Применение нейронных сетей для обнаружения аномального трафика в сетях Интернета вещей

Е.Е.Истратова

***Аннотация* — Актуальность решения задачи выбора моделей машинного обучения для обнаружения аномалий в сетевом трафике Интернета вещей связана с необходимостью анализировать большое число событий безопасности для выявления аномального поведения умных устройств. Цель исследования заключалась в разработке и исследовании программного обеспечения для обнаружения аномального трафика в сетях Интернета вещей на основе механизмов искусственных нейронных сетей. В статье приведены результаты разработки нейросетевой модели и программного обеспечения на ее основе для определения аномального трафика в сетях Интернета вещей на основе многослойного персептрона. Обученный на наборе данных UNSW-NB15, многослойный персептрон использует 47 входных признаков. При этом точность обнаружения аномального трафика составила 98.82 % при времени обучения модели в 13 мс. Также в рамках исследования было выполнено сравнение разработанной модели с программными аналогами. Различие в точности обнаружения аномалий разными моделями не превышает 1 %, в то время как время обучения модели значительно ниже у предложенной модели, что позволяет применять ее в режиме реального времени.**

***Ключевые слова* — Интернет вещей, нейронные сети, машинное обучение, аномальный трафик, обнаружение вторжений.**

I. Введение

Несмотря на то, что активный рост и развитие телекоммуникационных технологий, обусловленные увеличением числа подключаемых к сети Интернет устройств и повышением требований к пропускной способности компьютерных сетей, являются необходимыми условиями для расширения и повсеместного применения концепции Интернета вещей, данные факторы также приводят к возникновению ряда проблем в сфере информационной безопасности.

Одной из них считается наличие гетерогенного трафика в сетях, построенных в соответствии с концепцией Интернета вещей. В качестве примеров подобного трафика выступают следующие его виды: мультимедийный трафик передачи голоса и видео, который весьма чувствителен к задержкам; трафик мониторинга различных объектов; трафик передачи командно-сигнальной информации; трафик передачи сообщений и электронной почты и т.д. При этом должны выполняться заданные требования к качеству предоставляемых услуг и сервисов. Таким образом, сети Интернета вещей можно отнести к классу мультисервисных сетей со сложной логической и физической архитектурой, что приводит к возникновению объективных трудностей при проектировании подсистем управления сетью и в случае защиты сетевой и абонентской информации. В связи с этим, оперативное обнаружение состояния сети является одной из ключевых задач управления сетями Интернета вещей. Для решения данной задачи целесообразно своевременно обнаруживать и отслеживать аномальное поведение сетевого трафика.

В настоящее время существуют различные подходы к обнаружению аномального трафика в сети. Например, известны подходы, использующие историю изменения сетевого трафика, временные ряды из управляющей базы данных, непараметрические кумулятивные суммы, методы оценки максимальной энтропии. Существуют также решения, основанные на системах обнаружения вторжений, которые включают в себя активные подходы для предупреждения и устранения уязвимостей в системе. Однако перечисленные подходы не рассчитаны на ключевые особенности сетей Интернета вещей, к которым относятся сильно сегментированная топология и наличие нескольких точек сопряжения с другими сетями, из-за чего общий трафик системы затруднительно контролировать из одной точки. Таким образом, для Интернета вещей целесообразно применение централизованно-децентрализованной системы управления сетью, которая дает возможность не только повысить оперативность принятия решений по противодействию каким-либо деструктивным воздействиям на сеть, но и снизить объем служебного трафика. Помимо этого, для реагирования на угрозы безопасности необходимы инструменты анализа большого числа событий в системах Интернета вещей, которые содержатся в сетевом трафике, логах и иных данных, объем которых порой очень велик. Одним из подходов решения данной проблемы может быть применение машинного обучения для анализа проходящего трафика и обнаружения в нем аномалий [1]. Однако сравнивать между собой различные модели машинного обучения достаточно сложно. Это связано с тем, что в оценке эффективности применения моделей исследователи используют разные наборы данных или отличающиеся подмножества конкретного набора. В связи с этим, цель исследования заключалась в разработке модели на основе нейронных сетей для обнаружения аномалий в сетевом трафике Интернета вещей и ее апробации на одинаковых подмножествах

Истратова Евгения Евгеньевна. Новосибирский государственный технический университет, istratova@mail.ru

набора данных для обучения и тестирования.

II. Обзор существующих решений

Большая часть исследователей в области безопасности Интернета вещей рассматривает методы машинного обучения в рамках подходов к обнаружению атак и аномального поведения устройств. Основными преимуществами методов машинного обучения являются: высокая производительность и масштабируемость для растущего объема данных, а также возможность автоматически отбирать информативные признаки из необработанных данных.

В статье [2] осуществляется сравнение разработанной модели с классификаторами, основанными на следующих методах машинного обучения: методе опорных векторов, наивном байесовском классификаторе, случайном лесе, бустинге и методе k-ближайших соседей. Результаты анализа подтвердили, что наиболее точные данные были получены при использовании глубокого обучения.

В статье [3] предлагается распределенная облачная среда машинного обучения для обнаружения и предотвращения фишинговых и ботнетатак на умные устройства. Разработанная модель сравнивается с моделями, разработанными другими исследователями. Основным недостатком сравнительного анализа в данной работе является то, что рассматриваемые модели оцениваются не на одинаковых наборах данных.

В статье [4] описана роль методов искусственного интеллекта в процессе обеспечения кибербезопасности сетей Интернета вещей, приведены основные методы атак на устройства и модели машинного обучения, используемые для их защиты. В качестве таких моделей были рассмотрены следующие: деревья решений, модели к-ближайших соседей, модели опорных векторов, искусственные нейронные сети.

В статье [5] представлен обзор современных систем обнаружения вторжений, разработанных для модели Интернета вещей. Авторами представлен анализ уязвимостей архитектуры с акцентом на соответствующие методы, функции и механизмы и их связи со слоями архитектуры.

Авторы статьи [6] для обнаружения и удаления вредоносных пакетов из сети Интернета вещей предлагают применять функциональные кластеры с точки зрения потока, передачи телеметрии очереди сообщений и протокола управления передачей с использованием функций в наборе данных UNSW-NB15. Авторами были использованы такие алгоритмы контролируемого машинного обучения, как: случайный лес, модель опорных векторов и искусственные нейронные сети на кластерах. Исследование показало, что предлагаемые кластеры функций обеспечивают более высокую точность и требуют меньшего времени обучения по сравнению с другими современными подходами на основе контролируемого машинного обучения.

Таким образом, в результате анализа существующих подходов можно выделить ключевые особенности, необходимые для реализации модели машинного обучения. К таким особенностям относятся следующие: проведение эксперимента должно осуществляться на едином наборе данных; необходимость введения, помимо точности, еще и оценки временных затрат на обучение модели.

III. Разработка модели машинного обучения для обнаружения аномалий

Ключевыми элементами трафика в сетях Интернета вещей являются: тренд, сезонность и случайное значение. Под трендом понимается исследование общего поведения ряда при убывании или возрастании значений. Сезонность представляет собой исследование периодичности колебаний значений, связанных с различными временными характеристиками. Под случайным значением понимается результат, оставшийся после исключения из ряда других элементов. Именно здесь необходимо осуществлять поиск аномалий. Таким образом, для анализа сетевого трафика была предложена модель, основанная на изучении не только тренда и сезонности, но и случайных значений как основного источника аномалий трафика.

В качестве примеров аномалий сетевого трафика в сетях Интернета вещей могут выступать изменение распределения значений, выброс, отклонение от обычного, сдвиг и гибридные аномалии. Исходя из этого, при проектировании модели были предложены следующие операции по обработке сетевого трафика. В первую очередь, необходимо разложить трафик на компоненты, затем определить в нем тренд, сгладив исходные данные при помощи таких инструментов, как: скользящее окно, экспоненциальное сглаживание, регрессия. Далее из исходных данных необходимо вычесть тренд для определения сезонной составляющей, поскольку усредненный сезон определяется путем деления полученного результата на конкретный период. После удаления из исходного ряда тренда и сезонного фактора получается искомое случайное значение, необходимое для анализа аномальности трафика.

Предложенная модель машинного обучения для задач обнаружения сетевых аномалий Интернета вещей включает следующие этапы:

1. Предобработка данных.
2. Обучение модели.
3. Оценка эффективности обнаружения аномалий.

Предобработка данных, которая заключается в преобразовании входного набора данных, представленного признаками сетевых соединений и метками класса, в форму, подаваемую на вход анализируемым моделям. К признакам номинального типа в данном случае применяется метод представления категориальных переменных в виде двоичных векторов. Далее производится нормализация значений и приведение всех признаков к диапазону в пределах от 0 до 1. Нормализация данных осуществляется, так как дисбаланс между значениями признаков может вызвать неустойчивость работы модели, ухудшить результаты обучения и замедлить процесс моделирования. В качестве данных для обучения модели было выбрано

80% от исходного набора данных, что составило 1 547 081 запись, а для тестирования модели — 20%, то есть 386 771 запись. Важной особенностью данного этапа исследований является отсутствие высокой сбалансированности нормального и аномального класса сетевых соединений, что наиболее близко к реальным условиям при возникновении аномалий в сетевом трафике. Так, в данном случае отношение аномальных данных к нормальным составляет 1:4. Обучающая и тестовая выборка являются однородными.

Обучение модели, которое осуществляется на одинаковом тренировочном наборе данных, и обнаружение аномалий, проводимое на одинаковом тестовом наборе данных. Для обучения и валидации модели машинного обучения использовались следующие параметры: размер пакета 64, алгоритм оптимизации adam, функция потерь binary cross-entropy.

Разработанная модель машинного обучения для обнаружения аномалий в сетевом трафике Интернета вещей может работать в одном из следующих трех режимов:

1. Обнаружение с учителем, при этом доступен обучающий набор с трафиком, помеченным как нормальный или аномальный. Основным недостатком данного подхода является сложность формирования и последующей классификации полного набора обучения со всеми помеченными верно аномальными трафиками.
2. Частично-контролируемое обнаружение, при котором обучающий набор содержит только обычный трафик, а все, что не относится к данному виду трафика, считается аномальным. Несмотря на то, что в данном режиме алгоритм обнаружения не привязан к конкретным типам аномального трафика и может сам определять аномалии нового типа, но он обладает меньшей точностью на известной выборке по сравнению с первым режимом.
3. Обнаружение без учителя, при котором нет необходимости в маркированном обучающем наборе. Данный режим имеет минимальную точность обнаружения аномалий в сети Интернета вещей, но при этом не требует наличия обучающей выборки.

На основе предложенной модели машинного обучения было разработано программное обеспечение для обнаружения аномального трафика в сетях Интернета вещей. Архитектура разработанной системы включает следующие ключевые элементы:

1. Подсистема для сбора сетевого трафика применяется для записи данных о состоянии сети со всех сетевых устройств в базу данных.
2. База данных для хранения исходных событий, то есть информации, которую требуется проанализировать на наличие аномального трафика, и результатов интеллектуального анализа трафика.
3. Подсистема интеллектуального анализа сетевого трафика, необходимая для исследования каждой записи, хранящейся в базе данных исходных событий, на предмет обнаружения аномального трафика с помощью методов машинного обучения.
4. Подсистема визуализации результатов работы программы, представляющая собой систему оповещения о выявленных инцидентах для отображения обнаруженных аномалий в удобном для пользователя виде с возможностью формирования отчетов.

Разработанная модель машинного обучения была реализована на языке программирования Python с использованием фреймворка Tensorflow. Все эксперименты проводились на Acer Swift SF315-52G с процессором Intel Core i5 с тактовой частотой 1.8 ГГц, ОЗУ 8 ГБ и операционной системой Windows 10.

IV. Исследование разработанной модели машинного обучения

Оценка производительности любых систем обнаружения аномалий для технологии Интернета вещей требует наличия исходных данных, включающих в себя набор сетевых признаков, таких как: признаки на основе номеров портов источника и назначения, полезной нагрузки, поведения и потока данных.

В качестве экспериментальных данных для анализа моделей машинного обучения в задачах обнаружения сетевых аномалий Интернета вещей был выбран открытый набор данных UNSW-NB15, содержащий 2 540 044 записей — векторов признаков сетевых соединений TCP/IP и соответствующих им меток классов. В этом наборе данных сетевые пакеты включают как информацию о реальной нормальной активности сети, так и девять типов атак: фаззеры, анализаторы, бэкдоры, отказ в обслуживании, эксплоиты, обобщенные атаки, разведывательные атаки, шелл-код и черви. Данные набора UNSW-NB15 для обучения и тестирования систем обнаружения вторжений содержат 47 признаков, таких каксреди которых можно выделить IP-адреса, номера портов, байты транзакции и др., и две метки класса — категорию атаки и метку аномальности соединения. Первые 35 признаков представляют собой интегрированную информацию из пакетов данных, а остальные определяются отдельно для сценариев подключения.

Обнаружение аномалий представляет собой процесс идентификации отклонений от нормального профиля системы. Таким образом, для обнаружения аномалий в сетевом трафике при помощи набора UNSW-NB15 используется бинарная классификация, где в качестве метки класса выступает критерий аномальности соединения, при котором 0 соответствует нормальному профилю, а 1 — аномалии.

Разработанное программное обеспечение было протестировано на множестве записей из набора данных UNSW-NB15. Для определения эффективности работы предложенного программного обеспечения было проведено сравнение полученных результатов с результатами, полученными на аналогичных

нейросетевых моделях при помощи набора данных UNSW-NB15. В качестве критериев оценки были использованы точность и время обучения модели. Под точностью понималась доля верно классифицированных экземпляров сетевых соединений относительно всех экземпляров сетевого трафика.

В статье [7] авторами была предложена модель на основе многослойного персептрона с двумя скрытыми слоями, построенная в среде Matlab Neural Network Toolbox. Готовое решение позволяет обнаружить аномальный трафик с точностью до 91.16%.

В исследовании, представленном на BIWA Summit разработчиками компании Oracle, была описана модель на основе многослойного персептрона с одним скрытым слоем, показавшая точность 98.11% на наборе данных UNSW-NB15 [8].

В статье [9] были опубликованы результаты разработки и исследования интеллектуальной системы для обнаружения аномального сетевого трафика на основе набора данных UNSW-NB15. Полученная точность обнаружения составила 98.87%.

Авторами [10] была получена модель, отличительной особенностью которой является наличие 32 входных параметров, что меньше по сравнению с аналогами, при этом модель показала точность равную 98,99% на наборе данных UNSW-NB15.

Результаты сравнительного анализа разработанного программного обеспечения с программами-аналогами приведены в табл. 1.

Таблица 1. Результаты сравнения разработанного программного модуля с другими программными продуктами

Ссылка на модель	**Точность, %**	**Время обучения, мс**
[7]	91.16	46
[8]	98.11	12
[9]	98.87	22
[10]	98.99	21
Разработанная модель	98.82	13

Результаты проведенных экспериментов позволяют сделать вывод, что большинство моделей машинного обучения обладает высокой точностью обнаружения аномалий в гетерогенном трафике большого объема для применения их на практике. При сравнении между собой исследуемых моделей машинного обучения разных авторов можно установить, что различие в точности обнаружения аномалий не является весьма значительным — не более 1 %, за исключением модели [7].

Более разнящейся характеристикой является время обучения сети. Стоит отметить, что подготовка моделей машинного обучения с нескольким числом слоев занимает больше времени, что связано с тем, что применение данных моделей обучения требует большего количества вычислительных мощностей. Для систем, работающих в режиме реального времени и часто обновляемых, скорость моделирования является значимой характеристикой и должна быть минимизирована. В то время как для некоторых систем, обучаемых оффлайн, время моделирования может быть увеличено для более тщательной настройки и повышения эффективности функционирования.

V. Заключение

Таким образом, исходя из результатов сравнительного анализа можно сделать вывод о том, что применение разработанной модели является целесообразным. Она может быть использована для обнаружения аномального трафика в сетях Интернета вещей в режиме реального времени, показывая хорошую точность, а также отличную скорость обучения модели.

В результате работы была предложена нейросетевая модель для определения аномального трафика в сетях Интернета вещей, на основе которой было разработано программное обеспечение. Обученный на наборе данных UNSW-NB15 многослойный персептрон использует 47 входных признаков. При этом точность обнаружения аномального трафика составила 98.82% при времени обучения модели в 13 мс. В дальнейших исследованиях для увеличения точности обнаружения аномального трафика планируется ввести в подсистему интеллектуального анализа сетевого трафика возможность переобучения нейронной сети в процессе работы.

Библиография

[1] Браницкий А.А. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов / А.А. Браницкий, И.В. Котенко // Информационно-управляющие системы. – 2015. – № 4 (77). – С. 69-77.

[2] Moustafa N., Turnbull B., Choo K. R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 2019, vol. 6, no. 3, pp. 4815–4830. doi:10.1109/JIOT.2018.2871719.

[3] Al-Garadi M. A., Mohamed A., Al-Ali A., Du X., Guizani M. A Survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 2020, vol. 22, no. 3, pp. 1646–1685. doi:10.1109/COMST.2020.2988293.

[4] Гетьман А.И. Обзор методов классификации сетевого трафика с использованием машинного обучения / А.И. Гельтман, М.К. Иконникова // Труды ИСП РАН. – Т. 32. – № 6. – С. 137-154.

[5] Levshun D., Gaifulina D., Chechulin A., Kotenko I. Problematic issues of information security of cyber-physical systems. Informatics and Automation, 2020, vol. 19, no. 5, pp. 1050–1088. doi:10.15622/ia.2020.19.5.6.

[6] Roopak M., Tian G. Y., Chambers J. Deep learning models for cyber security in IoT networks. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, USA, 2019, pp. 0452–0457. doi:10.1109/CCWC.2019.8666588.

[7] Dipali Gangadhar Mogal, Sheshnarayan R. Ghungrad, Bapusaheb B. Bhusare. NIDS using Machine Learning Classifiers on UNSW-NB15 and KDDCUP99 Datasets. // International Journal of Advanced Research in Computer and Communication Engineering.Vol. 6, Issue 4, April 2017. pp. 533-537.

[8] Суворов А.О. Интеллектуальный анализ сетевого трафика для идентификации компьютерных вторжений / А.О. Суворов, В.А. Суворова // Защита информации и системы безопасности. – 2019. – № 1. – С. 62-73.

[9] Чаругин В.В. Анализ и формирование наборов данных сетевого трафика для обнаружения компьютерных атак / В.В. Чаругин, А.Н. Чесалин // International Journal of Open Information Technologies. – 2023. – Т. 11. – № 6. – С. 100-106.

[10] Гетьман А.И. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак / А.И. Гельман, М.Н. Горюнов, А.Г. Мацкевич // Труды ИСП РАН. – 2021. – Т. 33. – № 5. – С. 83-104.

Application of neural networks to detect abnormal traffic in the Internet of Things networks

E.E. Istratova

***Abstract* — The relevance of solving the problem of choosing machine learning models for detecting anomalies in the Internet of Things network traffic is related to the need to analyze a large number of security events to identify abnormal behavior of smart devices. The purpose of the study was to develop and research software for detecting abnormal traffic in the Internet of Things networks based on artificial neural network mechanisms. The article presents the results of the development of a neural network model and software based on it for determining abnormal traffic in the Internet of Things networks based on a multilayer perceptron. Trained on the UNSW-NB15 dataset, the multilayer perceptron uses 47 input features. At the same time, the accuracy of detecting abnormal traffic was 98.82% with a model training time of 13 ms. Also, as part of the study, a comparison of the developed model with software analogues was performed. The difference in the accuracy of anomaly detection by different models does not exceed 1%, while the model training time is significantly lower for the proposed model, which allows it to be applied in real time.**

***Keywords* — Internet of Things, neural networks, machine learning, abnormal traffic, intrusion detection.**

REFERENCES

[1] Branitskii A.A. Obnaruzhenie setevykh atak na osnove kompleksirovaniya neironnykh, immunnykh i neironechetkikh klassifikatorov / A.A. Branitskii, I.V. Kotenko // Informatsionno-upravlyayushchie sistemy. – 2015. – № 4 (77). – S. 69-77.

[2] Moustafa N., Turnbull B., Choo K. R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 2019, vol. 6, no. 3, pp. 4815–4830. doi:10.1109/JIOT.2018.2871719.

[3] Al-Garadi M. A., Mohamed A., Al-Ali A., Du X., Guizani M. A Survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 2020, vol. 22, no. 3, pp. 1646–1685. doi:10.1109/COMST.2020.2988293.

[4] Getman A.I. Obzor metodov klassifikatsii setevogo trafika s ispol'zovaniem mashinnogo obucheniya / A.I. Getman, M.K. Ikonnikova // Trudy ISP RAN. – T. 32. – № 6. – S. 137-154.

[5] Levshun D., Gaifulina D., Chechulin A., Kotenko I. Problematic issues of information security of cyber-physical systems. Informatics and Automation, 2020, vol. 19, no. 5, pp. 1050–1088. doi:10.15622/ia.2020.19.5.6.

[6] Roopak M., Tian G. Y., Chambers J. Deep learning models for cyber security in IoT networks. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, USA, 2019, pp. 0452–0457. doi:10.1109/CCWC.2019.8666588.

[7] Dipali Gangadhar Mogal, Sheshnarayan R. Ghungrad, Bapusaheb B. Bhusare. NIDS using Machine Learning Classifiers on UNSW-NB15 and KDDCUP99 Datasets. // International Journal of Advanced Research in Computer and Communication Engineering.Vol. 6, Issue 4, April 2017. pp. 533-537.

[8] Suvorov A.O. Intellektual'nyi analiz setevogo trafika dlya identifikatsii komp'yuternykh vtorzhenii / A.O. Suvorov, V.A. Suvorova // Zashchita informatsii i sistemy bezopasnosti. – 2019. – № 1. – S. 62-73.

[9] Charugin V.V. Analiz i formirovanie naborov dannykh setevogo trafika dlya obnaruzheniya komp'yuternykh atak / V.V. Charugin, A.N. Chesalin // International Journal of Open Information Technologies. – 2023. – T. 11. – № 6. – S. 100-106.

[10] Getman A.I. Metodika sbora obuchayushchego nabora dannykh dlya modeli obnaruzheniya komp'yuternykh atak / A.I. Getman, M.N. Goryunov, A.G. Matskevich // Trudy ISP RAN. – 2021. – T. 33. – № 5. – S. 83-104.