УДК 004.89

М.П. КОМАР

НЕЙРОМЕРЕЖЕВИЙ МЕТОД ІДЕНТИФІКАЦІЇ КОМП'ЮТЕРНИХ АТАК

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46009, Україна,

Анотація. В даній статті представлена система аналізу мережевого трафіку для виявлення мережевих атак на комп'ютерні системи, заснована на застосуванні методу штучного інтелекту - штучних нейронних мережах. Застосування нейронних мереж дозволило створити «інтелектуальну» систему, в якій детектори здатні ефективно виявляти не тільки відомі, але і невідомі комп'ютерні атаки. Наведено структуру і алгоритми навчання та функціонування нейромережевих детекторів. Представлені результати досліджень, що доводять ефективність розробленого підходу.

Аннотация. В данной статье представлена система анализа сетевого трафика для обнаружения сетевых атак на компьютерные системы, основанная на применении метода искусственного интеллекта - искусственных нейронных сетей. Применение нейронных сетей позволило создать «интеллектуальную» систему, в которой детекторы способны эффективно обнаруживать не только известные, но и неизвестные компьютерные атаки. Приведена структура и алгоритмы обучения и функционирования нейросетевых детекторов. Представлены результаты исследований, доказывающие эффективность разработанного подхода.

Abstract. This paper presents network traffic analysis system for detecting network attacks on computer systems based on application method of artificial intelligence - artificial neural networks. The Neural networks allow to create "intelligent" system in which the detectors can effectively detect not only known but also unknown cyber attacks. The structure, functioning and learning algorithms of neural detectors are presented. The results of studies that prove the effectiveness of the proposed approach are also presented.

Ключові слова: мережевий трафік, мережеві атаки, нейронні мережі, нейромережеві детектори, система виявлення вторгнень.

ВСТУП

Забезпечення інформаційної безпеки є першочерговим завданням кожної держави. В епоху комп'ютеризації і автоматизації проблема комп'ютерної безпеки виходить на перший план. Одним із завдань, яке доводиться вирішувати в контексті інформаційної безпеки є захист інформації, яка зберігається, обробляється і передається в комп'ютерних системах і мережах. Однією із загроз комп'ютерної безпеки є мережеві атаки. Під мережевою (або хакерською) атакою розуміється інформаційний руйнівний вплив, який здійснюється програмним методом і спрямований на розподілену обчислювальну систему [1]. У залежності від методу організації мережевої атаки і засобів, які використовуються виділяють кілька різновидів мережевих атак - DoS, U2R, R2L і Probe (докладний опис кожного з різновиду атак представлений нижче).

Існують два напрямки забезпечення комп'ютерної інформаційної безпеки. Першим напрямком є запровадження адміністративних та кримінальних покарань за вчинення комп'ютерних злочинів. Другим напрямком є розробка апаратно-програмних засобів виявлення і захисту від мережевих вторгнень і шкідливих програм.

Незважаючи на кроки, які проводяться з боку світового співтовариства, спрямовані на постійне посилення покарань за комп'ютерні злочини, кіберзлочинці продовжують удосконалювати і розвивати методи і засоби організації мережевих атак. На сьогоднішній день склалася така ситуація, коли запропоновані методи захисту комп'ютерних систем і мереж не здатні на належному рівні забезпечити інформаційну безпеку. Комп'ютерні системи безперервно піддаються різного роду загрозам, і користувач не може бути впевнений у захищеності важливої інформації. Ситуація, що склалася стимулює пошук і розробку нових методів і рішень, спрямованих на підвищення рівня захищеності комп'ютерних систем від шкідливих впливів.

У даній статті представлено систему виявлення віддалених мережевих атак, засновану на застосуванні методу штучного інтелекту. В якості детекторів мережевих атак використовуються

нейронні мережі, які добре зарекомендували себе у вирішенні численних складних технічних завдань, таких як прогнозування, розпізнавання, адаптація, управління та ін. Нейромережеві детектори здатні до навчання і класифікації. Навчені на обмеженому обсязі даних вони показують добрі результати виявлення різних типів мережевих атак. Для визначення мережевих атак система аналізує мережевий трафік і приймає рішення про шкідливість. Стаття організована таким чином. У першому розділі розглянуто існуючі методи виявлення мережевих атак і виявлено їх недоліки. Також розглянуто різні типи мережевих атак. Другий розділ містить структуру детектора для аналізу мережевого трафіку, в основі якого лежить нейронна мережа. У третьому розділі представлені результати експериментів, які підтверджують прийнятність розробленого підходу.

СИСТЕМИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

Виявлення мережевих атак на комп'ютерну систему відбувається за допомогою аналізу мережевого трафіку - дані, які надходять в систему або відправляються з неї. Для ясності процесу виявлення розглянемо параметри мережевого трафіку, які аналізуються для забезпечення безпеки комп'ютерних систем, а також типи мережевих атак.

Дані в комп'ютерних мережах передаються у вигляді мережевих пакетів. У структурі мережевого пакету виділяють три основні поля (рис. 1): заголовок пакету, поле даних пакету, закінчення пакету.

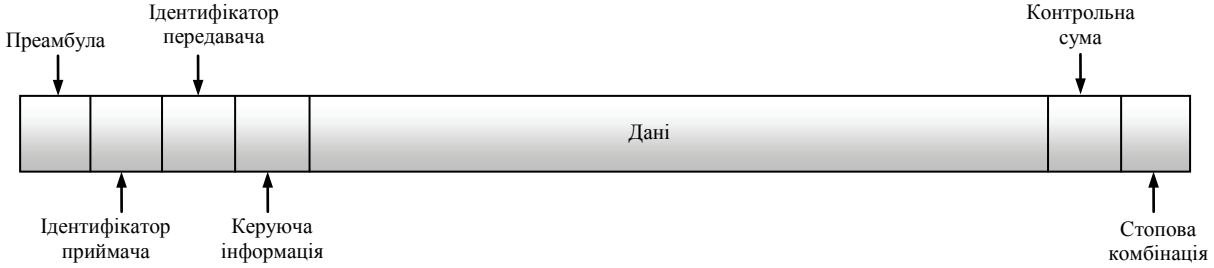

Рис. 1. Структура мережевого пакету

Заголовок пакету містить стартову комбінацію, яка забезпечує налаштування мережевого обладнання на прийом і обробку пакету, а також мережеві адреси приймача і передавача пакету і деяку загальну службову інформацію.

Поле даних пакету містить в собі, власне, інформацію, яка і передається від передавача до приймача.

Закінчення пакету містить в собі контрольну суму, яка дозволяє судити про успішність передачі інформації, стопову комбінацію, яка служить для інформування про закінчення пакету, а також деяку службову інформацію.

Виділяють 41 параметр (або атрибут) мережевого з'єднання, які в свою чергу об'єднані в 3 групи:

1. Вбудовані атрибути. Ці атрибути отримуються із зони заголовку мережевих пакетів. Виділяють 9 вбудованих атрибутів, які містять інформацію про час роботи з'єднання, тип протоколу, кількість переданих байт і т.д.

2. Атрибути контенту, які отримуються із зони контенту і містять таку інформацію як: кількість невдалих спроб реєстрації, кількість невдалих спроб реєстрації в системі, кількість виникнень помилок, кількість операцій створення файлів і т.д. Існує 13 атрибутів контенту.

3. Атрибути трафіку. Обчислюються виходячи з попередніх з’єднань. У свою чергу виділяють атрибути тимчасового і машинного трафіку. 19 атрибутів трафіку містять наступну інформацію: кількість з'єднань до цієї ж IP-адреси, кількість з'єднань до цього ж номеру порту і т.д.

У залежності від використовуваних технік при здійсненні несанкціонованих впливів на комп'ютерну систему, виділяють 4 типи мережевих атак.

DoS (denial of service) атаки - це мережеві атаки, спрямовані на виникнення ситуації, коли в системі, що атакується відбувається відмова в обслуговуванні. Дані атаки характеризуються генерацією великого обсягу трафіку, що призводить до перевантаження та блокування сервера. Виділяють шість DoS атак: back, land, neptune, pod, smurf, teardrop.

U2R (user-to-root) атаки передбачають отримання зареєстрованим користувачам привілеїв локального суперкористувача (адміністратора). Виділяють чотири типи U2R атак: buffer_overflow, loadmodule, perl, rootkit.

R2L (remote-to-local) атаки характеризуються отриманням доступу незареєстрованого користувача до комп'ютера з боку віддаленої машини. Виділяють вісім типів R2L атак: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster.

Probe атаки полягають в скануванні мережевих портів з метою отримання конфіденційної інформації. Виділяють чотири типи Probe атак: ipsweep, nmap, portsweep, satan.

У самому простому випадку система захисту від мережевих атак може представляти собою міжмережевий екран (firewall), він же брандмауер [2, 3]. Мережевий екран – це програмний чи апаратний засіб фільтрації мережевого трафіку за допомогою аналізу його параметрів, таких як адреси джерела і приймача, типів мережевих протоколів і служб, і т.д. Головною відмінністю мережевого екрану від системи виявлення вторгнень (див. нижче) є те, що в ньому відсутній аналіз вмісту переданих пакетів. Відповідно, мережеві екрани мають високу швидкість обробки вхідних і вихідних мережевих пакетів, і працюють, як правило, ґрунтуючись на наборі правил. Недоліком таких систем є низький рівень захисту, що надається, оскільки відсутній аналіз вмісту пакетів.

Система виявлення вторгнень (Intrusion Detection System - IDS) [4] на сьогоднішній день є невід'ємною частиною системи безпеки будь-якої комп'ютерної системи, підключеної до локальної або глобальної комп'ютерної мережі. IDS, як правило, це програма або апаратний засіб, який є «фільтром», знаходиться між комп'ютерною системою та комп'ютерною мережею, і аналізує параметри вхідного і вихідного трафіку з метою виявлення фактів несанкціонованого доступу. IDS перехоплює весь мережевий трафік і аналізує вміст кожного пакета на наявність шкідливих компонентів. Крім явних переваг, існуючі системи виявлення вторгнень мають ряд істотних недоліків. А саме: а) вони мають високу ресурсомісткість, через це не завжди є можливість обробляти і аналізувати усі мережеві пакети, що призводить до пропуску атаки; б) не здатні аналізувати зашифровану інформацію; в) мають слабкі можливості виявляти нові типи атак, г) вимагають певного рівня знань в галузі безпеки; д) високий рівень помилок, коли нормальне з'єднання приймається за атаку і навпаки.

Проведений аналіз пропонованих методів і засобів захисту комп'ютерних систем від шкідливих впливів виявляє недосконаліть існуючих методів захисту комп'ютерних систем від мережних атак. У зв'язку з цим, розробка нових методів захисту інформації, що дозволяють підвищити рівень захищеності комп'ютерних систем від несанкціонованого впливу є актуальною.

МЕТОД НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

Штучна нейронна мережа (ШНМ) є математичною (а також програмною або апаратною) моделлю, побудованою за принципом організації та функціонування біологічних нейронних мереж. Сьогодні існує кілька архітектур штучних нейронних мереж, які з успіхом застосовуються для вирішення складних технічних і економічних завдань. Деякими з особливостей ШНМ є здатність в процесі навчання виявляти складні залежності між вхідною і вихідною інформацією, яка була відсутня в навчальній вибірці, і, здатність коректно класифікувати зашумлені образи. Нейронні мережі мають ряд переваг, які вигідно відрізняють їх від традиційних рішень. Деякі з них: висока ступінь паралелізму обробки інформації; здатність до узагальнення, адаптація до змін навколишнього середовища; розпізнавання зашумлених образів; низький рівень ресурсоємності і т.д. Перераховані особливості та переваги послужили основою для вибору структури детектора виявлення мережевих атак.

В якості нейромережевого детектора для виявлення мережевих атак вибрана багатошарова нейронна мережа з одним прихованим шаром, що складається з нейронів Кохонена [5] (рис. 2).

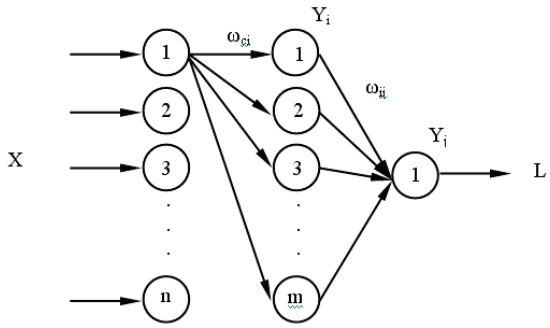

Рис. 2. Структура нейромережевого детектора

Перший шар нейронних елементів розподіляє вхідні сигнали *X* - 41 параметр мережевого з'єднання, на нейронні елементи прихованого шару. Кількість нейронних елементів розподільного шару дорівнює кількості атрибутів мережевого трафіку $n = 41$.

Другий шар складається з $m = 41$ нейронів Кохонена, які використовують конкурентний принцип навчання та функціонування відповідно до правила «переможець бере все» (*winner-take-*

all) [5,6]. Це означає, що вихідне значення нейрона-переможця дорівнює «1», а вихідні значення інших нейронних елементів дорівнюють «0». Для визначення нейрона-переможця використовується Евклідова відстань між вхідним і ваговими векторами. Так Евклідова відстань між вхідним і ваговим вектором *i*-го нейронного елемента визначається наступним чином:

$$D_i = \left|X - \omega_i\right| = \sqrt{(X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + ... + (X_c - \omega_{ci})^2}, \quad (1)$$

де ω_{1i} - ваговий коефіцієнт між *c*-м нейроном розподільного шару і *i*-м нейроном шару Кохонена, $X = [X_1, X_2, ..., X_n,]$ - вхідний образ.

Нейронний елемент-переможець з номером *k* визначається відповідно до мінімальної Евклідової відстані.

Варто зазначити, що кількість нейронів шару Кохонена *m* не обов'язково має бути рівною *41*. Проведені експерименти показали, що для різного класу атак при різній розмірності навчаючої вибірки, нейромережевий детектор швидше навчається при різних значеннях *m*. Однак, вплив кількості нейронів прихованого шару не настільки суттєвий, і може змінюватись в межах від *10* до *41*.

Третій шар складається з одного лінійного нейронного елемента, який здійснює відображення кластерів, сформованих шаром Кохонена, в два класи, які характеризують нормальне з'єднання або атаку. Активність вихідного нейрона, коли значення його дорівнює одиниці, характеризує атаку. Нуль на виході характеризує нормальне з'єднання.

Для кожного типу мережевої атаки, а їх налічується 22 типи, формується окремий нейромережевий детектор. Для навчання запропонованого нейромережевого детектора використовується навчальна вибірка, що складається з 80% з'єднань одного з типів атак і 20% нормальних з'єднань. Результати експериментів показали, що найкращий відсоток здатності до навчання і виявлення відбувається, коли навчання проводиться на 32 з'єднаннях мережевої атаки і 8 з'єднаннях легітимного, нормального трафіку.

У результаті, запропонована система виявлення мережевих вторгнень складається з 22 нейромережевих детекторів, кожен з яких характеризує певний тип атаки. На нейромережеві детектори черзі подається 41 параметр мережевого з'єднання і відбувається перевірка на наявність заборонених дій (рис. 3).

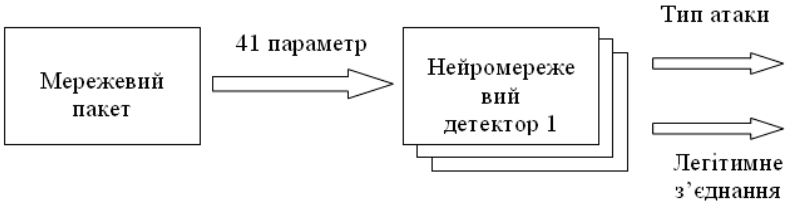

Рис. 3. Система виявлення вторгнень

РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТІВ

Для тестування розробленої системи було проведено низку експериментів. В якості вхідних даних для навчання та тестування використовувалася база даних KDD Cup1999 Data [8]. Дана база була сформована в рамках проведення міжнародної наукової конференції KDD-99, метою якої було стимулювання досліджень в області обробки даних і створення нових алгоритмів виявлення мережевих атак. База містить параметри як нормальних мережевих з'єднань, так і мережевих атак.

Таблиця 1 містить результати виявлення мережних атак різних класів різними методами. Як видно з представлених результатів, пропонований підхід показує кращі результати пошуку мережевих атак. Слід зазначити, що відсоток помилкових виявлень, коли легітимне з'єднання приймається за атаку, становить менше 10%. Також, варто відзначити, що в таблиці представлені середні результати по 4 класах мережевих атак.

Якщо брати окремі типи атак, то тут явно можна виділити такі атаки, виявлення яких відбувається з 100% вірогідністю (наприклад, neptune, teardrop), і атаки, виявлення яких не відбувається (наприклад, guess_passwd, spy).

Таблиця 1

Результати виявлення мережевих атак

Методи виявлення атак	DoS, %	Probe, %	R2L, %	U2R, %
Нейромережевий детектор	**98,0**	**92,8**	**36,5**	**30,8**
Гауссовський класифікатор	82,4	90,2	9,6	22,8
K-NN	97,3	87,6	6,4	29,8
Алгоритм найближчого кластера	97,1	88,8	3,4	2,2
Лідер-алгоритм	97,2	83,8	1,0	6,6
Алгоритм гіперсфери	97,2	84,8	1,0	8,3
Fuzzy Art Map	97,0	77,2	3,7	6,1
Дерево рішень C4.5	97,0	80,8	4,6	1,8
Переможець KDD-99	97,1	83,3	13,1	8,4

ВИСНОВКИ

Запропонований підхід, заснований на застосуванні методу нейронних мереж в якості детекторів мережевих атак, дозволяє підвищити рівень виявлення мережевих вторгнень на комп'ютерні системи. Виявлення деяких типів атак відбувається з 100% ймовірністю при незначному рівні помилкових виявлень. Крім цього, запропонований підхід не вимогливий до ресурсів системи і здатний виявляти невідомі типи атак (детектори, яких навчають, на одному типі атак, часто показують хороші результати виявлення інших типів атак, тобто на тих даних, на яких навчання не проводилося).

Однак, не всі типи мережевих атак піддаються виявленню і можуть бути пропущені. Для вирішення цієї проблеми, надалі пропонується змінити структуру нейромережевого детектора, та доопрацювати алгоритм навчання нейронної мережі.

СПИСОК ЛІТЕРАТУРИ

1. Удаленные сетевые атаки. [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Удаленные_сетевые_атаки.
2. Лукацкий, А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ-Петербург, 2003. – 596 с.
3. Межсетевой экран. [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Межсетевой_экран.
4. D. Denning. An Intrusion Detection Model / In Proceedings of IEEE Conference on Security and Privacy – Oakland, USA, 1986. – P. 118-131.
5. Kohonen, T. Sell-organised formation of topologically correct feature maps / T. Kohonen // Biological Cybernetics. – 1982. – N43. – P. 59-69.
6. Головко, В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение : учеб. пособие / В.А. Головко. – М., 2001 – 256 с.
7. Хайкин, С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1104 с.
8. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999.

Надійшла до редакції 21.11.2010р.

КОМАР М.П. – аспірант кафедри інформаційно-обчислювальних систем та управління, Тернопільський національний економічний університет, Тернопіль, Україна.