Проанализировав результаты проведенных экспериментов, можно сделать вывод о том, что автоматизированная система распознавания римских цифр работает эффективно. Из результатов также видно, что процент верных распознаваний римских цифр с помощью нейронной сети Кохонена уменьшается с увеличением коэффициента обучения. Сравнивая результаты экспериментов, проделанных при помощи алгоритма Кохонена с разными типами соседства можно сделать вывод: при использовании алгоритма с Гауссовым соседством процент верных распознаваний, как правило, выше чем при использовании алгоритма с прямоугольным соседством.

Литература

1. Барский, А. Б. Нейронные сети: распознавание, управление, принятие решений [Текст] / А.Б. Барский // М.: Финансы и статистика, 2004. — 176 с.
2. Борисов, Е. Кластеризатор на основе нейронной сети Кохонена [Электронный ресурс] режим доступа: http://mechanoid.kiev.ua/neural-net-kohonen-clusterization.html, свободный.
3. Осовский, С. Нейронные сети для обработки информации [Текст] / Осовский С.: Пер. с польского И.Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с..
4. Солдатова, О.П. Основы нейроинфоматики [Текст] : учеб. пособие / О.П. Солдатова. – Самара: Изд-во Самар, гос. аэрокосм, ун-та, 2006. – 132 с. : ил.– ISBN 5-7883-0467-9.

С.С. Волков[I, II], И.И. Курочкин[III]

ПРИМЕНЕНИЕ ГЛУБОКИХ НЕЙРОННЫХ СЕТЕЙ, ОСНОВАННЫХ НА LSTM, ДЛЯ РЕШЕНИЯ ЗАДАЧ КЛАССИФИКАЦИИ[1]

(Российский университет дружбы народов[I], ФИЦ ИУ РАН[II], ИППИ РАН[III])

Введение

Машинное обучение – обширный подраздел научного направления искусственного интеллекта, отвечающий за изучение алгоритмов, способных обучаться на основе имеющихся данных. Наиболее часто методы машинного обучения применяются для решения задач классификации, кластеризации, прогнозирования и извлечения информации. Важной особенностью алгоритмов машинного обучения является то, что они способны хорошо работать с большими данными. В данной работе речь пойдет о задачах классификации. Этот класс задач относится к категории обучения с учителем. При обучении с учителем машина обучается на примерах. Оператор обеспечивает алгоритм машинного обучения набором известных данных, который содержит необходимые входные значения (признаки) и выходные. Задача заключается в установлении принципа

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №18-29-03264.

получения выходных данных из признаков. Алгоритмы машинного обучения выявляют закономерности в данных, обучаясь на примерах, и затем делают собственные прогнозы.

Для решения задач классификации существует большое количество алгоритмов машинного обучения (деревья решений, байесовский классификатор, метод ближайших соседей, нейронные сети и т. д.). Данная работа исследует применение нейронных сетей в задачах классификации в двух различных областях:

- анализ и классификация сетевого трафика - решается в рамках исследования систем обнаружения вторжений в программно-конфигурируемых сетях. Применение нейронных сетей для решения данной задачи обусловлено тем, что на обучение нейронной сети уходит много времени, но обученная сеть способна быстро анализировать входящие данные и производить классификацию. Данное свойство необходимо для анализа сетевого трафика в реальном времени;
- классификация дискурсивных отношений между фрагментами текстов - решается в рамках исследования возможности генерации текстов с помощью алгоритмов машинного обучения и дальнейшего выявления автоматически сгенерированных текстов.

В обеих задачах основное внимание уделяется глубоким нейронным сетям с обратными связями, основанным на LSTM [1]. Производится сравнение эффективности работы данных нейронных сетей с альтернативными (более простыми или сложными) вариантами.

LSTM в задачах анализа сетевого трафика

Программно-конфигурируемые сети - сети передачи данных, в которых уровень управления абстрагирован от нижележащего уровня передачи пакетов [2, 3]. Исследование направлено на решение вопроса безопасности программно-конфигурируемых сетей. Основным предметом исследования является система обнаружения вторжений, а именно - ее ядро, основанное на методах машинного обучения. Это ядро анализирует полученные данные, обнаруживает и классифицирует вредоносный трафик.

Для исследования было решено использовать набор данных CSE-CIC-IDS2018 [4], предоставленный Канадским институтом кибербезопасности (CIC) на AWS (Amazon Web Services). Авторы набора данных предлагают обработанную версию, созданную специально для работы с алгоритмами машинного обучения. Этот набор состоит из нескольких файлов CSV. Они содержат набор записей из 80 признаков, а также метки с указанием класса трафика. В процессе анализа признаков будут использованы 78 из 80. Были исключены метки классов (Labels), а также время старта потока.

На выбранном наборе данных были проведены эксперименты с использованием следующих нейронных сетей:

- Многослойный перцептрон;
- глубокая нейронная сеть с GRU [5] слоями;
- глубокая нейронная сеть с LSTM [6] слоями.

Результаты исследования показали, что даже многослойный перцептрон с умеренной точностью способен решать данную задачу. Однако в контексте обнаружения сетевых атак этой точности будет недостаточно. Глубокие нейронные сети отлично справились с поставленной задачей. Сеть с GRU слоями показала очень близкие результаты с сетью LSTM, но качество работы нейронной сети, использующей LSTM слои оказалось чуть выше.

LSTM в задачах классификации дискурсивных отношений

Дискурсивные отношения - подчиненные отношения, которые связывают между собой две части текста. С их помощью можно представить систематический способ анализа текста. Анализ обычно строится путем чтения текста и построения дерева с использованием отношений. В данном контексте части текста можно представить в двух видах: спутники и ядра. Ядра считаются наиболее важными частями текста, тогда как спутники вносят вклад в ядра и являются вторичными (или зависимыми). Данное разбиение необходимо для того, чтобы можно было определить направление дискурсивного отношения.

Для получения набора данных с дискурсивными отношениями необходимо произвести разметку текстов. Одним из недостатков методов машинного обучения, в том числе и реализующих нейронные сети, является требование большого количества примеров для обучения. Поскольку разметка текстов - очень трудоемкий процесс и производится вручную, наборы данных недостаточно велики для успешного обучения алгоритмов. Следовательно необходимо увеличить количество примеров, используемых при обучении. Для этого можно воспользоваться средствами автоматической дискурсивной разметки.

Для исследования было решено использовать набор размеченных новостных текстов RST Discourse Treebank LDC2002T07 [7]. Набор представляет собой записи пар текстов и тип отношения между ними. Всего в наборе определено 31 отношение с учетом направления (ядро-спутник или спутник-ядро). Данный набор разбит на тренировочную и тестовую выборку. Обе выборки содержат небольшое количество примером. Поэтому на тестовой выборке будет проверяться итоговое качество работы модели, а на тренировочной выборке будет производиться дообучение модели, заранее предобученной на автоматически размеченных данных. Для автоматической разметки данных использовался разметчик Two-stage Discourse Parser [8]. Разметка производилась на корпусе новостных текстов портала reddit. Основной этап обучения модели производился на полученных с помощью автоматического разметчика данных.

В данном эксперименте глубокие нейронные сети с GRU и LSTM слоями справились с задачей, но точность классификации оказалась недостаточно высокой. Проведено сравнение с результатами работы нейронной сети BERT [9], созданной специально для обработки естественного языка. По результатам сравнения можно сделать вывод о том, что дальнейшие эксперименты имеет смысл проводить с различными модификациями нейронной сети BERT, так как она имеет более высокую точность работы в рамках данной задачи.

Литература

1. Hochreiter S., Schmidhuber J. Long short-term memory //Neural computation. – 1997. – Т. 9. – №. 8. – С. 1735-1780.
2. Casado M. et al. SANE: A Protection Architecture for Enterprise Networks //USENIX Security Symposium. – 2006. – Т. 49. – С. 50.
3. McKeown N. et al. OpenFlow: enabling innovation in campus networks //ACM SIGCOMM computer communication review. – 2008. – Т. 38. – №. 2. – С. 69-74.
4. Datasets. Research. Canadian Institute of cybersecurity. https://www.unb.ca/cic/datasets/index.html (Accessed 25 March 2021).
5. Kurochkin I. I., Volkov S. S. Using GRU based deep neural network for intrusion detection in software-defined networks //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2020. – Т. 927. – №. 1. – С. 012035.
6. Volkov S. S., Kurochkin I. I. Network attacks classification using Long Short-term memory based neural networks in Software-Defined Networks //Procedia Computer Science. – 2020. – Т. 178. – С. 394-403.
7. Carlson L., Okurowski M. E., Marcu D. RST discourse treebank. – Linguistic Data Consortium, University of Pennsylvania, 2002.
8. Wang Y., Li S., Wang H. A two-stage parsing method for text-level discourse analysis //Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers). – 2017. – С. 184-188.
9. Devlin J. et al. Bert: Pre-training of deep bidirectional transformers for language understanding //arXiv preprint arXiv:1810.04805. – 2018.

Р.М. Ганеев, А.А. Столбова

ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ВЫЯВЛЕНИЯ ПОДДЕЛЬНЫХ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

(Самарский университет)

Использование поддельных аккаунтов является одним из наиболее распространенных способов для совершения злонамеренных действий в социальных сетях: рассылка спама, мошенничество или иное злоупотребление возможностями социальной сети. Своевременное обнаружение и принятие мер в отношении таких аккаунтов необходимы для защиты подлинных участников социальных сетей, а также для поддержания надежности самой сети. Тем не менее, любой поддельный аккаунт может иметь правдоподобный и заполненный профиль что делает его неотличимым от подлинных аккаунтов и существенно затрудняет обнаружение [1, 2].

В рамках данной работы предлагается разработать автоматизированную систему, позволяющую выявлять поддельные аккаунты в социальных сетях. В качестве исследуемой социальной сети выбрана сеть «ВКонтакте», поскольку данная сеть занимает лидирующую позицию в рейтинге социальных сетей по