В подальшому авторами планується аналіз інших відомих протоколів сліпого підпису за критерієм анонімності.

Література: ***1.*** *Молдовян Н. А. Новые протоколы слепой подписи / Н. А. Молдовян, Е. В. Морозова, А. А. Костин, С. Е. Доронин // Программные продукты и системы. – 2008. – № 4. – С. 161–164.* ***2.*** *Молдовян Н. А. Новые протоколы слепой подписи / Н. А. Молдовян, П. А. Молдован // Безопасность информационных технологий. – М.:МИФИ. – 2007. – № 3. – С. 17-21.* ***3.*** *Ростовцев А. Г. Подпись "вслепую" на эллиптической кривой для электронных денег / А. Г. Ростовцев // Проблемы информационной безопасности. Компьютерные системы. – 2000. - № 1. – С. 40–45.* ***4.*** *Костин А. А. О реализации протоколов слепой подписи и коллективной подписи на основе стандартов цифровой подписи / Костин А. А, Молдован Н. А., Фаль А. М. //Материалы V1 Санкт-Петербургской межрегиональной конференции «Информационная безопасность России (ИБРР-2009). Санкт-Петербург, 28–30 октября. СПб.: СПОИСУ, 2009, с. 111.*

УДК 681.3.06

ВДОСКОНАЛЕННЯ АЛГОРИТМУ НАВЧАННЯ БАГАТОШАРОВОГО ПЕРСПЕТРОНУ, ПРИЗНАЧЕНОГО ДЛЯ РОЗПІЗНАВАННЯ МЕРЕЖЕВИХ АТАК

Ігор Терейковський
Національний технічний університет України "КПІ"

Анотація: **Обґрунтована необхідність та проведено вдосконалення математичного забезпечення алгоритму навчання багатошарового перспетрону, призначеного для розпізнавання мережевих атак на комп'ютерні системи та мережі.**
Summary: **The necessity and carried out the improvement of mathematics learning algorithm for multilayer perspetron designed to detect network attacks on computer systems and networks.**
Ключові слова: **Багатошаровий перспетрон, захист інформації, розпізнавання мережевих атак.**

Практичний досвід та аналіз публікацій [1 – 3] вказують на те, що в останнє десятиліття розпізнавання атак на інформацію комп'ютерних систем та мереж (КСМ) є однією із найбільш важливих та актуальних проблем в галузі захисту інформації. Складність проблеми обумовлена багатофакторною динамікою функціонування сучасних КСМ, великою різноваріантністю відомих та постійним виникненням нових видів атак. Тому розпізнати атаку за допомогою методів, які базуються на класичному аналізі статистики функціональних параметрів КСМ, в багатьох випадках практично неможливо. Як наслідок знаходять застосування різноманітні альтернативні математичні теорії, в тому числі і теорія штучних нейронних мереж (НМ), що довела свою ефективність в задачах аналізу багатопараметричних зашумлених даних. Однак, не зважаючи на окремі вдалі спроби та загальновизнану перспективність систем розпізнавання атак на базі НМ їх достовірність залишається не достатньою. Цим визначається актуальність досліджень щодо застосування НМ для розпізнавання атак на КСМ.

І Аналіз нейромережевих методів розпізнавання атак

Відповідно до [1 – 3] суть загальнопоширених нейромережевих методів розпізнавання атак полягає у визначенні значимих відмінностей характеристик поточного функціонування КСМ від характеристик функціонування в нормальних умовах. Відомі вдалі спроби розпізнавати за допомогою НМ віддалені мережеві атаки, комп'ютерні віруси, приховані факти передачі зашифрованих даних, спам-листи електронної пошти. При цьому типовий алгоритм застосування НМ в системах розпізнавання атак складається з наступних етапів:

– Визначається номенклатура фізичних параметрів підзахисного об'єкта, що відповідають вхідним параметрам НМ;
– проводиться попередня обробка та кодування фізичних параметрів з метою їх адаптації до НМ;
– визначається номенклатура вихідних параметрів НМ;
– розробляється система кодування вихідних параметрів НМ;
– визначається оптимальний тип архітектури НМ;
– оптимізуються параметри архітектури НМ;

– формуються навчальні та тестові вибірки;
– проводиться навчання та тестування НМ;
– уточняються оптимальні параметри архітектури НМ.

Розглянемо застосування цього алгоритму в описаних системах розпізнавання атак.

Як вхідні параметри НМ використовуються параметри, що характеризують функціонування конкретного підзахисного об'єкта. Наприклад, для розпізнавання мережевих атак в [2] використано такі параметри TCP-з'єднання як:

– загальна кількість байт, переданих з'єднанням в обох напрямках;
– середня, максимальна та мінімальна кількість байт, переданих одним пакетом в обох напрямках;
– дисперсія кількості байт для послідовності пакетів з'єднання, також в обох напрямках;
– кількість пакетів, що несуть службові поля протоколу TCP: URG, PUSH та RST в обох напрямках;
– індикатори нормального відкриття та нормального закриття з'єднання;
– тривалість з'єднання в мілісекундах;
– кількість з'єднань на сокеті даного сервісу на момент відкриття даного з'єднання.

В найпростішому випадку попередня обробка фізичних параметрів полягала в їх нормалізації відповідно до виразу

$$\bar{x}_i = \frac{x_i - x_{min}}{x_{max} - x_{min}}, \tag{1}$$

де $x_i, \bar{x}_i$ – реальні та приведені величини *i*-го параметру, x_{max}, x_{min} – максимальна та мінімальна величина параметра.

Описана найпростіша методика попередньої обробки має ряд недоліків: відсутня фільтрація неінформативних параметрів, неможливість реалізації в реальному масштабі часу, приведені величини параметру належать діапазону від 0 до 1. Виправити більшість недоліків можливо використовуючи результати [4 – 6]. Невирішеною залишається лише задача визначення малоінформативних параметрів [4, 7]. Також не до кінця вирішені задачі визначення кількості вихідних параметрів та кодування величин цих параметрів. Однак в багатьох випадках використовують:

– один вихід, величина якого відповідає ймовірності реалізації атаки;
– декілька виходів, кожен з яких відповідає ймовірності певного стану КСМ.

Для розпізнавання мережевих атак, комп'ютерних вірусів та передачі зашифрованих даних використано НМ типу багатошарового перспетрону (БШП). Також в антивірусних системах, як і в системах розпізнавання спаму використано НМ типу карти Кохонена. При цьому відповідно до аналізу [3 – 6] за своїми обчислювальними можливостями карта Кохонена значно поступається БШП. Тому, якщо не брати до уваги можливості самонавчання та візуалізації вихідної інформації, БШП має вищий приорітет, що підтверджується в [3] .

Крім кількості вхідних та вихідних нейронів до основних параметрів БШП відносяться:

– кількість схованих шарів та кількість нейронів у кожному схованому шарі;
– тип та параметри функцій активації;
– тип та параметри методу навчання.

Зазначимо, що на сьогодні теоретичні аспекти задачі визначення кількості схованих шарів та нейронів у схованому шарі вирішені далеко не повністю. Навіть в підходах до такого визначення існують деякі протиріччя. Так в [6] використовується принцип мінімізації кількості синаптичних зв'язків, необхідних для навчання мережі на заданій множині прикладів. Вказаний принцип суперечить [7], де стверджується, що редукція розмірів мережі не призводить до зростання її узагальнюючих можливостей. При цьому в більшості робіт, присвячених розпізнаванню атак, методика розрахунку структури БШП не обґрунтована. Водночас зазначається, що використовуються сигмоїдальні активаційні функція та метод навчання на основі алгоритму зворотнього поширення помилки. Даний алгоритм навчання спрямований на мінімізацію функції помилки

$$\varepsilon(W) \to min, \tag{2}$$

де ε – загальна помилка навчання БШП, W – матриця вагових коефіцієнтів синаптичних зв'язків.

Як правило, використовується середньоквадратичний функціонал помилки виду

$$\varepsilon^2(W) = \left(y_i - y_i^r\right)^2, \tag{3}$$

де y_i, y_i^r – очікуваний та реальний вихідний сигнал *i*-го вихідного нейрону БШП.

В [4] зазначається, що використання (3) може привести до незадовільних результатів на навчальних вибірках з так званими "важкими хвостами". В цих випадках рекомендуються цільові функціонали типу логістичної функції Велша, функцій Хубера, Талвара та Хемпела.

Для пошуку мінімуму загальної помилки нейронної мережі найчастіше використовується метод градієнтного спуску. Критика алгоритму зворотнього поширення помилки в основному пов'язана з низькою швидкістю навчання, можливим паралічем НМ та можливість хибного сприйняття локального мінімуму як глобального. Крім того, автором виявлено особливість, що проявляється при вирішенні НМ прямого поширення сигналу задачі апроксимації заданої табличної функції, мінімальні та максимальні значення якої значно відрізняються між собою

$$y = f(x),\ \exists\ y_{max} >> y_{min}\,. \tag{4}$$

В цьому випадку використання (2), (3) призводить до різкого зростання відносної помилки навчання в точках, що знаходяться в області y_{min}, при задовільних значеннях помилки для всіх інших точок навчальної вибірки та задовільній загальній помилці БШП. Проведені за допомогою емулятора НМ NeuroPro чисельні експерименти підтвердили існування вказаної особливості. Для прикладу на рис. 1 показано графік залежності абсолютної помилки навчання БШП від очікуваного виходу, а на рис. 2 – графік залежності відносної помилки. БШП навчався апроксимувати функцію y=1000x, для $x\in$[10,100]. Застосовано БШП з одним вихідним нейроном. За цієї причини загальна помилка БШП відповідає помилці єдиного вихідного нейрону. Абсолютна помилка навчання $|\varepsilon_i|$ та відносна помилка навчання $|\bar{\varepsilon}_i|$ для i-го вихідного нейрону розраховувались так:

$$|\varepsilon_i| = |y_i - y_i^r|\,, \tag{5}$$

$$|\bar{\varepsilon}_i| = \frac{|y_i - y_i^r|}{|y_i|} = \frac{|\varepsilon_i|}{|y_i|}, \tag{6}$$

де y_i, y_i^r – очікуваний та реальний вихідні сигнали i-го вихідного нейрону.

На рис. 2 чітко прослідковується стрімке зростання відносної помилки навчання в області мінімальних значень y, при цьому як видно на рис. 1 зміні величини абсолютної помилки притаманний гаусівський характер.

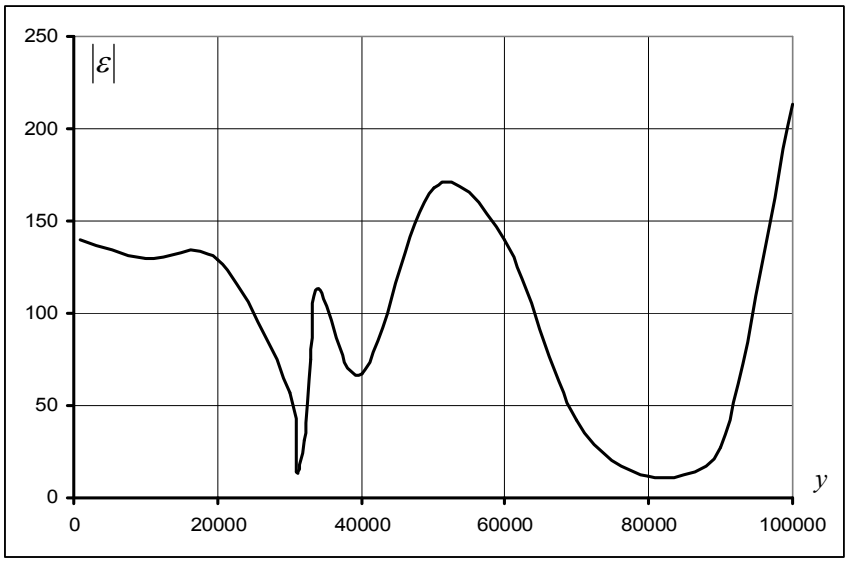

Рисунок 1 – Залежність абсолютної помилки навчання від очікуваної величини вихідного сигналу

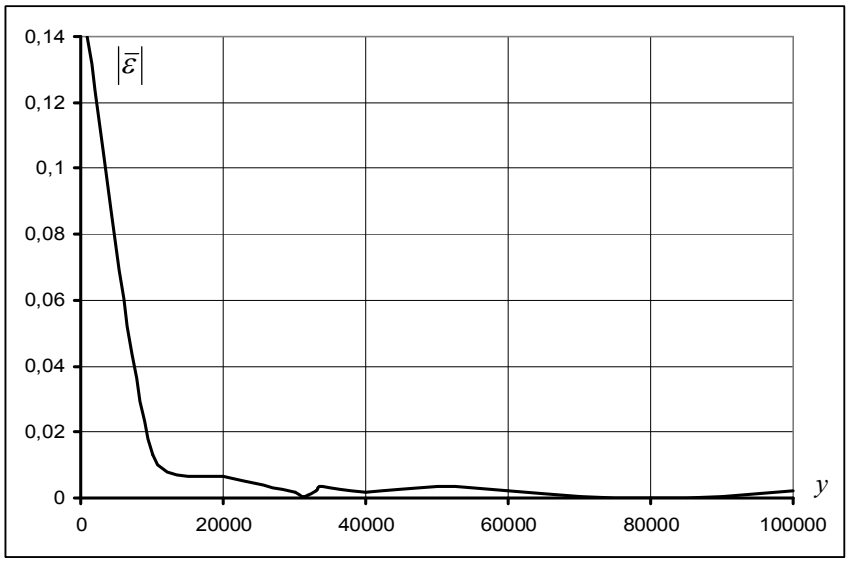

Рисунок 2 – Залежність відносної помилки навчання від очікуваної величини вихідного сигналу

Використання замість методу градієнтного спуску інших методів пошуку загальної помилки не змінило характер залежностей показаних на рис. 1, 2. Числові експерименти також вказують на однаковий характер залежностей помилок навчання та узагальнення. Зазначимо, що виявлена особливість є серйозним недоліком при розпізнаванні багатьох типів атак на КСМ, коли за допомогою БШП слід визначити допустимість відхилення контролюємих параметрів від шаблону нормальної поведінки, або від шаблону атаки. Наприклад, при розпізнаванні мережевих атак з метою порушення доступності Веб-серверу, або з метою підбору парольних даних. Очевидно, що виправити виявлений недолік можливо за рахунок вдосконалення алгоритму навчання БШП.

II Вдосконалення алгоритму навчання багатошарового перспетрону

Проведені дослідження вказують на те, що основною причиною великої відносної помилки навчання в області мінімальних значень вхідних параметрів БШП є використання квадратичного функціонала виду (3). Можливим шляхом вдосконалення алгоритму є використання в (2) функціоналу приведеної квадратичної помилки. Для цього модифікуємо (3) так

$$\bar{\varepsilon}_i^2(W) = \left(\frac{\varepsilon_i(W)}{y_i}\right)^2 = \left(\frac{y_i - y_i^r}{y_i}\right)^2, \tag{7}$$

де $\bar{\varepsilon}_i$ – приведена помилка навчання *i*-го вихідного нейрону.

Модифікація (7) призводить до певних змін у математичній моделі класичного алгоритму зворотнього поширення помилки. Визначимо ці зміни для двох останніх шарів БШП, базуючись на описі алгоритму, наведеному в [5], та використовуючи для розрахунку вихідного сигналу нейрону логістичну функцію активації

$$y^r(z) = \frac{1}{1+e^{-\alpha \cdot z}}, \tag{8}$$

де α – деякий коефіцієнт, z – зважена сума вхідних сигналів для нейрону,

$$\frac{d}{dz} y^r(z) = \alpha y^r(z)\left(1 - y^r(z)\right). \tag{9}$$

Розглянемо обчислення вагових коефіцієнтів зв'язків *i*-го нейрону вихідного шару. Використання приведеного квадратичного критерію якості навчання (2), (7) дозволяє записати градієнтний алгоритм корекції вагових коефіцієнтів в наступному вигляді

$$\Delta w_{s,i} = -\gamma_{s,i} \frac{\partial \bar{\varepsilon}_i^2}{\partial w_{s,i}}, \tag{10}$$

де $\gamma_{s,i}$ – коефіцієнт швидкості навчання синаптичного зв'язку між *i*-им нейроном вихідного шару та *s*-им нейроном попереднього шару, $\Delta w_{s,i}$ – величина корекції зв'язку між *i*-им нейроном вихідного шару та *s*-им нейроном попереднього шару, $\bar{\varepsilon}_i$ – приведена помилка начвання *i*-ого нейрону вихідного шару.

Розрахуємо частинну похідну

$$\frac{\partial \bar{\varepsilon}_i^2}{\partial w_{s,i}} = \frac{\partial \bar{\varepsilon}_i^2}{\partial y_i^r} \frac{\partial y_i^r}{\partial z_i} \frac{\partial z_i}{\partial w_{s,i}}, \tag{11}$$

де y_i^r – реальний вихідний сигнал *i*-го вихідного нейрону, z_i – зважена сума вхідних сигналів для *i*-го вихідного нейрону.

Зазначимо, що z_i розраховується так

$$z_i = \sum_{s=1}^{S} (w_{s,i} y_i^r), \tag{12}$$

де *S* – кількість нейронів в передостанньому схованому шарі нейронів, що є попереднім для вихідного шару.

Враховуючи (5), (6), (9), (12) визначимо множники добутку (11)

$$\frac{\partial \bar{\varepsilon}_i^2}{\partial y_i^r} = \frac{\partial \left(\frac{y_i - y_i^r}{y_i} \right)^2}{\partial y_i^r} = \frac{1}{y_i^2} \frac{\partial \left(y_i - y_i^r \right)^2}{\partial y_i^r} = -\frac{2\left(y_i - y_i^r \right)}{y_i^2} = -\frac{2\varepsilon_i}{y_i^2}. \tag{13}$$

$$\frac{\partial y_i^r}{\partial z_i} = \alpha y_i^r \left(1 - y_i^r \right). \tag{14}$$

$$\frac{\partial z_i}{\partial w_{s,i}} = y_s^r, \tag{15}$$

де y_s^r – вихід *s*-го нейрону схованого шару, пов'язаного з *i*-им нейроном вихідного шару.

Підставивши (13) – (15) в (10) отримаємо величину корекції зв'язку між *i*-им нейроном вихідного шару та *s*-им нейроном попереднього шару

$$\Delta w_{s,i} = 2\alpha \gamma_{s,i} y_i^{-2} y_i^r \left(1 - y_i^r \right) \left(y_i - y_i^r \right) y_s^r. \tag{16}$$

Розглянемо математичний апарат визначення величини корекції зв'язку між *s*-им нейроном останнього *j*-го схованого шару та *k*-им нейроном попереднього шару ($\Delta w_{k,s}^{(j)}$). Використовуючи приведений функціонал помилки величину корекції вказаного зв'язку запишемо так

$$\Delta w_{k,s}^{(j)} = -\gamma_{k,s} \frac{\partial \bar{\varepsilon}_s}{\partial w_{k,s}^{(j)}}, \tag{17}$$

де $\bar{\varepsilon}_i$ – приведена помилка вихідного сигналу *s*-ого нейрону *j*-го схованого шару, $\gamma_{k,s}$ – параметр швидкості навчання зв'язку між *s*-им нейроном схованого шару та *k*-им нейроном попереднього (*j* – 1)-го шару.

Обчислимо частинну похідну

$$\frac{\partial \bar{\varepsilon}_s}{\partial w_{k,s}^{(j)}} = \sum_{i=1}^{M} \frac{\partial \bar{\varepsilon}_i^2}{\partial w_{k,s}^{(j)}} = \sum_{i=1}^{M} \frac{\partial \left(\frac{y_i - y_i^r}{y_i} \right)^2}{\partial w_{k,s}^{(j)}} = \frac{1}{y_i^2} \sum_{i=1}^{M} \frac{\partial \varepsilon_i^2}{\partial y_i^r} \frac{\partial y_i^r}{\partial z_i} \frac{\partial z_i}{\partial y_s^{(j)}} \frac{\partial y_s^{(j)}}{\partial z_s^{(j)}} \frac{\partial z_s^{(j)}}{\partial w_{k,s}^{(j)}}, \tag{18}$$

де *M* – кількість нейронів у вихідному шарі, $\bar{\varepsilon}_i$ – приведена помилка на *i*-му виході БШП, $z_s^{(j)}$ – зважена сума вхідних сигналів для *s*-го нейрону в *j*-му шарі, $y_s^{(j)}$ – реальний вихід *s*-го нейрону в *j*-му шарі.

Запишемо вирази для визначення множників добутку (18)

$$\frac{\partial \varepsilon_i^2}{\partial y_i^r} = -2\left(y_i - y_i^r\right), \tag{19}$$

$$\frac{\partial y_i^r}{\partial z_i} = \alpha y_i^r \left(1 - y_i^r\right), \tag{20}$$

$$\frac{\partial z_i}{\partial y_s^{(j)}} = w_{s,i}, \tag{21}$$

$$\frac{\partial y_s^{(j)}}{\partial z_s^{(j)}} = \alpha y_s^{(j)} \left(1 - y_s^{(j)}\right), \tag{22}$$

$$\frac{\partial z_s^{(j)}}{\partial w_{k,s}^{(j)}} = y_k^{(j-1)}, \tag{23}$$

де $y_k^{(j-1)}$ – вихідний сигнал k-го нейрону $(j-1)$-го шару.

Підставивши (18) – (23) в (17) отримаємо

$$\Delta w_{k,s}^{(j)} = -2\gamma_{k,s}\alpha^2 y_i^{-2} \sum_{i=1}^{M} \left(\left(y_i - y_i^r\right) y_i^r \left(1 - y_i^r\right) w_{s,i} y_s^{(j)} \left(1 - y_s^{(j)}\right) y_k^{(j)}\right). \tag{24}$$

По аналогії з (17) – (24) можливо визначити математичний апарат для розрахунку корекції вагових коефіцієнтів будь якого схованого шару БШП. При цьому слід зазначити, що для першого схованого шару як $y_k^{(j-1)}$ слід використовувати вхідні параметри БШП.

IV Висновки

Більшість сучасних нейромережевих методів розпізнавання атак на КСМ базуються на використанні БШП, основною задачею якого є визначення допустимості відхилень параметрів поточного функціонування КСМ від параметрів функціонування в нормальних умовах.

Одним із найбільш значимих недоліків БШП є недостатня достовірність визначення допустимості відхилень параметрів поточного функціонування в області їх мінімальних значень. Показано, що вказаний недолік спричинений неадекватністю цільового функціоналу алгоритму зворотнього поширення помилки, який застосовується для навчання БШП.

Для виправлення вказаного недоліку запропоновано вдосконалити алгоритм зворотнього поширення помилки шляхом застосування цільового функціоналу у вигляді квадратичної приведеної помилки навчання. Розроблене відповідне математичне забезпечення корекції вагових коефіцієнтів синаптичних зв'язків.

Перспективним шляхом підвищення ефективності застосування БШП є розробка методики оптимізації його структури відповідно до умов конкретних задач розпізнавання атак на КСМ.

Література: ***1.*** *Архипов А. Применение моделей обнаружения аномалий для выявления атак / А. Архипов, А. Ишутин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. конф., 1-3 берез. 2006 р.: тези доп. – К., 2006. – С. 71-72.* ***2.*** *Новіков О. Розпізнавання сервісів TCP/IP за допомогою нейронних мереж / О. Новіков, С. Кащенко //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: наук.-техн. конф., 1-3 берез. 2006 р. : тези доп. – К., 2006. – С. 199-203.* ***3.*** *Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.* ***4.*** *Бодянский Е. В. Искусственные нейронные сети: архитектуры, обучение, применения. / Е. В. Бодянский, О. Г. Руденко. – Харьков: ТЕЛЕТЕХ, 2004. – 396 с.* ***5.*** *Руденко О. Г. Штучні нейронні мережі. Навч. посіб. / О. Г. Руденко, Є. В. Бодянський. – Харків: ТОВ "Компанія СМІТ", 2006. – 404 с.* ***6.*** *Хайкин С. Нейронные сети: полный курс, 2-е изд., испр. / Хайкин С.; пер. с англ. Н. Н. Куссуль – М. : Вильямс, 2006. – 1104 с.* ***7.*** *Царегородцев В. Г. Редукция размеров нейросети не приводит к повышению обобщающих способностей / В. Г. Царегородцев // Материалы XII Всеросс. семинара "Нейроинофрматика и ее приложения". – Красноярск: КГТУ, 2004. – С. 163–165.*