МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра системного программирования

Разработка модели раннего обнаружения DDoS-атак на основе анализа сетевого трафика

Рецензент:
доцент кафедры ИИТиМОИ
ФБОУ ВО «ЮУрГГПУ», к.п.н.
О.А. Дмитриева

Автор работы:
студент группы КЭ-229
К.Е. Бакунина

Руководитель:
доцент кафедры СП, к.п.н.
О.Н. Иванова

Челябинск, 2024 г.

Актуальность

Актуальность выпускной квалификационной работы обусловлена активным ростом количества совершенных кибератак за последние годы.

Одной из самых распространенных кибератак является распределенная атака типа «отказ в обслуживании».

Некоторые из основных статистических данных о DDoS-атаках за 2022–2023 годы:

- согласно ежеквартальному отчету компании «Лаборатория Касперского», было зарегистрировано около 57 000 DDoS-атак;
- согласно данным компании «Cloudflare», в 2022 году количество DDoS-атак с целью выкупа выросло на 67%.

Цель и задачи

Целью выпускной квалификационной работы является разработка модели раннего обнаружения DDoS-атак на основе анализа сетевого трафика.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1) провести анализ предметной области и аналогичных решений;
2) провести выбор и предобработку набора данных;
3) разработать и обучить нейросетевую модель;
4) оценить результаты работы полученной модели.

Анализ аналогичных решений

Название исследования	Метод классификации	Результат классификации
Perakovic, D. Model for Detection and Classification of DDoS Traffic Based on Artificial Neural Network [PDF]	MLP	95,6%
Saied, A. Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks [PDF]	ANN	98%
Li, Y. DDoS attack detection method based on feature extraction of deep belief network [PDF]	LSTM	Не указано
Zeinalpour, A. Addressing the Effectiveness of DDoS Attack Detection Methods Based on the Clustering Method Using an Ensemble Method [PDF]	K-means, SOMs	98,8%
David, J. DDoS Attack Detection using Fast Entropy Approach on Flow-Based Network Traffic [PDF]	Fast Entropy	Не указано
Lopez, A. Network Traffic Behavioral Analytics for Detection of DDoS Attacks [PDF]	RF	99%
Mishra, A. Prediction Approach against DDoS Attack based on Machine Learning Multiclassfier [PDF]	RF, SVM	99,99%
Alduailij, M. Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method [PDF]	RF	99,9977%

Анализ работ по раннему обнаружению

Критерии анализа:

1) параметр t – время до обнаружения DDoS-атаки;
2) методы – методы сокращения времени до обнаружения DDoS-атаки;
3) результаты обнаружения – оценка результатов обнаружения DDoS-атаки при различных значениях параметра t.

Название исследования	Метод сокращения времени	Время обнаружения, с		
		Эксперимент №1	Эксперимент №2	Эксперимент №3
Xylogiannopoulos, K. Early DDoS Detection Based on Data Mining Techniques [PDF]	Уменьшение времени между запусками алгоритма	1,1	4,3	43,0

Анализ наборов данных

Набор данных	Количество атрибутов	Размерность	Типы атак
CIC-DDoS2019	89	431 327	PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, SNMP
CIC-DoS2017	77	2 830 743 (DDoS записей – 128 027)	TCP SYN, UDP, HTTP
DDoSDB	10	–	UDP, TCP, SSDP, NTP, DNS, Chargen и др.
CSE-CIC-IDS2018	80	1 048 575	LOIC-HTTP, LOIC-UDP, HOIC, SQL Injection и др.

Характеристики выбранного файла из набора данных CIC-DDoS2019:

1) 85 атрибутов;
2) 225 745 строк – 128 027 строк DDoS-трафика и 97 718 строк легитимного трафика;
3) временной промежуток продолжительностью в 90 минут;
4) 22 DDoS-атаки.

Предобработка выбранного набора данных

Процедуры предобработки данных:

1) удаление дубликатов;
2) обработка отсутствующих значений;
3) нормализация данных;
4) кодирование категориальных признаков;
5) масштабирование признаков;
6) удаление выбросов.

Отбор атрибутов набора данных производился с помощью оценщика признаков ExtraTreesClassifier и мета-трансформатора SelectFromModel.

Категориальная метка DDoS-атаки:

– 0 – легитимный трафик (отсутствие DDoS-атаки);
– 1 – вредоносный трафик (наличие DDoS-атаки).

Предобработка выбранного набора данных

№	Атрибут	Описание	№	Атрибут	Описание
1	Timestamp	Время сеанса	8	Flow ID	Внутренний числовой идентификатор потока
2	Min Packet Length	Минимальная длина пакета	9	Packet Length Mean	Средняя длина пакета
3	Source Port	Исходный порт, используемый сеансом	10	Max Packet Length	Максимальная длина пакета
4	Destination Port	Порт назначения, используемый сеансом	11	Average Packet Size	Средний размер пакета
5	Source IP	IP-адрес источника исходного сеанса	12	Packet Length Std	Стандартное отклонение длины пакета
6	Destination IP	IP-адрес пункта назначения сеанса	13	Packet Length Variance	Разброс длин пакетов данных
7	Protocol	Протокол, используемый сеансом	14	Down/ Up Ratio	Коэффициент загрузки и выгрузки

Предобработка выбранного набора данных

Набор данных	Использование	Описание	Количество атрибутов	Количество строк
DDoS	Обучение модели	С начала датасета по конец 19-ой DDoS-атаки	26 (25 наиболее релевантных атрибутов и метка класса)	173 132
DDoS_20	Тестирование метрик и времени обнаружения DDoS-атак	С конца 19-ой DDoS-атаки по конец 20-ой DDoS-атаки		11 210
DDoS_21		С конца 20-ой DDoS-атаки по конец 21-ой DDoS-атаки		9 104
DDoS_22		С конца 21-ой DDoS-атаки по конец 22-ой DDoS-атаки		4 097

Наборы данных DDoS_20–DDoS_22 состоят из легитимного трафика с последующей DDoS-атакой.

Разделение набора данных DDoS на обучающую и валидационную выборки производилось с помощью train_test_split(X, y, test_size=0.2, random_state=42).

Реализация моделей RFC и GBC

GridSearchCV – метод поиска наилучших гиперпараметров путем перебора всех возможных комбинаций значений гиперпараметров из заданного набора.

RandomForestClassifier ()

- n_estimators : 10, **20**, 50;
- min_samples_leaf : **1**, 3, 5;
- min_samples_split : **5**, 10, 50;
- max_depth : **3**, 5, 7.

GradientBoostingClassifier ()

- n_estimators : **100**, 150, 200;
- learning_rate : **0,01**, 0,1, 0,2;
- min_samples_split : **5**, 10, 50;
- max_depth: **3**, 5, 7.

Реализация модели BidirectionalLSTM

BidirectionalLSTM

- двунаправленный слой LSTM с 128 нейронами
- двунаправленный слой LSTM с 64 нейронами
- двунаправленный слой LSTM с 32 нейронами
- полносвязный слой Dense с 1 нейроном и сигмоидной функцией активации

Параметры компиляции:

- оптимизатор – Adam;
- функция потерь – Binary Cross-Entropy;
- метрики – Accuracy.

Параметры обучения:

- количество эпох обучения – 3;
- batch_size – 64.

Метрики оценки качества работы модели

Метрики	RandomForestClassifier			GradientBoostingClassifier			BidirectionalLSTM		
	DDoS_20	DDoS_21	DDoS_22	DDoS_20	DDoS_21	DDoS_22	DDoS_20	DDoS_20	DDoS_20
Матрица ошибок	[4775 0] [0 6435]	[2839 0] [0 6265]	[2749 0] [0 1348]	[4775 0] [0 6435]	[2835 4] [0 6265]	[2748 1] [0 1348]	[4758 17] [3 6432]	[2780 59] [0 6265]	[2521 228] [0 1348]
Accuracy, %	100	100	100	100	99,96	99,98	99,82	99,35	94,43
Precision, %	100	100	100	100	99,94	99,93	99,74	99,07	85,53
Recall, %	100	100	100	100	100	100	99,95	100	100
Specificity, %	100	100	100	100	99,86	99,96	99,64	97,92	91,71
F1-score, %	100	100	100	100	99,97	99,96	99,84	99,53	92,20
Время обнаружения, с	0,0023	0,0025	0,0022	0,0014	0,0020	0,0017	0,0220	0,0250	0,0210

Сравнение времени обнаружения

Время обнаружения – время в секундах от начала моделируемой DDoS-атаки до момента предсказания моделью метки DDoS-атаки.

Набор данных	Модель	Время обнаружения DDoS-атаки, с
DDoS_20	GradientBoostingClassifier	0,0014
	KNeighborsClassifier [notebook]	0,0130
	C-SupportVectorClassifier [notebook]	0,0048
	Модель ИИ на основе Dense с Dropout [notebook]	Модель не определила DDoS-атаку

Основные результаты

В ходе выполнения выпускной квалификационной работы:

1) было использовано большее количество признаков из набора данных CIC-DDoS2019 для обучения и тестирования разработанной модели в сравнении с аналогичными моделями;
2) было произведено измерение времени обнаружения DDoS-атак с использованием разработанной модели;
3) было произведено сравнение времени обнаружения DDoS-атак с использованием разработанной модели и аналогичных моделей, обученных на наборе данных CIC-DDoS2019.

Основные результаты

В результате выполнения выпускной квалификационной работы были решены следующие задачи:

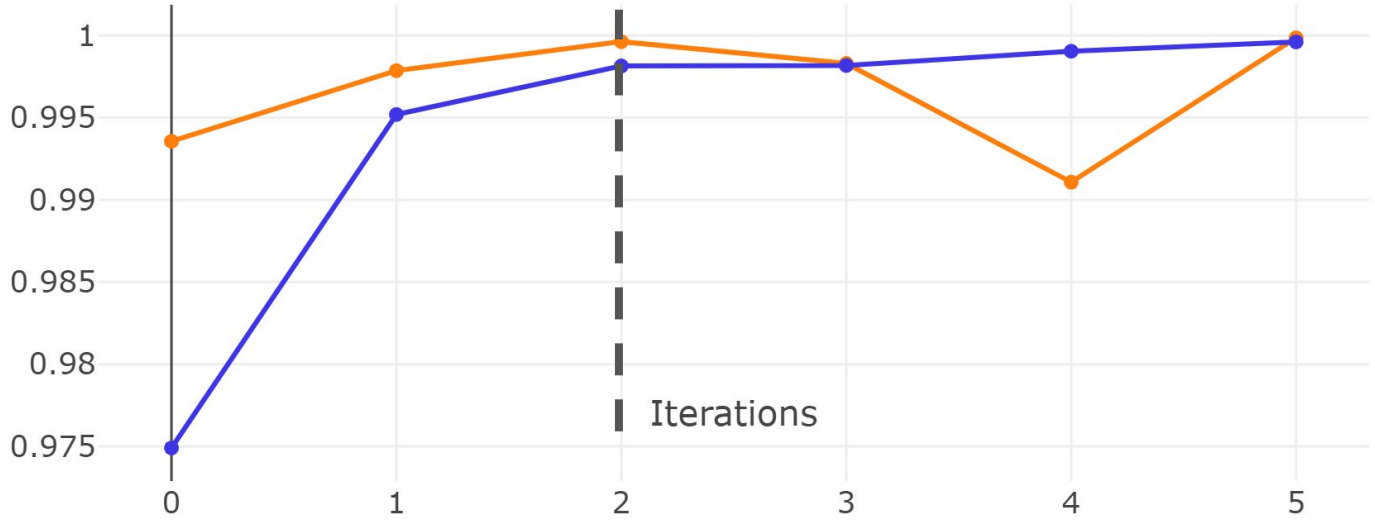
1) произведен анализ предметной области и аналогичных решений;
2) произведен анализ и выбор набора данных;
3) определена архитектура разрабатываемой модели;
4) проведено обучение разрабатываемой модели;
5) проведена оценка результатов работы полученной модели.

Направление дальнейших исследований включает доработку модели в контексте анализа признаков временных рядов сетевого трафика, дальнейшую интеграцию модели в системы администрирования компьютерных сетей.

Обучение модели BidirectionalLSTM

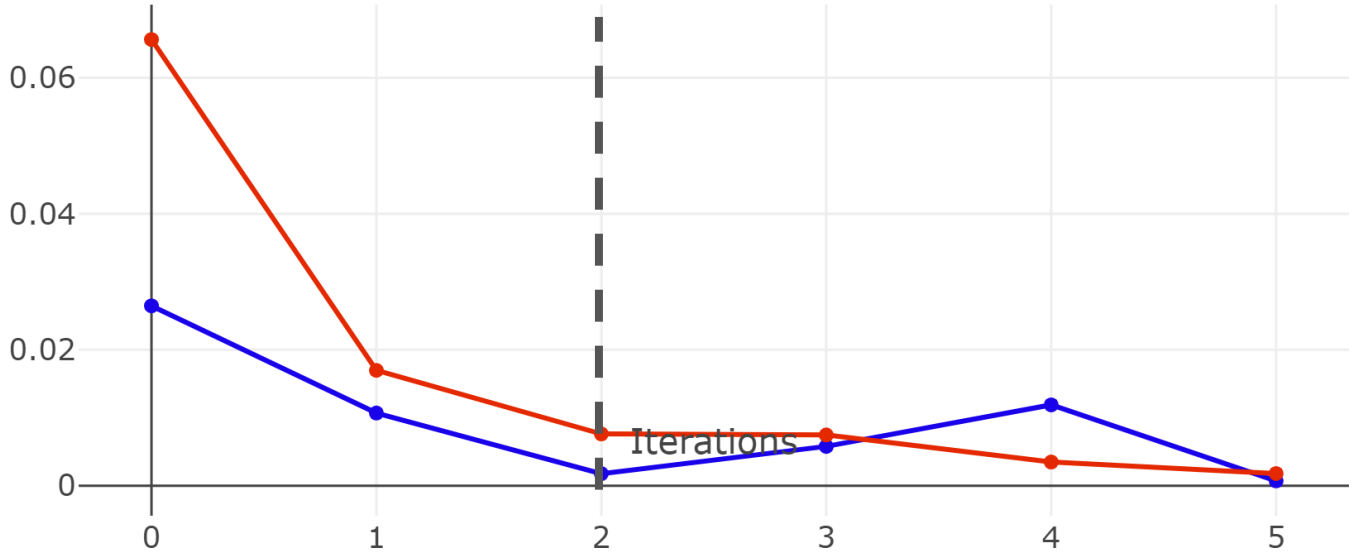
epoch accuracy

validation epoch accuracy



epoch loss

validation epoch loss



Исходный код