УДК 004.9

НЕЙРОМЕРЕЖЕВИЙ ПІДХІД ІДЕНТИФІКАЦІЇ КОМП'ЮТЕРНИХ АТАК

Булгакова О.С., Кудрявцев А.В., Козирь В.В.

Миколаївський національний університет ім. В.О. Сухомлинського, вул. Нікольська, 24, Миколаїв, 54030, Україна

sashabulgakova@list.ru, andreykudravtsev@mail.ru, kozyrvova@mail.ru

В роботі розглядається дослідження методики застосування інтелектуального аналізу даних для захисту комп'ютерних систем з метою ідентифікації аномальних станів мережевого тарфика за допомогою нейронних мереж. Створена експериментальна програма виявлення вторгнень, що дає змогу розпізнати (ідентифікувати) аномальні стани в комп'ютерних мережах.
Ключові слова: інтелектуальний аналіз даних, трафік, нейронна мережа, атаки.

This paper presents research of data mining application technique for protection computer systems to identify abnormal network conditions traffic using neural networks. An experimental program of IDS, which allows to recognize (identify) the abnormal condition of computer networks.
Keywords: data mining, traffic, neural network attacks.

В работе рассматривается исследование методики применения интеллектуального анализа данных для защиты компьютерных систем с целью идентификации аномальных состояний сетевого тарфика с помощью нейронных сетей. Создана экспериментальная программа обнаружения вторжений, что позволяет распознать (идентифицировать) аномальные состояния в компьютерных сетях.
Ключевые слова: интеллектуальный анализ данных, трафик, нейронная сеть, атаки.

Вступ

В даний час існує велика кількість механізмів захисту, які відрізняються як самим підходом до захисту комп'ютерної системи, так і конкретними способами його реалізації.

Системи виявлення аномалій, на відміну від експертних систем, є більш гнучкими. Вони будуються на припущенні, що всі дії зловмисника обов'язково чимось відрізняються від поведінки звичайного користувача. Іншими словами, такі дії можна розглядати як аномалії поведінки. Роботі системи виявлення аномалій передує період накопичення інформації, протягом якого складається деяка концепція нормальної активності системи або користувача. Вона вважається еталоном, щодо якого оцінюються всі наступні дії. На цьому етапі зазвичай визначається перелік факторів, за якими можна вести спостереження за діяльністю користувачів в системі.

Теоретично, після складання шаблону нормальної поведінки, можна фіксувати всі параметри системи (або їх необхідну частину) і сигналізувати про

відхилення цих параметрів від звичайних значень. Проте обсяг інформації, що генерується у великих системах (файли аудиту, потік даних в комп'ютерних мережах і тому подібна інформація) може досягати декількох мегабайт за годину і, зрозуміло, людина не в змозі вручну обробити таку кількість даних. Крім того, сама постановка завдання – виявити аномальну поведінка користувача, чим-небудь відрізняється від звичайного – погано формалізується.

Тому останнім часом все частіше робляться спроби аналізу аномального поведінки користувачів на основі інтелектуальних методів обробки даних, у тому числі із застосуванням нейронних мереж [1-2].

1. Методи і технології інтелектуального аналізу в задачах інформаційної безпеки

Нижче наведені деякі технології інтелектуального аналізу, які використовуються при вирішенні задач інформаційної безпеки.

Продукційні системи – системи, які використовують продукційну модель представлення знань. Ця модель описує будь-які знання як правила виду [3]: ЯКЩО <умова> ТО <дія>.

Продукційні системи використовуються при сигнатурному методі аналізу [4]. Такий аналіз передбачає, що більшість атак розвиваються за схожим сценарієм і мають спільні риси. У системах захисту інформації сигнатури описують характерні особливості, необхідні умови, задіяні пристрої і послідовність дій при проведенні атаки. Однією з реалізацій даного підходу є використання БД з сигнатурами відомих вторгнень і перевірка з ними поточних дій користувача і параметрів системи. У разі часткового збігу система захисту оповіщає системного адміністратора про можливе вторгнення. Повний збіг сигнатури з поточною активністю малоймовірно, тому що сценарій атаки може змінюватися або сигнатура «зашумлена» іншими користувачами, тому необхідно використовувати саме частковий збіг характеристик. Щоб розпізнати такий збіг часто використовуються продукційні системи. Яскравими представниками програм, які в своїй роботі використовують метод сигнатурного аналізу, є системи виявлення мережевих атак (наприклад, Snort, RealSecure, eTrust Intrusion Detection і ін.) І антивірусні сканери (наприклад, AVZ, Kaspersky Anti-Virus, Microsoft Security Essentials та ін .).

Продукційні системи мають ряд переваг, які вплинули на їх широке розповсюдження. Серед переваг можна виділити поділ вирішення проблеми і її формулювання, стійкість і високу точність виявлення відомих загроз. Однак разом з перевагами є і велика кількість недоліків, які ускладнює застосування ЕС для аналізу захищеності: виявляються лише відомі; необхідність наявності кваліфікованого адміністратора системи для її налаштування; недостатня ефективність при роботі з великими обсягами даних; кількість нових видів загроз постійно зростає, а продукційним системам для успішної роботи необхідно містити інформацію про кожну відому атаку. Підготовка,

поширення, зберігання і обробка таких величезних обсягів даних ускладнює використання продукційних систем.

Усунути деякі з недоліків дозволяє комбінація з іншими підходами штучного інтелекту.

Нейронні мережі. Штучні нейронні мережі (або просто нейронні мережі (НМ)) – математичні моделі, а також їх програмні або апаратні реалізації, побудовані за принципом організації та функціонування біологічних нейронних мереж – мереж нервових клітин живого організму [5].

Активно НМ застосовуються і для вирішення різних завдань захисту інформації в комп'ютерних системах. Наприклад, для ідентифікації поведінки користувача в комп'ютерній мережі [6]. Для цього НС навчається прогнозувати його наступну команду. Якщо відносна кількість правильно команд протягом сеансу роботи користувача вище заданого порогу, то поведінка вважається «нормальною», інакше або користувач різко змінив свою поведінку, або під його ім'ям працює порушник. Перевага підходу полягає в незалежності від кількості користувачів в системі, оскільки з кожним користувачем зв'язується окрема НМ. До недоліків можна віднести те, що топологія мережі і ваги вузлів визначаються тільки після досить великої кількості проб і помилок.

Багатоагентні системи. В теорії багатоагентних систем (БАС) використовується наступний принцип роботи: вся система ділиться на множину агентів і справедливо передбачається, що кожен з них може вирішити тільки деяку локальну задачу, оскільки не володіє вичерпними знаннями про глобальну проблему. Тому рішення вихідної задачі полягає в реалізації множини агентів і організації ефективної взаємодії між ними. У БАС вихідна задача декомпозується і її частини за певними правилами призначаються агентам. Призначення завдання агенту означає привласнення йому ролі, складність якої визначається виходячи з можливостей агента. Для вирішення загального завдання агенти об'єднуються в організації або групи.

На основі аналізу розглянутих методів, і їх використання для вирішення завдань контролю безпеки виділені методи на основі НМ для подальшого використання в роботі

2. Розробка експериментальної програми аналізу і ідентифікації аномальних станів мережевого трафіку

Виявлення мережевих атак на комп'ютерну систему відбувається за допомогою аналізу мережевого трафіку – дані, які надходять в систему або відправляються з неї.

В рамках даної роботи для навчання експериментальної СВВ виділяється 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 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.

Реалізований в рамках даної роботи прототип СВВ, побудованої з використанням модульного підходу, складається з 3 рівнів:

- джерело даних;
- обробник даних;
- аналізатор даних;

Налагодження та тестування моделі виконані на основі аналізу інформації, отриманої при обробці реальних IP-трафіків, інформація про яких представлена в загальнодоступній базі зразків мережевого трафіку KDD Cup 1999 [7]. Використовувані з цієї бази вхідні дані структурно являють собою *n*-мірні вектора, про які апріорі відомо, що вони належать до одного з наступних виділених п'яти класів можливих станів трафіку:

- Normal – нормальний стан.
- 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 – сканування портів з метою виявлення вразливостей у системі. Виділяють чотири типи Prob атак: portsweep, ipsweep, satan, nmap.

Для навчання мережі вхідна вибірка бази даних розбивається на 3 частини:

- Training set – на цих прикладах буде відбуватися навчання мережі;
- Testing set – на цьому наборі даних буде тестуватися мережа;

– Validation set – підтверджуючий набір даних сигнатур окремих атак, сгенерованих з реального он-лайн IP-трафіку за допомогою ряду допоміжних програм.

Після навчання і тестування СВВ на базі даних KDD-99, проводиться тестування та аналіз результатів на базі записів сигнатур окремих атак реального IP-трафіку. У процесі тестування, на вхід СВВ подаються послідовно записи з прикладами різних міжмережевих взаємодій, які входили в навчальну вибірку. Реалізація модульного підходу до побудови СВВ, створена в рамках цієї роботи, не є системою, що працює в масштабі реального часу. Це означає те, що обробка та аналіз вхідних даних здійснюється вже після того, як здійснений збір інформації.

Таким чином, подальша робота СВВ складається з наступних етапів:

- збір інформації про стан мережевого взаємодії з мережі;
- підготовка цієї інформації та генерація набору вхідних векторів;
- обробка вхідних векторів за допомогою експериментальної СВВ;

аналіз результатів та їх інтерпретація.

Детальний опис 41 атрибута мережевого трафіку, які використовуються в базах даних KDD можна знайти на сайті http://kdd.ics.uci.edu/.

3. Алгоритм створення експериментальної системи виявлення вторгнень

Алгоритм пошуку вторгнень, який здійснюється за допомогою прототипу СВВ, побудованої з використанням модульного підходу, складається з таких етапів:

1. Підготовка даних. Підготовка training і test наборів даних KDD. Для системи виявлення атак використовувалася 10% вибірка з баз KDD (майже 500 тисяч записів). У роботі розглядався аналіз системи мережевої взаємодії і параметри, які брали участь у процесі навчання і тестування, безпосередньо були пов'язані зі стеком протоколів TCP/IP. Аналізовані параметри характеризували потік даних в рамках різних протоколів і відображали зміст, цілісність, інтенсивність і стан мережевого трафіку. Аналізу піддавалася, насамперед, наступна інформація: вміст заголовків протоколів мережевого і транспортного рівнів; інтенсивність обміну інформацією по мережі на 3 різних рівнях (мережевий, транспортний, прикладний); статистична інформація, відносно прикладних даних на транспортному рівні; інформація, пов'язана з роботою різних протоколів прикладного рівня.
2. Нормалізація та обробка даних для подальшого використання нейронною мережею.
3. Вибрати систему ознак, характерних для даного завдання, і перетворити дані відповіднім чином для подачі на вхід мережі (нормування,

стандартизація і т.д.). В результаті бажано отримати лінійно відокремлюваній простір множини зразків.

4. Вибрати систему кодування вихідних значень (класичне кодування, 2 на 2 кодування і т.д.).

5. Конструювання, навчання та оцінка якості нейронної мережі.

У роботі проведені додаткові дослідження, метою яких є визначення типів НМ і алгоритмів навчання, які ефективно зможуть вирішити поставлене завдання при побудові прототипу СВВ. Для визначення оптимального типу НМ і алгоритму навчання проводилися експерименти, які дозволяють визначити ефективність виявлення вторгнень. Критерієм ефективності в даному випадку був відсоток виявлених атак. В якості навчальної та тестуючої вибірки використовувалися дані KDD-99.У якості аналізатора даних використовувався алгоритм прямого поширення. НМ складається з одного прихованого шару, з кількістю нейронів прихованого шару рівним *(n, 2n+1, c),* де *n* – кількість входів першого шару, *2n+1* – кількість нейронів прихованого шару і *c* – кількість класів різних атак плюс клас нормальної взаємодії. Навчання відбувається на основі методу зворотного поширення помилки. Схема роботи розробленої СВВ представлена на рис. 1.

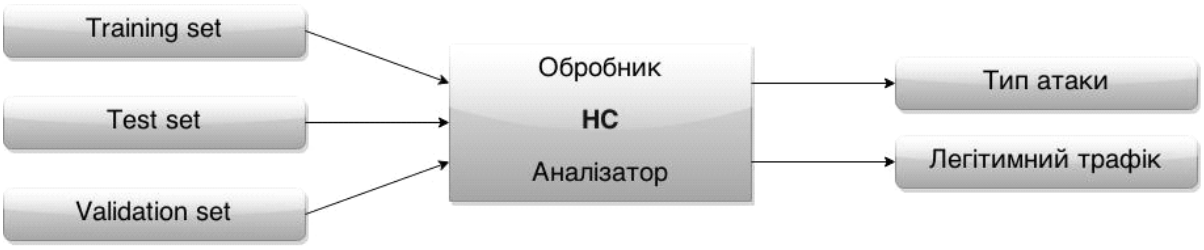

Рис. 1. Загальна схема роботи СВВ.

6. Обрати топологію мережі: кількість шарів, число нейронів у шарах і т.д.

7. Обрати функцію активації нейронів (наприклад "сигмоїд").

8. Обрати алгоритм навчання мережі.

9. Оцінити якість роботи мережі на основі підтверджуючої множини або іншому критерію, оптимізувати архітектуру (зменшення ваг, проріджування простору ознак).

10. Зупинитися на варіанті мережі, який забезпечує найкращу здатність до узагальнення та оцінити якість роботи по тестовій множині.

11. Аналіз результатів навчання. Аналіз отриманих результатів навчання на основі даних бази KDD-99.

12. З'ясувати ступінь впливу різних факторів на прийняття рішення (евристичний підхід).

13. Переконатися, що мережа дає необхідну точність класифікації.

14. При необхідності повернутися на етап 2, змінивши спосіб представлення зразків або змінивши базу даних.

15. Підготовка даних сигнатур реальних атак мережевого трафіку. Підготовка тестової бази даних сигнатур окремих атак за допомогою ряду допоміжних програм (див. далі). Сортування прикладів атак за типами, проведення їх класифікації, аналіз і видалення суперечливих або нульових прикладів.

16. Тестування навченої нейронної мережі на предмет виявлення вторгнень.

17. Аналіз отриманих результатів та вивід статистики.

4. Програмна реалізація алгоритму

Крок 1. *Завантаження даних для навчання та налаштування нейронної мережі.* На даному етапі можливо вибрати кількість нейронів у прихованому шарі і кількість ітерацій навчання. Ітерація навчання – це один цикл проходу по навчальним даним з регулярним оновленням графіка мінімізації помилки навчання.

Крок 2. *Навчання нейронної мережі і висновок результату.*

У процесі навчання відбувається оновлення графіку мінімізації помилки навчання після кожних 5000 переглянутих векторів в навчальних даних. Потім СВВ виводить результат навчання мережі в таблицю.

Крок 3. *Перевірка навченої нейронної мережі на розпізнаванні тестових даних.* Після навчання нейронної мережі за допомогою навчальний даних, на вхід програми потрібно завантажити файл з тестовими даними для перевірки якості навчання мережі. Після завантаження тестових даних потрібно натиснути кнопку "Розпізнавання". Після обробки файлу з тестовими даними програма виведе результат розпізнавання.

Крок 4. *Перевірка нейронної мережі на підставі векторів атак реального мережного графіка. Аналіз результатів.* Навчена СВВ була протестована на виявлення всіх 10 класів стану мережевого трафіку. Результат розпізнавання наведено в таблиці 1.

Таблиця 1

Результат розпізнавання окремих атак експериментальної СВВ.

Клас	Вірно	Невірно
normal	97173 (99,892%)	105 (0,108%)
back	2195 (99,637%)	8 (0,363%)
ipsweep	1209 (96,553%)	38 (3,047%)
neptune	107193 (99,993%)	8 (0,007%)
nmap	202 (87,446%)	29 (12,554%)
portsweep	1024 (98,462%)	16 (1,538%)
satan	1570 (98,804%)	19 (1,196%)

Продовження таблиці 1

smurf	280775 (99,995%)	14 (0,005%)
teardrop	979 (100%)	0 (0%)
warezclient	965 (94,608%)	55 (5,392%)

Отримані результати дозволяють стверджувати, що розроблена експериментальна СВВ дозволяє ефективно виявляти факт наявності атаки.

5. Висновки

В результаті експерименту була створена модель, стійка до виявлення різних типів атак на відмову в обслуговуванні, визначені ключові атрибути мережевого трафіку і оптимальні методи DataMining. Результати роботи можуть бути корисні при проектуванні систем протидії DDoS атакам спільно з експертними системами. Проведені тести зараз знаходяться в стадії обробки, але попередня приблизна оцінка показує, що нейронна мережа здатна приймати правильні рішення з відносною помилкою 2-6%.

Надалі планується доопрацювати архітектуру мережі, а також вибрати найбільш ефективні «ознаки», за якими буде навчатися мережа, зменшивши тим самим кількість помилок на виході мережі.

Література

1. Tan K. The Application Of Neural Networks To UNIX Computer Security// Proc. Of the IEEE International Conference on Neural Networks (Perth, Western Australia) 1995. – С. 476-481.
2. Debar H., Dorizzi B. An Application of a Recurrent Network to an Intrusion Detection System// Proc. of 6-th International Joint Conference on Neural Networks (Baltimore, Maryland, USA) – 1992. С. 478-483.
3. Уэно Х., Исидзука М. Представление и использование знаний. – М.: Мир, 1989. – 220 с.
4. Лукацкий А.В. Обнаружение атак. – СПб.: «БХВ-Петербург», 2001. – 596с.
5. Малыхина М.П., Бегман Ю.В. Нейросетевая экспертная система на основе прецедентов для решения проблем абонентов сотовой связи: монография. – Краснодар, 2011.
6. Резник А.М., Куссуль Н.Н., Соколов А.М. Нейросетевая идентификация поведения пользователей компьютерных систем. – Кибернетика и выч. техника, 1999. – Вып. 123, с. 70-79DARPA. Knowledge Discovery in Databases. 1999. DARPA archive. [Електронний ресурс]. — URL: http://www.kdd.ics.uci.edu/databases/kddcup99/task.htm.