Особенности применения методов искусственного интеллекта при решении задачи мониторинга сетевого трафика с целью обнаружения атак

Н.А. Семыкина[1], *Н.М. Садовникова*[2]

[1] *Тверской государственный университет*
[2] *ЦНИИ ВВС (Минобороны России), Москва*

Аннотация: При активном внедрении и использовании интернет-технологий во все сферы жизни человека, обеспечение сетевой безопасности является важной и актуальной задачей. В статье проанализированы перспективы использования искусственных нейронных сетей для анализа сетевого трафика с целью обнаружения компьютерных атак. Рассмотрены различные конфигурации сетей в качестве метода машинного обучения. Для обучения и тестирования был использован набор данных UNSW-NB 15, имеющий свободный доступ. Данный датасет, созданный Австралийским центром кибербезопасности, содержит параметры как нормального трафика, так и аномального трафика. Представлены результаты вычислительных экспериментов, по результатам которых сделаны выводы.
Ключевые слова: сетевой трафик, компьютерная атака, искусственная нейронная сеть, анализ трафика, конфигурация нейронной сети.

Введение

Обнаружение, классификация сетевых атак и предотвращение вторжений – приоритетны для сферы информационной безопасности. По данным российской компании Positive Technologies в 2022 году количество инцидентов по всему миру увеличилось на 20,8%. Если говорить о России, то количество атак возросло почти в два раза [1-2]. Это связано с тем, что современные сценарии атак характеризуются большой сложностью, многоэтапностью и автоматизированностью. Злоумышленники имеют высокий технический уровень подготовки и активно используют методы искусственного интеллекта. Общая динамика роста атак заставляет изменить принципы построения средств защиты и учитывать новейшие технологии анализа сетевого трафика на ранних стадиях разработки [2].

Анализ сетевого трафика с целью обнаружения угроз и аномалий сопряжен с обработкой большого количества данных в реальном времени.

Одно из направлений исследования этой проблемы – использование искусственных нейронных сетей (далее ИНС). При этом, сеть должна являться комбинацией нескольких типов ИНС и изначально быть обучена при штатном функционировании системы. Эти условия позволят снять часть сложностей в процессе применения технологий ИНС в распознавании атаки в сетевом трафике [3-4].

Российские IT-компании активно развивают решения, применяющие нейронные сети. Например, Positive Technologies разработала нечеткий нейроанализатор кода Application Inspector, основанный на использовании универсальных нечетких шкал лингвистических переменных и нейронной сети. При этом, обучение ИНС с двумя скрытыми слоями происходит на заданных эталонах [5]. Компания Kaspersky создала систему раннего обнаружения аномалий в режиме реального времени (Machine Learning for Anomaly Detection, далее MLAD) [6]. Для этого отслеживаются параметры технологического процесса и сравниваются с нормальным режимом, определяемого физическими законами. Так как все параметры явно или косвенно взаимосвязаны, то изменение показателей одного из них влечет за собой изменение других параметров. Нейронная сеть в составе Kaspersky MLAD обучается без учителя, выявляет взаимосвязи параметров и их влияние на последовательность событий, диагностирует аномальные отклонения в работе объекта. Настройка MLAD происходит для конкретного объекта со своим набором правил и исключений.

На сегодняшний день универсального решения задачи анализа сетевого трафика с помощью ИНС не существует.

Сравнение архитектур ИНС

Задача обнаружения атаки на сетевой трафик с помощью ИНС представляет собой задачу бинарной классификации, т. е. по набору параметров трафика определить, к какому множеству будет принадлежать

передающийся пакет информации: трафик с аномалией или нормальный трафик. В последнее время все больше ученых решают вопросы классификации в различных областях исследования с помощью ИНС, так как это позволяет автоматизировать процесс, а обученные нейронные сети на качественной выборке большой мощности дают возможность использовать их в режиме реального времени.

Для обучения ИНС требуется сформировать качественный набор данных, который поможет однозначно выделить признаки атак на сетевой трафик. В открытом доступе можно найти большое количество датасетов, которые описывают определенное множество атак. В работе будем использовать набор данных UNSW-NB 15 [7]. UNSW-NB 15 представляет собой набор параметров сетевого трафика, сгенерированный с помощью инструмента IXIA PerfectStorm в лаборатории Cyber Range Австралийского центра кибербезопасности (ACCS). Датасет состоит из нормального трафика и трафика, характеризующий один из девяти типов сетевых атак: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms. Количество записей в обучающей выборке составляет более 175 тысяч записей, набор для тестирования – более 82 тысяч записей [7].

Используем для программной реализации язык Python с библиотекой глубокого обучения Keras и библиотекой обработки данных Pandas. Для исследования рассмотрим различные типы ИНС:

1. Многослойный персептрон (MLP) [8] характеризуется 9 последовательно связанными слоями, 3 из которых скрытые слоя и 3 слоя исключения. На слое активации в качестве функции активации используем функцию ReLu, которая возвращает значение аргумента, если он положителен ($max\{0, x\}$). Функция потерь – бинарная перекрестная энтропия.

2. Рекуррентная нейронная сеть (Simple RNN) [8-9] состоит из 5 слоев, из них 2 скрытых слоя и 1 слой активации с функцией активации - сигмоида. Функция потерь – бинарная перекрестная энтропия.

3. Сеть долгой краткосрочной памяти (LSTM) является подвидом рекуррентной нейронной сети [9]. В исследовании рассмотрена сеть, содержащая 9 слоев, где 4 скрытых слоя, 3 слоя исключения. Слой активации использует функцию сигмоида. Функция потерь – бинарная перекрестная энтропия.

4. Управляющий рекуррентный блок (GRU) [9] – механизм нейронных сетей, объединяющий кратковременную и долговременную памяти в одно состояние, состоит из 7 слоев, из них 3 скрытых слоя и 2 слоя исключения. Выходной слой активации с функцией активации - сигмоида. Функция потерь – бинарная перекрестная энтропия.

5. Сверточная нейронная сеть (CNN) [10] состоит из 8 слоев, 2 из которых слои 1D свертки, 1 слой субдискретизации, 1 слой преобразования тензора, 1 срытый слой и 1 слой исключения. Выходной слой использует функцию активации ReLu. Функция потерь – бинарная перекрестная энтропия.

Для всех перечисленных конфигураций нейронных сетей проблему переобучения решаем с помощью метода исключений. В первых четырех конфигурациях сетей рассматривалось 10% отсеиваемых нейронов, а для сверточной сети – 35%. В таблице 1 приведены результаты численных экспериментов для перечисленных архитектур ИНС.

Как можно заметить лучшие результаты по точности обучения показала простая рекуррентная нейронная сеть (Simple RNN), однако по времени обучения лучшие результаты у сверточной нейронной сети (CNN). Были проведены дополнительные численные исследования. У

перечисленных ИНС производилось добавление скрытых слов. Это привело к увеличению времени обучения и слабо повлияло на точность.

Таблица № 1

Результаты обучения ИНС

№ п/п	Конфигурация ИНС	Точность, %	Время обучения, с
1	MLP Keras	87.21	429.3
2	Simple RNN Keras	93.52	532.9
3	GRU Keras	86.75	672.0
4	LSTM Keras	88.38	661.3
5	CNN Keras	91.11	412.5

Заключение

В работе были представлены результаты тестирования различных типов нейронных сетей для применения в задаче бинарной классификации сетевого трафика в условиях кибератак. По совокупности характеристик (точность и время обучения), наиболее удачной конфигурацией является сверточная нейронная сеть.

Изучение типов ИНС, их анализ и сравнение позволит в дальнейшем оптимизировать процесс нахождение параметров самой нейронной сети, что даст возможность уменьшить вычислительные ресурсы системы.

Литература

1. Актуальные киберугрозы: итоги 2022 года. // Positive Technologies URL: ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/. (дата обращения: 17.03.2023).

2. Кибербезопасность 2022 – 2023. Тренды и прогнозы. // Positive Technologies URL: ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/. (дата обращения: 17.03.2023)

3. Федоров В.Х., Васюков Д.Ю., Лаута О.С, Баленко Е.Г., Иванов Д.А. Подход к работе системы защиты сети передачи данных от компьютерных атак на основе гибридной нейронной сети // Инженерный вестник Дона,

2023, №1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8163 (дата обращения: 24.03.23).

4. Глушанский С.М., Буглов В.Е. Разработка гибридной нейросети для классификации изображений // Инженерный вестник Дона, 2023, №1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8150 (дата обращения: 22.03.23).

5. Как мы анализируем уязвимости с помощью нейронных сетей и нечеткой логики // Хабр URL: habr.com/ru/company/alexhost/blog/528796/ (дата обращения: 24.02.23).

6. Kaspersky Machine Learning for Anomaly Detection // Kaspersky Machine Learning for Anomaly Detection URL: mlad.kaspersky.ru/ (дата обращения: 24.02.23).

7. The UNSW-NB15 Dataset // UNSW Research URL: research.unsw.edu.au/projects/unsw-nb15-dataset (дата обращения: 10.02.2023).

8. Хайкин С. Нейронные сети: полный курс. - 2-е изд. - М, Издательский дом "Вильямс", 2006. 1104 с.

9. RNN, LSTM, GRU и другие рекуррентные нейронные сети. // Записная книжка. URL: vbystricky.ru/2021/05/rnn_lstm_gru_etc.html# recurrent-neuralnetwork (дата обращения 21.10.22).

10. Гафаров Ф.М., Галимянов А.Ф. Искусственные нейронные сети и приложения. Казань: Изд-во Казан. ун-та, 2018. 121с.

References

1. Aktual`nye kiberugrozy: itogi 2022 goda. Positive Technologies URL: ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022.

2. Kiberbezopasnost 2022 – 2023. Trendy i prognozy. Positive Technologies URL: ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/.

3. Fedorov V.X., Vasyukov D.Yu., Lauta O.S, Balenko E.G., Ivanov D.A. Inzhenernyj vestnik Dona, 2023, №1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8163.

4. Glushanskij S.M., Buglov V.E. Inzhenernyj vestnik Dona, 2023, №1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8150.

5. Kak my analiziruem uyazvimosti s pomoshhyu nejronnyx setej i nechetkoj logiki. [How we analyze vulnerabilities with neural networks and fuzzy logic]. Xabr. URL: habr.com/ru/company/alexhost/blog/528796.

6. Kaspersky Machine Learning for Anomaly Detection. Kaspersky Machine Learning for Anomaly Detection URL: mlad.kaspersky.ru.

7. The UNSW-NB15 Dataset. UNSW Research. URL: research.unsw.edu.au/projects/unsw-nb15-dataset.

8. Xaykin S. Nejronny`e seti: polny`j kurs. [Neural networks. A comprehensive foundation]. Moskva, Izdatel`skij dom "Williams", 2006. 1104 p.

9. RNN, LSTM, GRU i drugie rekurrentnye nejronnye seti. URL: vbystricky.ru/2021/05/rnn_lstm_gru_etc.html# recurrent-neuralnetwork.

10. Gafarov F.M., Galimyanov A.F. Iskusstvennye nejronnye seti i prilozheniya [Artificial neural networks and applications]. Kazan`: KFU, 2018. 121 p.