

ТЕХНИЧЕСКИЕ НАУКИ — МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ (05.13.18)

05.13.18

Н.А. Семыкина, И.А. Шаповалова

Тверской государственный университет,
математический факультет,
кафедра компьютерной безопасности и математических методов управления,
Тверь, Semykina.NA@tversu.ru, Shapovalova.IA@tversu.ru

НЕЙРОСЕТЕВОЙ ПОДХОД ПРИ МОДЕЛИРОВАНИИ ОБНАРУЖЕНИЯ DDOS-АТАК

В работе представлены результаты реализации механизма выявления кибератак в сетевом трафике. В основе метода лежит нейросетевой подход. Рассмотрена архитектура рекуррентной нейронной сети с долгой краткосрочной памятью, так как она лучше всего подходит для анализа информации с учетом предыдущих данных.

Ключевые слова: DDoS-атака, математическая модель, рекуррентная нейронная сеть.

С активным внедрением цифровых технологий в различные сферы жизни человека и общества защита и предупреждение сетевых атак стала одной из важнейших тем в области информационной безопасности. Одна из самых распространенных компьютерных атак — «распределенный отказ в обслуживании» (DDoS-атака). Вследствие действий злоумышленников происходит подавление нормальной работы сетевого ресурса трафиком из большого числа источников, и как следствие — нарушение доступности данных и сервисов [1].

В прошедшем 2021 году были зарегистрированы крупнейшие DDoS-атаки за всю историю Интернета. Сеть компьютеров с вредоносным программным обеспечением (ботнет) мощностью более 20 миллионов запросов в секунду атаковала сайты Яндекс и Хабр. Фирма Microsoft отбила атаку на 2,4 Тбит/с ботнета, состоящей из 70000 компьютеров [2]. И это только самые громкие инциденты усиления киберугроз. Основная тенденция DDoS-кампаний 2021 года — это совмещение самой атаки с вымогательством. Увеличение такой угрозы на 175% произошло в четвертом квартале прошедшего года. Причем, направление деятельности объекта шантажа не играет роли. Это могут быть школы, медицинские и финансовые учреждения, организации индустрии услуг, госсектор и предприятия промышленности и т.д. [3].

Последние исследования показали, что злоумышленники начинают активно использовать недостатки промежуточных устройств, таких как коммутаторы, концентраторы, модемы, маршрутизаторы, межсетевые экраны, балансировщики нагрузки, DPI и так далее. Правонарушители отправляют промежуточному устройству с чужих IP-адресов последовательность TCP-пакетов, которые имитируют попытки подключения к запрещенным цензурой сайтам. Устройство отвечает блокировкой, которая перенаправляется пользователям. Учеными было протестировано интернет-пространство. В результате обнаружено около 200 мил. IP-адресов, которые можно использовать для такой атаки [4].

Последнее время многие отечественные и зарубежные специалисты активно используют искусственные нейронные сети для обнаружения сетевых атак на ранней стадии. Это позволяет разрабатывать технологии, основанные на комплексном подходе и сочетать в себе решения на разных уровнях: от физического до прикладного.

Рассмотрим рекуррентную нейронную сеть LSTM (Long-Short Term Memory — долгая краткосрочная память). Особенность данной архитектуры нейросети состоит в том, что благодаря применению специального фильтра эффективность работы сети не зависит от разрыва между предыдущей информацией и ее использованием или неиспользованием [5].

В архитектуре данной нейронной сети для обработки информации используются четыре слоя. Вводятся дополнительные ячейки состояния, которые хранят в себе предыдущую информацию, и три специальных фильтра (гейта): забывающий, входной и выходной. Ниже приведем принцип работы LSTM-сети более подробно [6].

На первом рекуррентном нейронном слое происходит обработка информации с помощью забывающего фильтра. На вход в момент времени t поступает информация x_t , значение предыдущего скрытого слоя h_{t-1} , вектор состояния (ячейка памяти) C_{t-1} . Начальный этап работы заключается в определении процентного соотношения информации, которая будет отброшена по формуле

$$f_t = \sigma(W_f x_t + W_f h_{t-1} + b_f).$$

Здесь W_f – веса забывающего гейта, b_f – вектор свободных членов забывающего гейта, σ – сигмоидальная функция активации.

На следующем слое информация передается во входной фильтр, где выделяются необходимые параметры. Во-первых, значения x_t и h_{t-1} подаются в сигмоидальный слой входного гейта; во-вторых, значения x_t и h_{t-1} подаются в слой гиперболического тангенса с целью создания вектора кандидатов значений \tilde{C}_t для добавления в состояние памяти.

$$\begin{aligned} i_t &= \sigma(W_i x_t + W_i h_{t-1} + b_i), \\ \tilde{C}_t &= \tanh(W_C x_t + W_C h_{t-1} + b_C). \end{aligned}$$

В последних равенствах использованы обозначения: W_i – весовые коэффициенты входа, W_C – веса для последующего изменения состояния памяти, σ – сигмоидальная функция активации, b_i , b_C – векторы свободных членов входа и обновления памяти, соответственно.

На третьем слое происходит добавление информации в ячейку состояния, при этом используются параметры, выделенные входным фильтром. В результате применения покоординатного умножения векторов i_t и \tilde{C}_t , ранее вычисленной функции f_t и входной информации C_{t-1} становится возможным обновление состояния памяти C_t .

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t.$$

На последнем слое с помощью выходного фильтра определяются параметры информации, которая будет передана в выходной слой. Выходное значение модуля LSTM зависит от C_t . Сигмоидальный слой определяет, какая часть данных будет использована, затем C_t поступает в слой гиперболического тангенса, после чего полученные значения проходят через выходной гейт.

$$\begin{aligned} o_t &= \sigma(W_o x_t + W_o h_{t-1} + b_o), \\ h_t &= o_t * \tanh(C_t). \end{aligned}$$

Здесь W_o – весовые коэффициенты выхода из модуля, b_o – вектор свободных членов выхода, σ – сигмоидальная функция.

Для экспериментального исследования и выявления DDos-атак в сетевом трафике с помощью нейросетевого подхода выбран набор данных KDD 1999 [7]. Он создан на основе имитации работы американской сети военно-воздушных сил. Обучающая и тестирующая выборки были составлены из записей, описывающих 7 недель работы этой сети (около 5 миллионов записей о соединениях). Была воссоздана имитация атак на сеть.

Для реализации LSTM-сети применен язык JavaScript с использованием библиотеки Brain.js. Вычислительный эксперимент состоял из этапов: создание и обучение рекуррентной нейронной сети; реализация тестового эксперимента.

При построении рекуррентной нейронной сети использованы следующие параметры: входной слой содержит 17 нейронов, выходной слой содержит 3 нейрона, скрытый слой состоит из двух уровней, каждый из которых состоит из 40 нейронов. В эксперименте использовался механизм обучения с учителем.

Обучающая выборка включала в себя 3400 строк. Около 60% их них составляли данные о нормальном трафике, примерно 40% отводилось на компьютерные атаки. Для подбора и корректировки параметров искусственной нейронной сети использовался набор данных из 2340 строк.

Рассматривались ошибки обучения: определение нормального трафика как атаки (ошибки I рода), определение атаки как нормального трафика (ошибки II рода). Ниже, в таблице представлены результаты по обучающим выборкам на основе разного количества итераций.

Таблица – Результаты обучения

Кол-во эпох обучения	Кол-во ошибок I рода (%)	Кол-во ошибок II рода (%)
8	31,58	2,13
9	5,16	0,08
10	6,66	0,81
11	13,23	1,49
12	9,69	3,45

Как можно заметить, при 9 эпохах обучения достигается наилучший процент точности и наименьший процент ошибок второго рода.

Для построенной модели реализовано тестирование на выборке, состоящей из 5100 строк. Эксперимент показал, что точность определения DDoS-атак соответствует 99,54%. Процент событий, когда атака определялась как нормальный трафик, составил 0,31%.

Полученный механизм выявления атак в сетевом трафике на основе нейронных сетей показал довольно хорошие перспективы. Внедрение и совместное использование заданного механизма в совокупности со сторонними средствами анализа сетевого трафика могут повысить безопасность сети.

Список литературы

1. Порядок действий при обнаружении сетевых атак. [Электронный ресурс]. – Режим доступа: <https://comprnote.ru/otdelit/poryadok-deystviy-pri-obnaruzhenii-setevyih-atak/> (дата обращения: 25.01.2022).
2. Нефёдова М. Самые громкие и интересные события мира безопасности за 2021 год. [Электронный ресурс]. – Режим доступа: <https://xakep.ru/2021/12/31/meganews-2021/> (дата обращения: 10.02.2022).
3. Тенденции DDoS-атак в 4-м квартале 2021 года. [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/company/skillfactory/blog/646347/>(дата обращения: 10.02.2022).
4. Нефёдова М. Ученые считают, что промежуточные устройства можно использовать для масштабных DDOS-атак. [Электронный ресурс]. – Режим доступа: <https://xakep.ru/2021/08/17/tcp-ddos/> (дата обращения: 10.02.2022).
5. Рекуррентные нейронные сети: типы, обучение, примеры и применение [Электронный ресурс] // Neurohive: базовый курс. 2018. – Режим доступа: <https://neurohive.io/ru/osnovy-data-science/rekurrentnye-nejronnye-seti/> (дата обращения: 19.02.2022).
6. Horeiter S., Schmidhuber J. Long Short-Term Memory // Neural Computation. – 1997. – P. 1735-1780.
7. KDD Cup1999 Data [Электронный ресурс]. – Режим доступа: <https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html> (дата обращения: 10.02.2020).