УДК 004.9

Ткачук Р.О., аспірант
Шуліка Я.П., аспірант
Шимко С.В., аспірант
Мелешко Є.В., докт. техн. наук, професор
Центральноукраїнський національний технічний університет, м. Кропивницький,
elismeleshko@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ПРИ АНАЛІЗІ МЕРЕЖЕВОГО ТРАФІКУ

Метою роботи було дослідження методів застосування нейронних мереж для виявлення інформаційних атак на комп'ютерні мережі шляхом аналізу мережевого трафіку.

Як показало дослідження, для аналізу мережного трафіку та виявлення аномалій або інформаційних атак можна використовувати нейронні мережі, які здатні моделювати часові та просторові залежності в даних, зокрема, багатошарові нейронні мережі (MLP) [1], рекурентні нейронні мережі (RNN) [2, 3], згортково-рекурентні мережі (CRNN) [4], графові нейронні мережі (GNN) [5, 6].

Багатошарові нейронні мережі прямого поширення – мережі, у яких сигнал поширюється в одному напрямку – від входу до виходу, навчання – на основі градієнтного спуску. Можуть використовуватися для аналізу часових рядів мережевого трафіку.

Рекурентні нейронні мережі – мають пам'ять і можуть аналізувати послідовності. Високоефективні в аналізі часових рядів з нестаціонарною структурою та динамікою.

Згорткові нейронних мережі – використовують локальний з'єднуючий шар і фільтри для отримання ознак із даних. Знаходять довгострокові залежності в часових рядах та швидко навчаються. *Рекурентно-згорткові нейронні мережі* – це комбінація рекурентних та згорткових мереж яка може моделювати складні нелінійні залежності та знаходити високорівневі ознаки у часових рядах мережевого трафіку.

Графові нейронні мережі – можуть враховувати топологічну структуру комп'ютерної мережі та взаємозв'язок між вузлами та ребрами, що може підвищити точність виявлення аномалій, атак або вторгнень, можуть витягувати приховані ознаки з сирих даних трафіку, такі як пакети, потоки або сесії, без необхідності ручної інженерії ознак.

Аналіз мережного трафіку за допомогою нейронних мереж для виявлення інформаційних атак потребує таких кроків:

1. *Попередня обробка даних*. Мережевий трафік є потоком пакетів, які мають різні параметри, такі як IP-адреси, порти, протоколи тощо. Для аналізу цих даних необхідно перетворити їх на числові або категоріальні ознаки, які можуть бути подані на вхід нейронної мережі. Наприклад, можна використати швидке кодування (one-hot encoding) для категоріальних ознак або нормалізацію для числових ознак. Також можна використати методи відбору ознак для зменшення розмірності даних та усунення шуму чи надмірності.

2. *Вибір архітектури нейронної мережі*. Залежно від характеру даних та мети аналізу можна вибрати різні типи нейронних мереж, наприклад, багатошаровий перцептрон (MLP), рекурентну нейронну мережу (RNN), згорткову нейронну мережу (CNN), графову нейронну мережу (GNN) тощо. Кожен тип нейромережі має свої переваги та недоліки, а також специфічні параметри. Є доцільним для конкретної задачі спробувати та порівняти різні нейромережі у процесі навчання і тестування, і тільки після обрати найкращу для неї.

3. *Навчання нейронної мережі*. Для навчання нейромережі необхідно розділити дані на навчальну, валідаційну та тестову вибірки. Навчальна вибірка використовується для налаштування ваг нейромережі за допомогою алгоритму навчання, такого як стохастичний градієнтний спуск (SGD) або адаптивний градієнтний спуск (Adam). Валідаційна вибірка використовується для перевірки якості навчання та регуляризації моделі, наприклад, за

допомогою ранньої зупинки (early stopping) або методу відсіву (dropout). Тестова вибірка використовується для оцінки якості роботи мережі на нових даних.

4. *Оцінка та інтерпретація результатів*. Для оцінки результатів аналізу мережного трафіку можна використовувати різні метрики та засоби, такі як точність (precision), повнота (recall), F-мера, ROC-крива тощо. Це дозволяє виміряти, наскільки добре модель здатна класифікувати трафік на нормальний та аномальний, виявляти різні типи атак. Для інтерпретації результатів можна використовувати різні методи візуалізації чи пояснення роботи моделі, наприклад, методи важливості ознак чи локальних апроксимацій. Вони дозволяють зрозуміти, які ознаки чи частини даних впливають на рішення моделі і чому.

Нейромережі можуть виявляти складні залежності у часових рядах трафіку і здатні знаходити закономірності та ознаки, що дозволяють розпізнавати інформаційні атаки. Різні типи нейромереж мають свої переваги і недоліки для аналізу мережевого трафіку.

Багатошарові нейромережі прямого поширення прості і універсальні, але не можуть ефективно моделювати складні нелінійні залежності і не мають довгострокову пам’ять для аналізу часового ряду. Рекурентні нейромережі є потужними засобами для обробки послідовностей даних, але вони складні у побудові і тренуванні і схильні до перенавчання і зникання градієнтів. Згорткові нейромережі ефективні для знаходження закономірностей в сигналах та часових рядах, але вони потребують багато параметрів і обчислювальних ресурсів і не завжди добре підходять для одновимірних часових рядів, адже основне їх призначення – робота з зображеннями. Рекурентно-згорткові нейромережі поєднують переваги обох типів мереж і долають їх недоліки, але вони складні у побудові і тренуванні і потребують налаштування багатьох гіперпараметрів. Графові нейромережі можуть враховувати топологічну структуру комп’ютерної мережі, що підвищує точність виявлення аномалій та інформаційних атак. Але вони обчислювально складні та ресурсозатратні, вимагають великого об’єму навчаючої вибірки. Тому при виборі нейромережі для виявлення атак слід враховувати особливості даних та наявність обчислювальних можливостей. Також слід проводити експерименти і порівняльний аналіз різних типів нейромереж на цільових даних та оцінювати їх якість за допомогою різних метрик.

Нейронні мережі є потужним інструментом для аналізу мережевого трафіку та виявлення кібератак, оскільки вони здатні навчатися та адаптуватися до нових типів загроз. Але вони вимагають передобробки даних, вибору архітектури, навчання та оцінки результатів. Для кожного етапу існують різні методи та параметри, які потрібно підбирати залежно від характеру даних та мети аналізу. Тож, розробникам доводиться багато експериментувати та підбирати потрібну архітектуру і параметри. Також нейронні мережі мають високу обчислювальну складність, необхідність великого обсягу навчальних даних, ризик перенавчання чи недонавчання, складність інтерпретації результатів тощо.

Список посилань

1. Wang M., Lu Y., Qin J. A dynamic MLP-based DDoS attack detection method using feature selection and feedback // Computers & Security, Vol. 88, 2020, doi: https://doi.org/10.1016/j.cose.2019.101645

2. Sherstinsky A. Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network // Physica D: Nonlinear Phenomena, Vol. 404, 2020.

3. Sivamohan S., Sridhar S. S., Krishnaveni S. An effective recurrent neural network (RNN) based intrusion detection via bi-directional long short-term memory // In 2021 international conference on intelligent tech-nologies (CONIT), IEEE, 2021, pp. 1-5.

4. Liu H., Lang B., Liu M., Yan H. CNN and RNN based payload classification methods for attack detection // Knowledge-Based Systems, Vol. 163, 2019, pp. 332-341.

5. Scarselli F., Gori M., Tsoi A. C., Hagenbuchner M., Monfardini G. The Graph Neural Network Mod-el // IEEE Transactions on Neural Networks, Vol. 20, Issue 1, 2009, pp. 61-80.

6. Zhang B., Li J., Chen C., Lee K., Lee I. A Practical Botnet Traffic Detection System Using GNN // In: Meng, W., Conti, M. (eds) Cyberspace Safety and Security, CSS 2021. Lecture Notes in Computer Science(), vol. 13172, Springer, Cham, 2022, doi: https://doi.org/10.1007/978-3-030-94029-4_5