Застосування нейронної мережі типу PNN для розпізнавання мережевих кібератак

Гойко Франц, студент [1](ORCID: 0009-0009-0562-6962)
Терейковська Людмила, проф., д-р техн. наук [2](ORCID: 0000-0002-8830-0790)
[1] *Київський національний університет будівництва і архітектури, Україна*

АНОТАЦІЯ

Представлено результати дослідження застосування ймовірнісної нейронної мережі типу PNN у задачі класифікації кібератак. Важливість цієї задачі обумовлена тим, що зростання кількості та складності кібератак у сучасних інформаційних системах вимагає розробки ефективних методів їхнього виявлення та класифікації для своєчасного реагування та мінімізації ризиків. Як показує практичних досвід та результати аналізу науково-практичних джерел, застосування ймовірнісної нейронної мережі типу PNN потребує адаптації до задачі класифікації кібератак задля вдосконалення систем кіберзахисту та підвищенню рівня інформаційної безпеки.

Ключові слова: ймовірнісні нейронні мережі, PNN, кіберзахист, машинне навчання, класифікація кібератак, мережевий трафік, інформаційна безпека.

1. ВСТУП

Стрімке зростання кількості кібератак у сучасних мережах створює серйозні виклики для систем інформаційної безпеки. За даними міжнародних звітів, щороку з'являються сотні нових типів шкідливих дій, більшість із яких традиційні методи виявлення не здатні своєчасно ідентифікувати. Це зумовлює потребу у впровадженні інтелектуальних технологій, здатних працювати у режимі реального часу. Дослідження останніх років [1–4] підтверджують, що застосування у задачах класифікації ймовірнісної нейронної мережі типу PNN демонструє високу ефективність при виявленні різних типів атак, однак залишаються відкритими питання щодо оптимізації продуктивності та адаптивності.

2. МЕТА

Метою даної роботи є визначення перспективних шляхів вдосконалення нейронної мережі типу PNN для застосування у задачах розпізнавання мережевих атак.

3. ПЕРСПЕКТИВНІ ШЛЯХИ ВДОСКОНАЛЕННЯ НЕЙРОННОЇ МЕРЕЖІ ТИПУ PNN ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ЗАГРОЗ

Аналіз окремих науково-практичних рішень свідчить про високий потенціал цього підходу. Так, у дослідженні [1], де PNN було застосовано для класифікації атак з використанням набору даних NSL-KDD, що охоплює категорії DoS, Probe, U2R та R2L, модель продемонструвала точність понад 92% при виявленні поширених атак, зокрема DoS. Додатковою перевагою є безітераційність навчання, а отже короткий термін та стабільність навчання.

Навчання мережі здійснюється швидко за рахунок додавання нейронів, що співвідносяться із новими образами кібератак, у шар образі. Завдяки цьому система може ефективно адаптуватися до змін мережевого трафіку в реальному часі. Водночас точність класифікації рідкісних атак залишалася нижчою, що вказує на необхідність подальших удосконалень і комбінування PNN з іншими підходами. Зокрема, перспективним є інтегрування цього методу з алгоритмами вибору ознак або глибинними моделями, що дозволить зменшити вплив шумових даних та підвищити чутливість до складних і малопоширених загроз.

Таким чином, результати дослідження підтверджують, що ймовірнісні нейронні мережі можуть стати важливим інструментом у сучасних системах виявлення вторгнень, однак їх ефективність значною мірою залежить від поєднання з іншими методами та від оптимізації структури мережі.

У статті [2] описано підхід, де ймовірнісну нейронну мережу PNN поєднано з алгоритмами вибору ознак для зменшення надлишкової та шумової інформації у вхідних даних. Автори стверджують, що застосування методів кореляційного аналізу та статистичної селекції параметрів мережевого трафіку дозволило не лише знизити обчислювальні витрати, а й підвищити точність розпізнавання атак класу R2L до 87%.

Також автори підкреслюють, що саме ретельна оптимізація вибору ознак є критичним фактором підвищення ефективності PNN, оскільки надмірна або шумова інформація може істотно знизити продуктивність мережі. Такий підхід демонструє перспективність у побудові адаптивних систем виявлення атак, здатних ефективно працювати з великими багатовимірними наборами даних у режимі реального часу.

Перспективним є інтегрування цього методу з алгоритмами вибору ознак або глибинними моделями, що дозволить зменшити вплив шумових даних та підвищити чутливість до складних і малопоширених загроз. Таким чином, результати дослідження підтверджують, що ймовірнісні нейронні мережі можуть стати важливим інструментом у сучасних системах виявлення вторгнень, однак їх ефективність значною мірою залежить від поєднання з іншими методами та від оптимізації структури мережі.

У роботі [3] описано підхід пов'язаний до застосування PNN у складі інтегрованих систем виявлення та запобігання вторгнень (IDS/IPS), що дозволяє підвищити ефективність моніторингу мережевого трафіку у реальному часі. Запропонована модель аналізувала дані, що характеризувалася високою неоднорідністю, дисбалансом класів та значними обсягами інформації. Експериментальні результати показали, що PNN досягає точності на рівні

90–95% при виявленні DoS та Botnet-атак, забезпечуючи швидке реагування на загрози. Авторами наведено порівняння мережі PNN з моделями Random Forest та SVM, PNN, що продемонструвала вищу швидкодію, простоту налаштування та здатність до адаптації під різні умови мережевого середовища. Разом з тим зберігалася проблема збільшеного споживання пам'яті при роботі із збільшенням обсягів датасету.

У дослідженні розглянуто використання методів попередньої обробки даних та відбору ознак, що дозволяє зменшити вплив шумової інформації та підвищити точність класифікації.

Автори запропонували адаптивну конфігурацію параметрів PNN для автоматичного підстроювання під змінні характеристики мережевого трафіку, що особливо важливо для великих корпоративних мереж з постійно змінюваним навантаженням. У перспективі зазначається можливість інтеграції PNN з іншими алгоритмами машинного навчання у гібридні системи, що поєднують швидку обробку з високою точністю, а також застосування розподілених обчислень для зменшення витрат пам'яті та прискорення обробки великих потоків даних.

У статті [4] запропоновано дворівневу систему, яка поєднує глибинне навчання та ймовірнісну нейронну мережу PNN, що дозволяє значно підвищити точність розпізнавання мережевих кібератак. На першому етапі згорткова нейронна мережа CNN застосовується для автоматичного вилучення релевантних ознак із сирого мережевого трафіку, після чого PNN виконує класифікацію атак, враховуючи багатовимірні характеристики даних. Такий підхід забезпечив точність понад 96% при виявленні складних атак, включаючи zero-day, які важко ідентифікувати традиційними методами.

Автори провели випробування на класичних наборах NSL-KDD та CICIDS2017, а також на власних корпоративних даних, що підтвердило практичну придатність моделі. Результати демонструють високий потенціал поєднання PNN із глибинними моделями для створення ефективних та адаптивних систем кіберзахисту.

Дослідження також відзначає переваги дворівневої архітектури: CNN зменшує розмірність даних і виділяє ключові ознаки, тоді як PNN забезпечує швидку адаптивну класифікацію з високою точністю.

Результати демонструють високий потенціал поєднання PNN із глибинними моделями для створення ефективних та адаптивних систем кіберзахисту. У перспективі автори пропонують інтегрувати модель у розподілені IDS/IPS та використовувати додаткові алгоритми оптимізації параметрів PNN для подальшого зменшення часу обробки та зниження витрат пам'яті при аналізі великих потоків мережевого трафіку.

Проведений аналіз науково-практичних досліджень [1–4] свідчить, що подальший розвиток застосування ймовірнісних нейронних мереж PNN у сфері кібербезпеки доцільно пов'язувати з кількома ключовими напрямами.

По-перше, актуальною є оптимізація вибору ознак у даних для зниження впливу шумової інформації та скорочення обчислювальних витрат.

По-друге, перспективним вважається поєднання PNN із глибинними архітектурами, такими як згорткові нейронні мережі, що підвищує здатність систем до розпізнавання складних та zero-day атак.

Додаткову увагу слід приділити питанням масштабованості та роботи з дисбалансом класів, адже саме ці фактори істотно впливають на якість виявлення рідкісних вторгнень.

4. ВИСНОВОКИ

Узагальнення результатів показує, що перспективними шляхами вдосконалення нейронної мережі типу PNN у задачах розпізнавання мережевих атак є їх інтеграція з методами глибинного навчання, удосконалення механізмів відбору ознак та підвищення стійкості до великих і різнорідних потоків даних. Такий підхід дозволить створити більш ефективні, адаптивні та надійні системи протидії кіберзагрозам.

Крім того, подальший розвиток PNN може бути спрямований на зменшення обчислювальної складності та оптимізацію використання пам'яті, що є критично важливим при роботі з високошвидкісним трафіком. Важливим напрямом є також комбінування PNN з іншими алгоритмами машинного навчання, такими як Random Forest чи SVM, що дає змогу компенсувати слабкі сторони кожного підходу та підвищити загальну ефективність системи. Комбінування методів сприяє формуванню стійких моделей, які здатні вчасно ідентифікувати кібератаки.

Список літератури

[1] Godfrey A., Daniel K., Robert A. Network Intrusion Detection and Prevention System Using Probabilistic Neural Networks. International Journal of Computer Science and Network Security. 2024. 24(5), 1–10. DOI: http://dx.doi.org/10.1155/2024/5775671

[2] Yanyan S., Gaoyuan L. , Boxiong Y. , Yong C., Zhenbao L. A feature selection algorithm for PNN optimized by binary PSO. Proceedings of the International Conference on Information Technology and Computer Science (IC-ITECHS) 2024. 33-38 DOI: https://doi.org/10.32664/ic-itechs.v5i1.1510

[3] Nadir O., Ahmed H., Ahmed I., Rasha M. A novel optimized probabilistic neural network approach for intrusion detection and categorization. Journal of King Saud University - Computer and Information Sciences. 2023. 176(30),1–7. DOI: https://doi.org/10.1016/j.aej.2023.03.093

[4] Al-Turaiki, I., & Altwaijry, N. A Convolutional Neural Network for Improved Anomaly-Based Intrusion Detection. Journal of King Saud University - Computer and Information Sciences. 2021. 215, 103137.. URL: https://www.researchgate.net/publication/352502419_A_Convolutional_Neural_Network_for_Improved_Anomaly-Based_Network_Intrusion_Detection