

ОПТИМІЗАЦІЯ ВИЛУЧЕННЯ ОЗНАК У ТРАНСФОРМЕРАХ ЗА ДОПОМОГОЮ КОМБІНАЦІЇ GLOBALAVERAGEPOOLING1D І GLOBALMAXPOOLING1D ДЛЯ КЛАСИФІКАЦІЇ МЕРЕЖЕВИХ АТАК

Полторацький В.О., Гавриленко С.Ю.

Національний технічний університет

"Харківський політехнічний інститут", м. Харків

У задачах класифікації мережеских атак трансформери виявляють високу ефективність завдяки здатності моделювати складні взаємозв'язки в мережеских даних [1]. Однак їхня складна архітектура та висока розмірність вхідних ознак можуть призводити до перенавчання, особливо при роботі з неоднорідними даними. Ефективна агрегація ознак дозволяє зменшити цю проблему, забезпечуючи кращу узагальнюючу здатність і підвищуючи точність виявлення рідкісних класів [2].

Окреме використання традиційних методів агрегації "GlobalAveragePooling1D" або "GlobalMaxPooling1D", може призвести до втрати локальних особливостей або глобального контексту даних, що знижує точність у задачах із високою варіативністю класів, таких як виявлення рідкісних атак.

Для підвищення ефективності роботи моделей досліджено можливість комплексного використання комбінації "GlobalAveragePooling1D" і "GlobalMaxPooling1D", що забезпечує збалансований підхід для захоплення як узагальнених, так і пікових ознак. Це створює більш інформативне представлення, яке передається до щільних шарів класифікаційної моделі. Такий підхід дозволяє моделі одночасно враховувати глобальний контекст мережевого трафіку та локальні аномалії, що є критичним для розмежування класів. Розроблено програмні моделі трансформерів як з окремим використанням зазначених пулінгів так і з використанням їх комбінації. У якості вихідних даних використано датасет, що містить інформацію про мережескі вторгнення UNSW-NB15, із 4 класами (Normal, Exploits, Fuzzers, Generic). Використано такі налаштування моделі: 2 блоки трансформера, batch size 128, до 30 епох із EarlyStopping.

Використання комбінації "GlobalAveragePooling1D" і "GlobalMaxPooling1D" дозволило знизити показник loss-функції в середньому на 12% та підвищити точність класифікації на 1% порівняно з окремим використанням пулінгів.

Література:

1. Gavrylenko S., Poltoratskyi V., Nechyporenko A., Intrusion detection model based on improved transformer. *Advanced Information Systems*, 2024, 8(1), p. 94–99.
2. Gholamalinejad, Hossein & Khosravi, Hossein. (2020). Pooling Methods in Deep Neural Networks, a Review. 10.48550/arXiv.2009.07485.