АНАЛІЗ ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ В КРИПТОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ

Нікітенко А.О., аспірант, andrii.nikitenko@donntu.edu.ua
ДВНЗ «Донецький національний технічний університет»,
м. Луцьк, Україна

В епоху безперервного експоненціального розвитку цифрових технологій та збільшення обсягів інформації постає питання щодо сучасного та надійного захисту даних, що передаються. Одним з основних способів захисту даних є їх шифрування. З підвищенням продуктивності вимірної техніки відзначається зростання ефективності методів криптоаналізу, тому виникла необхідність у застосуванні більш складних підходів до шифрування. Зокрема, у використанні такого перспективного підходу, як використання нейронних мереж для шифрування даних – нейрокриптографії. Погана вивченість криптостійкості нейромережевих методів шифрування робить актуальною задачу дослідження характерних особливостей та пошуку вразливостей нейромережевих криптографічних алгоритмів.

Нейронними мережами можна назвати сімейство статистичних моделей навчання, натхненних біологічними нейронними мережами, які використовуються для оцінки функції, яка може залежати від великої кількості вхідних даних і зазвичай невідома. Нейронна мережа належить до взаємозв'язку між нейронами на різних рівнях системи. Перший рівень має вхідні нейрони, які надсилають дані на другий рівень, а потім через синапси на третій рівень вихідних нейронів. Більш складна система матиме більше шарів нейронів. Синапси зберігають параметри, які називаються «вагами», які маніпулюють даними під час обчислення. Нейронна мережа зазвичай визначається трьома типами параметрів:

1) Схема взаємозв’язку: між різними шарами нейронів;

2) Процес навчання: для оновлення ваг взаємозв'язку;

3) Функція активації: для перетворення зваженого вхідного сигналу нейронів у вихідну активацію.

Типи нейронних мереж варіюються від тих, що мають лише один або два рівні односпрямованої логіки, до складних з кількома входами, багатьма спрямованими петлями та шарами зворотного зв’язку. Загалом ці системи використовують алгоритми у своєму програмуванні для визначення контролю та організації своєї функції. Більшість систем використовують «ваги» для зміни параметрів пропускної здатності та різноманітних з’єднань із нейронами. Нейронні мережі можуть бути автономними та навчатися за допомогою зовнішнього «вчителя» або навіть самонавчання [1].

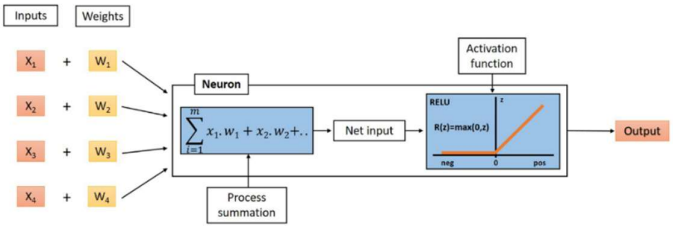

Рисунок 1. Схема навчання нейронної мережі
Джерело: [2]

Навчання нейронної мережі досягається шляхом багаторазового оновлення вагових значень під час зворотного розповсюдження, доки не буде знайдено поєднання значень, яке найкраще відображає вхідні дані на виході. Схему навчання нейронної мережі наведено на рис. 1.

Існують різні підходи, які засновані на нейронних мережах у криптографії, основні з них: стегоаналіз, генерація псевдовипадкових чисел, хешування, керування ключами, їх генерація та обмін [1].

Також існують інші способи захисту інформації до яких можна віднести використання нейронних мереж для виявлення різноманітних кіберзагроз та використання хаотичних нейронних мереж.

В одній із робіт було реалізовано хеш-функцію на основі простої структури хаотичної нейронної мережі. Її основними компонентами є ефективний хаотичний генератор та нейронна мережа, що складається з двох шарів: вхідного шару та вихідного шару. Отримані результати показують задовільну однорідність хеш-значень [8]. Таким чином, реалізована хаотична хеш-функція може використовуватися для забезпечення цілісності даних, аутентифікації та цифрового підпису.

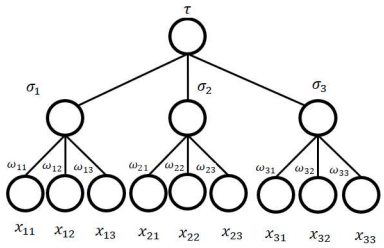

Рисунок 2. Приклад структури деревоподібної машини парності
Джерело: Авторський рисунок

Найпоширенішим сьогодні напрямком є дослідження взаємної синхронізації нейронних мереж. Нейронні мережі прямого поширення, які використовуються в криптографії для взаємної синхронізації, називаються деревоподібними машинами парності (ДМП) [3], які являють собою особливий вид багаторівневої штучної нейронної мережі прямого поширення. Приклад структури класичної ДМП наведено на рис. 2.

Суть ДМП полягає у поступовій взаємній синхронізації двох абонентів, у процесі якої відбувається оновлення та порівняння вагових коефіцієнтів. Синхронізація буде досягнута у разі, якщо вагові коефіцієнти двох ДМП дорівнюють один одному.

Після досягнення синхронізації вагові коефіцієнти можна використовувати як секретний ключ для симетричного алгоритму шифрування, наприклад AES, або як початкове значення для генератора псевдовипадкових чисел.

Головна перевага даного підходу полягає в тому, що ключ можна паралельно створити у двох кінцевих користувачів і його не потрібно передавати через мережу. Що значно зменшує ймовірність злому такого ключа [3].

У роботі [4] були проведені дослідження щодо вибору оптимальної конфігурації ДМП. Використовувалися 5 різних комбінацій співмножників K і N: 1 і 16, 2 і 8, 4 і 4, 8 і 2, 16 і 1. В результаті було визначено, що оптимальною конфігурацією ДМП, яка містить 16 зважених зв'язків, буде $K = 4$, $N = 4$. Якщо число прихованих нейронів пропорційно числу входів у кожного з них – це дає оптимальне співвідношення криптостійкості та швидкості синхронізації машин парності. Треба зауважити, що при великих значеннях L значно підвищується криптостійкість системи, але водночас збільшується обчислювальна складність та необхідний для синхронізації час.

В останні роки з'явилася достатня кількість модифікацій, спрямованих на зменшення часу синхронізації та підвищення криптостійкості ДМП.

У ДМП з використанням комплексних чисел [5] використовуються комплексні числа як ваги, водночас вхідні та вихідні дані не відрізняються від класичної ДМП. В результаті проведення експериментів автор стверджує про підвищення безпеки у порівнянні з класичною ДМП, але для завершення синхронізації потрібно багато часу.

У ДМП з використанням векторів [6] використовуються вектори як ваги, вхідні та вихідні дані. Автор показав, що час синхронізації ДМП з використанням векторів ідентична класичній ДМП та її безпеку можна збільшити з такою самою синаптичною глибиною, відповідно до кількості векторів.

Слід врахувати, що на відміну від ДМП з використанням векторів, у ДМП з використанням комплексних чисел розглядали лише геометричну атаку, і, отже, неясно, чи вона забезпечує достатній захист від більшості атак.

У ДМП з використанням не бінарних векторів [7] автор додає новий параметр M, який позначає мінімальне/максимальне значення кожного елемента вхідного вектора X. В результаті проведення експериментів автор стверджує, що наявність параметра M зменшує час синхронізації та чим швидше синхронізуються ДМП – тим безпечнішою є система. Однак прискорення процесу призводить до нерівномірного розподілу ваги ДМП.

Вищенаведені дослідження показують, що навіть сьогодні існують проблеми забезпечення захисту інформації з використанням штучних нейронних мереж, а саме забезпечення достатньої криптостійкості зі зберіганням часу синхронізації.

Література

1. Ms. Pranita P. Hadke and Mrs. Swati G. Kale, “Use of Neural Networks in Cryptography: A Review,” *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR’1*, 2016.

2. A. I. Georgevici and M. Terblanche, “Neural networks and deep learning: a brief introduction,” *Intensive Care Medicine*, vol. 45, no. 5. Springer Verlag, pp. 712–714, May 01, 2019. doi: 10.1007/s00134-019-05537-w.

3. Александров Никита, “Атаки на ваимную синхронизацию сетей в криптографии,” *Computer Science and Technologies*, pp. 15–22, 2020.

4. Ушаков А.К., “Выбор оптимальной конфигурации древовидных машин четности при их использовании для генерации секретного ключа информации,” *Научный журнал*, pp. 35–39, 2018.

5. T. Dong and T. Huang, “Neural Cryptography Based on Complex-Valued Neural Network,” *IEEE Trans Neural Netw Learn Syst*, vol. 31, no. 11, pp. 4999–5004, Nov. 2020, doi: 10.1109/TNNLS.2019.2955165.

6. S. Jeong, C. Park, D. Hong, C. Seo, and N. Jho, “Neural Cryptography Based on Generalized Tree Parity Machine for Real-Life Systems,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/6680782.

7. M. Stypiński and M. Niemiec, “Synchronization of Tree Parity Machines using non-binary input vectors,” Apr. 2021, [Online]. Available: http://arxiv.org/abs/2104.11105

8. N. Abdoun, S. El Assad, M. A. Taha, R. Assaf, O. Deforges and M. Khalil, "Secure Hash Algorithm based on Efficient Chaotic Neural Network," *2016 International Conference on Communications (COMM)*, 2016, pp. 405-410, doi: 10.1109/ICComm.2016.7528304.

Аннотація

З розвитком цифрових технологій поступово підвищується продуктивність обчислювальної техніки, що призводить до підвищення ефективності методів криптоаналізу, тому завдання захисту даних на сьогодні дуже актуальне, зокрема використання такого перспективного підходу, як використання нейронних мереж для шифрування даних – нейрокриптографії. У статті розглядається поняття нейронних мереж та існуючі на сьогоднішній день дослідження у цій галузі.

Ключові слова: нейронна мережа, нейрокриптографія, деревоподібні машини парності, захист даних.

Abstract

With the evolution of digital technologies, the efficiency of computing technology is progressively increasing, which leads to improving the performance of cryptanalysis methods, so the problem of data protection today is very relevant, in particular the use of such a perspective approach, as the use of neural networks for data encryption – neural cryptography. The paper covers the concept of neural networks and current researchers in this area.

Keywords: neural network, neural cryptography, tree parity machines, data security.