УДК 681.3.06

І.А. Терейковський

Київський національний університет будівництва і архітектури, Київ

ВИКОРИСТАННЯ НЕЙРОННОЇ МЕРЕЖІ З РАДІАЛЬНИМИ БАЗИСНИМИ ФУНКЦІЯМИ В ЗАДАЧАХ ДІАГНОСТИКИ СТАНУ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Визначено доцільності використання класичної нейронної мережі з радіальною базисною функцією для розв'язання задач діагностики стану захищеності програмного забезпечення. Розглянуто методику побудови мережі, проведено її верифікацію та проаналізовано обчислювальні обмеження. Обґрунтовано можливі сфери використання мережі.

Ключові слова: діагностика захисту, захист інформації, нейронна мережа з радіальними базисними функціями

Постановка проблеми

За останні декілька років відчутно зріс інтерес до застосування нейронних мереж (НМ) в засобах технічного контролю та діагностики. Нейронні мережі переважно використовуються в якості управляючого елемента в блоках розпізнавання стану технічних систем. Доведено, що ефективність застосування багато в чому залежить від обчислювальних можливостей НМ, які в свою чергу визначаються їх архітектурою. Однією із перспективних архітектур визнано мережу з радіальними базисними функціями (РБФ) [1;2]. Очевидно, що дана мережа має певні перспективи і в засобах діагностики параметрів захисту програмного забезпечення комп'ютерних систем. Визначення цих перспектив і є основною проблемою даної статті. Проблема безпосередньо пов'язана з таким важливим науково-практичним завданням, як забезпечення надійності функціонування розподілених комп'ютерних систем та мереж.

Аналіз останніх досліджень і публікацій

Використання НМ з РБФ базується на посиланні про те, що для підвищення ймовірності лінійного поділу образів на класи, необхідно розмістити ці образи в просторі високої розмірності деяким нелінійним чином [3]. В найбільш простій формі РБФ являє собою НМ, що складається із трьох шарів: вхідного, схованого та вихідного. Спрощена схема РБФ з одним нейроном у вихідному шарі показана на рис.1. В задачу вхідного шару входить розподіл вхідних даних по нейронам схованого шару НМ. В схованому шарі містяться нейрони з радіально-симетричною функцією активації. Кожен із схованих нейронів призначений для зберігання окремого еталонного образу, який відповідає окремому класу. Досить часто кількість нейронів в схованому шарі більша кількості вхідних нейронів.

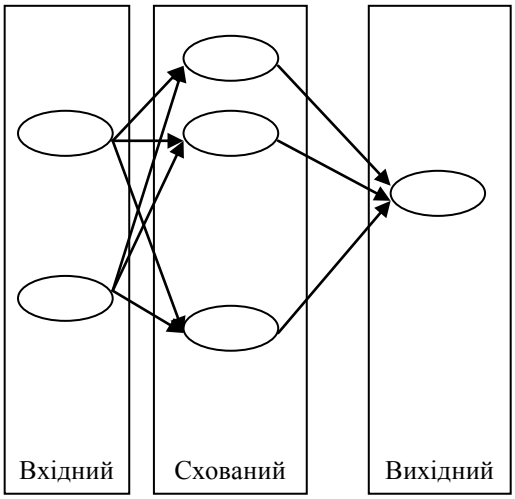

Рис.1. Спрощена схема РБФ

Для j-го нейрону в схованому шарі сумарний вхідний сигнал (net) від деякого вхідного вектора x розраховується як евклідова норма:

$$net_j = \sqrt{\sum_{i=1}^{N} (x_i - w_{ij})^2}\,, \qquad (1)$$

де x_i – i-та компонента вхідного вектору x; w_{ij} – ваговий коефіцієнт j-го схованого нейрону з і-тим вхідним нейроном; N – кількість вхідних нейронів.

В якості функції активації φ для нейронів в схованому шарі типовим є використання функції Гаусса:

$$\varphi_j(net) = exp\left(-\frac{1}{2\sigma}\sum_{i=1}^{N}(c_i - x_i)^2\right), \qquad (2)$$

де $\varphi_j(net)$ – функція активації j-го нейрону проміжного шару; net – сумарний вхідний сигнал;

x – вхідний вектор; c – центр функції Гаусса; σ – радіус функції Гаусса.

Після нелінійного перетворення сигнали від нейронів схованого шару потрапляють у вихідний шар нейронів, що мають лінійні функції активації. Розрахунок сумарного вхідного сигналу для будь-якого нейрону вихідного шару проводиться відповідно до (1). Зазначимо, що сукупність значень активностей всіх схованих нейронів визначає вектор, на який відображається вхідний вектор:

$$\varphi(x) = \left| \varphi_1(x), \varphi_2(x), ..., \varphi_M(x) \right|, \quad (3)$$

де x – вхідний вектор; $\varphi(x)$ – вихідний вектор; $\varphi_i(x)$ – компонента вихідного вектору; пов'язана з i-тим схованим нейроном; M – кількість схованих нейронів.

Оскільки функція активації нейронів схованого шару – $\varphi_i(x)$ є нелінійною, то для моделювання будь-якої вхідної інформації достатньо одного проміжного шару з достатньо великою кількістю нейронів. Загальну кількість синаптичних зв'язків (Z_Σ) мережі РБФ можна розрахувати так:

$$Z_\Sigma = Z_1 + Z_2, \quad (4)$$

$$Z_1 = N \times M, \quad (5)$$

$$Z_2 = M \times K, \quad (6)$$

де Z_1 – кількість синаптичних зв'язків схованих нейронів; Z_2 – кількість синаптичних зв'язків вихідних нейронів.

Навчання РБФ проводиться поетапно. На першому етапі розраховують кількість нейронів в схованому шарі та коефіцієнти (центр і радіус функції Гаусса) для функцій активації нейронів схованого шару. Для розрахунку центра функції Гаусса рекомендується використовувати метод "К-середніх" або метод навчання мережі Кохонена – "переможець забирає все" [3]. Наступним етапом навчання є розрахунок радіусів функцій Гаусса. Для цього можна використовувати метод "К найближчих сусідів". Після розрахунку параметрів функції Гаусса, які за своєю суттю представляють вагові коефіцієнти нейронів схованого шару необхідно визначити вагові коефіцієнти нейронів вихідного шару. У роботі [3] визначення пропонується реалізувати методом "навчання з вчителем" за правилом Відроу-Хофа:

$$\Delta w_j = \eta \times net_j \times \delta_j, \quad (7)$$

де Δw_j – корекція вагових коефіцієнтів j-го нейрону вихідного шару; η – норма навчання; δ_j – помилка вихідного сигналу j-го вихідного нейрону; net_j – сумарний вхідний сигнал j-го вихідного нейрону.

У свою чергу помилка вихідного сигналу для j-го нейрону розраховується так:

$$\delta_j = w_j^f - w_j^o, \quad (8)$$

де w_{fj} – фактичний вихід; w_{oj} – очікуваний вихід j-го вихідного нейрону.

У багатьох випадках при розрахунках (7), (8) вважається, що всі зв'язки вихідних нейронів потребують однакової величини корекції вагових коефіцієнтів. Тому для РБФ з одним вихідним нейроном (7), (8) можна переписати так:

$$\Delta w_j = \frac{\eta \times net \times \delta}{M}, \quad (9)$$

$$\delta = w^f - w^j, \quad (10)$$

де M – кількість схованих нейронів; w_f – фактичний вихід; w_o – очікуваний вихід мережі; net – сумарний вхідний сигнал вихідного нейрону.

Використання (7) – (10) вказує на ітераційний процес навчання. При цьому знайти теоретичну залежність оптимальної кількості ітерацій навчання від параметрів РБФ автору не вдалось. Водночас кількість ітерацій i, схованих M, вхідних N та вихідних нейронів K безпосередньо впливають на тривалість навчання T, яка є однією з головних характеристик НМ:

$$T \approx i \times K \times N \times M. \quad (11)$$

Після навчання рекомендується перевірити якість розпізнавання РБФ на тестових прикладах, що не входять до навчальної вибірки. Якщо якість незадовільна, то проводиться корегування вагових коефіцієнтів, спочатку схованого, а потім вихідного шару нейронів. Проведений аналіз математичного забезпечення та функціональних особливостей мережі РБФ дає змогу перейти до визначення:

– переваг та недоліків її застосування в задачах захисту інформації щодо інших типів НМ;

– конкретних напрямків застосування для розв'язання задач захисту інформації.

Формулювання мети статті

Оцінити можливості використання мережі РБФ для розв'язання задач діагностики параметрів захисту програмного забезпечення комп'ютерних систем.

Виклад основного матеріалу дослідження

На першому етапі досліджень було проведено числові експерименти спрямовані на верифікацію моделі РБФ (1) – (10) та на визначення оптимальної кількості навчальних ітерацій, яка безпосередньо впливає на обчислювальну ефективність мережі. Експерименти проводились за допомогою двох програм, створених автором. У першій серії експериментів було проведено апроксимацію функції $y = 0{,}5x + 2x^2 - x^3$. Вибір функції зумовлений тим, що саме вона представлена як

приклад використання РБФ в [3]. Як і в [3] застосована мережа РБФ та навчальні приклади з такими параметрами: радіус функції Гаусса σ=0,5, норма навчання η=0,1, кількість схованих нейронів – 9, кількість вхідних та вихідних нейронів – 1, кількість навчальних прикладів, в яких $x \in [-1,1]$ дорівнює 30, центри функцій Гаусса знаходяться в точках 0.88889, 0.66667, 0.44444, 0.22222, 0, 0.222222, 0.444444, 0.666667, 0.888889. Фрагмент розрахованих показників виходу РБФ показаний в табл. 1.

Таблиця 1

Величина виходу РБФ для різної кількості навчальних ітерацій

№	Кількість ітерацій			Фактичне значення функції
	1	100	1000	
1	-0,8365	1,1255	2,0503	2,5
2	-0,9034	1,8632	1,5626	1,392
3	-0,8655	1,4190	0,9246	0,636
4	-0,6997	0,4050	0,3194	0,184
5	-0,4083	-0,0140	-0,0752	-0,012

Аналіз даних табл.1 вказує на те, що як максимальна, так і середня відносна помилка виходу РБФ стабілізується при кількості навчальних ітерацій понад 100. Збільшення кількості навчальних ітерацій не зменшує величин цих помилок, хоча й значно впливає на величини вагових коефіцієнтів вихідного нейрону. Для збільшення наочності отриманих результатів на рис. 2 показано графік функцій апроксимованої РБФ, яка навчалась 1000 ітерацій та фактичний графік функції $y = 0{,}5x + 2x^2 - x^3$.

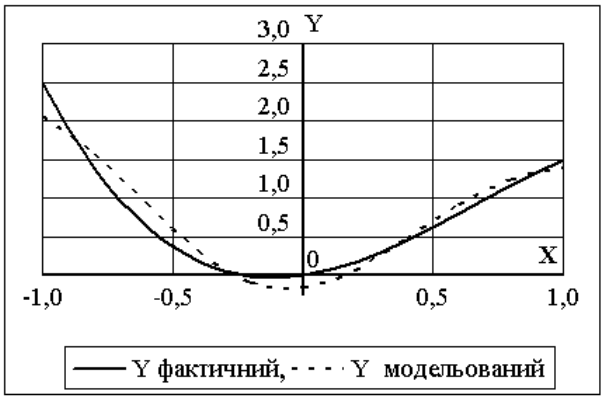

Рис.2. Фактичний та модельований РБФ графік функції

Спостерігається близкість змодельованого та фактичного графіків, що є підтвердженням точності моделі. Крім того проведені експерименти з метою апроксимації РБФ лінійних та квадратичних функцій, що залежать від двох та трьох змінних. Навчання моделі проводилось в діапазоні навчальних прикладів від 10 до 100 при кількості схованих нейронів від 10 до 20. Модель показала достатню точність апроксимації лінійних функцій після 100 навчальних ітерацій, квадратичних функцій – після 1000 ітерацій. При цьому відносна середня похибка апроксимації знаходилась в межах 1%, а відносна максимальна похибка – в межах 3%. Таким чином, оптимальна кількість навчальних ітерацій безпосередньо залежить від кількості вхідних параметрів та виду модельованої функції. При цьому обчислювальна складність навчальної ітерації пропорційно залежить від кількості схованих нейронів. З цієї причини, в складних випадках навчання РБФ може потребувати значної кількості обчислень, що суперечить відомим теоретичним висновкам [3]. Результати експериментів та висновки [2; 3] дають змогу вказати на деякі переваги мережі РБФ у порівнянні з багатошаровим перспетроном, обраним в якості порівняльного базису застосування інших типів НМ в задачах захисту. По-перше, РБФ дає змогу моделювати довільну функцію за допомогою всього одного проміжного шару, що деякою мірою спрощує архітектуру мережі. По-друге, навчання проміжного та вихідного шару нейронів РБФ можна проводити за допомогою достатньо апробованих методів лінійного моделювання. Ще однією перевагою РБФ є проста програмна реалізація, яка досягається за рахунок більш простої методики навчання. У той же час результати порівняння обчислювальних можливостей РБФ та багатошарового перспетрону наведені в роботах [1; 2] вказують на те, що для моделювання складних функції мережа РБФ потребує дещо більшого числа нейронів. Це пояснюється тим, що в процесі апроксимації даних біля будь-якої точки в перспетроні задіяні всі сховані нейрони, а в РБФ задіяні тільки найближчі. Тому для РБФ кількість нейронів, необхідних для апроксимації функції з заданою точністю зростає експоненційно зі зростанням розмірності вхідного сигналу. Як наслідок, програмна реалізація РБФ буде проводити класифікацію довше, витрачати більше ресурсів, але навчатись швидше, ніж програмна реалізація багатошарового перспетрону. Таким чином застосування РБФ в задачах захисту інформації має полягати у проведенні оперативного аналізу інформації, у процесі якого питання швидкості приблизного визначення класів превалюють над задачами точності класифікації. У традиційних сферах застосування досить часто такий аналіз проводять з метою приблизної оцінки архітектури перспетрону, для більш точного розв'язування

аналогічної задачі. Відповідна мета може ставитись перед РБФ і у сфері захисту інформації.

Також можна зробити висновок про те, що мережу РБФ доцільно використовувати в тих засобах захисту, які базуються на аналізі множини взаємокорельованих дискретних параметрів. До таких засобів захисту належать системи розпізнавання атак, системи розпізнавання вразливостей, антивіруси та антикейлогери. Можливі вхідні параметри мережі РБФ для цих засобів захисту наведені в табл. 2.

Таблиця 2

Вхідні параметри мережі РБФ в засобах захисту

Назва засобів захисту	Вхідні параметри
Система розпізнавання атак	Параметри мережевих запитів та подій в комп'ютерній системі: вхід/вихід користувачів, кількість процесів, доступ до файлів, часові інтервали запитів до об'єктів комп'ютерної системи.
Система розпізнавання вразливостей	Параметри настройок комп'ютерної системи: кількість користувачів, привілеї користувачів, параметри доступу до об'єктів комп'ютерної системи, кількість і номенклатура відкритих портів, запущені мережеві служби, параметри адміністративних настройок служб DCOM/COM+
Антивіруси, антикейлогери	Параметри подій в комп'ютерній системі: кількість і номенклатура запущених програм та процесів, доступ процесів до файлів, спроби доступу до мережевих служб, спроби зміни файлів, які виконуються, доступ до API операційної системи. Параметри сигнатур програмного коду, що відповідають за саморозмноження та деструктивні дії: звернення до файлових об'єктів, оператори перехвату помилкових ситуацій, функції для роботи з мережевими ресурсами

На погляд автора основними обмеженнями використання мережі РБФ у сфері захисту є:

- недостатньо вивчені можливості в області узагальнення та формування нових знань;
- неможливість самостійного навчання в процесі практичної експлуатації;

На практиці вказані обмеження можуть негативно вплинути на можливості діагностування нових видів атак або невідомих вразливостей. Для вирішення цієї проблеми слід розробити методику формування якісної першочергової навчальної вибірки та провести дослідження в напрямку розвитку такої характеристики РБФ, як узагальнення подібної вхідної інформації. Крім того слід провести дослідження в напрямку комбінованого використання РБФ з іншими видами НМ.

Висновки

Загальними передумовами застосування мережі РБФ є: простота структури, яка зумовлює простоту програмної реалізації та висока швидкість навчання.

До загальних обмежень мережі РБФ належать: обмеженість обчислювальних можливостей у порівнянні з багатошаровим перспетроном, велика кількість емпіричних параметрів, що використовуються при навчанні схованого шару та погана екстраполяція результатів за межами області навчальних даних. Тому в навчальній виборці повинен бути представлений практично весь діапазон можливих вхідних даних.

Застосування РБФ доцільне в задачах захисту інформації за необхідності проведення швидкого оперативного аналізу даних з метою подальшого використання результатів в більш потужних системах. Наприклад, за допомогою лабораторного аналізу РБФ сигнатур комп'ютерних вірусів можна приблизно визначити характеристики багатошарового перспетрону, призначеного для використання в блоці розпізнавання антивірусних засобів.

Список літератури

1. Терейковський І.А. Використання нейронних мереж при розпізнаванні макровірусів // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні-Вип. 2 (13), - 2006, С.176-183

2. Огарок А. Виртуальные войны. Искусственный интеллект на защите от вирусов и программных закладок / А. Огарок, Д. Комашинский, Д. Школьников // Конфидент. – 2003. – №2 (50). – С. 64–69, 97.

3. Ежов А. А. Нейрокомпьютинг и его применения в экономике и бизнесе / А. А. Ежов, С. А. Шумский. – М. : МИФИ, 1998. – 224 с.

4. Каллан Р. Основные концепции нейронных сетей / Каллан Р. ; пер. с англ. А. Г. Сивака. – М. : Вильямс, 2003. – 288 с.

Стаття надійшла до редколегії:15.11.2010

Рецензент: д-р техн. наук, проф. С.В. Цюцюра, Київський національний університет будівництва і архітектури, Київ.