ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ GRU И LSTM ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В СИСТЕМАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Бекмуратов Б.А.
магистрант 2 курса, Ташкентского государственного университета информационных технологий имени Мухаммада аль-Хоразмий.
Гуломов Ш.Р.
Научный руководитель. DSc., профессор.
https://doi.org/10.5281/zenodo.20215110

Аннотация. *В статье сравниваются две рекуррентные нейронные сети -GRU и LSTM -для обнаружения сетевых атак. Эксперименты выполнены на наборе данных CIC-IDS2017 [1]. Точность GRU составила 98,3%, LSTM- 98,1%. Разница незначима. Время инференса GRU - 7,4 мс на поток. LSTM обрабатывает поток за 14,8 мс. Это в два раза дольше. Для сравнения: SVM дал точность 89,4%, Random Forest - 94,2%. Сделан вывод: GRU лучше подходит для систем реального времени в высоконагруженных сетях.*

Ключевые слова: *GRU, LSTM, обнаружение вторжений, CIC-IDS2017, глубокое обучение, системы обработки персональных данных, отбор признаков, время инференса, рекуррентные нейронные сети, компьютерная безопасность.*

1. ВВЕДЕНИЕ

Республика Узбекистан реализует стратегию «Цифровой Узбекистан - 2030» [2]. В стране создаются крупные системы обработки персональных данных (СОПД). Такие системы работают в банках, больницах, школах и госучреждениях.

Объёмы персональных данных растут. Одновременно усложняются кибератаки.

Традиционные сигнатурные системы (Snort, Suricata) плохо работают против новых угроз. Они не видят атаки «нулевого дня». Не видят полиморфные вирусы [3, 4].

Законы Узбекистана «О персональных данных» и «О кибербезопасности» требуют автоматизированного мониторинга событий безопасности [5, 6]. Операторы СОПД обязаны внедрять такие системы.

Методы глубокого обучения решают эту задачу. Рекуррентные сети LSTM и GRU учитывают временную структуру трафика. Это свойство важно для обнаружения многоэтапных атак [7].

LSTM долго считалась стандартом для анализа последовательностей [8]. GRU появилась позже. У GRU меньше параметров. Вместо трёх вентилей - два [9]. Это потенциально даёт выигрыш в скорости.

2. ОБЗОР ЛИТЕРАТУРЫ

Для обучения моделей обнаружения вторжений нужны качественные наборы данных. Один из лучших - CIC-IDS2017. Sharafaldin и его команда собрали реальный трафик с современными атаками. В датасете 78 признаков на поток и 2,5 млн записей [1].

Многие исследователи используют этот набор как стандарт.

Архитектуру GRU предложили Chung и соавторы [8]. Они показали, что сеть решает проблему затухания градиента. Это важное преимущество перед простыми RNN. Позже Cho с коллегами применили GRU к машинному переводу [9]. Сеть хорошо работала на последовательностях разной длины.

Yang провёл сравнение GRU и LSTM [10]. Он выяснил, что у GRU на 25–26% меньше параметров. При этом точность обеих сетей почти одинаковая. Зато GRU обучается на 30–40% быстрее.

Djaidja с соавторами добавили в рекуррентные сети механизмы внимания [7]. Это позволило им обнаруживать атаки на ранних стадиях. Sakib и Tabassum испытали GRU, LSTM, BiLSTM и DBN на CIC-IDS2017 [11]. Точность моделей достигла 98–99%. Но авторы не измерили время инференса.

Для Узбекистана проблему адаптации IDS исследовали Гуломов и его коллеги [3].

Они отметили, что в стране высокая доля мобильного трафика. Глобальные модели нужно настраивать под местные условия.

Пробел в существующих работах очевиден. Прямого сравнения GRU и LSTM по скорости инференса почти нет. Данное исследование восполняет этот пробел.

3. МЕТОДОЛОГИЯ

3.1. Набор данных. Использован датасет CIC-IDS2017 [1]. В нём 2,5 млн записей сетевых потоков. Данные собраны за пять дней. Каждый поток размечен одним из классов: Benign, DDoS, DoS, PortScan, Brute Force, Infiltration, Web Attack.

Таблица 1

Распределение атак по дням

День	Типы атак	Количество записей
Понедельник	Только легитимный трафик	~500 000
Вторник	Brute Force, DoS	~350 000
Среда	DoS, DDoS	~400 000
Четверг	PortScan, Infiltration	~600 000
Пятница	DDoS, Web Attack	~650 000

После очистки осталось 2,2 млн записей. Пропуски составили менее 0,5%. Выбросы заменены граничными значениями (метод IQR).

3.2. Отбор признаков. Из 78 признаков отобрано 22. Процедура включала три этапа.

Первый этап - корреляционный анализ Пирсона. Удалены признаки с $|r| > 0,95$.

Множество сократилось с 78 до 62.

Второй этап - метод взаимной информации. Оценён вклад каждого признака в определение класса. Признаки отсортированы по убыванию.

Третий этап - рекурсивное исключение признаков (RFE) с Random Forest. На каждой итерации удалялся наименее важный признак. Процесс повторялся, пока не осталось 22 признака.

Таблица 2

Отобранные признаки (22)

№	Признак
1	Flow Duration
2	Total Fwd Packets
3	Total Backward Packets
4	Fwd Packet Length Mean
5	Bwd Packet Length Mean
6	Flow IAT Mean
7	Flow IAT Std
8	Fwd IAT Total
9	Bwd IAT Total
10	Fwd PSH Flags
11	Bwd PSH Flags
12	Fwd URG Flags
13	Bwd URG Flags
14	FIN Flag Count
15	SYN Flag Count
16	RST Flag Count
17	Fwd Seg Size Min
18	Active Mean
19	Idle Mean
20	Fwd Bytes/Bulk Avg
21	Subflow Fwd Bytes
22	Init_Win_bytes_forward

Все признаки нормализованы методом Min-Max в диапазон [0,1].

3.3. Балансировка классов. В датасете сильный дисбаланс. Легитимный трафик (Benign) - 80% записей. Атаки Infiltration - менее 0,3%. Для компенсации использована взвешенная кросс-энтропия. Вес класса обратно пропорционален его частоте.

3.4. Архитектура моделей. Сравнивались четыре модели.

- SVM с линейным ядром.
- Random Forest (100 деревьев).
- LSTM (2 слоя, hidden size 128, Dropout 0,2).
- GRU (2 слоя, hidden size 128, Dropout 0,2).

Гиперпараметры GRU и LSTM приведены в таблице 3.

Таблица 3

Гиперпараметры

Параметр	Значение
Слоёв	2
Hidden size	128
Dropout	0,2
Оптимизатор	Adam

Learning rate	0,001
Batch size	64
Early stopping patience	5

Для GRU и LSTM сформированы последовательности из 10 пакетов. Размерность входа - 10 × 22.

3.5. Экспериментальная процедура. Выборка разделена на 80% обучения и 20% теста (стратифицированное разбиение). Обучение останавливалось, когда валидационная точность не росла 5 эпох.

Оценка велась по метрикам Accuracy, Precision, Recall, F1-Score. Также замерялось время инференса на один поток. Стенд: CPU Intel Core i7-10700 (8 ядер, 2,9 ГГц), GPU NVIDIA RTX 3060 (12 ГБ).

4. РЕЗУЛЬТАТЫ

4.1. Точность. Таблица 4 показывает точность моделей.

Таблица 4

Точность моделей

Модель	Accuracy	F1-Score	Precision	Recall
SVM	89,4%	88,7%	89,1%	88,4%
Random Forest	94,2%	93,8%	94,0%	93,5%
LSTM	98,1%	98,0%	98,2%	97,9%
GRU	98,3%	98,2%	98,3%	98,1%

Разница между GRU и LSTM незначима (менее 0,3%). Обе сети превосходят SVM и Random Forest.

Наилучший результат у классов Benign (99,3% F1) и DDoS (98,6% F1). Худший - у Infiltration (96,1% F1).

Причина - малая доля этого класса в выборке (менее 0,3%).

4.2. Скорость обработки. Таблица 5 показывает время инференса.

Таблица 5

Время инференса

Модель	Время (мс/поток)	Относительная скорость
SVM	1,2	1×
Random Forest	2,5	2×
LSTM	14,8	12×
GRU	7,4	6×

GRU работает в два раза быстрее LSTM. Полный цикл обработки потока для GRU - 12,5 мс.

Пропускная способность одного сенсора - 80 потоков в секунду.

4.3. Матрица ошибок. Таблица 6 показывает матрицу ошибок GRU (нормализована по строкам).

Таблица 6

Матрица ошибок GRU (%)

	Benign	DDoS	PortScan	Brute Force	DoS	Infiltration
Benign	99,2	0,4	0,2	0,1	0,1	0,0
DDoS	0,4	98,5	0,5	0,3	0,3	0,0
PortScan	0,5	0,3	97,8	0,8	0,4	0,2
Brute Force	0,8	0,2	0,6	97,0	0,8	0,6
DoS	1,0	0,5	0,3	0,7	96,5	1,0
Infiltration	1,2	0,0	0,8	0,5	0,5	96,1

Уровень ложных срабатываний - 1,2%. Ошибки возникают из-за двух причин.

Первая - легитимный высоконагруженный трафик путается с DDoS-атаками. Вторая - медленное сканирование портов путается с нормальными обращениями к разным сервисам.

5. ОБСУЖДЕНИЕ

5.1. Причины разницы в скорости. Почему GRU быстрее? У GRU два вентиля (сброса и обновления). У LSTM три (входной, забывания, выходной) [9]. Меньше вентилей - меньше матричных операций. Параметров у GRU на 25–26% меньше, чем у LSTM, при одинаковом hidden size [10]. В данной конфигурации GRU содержит 157 тыс. параметров, LSTM - 200 тыс. Это скорость.

5.2. Сравнение с другими работами. Полученные результаты совпадают с выводами Yang [10]. GRU и LSTM дают близкую точность. GRU заметно быстрее. Sakib и Tabassum [11] получили точность 98–99%, но не замеряли скорость. Данное исследование дополняет их работу данными по времени инференса. Djaidja с соавторами [7] показали, что рекуррентные сети работают на коротких последовательностях (5–10 пакетов). Это подтверждается. Длина последовательности в эксперименте - 10 пакетов.

Guillaume с коллегами [12] отметили, что LSTM требует много ресурсов. Это ограничивает её использование на периферийных устройствах. Полученные данные подтверждают: GRU легче и быстрее.

5.3. Ограничения. У исследования есть ограничения.

Во-первых, эксперименты проведены только на CIC-IDS2017 [1]. Реальный трафик может отличаться.

Во-вторых, обучение велось на ограниченном наборе атак. Другие типы угроз не рассматривались.

В-третьих, замеры сделаны на одной конфигурации железа. На других устройствах результаты могут измениться.

Для устранения этих ограничений нужны дополнительные тесты.

6. ЗАКЛЮЧЕНИЕ

Проведено экспериментальное сравнение GRU, LSTM, SVM и Random Forest на CIC-IDS2017.

Основные выводы:

1. GRU достиг точности 98,3%, LSTM - 98,1%. Разница статистически незначима.

2. Время инференса GRU - 7,4 мс на поток. LSTM - 14,8 мс. GRU работает в два раза быстрее.
3. SVM и Random Forest значительно уступают по точности (89,4% и 94,2%).

Рекомендация. GRU оптимальна для обнаружения вторжений в реальном времени в высоконагруженных СОПД.

Дальнейшие исследования. Стоит рассмотреть BiGRU (двунаправленные сети), добавить механизмы внимания, разработать методы онлайн-обучения. Также необходимо протестировать модель на реальном трафике организаций Узбекистана.

ЛИТЕРАТУРА

1. Sharafaldin, I., Lashkari, A. H., Ghorbani, A. A. Toward a Lifetime Dataset for Network Intrusion Detection // Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP). 2018. P. 1-11. DOI: 10.5220/0006639800850095
2. Указ Президента Республики Узбекистан № УП-6079 «Об утверждении стратегии "Цифровой Узбекистан – 2030"» от 5 октября 2020 года.
3. Гуломов Ш.Р., Каримов М.М., Ташев К.А. Интеллектуальные системы обнаружения вторжений в корпоративных сетях // Вестник Ташкентского университета информационных технологий. 2022. № 3. С. 45-52.
4. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press. 2016. 800 p.
5. Закон Республики Узбекистан «О персональных данных» № ЗРУ-547 от 2 июля 2019 года.
6. Закон Республики Узбекистан «О кибербезопасности» № ЗРУ-764 от 15 апреля 2022 года.
7. Djaidja, T. E. T., Brik, B., Senouci, S. M., Boualouache, A., Ghamri-Doudane, Y. Early Network Intrusion Detection Enabled by Attention Mechanisms and RNNs // IEEE Transactions on Information Forensics and Security. 2024. DOI: 10.1109/TIFS.2024.3441862
8. Chung, J., Gulcehre, C., Cho, K., Bengio, Y. Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling // arXiv preprint arXiv:1412.3555. 2014.
9. Cho, K., Van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., Bengio, Y. Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation // arXiv preprint arXiv:1406.1078. 2014.
10. Yang, B. Trade-off Analysis of Efficiency and Accuracy in GRU vs LSTM // ITM Web of Conferences. 2025. Vol. 80. Article 01017. DOI: 10.1051/itmconf/20258001017
11. Sakib, M. S., Tabassum, N. Analyzing Deep Learning Model Performance for Intrusion Detection on CIC-IDS2017 Dataset // GitHub Repository. 2025.
12. Guillaume, R. B. L., Chen, Z., Liu, T. Decision-based Method for Network Intrusion Detection using GRU // Journal of Cyber Security. 2022. Vol. 4. No. 3. P. 1-15.