«Генерация и анализ сетевого трафика в режиме реального времени»

Репозиторий (закрытый) https://gitflic.ru/project/ivanovga/yalynara_py

---

o 1. Авторы

- **Лаврова Е.В.** - проф., д.т.н. директор Учебно-научного института информационных технологий.
- **Ялына Р.А.** - старший преподаватель кафедры Информационной безопасности
- **Иванов Г. А.** - ассистент кафедры Информационной безопасности

o 2. Общее описание

Проект представляет собой интегрированную систему, разработанную при кафедре Информационной безопасности . Он объединяет в единой информационной системе следующие функциональные блоки:

Модуль	**Описание**	**Ключевые технологии**
Парсинг pcap	Чтение пакетов из файлов формата PCAP с помощью Scapy и `RawPcapReader`, разделение на чанки по 10 000 пакетов и распараллеливание с помощью `multiprocessing.Pool`.	Scapy, многопоточность, itertools
Обнаружение угроз	Пороговые алгоритмы для сканирования портов, DDoS-атак, брутфорса по протоколу SSH и HTTP, основанные на статистике уникальных портов, частоте пакетов и временных окнах (60 минут).	Python-коллекции, datetime, Counter
Синтетическая генерация	Класс `PacketGenerator` моделирует обычный поток данных и атаки (syn-flood, ssh-bruteforce, сканирование портов, HTTP-атака с неудачной аутентификацией) с произвольным временем начала и продолжительностью.	random, datetime, multiprocessing
Разработка признаков	Для каждой пары IP-адресов вычисляются интервалы между пакетами, их гистограмма, энтропия, частота использования протоколов, индикаторы	NumPy, SciPy, HuggingFace Transformers

Модуль	Описание	Ключевые технологии
	«top-port», а также эмбеддинги из трансформерной модели (архитектура, подобная BERT).	
Нейронный классификатор	Комбинированный MLP–LSTM-классификатор, обучаемый на синтетических и реальных данных, выдает вероятности для 5 классов (сканирование портов, DDoS, брутфорс по SSH, брутфорс по HTTP, обычные атаки).	PyTorch, torch.nn, F.softmax
Онлайн-обработка	Пакетный поток, обновление признаков в реальном времени, отображение вероятностей и динамики атак с помощью графиков Matplotlib и интерактивного окна PyQt5.	matplotlib, PyQt5, collections.deque
Визуализация IP-кластеров	Полярная проекция, где каждая точка - это IP-адрес, цвет которого отражает вероятность атаки.	matplotlib, seaborn, ipaddress

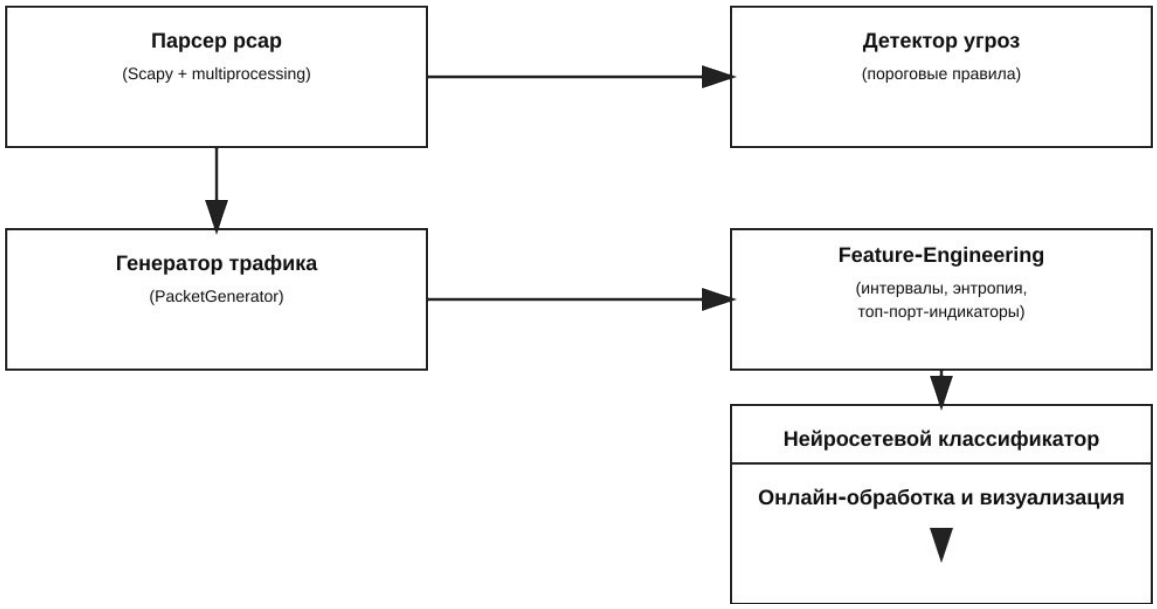
---

o 3. Цели и задачи исследования

1. **Разработка универсальной платформы** для анализа и классификации сетевого трафика, совместимой с любыми pcap-файлами.
2. **Создание генеративной модели** трафика, обеспечивающей реалистичную имитацию атак и нормального поведения.
3. **Внедрение адаптивного онлайн-классификатора** с низкой задержкой (< 50 мс) для реального мониторинга.
4. **Обеспечение визуальной интуитивности** результатов через графический интерфейс и полярную карту IP-кластеров.
5. **Оценка эффективности** по метрикам точности, полноты и ROC-AUC в сравнении с существующими методами (см. Список литературы).

---

o 4. Архитектура системы



o

o 5. Установка и запуск

1. Клонирование репозитория (доступ по запросу)
git clone https://gitflic.ru/project/ivanovga/yalynara_py.git
cd yalynara_py
2. Создание виртуальной среды
python3 -m venv venv source venv/bin/activate
3. Установка зависимостей
pip install -r requirements.txt
4. Запуск анализа pcap
python src/analyze_pcap.py --pcap_file data/traffic.pcap --output_dir results/ --no_details
5. Запуск онлайн-классификатора
python src/online_classifier.py --model_dir models/ --iface eth0
Примечание: для работы с pcap-файлами необходим пакет `tshark` и утилита `editcap` (Wireshark).
6. Примеры использования
6.1. Детерминированный анализ
python src/analyze_pcap.py -f data/traffic.pcap -o results/ -d
Содержит подробный текстовый отчет и файлы JSONL с размеченными пакетами.

§

§ 6.2. Визуализация на платформе

python src/gui_visualization.py --model_path модели/ --iface eth0