УДК 004.85

Хусаенов Фазыл Almазович, магистрант,
Казанский государственный энергетический университет,
г. Казань

Исмагилов Ильдар Рашидович, кандидат технических наук, доцент,
Казанский государственный энергетический университет,
г. Казань

АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕВОГО ТРАФИКА С ПОМОЩЬЮ ГЛУБОКОГО ОБУЧЕНИЯ

Аннотация: В данной статье исследуется применение глубокого обучения для анализа безопасности сетевого трафика. Сетевой трафик играет важную роль в современных информационных системах. В последние годы глубокое обучение стало мощным инструментом для анализа данных, включая анализ сетевого трафика. В этой статье рассмотрены различные методы и подходы к анализу безопасности сетевого трафика с использованием глубокого обучения и оценена их эффективность.

Abstract: This article explores the application of deep learning to analyze network traffic security. Network traffic plays an important role in modern information systems. This article discusses various methods and approaches to analyzing network traffic security using deep learning and evaluates their effectiveness.

Ключевые слова: сетевой трафик, глубокое обучение, искусственные нейронные сети, многослойный персептрон.

Keywords: network traffic, deep learning, artificial neural networks, multilayer perceptron.

Сетевой трафик является ключевым компонентом современных информационных систем, и его безопасность имеет критическое значение. Однако, с ростом сложности и объема данных, стандартные методы анализа и обнаружения угроз становятся недостаточно эффективными. В этой статье рассмотрено применение глубокого обучения для повышения эффективности анализа безопасности сетевого трафика.

Рассмотрим существующие методы анализа сетевого трафика с использованием машинного обучения. В работе [1] сделан следующий вывод о методах кибербезопасности: «Такие методы обучения, как деревья решений, SVM (машины опорных векторов) и KNN (k ближайших соседей), являются наиболее распространенными и изучаются для повышения их эффективности в решении проблем кибербезопасности. Однако методы глубокого обучения, такие как DBN (сети высокого доверия), RNN (рекурентные нейронные сети) и CNN (сверточные нейронные сети), более продвинуты, чем методы машинного обучения».

О. С. Амосов сделал следующие выводы насчёт рекурентных и свёрточных сетей: «Стоит отметить, что для рекуррентных сетей предпочтительней использовать алгоритм k-means. Точность классификации 88% в отличие от 81% при использовании BIRCH (сбалансированное итеративное сокращение и кластеризация с помощью иерархий). Для сверточных сетей BIRCH дает более высокий результат классификации – 97%. Увеличение количества сверточных слоев повышает точность классификации до 98%, но усложняет модель в части вычислений. Для распознавания аномалий сетевого трафика предлагается вычислительный метод с использованием глубоких нейронных сетей и методов кластеризации.» [2].

Один из методов анализа сетевого трафика CPN (сеть встречного направления). Кандидат технических наук Трещев И. А считает, что после обучения, данные нейронные сети «способны адаптироваться под новые типы угроз, распознавая их» [3]. CPN подходит для задач классификации.

Следующий метод – это рекурсивные нейронные сети (Recursive neural network, ReNN). Они способны работать с данными переменной длины и использовать иерархические структуры образцов при обучении [4]. Рекурсивные нейронные сети успешно применяются для обучения последовательных структур и деревьев, причем фразы и предложения моделируются через векторное представление слов [5].

Лаврова, Д. С. использует математический аппарат вейвлет-преобразований для обнаружения атак в сетевом трафике. Метод заключается в осуществлении дискретного вейвлет-преобразования над параметрами сетевых пакетов, извлеченными из трафика, и в отслеживании степени зависимости различных параметров сетевого пакета с использованием коэффициента множественной корреляции [6].

Борисенко Б. Б. предлагает использовать алгоритм LSTM (разновидность архитектуры RNN) и многослойный персептрон [7]. Данный метод используется при классификации сетевого трафика. Подобный метод применяет и Зуев В. Н. в своей работе [8]. В его работе рассматривается использование глубокого многослойного персептрона, обучаемого обычным методом и с помощью модифицированного алгоритма обучения. В похожем труде Татарникова Т. М., Бимбетов Ф. и Богданов П. Ю. использовали тот же многослойный персептрон для выявлений аномалий сетевого трафика [9].

Анализ источников показал, что целесообразно более подробно рассмотреть многослойный персептрон для задачи анализа безопасности сетевого трафика.

Многослойный персептрон – это нейронная сеть прямого распространения, состоящая из следующих элементов [7]

– входные данные, составляющие входной слой;

– скрытые слои;

– один выходной слой.

Многослойный персептрон, используемый в системах обнаружения вторжений, обучается с помощью искусственных нейронных сетей (ИНС) для классификации. Функция активации срабатывает, обеспечивая выход сети, который является суммой весов связей между скрытыми и выходным слоями. В данном случае, метод обучения с учителем применяется для обучения многослойного персептрона. У многослойного персептрона есть способность обучаться и выполнять нелинейные аппроксимации функций для классификации и регрессии, учитывая набор признаков X (x1, x2,...,xm). Каждый нейрон в скрытом слое преобразует значения из предыдущего слоя с помощью взвешенного линейного суммирования WiX), а затем применяет нелинейную функцию активации, наподобие гиперболического тангенса. Выходной слой получает значения из последнего скрытого слоя и преобразует их в выходные значения [7].

Недостатки многослойного персептрона:

– разные инициализации случайных весов могут привести к разной точности проверки в силу невыпуклости функции потерь при наличии более одного локального минимума;

– необходимость настройки ряда гиперпараметров (количество скрытых нейронов, слоев и итераций).

Анализ экспериментов. Зуев В. Н. при проверке разработанных моделей многослойного персептрона с 38 нейронами входного слоя, 12 нейронами скрытого первого слоя и 12 нейронами второго, 6 нейронами выходного слоя, на тестовой выборке посчитал среднюю точность классификации сетевых вторжений 91 % [8]. Использовался набор данных: NSL – KDD.

В работе Татарниковой Т. М. после обучения с таким же набором данных точность стала равным 92.5%. Использовался многослойный персептрон с десятью нейронами входного слоя, одним скрытым слоем с двенадцатью нейронами и шестью нейронами выходного слоя [9].

Из данных экспериментов можно сделать вывод, что многослойный персептрон достаточно точно классифицирует сетевые вторжения.

Для наглядности можно сравнить 2 искусственные нейронные сети: LSTM и многослойный персептрон.

LSTM – особая разновидность архитектуры рекуррентных нейронных сетей [7].

При проведении эксперимента с набором данных CSE-CICIDS2018 обнаружилось, что точность классификации многослойного персептрона составила 83,75%, а LSTM 83, 5% [7].

Многослойный персептрон лучше справился с идентификацией атак, что свидетельствует о его универсальности при решении задачи идентификации компьютерных атак [7].

Заключение. Рассмотрено применение глубокого обучения для анализа безопасности сетевого трафика. Сделаны выводы о различных архитектурах нейронных сетей, такие как сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), CPN, ReNN, математический аппарат вейвлет-преобразований, многослойный персептрон, которые могут быть использованы для обнаружения аномалий, классификации и обработки сетевого трафика. Метод с использованием многослойного персептрона определён как наиболее подходящий для анализа сетевого трафика. Выполнен анализ экспериментов, а также проведено сравнение архитектур нейронных сетей, где доказывается, что многослойный персептрон лучший метод для классификации и идентификации компьютерных атак.

Список литературы:

1. Аль-Ани М. М., Алшаиби А. Д., Костюченко Е. Ю. Эффективность глубокого обучения и методы машинного обучения в кибербезопасности //Проблемы правовой и технической защиты информации. – 2021. – №. 9. – С. 7-9.

2. Исследование архитектур глубоких нейронных сетей со сверточными и рекуррентными слоями для задач распознавания аномалий сетевого трафика в компьютерных системах / О. С. Амосов, С. Г. Амосова, Ю. С. Иванов, С. В. Жиганов // Управление развитием крупномасштабных систем (MLSD'2019): Материалы двенадцатой международной конференции, Москва, 01–03 октября 2019 года / Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. – Москва: Международный научно-исследовательский институт проблем управления РАН, 2019. – С. 995-1005.

3. Ложников К. А., Трещев И. А. Эвристический анализ сетевого трафика с использованием CPN нейронных сетей //Актуальные проблемы информационно-телекоммуникационных технологий и математического моделирования в современной науке и промышленности. – 2021. – С. 284-287.

4. Goodfellow I., Bengio Y., Courville A. Deep learning // MIT press. 2016. 800 p.

5. Гайфулина, Д. А. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 / Д. А. Гайфулина, И. В. Котенко // Вопросы кибербезопасности. – 2020. – № 3 (37). – С. 76-86.

6. Лаврова, Д. С. Анализ безопасности на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования / Д. С. Лаврова, И. В. Алексеев, А. А. Штыркина // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 2. – С. 9-15. – EDN XTKTED.

7. Борисенко Б. Б. и др. Обнаружение компьютерных атак при использовании многослойного персептрона и сетей с долгой краткосрочной памятью //Системы синхронизации, формирования и обработки сигналов. – 2021. – Т. 12. – №. 5. – С. 4.

8. Зуев В. Н. Обнаружение аномалий сетевого трафика методом глубокого обучения //Программные продукты и системы. – 2021. – Т. 34. – №. 1. – С. 91-97.

9. Татарникова Т. М., Бимбетов Ф., Богданов П. Ю. Выявление аномалий сетевого трафика методом глубокого обучения //Известия СПбГЭТУ ЛЭТИ. – 2021. – №. 4. – С. 36-41.

10. Гайфулина Д. А., Котенко И. В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 2 //Вопросы кибербезопасности. – 2020. – №. 4 (38). – С. 11-21.