Ляшков М.А., Арзамасцев А.А. Разработка методов обнаружения атак на веб-приложения с помощью рекуррентных сетей. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 76-80.

УДК 004.896

РАЗРАБОТКА МЕТОДОВ ОБНАРУЖЕНИЯ АТАК НА ВЕБ-ПРИЛОЖЕНИЯ С ПОМОЩЬЮ РЕККУРЕНТНЫХ СЕТЕЙ

М.А. Ляшков, А.А. Арзамасцев

DEVELOPMENT OF THE METHODS OF ATTACKS DETECTION FOR WEB APPLICATIONS BY MEANS OF RECURRENT NETWORKS

M.A. Lyashkov, A.A. Arzamastsev

Аннотация

Предмет. В работе исследуется применимость разновидности рекуррентных нейронных сетей для обнаружения аномалий в HTTP-трафике. Объектом оценки является единичный HTTP-запрос.

Цели. Создание модели глубокого обучения, которая не требует априорных знаний для извлечения значимых признаков из HTTP-запроса и будет давать интерпретируемые результаты.

Методология. Предлагается рассматривать текстовый запрос HTTP как последовательность. Используется seq2seq архитектура для тренировки кодера-энкодера на нормальных HTTP-запросах. Степень восприимчивости к ошибкам регулируется с помощью порогового значения. Экспериментальную проверку применимости метода осуществляли на HTTP Dataset CSIC, содержащем 36 тысяч нормальных и 25 тысяч аномальных HTTP-запросов.

Результаты. После тренировки на 33 тысячах запросах, модель была протестирована на 3 тысячах типичных и 25 тысячах аномальных запросов. Тестирование осуществляли на запросах, которые ранее не использовали при тренировке. Пороговое значение подбирали из анализа ROC-кривой. Модель показала точность 0.9764 и полноту 1.000, площадь под ROC-кривой 0.9999.

Выводы. Несмотря на вычислительную сложность тренировки модели, получение типичного трафика для конкретного веб-приложения с серверной стороны является тривиальной задачей. Модель дает интерпретируемые результаты.

Ключевые слова: рекуррентные нейронные сети, обнаружение аномалий, долгая краткосрочная память, HTTP-трафик

Abstract.

Object. The ability to lease computing resources on demand opens up new opportunities for testing deep learning models for small and medium enterprises. Models of deep learning do not require manual selection of significant features, which allows saving on expensive specialized expertise.

Goals. This paper investigates the applicability of recurrent neural networks for detecting anomalies in HTTP traffic. The object of evaluation is a single HTTP request.

Methods. It is proposed to look at the HTTP text request as a sequence of symbols. The seq2seq architecture is used to train the encoder-encoder on normal HTTP requests. When an abnormal input request is received, the encoder-encoder frame gives an output with a greater error than during normal traffic. The degree of error susceptibility is regulatedby a threshold value. Experimental verification of the applicability of the method was carried out on HTTP Dataset CSIC, containing 36 thousand normal and 25 thousand abnormal HTTP requests.

Results. The model was tested on 3 thousand typical and 25 thousand abnormal requests after training on 33 thousand requests. Testing was carried out on requests that were not previously used during training. The threshold value was selected from the analysis of the ROC curve. The model showed an accuracy of 0.9764 and a completeness of 1.000, the ROC AUC is 0.9999.

Conclusions and Relevance. Despite the computational complexity of training the model, obtaining typical traffic for a particular web application from the server side is a trivial task. The model gives interpretable results.

Keywords: recurrent neural networks, anomaly detection, long short-term memory, HTTP traffic

Возможность аренды вычислительных ресурсов по требованию открывает новые перспективы апробации моделей глубокого обучения для малых и средних предприятий. Модели глубокого обучения не требуют ручного выделения значимых признаков, что позволяет экономить на дорогой профильной экспертизе. Данная работа сфокусирована на проблеме определения аномалий в HTTP-трафике с точки зрения сервера. Объектом предсказания является единичный HTTP-запрос. Аномалии, которые образуются с помощью нескольких запросов, находятся за рамками рассмотрения этого исследования. Аномалии – вещь субъективная, один и тот же запрос может являться нормой для одного приложения и аномалией для другого. Для формирования обучающей выборки необходимо выделить нормальные запросы. Для выделения нормальных запросов можно использовать 2 метода. Во-первых, можно предположить, что мы имеем дело с обычным веб-приложением и большинство веб-запросов к нему являются нормальными, тогда выбираем самые частые запросы, которые были зарегистрированы за определенный временной промежуток. Временной промежуток следует выбирать в зависимости от интенсивности запросов к приложению. Во-вторых, можно использовать для разметки стороннюю систему защитного экрана уровня приложений, которая может работать, например, с помощью сигнатур. При таком подходе предполагается, что запрос считается нормальным, если на нем не было срабатывания сторонней системы защитного экрана уровня приложений. На практике лучше комбинировать эти подходы: выбирать самые частые HTTP-запросы, на которых не было срабатываний сторонней системы защитного экрана уровня приложений. Единичный HTTP-запрос рассматривается как последовательность символов. Рекуррентные сети выбраны потому, что если рассматривать запрос как последовательность символов, а также есть необходимость учитывать контекст (под контекстом здесь понимаются соседние символы, не обязательно ближайшие), то необходимо использовать нейронные сети с памятью. Стандартные рекуррентные сети имеют проблемы с долгосрочной памятью: чем больше циклов прошло с момента получения той или иной информации, тем больше вероятность, что значимость этих данных не будет играть большой роли на новом цикле работы. Эти проблемы были решены в сетях долгой краткосрочной памяти за счет усложнения структуры нейрона. В работе проводилось обучение каскада кодера-декодера с архитектурой seq2seq [1, 2]. На вход и выход модели подавали нормальные HTTP-запросы, таким образом, модель училась их реконструировать. В условиях отсутствия тестовой выборки предлагается использовать математическое ожидание ошибки на обучающей выборке и среднеквадратичное отклонение для определения порога срабатывания. Для экспериментальной проверки был использован HTTP Dataset CSIC [3]. Тренировка модели проводилась на 33 тысячах случайно выбранных нормальных HTTP-запросов, модель была протестирована на 3 тысячах типичных и 25 тысячах аномальных запросов. Тестирование осуществляли на запросах, которые ранее не использовали при тренировке. Пороговое значение подбирали из анализа ROC-кривой. Модель

показала точность 0.9764 и полноту 1.000, площадь под ROC-кривой 0.9999. Обучение модели заняло 18 часов на 8 ГБ видеопамяти на видеокарте GTX1080. Несмотря на вычислительную сложность тренировки модели, предсказание является вычислительно простой процедурой. Получение типичного трафика для конкретного веб-приложения с серверной стороны является тривиальной задачей. Модель дает интерпретируемые результаты. Матрица ошибок модели представлена в таблице, где $\tilde{y}$ – предсказанная метка класса, а y – настоящая метка класса, 0 – нормальный запрос, а 1 – аномальный.

Матрица ошибок для seq2seq-модели

	y=0	y=1
$\tilde{y}$=0	3003	597
$\tilde{y}$=1	0	24668

Благодарности

Авторы выражают признательность Арсению Реутову, Ирине Степанюк и Федору Сахарову за их выступление на AI Village 2018.

Библиографический список

1. Ilya Sutskever, Oriol Vinyals, Quoc V. Le Sequence to Sequence Learning With Neural Networks, 2014, 9 p.

2. Tong Wang, Ping Chen, Kevin Amaral, Jipeng Qiang An Experimental Study of LSTM Encoder-Decoder Model for Text Simplification, 2016, 8 p.

3. HTTP DATASET CSIC 2010. URL: http://www.isi.csic.es/dataset/

Ляшков Михаил Андреевич
Тамбовский государственный
университет им. Г.Р. Державина,
г. Тамбов, Россия

Lyashkov M.A.
Tambov State University
named after G.R. Derzhavin,
Tambov, Russia

Арзамасцев Александр Анатольевич
Тамбовский государственный
университет им. Г.Р. Державина,
г. Тамбов, Россия

Arzamastsev A.A.
Tambov State University
named after G.R. Derzhavin,
Tambov, Russia