1 ВСТУП

1.1 Огляд продукту

Система, розроблена у кваліфікаційній роботі Великороднього А. В., являє собою інноваційне рішення для автоматичного виявлення DDoS-атак у зашифрованому мережевому трафіку за допомогою методів глибинного навчання з підкріпленням (Reinforcement Learning, RL). На відміну від традиційних підходів, що базуються на аналізі сигнатур або глибокій інспекції пакетів, запропонована методика використовує лише метадані мережевих потоків, такі як розмір пакетів, інтервали між ними, частота сеансів та інші статистичні характеристики.

Процес роботи системи складається з кількох етапів. Спочатку виконується попередня фільтрація потоків за допомогою евристичних методів для виявлення очевидних аномалій. Далі застосовується агент на основі алгоритму Double Deep Q-Network (DDQN), який аналізує складніші моделі поведінки трафіку. Агент навчається у симульованому середовищі та отримує зворотний зв’язок у вигляді винагороди за правильні рішення щодо класифікації потоків як легітимних або шкідливих.

1.2 Мета

Метою роботи є дослідження методів аналізу зашифрованого мережевого трафіку та створення прототипу, що забезпечує точне й швидке виявлення DDoS‑атак без необхідності доступу до вмісту TLS‑з’єднань.

1.3 Межі

Система працює лише з метаданими NetFlow/IPFIX або згенерованих CICFlowMeter потоків; розшифрування трафіку або DPI‑аналіз не передбачені. Модель протестовано на 17 000 потоках із публічних датасетів CIC‑DDoS2019 та HIKARI 2021, що підтверджує її застосовність до різних протоколів і сценаріїв атак.

Продуктивність обмежена 1 000 потоками за ≤5 с на одній інстанції;

1.4 Посилання

В проєкті були використані такі посилання:

1. Kheddar H., Messai N., Himeur Y., Awad A. Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review // Journal of Network and Computer Applications. – 2023. URL: <https://doi.org/10.1016/j.jnca.2023.103760>
2. Ferriyan H., Wibisono A., Muchtar A. HIKARI-2021 Dataset: Benchmark for Encrypted Traffic DDoS Detection // IEEE Access. – 2021. URL: <https://doi.org/10.3390/app11177868>
3. Vargas-Rosales C., Lopez-Ortiz G., Mendez-Hernandez H. SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning: // IEEE Access – 2021. URL: <https://doi.org/10.1109/ACCESS.2021.3101650>.
4. Yang J., Liang G., Wen G., Gao T. A deep-learning- and reinforcement-learning-based system for encrypted network malicious traffic detection // Information and communications – 2021. URL: [https://doi.org/10.1049/ell2.12125](https://doi.org/10.1049/ell2.12125%20)
5. Hu J., Yang X., Hu J., Peng Y. A Q-learning algorithm for Markov decision processes with continuous state spaces // Systems & Control Letters – 2024. URL: <https://doi.org/10.1016/j.sysconle.2024.105782>
6. Yungaicela-Naula M., Vagras-Rosales C., Perez-Dias J., Carrera D. A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning // Journal of Network and Computer Applications – 2022. URL: <https://doi.org/10.1016/j.jnca.2022.103444>
7. OpenAI Gym. Documentation [Електронний ресурс]. URL: [https://gym.openai.com/](https://gym.openai.com/" \t "_new)
8. PyTorch Documentation [Електронний ресурс]. URL: <https://pytorch.org/docs/>
9. InfluxDB Documentation [Електронний ресурс]. URL: <https://docs.influxdata.com/influxdb/v2/>
10. О.Ф. Лановий, І.В. Кобзев, О.С. Удовенко «Система підрахунку трафіку мережі з використанням засобів об’єктно-орієнтованого програмування». Право і Безпека 7,№ 2 с. 213-217 2008. URL: <http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Pib_2008_7_2_46.pdf>
11. Поліщук В. Розробка системи виявлення вторгнень на основі аналізу аномалій у мережевому трафіку з використанням машинного навчання // Матеріали Ⅻ науково-технічної конференції „Інформаційні моделі, системи та технології“. – 2024. – С. 76-76. [6]
12. Головенко Б. В. Розробка програмного забезпечення для виявлення DDOS aтак : дис. – ТНТУ, 2022.

1.5 Означення та абревіатури

|  |  |
| --- | --- |
| Абревіатура | Розшифрування та пояснення |
| **TLS** | Transport Layer Security – Протокол шифрування транспортного рівня. |
| **Flow** | Агрегований запис характеристик мережевого сеансу (5‑tuple). |
| **SOC** | Security Operations Center – Центр управління інформаційною безпекою. |
| **SIEM/SOAR** | Платформи збору та кореляції подій безпеки та автоматизованого реагування. |
| **TPR** | True Positive Rate – Повнота виявлення атак. |
| **FPR** | False Positive Rate – Частка хибнопозитивних спрацювань. |
| **RL** | Reinforcement Learning – Глибинне навчання з підкріпленням. |
| **DDQN** | Double Deep Q-Network – Тип RL-алгоритму з покращеною стабільністю. |
| **MVP** | Minimum Viable Product – Мінімально життєздатний продукт (прототип системи). |

2 ЗАГАЛЬНИЙ ОПИС

2.1 Перспективи продукту Подальший розвиток прототипу системи виявлення DDoS‑атак у зашифрованому трафіку передбачає перехід до хмарної багатозонної інфраструктури зі автоматичним масштабуванням. Використання керованих сервісів Amazon RDS Multi‑AZ для PostgreSQL та TimescaleDB для time‑series аналітики з архівацією історичних даних у S3 підвищить відмовостійкість і спростить довгострокове зберігання. Для обробки десятків мільйонів мережевих потоків планується горизонтальне масштабування баз даних і потокової обробки, а всі компоненти будуть контейнеризовані у Docker. Планується продовження роботи над RL‑моделлю (Double DQN) з автоматичним оновленням політики без простою сервісу та дослідження додаткових технік оптимізації гіперпараметрів для підвищення стабільності та точності.

Інтерфейс аналітика буде розширено топологічними картами джерел атак, тепловими картами пікових навантажень і можливістю налаштування порогів спрацювання через GUI. Стек спостережності на основі Prometheus і Grafana буде доповнено SLA‑алармами та бізнес‑дашбордами.

2.2 Функції продукту

* Збір NetFlow/IPFIX у реальному часі;
* Формування ознак мережевого потоку;
* Попередня обробка та нормалізація трафіку;
* Виявлення зловмисного трафіку за допомогою RL-агента;
* Збереження результатів у PostgreSQL та TimescaleDB.

2.3 Характеристики користувачів Типові користувачі:

* Аналітик SOC‑центру;
* Інженер DevSecOps.

2.4 Загальні обмеження

Система не виконує активного блоку трафіку; інтеграція з фаєрволами можлива через SOAR. Виявлення адаптивних атак потребує оновлення політики RL‑агента.

2.5 Припущення та залежності

* Python 3.10 + PyTorch 2.1.0
* Docker 26.0; Docker Compose
* PostgreSQL 15, TimescaleDB

3 КОНКРЕТНІ ВИМОГИ

3.1 Вимоги до зовнішніх інтерфейсів

3.1.1 Інтерфейс користувача

Головна сторінка дашборда показує: TPR, FPR, графік потоків за останні 24 год, карту джерел атак, таблицю TOP‑IP. Деталізація потоку включає хронологію подій, значення ознак, рішення RL-моделі.

3.1.2 Програмний інтерфейс

REST API відповідає OpenAPI 3.0. Підтримується пагінація (500 записів), максимальний розмір відповіді – 1 МБ.

3.1.3 Продуктивність

Затримка від появи потоку до ALARM ≤ 5 с при 1 000 потоках/сек. RL‑модель виконує інференс на CPU (i7‑11700) за ~40 мс.

3.2 Властивості програмного продукту

* Доступність: дві зони доступності в AWS, 99,9 % часу безвідмовної роботи;
* Безпека: TLS 1.3 між сервісами, контроль доступу до GUI;
* Супроводжуваність: CI/CD на GitHub Actions, тестове покриття >60%;
* Переносимість: x86\_64 і ARM64;
* Масштабованість: auto-scaling, Kafka для балансування черг.

3.3 Вимоги до бази даних

* Таблиця Flows: час, адреси, обсяги трафіку;
* Таблиця Alerts: час, тип атаки, ймовірність.
* TimescaleDB: часова метрика впевненості RL-агента.

3.4 Алгоритми

RL-агент

* Double DQN, зворотній зв’язок на основі функції винагороди. Параметри навчання: 50 епох, batch = 128, epsilon decay, early stop.

3.5 Експериментальні результати

Проведено навчання/валідацію на змішаному датасеті (17 032 потоки). Середня точність 92 %, TPR 89.6 %, FPR 9.2 %. Час обробки – 43 с на EC2 m6i.large.