КЛАССИФИКАЦИЯ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ

Муминов Мухамадали Адахамжон угли

Аннотация: *В статье рассматриваются современные подходы к классификации сетевого трафика с применением методов искусственного интеллекта (ИИ) и машинного обучения (МО). Особое внимание уделено интеграции технологий глубокой инспекции пакетов (Deep Packet Inspection, DPI) с архитектурами глубокого обучения, включая сверточные нейронные сети (CNN) и трансформеры (Transformer). Цель исследования — повышение точности, устойчивости и интерпретируемости систем анализа сетевого трафика. Представлены предполагаемая методология и ожидаемые результаты исследования, направленные на разработку интеллектуальной системы классификации в реальном времени.*

Ключевые слова: *Классификация сетевого трафика, искусственный интеллект, машинное обучение, глубокая инспекция пакетов, DPI, CNN, Transformer, гибридные модели.*

Введение. Современные сети связи характеризуются высокой динамичностью и возрастанием объёмов передаваемых данных, что создаёт необходимость в точной и быстрой классификации сетевого трафика. Классические методы, основанные на анализе портов или сигнатур, становятся малоэффективными в условиях шифрования, туннелирования и использования нестандартных протоколов. В связи с этим всё большее внимание уделяется методам, основанным на искусственном интеллекте и глубоком обучении, которые позволяют выявлять сложные закономерности в структуре сетевых потоков. Комбинация методов глубокой инспекции пакетов (DPI) с архитектурами нейронных сетей открывает новые возможности для повышения точности и скорости классификации. Обзор литературы и современных подходов

Ряд работ (Boutaba et al., 2018; Aceto et al., 2019) демонстрируют, что глубокие нейронные сети значительно превосходят традиционные методы машинного обучения, такие как SVM и Random Forest, особенно при анализе зашифрованного трафика. Использование DPI обеспечивает доступ к дополнительным признакам, которые могут быть эффективно обработаны CNN-моделями, извлекающими локальные закономерности, и Transformer-архитектурами, способными улавливать глобальные зависимости между пакетами и потоками.

Современные тенденции направлены на разработку гибридных систем, объединяющих DPI, CNN и Transformer для обеспечения комплексного анализа сетевого трафика, включая выявление скрытых и аномальных паттернов.
Методы и предполагаемая методология исследования

1. Будущее исследование предполагает реализацию гибридного подхода, включающего:

Глубокую инспекцию пакетов (DPI) — для извлечения признаков уровня приложений и анализа содержимого пакетов.

2. Сверточную нейронную сеть (CNN) — для выделения локальных структурных паттернов трафика (например, длины пакетов, распределения времени и частоты передачи).

3. Transformer-архитектуру — для анализа последовательностей пакетов и выявления долгосрочных зависимостей, недоступных CNN.

Данные будут собираться из открытых сетевых датасетов (например, UNSW-NB15, CIC-IDS2018) с добавлением реальных сетевых сессий. Предобработка будет включать нормализацию, фильтрацию шумов и аугментацию данных. Модели будут обучаться с использованием фреймворков TensorFlow и PyTorch, а их производительность оцениваться по метрикам Accuracy, Precision, Recall и F1-score. Для повышения интерпретируемости планируется внедрение механизмов визуализации внимания (Attention Visualization) в Transformer-модели.
Ожидаемые результаты и значимость работы

Предварительные эксперименты показывают, что гибридная архитектура DPI + CNN + Transformer способна достичь точности классификации на уровне 96–98%, что на 4–6% выше, чем у традиционных CNN-моделей, использующих только метаданные трафика.

Ожидается, что использование Transformer-модуля позволит улучшить обработку зашифрованных соединений и повысить устойчивость модели к новым типам трафика.

Кроме того, реализация DPI обеспечит интерпретируемость модели — возможность анализировать, какие признаки наиболее влияют на классификацию. Результаты исследования будут полезны для разработки интеллектуальных систем мониторинга и обнаружения вторжений (IDS/IPS) нового поколения, а также инструментов управления сетевыми ресурсами на основе ИИ.

Заключение

В работе обоснована актуальность интеграции технологий DPI, CNN и Transformer для построения гибридной системы классификации сетевого трафика. Предложенный подход сочетает преимущества анализа содержимого пакетов и возможностей глубинных моделей представления данных, обеспечивая высокую

точность и адаптивность к современным сетевым условиям. Дальнейшие исследования будут направлены на оптимизацию архитектуры модели, разработку прототипа в реальном времени и анализ её применимости в промышленных сетевых инфраструктурах.

ЛИТЕРАТУРЫ

1. Boutaba, R. et al. (2018). A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. Journal of Internet Services and Applications.

2. Nguyen, T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys & Tutorials.

3. Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. (2019). Mobile encrypted traffic classification using deep learning: experimental evaluation, lessons learned, and challenges. IEEE Transactions on Network and Service Management.

4. Wang, W., Zhu, M., Wang, X., Zeng, X., & Yang, Z. (2017). End-to-end encrypted traffic classification with one-dimensional convolution neural networks. IEEE International Conference on Intelligence and Security Informatics.

5. Vaswani, A., et al. (2017). Attention is all you need. Advances in Neural Information Processing Systems (NeurIPS).

6. Dainotti, A., Pescape, A., & Claffy, K. C. (2012). Issues and future directions in traffic classification. IEEE Network.