СЕКЦИЯ 13: МЕТОДОЛОГИЯ, МЕТОДЫ И ПРОГРАММНО-АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАБОТКИ И ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА БОЛЬШИХ МАССИВОВ ИНФОРМАЦИИ

ИСПОЛЬЗОВАНИЕ ГЛУБОКИХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РАСПОЗНАВАНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ПРЕДПРИЯТИЙ

Амосов О.С., Амосова С.Г.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная, д.65
osa18@yandex.ru, amosovasg@yandex.ru,

Иванов Ю.С., Жиганов С.В.

Комсомольский-на-Амуре государственный университет,
Россия, г. Комсомольск-на-Амуре, ул. Ленина, д.27
ivanov_ys@icloud.com, zhiganov@knastu.ru

Аннотация: Предлагается распознавание аномалий сетевого трафика с использованием различных архитектур глубоких нейронных сетей. Проведен эксперимент по обнаружению DoS атак. Выявлены влияния комбинаций слоев нейронных сетей на характеристики точности. Новым является усиление классификации путем подкрепления входного вектора его кластерной оценкой.

Ключевые слова: аномалия сетевого трафика, сетевая атака, классификация, глубокая нейронная сеть, DoS.

Введение

Распознавание аномального трафика, вызванного сетевой атакой, является одной из актуальных проблем защиты информации в корпоративных сетях. Наиболее распространенной атакой является DoS-атака (англ. Denial of Service), приводящая к отказу в обслуживании. Для решения данной задачи предлагалось использовать решающие деревья [1], фрактальный и вейвлет-анализ [2, 3], генетические алгоритмы [4], нечеткую логику [5], машинное обучение [6] и глубокие нейронные сети (ГНС) [7, 8].

В настоящее время в связи с большим интересом к ГНС представляет интерес разработка эффективного по точности и быстродействию метода интеллектуального анализа аномалий сетевого трафика в режиме реального времени на основе глубоких НС. Этому и посвящена статья.

1 Постановка задачи

Пусть имеются: множество образов сетевого трафика $\omega \in \Omega$, заданных признаками x_i, $i=\overline{1,n}$, совокупность которых для образа ω представлена векторными описаниями $\mathbf{\Phi}(\omega)=(x_1(\omega),x_2(\omega),...,x_n(\omega))=\mathbf{x}$; множество классов $\mathrm{B}=\{\beta_1,...,\beta_k,...,\beta_c,\}$, c – количество классов. Априорная информация представлена обучающим множеством (датасетом) $\mathrm{D}=\left\{\left(\mathbf{x}^j,\beta^j\right)\right\}, j=\overline{1,L}$.

Заметим, что обучающее множество характеризует неизвестное отображение $^*\mathbf{F}:\Omega\to\mathrm{B}$.

Требуется по имеющимся пакетам $\mathbf{P}_t$ непрерывного сетевого трафика $\mathbf{N}=(\mathbf{P}_1,..,\mathbf{P}_t,..,\mathbf{P}_\tau)$ и априорной информации, решить задачу распознавания образов: обнаружить образы ω в виде оценки признаков $\tilde{\mathbf{x}}$ с помощью отображения [9] $\mathbf{F}_1:\mathbf{P}_t\to\tilde{\mathbf{x}}$ и классифицировать их с использованием отображения $\mathbf{F}_2:\tilde{\mathbf{x}}\to\beta_k$, $k=\overline{1,c}$ в соответствии с заданным критерием $\mathrm{P}(\tilde{\mathbf{x}})$, минимизирующим вероятность ошибки. Таким образом, необходимо найти отображение $\mathbf{F}:\mathbf{P}_t\to\beta_k$, $k=\overline{1,c}$, при котором $\mathbf{F}$ – является набором функций и алгоритмов $\mathbf{f}_i$, $i=\overline{1,N_f}$.

Отображение $\mathbf{F}:\mathbf{P}_t\to\beta_k$ реализуется на основе предлагаемого вычислительного метода, содержащего следующие этапы: 1) предобработка данных; 2) уточнение области интереса; 3) выделение информативных признаков и классификация.

2 Решение задачи распознавания аномалий сетевого трафика

2.1 Предобработка данных

Нормализация признаков. Для обучения и тестирования использовался датасет CICIDS2017 [6]. Для увеличения количества примеров под DoS атакой будем понимать все виды DoS атак датасета.

Значения параметров в векторе для обучения имеют очень большой разброс (распределение) и масштаб. Необходимо выполнить нормализацию при помощи метода Z-score.

Кластеризация обучающей выборки. Для снижения размерности необходимо провести кластеризацию обучающей выборки, в которой присутствовало 97 686 примеров DoS атак и 128 025 нормальных пакетов. В качестве алгоритма кластеризации предлагается использовать двуэтапный алгоритм BIRCH [10] (англ. Balanced Iterative Reducing and Clustering using Hierarchies).

В результате кластеризации выборка была разбита на 2000 кластеров, а каждый нормированный вектор пакета $\mathbf{z}$ был представлен его кластерной оценкой $\tilde{\mathbf{z}}$ – номером кластера $v = \overline{1,2000}$.

На рисунке 3 представлена визуализация сетевой атаки типа DoS (а) и нормального трафика (б) в виде временного ряда, где по оси Ox –сетевые пакеты, а по оси Oy – номера кластеров.

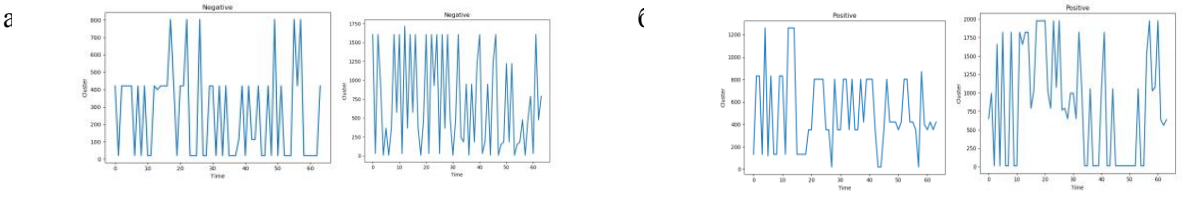

Рис. 3. Визуализация трафика

2.2 Уточнение области интереса

Необходимо выполнить анализ последовательности сетевых пакетов и обобщить полученную информацию за определенный временной интервал. Тогда сканирующим окном является последовательность исходных пакетов:

$$\mathbf{W}_t = concat(\mathbf{P}_t, \ldots \mathbf{P}_{t+n}) \cong concat(\mathbf{z}_t, \ldots \mathbf{z}_{t+n}) \cong [\tilde{\mathbf{z}}_t, \ldots \tilde{\mathbf{z}}_{t+n}], \quad (1)$$

где $n = 64$ – количество пакетов, concat – операция конкатенации нескольких подряд идущих кадров в многомерный массив, $\tilde{\mathbf{z}}_t$ – номер кластера нормированного пакета $\mathbf{z}_t$, а смещение окна равно 10. Также можно сканировать трафик по последовательности нормированных пакетов или последовательности номеров кластеров.

2.3 Выделение информативных признаков и классификация

В качестве классификатора DoS атаки нами разработаны и протестированы 8 различных архитектур ГНС, построенных комбинацией слоев одномерной свертки, полносвязных слоев (англ. Dense) и рекуррентных слоев LSTM. Обучение ГНС производится с использованием обучающего множества, состоящего из 691 406 пакетов, разбитых на 69 141 окон.

2.4 Пример обнаружения аномального сетевого трафика

Был проведен эксперимент на оборудовании со следующими параметрами: ЦПУ Intel Core i7-5820K, графический процессор (ГПУ) 1080 Ti. Размер тестирующей выборки – 225711 последовательных пакетов, разбитых на 22565 сканирующих окон. Были получены результаты (таблица 1) для метрик Precision, Recall F1-score по классам и для Accuracy, AUC – в общем.

Таблица 1. Результат классификации

Показатель 0/1 или общий / Нейронная сеть	**Precision**	**Recall**	**F1-score**	**Acc.**	**AUC**
2 рекуррентных слоя LSTM	1,00/0,89	0,83/1,00	0,90/0,94	0,92	0,91
6 слоев свертки	0,99/0,99	0,99/0,99	0,99/0,99	0,99	0,99
K-means и 2 рекуррентных слоя LSTM	0,95/0,87	0,80/0,97	0,87/0,91	0,90	0,88
BIRCH и 2 рекуррентных слоя LSTM	0,76/0,85	0,81/0,81	0,79/0,73	0,81	0,81
K-means и 6 слоев свертки	0,99/0,96	0,95/0,99	0,97/0,98	0,97	0,97
BIRCH и 6 слоев свертки	0,98/0,97	0,96/0,99	0,97/0,98	0,97	0,97
BIRCH и 9 слоев свертки	0,99/0,98	0,98/0,99	0,98/0,99	0,99	0,98

Показатель 0/1 или общий / Нейронная сеть	**Precision**	**Recall**	**F1-score**	**Acc.**	**AUC**
2 рекуррентных слоя LSTM	1,00/0,89	0,83/1,00	0,90/0,94	0,92	0,91
6 слоев свертки	0,99/0,99	0,99/0,99	0,99/0,99	0,99	0,99
Дуальная архитектура с 6 слоями свертки	0,99/0,99	0,99/1,00	0,99/0,99	0,99	0,99

Дуальная архитектура сети позволяет повысить точность классификации до 99% путем подкрепления входного вектора меткой его кластера. Применение кластеризации в качестве предобработки для глубоких архитектур нейросетей, работающих на ГПУ, позволяет значительно повысить скорость обработки и делает возможным обнаружение DoS атак в высоконагруженных корпоративных сетях. Скорость обработки 32 768 окон, соответствующих 512 с трафика, составляет от 1,8 с до 2 с, что достаточно для работы в реальном времени.

Заключение

Дана постановка задачи распознавания аномалий сетевого трафика.

Для распознавания аномалий сетевого трафика предлагается вычислительный метод с использованием глубоких нейронных сетей и методов кластеризации. Экспериментально показано, что применение кластеризации совместно со сверточными слоями позволяет достигнуть хороших результатов в режиме реального времени при решении задач информационной безопасности. За счет применения операции свертки существенно снижается количество настраиваемых параметров по сравнению с традиционными НС, а чередование сверточных слоев позволяет выстроить иерархию признаков и с достаточно высокой скоростью и точностью распознавать начало атаки. С использованием дуальной сети была получена точность классификации 99,26%.

Реализован подход для обнаружения сетевой атаки типа DoS. В отличие от предлагаемых ранее подходов в работе применяется сканирующее окно, размерность которого снижена путем кластеризации данных. Перспективным направлением исследования является реализация многоклассовой классификации, алгоритма реакции и предотвращения последствий атаки с использованием алгоритмов нечеткой логики.

Благодарности

Работа выполнена при поддержке Минобрнауки России научного проекта – госзадания в рамках проектной части № 2.1898.2017/ПЧ "Создание математического и алгоритмического обеспечения интеллектуальной информационно-телекоммуникационной системы безопасности вуза".

Литература

1. Riyazahmed A.J. Network Intrusion Detection System Using Machine Learning // Indian Journal of Science and Technology Vol. 11. 2018, №48. – P. 1-6 .

2. Амосов О.С., Магола Д.С., Баена С.Г. Сетевая классификация атак в задачах информационной безопасности на основе интеллектуальных технологий, фрактального и вейвлет-анализа // Ученые записки КнАГТУ. 2017. № IV-1 (32). – С. 19-29.

3. Пащенко Ф.Ф., Амосов О.С., Муллер Н.В. Структурно-параметрическая идентификация временного ряда с применением фрактального и вейвлет-анализа // Информатика и системы управления. 2015. №2(44).– С.80-88.

4. Resende P.A.A., Drummond A.C. Adaptive anomaly based intrusion detection system using genetic algorithm and profiling // Security Privacy Vol. 1. 2018, №4. – P. 1-13.

5. Haripriya A.P., Kulothungan K. Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things // EURASIP Journal on Wireless Communications and Networking Vol. 2019. 2019, №1. -P 90-105.

6. Sharafaldin I., Habibi Lashkari A., Ghorbani A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // In Proceedings of the 4th International Conference on Information Systems Security and Privacy Vol. 1. -P 108-116.

7. Chockwanich N., Visoottiviseth V. Intrusion Detection by Deep Learning with TensorFlow // 21st International Conference on Advanced Communication Technology (ICACT). 2019. – P. 654-659.

8. *Амосов О.С., Магола Д.С., Пащенко Ф.Ф., Амосова С.Г.* Классификация сетевых атак на основе глубоких нейронных сетей с 1D-сверточными и рекуррентными слоями // XIII Всероссийское совещание по проблемам управления, ВСПУ-2019, Москва, 17-20 июня 2019 г. – С. 1-5.

9. Амосов О.С. Фильтрация Марковских последовательностей на основе байесовского, нейросетевого подходов и систем нечеткой логики при обработке навигационной информации // Известия Российской академии наук. Теория и системы управления. 2004, № 4. – С. 61-69.

10. Zhang T., Ramakrishnan R., Livny M. BIRCH: An Efficient Data Clustering Method for Very Large Databases // Proceedings of the 1996 ACM SIGMOD International Conference on Management of Data. 2019. -P 103-114

11. *Friedman J.H.* Stochastic gradient boosting // Computational Statistics and Data Analysis Computational Statistics & Data Analysis Vol. 38, Issue 4, 2002, P. 367-378