоначально наиболее простым решением стала классификация, основанная именно на этих сведениях.

Достаточно продолжительное время в системах мониторинга трафика применялась классификация на основе номеров портов сетевого и транспортного уровня OSI. Это позволяло определять принадлежность данных к конкретному приложению на основе номера порта, указанного в заголовке пакета, а также получать общую характеристику сети. Как правило, такая классификация носила либо протокольный, либо статистический характер. В первом случае процедура опиралась на эвристику, полученную эмпирически на основе сведений только о значении портов, видимых в заголовках пакетов, а во втором – на более глубокий анализ пакетов.

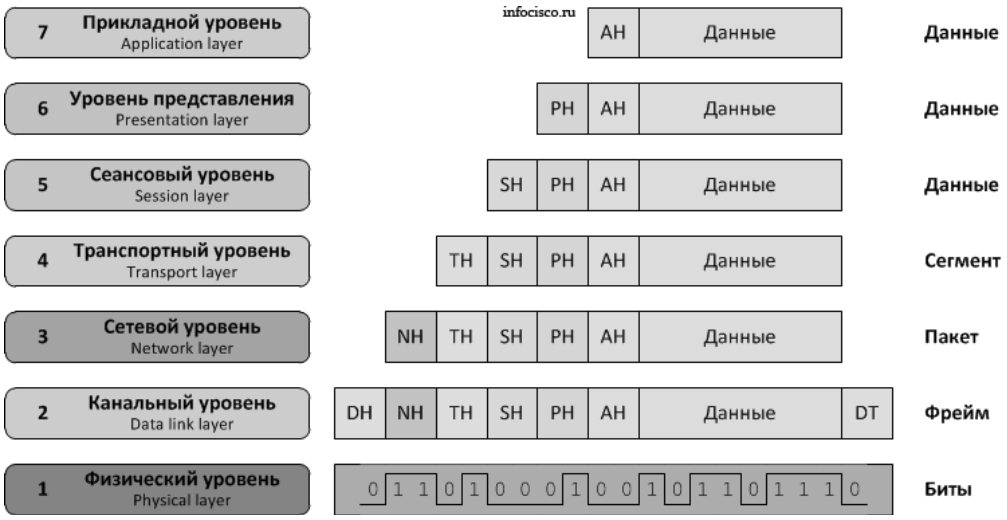

Рисунок 1 – Уровни заголовка согласно модели OSI

Первый метод осуществлял классификацию трафика, исходя из значений портов, т.е. базировался на данных протокола транспортного уровня. Достоинством первого способа являются достаточно низкие системные требования вследствие небольшого количества анализируемых данных и анализа только заголовков пакетов.

Однако в настоящее время программы зачастую не имеют стандартного порта, что связано с попыткой программ обойти файерволл и мониторы безопасности. В связи с этим они применяют различные способы шифрования передаваемых данных – туннелирование, инкапсуляцию и ряд других технологий. И если раньше такой метод давал достаточно точную классификацию сетевых приложений, то сейчас отмечается [2], что его результативность и точность стали достаточно низки.

Статистический метод, применяемый для классификации трафика, основывается на технологии глубокого анализа пакетов DPI (Deep Packet Inspector). Он позволяет анализировать не только заголовки сетевых пакетов, но и полное содержание пакетов, и работает с данными, начиная с канального уровня OSI и выше.

Результатом работы технологии DPI является получение многоуровневой сигнатуры для каждого приложения, а также осуществление поведенческого анализа, основанного на сведениях о структуре передаваемых данных [3].

К положительным сторонам данного метода можно отнести возможность работы со сложными данными потокового мультимедиа, одноранговых сетей и т.д., а также высокую точность получаемых результатов классификации вследствие глубокого и более полного анализа данных.

Однако одна из основных проблем такой классификации трафика – это необходимость обработки огромного количества данных и, соответственно, огромные вычислительные мощности системы, через которую проходит трафик. Кроме того, под каждое новое приложение необходимо обновлять сигнатуру классификации, что достаточно сложно. Также к недостатку DPI относят неспособность работать с зашифрованным трафиком, т.к. получение данных с верхнего уровня чревато нарушениями конфиденциальности и нарушением закона о защите персональных данных. И самый большой недостаток полноценных DPI-систем – это высокая стоимость программного комплекса.

Таким образом, в современных условиях традиционные методы классификации трафика требуют пересмотра их основной концепции, а также повышения эффективности при снижении финансовых и системных ресурсов с целью соответствия современным потребностям. В настоящее время активно ведутся разработки новых методов анализа трафика, основанных на его статистических свойствах (размер пакета, время между пакетами и др.), и реализуемых с помощью искусственного интеллекта [4, 5].

Системы искусственного интеллекта не только позволяют проводить распознавание речи и изображений, но и являются основой различных экспертных систем и систем машинного зрения.

Работа таких систем включает три основных этапа:

- обучение, которое, как правило, производится на некоторой эталонной модели;
- рассуждение, к какому классу отнести новый обнаруженный объект;
- самокоррекция, т.е. изменение своих поведенческих настроек, что по сути приводит к самообучению системы.

Среди методов искусственного интеллекта можно выделить два самых важных – машинное обучение и глубокое обучение (рисунок 2).

Машинное обучение – это одна из областей искусственного интеллекта, основанная на системах и алгоритмах, способных обучаться на основе исходных данных и накопленного опыта работы активной сети.

Рисунок 2 – Структура искусственного интеллекта

Существует два способа машинного обучения: контролируемое обучение, также известное как обучение с учителем, и неконтролируемое – обучение без учителя [6].

Контролируемое обучение включает в себя процедуру, в которой обучающий набор дается в качестве входных данных для системы, где каждый пример помечен желаемым выходным значением. Обучение в этом типе выполняется с использованием минимизации конкретной функции потерь, которая представляет ошибку вывода относительно требуемой системы вывода (рисунок 3).

После завершения обучения точность каждой модели измеряется в отношении непересекающихся примеров из обучающего набора, также называемого проверочным набором.

К основным методам обучения с учителем относят:

- однослойный персептрон;
- метод k-ближайших соседей;
- метод опорных векторов;
- метод обратного распространения ошибки.

В обучении без учителя используются примеры обучения, которые не обозначены системой, к которой они относятся. Система ищет данные, которые имеют общие характеристики, и изменяет их, основываясь на

внутренних особенностях знаний (рисунок 4). Этот тип алгоритмов обучения, в основном, используется при кластеризации.

К основным методам обучения без учителя относят многослойный персептрон, метод k-средних, самоорганизующиеся карты Кохонена.

Глубокое обучение – это часть машинного обучения, которая отличается большей эффективностью и гибкостью по сравнению с базовым методом благодаря использованию иерархического обучения. Принцип действия глубокого обучения сводится к последовательному усложнению архитектуры слоев, что, в итоге, приводит к определению категорий через скрытую информацию о слоях.

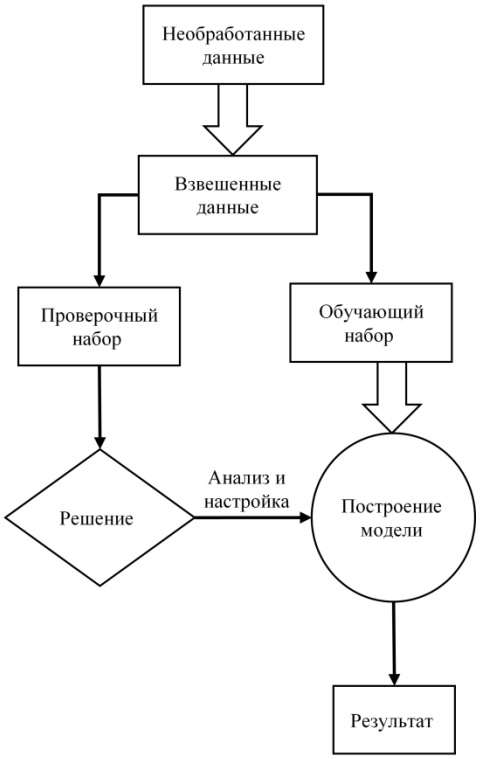

Рисунок 3 – Алгоритм обучения с учителем

Вся ценность глубокого обучения сегодня заключается в контролируемом обучении или обучении с использованием маркированных данных и алгоритмов.

Каждый алгоритм глубокого обучения проходит один и тот же процесс. Он включает в себя иерархию нелинейного преобразования входных данных, которые можно использовать для создания статистической модели в качестве выходных данных.

Рассмотрим следующие шаги, которые определяют процесс машинного обучения:

- идентификация соответствующих наборов данных и подготовка их для анализа;
- выбор типа алгоритма для использования;
- создание аналитической модели на основе используемого алгоритма;
- обучение модели на тестовых наборах данных, пересматривая ее по мере необходимости;
- запуск модели для генерации результатов тестов.

Рисунок 4 – Алгоритм обучения без учителя

Разница между машинным и глубоким обучением состоит в том, что при увеличении исходного количества параметров для машинного обучения наблюдается невысокий прирост производительности в то время, как для глубокого обучения эффективность работы возрастает почти экспоненциально (рисунок 5). Поэтому метод глубокого обучения существенно превосходит машинное и представляет огромный интерес для исследователей.

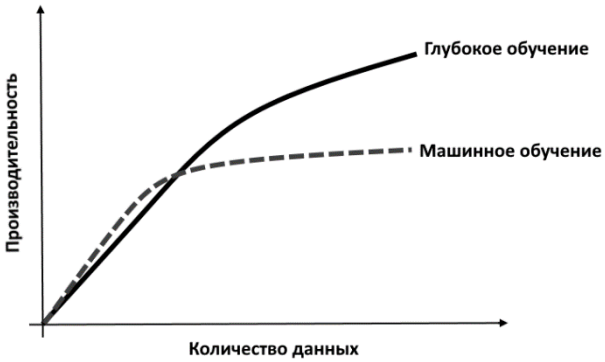

Рисунок 5 – Зависимость эффективности системы от количества используемых данных

В системах глубокого обучения используются два основных типа нейронных сетей:

1. Сверточные нейронные сети (CNN);
2. Рекуррентные нейронные сети (RNN).

Сверточная нейронная сеть представляет собой многослойный персептрон, который является специальной конструкцией для идентификации информации двумерного изображения. Такой тип сети применяется, в первую очередь, для распознавания изображений и распознавания лиц.

Основное различие между CNN и обычной нейронной сетью состоит в том, что CNN принимает входные данные в виде двумерного массива и работает непосредственно с изображениями, а не фокусируется на извлечении признаков, на которых сосредоточены другие нейронные сети.

Как правило, такие сети имеют несколько слоев:

- входной слой, который содержит исходные данные в виде двухмерной матрицы определенного размера;
- слой свертки, или уровень объединения, на котором происходит преобразование («свёртка») исходных данных с формированием новой матрицы меньшего размера. Для осуществления процесса свертки используется матрица весов (так называемое ядро свертки). При ее движении со смещением происходит преобразование небольшого фрагмента исходной матрицы в один элемент матрицы следующего слоя. Таким образом, формируется новый сжатый слой. Отображение соединений от входного слоя к карте скрытых объектов определяется как «общие веса», а включенное смещение называется «общим смещением»;
- слой подвыборки (также называется слоем субдискретизации или слоем пулинга), который предназначен для уплотнения предыдущего слоя. Он появляется в тот момент, когда для последующего обучения нет необходимости в сохранении заданной точности. В настоящее время является необязательным;
- выходной слой, который представляет собой персептрон, работающий как обычная нейронная сеть.

Кроме того, в глубокой сетевой архитектуре уровень свертки и уровень подвыборки могут быть представлены несколькими слоями.

CNN использует пространственные корреляции, которые существуют во входных данных. Каждый параллельный слой нейронной сети соединяет несколько входных нейронов. Этот конкретный регион называется локальным рецептивным полем. Местное рецептивное поле фокусируется на скрытых нейронах. Скрытые нейроны обрабатывают входные данные внутри упомянутого поля, не осознавая изменений за пределами определенной границы (рисунок 6).

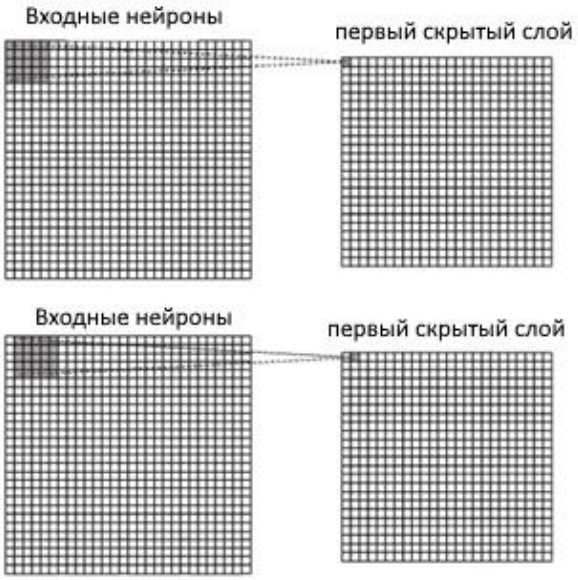

Рисунок 6 – Механизм построения сверточного слоя при работе CNN

С точки зрения системных требований CNN достаточно удобны. Это связано, в первую очередь, с упрощением вычислений благодаря упрощению входной матрицы и, как следствие, уменьшению количества обрабатываемых данных. Кроме того, такая система характеризуется достаточной устойчивостью к ошибкам [7].

В качестве недостатков CNN стоит отметить отсутствие единого правила подбора параметров сети. Это означает, что основные характеристики такой сети необходимо будет подбирать вручную для каждой отдельной задачи, что делает данные сети неприменимыми для анализа сетевого трафика.

Рекуррентные нейронные сети – это тип глубоко ориентированного на обучение алгоритма, который следует последовательному подходу. В отличие от классических нейронных сетей, где информация передается только в одном направлении – от предыдущего слоя к последующему, в рекуррентных сетях используется принцип обратного распространения, который реализован путем добавления к данным, поступающим на текущий слой нейронов, сведений о предыдущем состоянии системы. Благодаря этому у нейронной сети формируется функция памяти, что делает такие сети более эффективными [8].

Рассмотрим следующие шаги для обучения рекуррентной нейронной сети:

1. Ввод конкретного примера из имеющегося набора данных;
2. Произведение сетью вычислений на основе примера с использованием некоторых случайно определенных переменных;
3. Вычисление прогноза результата;
4. Выявление ошибки между фактически полученным и ожидаемым значением результата;
5. Коррекция переменных путем отслеживания ошибки по аналогичному пути распространения.

Данные этапы обучения повторяются до достижения достаточно полной сходимости переменных, необходимых для получения выходных данных.

С помощью переменных, полученных таким образом, выполняется прогнозирование данных, которые поступят на следующий слой (рисунок 7).

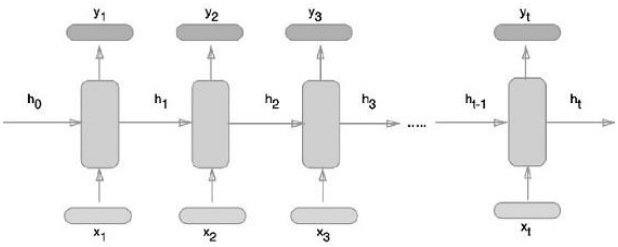

Рисунок 7 – Алгоритм работы рекуррентных нейронных сетей:
x_i и y_i – входные и выходные данные i-го слоя, соответственно; h_i – сведения о предыдущем состоянии системы.

Примером рекуррентной нейронной сети могут служить:

- сеть Хопфилда;
- сеть Элмана;
- сеть Коско или двунаправленная ассоциативная память;
- LSTM-сеть.

Рекуррентные нейронные сети нашли свое применение в синтезе и распознавании речи, машинном переводе, обработке и стилизации изображений и других областях.

К достоинствам RNN относятся, прежде всего, наличие функции памяти, возможность работы с данными, зависящими от времени, либо с данными, разбитыми на более мелкие фрагменты, а также более высокая точность получаемых данных.

Использование функции памяти, в то же время, приводит к увеличению количества обрабатываемых данных, что влечет за собой усложнение вычислений и повышение системных требований.

Однако, несмотря на вышеуказанные недостатки, рекуррентные нейронные сети характеризуются достаточной надежностью получаемых результатов, что в сочетании с относительно низкими системными требованиями по сравнению с DPI делает их привлекательными для применения в качестве компонентов систем анализа сетевого трафика.

СПИСОК ЛИТЕРАТУРЫ

1. Черниговский, А.В. Анализ методов распределения сетевого трафика между пользователями сети / А.В. Черниговский, М.В. Кривов // Вестник АнГТУ. – 2018. – № 12. – С. 168-173.

2. Moore, A. W. Toward the accurate identification of network applications / A. W. Moore, K. Papagiannaki // Passive and Active Network Measurement. 2005. pp 41-54.

3. Liao, M.-Y. Design and evaluation of deep packet inspection system: a case study / M.-Y. Liao, M.-Y. Luo, C.-S. Yang, C.-H. Chen, P.-C. Wu, Y.-W. Chen // The Institution

of Engineering and Technology. – 2012. Pp. 1 – 8.

4. Trivedi, Chintan. Classification of Internet Traffic using Artificial Neural Networks / Chintan Trivedi, Mo-Yuen Chow, Arne Nilsson, H. Joel Trussell // Department of Electrical and Computer Engineering. – pp. 1 -10.

5. Michael, A. K. Network traffic classification via neural networks / Michael A. K. J., Valla E., Neggatu N. S., Moore A. W. // Technical report. – University of Cambridge. – 2017, September. – 25 p.

6. Nielsen, Michael. Neural Networks and Deep Learning / The original online book. – pp. 1-224.

7. Khan, Asifullah. A Survey of the Recent Architectures of Deep Convolutional Neural Networks / Asifullah Khan, Anabia Sohail, Umme Zahoora, Aqsa Saeed Qureshi // Deep Learning Lab, pp 1-67.

8. Salehinejad, Hojjat. Recent Advances in Recurrent Neural Networks / Hojjat Salehinejad, Sharan Sankar, Joseph Barfett, Errol Colak, Shahrokh Valaee // - 2018. pp 1- 22.