УДК 004.89 DOi 10.30837/ bi.2022.1(98).03

М.М. Корабльов[1], О.О. Фомічов[2], Д.В. Васюк[3]

[1]доктор технічних наук, професор кафедри комп'ютерних інтелектуальних технологій та систем, Харківський національний університет радіоелектроніки, mykola.korablyov@nure.ua, ORCID ID: 0000-0002-8931-4350

[2]кандидат технічних наук, старший викладач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, oleksanr.fomichov@nure.ua, ORCID ID: 0000-0001-9273-9862

[3]студент групи КІТм-20-1, Харківський національний університет радіоелектроніки, dmytro.vasiuk@nure.ua, ORCID ID: 0000-0003-4730-3378

ПОШУК ПРАЦЕЗДАТНИХ PROXY-АДРЕСІВ З ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖЕВОГО ПІДХОДУ

Для підключення користувача до Інтернету можна використовувати proxy-сервери, які забезпечують різні рівні функціональності, безпеки та конфіденційності, і які можна налаштувати як веб-фільтри або брандмауери, що захищають комп'ютер від інтернет-загроз. Під працездатністю proxy-адресів мається на увазі можливість відправляти запити на різні ресурси або сервіси та отримувати відповіді. Якщо запит був відправлений, а відповідь так і не отримана, можна зробити висновок, що proxy-адреса не працездатна. У випадку отримання відповіді можна зробити висновок, що proxy-адреса працездатна. Розглянуті фактори, які можуть впливати на відправлення запиту та отримання відповіді від ресурсу. Аналіз розглянутих факторів показав, що неможливо однозначно зробити висновок про працездатність proxy-адреси, якщо брати до уваги лише факт наявності або відсутності відповіді від ресурсу. Виділені умови для підтвердження або спростування працездатності proxy-адреси, які взяті за вхідні дані моделі, яка пропонується для оцінки працездатності proxy-адреси. В якості моделі використана нейронна мережа у вигляді тришарового персептрону, навчання якої виконується методом зворотного розповсюдження помилки. Створену модель було перевірено на визначення стану працездатності proxy-адресів за допомогою тестових наборів даних. На основі результатів досліджень та проведених експериментів був створений додаток, який виконує пошук в Інтернеті ресурсів з proxy-адресами та перевіряє їх на працездатність.

PROXY-СЕРВЕР, PROXY-АДРЕСА, ЗАПИТ, ВІДПОВІДЬ, ПРАЦЕЗДАТНІСТЬ, КОРИСТУВАЧ, РЕСУРС, НЕЙРОННА МЕРЕЖА, ДОДАТОК

Korablyov M.M., Fomichev O.O., Vasyuk D.V. Finding operability proxy addresses using a neural network approach. Proxy servers can be used to connect the user to the Internet, which provides different levels of functionality, security, and privacy, and can be configured as web filters or firewalls that protect the computer from Internet threats Under the health of proxy addresses, we mean the ability to send requests to various resources or services and receive responses. If the request was sent and no response was received, it can be concluded that the proxy address is not working. If a response is received, it can be concluded that the proxy address is operational. Factors that can influence, sending a request and receiving a response from a resource are considered. An analysis of the considered factors showed that it is impossible to unambiguously conclude the performance of a proxy address if we take into account only the fact of the presence or absence of a response from the resource. The conditions for confirming or refuting the performance of a proxy address are identified, which are taken as input data of the model proposed for assessing the performance of a proxy address. As a model, a neural network in the form of a three-layer perceptron was used, the training of which is performed by the method of error backpropagation. The created model was tested to determine the health status of proxy addresses using test datasets. Based on the results of research and experiments, an application was created that searches the Internet for resources with proxy addresses and checks their performance.

PROXY-SERVER, PROXY-ADDRESS, REQUEST, ANSWER, OPERABILITY, USER, RESOURCE, NEURAL NETWORK, APPENDIX

Вступ

Сьогодні неможливо представити сучасний світ без використання Інтернету, який надає користувачеві різні послуги. Підключення користувача до Інтернету може виконуватися безпосередньо через Інтернет-провайдер, або використовувати додатково транзитний веб-сервер – proxy-сервер (посередник), який залежно від потреб використання забезпечує різні рівні функціональності, безпеки та конфіденційності [1]. Роль proxy-сервера у схемі передачі даних між користувачем та кінцевим ресурсом наведена на рис. 1.

Рис. 1. Роль proxy у схемі передачі даних між користувачем та кінцевим ресурсом

Proxy-сервер є системою або маршрутизатором, який забезпечує шлюз між користувачами та Інтернетом, що допомагає запобігти проникненню кібер-зловмисників у приватну мережу. Його можна налаштувати як веб-фільтр або брандмауер, що захищає комп'ютер від інтернет-загроз, наприклад, таких як шкідливе програмне забезпечення. Proxy-сервер може знаходитися на локальному комп'ютері користувача або в будь-якій точці між комп'ютером користувача та цільовими серверами в Інтернеті.

Існують апаратні та програмні версії proxy-серверів [2]. Апаратні з'єднання знаходяться між комп'ютерною мережею та Інтернетом, де вони отримують, надсилають та пересилають дані з Інтернету. Програмні proxy-сервери зазвичай розміщуються у постачальника або знаходяться у хмарі. Тоді необхідно завантажити та встановити відповідну програму на комп'ютер, яка полегшує взаємодію з proxy-сервером.

Коли комп'ютер підключається до Інтернету, він використовує IP-адресу, яка схожа на поштову адресу, повідомляючи вхідні дані, куди йти, і позначаючи вихідні дані зворотною адресою для автентифікації інших пристроїв. Proxy-сервер – це, по суті, комп'ютер в Інтернеті, який має власну IP-адресу. Оскільки proxy-сервер має власну IP-адресу, він діє як посередник між комп'ютером та Інтернетом. Комп'ютер знає цю адресу, і коли подається веб-запит до Інтернету на використання ресурсу, він надсилається на proxy-сервер, який оцінює запит та виконує необхідні мережеві транзакції: отримує відповідь від веб-сервера і пересилає дані зі сторінки до браузера комп'ютера. Це дозволяє спростити, контролювати складність запиту або надати додаткові переваги, такі як балансування навантаження, конфіденційність або безпека.

1. Вибір типу proxy-сервера

Перш ніж почати пошук proxy-серверів, необхідно зрозуміти, що існує кілька доступних їх типів, кожен з яких виконує різні функції [3-5]. Тому важливо вибрати правильний proxy-сервер для ваших потреб. Слід зазначити, що не всі proxy-сервери працюють однаково. Важливо зрозуміти, які функції ви отримуєте від proxy-сервера, і переконатися, що даний сервер відповідає вашим цілям використання. Найчастіше proxy-сервери застосовуються для таких цілей [2]:

– забезпечення доступу комп'ютерів локальної мережі до Інтернету;

– кешування даних: для зниження навантаження на канал у зовнішню мережу та прискорення отримання клієнтом запитаної інформації, якщо часто відбуваються звернення до тих самих зовнішніх ресурсів;

– стиснення даних: proxy-сервер завантажує інформацію з Інтернету та передає інформацію кінцевому користувачеві в стислому вигляді для економії зовнішнього мережевого трафіку клієнта;

– захист локальної мережі від зовнішнього доступу: наприклад, можна налаштувати proxy-сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі (вони бачать тільки proxy-сервер);

– обмеження доступу з локальної мережі до зовнішньої: наприклад, можна заборонити доступ до певних веб-сайтів, обмежити використання Інтернету локальним користувачам, встановити квоти на трафік чи смугу пропускання, фільтрувати рекламу та віруси;

– анонімізація доступу до різних ресурсів: proxy-сервер може приховувати інформацію про джерело запиту або користувача. У такому разі цільовий сервер бачить лише інформацію про proxy-сервер, наприклад його IP-адресу, але не має можливості визначити справжнє джерело запиту; існують також спотворюючі proxy-сервери, які передають цільовому серверу неправдиву інформацію про справжнього користувача;

– обхід обмежень доступу: використовується, наприклад, користувачами країн, де доступ до деяких ресурсів обмежений законодавчо та фільтрується.

Використання proxy-серверів має ряд переваг [6]:

– посилений захист: proxy-сервер може діяти як брандмауер між вашими системами та Інтернетом;

– приватний перегляд, прослуховування та покупки;

– можна використовувати для обмеження доступу до певних сайтів.

Разом з тим, у proxy-серверів є недоліки [6]:

– відстеження: дані кешу, які використовують proxy, можуть запам'ятовувати всю особисту інформацію, включаючи паролі, і є ймовірність, що співробітники, які працюють під proxy, зловживають цією інформацією;

– безпека: хоча proxy забезпечують переваги анонімності, їм не вистачає шифрування;

– вартість: налаштування та обслуговування proxy-сервера можуть бути дорогими;

– конфігурації proxy попередньо запрограмовані для однієї конкретної мети.

При підключенні комп'ютера до Інтернету через proxy-сервер важливим являється визначення його працездатності, що впливає на якість послуг, які надаються. Враховуючи наведені властивості proxy-серверів необхідно провести аналіз підходів, які використовуються для аналізу їх працездатності, факторів, які на це впливають, а також умов для визначення працездатності proxy-адресів.

2. Працездатність proxy-сервера

Під працездатністю proxy-серверу мається на увазі можливість відправляти запити на різні ресурси або сервіси та отримувати відповіді (request/response) [7]. Якщо запит був відправлений, а відповідь так і не отримана, можна зробити висновок, що proxy-сервер, який використовувався в запиті, не працездатний. У випадку отримання відповіді можна зробити висновок, що proxy-сервер працездатний.

Але все не так однозначно. З логічної точки зору, якщо результат отриманий, то proxy-сервер працездатний, якщо результат був не отриманий, то ні (1 або 0). Але не у всіх випадках. На відправлення запиту, з використанням proxy-адреси, та отримання відповіді від ресурсу можуть впливати наступні фактори [8-10]:

1) connection timeout – проміжок часу, протягом якого слід встановити зв'язок між відправником запиту та ресурсом відповідача;

2) request timeout – час очікування відповіді від ресурсу. Після встановлення з'єднання між відправником та ресурсом, відправник повинен періодично інформувати ресурс про те, що він ще там, посилаючи інформацію на цей інформаційний ресурс. Якщо відправник не може надсилати будь-яку інформацію на ресурс у вказаний час, ресурс просто знімає це підключення, оскільки він «думає», що відправника більше немає, щоб не витрачати марно ресурси;

3) завантаженість proxy-адреси – кількість користувачів, що одночасно використовують одну й ту ж proxy-адресу. Від цього фактору залежать двоє попередніх факторів;

4) завантаженість ресурсу – максимальна кількість одночасно оброблюваних запитів;

5) швидкість proxy-адресу – залежить від швидкості Інтернету;

6) нестабільне з'єднання з інтернет мережею.

Якщо брати до уваги той факт, що використовуються proxy-адреси, які знаходяться у вільному доступі, можна доповнити список факторів наступними [8-10]:

1) життєвий період – зазвичай proxy-адреси з вільного доступу мають життєвий період в 2-3 дні. Після третього дня ймовірність працездатності proxy-адреси майже нульова;

2) можлива наявність авторизації на proxy-сервері;

3) підробка proxy-адреси – деякі сервіси дають безкоштовно користуватись їх proxy-адресами, але заздалегідь разом з працездатними адресами йдуть і підробки;

4) старі proxy-адреси – ресурс, з якого беруться адреси, може рідко оновлювати свій список.

Враховуючи ці фактори, можна відзначити, що неможливо однозначно зробити висновок про працездатність proxy-адреси, якщо брати до уваги всього лише факт наявності відповіді від ресурсу або її відсутності. Тому для пошуку працездатних proxy-адресів необхідно застосовувати формалізований підхід, заснований на використанні математичної моделі, яка б дозволяла більш об'єктивно і точно оцінювати працездатність proxy-адресів.

Розглянемо умови для визначення працездатності proxy-адресів. На основі факторів, які можуть впливати на відсутність відповіді, можна виділити наступні умови для підтвердження або спростування працездатності proxy-адреси [6-8]:

1) наявність відповіді від ресурсу;

2) чи був proxy-адрес доданий раніше, чи поточний адрес був доданий вперше;

3) наявність відповіді в попередній раз;

4) перевірка дати додання в базу даних, дата додання може більше або менше трьох днів;

5) частота оновлювання proxy-адреси, як часто proxy-адреса потрапляє в базу даних;

6) відсоткове відношення між кількістю успішно отриманих відповідей від ресурсу та кількістю невдалих, під час перевірки proxy-адреси;

7) відсоткове відношення між кількістю успішно отриманих відповідей від ресурсу та кількістю невдалих, під час відправки запитів від клієнта;

8) перевірка на кількість невдало отриманих відповідей поспіль.

Визначені умови будемо вважати за вхідні дані моделі, яка буде використовуватися для оцінки працездатності proxy-адреси.

3. Модель оцінки працездатності proxy-адреси

Для оцінки працездатності proxy-адреси можна використати різні моделі, що основані на застосуванні тих чи інших методів інтелектуальної обробки інформації, основними з яких є такі [11]:

1) штучні нейронні мережі (НМ), перевагою яких є здатність представляти будь-яку обмежену безперервну функцію з будь-якою невеликою помилкою апроксимації;

2) нечітка логіка, яка дозволяє відображати вхідні дані або змінні в проблемі рішення так, як люди міркують про них;

3) експертні системи, які застосовуються для опису проблеми і використовують інтелект одного або кількох ідентифікованих експертів;

4) еволюційні обчислення, які характеризуються здатністю адаптації з метою пристосування до навколишнього середовища, моделюючи появу, виживання та вдосконалення популяції індивідів;

5) мультиагентні системи, що складаються з груп агентів з різними цілями та завданнями, які мають певні характеристики, і являються активною сферою досліджень у складних додатках.

Для створення моделі оцінки працездатності proxy-адресів будемо використовувати нейромережевий підхід, який є ефективним для розв'язання широкого спектра задач інтелектуального аналізу даних, до яких можна віднести і задачу аналізу proxy-адресів. Існує велика кількість типів НМ, кожна з яких використовується для розв'язання відповідної задачі [12]. В якості моделі для оцінки працездатності proxy-адреси достатньо використати просту НМ у вигляді тришарового персептрона (рис. 2).

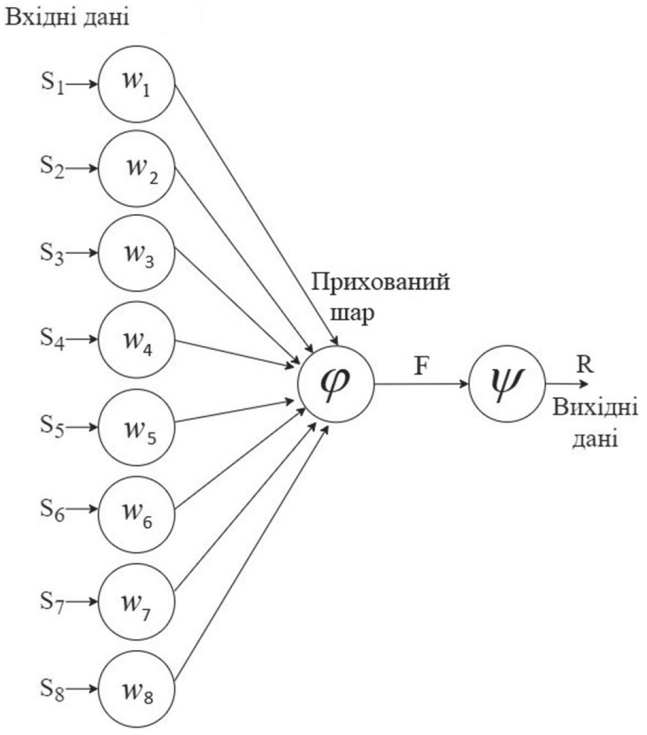

Рис. 2. Нейромережева модель для оцінки працездатності proxy-адресів

Вхідний шар складається з вхідних нейронів, на які подаються значення (S_1 – S_8) конвертованих умов працездатності proxy-адреси, кожне значення яких дорівнює 0 або 1. З вхідних нейронів інформація з вагами (синапсами) передається в прихований шар, який складається з одного нейрона і реалізує нелінійну функцію:

$$F = \phi(\sum_{j=1}^{n} w_j \cdot s_j)$$

з сигмоїдальною функцією активації

$$\phi(u) = \frac{1}{1+e^{-\lambda \cdot u}},$$

де $S = \{s_1, s_2, ..., s_n\}$ – вхідні змінні; $W = \{w_1, w_2, ..., w_n\}$ – набір ваг, що утворюють пам'ять нейрона.

Прихований шар, в свою чергу, передає інформацію у вихідний шар, який складається з одного нейрона, в якості функції активації ψ якого обрана бінарна порогова функція:

$$R = \psi(\phi(w,s)) = \begin{cases} 1, \text{ якщо } \phi(w,s) > 0{,}5; \\ 0, \text{ якщо } \phi(w,s) \le 0{,}5. \end{cases}$$

На виході персептрона отримуємо значення працездатності proxy-адреси: 1 – proxy-адреса працездатна, 0 – ні.

Розглянемо вхідні змінні НМ, яких вісім, і умови їх конвертації у відповідні значення.

S_1 – наявність відповіді від ресурсу. Якщо під час тестування proxy-адреси відповідь з ресурсу була отримана, значенню буде присвоєно 1, якщо ні – 0.

S_2 – чи є дана proxy-адреса новою, чи ні. Якщо proxy-адреса нова, то значенню буде присвоєно 1, якщо ні – 0.

S_3 – наявність відповіді під час перевірки в попередній раз. Якщо відповідь була отримана в попередній раз, значенню буде присвоєно 1, в іншому випадку – 0.

S_4 – чи пройшло з початку додання proxy-адреси до бази даних три дні, чи ні. Якщо проміжок часу між датою додання та поточною більше або дорівнює три доби, значенню буде присвоєно 1, якщо ні – 0.

S_5 – наявність proxy-адреси на різних джерелах. Якщо кількість джерел у сумі складає 35 і більше відсотків, значенню буде присвоєно 1, якщо ні – 0.

S_6 – кількість разів, коли було отримано відповідь від ресурсу під час тестової перевірки proxy-адреси. Якщо кількість разів у сумі складає 30% і більше, значенню буде присвоєно 1, якщо ні – 0.

S_7 – кількість разів, коли було отримано відповідь від ресурсу під час відправки запитів клієнтом. Якщо кількість разів у сумі складає 7 і більше відсотків, значенню буде присвоєно 1, в іншому випадку – 0.

S_8 – наявність п'яти поспіль не отриманих відповідей від ресурсу. Якщо умова буде виконана, значенню буде присвоєно 1, якщо ні – 0.

Вихідною змінною НМ є значення працездатності proxy-адреси R: 1 – працездатна, 0 – непрацездатна.

4. Експериментальні дослідження

Щоб перевірити правильність функціонування НМ, було задано набір з 10 прикладів тестових вхідних значень, які наведені в табл. 1, де (N_1 – N_{10}) – номери тестових даних, (S_1 – S_8) – вхідні дані, R – результат роботи НМ.

Таблиця 1

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	R
N_2	0	0	0	0	0	1	1	0	1
N_3	0	0	0	1	0	1	1	0	0
N_4	0	0	0	1	1	1	1	0	1
N_5	0	0	1	1	0	0	0	0	1
N_6	0	1	0	1	0	0	0	0	0
N_7	1	0	0	0	0	0	0	0	1

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	R
N_8	0	0	0	0	0	1	1	1	0
N_9	0	0	1	0	1	1	1	1	0
N_{10}	1	0	0	1	0	0	0	0	1

Для тестування НМ на вхід подавався набір тестових даних ($N_1 - N_{10}$), які вказані в табл. 1. Ваги для кожного входу були обрані випадковими:

$w_1 = 0.6294,\ w_2 = 0.8116,\ w_3 = -0.7460,$
$w_4 = 0.8268,\ w_5 = 0.2647,\ w_6 = -0.8049,$
$w_7 = -0.4430,\ w_8 = 0.0938.$

Після задання ваг виконувалася симуляція НМ, результати якої представлені в табл. 2, де Σ_W – сума ваг кожного вхідного значення, F – результат на виході нейрона прихованого шару, R – вихідне значення НМ.

Таблиця 2

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	Σ_W	F	R
N_1	0	0	0	0	1	1	0	0	3.5146	0.8431	1
N_2	0	0	0	0	0	1	1	0	4.6324	0.9904	1
N_3	0	0	0	1	0	1	1	0	0.0561	0.5140	1
N_4	0	0	0	1	1	1	1	0	-4.4086	0.0120	0
N_5	0	0	1	1	0	0	0	0	4.7822	0.9917	1
N_6	0	1	0	1	0	0	0	0	0.5608	0.6366	1
N_7	1	0	0	0	0	0	0	0	5.1370	0.9942	1
N_8	0	0	0	0	0	1	1	1	-0.5044	0.3765	0
N_9	0	0	1	0	1	1	1	1	4.3895	0.9877	1
N_{10}	1	0	0	1	0	0	0	0	0.5607	0.6366	1

З проведеної симуляції (табл. 2) можна зробити висновки, що її результати не збігаються тестовими вхідними даними (табл. 1). Для отримання потрібних результатів необхідно навчити НМ. З цією метою був складений набір з 30 комбінацій навчальних значень, за якими проводилося навчання НМ методом зворотного розповсюдження похибки. Були отримані нові, більш коректні значення ваг:

$w_1 = 0.6294,\ w_2 = 0.8116,\ w_3 = -0.7460,$
$w_4 = -4.8160,\ w_5 = -4.8074,\ w_6 = -4.8077,$
$w_7 = -4.8076,\ w_8 = -4.8187,$

та проведена симуляція на тестових даних (табл. 1). Результати роботи НМ представлені в табл. 3.

Таблиця 3

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	Σ_W	F	R
N_1	0	0	0	0	1	1	0	0	-3.5812	0.0016	0
N_2	0	0	0	0	0	1	1	0	-6.4568	0.0016	0
N_3	0	0	0	1	0	1	1	0	-11.2547	1.2946e-05	0
N_4	0	0	0	1	1	1	1	0	-14.4831	5.1292e-07	0
N_5	0	0	1	1	0	0	0	0	8.3244	0.9998	1
N_6	0	1	0	1	0	0	0	0	10.5064	1.0000	1
N_7	1	0	0	0	0	0	0	0	15.1222	1.0000	1
N_8	0	0	0	0	0	1	1	1	-23.1957	8.4379e-11	0
N_9	0	0	1	0	1	1	1	1	-13.3018	1.6716e-06	0
N_{10}	1	0	0	1	0	0	0	0	10.3242	1.0000	1

Із результатів симуляції (табл. 3) можна зробити висновки, що НМ ще не обчислює потрібні значення і потребує більшої кількості навчальних наборів. Додатково було використано ще 60 комбінацій навчальних значень, за якими проводилося до навчання НМ і були отримані нові значення ваг:

$w_1 = 15.1222,\ w_2 = 15.3044,\ w_3 = 13.1223,$
$w_4 = -4.7979,\ w_5 = -3.2284,\ w_6 = -3.2284,$
$w_7 = -3.2284,\ w_8 = -16.7389.$

Результати роботи НМ після проведеної симуляції представлені в табл. 4. Видно, що отримані результати (табл. 4), збігаються з тестовими (табл. 1). Таким чином, можна зробити висновок, що НМ успішно завершила навчання.

На основі проведених досліджень по навчанню і тестуванню НМ, що оцінює працездатність proxy-адресів, побудовано сервіс «ProxyClassifier», який приймає масив класів і конверторів умов. Дані класи конвертують поточний стан proxy-адреси в зрозумілі для нього значення – 0 або 1, після чого відбувається процес аналізу proxy-адреси на її працездатність. У разі успішного підтвердження буде повернуто 1, в іншому випадку – 0.

Таблиця 4

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	Σ_W	F	R
N_1	0	0	0	0	1	1	0	0	-1.1027	0.2492	0
N_2	0	0	0	0	0	1	1	0	1.1191	0.7538	1
N_3	0	0	0	1	0	1	1	0	-0.7898	0.3122	0
N_4	0	0	0	1	1	1	1	0	0.6025	0.6462	1
N_5	0	0	1	1	0	0	0	0	5.9900	0.9975	1

N_6	0	1	0	1	0	0	0	0	-1.4840	0.1848	0
N_7	1	0	0	0	0	0	0	0	6.6357	0.9987	1
N_8	0	0	0	0	0	1	1	1	-2.6600	0.0654	0
N_9	0	0	1	0	1	1	1	1	-10.2696	3.4672e-05	0
N_{10}	1	0	0	1	0	0	0	0	3.8676	0.9795	1

На основі результатів досліджень та проведених експериментів був створений додаток, який виконує пошук в Інтернеті ресурсів з proxy-адресами та перевіряє їх на працездатність. В основі додатку використовувалася мова програмування PHP та фреймворк Symfony. Знайдені proxy-адреси зберігаються в базі даних, яка використовується в додатку (MySql). Це пов'язано з тим, що фреймворк Symfony має вбудований функціонал для швидкого підключення і безпосередньої роботи з реляційними базами даних. Даний додаток було реалізовано як команду, яку можна запускати в реальному часі і результати виконання якої заносяться в базу даних. Розроблений додаток може бути модифікований або інтегрований як сервіс в інші додатки.

Висновки

Proxy-сервер залежно від потреб використання забезпечує різні рівні функціональності, безпеки та конфіденційності, і який можна налаштувати як вебфільтр або брандмауер, що захищає комп'ютер від інтернет-загроз. При підключенні до proxy-серверу необхідно визначати його працездатність, тобто можливість відправляти запити на різні ресурси або сервіси та отримувати відповіді (request/response).

Відзначені фактори, які можуть впливати на відправлення запиту, з використанням proxy-адреси, та отримання відповіді від ресурсу, а також розглянуті умови для визначення працездатності proxy-адресів. Було проаналізовано роботу proxy-адресів, proxy-серверів, та умови, при яких можна вважати proxy-адресу працездатною, а при яких ні.

Для створення моделі оцінки працездатності proxy-адресів було застосовано нейромережевий підхід. В якості моделі для оцінки працездатності proxy-адреси використано НМ у вигляді тришарового персептрону. Були сформовані набори навчальних даних, що відповідають стану працездатності proxy-адресів, котрі знаходяться у вільному доступі, і виконане навчання НМ методом зворотного розповсюдження помилки.

Створену НМ було перевірено на визначення стану працездатності proxy-адресів за допомогою тестових наборів даних. Отримані результати показали здатність НМ виявляти працездатні та не працездатні proxy-адреси.

На основі результатів досліджень та проведених експериментів був створений додаток, який виконує пошук в Інтернеті ресурсів з proxy-адресами, перевіряє їх на працездатність та може бути модифікований або інтегрований як сервіс в інші додатки.

Список літератури:

[1] What is a Proxy Server? How does it work? URL: https://www.fortinet.com/resources/cyberglossary/ proxy-server.

[2] *Adrian R.* Compare Different Types of Proxies. Best Proxy Reviews. URL: https://www.bestproxyreviews.com/different-types-of-proxies/#types-of-proxies-based-on-ip-origin.

[3] Anonymous network proxy server. Proxy security or Should I trust Public Proxy Servers. URL: https://comuedu.ru/en/windows/anonymous-network-proxy-server-proxy-security-or-should-i-trust-public-proxy-servers.html.

[4] Transparent proxy. URL:https://www.imperva.com/learn/ddos/transparent-proxy/.

[5] What is an Anonymous Proxy and How Can It Benefit You? URL: https://proxyway.com/guides/what-is-ananonymous-proxy.

[6] The Different Pros and Cons of a Proxy Server URL: https://securityonline.info/the-different-pros-and-cons-of-a-proxy-server/.

[7] How to check if the proxy is operable? URL: https://socproxy.ru/blog/post/proverka-rabotosposobnosti-proksi.

[8] Online proxy server verification URL: https://hidemy.name/en/proxy-checker/.

[9] Implementing health checks by David Yanacek. URL: https://aws.amazon.com/builders-library/implementing-health-checks/.

[10] Timeouts, retries, and backoffs with jitter by Marc Brooker. URL: https://aws.amazon.com/builders-library/timeouts-retries-and-backoff-with-jitter/.

[11] *Stuart J.* Russell and Peter Norvig. Artificial Intelligence: A Modern Approach, 4th US Edition, 2022. – 1151 p.

[12] *Khaikin S.* Neural networks. Full course: A Comprehensive Foundation, 2nd edn, Williams, Moscow, 2006. – 1104 p.

Надійшла до редколегії 24.05.2022