ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

УДК 004.056.53:004.8:004.382 DOI: 10.20998/2411-0558.2026.02.06

О. Ю. ЗАКОВОРОТНИЙ, д-р техн. наук, проф., НТУ "ХПІ",
А. В. ХУЛАП, асп., НТУ "ХПІ"

ОПТИМІЗАЦІЯ ОБЧИСЛЕНЬ НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ У СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ НА МІКРОКОНТРОЛЕРНИХ ПЛАТФОРМАХ

У роботі розглянуто проблему застосування нейромережевих методів для виявлення мережевих вторгнень у комп'ютерних системах Інтернету речей за умов обмежених обчислювальних ресурсів вбудованих пристроїв. У таких системах аналіз мережевого трафіку, розпізнавання аномальних подій та забезпечення безпеки повинні виконуватися у режимі, наближеному до реального часу, безпосередньо на периферійних вузлах інфраструктури граничних обчислень. Використання моделей на основі нейронних мереж у подібних вбудованих системах ускладнюється значними обчислювальними витратами під час виконання обчислень, що обмежує можливість їх реалізації на мікроконтролерних платформах комп'ютерних систем.

Метою роботи є підвищення ефективності виконання нейромережевих алгоритмів виявлення вторгнень шляхом оптимізації обчислювальних процесів для вбудованих систем. У роботі запропоновано підхід до оптимізації обчислень нейромережевих моделей, що базується на використанні цілочисельного fixed-point представлення параметрів та табличної апроксимації сигмоїдної функції активації. Для експериментальної перевірки ефективності підходу сформовано компактні нейромережеві моделі для задачі класифікації мережевого трафіку на основі загальнодоступних наборів даних NSL-KDD та UNSW-NB15. Реалізацію моделей виконано мовою C та досліджено на мікроконтролерній платформі STM32L476, що використовується у вбудованих комп'ютерних системах.

Проведені експериментальні дослідження показали, що застосування запропонованих методів дозволяє суттєво зменшити час виконання нейромережевих обчислень на вбудованих пристроях при збереженні прийнятного рівня точності класифікації мережевого трафіку. Отримані результати підтверджують доцільність використання оптимізованих нейромережевих моделей у системах виявлення вторгнень для комп'ютерних систем Інтернету речей та вбудованих систем, що функціонують у режимі реального часу. Іл.: 4. Табл.: 2. Бібліогр.: 17 назв.

Ключові слова: нейронна мережа, модель, Інтернет речей, мережевий трафік, розпізнавання, комп'ютерні системи, вбудовані системи, граничні обчислення, системи реального часу, події, безпека.

Постановка проблеми. Стрімкий розвиток технологій Інтернету речей (IoT) призводить до значного збільшення кількості підключених пристроїв, які взаємодіють у комп'ютерних мережах та обмінюються великими обсягами даних. Такі системи широко застосовуються у промисловості, транспорті, енергетиці, системах розумного міста та інших галузях, що підвищує вимоги до забезпечення їх інформаційної безпеки. Однією з ключових проблем функціонування IoT-систем є виявлення мережевих атак, які можуть призводити до порушення роботи пристроїв, втрати або компрометації даних та несанкціонованого доступу до мережевих ресурсів [1, 2].

Для вирішення цієї задачі широко застосовуються системи виявлення вторгнень (Intrusion Detection Systems, IDS), що здійснюють аналіз мережевого трафіку з метою ідентифікації аномальної або шкідливої активності. Останніми роками значного поширення набули методи машинного навчання та нейронних мереж, які дозволяють підвищити точність виявлення атак завдяки автоматичному аналізу складних закономірностей у мережевих даних [3, 4].

Разом із тим використання нейронних мереж у системах Інтернету речей пов'язане з рядом суттєвих обмежень. Більшість IoT-пристроїв базуються на малоресурсних мікроконтролерах, які мають обмежені обчислювальні можливості, обсяг оперативної пам'яті та енергетичні ресурси. У таких умовах застосування традиційних нейромережевих моделей може бути ускладненим через значну обчислювальну складність процесу обчислення [5].

Таким чином, актуальною науково-технічною задачею є підвищення ефективності виконання нейромережевих алгоритмів виявлення вторгнень у системах Інтернету речей шляхом оптимізації обчислювальних процесів та адаптації моделей до умов обмежених апаратних ресурсів.

Аналіз літератури. Проблема виявлення мережевих вторгнень у комп'ютерних мережах активно досліджується протягом останніх десятиліть. З розвитком технологій Інтернету речей ця задача набула нової

актуальності через значне збільшення кількості мережевих пристроїв, обмеженість їхніх обчислювальних ресурсів та підвищені вимоги до швидкодії систем аналізу мережевого трафіку.

У роботах [6, 7] розглянуто загальні підходи до побудови систем виявлення вторгнень на основі аналізу мережевого трафіку. У цих дослідженнях показано, що використання методів машинного навчання дозволяє підвищити ефективність виявлення атак порівняно з традиційними сигнатурними підходами. Разом із тим зазначається, що ефективність таких систем значною мірою залежить від обраних моделей машинного навчання та наборів вхідних ознак.

Значна кількість сучасних досліджень присвячена застосуванню нейронних мереж для виявлення вторгнень. У роботах [8 – 10] досліджено використання глибоких нейронних мереж для класифікації мережевого трафіку та виявлення аномальної поведінки. Отримані результати демонструють високу точність класифікації, проте такі моделі зазвичай характеризуються значною обчислювальною складністю та потребують суттєвих апаратних ресурсів для виконання.

Окремий напрям досліджень пов’язаний із розробленням систем виявлення вторгнень, орієнтованих на застосування у середовищі Інтернету речей. У роботах [11, 12] запропоновано підходи до побудови IDS для IoT-систем із використанням методів машинного навчання та аналізу мережевого трафіку. Автори відзначають, що основною проблемою таких систем є необхідність забезпечення балансу між точністю класифікації та обчислювальною складністю алгоритмів.

У роботах [13, 14] досліджуються підходи до зменшення обчислювальної складності нейромережевих моделей для їх використання на периферійних пристроях (edge devices). Запропоновані методи включають спрощення архітектури нейронних мереж, зменшення кількості параметрів та оптимізацію процедур обчислення. Проте більшість таких підходів орієнтована на використання спеціалізованих бібліотек або апаратних прискорювачів, що обмежує можливість їх застосування на малоресурсних мікроконтролерах.

У попередніх роботах авторів [15 – 17] було проаналізовано існуючі моделі виявлення вторгнень та досліджено можливість оптимізації обчислень нейронних мереж за рахунок використання цілочисельної

арифметики. Результати цих досліджень показали, що застосування таких підходів може суттєво зменшити обчислювальні витрати при виконанні нейромережевих алгоритмів.

Таким чином, аналіз сучасних досліджень показує, що існуючі підходи до виявлення мережевих вторгнень або забезпечують високу точність за рахунок використання складних моделей, або орієнтовані на обчислювально потужні платформи. При цьому питання ефективної реалізації нейромережевих алгоритмів виявлення вторгнень на малоресурсних мікроконтролерних платформах залишається недостатньо дослідженим.

Метою статті є підвищення ефективності застосування нейромережевих методів для виявлення мережевих вторгнень у системах Інтернету речей шляхом зменшення обчислювальної складності процесу обчислення та адаптації нейромережевих моделей до виконання на вбудованих мікроконтролерних платформах з обмеженими апаратними ресурсами.

Для досягнення цієї мети запропоновано підхід до оптимізації обчислень нейронної мережі, що базується на використанні компактної архітектури моделі, скороченого набору інформативних ознак мережевого трафіку та переході до цілочисельного fixed-point представлення параметрів і обчислювальних операцій. Ефективність запропонованого підходу підтверджено експериментальними дослідженнями на мікроконтролерній платформі STM32L476.

Метод оптимізації обчислень нейромережевих моделей. Запропонований у роботі підхід спрямований на забезпечення можливості використання нейромережевих моделей для виявлення мережевих вторгнень безпосередньо на периферійних пристроях Інтернету речей. Основною проблемою таких систем є обмежені обчислювальні ресурси мікроконтролерних платформ, що ускладнює використання традиційних реалізацій нейронних мереж, орієнтованих на застосування чисел з плаваючою комою та обчислювально складних функцій активації.

У запропонованому підході аналіз мережевого трафіку виконується безпосередньо на edge-пристрої. Вхідними даними для нейромережевої

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

моделі є параметри мережевого трафіку, отримані під час аналізу мережевих пакетів або потоків даних. Для зменшення обчислювальної складності використовується компактна архітектура повнозв'язної нейронної мережі з одним прихованим шаром та обмеженою кількістю нейронів.

З метою зменшення розмірності вхідних даних використовується скорочений набір інформативних параметрів мережевого трафіку. На основі аналізу інформативності ознак було сформовано компактний набір із десяти параметрів, що характеризують основні властивості мережевого з'єднання. Використання такого набору дозволяє зменшити кількість вхідних параметрів нейронної мережі та відповідно знизити обчислювальну складність процесу обчислення.

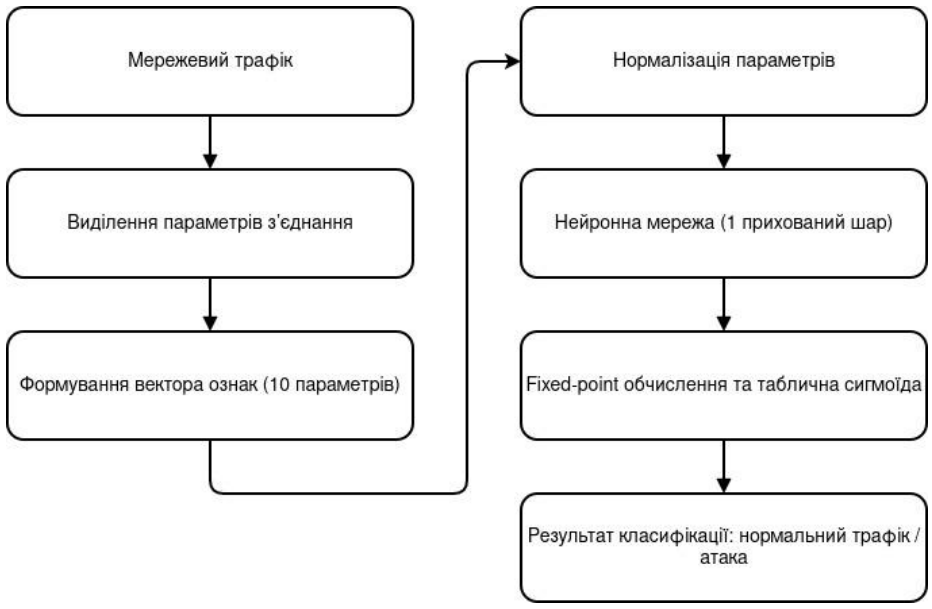

Рис. 1. Узагальнена схема обробки мережевого трафіку в системі виявлення вторгнень

Для подальшого зменшення обчислювальних витрат у роботі запропоновано використовувати цілочисельне представлення параметрів нейронної мережі у форматі fixed-point. Такий підхід дозволяє виконувати основні арифметичні операції з використанням цілочисельної

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

арифметики, що забезпечує суттєве скорочення часу виконання обчислень на мікроконтролерних платформах.

Крім того, для обчислення функції активації використовується таблична апроксимація сигмоїдальної функції. Значення функції попередньо обчислюються та зберігаються у вигляді таблиці, що дозволяє замінити обчислення експоненціальної функції операцією звернення до масиву.

Узагальнена схема оброблення даних у запропонованому підході наведена на рис. 1.

Експериментальне дослідження. Для оцінювання ефективності запропонованого підходу було проведено експериментальні дослідження з використанням загальнодоступних наборів даних для задачі виявлення мережевих вторгнень. Зокрема, у роботі використано набори даних NSL-KDD та UNSW-NB15, які широко застосовуються у дослідженнях систем виявлення вторгнень.

З метою зменшення обчислювальної складності моделі було використано скорочений набір із десяти параметрів мережевого трафіку, сформований на основі аналізу інформативності ознак. На основі цих параметрів було сформовано нейромережеві моделі з одним прихованим шаром, що містив 8, 16 та 32 нейрони. Навчання моделей виконувалося у середовищі Brain.js з використанням тренувальних підмножин відповідних наборів даних.

Після навчання параметри нейронних мереж були експортовані та використані для реалізації алгоритмів розрахунку мовою C. Для дослідження ефективності обчислень було реалізовано три варіанти виконання нейромережевої моделі:

- реалізацію з використанням чисел з плаваючою комою (float32);
- реалізацію з використанням цілочисельного fixed-point представлення (32-bit);
- реалізацію з використанням 16-бітного fixed-point представлення.

У реалізації нейромережевого алгоритму використано цілочисельне представлення чисел у форматі fixed-point Q(m,n). У такому представленні число з фіксованою комою зберігається у вигляді цілого значення, де *m* бітів відводиться для цілої частини, а *n* бітів - для дробової. Використання

такого формату дозволяє виконувати більшість арифметичних операцій значно швидше порівняно з операціями над числами з плаваючою комою.

Зокрема, операції додавання та віднімання виконуються так само, як і для звичайних цілих чисел. Операція множення виконується як звичайне цілочисельне множення з подальшим зсувом результату на n бітів. Крім того, використання fixed-point представлення дозволяє уникнути додаткових операцій перетворення між форматами чисел з плаваючою комою та цілочисельними значеннями, що додатково зменшує обчислювальні витрати.

Для визначення параметрів формату $Q(m, n)$ було проведено аналіз максимального значення сумарного сигналу на вході нейронів. Оскільки всі вхідні параметри нейронної мережі нормалізуються до діапазону [0, 1], максимальне можливе значення часткової суми визначається сумою вагових коефіцієнтів та зміщення нейрона. На основі отриманих значень було визначено необхідну кількість бітів для представлення цілої частини числа. Значення параметра m визначалося таким чином, щоб забезпечити представлення максимально можливого значення часткової суми нейрона без переповнення, тоді як кількість дробових бітів n обиралася виходячи з розрядності використовуваного типу даних.

Результати оцінювання максимальних значень сум на нейронах для використаних наборів даних наведено у табл. 1. Використання такого підходу дозволяє забезпечити достатній динамічний діапазон для обчислень нейронної мережі та уникнути переповнення під час виконання операцій fixed-point арифметики.

Таблиця 1

Визначення параметрів fixed-point формату Q(m,n)

Набір даних	**Максимальна часткова сума**	**Необхідна кількість біт для цілої частини (m)**	**Формат $Q(m,n)$**
NSL-KDD	555.06	9	Q(9,22)
UNSW-NB15	2153.06	12	Q(12,19)

Експериментальні дослідження проводилися на мікроконтролерній платформі STM32L476, побудованій на основі процесорного ядра ARM Cortex-M4 з тактовою частотою 80 МГц. Програмна реалізація алгоритмів

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

виконувалася мовою C у середовищі STM32CubeIDE, а конфігурація апаратної платформи здійснювалася за допомогою STM32CubeMX.

Час виконання нейромережевого алгоритму вимірювався під час оброблення скороченого тестового набору даних, що містив 8000 записів. Для цього у програмі використовувався нескінченний цикл, у якому виконувався запуск процедури тестування нейромережевої моделі, а тривалість виконання вимірювалася за допомогою осцилографа через зміну стану світлодіода на відладочній платі.

На рис. 2 наведено приклад вимірювання часу виконання алгоритму за допомогою осцилографа.

Результати вимірювання часу виконання нейромережевого алгоритму для різних варіантів реалізації, а також відповідні значення точності класифікації наведено у табл. 2. Отримані результати показують, що використання fixed-point арифметики дозволяє суттєво зменшити час виконання обчислень, при цьому зменшення точності класифікації є незначним. Для набору даних NSL-KDD використання 32-бітного fixed-point представлення дозволяє зменшити час виконання алгоритму приблизно на 23 %, тоді як зниження точності класифікації не перевищує 0,6 %. Для набору даних UNSW-NB15 використання 16-бітного fixed-point представлення виявилося неможливим через недостатню кількість бітів для дробової частини, що призводить до значної деградації точності.

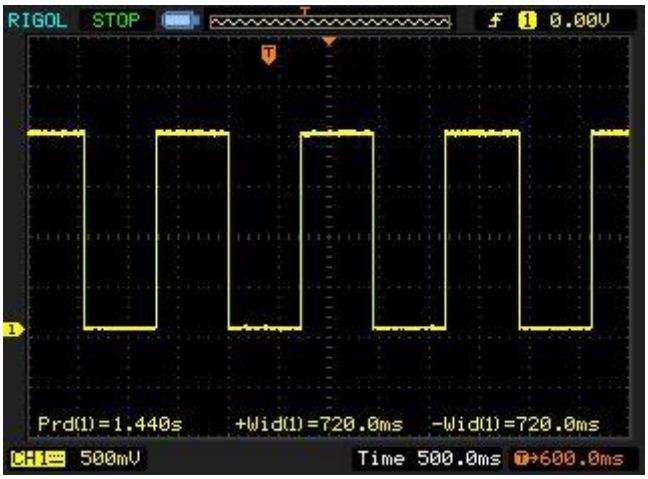

Рис. 2. Приклад вимірювання часу виконання нейромережевого алгоритму на мікроконтролері STM32

Залежність часу виконання алгоритму від кількості нейронів у прихованому шарі для різних типів арифметики наведено на рис. 3.

Крім того, було проведено порівняльний аналіз прискорення обчислень при використанні fixed-point арифметики відносно реалізації з числами з плаваючою комою. Відповідні результати наведено на рис. 4.

Таблиця 2

Час виконання нейромережевого алгоритму для різних варіантів реалізації.

Набір даних	**Нейрони**	**float32 час, мс**	**float32 acc**	**int32 час, мс**	**int32 acc**	**int16 час, мс**	**int16 acc**
NSL-KDD	8	316	0,81	268	0,82	240	0,81
NSL-KDD	16	580	0,80	420	0,80	364	0,76
NSL-KDD	32	1100	0,81	720	0,81	610	0,80
UNSW-NB15	8	328	0,74	264	0,75	240	0,59
UNSW-NB15	16	600	0,76	416	0,76	364	0,59
UNSW-NB15	32	1140	0,76	720	0,76	610	0,50

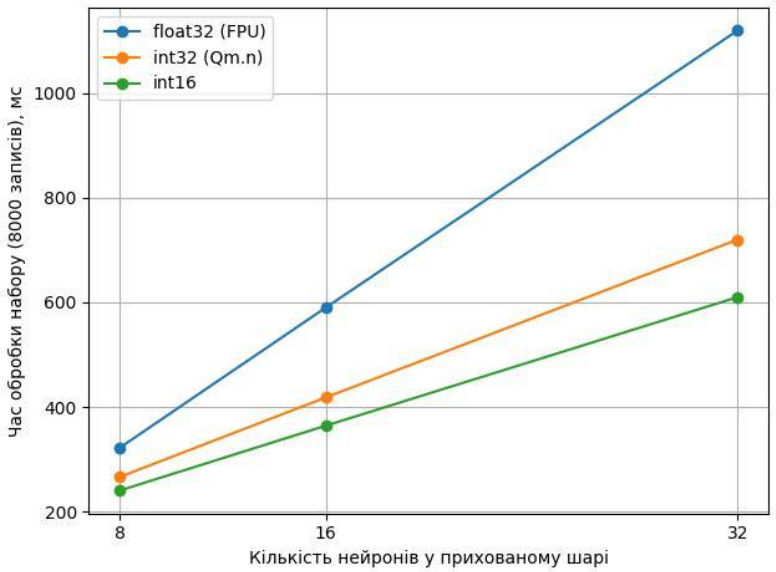

Рис. 3. Залежність часу виконання нейромережевого алгоритму від кількості нейронів у прихованому шарі

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

Проведені експериментальні дослідження показали, що використання запропонованого підходу дозволяє скоротити час виконання нейромережевого алгоритму у декілька разів без суттєвої втрати точності класифікації.

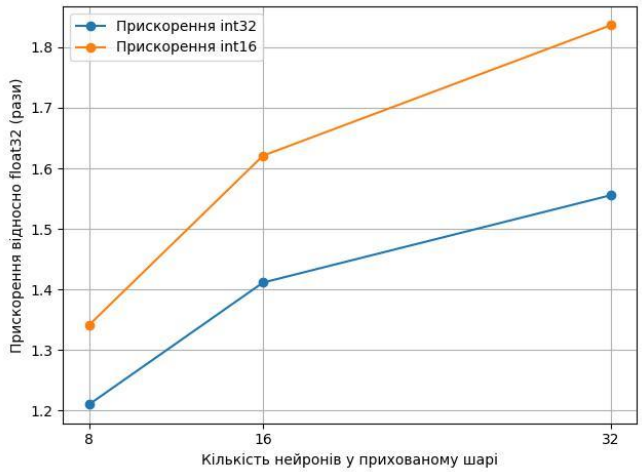

Рис. 4. Порівняння прискорення обчислень для різних варіантів реалізації нейромережевої моделі

Це підтверджує можливість використання нейромережевих методів для задачі виявлення вторгнень безпосередньо на вбудованих мікроконтролерних платформах.

Висновки. У статті досліджено можливість оптимізації обчислень нейромережевих моделей для задачі виявлення мережевих вторгнень у системах Інтернету речей.

Запропоновано підхід до реалізації нейромережевого алгоритму на малоресурсних мікроконтролерних платформах, який базується на використанні компактної архітектури нейронної мережі, скороченого набору інформативних ознак мережевого трафіку та цілочисельного fixed-point представлення параметрів і обчислювальних операцій.

Проведені експериментальні дослідження з використанням наборів даних NSL-KDD та UNSW-NB15 показали, що застосування запропонованого підходу дозволяє суттєво зменшити час виконання

нейромережевого алгоритму на мікроконтролерній платформі STM32L476 без значного зниження точності класифікації.

Отримані результати підтверджують можливість використання нейромережевих методів для задачі виявлення вторгнень безпосередньо на пристроях Інтернету речей з обмеженими обчислювальними ресурсами.

Список літератури:

1. *M. Koppula, L. J. L.M.I* (2024), "A Network Intrusion Detection System Based on Enhanced CNN2D for IoT Architecture", International Journal of Electronics and Communication Engineering, vol. 11, no. 4, pp. 68-79, doi: https://doi.org/10.14445/23488549/ijece-v11i4p108

2. *E. Rodríguez, P. B. Valls, B. E. A. Otero, J. J. Costa, J. Verdú, M. A. Pajuelo, et al.* (2022), "Transfer-Learning-Based Intrusion Detection Framework in IoT Networks", Sensors, vol. 22, no. 15, pp. 5621, doi: https://doi.org/10.3390/s22155621

3. *K. Yang, J. Ren, Y. Zhu, W. Zhang* (2018), "Active Learning for Wireless IoT Intrusion Detection", IEEE Wireless Communications, vol. 25, no. 6, pp. 19-25, doi: https://doi.org/10.1109/MWC.2017.1800079

4. *Y. Wang, Y. Houng, H. Chen, S. Tseng* (2023), "Network Anomaly Intrusion Detection Based on Deep Learning Approach", Sensors, vol. 23, no. 4, pp. 2171, doi: https://doi.org/10.3390/s23042171

5. *S. Hore, J. Ghadermazi, A. Shah, N. D. Bastian* (2024), "A sequential deep learning framework for a robust and resilient network intrusion detection system", Computers & Security, vol. 144, pp. 103928, doi: https://doi.org/10.1016/j.cose.2024.103928

6. *K. Saurabh, S. Sood, P. A. Kumar, U. Singh, R. Vyas, O. P. Vyas, et al.* (2022), "LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks", doi: https://doi.org/10.48550/arXiv.2207.00424

7. *R. Chinnasamy, M. Subramanian, N. Sengupta, R. Mp* (2025), "Contextual Internet of Things Intrusion Detection: A Sliding Window Convolutional Neural Network–Gated Recurrent Unit Model Enhanced by Graph Neural Networks", Cureus Journal of Computer Science, doi: https://doi.org/10.7759/s44389-025-06001-1

8. *A. R. Khudhu, K. Samsudin* (2022), "IoT Intrusion Detection using Auto-Encoder and Machine Learning Techniques", Journal of Computer Science, vol. 18, no. 10, pp. 904-912, doi: https://doi.org/10.3844/jcssp.2022.904.912

9. *M. Baz* (2022), "SEHIDS: Self Evolving Host-Based Intrusion Detection System for IoT Networks", Sensors, vol. 22, no. 17, pp. 6505, doi: https://doi.org/10.3390/s22176505

10. *S. Dhengre, A. Khadtare, P. Kakani, P. Jagtap*, *T. Jambhulkar* (2023), "The Proposed Intrusion Detection System using Support Vector Machine by IOT Enabled WSN", International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 6, pp. 989-997, doi: https://doi.org/10.22214/ijraset.2023.53584

11. *S. N. Gite, S. Kasar* (2024), "Enhancing Security for NFV-Based IOT Networks through Machine Learning: A Comprehensive Review and Analysis", Educational Administration Theory and Practices, doi: https://doi.org/10.53555/kuey.v30i5.5656

12. *J. Zhao, Z. Zhang, P. Xing, J. Wu* (2022), "Network Intrusion Detection System Based on One-Dimensional Convolutional Neural Networks", Highlights in Science, Engineering and Technology, vol. 23, pp. 154-160, doi: https://doi.org/10.54097/hset.v23i.3217
13. *V. Sravani (2025)*, "Enhanced Healthcare Data Security Through MI-Based Cyberattack Detection in SDN", INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, vol. 09, no. 03, pp. 1-9, doi: https://doi.org/10.55041/ijsrem42953
14. *H. Ma* (2023), "Presentation of a New Method for Intrusion Detection by using Deep Learning in Network", International Journal of Advanced Computer Science and Applications, vol. 14, no. 12, doi: https://doi.org/10.14569/ijacsa.2023.0141287
15. *Заковоротний О.Ю., Хулап А.В* (2024), "Оптимізація обчислення нейромереж за допомогою використання цілочисельної арифметики". Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ. Т. 2 (76). С. 90-94, doi: 10.26906/SUNZ.2024.2.090
16. *Zakovorotnyi O., Khulap A.* (2024), "Optimization of neural network calculations using integer arithmetic". 2024 IEEE KhPI Week, doi:10.1109/KhPIWeek61434.2024.10877949
17. *Заковоротний О. Ю., Хулап А. В.* (2025), "Аналіз моделей виявлення вторгнень на основі нейромереж у системах Інтернету речей". Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ. Т. 2 (80). С 125-131, doi: 10.26906/SUNZ.2025.2.125-131

References:

1. M. Koppula, L. J. L.M.I (2024) A Network Intrusion Detection System Based on Enhanced CNN2D for IoT Architecture. International Journal of Electronics and Communication Engineering, 11(4), pp. 68-79. Available from: https://doi.org/10.14445/23488549/ijece-v11i4p108
2. E. Rodríguez, P. B. Valls, B. E. A. Otero, J. J. Costa, J. Verdú, M. A. Pajuelo, et al. (2022) Transfer-Learning-Based Intrusion Detection Framework in IoT Networks. Sensors, 22(15), pp. 5621. Available from: https://doi.org/10.3390/s22155621
3. K. Yang, J. Ren, Y. Zhu, W. Zhang (2018) Active Learning for Wireless IoT Intrusion Detection. IEEE Wireless Communications, 25(6), pp. 19-25. Available from: https://doi.org/10.1109/MWC.2017.1800079
4. Y. Wang, Y. Houng, H. Chen, S. Tseng (2023) Network Anomaly Intrusion Detection Based on Deep Learning Approach. Sensors, 23(4), pp. 2171. Available from: https://doi.org/10.3390/s23042171
5. S. Hore, J. Ghadermazi, A. Shah, N. D. Bastian (2024) A sequential deep learning framework for a robust and resilient network intrusion detection system. Computers & Security, 144, pp. 103928. Available from: https://doi.org/10.1016/j.cose.2024.103928
6. K. Saurabh, S. Sood, P. A. Kumar, U. Singh, R. Vyas, O. P. Vyas, et al. (2022) LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks. Available from: https://doi.org/10.48550/arXiv.2207.00424

7. R. Chinnasamy, M. Subramanian, N. Sengupta, R. Mp (2025) Contextual Internet of Things Intrusion Detection: A Sliding Window Convolutional Neural Network–Gated Recurrent Unit Model Enhanced by Graph Neural Networks. Cureus Journal of Computer Science. Available from: https://doi.org/10.7759/s44389-025-06001-1

8. A. R. Khudhu, K. Samsudin (2022) IoT Intrusion Detection using Auto-Encoder and Machine Learning Techniques. Journal of Computer Science, 18(10), pp. 904-912. Available from: https://doi.org/10.3844/jcssp.2022.904.912

9. M. Baz (2022) SEHIDS: Self Evolving Host-Based Intrusion Detection System for IoT Networks. Sensors, 22(17), pp. 6505. Available from: https://doi.org/10.3390/s22176505

10. S. Dhengre, A. Khadtare, P. Kakani, P. Jagtap, T. Jambhulkar (2023) The Proposed Intrusion Detection System using Support Vector Machine by IOT Enabled WSN. International Journal for Research in Applied Science and Engineering Technology, 11(6), pp. 989-997. Available from: https://doi.org/10.22214/ijraset.2023.53584

11. S. N. Gite, S. Kasar (2024) Enhancing Security for NFV-Based IOT Networks through Machine Learning: A Comprehensive Review and Analysis. Educational Administration Theory and Practices. Available from: https://doi.org/10.53555/kuey.v30i5.5656

12. J. Zhao, Z. Zhang, P. Xing, J. Wu (2022) Network Intrusion Detection System Based on One-Dimensional Convolutional Neural Networks. Highlights in Science, Engineering and Technology, 23, pp. 154-160. Available from: https://doi.org/10.54097/hset.v23i.3217

13. V. Sravani (2025) Enhanced Healthcare Data Security Through MI-Based Cyberattack Detection in SDN. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 09(03), pp. 1-9. Available from: https://doi.org/10.55041/ijsrem42953

14. H. Ma (2023) Presentation of a New Method for Intrusion Detection by using Deep Learning in Network. International Journal of Advanced Computer Science and Applications, 14(12). Available from: https://doi.org/10.14569/ijacsa.2023.0141287

15. O. Zakovorotnyi, A. Khulap (2024) Optimization of neural network computation using integer arithmetic. Control, Navigation and Communication Systems, Vol. 2 No. 76 (2024). Available from: https://doi.org/10.26906/SUNZ.2024.2.090

16. O. Zakovorotnyi, A. Khulap (2024) Optimization of neural network calculations using integer arithmetic. 2024 IEEE KhPI Week. Available from: https://doi.org/10.1109/KhPIWeek61434.2024.10877949

17. O. Zakovorotnyi, A. Khulap (2025) Analysis of neural network-based intrusion detection models in internet of things systems. Control, Navigation and Communication Systems, Vol. 2 No. 80 (2025). Available from: https://doi.org/10.26906/SUNZ.2025.2.125

Статтю представив д-р техн. наук, проф. НТУ "ХПІ" Леонов С.Ю.

Надійшла (received) 13.01.2026
Стаття прийнята до друку 27.01.2026
Опублікована 27.03.2026

Zakovorotnyi Oleksandr, Dr. Tech. Sci., Professor
National Technical University «Kharkiv Polytechnic Institute»
Str. Kirpichova, 2, Kharkiv, Ukraine, 61002
Tel.: +38 (097) 967-32-71, e-mail: Oleksandr.Zakovorotnyi@khpi.edu.ua
ORCID ID: 0000-0003-4415-838X

Andrii Khulap, PhD student
National Technical University «Kharkiv Polytechnic Institute»
Str. Kirpichova, 2, Kharkiv, Ukraine, 61002
Tel.: +38 (093) 65-25-185, e-mail: Andrii.Khulap@cs.khpi.edu.ua
ORCID ID: 0000-0002-4103-7972

УДК 004.056.53:004.8:004.382

Оптимізація обчислень нейромережевих моделей для виявлення мережевих вторгнень у системах інтернету речей на мікроконтролерних платформах / Заковоротний О.Ю., Хулап А.В. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2026. – № 2 (16). – С. 96 – 111.

У роботі розглянуто проблему застосування нейромережевих методів для виявлення мережевих вторгнень у комп'ютерних системах Інтернету речей за умов обмежених обчислювальних ресурсів вбудованих пристроїв. У таких системах аналіз мережевого трафіку, розпізнавання аномальних подій та забезпечення безпеки повинні виконуватися у режимі, наближеному до реального часу, безпосередньо на периферійних вузлах інфраструктури граничних обчислень. Використання моделей на основі нейронних мереж у подібних вбудованих системах ускладнюється значними обчислювальними витратами під час виконання обчислень, що обмежує можливість їх реалізації на мікроконтролерних платформах комп'ютерних систем.

Метою роботи є підвищення ефективності виконання нейромережевих алгоритмів виявлення вторгнень шляхом оптимізації обчислювальних процесів для вбудованих систем. У роботі запропоновано підхід до оптимізації обчислень нейромережевих моделей, що базується на використанні цілочисельного fixed-point представлення параметрів та табличної апроксимації сигмоїдної функції активації. Для експериментальної перевірки ефективності підходу сформовано компактні нейромережеві моделі для задачі класифікації мережевого трафіку на основі загальнодоступних наборів даних NSL-KDD та UNSW-NB15. Реалізацію моделей виконано мовою C та досліджено на мікроконтролерній платформі STM32L476, що використовується у вбудованих комп'ютерних системах.

Проведені експериментальні дослідження показали, що застосування запропонованих методів дозволяє суттєво зменшити час виконання нейромережевих обчислень на вбудованих пристроях при збереженні прийнятного рівня точності класифікації мережевого трафіку. Отримані результати підтверджують доцільність використання оптимізованих нейромережевих моделей у системах виявлення вторгнень для комп'ютерних систем Інтернету речей та вбудованих систем, що функціонують у режимі реального часу. Іл.: 4. Табл.: 2. Бібліогр.: 17 назв.

Ключові слова: нейронна мережа, модель, Інтернет речей, мережевий трафік, розпізнавання, комп'ютерні системи, вбудовані системи, граничні обчислення, системи реального часу, події, безпека.

UDC 004.056.53:004.8:004.382

Optimization of Neural Network Computations for Intrusion Detection in Internet of Things Systems on Microcontroller Platforms / Zakovorotnyi O.Yu., Khulap A.V. // Herald of the National Technical University "KhPI". Series of "Informatics and Modeling". – Kharkiv: NTU "KhPI". – 2026. – No. 2 (16). – P. 96 – 111.

This paper addresses the problem of applying neural network methods for detecting network intrusions in computer systems of the Internet of Things under the conditions of limited computational resources of embedded devices. In such systems, network traffic analysis, recognition of anomalous events, and security assurance must be performed in near real time directly on peripheral nodes of edge computing infrastructure. The use of models based on neural networks in such embedded systems is complicated by significant computational costs during inference, which limits the possibility of their implementation on microcontroller platforms of computer systems.

The aim of this work is to improve the efficiency of neural network–based intrusion detection algorithms by optimizing computational processes for embedded systems. An approach to optimizing the computation of neural network models is proposed, based on the use of integer fixed-point representation of parameters and lookup-table approximation of the sigmoid activation function. For experimental verification of the proposed approach, compact neural network models for network traffic classification were developed using the publicly available NSL-KDD and UNSW-NB15 datasets. The models were implemented in the C programming language and evaluated on the STM32L476 microcontroller platform used in embedded computer systems.

Experimental studies have shown that the application of the proposed methods significantly reduces the execution time of neural network computations on embedded devices while maintaining an acceptable level of network traffic classification accuracy. The obtained results confirm the feasibility of using optimized neural network models in intrusion detection systems for Internet of Things computer systems and embedded systems operating in real time. Figs.: 4. Tabl.: 2. Refs.: 17 items.

Keywords: neural network, model, Internet of Things, network traffic, recognition, computer systems, embedded systems, edge computing, real-time systems, events, security.