УДК 004.85

канд. техн. наук Макарчук О. М. ORCID: 0000-0002-0374-369X (ВІТІ)
Бовда В. Е. ORCID: 0000-0002-4072-771X (ВІТІ)
Остапчук В. М. (ВІТІ)

КОМБІНОВАНИЙ АЛГОРИТМ НАВЧАННЯ НЕЙРОННИХ МЕРЕЖ ПРЯМОГО ПОШИРЕННЯ

Суть навчання нейронних мереж прямого поширення полягає в мінімізації функції середньоквадратичної помилки виходу. Ця функція мультимодальна, тобто має декілька локальних мінімумів. Для пошуку мінімуму таких функцій найчастіше використовуються градієнтні і стохастичні методи, які не гарантують знаходження глобального мінімуму. У статті аналізуються градієнтний алгоритм зворотного поширення помилки і стохастичний метод рою частинок для навчання нейронних мереж прямого поширення, вказані їх переваги і недоліки. Пропонується об'єднати переваги обох методів у комбінованому алгоритмі.

Процес навчання за допомогою комбінованого алгоритму здійснюється в два етапи. На першому етапі стохастичний метод рою частинок проводить задану кількість епох навчання і визначає множину точок, в околиці яких можуть знаходитись точки локального мінімуму. На другому етапі градієнтний алгоритм зворотного поширення помилки знаходить локальний мінімум для кожної точки і вибирає з них оптимальний. Якщо задане значення середньоквадратичної помилки виходу не досягнуто, то етапи навчання повторюються.

Для оцінки ефективності запропонованого підходу до навчання нейронних мереж проведена серія порівняльних експериментів з використанням відомої бази даних розпізнавання комп'ютерних атак KDD Cup 1999 Data. В експериментах порівнювались результати навчання нейронної мережі прямого поширення для методу рою частинок, алгоритму зворотного поширення помилки і комбінованого алгоритму. Результати експериментів довели перевагу комбінованого алгоритму.

Ключові слова: *нейронна мережа, градієнтний метод, метод рою частинок, алгоритм зворотного поширення помилки.*

O. Makarchuk, V. Bovda. V. Ostapchuk Combined algorithm for training neural networks of direct propagation

The essence of learning neural networks of direct propagation is to minimize the function of the root mean square error of the output. This function is multimodal, ie it has several local minima. To find the minimum of such functions, gradient and stochastic methods are most often used, which do not guarantee finding the global minimum. The article analyzes the gradient algorithm of inverse error propagation and the stochastic method of particle swarm for training neural networks of direct propagation, their advantages and disadvantages are indicated. It is proposed to combine the advantages of both methods in a combined algorithm.

The learning process using a combined algorithm is carried out in two stages. At the first stage, the stochastic method of particle swarm conducts a given number of learning epochs and determines the set of points in the vicinity of which there may be points of local minimum. In the second stage, the gradient backpropagation algorithm finds the local minimum for each point and selects the optimal one. If the set value of the standard error of the output is not reached, the learning steps are repeated

To evaluate the effectiveness of the proposed approach to the training of neural networks, a series of comparative experiments using the well-known database of computer attack recognition KDD Cup 1999 Data. The experiments compared the results of training the direct propagation neural network for the particle swarm method, the inverse error propagation algorithm, and the combined algorithm. The experimental results proved the superiority of the combined algorithm.

Keywords: *neural networks, gradient method, particle swarm method, error backpropagation algorithm.*

Постановка завдання. Штучні нейронні мережі (ШНМ) знаходять все ширше застосування в різних сферах. Більшість з них являють собою багатошарові персептрони з прямим поширенням сигналу [1]. Важливим питанням практичної побудови ШНМ є її навчання, тобто адаптація до розв'язання конкретної задачі. ШНМ навчається шляхом зміни її параметрів. Розрізняють дві групи методів навчання: детерміністські та стохастичні.

Класичним детерміністським методом навчання є ітераційний алгоритм зворотного поширення помилки (АЗПП). В основі алгоритму лежить градієнтний метод найшвидшого спуску [2], який дозволяє мінімізувати середньоквадратичну помилку виходу (СПВ) за рахунок корекції ваг нейронів. Перевагою алгоритму є наявність добре розробленого математичного апарату, хороша збіжність до точки екстремуму і швидкодія.

Однак АЗПП має і ряд недоліків [2]:

функція обчислення СПВ є мультимодальною. Локальні мінімуми можуть суттєво відрізнятись значенням цільової функції. АЗПП знаходить точку локального мінімуму, який може бути не тільки не глобальним, але і менш ефективним за інші локальні мінімуми;

функція активації нейронів повинна мати похідну по всьому діапазону зміни аргументу, що не завжди виконується для деяких типів нейронних мереж;

алгоритм чутливий до початкової ініціалізації синаптичних ваг нейронів, оскільки вона визначає точку, з якої починається градієнтний спуск.

Стохастичні методи здійснюють псевдовипадкові зміни параметрів ШНМ з метою зменшення СПВ. Загальна ітераційна формула стохастичного пошуку має вигляд:

$$X_{k+1} = X_k + \zeta_k ,$$

де X_k і X_{k+1} – значення аргументів цільової функції на поточному і наступному кроці;

ζ_k – випадкова величина.

Існує декілька різновидів стохастичних методів, з яких при навчанні ШНМ найчастіше використовується метод рою частинок (МРЧ). Цей метод шукає точки екстремуму паралельно по всьому просторі визначення функції. Він також не гарантує знаходження глобального екстремуму, але з декількох локальних дозволяє вибрати кращий. Недоліком МРЧ є труднощі з налаштуванням параметрів рою, повільна збіжність до дна точки екстремуму і низька швидкодія.

Аналізуючи АЗПП і МРЧ, можна помітити, що вони певною мірою взаємно компенсують недоліки один одного. У зв'язку з вищевказаним сформульовано такі задачі дослідження:

1. Експериментально перевірити, наскільки суттєво локальні мінімуми функції обчислення СПВ відрізняються один від одного.

2. Запропонувати і дослідити спосіб підвищення ефективності навчання за рахунок комбінованого використання АЗПП і МРЧ.

Очевидно, другу задачу є сенс розв'язувати, коли локальні мінімуми можуть відрізнятися суттєво.

Аналіз останніх публікацій. Практичне використання нейронних мереж почалося після розробки АЗПП. З тих часів алгоритм не зазнав суттєвих змін і проблема локальних мінімумів залишилась [1].

Використання МРЧ для навчання ШНМ аналізувалось в [3–8]. Основні зусилля направлялись на обґрунтування методики налаштування параметрів рою для розв'язання конкретних задач. Зазначалось, що в цілому МРЧ дає кращі результати, ніж класичний АЗПП, так як пошук проводиться по всій області визначення цільової функції і декілька частинок рою можуть знаходитись в околиці локальних мінімумів.

Ідея комбінувати АЗПП і МРЧ в процесі навчання ШНМ досліджувалась в [6], але схема реалізації суттєво відрізнялась від запропонованої в статті. В даній схемі на кожній ітерації навчання спочатку працює АЗПП, а потім його результати корегуються МРЧ. На нашу думку, така схема не гарантує від попадання в неефективну точку локального мінімуму, оскільки околицю пошуку визначає АЗПП.

Метою статті є дослідження ефективності навчання ШНМ за допомогою запропонованого комбінованого алгоритму (КА), в якому поєднується робота АЗПП і МРЧ.

Виклад основного матеріалу. Процес навчання ШНМ за допомогою КА приведено на рис. 1. Він складається з двох етапів:

на першому етапі працює МРЧ. Він проводить N (визначається експериментально) епох навчання і формує множину точок-кандидатів на можливі точки мінімуму;

на другому етапі АЗПП досліджує точки-кандидати на мінімум. Процес продовжується до досягнення умов закінчення навчання. Якщо умови не досягнуті, то процес навчання повертається до першого етапу. МРЧ продовжує свою роботу з точки зупинки.

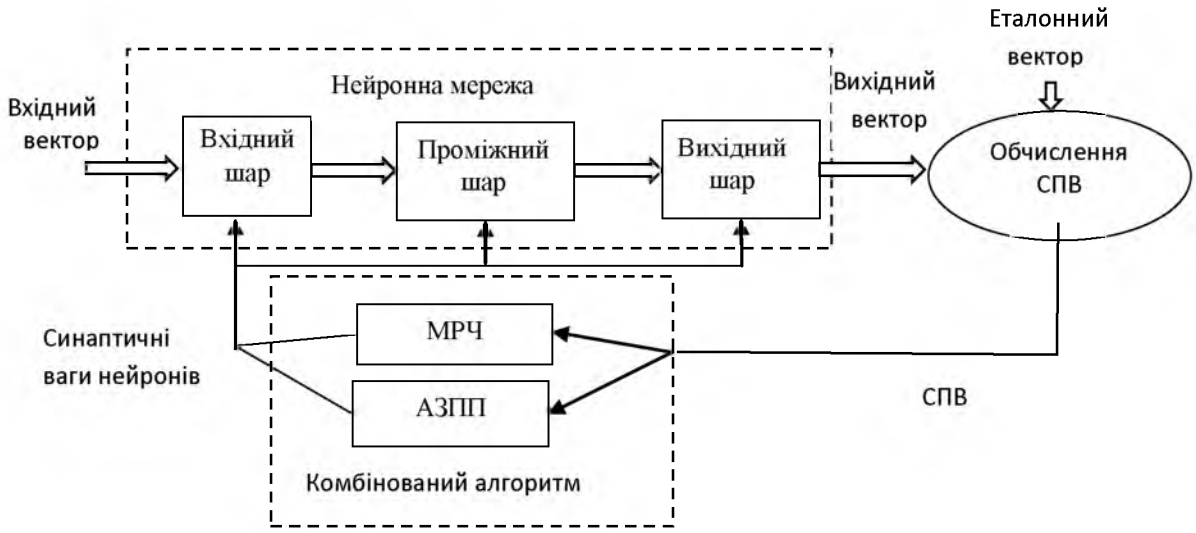

Рис. 1. Схема навчання нейронної мережі за допомогою комбінованого алгоритму

Існує декілька варіантів реалізації МРЧ [3]. Ідея методу була частково запозичена з досліджень поведінки скупчень живих істот (косяків риб, зграй птахів, натовпу людей тощо). Спочатку створюється сукупність (рій) частинок, які розкидані випадковим чином по всій області пошуку і кожна частинка має випадковий вектор швидкості. У кожній точці, де побувала частинка, розраховується значення цільової функції. При цьому кожна частинка запам'ятовує, яке (і де) краще значення цільової функції вона особисто знайшла. Також кожна частинка знає, де розташована точка, що є кращою серед усіх точок, які розвідали частинки. На кожній ітерації частинки коректують свою швидкість (модуль і напрямок), щоб з одного боку бути ближче до кращої точки, яку частинка знайшла сама (автори алгоритму назвали цей аспект поведінки «ностальгією»), і, в той же час, наблизитися до точки, яка в даний момент є глобально кращою. Через деяку кількість ітерацій частинки повинні зібратися поблизу найбільш хорошої точки, хоча можливо, що частина частинок залишиться десь у відносно непоганому локальному екстремумі, але головне, щоб хоча б одна частинка виявилася поблизу глобального екстремуму.

На кожному кроці координата частинки X_{k+1} обчислюється за формулою:

$$X_{k+1} = X_k + V_{k+1},$$

де X_k і X_{k+1} – значення аргументів цільової функції на поточному і наступному кроці;

V_{k+1} – швидкість частинки.

Аргументами є синаптичні ваги нейронів.

Існує декілька варіантів реалізації методу, які відрізняються методикою обчислення V_{k+1} [4–5]. В найбільш поширеному варіанті швидкість частинки обчислюється за формулою:

$$V_{k+1} = \omega_k V_k + \varphi_p r_p (p_k - X_k) + \varphi_g r_g (g_k - X_k),$$

де ω_k – коефіцієнт інерції;

φ_p, φ_g – вагові коефіцієнти;

r_p, r_g – випадкові числа в інтервалі (0, 1);

p_k – координата кращого рішення для даної частинки;

g_k – координата кращого рішення для рою.

Коефіцієнти ω_k, φ_p, φ_g підбираються експериментально для конкретної задачі.

Для розв'язання поставлених задач дослідження необхідно окреслити конкретну область використання ШНМ, визначити структуру нейронної мережі, реалізувати, навчити її і провести ряд експериментів для набору статистики. Для навчання ШНМ потрібно створити власну базу даних навчальних і тестових прикладів або вибрати одну з публічних баз.

Дослідження проводились на базі даних KDD Cup 1999 Data для розпізнавання комп'ютерних атак [9]. Вибір обумовлено актуальністю дослідження засобів протидії комп'ютерним атакам і доступністю цієї бази даних для навчання ШНМ.

База даних KDD Cup 1999 Data містить відомості про комп'ютерні атаки різних типів (DOS, R2l, U2R, Probing). База містить близько 5 000 000 записів. Кожен запис в цій базі є образом мережевого з'єднання. З'єднання – послідовність TCP-пакетів за деякий кінцевий час, протягом якого дані передаються від IP-адреси джерела на IP-адресу приймача (і в зворотному напрямку), використовуючи деякий протокол.

Окремий запис містить 41 параметр мережевого трафіку та промаркований як «атака» або «не атака». Наприклад, перший параметр визначає тривалість з'єднання, другий – вказує протокол, що використовується, третій – цільову службу і т. д.

Нейронна мережа складається зі вхідного шару (41 нейрон по числу вхідних параметрів), проміжного шару (16 нейронів згідно з рекомендаціями в [8]), вихідного шару (2 нейрони). Один нейрон класифікує наявність атаки, інший – відсутність атаки. Для навчання нейронної мережі випадково вибирались навчальні та тестові приклади стосовно DOS-атак.

Перша серія експериментів з використанням АЗПП проводилась з метою визначити, наскільки суттєво відрізняються точки локального мінімуму за значенням СПВ. Експерименти відрізнялись початковою ініціалізацією ваг нейронів і закінчувались досягненням точки локального мінімуму. Недоліком підходу є те, що на кожному кроці не враховується інформація про попередні кроки. Експерименти довели, що АЗПП в процесі навчання може зупинятись в локальних точках мінімуму СПВ, які суттєво (на порядок і більше) відрізняються за ефективністю. Тому використання пошуку на множині локальних мінімумів у процесі навчання має сенс.

У другій серії експериментів визначалась середня кількість оброблених прикладів навчання для досягнення заданої СПВ кожним з вищезгаданих методів навчання. Результати експериментів приведені в таблиці 1.

Таблиця 1

Середньоквадратична помилка виходу	**Середня кількість оброблених прикладів**		
	АЗПП	**МРЧ**	**КА**
0,25	128	111	87
0,1	322	236	211
0,05	745	608	502
0,025	1452	1132	880
0,01	2720	2218	1873

Аналізуючи дані таблиці, можна відмітити, що КА для навчання потрібно менше еталонних прикладів, ніж його конкурентам. Ця перевага має суттєве значення, коли база еталонних прикладів обмежена. Зі зменшенням кількості оброблених прикладів зменшується і тривалість навчання.

Наступна серія експериментів проводилась з метою оцінки ефективності КА порівняно з АЗПП і МРЧ. Кожний експеримент повторювався тричі з однаковою початковою ініціалізацією ваг нейронів, але з різними методами навчання. Кожний повтор закінчувався по досягненню заданої кількості епох. В експерименті визначався кращий метод навчання. Результати показали, що АЗПП був кращим за показником мінімуму СПВ в 19 % експериментів, МРЧ – в 32 % і КА – в 49 %.

Тестування навчених досліджуваними методами ШНМ показало, що КА забезпечує також меншу (на 33 % порівняно з АЗПП і 24 % порівняно з МРЧ) ймовірність хибного розпізнавання DOS-атаки.

Висновок. Таким чином, запропонований алгоритм навчання ШНМ об'єднує переваги градієнтного АЗРП і стохастичного МРЧ та дозволяє скоротити кількість навчальних прикладів для досягнення заданої СПВ. Пропонується використовувати його переваги при побудові систем захисту від комп'ютерних атак на основі ШНМ.

В подальших дослідженнях планується оцінити ефективність запропонованого підходу до навчання інших типів ШНМ, зокрема рекурентних.

ЛІТЕРАТУРА

1. Хайкин С. Нейронные сети: полный курс. 2-е изд., испр. Пер. с англ. Москва: ООО «И. Д. Вильямс», 2006. 1104 с.

2. Уайлд, Д. Дж. Методы поиска экстремума. Москва: Главная редакция физико-математической литературы издательства «Наука», 2017. 268 с.

3. Карпенко А. П., Селиверстов Е. Ю. Обзор методов роя частиц для задачи глобальной оптимизации (Particle Swarm Optimization) // Наука и образование: электронное научно-техническое издание. 2009. № 3. URL: http://technomag.edu.ru/doc/116072.html.

4. Е. В. Пальчевский, О. И. Христодуло. Разработка импульсной нейронной сети с возможностью скоростного обучения для нейтрализации DDoS-атак //Программные продукты и системы. 2019. Том 32, № 4. С. 613–627.

5. Воробьева Ю. Н., Катасева Д. В., Катасев А. С., Кирпичников А. П. Нейросетевая модель выявления DDoS-атак // Вестник технологического университетата. 2018. Т. 21. № 2. С. 94–98.

6. Частикова В. А., Власов К. А., Картамышев Д. А. Обнаружение ddos-атак на основе нейронных сетей с применением метода роя частиц в качестве алгоритма обучения // Фундаментальные исследования 2014. № 8. С. 829–832.

7. Титюнников А. В., Кароль А. Д., Бессчетнов А. В. Применение метода роя частиц в качестве обучения нейронных сетей // CyberLeninka: научная электронная библиотека. URL: https://cyberleninka.ru/article/n/primenenie-metoda-roya-chastits-v-kachestve-obucheniya-neyronnyh-setey/viewer.

8. SaiedA., Overill R., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Net-works. Neurocomputing, 2016, vol. 172, pp. 385–393.

9. KDD Cup 1999 Data // UCI Knowledge Discovery in Databases Archive. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.