КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.298311
УДК 004.056

Пашорін Валерій Іванович
Приватний вищий навчальний заклад «Європейський університет»
ORCID ID: 0000-0001-6165-1147
v.pashorin@e-u.edu.ua

Остапчук Ілля Сергійович
Приватний вищий навчальний заклад «Європейський університет»
ORCID ID: 0009-0003-0878-4102
ilya.ostapchuk@e-u.edu.ua

Ніколаєвський Олександр Юрійович
Приватний вищий навчальний заклад «Європейський університет»
ORCID ID: 0000-0002-0786-5432
alexander.nikolaievskyi@e-u.edu.ua

Милашенко Віктор Миколайович
Приватний вищий навчальний заклад «Європейський університет»
ORCID ID: 0000-0002-1434-7609
viktor.mylashenko@e-u.edu.ua

МЕТОДИ ТА ЗАСОБИ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ КРИПТОГРАФІЇ

Анотація. У статті розглянуто можливості використання нейронних мереж у криптографії для покращення безпеки обміну ключами шифрування. Автори звертають увагу на зростаючі кіберзагрози та необхідність впровадження новітніх технологій для захисту інформації. Основною метою дослідження було оцінити ефективність нейронної мережі в контексті обміну ключами шифрування, спираючись на досягнення в галузі нейронної криптографії, та запропонувати нові методи захисту від кіберзагроз. Авторами розроблено нейронну модель, яка базується на концепції дерева парності і використовується для обміну ключами шифрування. Підготовчий етап включав ретельний аналіз існуючих моделей нейронних мереж для визначення сумісності з основною метою проєкту. Використовуючи знання, отримані в результаті аналогічних досліджень, автори створили спеціальну нейронну модель, використовуючи мову програмування Python для втілення теоретичних основ у життя. Подальша розробка спеціального тестового середовища сприяла проведенню ретельних оцінок, забезпечуючи стійкість і надійність нейронної мережі за різних умов. Зокрема, запропонована нейромережева модель має потенціал слугувати безпечною альтернативою усталеному методу обміну ключами Діффі-Хеллмана. Крім того, її очікувана стійкість до квантового дешифрування є значним кроком на шляху до зміцнення криптографічних протоколів проти нових загроз в епоху квантових обчислень. Ця модель демонструє високу ефективність навіть при відносно простих конфігураціях. Особливо підкреслюється здатність нейронних мереж швидко адаптуватися до нових загроз, що є критично важливим для підтримки безпеки у мінливих умовах. Дослідження також вказує на те, що глибина синаптичних зв'язків нейронної мережі значно ускладнює зловмисникам завдання зламу ключа, знижуючи шанси на успіх. У висновках наголошується на широких можливостях застосування нейронних мереж у різних сферах, таких як кібербезпека, телекомунікації та фінансове прогнозування. Незважаючи на певні труднощі з алгоритмами та високі вимоги до обчислювальних ресурсів, нейронні мережі мають значний потенціал для покращення криптографічних систем.

Ключові слова: нейронні мережі; криптографія; кібербезпека; шифрування; ключ шифрування.

ВСТУП

Постановка проблеми. В ході цієї роботи було розроблено та реалізовано нейронну модель, побудовану на основі концепції дерева парності. Основною метою було оцінити ефективність нейронної мережі в контексті обміну ключами шифрування, спираючись на досягнення в галузі нейронної криптографії.

Аналіз останніх досліджень і публікацій. Результати дослідження відкривають шлях до розробки інноваційних криптографічних рішень. Використовуючи нейронні мережі, дослідження сприяє створенню нових підходів до шифрування, дешифрування та управління ключами. Ці інновації мають практичне значення, оскільки надають фахівцям з інформаційної безпеки та криптографам різноманітний інструментарій для вирішення складних проблем безпеки, сприяючи створенню більш стійкої та адаптивної криптографічної інфраструктури.

Здатність нейронних мереж до адаптивного навчання, виявлена в ході дослідження, має практичне значення для впровадження адаптивних заходів безпеки. Результати можуть бути застосовані для створення криптографічних систем, які навчаються та адаптуються до мінливих моделей кіберзагроз. Така адаптивність гарантує, що заходи безпеки залишатимуться ефективними в умовах динамічних стратегій атак, пропонуючи проактивний механізм захисту від загроз, що еволюціонують.

Мета статті. Основна мета полягає у вирішенні сучасних викликів, пов’язаних з ландшафтом загроз, що постійно змінюється. Криптографічні методи, хоча і є основою інформаційної безпеки, стикаються з новими вимірами складності у протидії витонченим кіберзагрозам. Використовуючи адаптивність і здатність нейронних мереж до навчання, це дослідження має на меті надати уявлення про інноваційні підходи, які можуть зміцнити криптографічні системи для протидії новим викликам.

Дослідження має на меті заглибитися в динамічну природу нейронних мереж і зрозуміти, як ця адаптивність може бути використана для криптографічних цілей. Нейронні мережі, відомі своєю здатністю навчатися на основі даних і розпізнавати складні закономірності, представляють собою динамічний елемент, який відповідає вимогам криптографічних протоколів, що постійно змінюються. Мета полягає в тому, щоб дослідити, як ця динамічна природа може бути інтегрована в криптографічні методології для підвищення їхньої ефективності та швидкості реагування.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Дерево парності, криптографічна конструкція, що бере свій початок у кодах з виявленням помилок, знайшла практичне застосування для безпечного спільного використання криптографічних ключів між кількома сторонами. За своєю суттю TPM — це архітектура нейронної мережі, що характеризується взаємопов’язаними вузлами, структурованими в шари. Теоретична основа TPM передбачає складні обчислення на кожному вузлі, де вхідні дані перемножуються, агрегуються і проходять через функції активації. Ці обчислення створюють унікальний математичний ландшафт, що дозволяє TPM обробляти складні патерни і вирішувати складні проблеми. Розуміння теоретичних основ TPM має важливе значення для оцінки його обчислювальних можливостей і потенційних застосувань.

ISSN 2663 - 4023

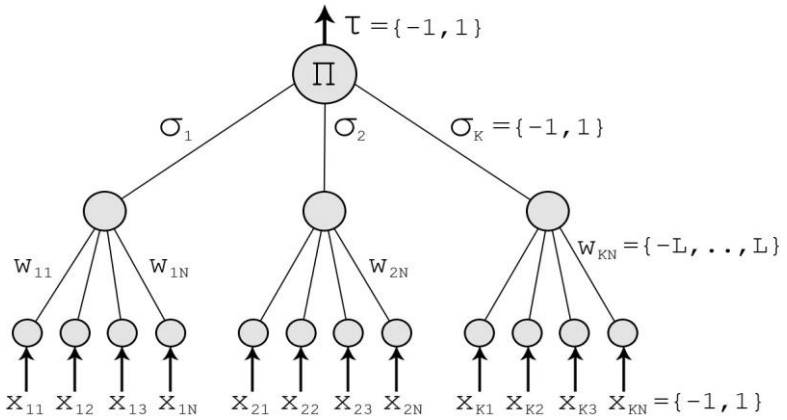

Рис. 1. Графічна структура ТРМ

Структурна складність ТРМ полягає в його багаторівневій архітектурі, як зображено на рис 1. Вхідні вузли, приховані вузли і вихідні вузли утворюють складну мережу, в якій відбуваються обчислення. Кожен рівень робить свій внесок у трансформацію вхідних даних, перетворюючи їх на змістовний вихід. Приховані вузли, зокрема, слугують обчислювальними потужностями нейромережі, втілюючи суть здатності ТРМ вирішувати проблеми. Розгадка цієї структурної складності дозволяє зрозуміти складні механізми, які керують обчислювальними можливостями ТРМ.

Навчання ТРМ включає в себе спеціалізовані алгоритми, призначені для налаштування параметрів мережі, що дозволяє їй навчатися і адаптуватися. Алгоритми навчання, такі як правило навчання Хеббана та алгоритм навчання персептрона, відіграють вирішальну роль у формуванні інтелекту ШНМ. Ці алгоритми сприяють здатності мережі розпізнавати закономірності, вирішувати складні завдання та адаптуватися до мінливого середовища. Розвиток інтелекту в ТРМ передбачає ретельну оркестровку цих алгоритмів, точне налаштування мережі для оптимальної продуктивності.

У порівнянні з алгоритмами, заснованими на теорії чисел, нейронний алгоритм має кілька переваг. По-перше, він надзвичайно простий. Алгоритм навчання по суті діє як лінійний фільтр, що робить його легко реалізованим на апаратному рівні. По-друге, обчислювальні зусилля, необхідні для генерації ключа, є низькими. Генерування ключа довжини N потребує лише порядку N обчислювальних кроків. По-третє, новий ключ можна генерувати для кожного повідомлення або навіть для кожного блоку повідомлення. Немає необхідності зберігати секретну інформацію протягом тривалого періоду.

Однак, згенеровані ключі повинні бути безпечними. Зловмисник E, який записує повідомлення між A і B, не повинен мати можливості обчислити секретний ключ. Методи протидії таким зловмисникам будуть розглянуті нижче.

Незважаючи на те, що ТРМ ґрунтується на теоретичних складнощах, він знаходить свою справжню суть у практичному застосуванні. Його здатність розпізнавати шаблони і вирішувати складні проблеми робить його безцінним в різних областях. У кібербезпеці ТРМ використовується для виявлення аномалій, ідентифікуючи нерегулярні патерни в потоках даних. У телекомунікаціях він оптимізує обробку сигналів, підвищуючи ефективність мереж зв’язку. Крім того, ТРМ знаходить застосування в задачах оптимізації, фінансового прогнозування і навіть у дослідженнях штучного інтелекту, що підкреслює його універсальність і актуальність у реальному світі.

Незважаючи на свою обчислювальну потужність, ТРМ не позбавлений викликів. Складність алгоритмів навчання в поєднанні з потребою в значних обчислювальних ресурсах створюють перешкоди для його широкого впровадження. Однак поточні

дослідження спрямовані на пом'якшення цих проблем, прокладаючи шлях до вдосконаленого впровадження TPM. Майбутнє TPM обіцяє вдосконалення методологій навчання, масштабованість та інтеграцію з новими технологіями. Подолання цих викликів, розкриття повного потенціалу MTM і дослідження незвіданих територій у сфері штучного інтелекту та комп'ютерних наук передбачає вирішення цих проблем.

Теоретичний протокол роботи Дерева парності полягає в тому, що кожна сторона (A і B) використовує власну машину парності (TPM) для синхронізації матриці ваги. Синхронізація TPM машин досягається наступними кроками:

1. Ініціалізація випадкових значень ваги.
2. Виконуємо ці кроки до повної синхронізації:
   2.1. генерування випадкового вхідного вектора X;
   2.2. обчислення значень прихованих нейронів;
   2.3. обчислення значення вихідного нейрона;
   2.4. порівнюємо значення обох машин парності дерева:
      a. виходи однакові: до ваг застосовано одне з відповідних правил навчання
      b. вихідні дані відрізняються: переходимо до пункту 2.1.

Після повної синхронізації (ваги w_{ij} обох TPM машин однакові), A і B можуть використовувати свої ваги як ключі.

Таким чином, Parity Tree є практичним і універсальним рішенням для безпечного розподілу спільних ключів в криптографічних додатках. Незалежно від того, чи застосовується воно для безпечних багатосторонніх обчислень, управління криптографічними ключами або інших сценаріїв, що вимагають спільної генерації ключів, інтеграція Parity Tree підвищує безпеку, надійність і відмовостійкість криптографічних систем. Оскільки дослідники продовжують вивчати інноваційні підходи до розподілу ключів і криптографічних протоколів, Parity Tree є значним внеском у розвиток безпечного і спільного обміну інформацією.

У кожній атаці вважається, що зловмисник E може підслуховувати повідомлення між сторонами A і B, але не має можливості змінити їх, як зображено на рис. 2.

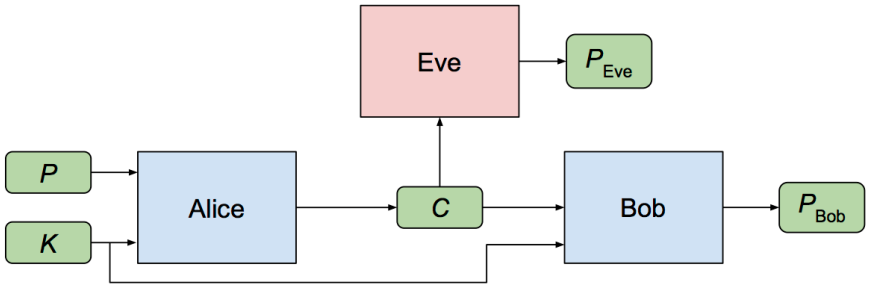

Рис. 2. Діаграма атаки

Щоб здійснити атаку грубою силою, зловмисник повинен протестувати всі можливі ключі (всі можливі значення ваг w_{ij}). При K прихованих нейронів, K×N вхідних нейронів та межі ваг L це дає (2L+1) KN можливостей. Наприклад, конфігурація K = 3, L = 3 і N = 100 дає нам 3*10253 ключових можливостей, що робить атаку неможливою з сучасними комп'ютерними потужностями.

Одна з базових атак може бути здійснена зловмисником, який володіє такою ж машиною парності дерева, що і сторони A та B. Він хоче синхронізувати свою машину парності дерева з цими двома сторонами. На кожному кроці можливі три ситуації:

Output(A) ≠ Output(B): Жодна зі сторін не оновлює свої ваги.

Output(A) = Output(B) = Output(E): Всі три сторони змінюють ваги у своїх машинах паритету.

Output(A) = Output(B) ≠ Output(E): Сторони A і B оновлюють свої машини парності дерев, але зловмисник не може цього зробити.

Через цю ситуацію його навчання відбувається повільніше, ніж синхронізація сторін A і B. Доведено, що синхронізація двох сторін відбувається швидше, ніж навчання зловмисника. Це можна покращити, збільшивши синаптичну глибину L нейронної мережі. Це дає цьому протоколу достатню безпеку, і зловмисник може дізнатися ключ лише з невеликою ймовірністю.

Для звичайних криптографічних систем можна підвищити безпеку протоколу шляхом збільшення довжини ключа. У випадку нейронної криптографії ми покращуємо її шляхом збільшення синаптичної глибини L нейронних мереж. Зміна цього параметра збільшує вартість успішної атаки в геометричній прогресії, в той час як зусилля користувачів зростають в поліноміальній прогресії. Тому злом безпеки нейронного обміну ключами відноситься до класу складності NP.

Стійкість дерева парності до різних атак, як зазначено в попередніх розділах, позиціонує його як безпечний метод обміну ключами, особливо в сценаріях, де підслуховування є першочерговим завданням. Однією з основних переваг є його стійкість до атак грубої сили. Враховуючи величезний простір ключів, що генерується комбінацією прихованих нейронів (K), вхідних нейронів (N) і вагових обмежень (L), кількість можливостей стає астрономічно великою. Наприклад, навіть при відносно скромній конфігурації, як K = 3, L = 3 і N = 100, кількість потенційних ключів досягає величини, яку сучасні обчислювальні потужності вважають нездоланною.

Інтригуючий сценарій виникає, коли зловмисник володіє такою ж машиною парності дерева, як у сторін A і B, і прагне синхронізуватися з ними. У цьому випадку зловмисник стикається з проблемами у підтримці темпу синхронізації сторін A і B. Три можливі ситуації на кожному кроці диктують динаміку оновлення ваг. Зокрема, коли Output(A) ≠ Output(B), жодна зі сторін не оновлює свої ваги. Якщо Output(A) = Output(B) = Output(E), всі три сторони змінюють свої ваги. Однак, коли Output(A) = Output(B) ≠ Output(E), сторони A і B синхронізуються, а зловмисник не може. Це внутрішнє обмеження сповільнює процес навчання зловмисника порівняно з синхронізацією легітимних сторін.

Для підвищення безпеки можна збільшити синаптичну глибину (L) нейронної мережі. Це стратегічне налаштування вводить рівень складності, який значно ускладнює здатність зловмисника ефективно вивчити ключ. Таким чином, безпека протоколу посилюється, а ймовірність успішного вивчення ключа зловмисником зводиться до мінімуму.

У звичайних криптографічних системах підвищення безпеки часто пов’язане зі збільшенням довжини ключа. У сфері нейронної криптографії еквівалентним параметром є синаптична глибина (L). Примітно, що зміна цього параметра призводить до експоненціального зростання вартості успішної атаки, в той час як зусилля, необхідні легальним користувачам, зростають поліноміально. Ця характеристика відносить безпеку нейронного обміну ключами до класу NP-твердості, що вказує на рівень обчислювальної складності, який відповідає важкорозв’язним проблемам.

На закінчення, аналіз підкреслює стійкість дерева парності до потенційних атак, забезпечуючи безпечну основу для обміну ключами в сценаріях, де підслуховування і зловмисні спроби синхронізації викликають занепокоєння. Стратегічне регулювання глибини синаптичних зв’язків додає додатковий рівень безпеки, роблячи нейронний

обмін ключами надійним і складним в обчислювальному плані підходом для безпечного спілкування.

Етап тестування був ретельно виконаний і включав кілька ітерацій з різними розмірами матриць і різними значеннями максимального числа. Для перевірки узгодженості результатів було застосовано ретельне повторення кожного тесту шість разів. Для полегшення цього комплексного тестування було використано бібліотеку Pandas. Pandas, надійна бібліотека з відкритим вихідним кодом для маніпулювання та аналізу даних для Python, виявилася цінним інструментом. Її можливості у створенні високопродуктивних, зручних для користувача структур даних у поєднанні з ефективними інструментами аналізу даних зробили процес роботи зі структурованими даними безперешкодним та ефективним.

Оцінка розбіжностей у налаштуваннях і синхронізації була виражена за шкалою, де 100,0 означає повну відсутність мережі. Ця кількісна метрика забезпечила чіткий і стандартизований вимір продуктивності, що дозволило отримати детальне розуміння поведінки мережі в різних умовах. Комплексне тестування, підтримане універсальністю бібліотеки Pandas, сприяло ретельному аналізу реакції та синхронізації нейронної мережі в різних сценаріях.

Таблиця 1.1

Тест правил оновлення Hebbian з низькими значеннями

	Налаштування мережі			
Ітерація	k: 3, n: 4, l: 6	k: 6, n: 8, l: 12	k: 9, n: 12, l: 18	k: 12, n: 16, l: 24
1	68.06	26.39	-6.10	-20.01
2	100.00	27.60	7.95	-62.50
3	100.00	100.00	-4.24	-39.80
4	43.75	29.51	-2.08	-15.49
5	100.00	18.06	-16.20	-46.18
6	63.19	39.93	-46.76	-51.69
Підсумок	3/6 Зламано	1/6 Зламано	0/6 Зламано	0/6 Зламано

Таблиця 1.2

Тест правил оновлення Hebbian з середніми значеннями

	Налаштування мережі			
Ітерація	k: 15, n: 20, l: 30	k: 18, n: 24, l: 36	k: 21, n: 28, l: 42	k: 24, n: 32, l: 48
1	-82.58	-65.91	-113.25	-173.34
2	-68.64	-119.97	-169.46	-220.14
3	-41.81	-110.20	-162.39	-170.56
4	-43.53	-134.53	-134.44	-121.16
5	-68.61	-124.92	-129.39	-144.98
6	-90.00	-103.67	-124.89	-150.53
Підсумок	0/6 Зламано	0/6 Зламано	0/6 Зламано	0/6 Зламано

ISSN 2663 - 4023

Таблиця 1.3

Тест правил оновлення Hebbian з високими значеннями

	Налаштування мережі	
Ітерація	k: 27, n: 36, l = 54	k: 30, n: 40, l: 60
1	-201.90	-234.14
2	-196.20	-267.10
3	-222.57	-225.72
4	-172.70	-248.35
5	-173.62	-211.30
6	-223.98	-243.28
Підсумок	0/6 Зламано	0/6 Зламано

Аналізуючи результати, наведені в таблиці 1.1, видно, що хакер міг успішно підключитися лише до першого та другого рівнів складності. З підвищенням рівня складності система демонструвала суттєве зростання стійкості, зміцнюючи свій захист від більш витончених спроб вторгнення.

Результати, представлені в таблиці 1.2, підкреслюють надійний захист системи, оскільки спроби хакера підключитися до мережі були постійно зірвані, що призвело до від'ємних значень синхронізації, які вказують на повну реверсію синхронізації, особливо при значеннях нижче –100. Цей надійний механізм захисту підкреслює стійкість мережі до спроб вторгнення.

У таблиці 1.3 хакер зіткнувся з нездоланними бар'єрами, не зумівши встановити з'єднання жодного разу. Постійне виникнення зворотної синхронізації ще більше підкреслює непроникність мережі в цих тестах. Ці результати є найстійкішими серед усіх ітерацій, демонструючи потужний захист системи від різних сценаріїв атак.

Таблиця 2.1

Тест правил оновлення Anti-Hebbian з низькими значеннями

	Налаштування мережі			
Ітерація	k: 3, n: 4, l: 6	k: 6, n: 8, l: 12	k: 9, n: 12, l: 18	k: 12, n: 16, l: 24
1	92.36	23.09	15.12	-15.15
2	75.00	44.79	3.40	-13.67
3	67.36	43.06	4.55	-8.25
4	78.47	55.38	18.98	-3.65
5	61.81	47.22	25.46	-42.14
6	64.58	43.23	29.17	7.07
Підсумок	0/6 Зламано	0/6 Зламано	0/6 Зламано	0/6 Зламано

Таблиця 2.2

Тест правил оновлення Anti-Hebbian з середніми значеннями

	Налаштування мережі			
Ітерація	k: 15, n: 20, l: 30	k: 18, n: 24, l: 36	k: 21, n: 28, l: 42	k: 24, n: 32, l: 48
1	-51.14	-53.36	-113.85	-143.95
2	-42.75	-40.49	-137.17	-162.99
3	-19.72	-39.27	-123.99	-152.19
4	-53.17	-44.81	-127.92	-157.01
5	-24.97	-102.41	-141.94	-110.43
6	-44.94	-58.22	-126.32	-82.04
Підсумок	0/6 Зламано	0/6 Зламано	0/6 Зламано	0/6 Зламано

Таблиця 2.3

Тест правил оновлення Anti-Hebbian з високими значеннями

	Налаштування мережі	
Ітерація	k: 27, n: 36, l: 54	k: 30, n: 40, l: 60
1	-125.91	-263.96
2	-156.89	-172.15
3	-165.47	-223.17
4	-159.07	-211.35
5	-136.00	-159.49
6	-208.38	-122.60
Підсумок	0/6 Зламано	0/6 Зламано

Порівняльний аналіз, представлений у таблицях 2.1 – 2.3, підкреслює значну різницю між механізмами навчання Hebbian та Anti-Hebbian. Зокрема, середні мінімальні значення синхронізації в Anti-Hebbian нижчі, що свідчить про вищий рівень безпеки. Незважаючи на це, основний висновок полягає в тому, що навчання Anti-Hebbian майже унеможливлює випадкові вгадування або спроби зовнішньої синхронізації, які можуть призвести до успіху.

Таким чином, виходячи з цієї оцінки, анти-геббівське навчання виявляється більш безпечним варіантом з-поміж двох. Його здатність протистояти випадковим вгадуванням і спробам зовнішньої синхронізації сприяє підвищенню рівня загальної безпеки криптографічних додатків. Цей висновок підкреслює важливість вибору відповідного механізму навчання для нейронних мереж у криптографічних контекстах, де безпека має першочергове значення.

Різниця між геббіанськими та антигеббіанськими правилами оновлення є ключовим аспектом у галузі механізмів навчання нейронних мереж. Ці правила визначають принципи, що керують синаптичною пластичністю, підкреслюючи різні аспекти взаємозв’язку між активаціями нейронів і відповідними коригуваннями синаптичних ваг.

Правило оновлення Хеббіана працює за принципом синаптичного підсилення на основі корельованої активності. Воно стверджує, що коли нейрони демонструють

одночасну і корельовану активацію, сила їхнього синаптичного зв'язку повинна збільшуватися. Це підкріплення, описане фразою «клітини, що стріляють разом, зв'язуються разом», лежить в основі асоціативного навчання та формування пам'яті. Геббіанське навчання сприяє створенню функціональних нейронних ланцюгів через посилення зв'язків, які узгоджуються з когерентними патернами стрільби.

На противагу цьому, антигеббіанське правило оновлення втілює концепцію послаблення синаптичних зв'язків у відповідь на некорельовану або розрізнену в часі активність нейронів. Суть анти-геббіанського навчання полягає в тому, що «клітини, які працюють не синхронно, втрачають свій зв'язок». Це правило вводить елемент конкуренції, вибірково послаблюючи зв'язки між нейронами, які не демонструють корельованих патернів стрільби. Анти-геббівське навчання слугує механізмом стабільності мережі, запобігаючи перезбудженню і сприяючи точності роботи мереж пам'яті.

Фундаментальна відмінність полягає у впливі цих правил на динаміку навчання в нейронних мережах. Геббіанське навчання сприяє асоціативному навчанню, формуванню пам'яті та створенню когерентних нейронних репрезентацій. І навпаки, антигеббіанське навчання доповнює цей процес, полегшуючи вибіркове відсікання менш релевантних або тимчасово роз'єднаних зв'язків, сприяючи стабільності мережі та запобігаючи виникненню непередбачуваного збудження.

Взаємодія між геббіанським і антигеббіанським навчанням є невід'ємною частиною мережевої пластичності та гомеостазу. У той час як геббіанське навчання адаптує синаптичні зв'язки до повторюваних патернів активації, антигеббіанське навчання діє як регуляторний механізм, забезпечуючи баланс у мережі шляхом усунення менш релевантних зв'язків. Ця делікатна взаємодія сприяє структурній і функціональній динаміці нейронних мереж, формуючи їхню здатність адаптуватися до мінливих умов, зберігаючи при цьому стабільність.

Отже, різниця між геббіанськими та антигеббіанськими правилами оновлення полягає у відповідних підходах до синаптичної пластичності. Геббіанське навчання посилює корельовану активність, сприяючи асоціативному навчанню та формуванню пам'яті, тоді як антигеббіанське навчання послаблює некорельовані зв'язки, сприяючи стабільності та гомеостазу мережі. Цей тонкий взаємозв'язок між механізмами підкріплення та послаблення є ключовим для розуміння фундаментальних принципів навчання нейронних мереж.

На додаток до надійного захисту, який забезпечують Anti-Hebbian та Random-Walk за різних умов, варто підкреслити адаптивність цих правил до динамічних ландшафтів кібербезпеки. Властива Anti-Hebbian здатність підтримувати безпеку на мінімальному рівні робить його надійним механізмом захисту від потенційних загроз, навіть у сценаріях, коли хакерська машина демонструє розширені можливості.

Більше того, правило Random-Walk є найбільш оптимальним вибором завдяки своїй здатності забезпечувати надійний захист не тільки на низьких, але і на високих налаштуваннях. Ця подвійна здатність забезпечує стійкий захист, пристосовуючись до потенційних коливань мережевих умов і кіберзагроз. Адаптивність Random-Walk стає особливо важливою, коли стикаєшся з витонченими атаками або непередбачуваними вразливостями, оскільки вона підтримує безпечне з'єднання навіть в умовах мінливого ландшафту загроз.

Крім того, ефективність Hebbian на більш високих налаштуваннях, особливо в досягненні чудової зворотної синхронізації, підкреслює його придатність для сценаріїв, де передові заходи безпеки мають першочергове значення. Використовуючи Hebbian в таких умовах, організації можуть покращити загальний стан кібербезпеки та зменшити

ризик складних атак, які можуть спробувати використати вразливості на підвищених налаштуваннях.

На завершення, всебічний аналіз правил Hebbian, Anti-Hebbian та Random-Walk пропонує нюансований підхід до кібербезпеки. У той час як Hebbian демонструє відмінні результати в специфічних сценаріях з високими налаштуваннями, Anti-Hebbian і Random-Walk є універсальними варіантами, здатними забезпечити надійний захист в різних умовах. Стратегічна комбінація цих правил може створити стійку систему захисту, що гарантує цілісність і конфіденційність з'єднань в умовах еволюції кіберзагроз і потенційних досягнень супротивника.

Правило випадкових блукань є особливим механізмом у сфері навчання нейронних мереж, який вносить стохастичний елемент у налаштування синаптичних ваг. На відміну від детермінованих правил, що керуються кореляційними патернами, правило Random-Walk охоплює непередбачуваність і випадковість у дослідженні простору синаптичних ваг. Цей науковий огляд має на меті висвітлити фундаментальні принципи та наслідки застосування правила випадкових блукань у нейронних мережах.

По суті, правило оновлення Random-Walk вносить певний рівень невизначеності в коригування синаптичних ваг. Замість того, щоб покладатися на явну кореляцію або антикореляцію між активаціями нейронів, правило Random-Walk допускає ймовірнісні зміни. Ця стохастичність дозволяє мережі проходити через цілий ряд станів, що потенційно полегшує відкриття нових конфігурацій, які можуть бути не одразу очевидними за допомогою детермінованих правил.

Філософія, що лежить в основі правила Random-Walk, схожа на стратегію випадкового пошуку в синаптичному ваговому просторі. Це дослідження узгоджується з уявленням про те, що мережа, завдяки імовірнісним налаштуванням, може уникати локальних оптимумів і досліджувати регіони, які можуть призвести до більш оптимальних конфігурацій. Цей елемент випадковості вносить невід'ємну адаптивність і гнучкість, дозволяючи нейронній мережі реагувати на різноманітні стимули навколишнього середовища.

З практичної точки зору, правило оновлення Random-Walk може бути застосоване в сценаріях, де певний ступінь дослідження і непередбачуваності є перевагою. Воно може сприяти подоланню локальних мінімумів в процесі навчання, дозволяючи мережі досліджувати альтернативні рішення і потенційно сходитися до більш глобально оптимальних конфігурацій. Така адаптивність особливо цінна в динамічних середовищах, де детерміновані правила можуть не впоратися з мінливими патернами або непередбачуваними викликами.

Впровадження випадковості в синаптичні вагові коригування, що полегшується правилом випадкових блукань, узгоджується з ширшою концепцією стохастичної оптимізації в нейронних мережах. Ця концепція визнає, що включення випадковості в процеси навчання може бути потужною стратегією для уникнення локальних оптимумів і досягнення більш надійних і адаптивних рішень.

Отже, правило випадкового блукання в нейронних мережах є відходом від детермінованих механізмів навчання, враховуючи стохастичність і непередбачуваність. Це правило вносить певний рівень випадковості в синаптичні коригування ваг, сприяючи дослідженню вагового простору і потенційно приводячи до відкриття більш оптимальних конфігурацій. Правило оновлення Random-Walk ілюструє адаптивність і гнучкість, які стохастичні елементи вносять у складну динаміку навчання в нейронних мережах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Машина дерева парності, як нейромережева архітектура, має багатообіцяючі характеристики для криптографічних додатків. Використання TPM в протоколах обміну ключами вносить динамічний елемент в процес, підвищуючи стійкість до потенційних загроз і вразливостей. Дослідження спрямоване на розуміння тонкощів TPM, їх здатності адаптуватися до мінливих моделей даних та їх потенціалу для посилення безпеки обміну криптографічними ключами.

Основна увага в дослідженні приділяється вирішенню сучасних проблем, з якими стикаються традиційні механізми обміну ключами. Включаючи TPM, дослідження має на меті запропонувати інноваційні рішення, які виходять за рамки традиційних парадигм. Це передбачає не лише захист процесу обміну ключами від атак зловмисників, але й оптимізацію обчислювальної ефективності криптографічних операцій.

В майбутньому, дослідження передбачає можливі розробки, які виходять за рамки машини дерева парності для обміну криптографічними ключами. Однією з важливих перспектив є дослідження справжніх нейронних методів шифрування/дешифрування. Ця розробка спрямована на створення симбіозу між існуючими машинами обміну ключами і справжніми нейронними методами шифрування/дешифрування.

Траєкторія криптографічних досліджень є динамічною, позначеною безперервним розвитком, спрямованим на вирішення нових викликів і використання нових технологій. Якщо уявити майбутнє реалізованого прототипу, то можна виділити декілька потенційних модернізацій, головною з яких є інтеграція передових архітектур, таких як машина парності дерева з векторною оцінкою (VV-TPM). Крім того, вдосконалення стратегій управління ключами, диверсифікація криптографічних алгоритмів та міркування щодо масштабованості є перспективними напрямками для посилення криптографічних можливостей прототипу.

Еволюція від традиційної машини парності дерева (TPM) до машини парності дерева з векторним значенням (VV-TPM) являє собою глибокий стрибок у розвитку архітектури нейронних мереж. У той час як звичайний TPM чудово відтворює складні патерни за допомогою ієрархічних структур, VV-TPM розширює ці можливості за рахунок введення векторних значень виходів. Таке доповнення дозволяє більш детально представляти інформацію, підвищуючи потенціал для обробки багатовимірних даних і складних взаємозв’язків у криптографічних контекстах.

Впровадження VV-TPM може підвищити стійкість до сучасних криптографічних атак, оскільки векторні значення на виході забезпечують багатше кодування шаблонів. Крім того, потенціал розпаралелювання обчислень у векторних операціях може підвищити обчислювальну ефективність криптографічних процесів. Тим не менш, інтеграція VV-TPM вимагає ретельної переоцінки правил навчання, механізмів оновлення ваг і стратегій синхронізації для адаптації до розширеної розмірності векторних виходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nikolayevsky, O. Yu., Skliarenko, O. V., & Sydorchuk, A. (2019). Analysis and comparison of face detection Apis. *Telecommunications and information technologies, 4(65),* 121–133
2. Kolodinska, Y. (2024). The use of artificial intelligence to manage the processes of creation and development of IT projects. *Artificial intelligence in science and education (AISE 2024),* 101–102.

3. Troyan, K. M., & Skliarenko, O. V. (2023). Practical cases and prospects for the development of artificial intelligence technologies. *Digital transformation in the economy, management and business. Problems of science, practice and education: Collection of materials of the XXVIII International Scientific and Practical Conference. European University Press*, 66–68.
4. Skliarenko, O. V., & Nikolayevsky, O. Y. (2021). Biometric security systems: face recognition. *Topical issues of cybersecurity and information protection. Proceedings of the VII International Scientific and Practical Conference, European University Press*, 85–87.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Valeryi Pashorin
Private Higher Educational Establishment "European University"
ORCID ID: 0000-0001-6165-1147
v.pashorin@e-u.edu.ua

Ilya Ostapchuk
Private Higher Educational Establishment "European University"
ORCID ID: 0009-0003-0878-4102
ilya.ostapchuk@e-u.edu.ua

Oleksandr Nikolayevsky
Private Higher Educational Establishment "European University"
ORCID ID: 0000-0002-0786-5432
alexander.nikolaievskyi@e-u.edu.ua

Viktor Milashenko
Private Higher Educational Establishment "European University"
ORCID ID: 0000-0002-1434-7609
viktor.mylashenko@e-u.edu.ua

METHODS AND MEANS OF USING NEURAL NETWORKS FOR CRYPTOGRAPHY

Abstract. The article discusses the possibilities of using neural networks in cryptography to improve the security of encryption key exchange. The authors draw attention to the growing cyber threats and the need to implement the latest technologies to protect information. The main goal of the study was to evaluate the effectiveness of a neural network in the context of encryption key exchange, based on advances in neural cryptography, and to propose new methods of protection against cyber threats. The authors have developed a neural model based on the concept of a parity tree, which is used to exchange encryption keys. The preparatory stage included a thorough analysis of existing neural network models to determine compatibility with the main goal of the project. Using the knowledge gained from similar studies, the authors created a special neural model using the Python programming language to implement the theoretical foundations. The subsequent development of a special test environment facilitated thorough evaluations, ensuring the stability and reliability of the neural network under various conditions. In particular, the proposed neural network model has the potential to serve as a secure alternative to the well-established Diffie-Hellman key exchange method. In addition, its expected resistance to quantum decryption is a significant step towards strengthening cryptographic protocols against new threats in the era of quantum computing. This model demonstrates high efficiency even with relatively simple configurations. The ability of neural networks to quickly adapt to new threats is particularly emphasized, which is critical to maintaining security in a changing environment. The study also indicates that the depth of synaptic connections in a neural network makes it much more difficult for attackers to crack a key, reducing the chances of success. The conclusions emphasize the wide range of applications of neural networks in various fields, such as cybersecurity, telecommunications, and financial forecasting. Despite certain difficulties with algorithms and high requirements for computing resources, neural networks have significant potential for improving cryptographic systems.

Keywords: neural networks; cryptography; cybersecurity; encryption; encryption key.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Nikolayevsky, O. Yu., Skliarenko, O. V., & Sydorchuk, A. (2019). Analysis and comparison of face detection Apis. *Telecommunications and information technologies, 4(65)*, 121–133
2. Kolodinska, Y. (2024). The use of artificial intelligence to manage the processes of creation and development of IT projects. *Artificial intelligence in science and education (AISE 2024)*, 101–102.
3. Troyan, K. M., & Skliarenko, O. V. (2023). Practical cases and prospects for the development of artificial intelligence technologies. *Digital transformation in the economy, management and business. Problems of*

science, practice and education: Collection of materials of the XXVIII International Scientific and Practical Conference. European University Press, 66–68.

4. Skliarenko, O. V., & Nikolayevsky, O. Y. (2021). Biometric security systems: face recognition. *Topical issues of cybersecurity and information protection. Proceedings of the VII International Scientific and Practical Conference, European University Press,* 85–87.