DOI 10.34185/1562-9945-3-140-2022-08
УДК 004.056.53:[004.7:004.032.26]

В М. Пахомова, А.Д. Видиш

ДОСЛІДЖЕННЯ КОМБІНОВАНОГО ВАРІАНТУ ВИЗНАЧЕННЯ АТАК З ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖНИХ ТЕХНОЛОГІЙ

Анотація. Сучасний світ неможливо уявити без комп'ютерних мереж: як локальних, так і глобальних; тому питання мережевої безпеки стає все більш злободенним. Наразі методики виявлення атак можна підсилити використанням нейронних мереж, що підтверджує актуальність теми. Мета дослідження є порівняльний аналіз параметрів якості визначення мережевих атак з використанням комбінованого варіанту, що складається із різних нейронних мереж. У якості методів дослідження використані: нейронечітка мережа; багатошаровий персептрон; самоорганізуюча карта Кохонена. Програмна реалізація самоорганізуючої карти Кохонена здійснена мовою Python з широким спектром сучасних стандартних засобів, створення багатошарового персептрону та нейронечіткої мережі – за допомогою пакетів Neural Network Toolbox та Fuzzy Logic Toolbox системи MatLAB. На створених нейронних мережах окремо та на їх комбінованому варіанті проведені дослідження параметрів якості визначення мережевих атак. Визначено, що помилка першого роду склала 11 %, 4 %, 10 % і 0 %, помилка другого роду – 7 %, 6 %, 9 % і 6 % на нейронечіткій мережі, багатошаровому персептроні, самоорганізуючої карти Кохонена та їх комбінованому варіанті відповідно, що доказує доцільність використання комбінованого варіанту.
Ключові слова: атака, категорія, клас, персептрон, нейронечітка мережі, самоорганізуюча карта Кохонена, комбінований варіант, параметри якості.

Постановка проблеми. З розвитком технологій та комп'ютерних мереж збільшилися випадки на них атак, але не завжди встановлені засоби захисту справляються з своєю задачею. Для того, щоб швидко та точно виявляти атаки, навіть які з'явилися щойно, доречно використання нейромережної технології. Дослідження мережевих атак доцільно проводити на двох рівнях: визначення категорії атаки (на першому рівні) та визначення мережевого класу відповідно до категорії (на другому рівні) [4, 13]. Відомо, що атаки поділяються на наступні категорії: DoS (back, land, neptune, pod, smurf, teardrop); U2R (buffer_overflow, loadmodule, perl, rootkit); R2L (ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster); Probe (ipsweep, nmap, portsweep, satan). Ці класи

представлені у базі даних NSL-KDD [9], яка є поліпшеною версією KDD-99. Загальна схема виявлення мережевих атак з використанням нейронних мереж (НМ) представлена на рис. 1.

Аналіз останніх досліджень і публікацій. Виконаний огляд наукових джерел [1-8, 10-13] показав можливість використання наступних НМ: багатошарового персептрону (Multi Layer Perceptron, MLP); радіально-базисної мережі (Radial Basis Function Network, RBF); самоорганізуючої карти Кохонена (Self Organizing Maps, SOM); нейронечіткої мережі (Adaptive-Network-Based Fuzzy Inference System, ANFIS) щодо виявлення атак на комп'ютерну мережу. У лабораторії штучних нейронних мереж Брестського державного технічного університету пропонувалися різні підходи до побудови систем виявлення атак за допомогою нейромережевих технологій. Наприклад, комбінуючи MLP та рециркуляційну НМ науковці змогли отримати потужний інструмент для виявлення та класифікації атак [5]. У роботі [2] запропонували технологію нейромережевого моніторингу мережевих атак з використанням IDS Snort; для нейромережевого моніторингу використовувалася наступна комбінація: рециркуляційна НМ; MLP; SOM. У роботі [6] запропонований комбінований варіант, що складався із наступних нейронних мереж: MLP; мережі RBF; SOM, а в роботі [7] – комбінований варіант, що складався із використання ANFIS та мережі RBF.

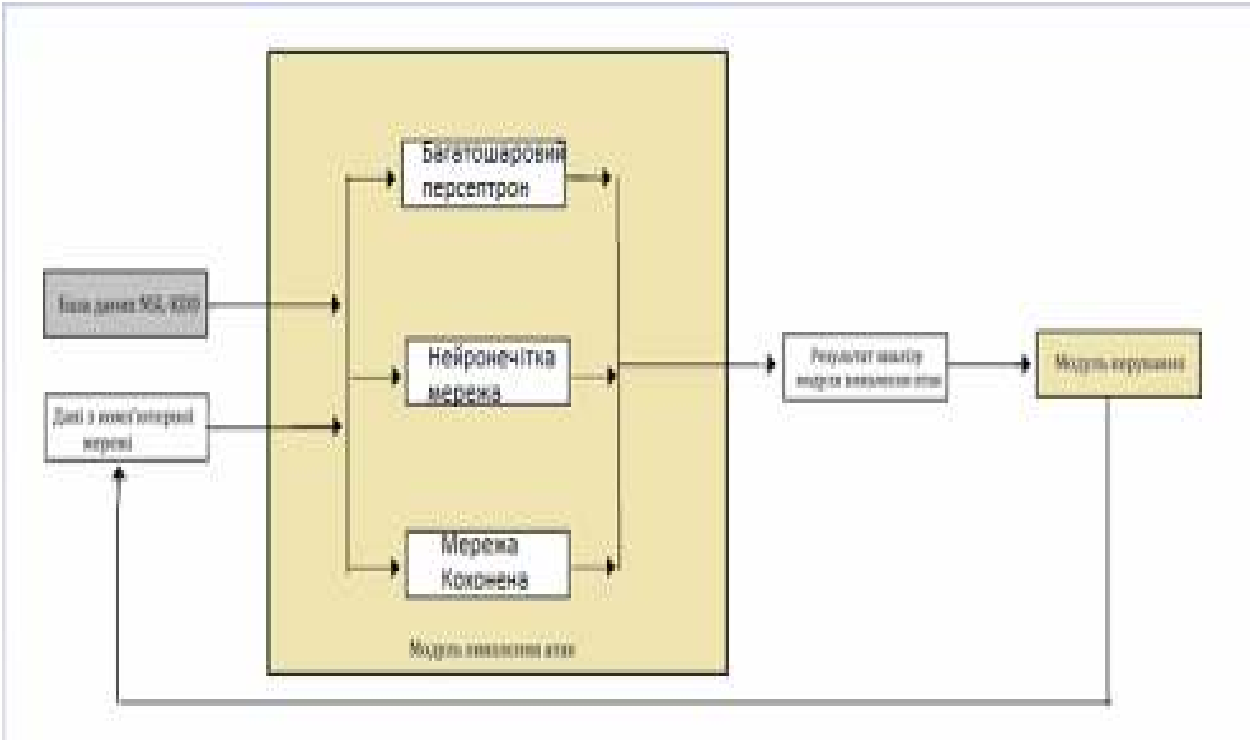

Рисунок 1 – Загальна схема виявлення мережевих атак

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Мета дослідження є порівняльний аналіз параметрів якості визначення мережевих атак з використанням комбінованого варіанту, що складається із наступних нейронних мереж: ANFIS; MLP та SOM.

Основний матеріал дослідження. Для визначення ступеню впевненості здійснення атаки створена за допомогою пакету Fuzzy Logic Toolbox в MatLAB ANFIS конфігурації 4-5-8-16-1, де 4 – кількість вхідних нейронів (кількість з'єднань на хост в поточній сесії за останні 2 с, відсоток з'єднань з хостом з count з SYN-помилками, відсоток з'єднань з різними сервісами, відсоток з'єднань з різними службами за час з'єднань по IP); 5 – загальна кількість шарів; 8 – кількість нейронів першого прихованого шару; 16 – кількість нейронів другого прихованого шару; 1 – кількість результуючих нейронів (терми: низький, середній, високий); у якості функції приналежності вхідних нейронів взято Гаусовську функцію. На створеній ANFIS проведено дослідження похибки на вибірках різної довжини: 500; 5000; 10000 та 15000 прикладів за різними методами оптимізації. Визначено, що найменше значення похибки ANFIS склало за методом Hybrid.

Для визначення категорій атак створений в MatLAB MLP конфігурації 41-1-30-5, де 41 – кількість вхідних нейронів (параметрів мережевого трафіку), 1 – кількість прихованих шарів, 30 – кількість прихованих нейронів, 5 – кількість результуючих нейронів; у якості функції активації нейронів прихованого шару взято гіперболічний тангенс, результуючого шару – лінійну функцію. На MLP проведено дослідження похибки та кількості епох на вибірках різної довжини за різними алгоритмами навчання: Levenberg-Marquardt; Bayesian Regularization; Scaled Conjugate Gradient. Визначено, що найменше значення похибки отримане за методом Levenberg-Marquardt.

Для визначення категорій атак створена в Python програма «SOM» з використанням апарату самоорганізуючої карти (шар Кохонена із п'яти нейронів), на вхід якої подаються 41 параметр мережевого трафіку, та наступних бібліотек: MiniSom, Matplotlib та Numpy. На програмі «SOM» проведені дослідження помилки квантування при різних розмірах карти: 30x30; 50x50; 70x70; 100x100. Визначено, що досить мати карту 70x70 (вибірка із 15000 прикладів), при якій помилка квантування склала 0,07.

При дослідженні розглянутий комбінований варіант ANFIS+MLP+SOM, процес отримання результуючого вектора для якого представлений на рис. 2; контрольна вибірка складалася із 50 прикладів.

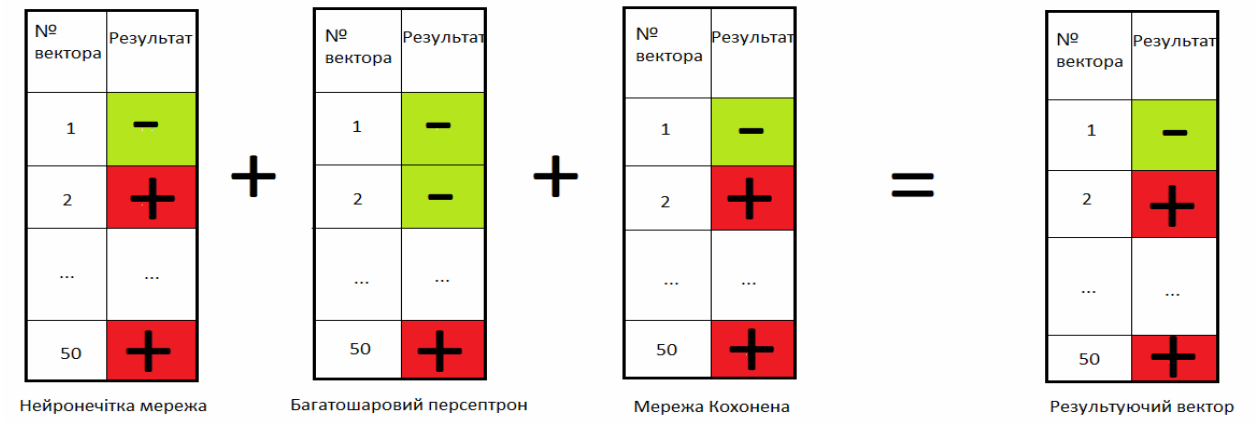

Рисунок 2 – Спрощене представлення формування результуючого вектора: «-» - атаки не було; «+» - атака відбулась

Усі показники оцінки якості виявлення мережевих атак на основі НМ окремо та їх комбінованого варіанту зведені до табл. 1.

Таблиця 1

Показники оцінки якості рішень за різними підходами

Показник	TP	FP	FN	TN	TPR	FPR	Accuracy	Precision	Recall
ANFIS	17	2	4	27	0,81	0,07	0,88	0,89	0,81
MLP	22	0	1	27	0,96	0,00	0,98	1,00	0,96
SOM	21	0	2	27	0,91	0,00	0,96	1,00	0,91
Комбінований варіант	20	0	3	27	0,87	0,00	0,94	1,00	0,87

Із таблиці видно, що комбінований варіант показує наявність атаки на 6 % краще, ніж ANFIS та на 4 % краще, ніж MLP та SOM.

Висновки. Для визначення атак категорій DOS, U2R, R2L, Probe з використанням відкритої бази NSL-KDD та подальшого дослідження обраний комбінований варіант: ANFIS+MLP+SOM. Для визначення ступеню впевненості здійснення атаки створена ANFIS конфігурації 4-5-8-16-1, у якості функції приналежності вхідних нейронів взято Гаусовську функцію. На створеній ANFIS проведено дослідження похибки на вибірках різної довжини за різними методами оптимізації. Для визначення категорій атак створений MLP конфігурації 41-1-30-5, у якості функції активації нейронів прихованого шару взято гіперболічний тангенс, результуючого шару – лінійну функцію. На MLP проведено дослідження похибки та кількості епох на вибірках різної довжини за різними алгоритмами навчання. Для визначення категорій атак створена в Python програма «SOM» з використанням апарату самоорганізуючої карти (шар

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Кохонена із п’яти нейронів), на вхід якої подаються 41 параметр мережевого трафіку. На програмі «SOM» проведені дослідження помилки квантування при різних розмірах карти. На створених НМ окремо та на їх комбінованому варіанті проведені дослідження параметрів якості: помилки першого та другого роду; коректності визначення мережевих атак; помилкових спрацьовувань; достовірності; точності та повноти. Визначено, що помилка першого роду склала 11 %, 4 %, 10 % і 0 %; помилка другого роду – 7 %, 6 %, 9 % і 6 % на ANFIS, MLP, SOM та їх комбінованого варіанту відповідно, що доказує доцільність використання комбінованого варіанту.

ЛІТЕРАТУРА

1. Браницкий А.А. Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта: автореф. дис.…канд. техн. наук : Санкт-Петербург, 2018. 18 с.

2. Емельянова Ю.Г., Талалаев А.А., Тищенко И. П., Фраленко В. П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы. Программные системы: теория и приложения, 2011. № 3(7). С. 3-15.

3. Мустафаев А. Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика. Вопросы безопасности, 2016. № 2. С. 1-7. DOI: 10.7256.2409-7543.2016.2.18834

4. Пахомова В. М., Коннов М.С. Дослідження двох підходів до вивлення мережних атак із використанням нейромережної технології. Наука та прогрес транспорту, 2020. №3(87). С. 81-93. URL: https://doi.org/10.15802/stp2020/208233

5. Технологии обнаружения сетевых атак. Брестский государственный технический університет. URL: https://www.bstu.by/~opo/templates_c/%25%25A1%5EA14%5EA14FF5EA%25%25index.html.php

6. Фролов П.В., Чухраев И. В., Гришанов К. М. Применение искусственных нейронных сетей в системах обнаружения вторжений. Системный администратор. 2018. № 9(190). URL: http://samag.ru/archive/article/3724

7. Amini M., Rezaeenour J., Hadavandi E. A Neural Network Ensemble Classifier for Effective Intrusion Detection using Fuzzy Clustering and Radial Basis Function Networks. International Journal on Artificial Intelligence Tools. 2016. Vol. 25. Iss. 02. P. 1–32. DOI: https://doi.org/10.1142/s0218213015500335

8. Dhangar K., Kulhare D., Khan A. A Proposed Intrusion Detection System. International Journal of Computer Applications. 2013. Vol. 65, N 23. p.p. 46-50.

9. NSL-KDD dataset. URL: https://www.unb.ca/cic/datasets/nsl.html

10. Pakhomova V.M., Bikovska D.G. Investigation of multilayer neural network parameters for determination of R2L category network attacks. Modern engineering and innovatite technologies. Germany, Karlsruhe: Sergeieva&Co, «ISE&E». 2021. № 18-02. pp. 39-43. DOI: 10.30890/2567-5273.2021-18-02-059.
11. Saied A., Overill R. E., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing. 2016. Vol. 172. P. 385–393. DOI: https://doi.org/10.1016/j.neucom.2015.04.101
12. Zhukovyts'kyy I. V., Pakhomova V. M. Identifying threats in computer network based on multilayer neural network. Наука та прогрес транспорту. 2018. № 2 (74). P. 114–123. DOI: https://doi.org/10.15802/stp2018/130797
13. Zhukovyts'kyy I. V., Pakhomova V. M., Ostapets D. O., Tsyhanok O. I. Detection of attacks on a computer network based on the use of neural network complex. Наука та прогрес транспорту. 2020. № 5(89). P. 68–79. URL: https://doi.org/10.15802/stp2020/218318

REFERENCES

1. Branitskiy A.A. Obnaruzhenie anomalnykh setevykh soedineniy na osnove gibridizatsii metodov vychislitelnogo intellekta (Extended abstract of PhD dissertation). St. Petersburg, Russia, 2018.
2. Emelyanova Yu. G., Talalaev A. A, Tishchenko I. P, Fralenko V. P. Neural network technology for detecting network attacks on information resources. Software systems: theory and applications, 2011. № 3(7). C. 3-15.
3. Mustafaev A. G. Neural network system for detecting computer attacks based on network traffic analysis. Security questions. Вопросы безопасности, 2016. № 2. C. 1-7. DOI: 10.7256.2409-7543.2016.2.18834
4. Pakhomova V. M., Konnov M. S. Research of two approaches to detect network attacks using neural network technologies. Science and Transport Progress, 2020, 3(87), 81-93. URL: https://doi.org/10.15802/stp2020/208233
5. Network attack detection technologies. Brest State Technical University. URL: https://www.bstu.by/~opo/templates_c/%25%25A1%5EA14%5EA14FF5EA%25%25index.html.php
6. Frolov P. V., Chukhraev I. V., Grishanov K. M. Application of artificial neural networks in intrusion detection systems. System administrator, 2018. 9(190). Retrieved from samag.ru/archve/article/3724
7. Amini, M., Rezaeenour, J., Hadavandi, E. A Neural Network Ensemble Classifier for Effective Intrusion Detection Using Fuzzy Clustering and Radial Basis Function

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Networks. International Journal on Artificial Intelligence Tools, 2016. 25(02), 1-32. DOI: https://doi.org/10.1142/s0218213015500335

8. Dhangar K., Kulhare D., Khan A. A Proposed Intrusion Detection System. International Journal of Computer Applications. 2013. Vol. 65, N 23. p.p. 46-50.

9. NSL-KDD dataset. URL: https://www.unb.ca/cic/datasets/nsl.html

10. Pakhomova V. M., Bikovska D. G. Investigation of multilayer neural network parameters for determination of R2L category network attacks. Modern engineering and innovatite technologies. Germany, Karlsruhe: Sergeieva&Co, «ISE&E», 2021. № 18-02. pp. 39-43. DOI: 10.30890/2567-5273.2021-18-02-059

11. Saied A., Overill R. E., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 2016. 172, 385-393. DOI: https://doi.org/10.1016/j.neucom.2015.04.101

12. Zhukovyts'kyy I. V., Pakhomova V. M. Identifying threats in computer network based on multilayer neural network. Science and Transport Progress, 2018. 2(74), 114-123. DOI: https://doi.org/10.15802/stp2018/130797

13. Zhukovyts'kyy I. V., Pakhomova V. M., Ostapets D. O., Tsyhanok O. I. Detection of attacks on a computer network based on the use of neural network complex. Наука та прогрес транспорту. 2020. № 5(89). 68-79. URL: https://doi.org/10.15802/stp2020/218318

Received 28.03.2022.
Accepted 30.03.2022.

Study of the combined variant of determination of attacks using neural network technologies

The modern world is impossible to imagine without computer networks: both local and global; therefore, the issue of network security is becoming increasingly topical. Currently, methods of detecting attacks can be strengthened by using neural networks, which confirms the relevance of the topic. The aim of the study is a comparative analysis of the quality parameters of network attacks using a combined variant consisting of different neural networks. As research methods used: neural network; multilayer perceptron; Kohonen's self-organizing map. The software implementation of the Kohonen self-organizing map is carried out in Python with a wide range of modern standard tools, creation of a multilayer perceptron and a fuzzy network - using Neural Network Toolbox packages, and Fuzzy Logic Toolbox system MatLAB. On the created neural networks separately and on their combined variant researches of parameters of quality of definition of network attacks are carried out. It was determined that the error of the first kind was 11%, 4%, 10% and 0%, the error of the second kind - 7%, 6%, 9% and 6% on the fuzzy network, multilayer perceptron, self-organizing Kohonen map and their combined version, respectively, which proves the feasibility of using the combined option.

Пахомова Вікторія Миколаївна – к.т.н., доц. кафедри електронних обчислювальних машин Українського державного університету науки та технологій (Дніпро); ORCID 0000-0002-0022-099X

Видиш Анастасія Денисівна – магістр спеціальності «Комп'ютерна інженерія» Українського державного університету науки та технологій (Дніпро); ORCID 0000-0001-5843-7377

Pakhomova Victoria Nikolaevna – Ph.D., Assoc. Department of Electronic Computers of the Ukrainian State University of Science and Technology (Dnipro); ORCID 0000-0002-0022-099X

Vydish Anastasia Denisovna - Master of Computer Engineering, Ukrainian State University of Science and Technology; ORCID 0000-0001-5843-7377

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)