

Довженко Тимур Павлович

кандидат технічних наук, доцент кафедри

Державний університет інформаційно-комунікаційних технологій, Київ, Україна

ORCID:0000-0002-0352-8391

timurdov@ukr.net

УЗГОДЖЕНА КЛАСИФІКАЦІЯ НОРМАЛЬНОГО ТРАФІКУ ТА ФЛУД-АТАКИ ЗА ПРОТОКОЛОМ UDP У МЕРЕЖАХ П'ЯТОГО ПОКОЛІННЯ МЕТОДОМ HYBRID AWRED

Анотація. У статті було розглянуто задачу багатокласового виявлення мережесих вторгнень у трафіку мереж п'ятого покоління. Основну увагу було приділено не тільки середній якості розпізнавання, а й характеру помилок між нормальним трафіком і флуд-атакою за протоколом UDP. Для практичних систем моніторингу це було важливо, оскільки високе значення узагальненої метрики ще не означало, що модель однаково прийнятно працювала для всіх важливих класів. Вона могла добре виглядати в середньому, але водночас надто часто відносити нормальний трафік до атаки.

Дослідження було виконано на наборі даних 5G-NIDD. Перед фінальним порівнянням було проведено попередній дробний факторний експеримент, який використано для вибору робочої області параметрів Hybrid AWRED. Докладний опис цього етапу було подано в основній частині статті. Фінальне порівняння було виконано для восьми підходів: BoostedTrees, RandomForest, MLP-CE, MLP-Focal, MLP-SupCon, LSTM, Transformer і Hybrid AWRED v8. Перевірку було проведено у п'яти прогонах із початковими станами генератора випадкових чисел 1081–1085.

У роботі Hybrid AWRED було розглянуто не як ще один звичайний класифікатор. Його роль була іншою: це гібридний механізм корекції профілю рішень у критичній парі класів. Він мав зменшити небажане зміщення між нормальним трафіком і флуд-атакою за протоколом UDP, але без втрати загальної якості багатокласового розпізнавання.

За результатами п'яти прогонів Hybrid AWRED v8 досяг значення Macro-F1 0.92747 ± 0.00048 , тобто залишився на рівні найсильніших конкурентів. Водночас головний результат полягав не у формальній перевазі за однією метрикою. Метод забезпечив найвищу повноту нормального трафіку 0.66373, найнижчу частку помилки Benign→UDPFlood 0.33490, конкурентну повноту класу UDPFlood 0.73703 та найвищий коридорний індекс 0.77618. Найближчим конкурентом за цим напрямом став MLP-Focal. Він також показав добрий профіль для критичної пари, однак поступився Hybrid AWRED v8 за повнотою нормального трафіку, часткою критичної помилки, Macro-F1 та коридорним індексом.

Отримані результати показали, що Hybrid AWRED доцільно розглядати як засіб формування більш збалансованої класифікації нормального трафіку та флуд-атаки за протоколом UDP у мережах п'ятого покоління.

Ключові слова: мережі п'ятого покоління, виявлення мережесих вторгнень, Hybrid AWRED, багатокласова класифікація, нормальний трафік, флуд-атака за протоколом UDP, критична пара класів.

Tymur P. Dovzhenko

Candidate of Technical Sciences, Associate Professor of the Department

State University of Information and Communication Technologies, Kyiv, Ukraine

ORCID:0000-0002-0352-8391

timurdov@ukr.net

CONSISTENT CLASSIFICATION OF NORMAL TRAFFIC AND UDP FLOOD ATTACKS IN FIFTH-GENERATION NETWORKS USING THE HYBRID AWRED METHOD

Abstract. The article considered the problem of multiclass network intrusion detection in fifth-generation network traffic. The main attention was paid not only to the average recognition quality, but also to the character of errors between normal traffic and a UDP-based flood attack. This was important for practical monitoring systems, because a high value of an aggregated metric did not yet mean that the model worked equally acceptably for all important classes. It could look good on average, but at the same time too often assign normal traffic to an attack class.

The study was carried out on the 5G-NIDD dataset. Before the final comparison, a preliminary fractional factorial experiment was conducted and used to select the working area of the Hybrid AWRED parameters. A detailed description of this stage was given in the main part of the article. The final comparison was performed for eight approaches: BoostedTrees, RandomForest, MLP-CE, MLP-Focal, MLP-SupCon, LSTM, Transformer, and Hybrid AWRED v8. The evaluation was carried out in five runs with initial random seeds 1081–1085.

In this work, Hybrid AWRED was not considered as just another ordinary classifier. Its role was different: it was treated as a hybrid mechanism for correcting the decision profile in a critical pair of classes. It had to reduce the undesirable shift between normal traffic and a UDP-based flood attack, but without losing the overall quality of multiclass recognition.

According to the results of five runs, Hybrid AWRED v8 achieved a Macro-F1 value of 0.92747 ± 0.00048 , which kept it at the level of the strongest competitors. At the same time, the main result was not a formal advantage in one metric. The method provided the highest recall of normal traffic, 0.66373, the lowest share of the Benign→UDPFlood error, 0.33490, competitive recall of the UDPFlood class, 0.73703, and the highest corridor index, 0.77618. MLP-Focal became the closest competitor in this direction. It also showed a good profile for the critical pair, but it was inferior to Hybrid AWRED v8 in normal traffic recall, critical error share, Macro-F1, and corridor index.

The obtained results showed that Hybrid AWRED should be considered as a means of forming a more balanced classification of normal traffic and a UDP-based flood attack in fifth-generation networks.

© 2026 Довженко Т.П. Цей матеріал ліцензовано за умовами CC BY 4.0.

<https://creativecommons.org/licenses/by/4.0/>

Keywords: *fifth-generation networks, network intrusion detection, Hybrid AWRED, multiclass classification, normal traffic, UDP-based flood attack, critical class pair.*

Вступ

Мережі п'ятого покоління стали основою для сервісів, де передавання даних має бути швидким, безперервним і захищеним. Це стосувалося промислових систем, транспорту, медичних сервісів, інтернету речей та інших розподілених середовищ. Разом із цим зростає й складність виявлення мережевих вторгнень. Помилка системи захисту могла мати різні наслідки: в одному випадку вона створювала зайві хибні тривоги, в іншому — залишала атаку непоміченою.

Для таких задач широко використовувалися методи машинного навчання. Вони давали змогу працювати з великим обсягом мережевих ознак і розпізнавати різні типи атак. Але в багатокласовій класифікації залишалася окрема проблема. Високий Macro-F1 ще не означав, що модель однаково прийнятно працювала для всіх важливих класів. Вона могла добре виглядати в середньому, але мати небажаний перекид між нормальною поведінкою мережі та певною атакою.

У цій роботі увагу було зосереджено на парі нормального трафіку та флуд-атаки за протоколом UDP. У наборі даних ці класи позначені як Benign і UDPFlood. Для цієї пари важливим був не тільки загальний рівень розпізнавання, а й напрям помилки. Надмірне віднесення нормального трафіку до атаки збільшувало кількість хибних тривог. Зворотна помилка могла означати пропуск атаки. Саме тому Hybrid AWRED було розглянуто не як ще один звичайний класифікатор, а як механізм коригування характеру рішень у критичній парі класів.

Постановка проблеми

У задачі виявлення вторгнень для мереж п'ятого покоління модель мала розпізнавати кілька класів трафіку одночасно. Це складніше, ніж простий поділ на норму й атаку. Окремі атаки мали близькі ознаки, а наслідки помилок були різними.

Звичайне порівняння моделей за середніми показниками було недостатнім. Macro-F1 показував загальну якість, але не пояснював, які саме класи плуталися між собою. Через це модель могла виглядати сильною за підсумковим показником, але залишати небажаний перекид у критичній парі Benign/UDPFlood.

Проблема полягала в тому, що стандартні класифікатори здебільшого оптимізували загальну межу розділення між класами. Вони не завжди формували збалансований характер рішень для нормального трафіку та флуд-атаки за протоколом UDP. Тому потрібно було перевірити, чи може Hybrid AWRED зменшити небажане зміщення нормального трафіку в бік UDPFlood і водночас зберегти якість багатокласового розпізнавання на рівні сильних конкурентів.

Аналіз останніх досліджень і публікацій

У роботах останніх років безпека мереж п'ятого покоління розглядалася як важлива сфера застосування машинного та глибокого навчання. Це було пов'язано з ускладненням мережевої інфраструктури, появою мережевих зрізів, віртуалізованих функцій і великої кількості підключених пристроїв. У праці [1] було показано, що методи машинного навчання можуть застосовуватися для виявлення аномалій, оцінювання ризиків і підтримки рішень у системах безпеки. Огляд [2] узагальнив стратегії машинного та переносного навчання для систем виявлення вторгнень у 5G і наступних мережах. У роботі [3] було порівняно алгоритми машинного й глибокого навчання для систем захисту мобільних мереж.

Окреме місце в цій темі займав набір даних 5G-NIDD. Його було подано як повністю розмічений набір трафіку, отриманий у функціональній тестовій мережі п'ятого покоління [4]. У подальших роботах цей набір використовували для візуального аналізу структури класів, зменшення розмірності та класифікації атак [5]. Було показано, що окремі класи можуть мати близькі ознакові прояви. У роботі [6] було проведено оцінювання контрольованих алгоритмів машинного навчання на 5G-NIDD. Такі результати дали важливу основу для порівняння, але не зняли питання про напрям помилки між окремими класами.

Поряд із класичними алгоритмами розвивалися нейромережеві та гібридні підходи. У праці [7] було використано згорткові нейронні мережі та суміш експертів для виявлення вторгнень у мережах п'ятого покоління. У роботі [8] було запропоновано систему Manticore на основі контрастивного навчання. Практичний бік цієї задачі також був важливим: у праці [9] було показано інтеграцію детекторів атак на основі машинного навчання в кіберполігон для мереж п'ятого покоління.

Отже, наявні роботи підтвердили придатність машинного навчання для виявлення вторгнень у сучасних мережах. Водночас більшість результатів подавалася через середні показники якості. Для багатокласових незбалансованих задач цього було замало, оскільки складність визначалася не тільки кількістю прикладів, а й перекриттям класів та різною ціною помилок [10]. Менш розкритою залишалася задача формування збалансованого характеру помилок у парі Benign/UDPFlood. Саме ця частина проблеми стала основою для застосування Hybrid AWRED у даній роботі.

Мета і задачі дослідження

Метою дослідження було обґрунтування застосування Hybrid AWRED для формування збалансованої класифікації нормального трафіку та флуд-атаки за протоколом UDP у мережах п'ятого покоління.

Для досягнення цієї мети було поставлено такі задачі:

- сформувати експериментальну підвибірку набору 5G-NIDD для багатокласового розпізнавання мережевого трафіку;
- визначити робочу область параметрів Hybrid AWRED за допомогою дробного факторного експерименту;
- провести фінальне порівняння Hybrid AWRED v8 з деревними, табличними нейромережевими та послідовними нейромережевими моделями;
- оцінити характер помилок у критичній парі Benign/UDPFlood за повнотою класів, частками взаємних помилок та коридорним індексом.

Результати дослідження

1. Набір даних та експериментальна підвибірка

Експериментальну перевірку було виконано на наборі даних 5G-NIDD. Повний набір містив 1 215 890 записів. Найбільші частки займали класи Benign — 477 737 записів, або 39,29 %, та UDPFlood — 457 340 записів, або 37,61 %. Інші класи були представлені значно менше, що зберігало типову для мережевого трафіку нерівномірність.

Для фінального експерименту було сформовано підвибірку обсягом 186 877 записів. Для класів Benign, HTTPFlood, SlowrateDoS і UDPFlood було взято по 30 000 записів, а для TCPConnectScan, SYNScan, UDPScan, SYNflood та ICMPFlood залишено доступну кількість. Така схема зменшувала домінування найбільших класів, але не робила задачу штучно рівномірною.

Структуру повного набору та експериментальної підвибірки наведено на рис. 1.

З рис. 1 видно, що в повному наборі Benign і UDPFlood разом формували понад три чверті всіх записів. У підвибірці їхній вплив було зменшено, однак саме ця пара залишилася центральною для аналізу. Причина не тільки кількісна. Помилка Benign→UDPFlood збільшувала кількість хибних тривог, а UDPFlood→Benign могла означати пропуск атаки.

2. Попереднє визначення робочої області параметрів Hybrid AWRED

Метод Hybrid AWRED спирався на попередній розвиток підходу, у якому поєднувалися реконструкційні, топологічні та коригувальні складові для виявлення аномалій [11]. Окремо Hybrid AWRED було розглянуто в задачах стійкого виявлення вторгнень за умов масованих кібератак [12]. У цій роботі цей напрям було перенесено до багатокласового розпізнавання трафіку 5G-NIDD і коригування характеру рішень для пари Benign/UDPFlood.

Перед фінальним порівнянням було виконано попередній дробний факторний експеримент. Він використовувався не як фінальна оцінка якості, а для звуження області параметрів Hybrid AWRED і фіксації робочої конфігурації.

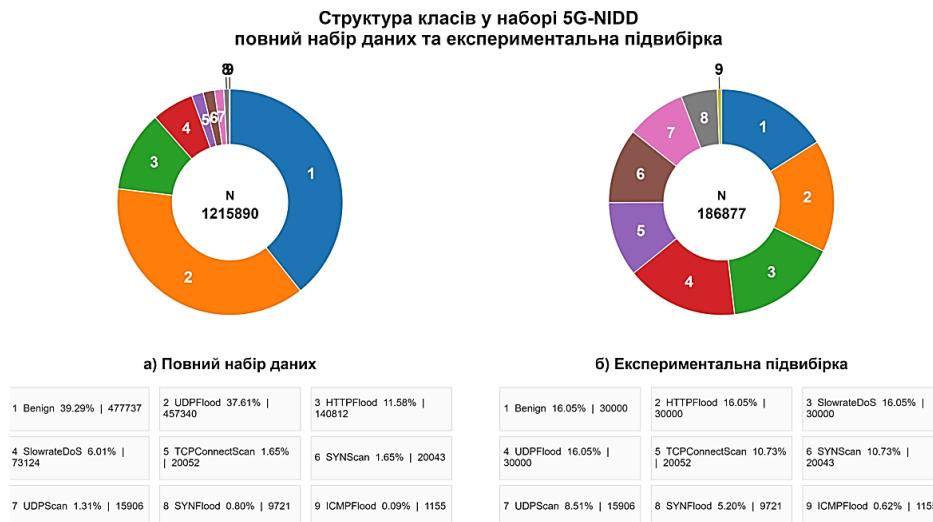


Рис. 1. Структура класів у наборі 5G-NIDD: повний набір даних та експериментальна підвибірка

Було застосовано дробний двофакторний план типу $2^{(8-4)}$, який містив 16 експериментальних комбінацій замість 256 у повному факторному плані. Такий підхід відповідав практиці формалізованого налаштування параметрів моделей і зменшував ризик випадкового ручного вибору конфігурації [13], [14]. До факторів було включено параметри інтенсивності AWRED-корекції, нижню межу надійності, параметри класової опори, обмеження компоненти функції розподілу та режим зміни коефіцієнта корекції.

Під час аналізу враховувалися головні впливи факторів і двофакторні взаємодії. Через структуру накладання ефектів результатів дробного плану трактувалися як попередні. За цим етапом було обрано робочу область параметрів, після чого фінальна перевірка проводилася вже на фіксованій конфігурації у п'яти початкових станах генератора випадкових чисел.

3. Метрики оцінювання та показники критичної пари

Для оцінювання моделей було використано загальну метрику багатокласового розпізнавання та окремі показники для критичної пари Benign/UDPFlood. Такий поділ був потрібний тому, що одна узагальнена метрика не завжди достатньо відображає характер помилок, особливо коли різні типи помилок мають різну практичну вагу [15]. Нехай n_{ij} позначало кількість прикладів, для яких істинний клас дорівнював i , а модель віднесла їх до класу j .

Повнота класу k визначалася так:

$$R_k = \frac{n_{kk}}{\sum_j n_{kj}}. \quad (1)$$

Точність класу k визначалася так:

$$P_k = \frac{n_{kk}}{\sum_i n_{ik}}. \quad (2)$$

На їх основі для кожного класу було розраховано $F1$ -міру:

$$F1_k = \frac{2P_k R_k}{P_k + R_k}. \quad (3)$$

Загальна якість багатокласового розпізнавання оцінювалася за Macro-F1:

$$MacroF1 = \frac{1}{K} \sum_{k=1}^K F1_k, \quad (4)$$

де K — кількість класів у задачі.

Клас Benign позначимо через B , а клас UDPFlood — через U . Частка помилки, за якої нормальний трафік відносився до флуд-атаки за протоколом UDP, визначалася так:

$$\Pi_{BU} = \frac{n_{BU}}{\sum_j n_{Bj}}. \quad (5)$$

Зворотний напрям, коли UDPFlood було віднесено до нормального трафіку, визначався так:

$$\Pi_{UB} = \frac{n_{UB}}{\sum_j n_{Uj}}. \quad (6)$$

Для оцінювання узгодженості повноти двох класів було використано показник:

$$S_{BU} = 1 - |R_B - R_U|. \quad (7)$$

Чим ближчим було значення S_{BU} до одиниці, тим менш вираженим був перекис між повнотою нормального трафіку та повнотою флуд-атаки за протоколом UDP.

Для узагальнення поведінки моделі в критичній парі було використано коридорний індекс:

$$CI_{BU} = \frac{MacroF1 + 2S_{BU} + (1 - \Pi_{BU}) + 3(1 - \Pi_{UB}) - 1}{6}. \quad (8)$$

Цей індекс поєднував Macro-F1, узгодженість повноти двох класів і два напрями помилок. Компонент $1 - \Pi_{UB}$ мав підвищену вагу, щоб зменшення хибних тривог не досягалося ціною різкого зростання пропусків UDPFlood.

4. Загальне порівняння моделей

Таблиця 1

Порівняння моделей за результатами п'яти прогонів на наборі 5G-NIDD

Метод	Macro-F1	Повнота Benign	Повнота UDPFlood	(Π_{BU})	(Π_{UB})	Коридорний індекс
BoostedTrees	0,92687 ± 0,00015	0,48893 ± 0,00162	0,91660 ± 0,00190	0,51073 ± 0,00162	0,08340 ± 0,00190	0,71843 ± 0,00062
RandomForest	0,92716 ± 0,00019	0,53627 ± 0,00205	0,85927 ± 0,00144	0,46307 ± 0,00204	0,14073 ± 0,00144	0,73265 ± 0,00092
MLP-CE	0,92226 ± 0,00178	0,45500 ± 0,11404	0,94833 ± 0,11553	0,54353 ± 0,11424	0,05167 ± 0,11553	0,70618 ± 0,03809
MLP-Focal	0,92067 ± 0,00393	0,62897 ± 0,00046	0,73677 ± 0,03536	0,36943 ± 0,00034	0,26323 ± 0,03536	0,75766 ± 0,00656
MLP-SupCon	0,92153 ± 0,00081	0,44943 ± 0,10066	0,94217 ± 0,12932	0,54947 ± 0,10079	0,05783 ± 0,12932	0,70218 ± 0,02867
LSTM	0,91285 ± 0,00440	0,39727 ± 0,00494	1,00000 ± 0,00000	0,59613 ± 0,00048	0,00000 ± 0,00000	0,68521 ± 0,00239
Transformer	0,90430 ± 0,00131	0,38277 ± 0,00490	1,00000 ± 0,00000	0,59533 ± 0,00039	0,00000 ± 0,00000	0,67908 ± 0,00175
Hybrid AWRED v8	0,92747 ± 0,00048	0,66373 ± 0,00721	0,73703 ± 0,00777	0,33490 ± 0,00729	0,26297 ± 0,00777	0,77618 ± 0,00227

У фінальному експерименті було порівняно вісім підходів: BoostedTrees, RandomForest, MLP-CE, MLP-Focal, MLP-SupCon, LSTM, Transformer і Hybrid AWRED v8. До порівняння було включено деревні ансамблі, табличні нейромережеві моделі та послідовні нейромережеві підходи. Такий склад конкурентів був важливим, оскільки ансамблеві та нейромережеві моделі широко використовувалися для задач із

незбалансованими класами й мережевим трафіком [16], [17]. Перевірку виконано у п'яти незалежних прогонах із seed (початковий стан генератора випадкових чисел) 1081–1085.

Підсумкові значення наведено в табл. 1.

Позначення (Π_{BU}) — частка помилок Benign→UDPFlood; (Π_{UB}) — частка помилок UDPFlood→Benign.

За Macro-F1 найкращий результат показав Hybrid AWRED v8 — $0,92747 \pm 0,00048$. Дуже близькі значення мали RandomForest — $0,92716 \pm 0,00019$ та BoostedTrees — $0,92687 \pm 0,00016$. Схожі групи моделей застосовувалися і в сучасних роботах з виявлення кібератак у програмно-керованих, розподілених і мобільних мережевих середовищах [18], [19]. Отже, Hybrid AWRED v8 не слід подавати як модель, що різко випередила конкурентів за інтегральним показником.

Основна різниця проявилася в критичній парі Benign/UDPFlood. Hybrid AWRED v8 мав найвищу повноту Benign — 0,66373. Для RandomForest цей показник становив 0,53627, для BoostedTrees — 0,48893. Повнота UDPFlood у Hybrid AWRED v8 дорівнювала 0,73703, тобто залишалася на рівні MLP-Focal і не руйнувала загальну якість багатокласового розпізнавання.

5. Критична пара Benign/UDPFlood

Для окремого аналізу було використано два напрями помилок. Показник (Π_{BU}) описував частку помилок Benign→UDPFlood, тобто випадки, коли нормальний трафік було віднесено до флуд-атаки за протоколом UDP. Показник (Π_{UB}) описував протилежний напрям — UDPFlood→Benign. Додатково використовувався коридорний індекс, який узагальнював якість поведінки моделі в цій парі.

Розташування моделей у просторі критичної пари наведено на рис. 2.

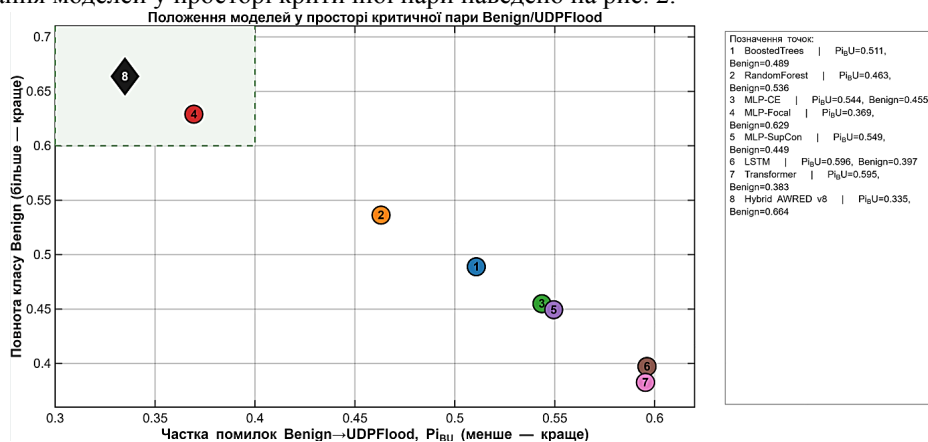


Рис. 2. Положення моделей у просторі критичної пари Benign/UDPFlood

На горизонтальній осі було відкладено Π_{BU} , де менше значення було кращим. На вертикальній осі показано повноту Benign. Бажаною була зона з малою часткою помилок Benign→UDPFlood і високою повнотою нормального трафіку.

Hybrid AWRED v8 опинився саме в цій зоні: Π_{BU} становило 0,33490, а повнота Benign — 0,66373. Найближчим конкурентом став MLP-Focal. Він також потрапив у коридор $\Pi_{BU}=0,30\text{--}0,40$, мав повноту Benign 0,62897 і повноту UDPFlood 0,73677. Тому MLP-Focal слід вважати найближчим конкурентом у межах коридору, а не слабкою базовою моделлю.

Детальні значення для критичної пари наведено в табл. 2.

Таблиця 2

Показники критичної пари Benign/UDPFlood для досліджуваних моделей

Метод	Повнота Benign	Повнота UDPFlood	(Π_{BU})	(Π_{UB})	Коридорний індекс	Нестійкі прогони
BoostedTrees	$0,48893 \pm 0,00162$	$0,91660 \pm 0,00190$	$0,51073 \pm 0,00162$	$0,08340 \pm 0,00190$	$0,71843 \pm 0,00062$	0
RandomForest	$0,53627 \pm 0,00205$	$0,85927 \pm 0,00144$	$0,46307 \pm 0,00204$	$0,14073 \pm 0,00144$	$0,73265 \pm 0,00092$	0
MLP-CE	$0,45500 \pm 0,11404$	$0,94833 \pm 0,11553$	$0,54353 \pm 0,11424$	$0,05167 \pm 0,11553$	$0,70618 \pm 0,03809$	4
MLP-Focal	$0,62897 \pm 0,00046$	$0,73677 \pm 0,03536$	$0,36943 \pm 0,00034$	$0,26323 \pm 0,03536$	$0,75766 \pm 0,00656$	0
MLP-SupCon	$0,44943 \pm 0,10066$	$0,94217 \pm 0,12932$	$0,54947 \pm 0,10079$	$0,05783 \pm 0,12932$	$0,70218 \pm 0,02867$	4
LSTM	$0,39727 \pm 0,00494$	$1,00000 \pm 0,00000$	$0,59613 \pm 0,00048$	$0,00000 \pm 0,00000$	$0,68521 \pm 0,00239$	5
Transformer	$0,38277 \pm 0,00490$	$1,00000 \pm 0,00000$	$0,59533 \pm 0,00039$	$0,00000 \pm 0,00000$	$0,67908 \pm 0,00175$	5
Hybrid AWRED v8	$0,66373 \pm 0,00721$	$0,73703 \pm 0,00777$	$0,33490 \pm 0,00729$	$0,26297 \pm 0,00777$	$0,77618 \pm 0,00227$	0

З табл. 2 видно, що Hybrid AWRED v8 мав найнижче середнє значення Π_{BU} і найвищий коридорний індекс — 0,77618. Для MLP-Focal цей індекс становив 0,75766. Різниця була не різкою, але послідовною: Hybrid AWRED v8 мав вищий Macro-F1, вищу повноту Benign, нижчу частку Benign→UDPFlood і майже таку саму повноту UDPFlood.

Інші моделі мали інший характер помилок. BoostedTrees і RandomForest краще зберігали UDPFlood, але значно частіше відносили Benign до UDPFlood. LSTM і Transformer майже не пропускали UDPFlood у нормальний клас, проте давали високий рівень хибних тривог для нормального трафіку.

6. Відносна перевага Hybrid AWRED v8

Матрицю відносної переваги Hybrid AWRED v8 над конкурентами наведено на рис. 3.

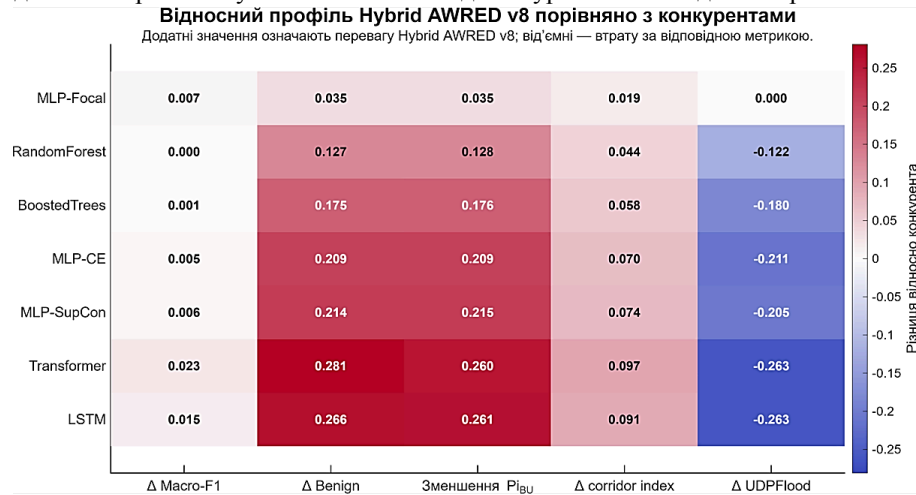


Рис. 3. Відносний профіль Hybrid AWRED v8 порівняно з конкурентами

Додатні значення на рис. 3 означали перевагу Hybrid AWRED v8, а від'ємні — втрату за відповідним показником. Найбільші позитивні зміни спостерігалися порівняно з LSTM, Transformer, MLP-CE і MLP-SupCon. Водночас Hybrid AWRED v8 поступався LSTM і Transformer за повнотою UDPFlood, але ця перевага послідовних моделей супроводжувалася значним зростанням помилки Benign→UDPFlood. Відносні числові значення наведено в таблиці 3.

Таблиця 3

Відносна перевага Hybrid AWRED v8 над конкурентами

Конкурент	Δ Macro-F1	Δ повноти Benign	Δ повноти UDPFlood	Зменшення (Π_{BU})	Зменшення (Π_{UD})	Δ коридорного індексу
LSTM	0,01461 $\pm$ 0,00397	0,26647 $\pm$ 0,01095	-0,26297 $\pm$ 0,00777	0,26123 $\pm$ 0,00742	-0,26297 $\pm$ 0,00777	0,09097 $\pm$ 0,00408
Transformer	0,02316 $\pm$ 0,00110	0,28097 $\pm$ 0,00451	-0,26297 $\pm$ 0,00777	0,26043 $\pm$ 0,00707	-0,26297 $\pm$ 0,00777	0,09709 $\pm$ 0,00148
MLP-SupCon	0,00594 $\pm$ 0,00095	0,21430 $\pm$ 0,09668	-0,20513 $\pm$ 0,12480	0,21457 $\pm$ 0,09693	-0,20513 $\pm$ 0,12480	0,07400 $\pm$ 0,02745
MLP-CE	0,00521 $\pm$ 0,00181	0,20873 $\pm$ 0,11005	-0,21130 $\pm$ 0,11103	0,20863 $\pm$ 0,11037	-0,21130 $\pm$ 0,11103	0,07000 $\pm$ 0,03686
BoostedTrees	0,00059 $\pm$ 0,00055	0,17480 $\pm$ 0,00621	-0,17956 $\pm$ 0,00672	0,17583 $\pm$ 0,00631	-0,17956 $\pm$ 0,00672	0,05774 $\pm$ 0,00200
RandomForest	0,00031 $\pm$ 0,00056	0,12746 $\pm$ 0,00665	-0,12223 $\pm$ 0,00661	0,12816 $\pm$ 0,00668	-0,12223 $\pm$ 0,00661	0,04353 $\pm$ 0,00223
MLP-Focal	0,00679 $\pm$ 0,00355	0,03476 $\pm$ 0,00733	0,00027 $\pm$ 0,03496	0,03453 $\pm$ 0,00733	0,00027 $\pm$ 0,03496	0,01852 $\pm$ 0,00740

Найважливішим був випадок MLP-Focal. Перевага Hybrid AWRED v8 над ним була помірною: 0,00679 за Macro-F1, 0,03476 за повнотою Benign, 0,03453 за зменшенням Π_{BU} і 0,01852 за коридорним індексом. Різниця за повнотою UDPFlood була майже нульовою. Це підтвердило, що MLP-Focal був найближчим конкурентом, але повний характер результатів залишився кращим у Hybrid AWRED v8.

7. Стійкість критичної помилки в п'яти прогонах

Стійкість Π_{BU} у п'яти прогонах із початковими станами генератора випадкових чисел 1081–1085 наведено на рис. 4.

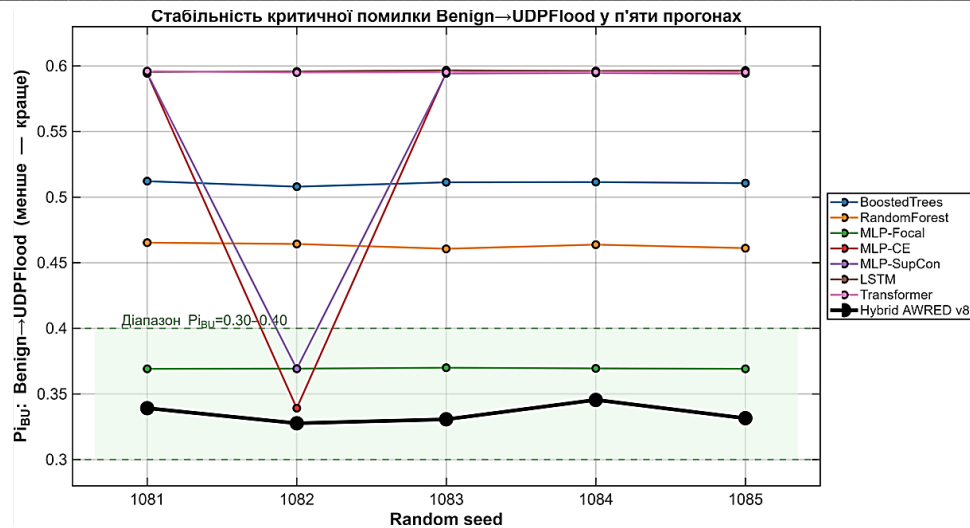


Рис. 4. Стабільність критичної помилки Benign→UDPFlood у п'яти прогонах

На рис.4 було виділено коридор $P_{BU}=0,30-0,40$. Усі п'ять значень Hybrid AWRED v8 залишалися всередині цього коридору й проходили нижче, ніж у MLP-Focal. Це показало, що перевага Hybrid AWRED v8 не була випадковою для одного прогону.

MLP-Focal також залишався в межах коридору, але його значення P_{BU} були стабільно вищими. Інші моделі або перебували вище коридору майже в усіх прогонах, або мали небажані коливання. Отже, Hybrid AWRED v8 сформував більш стійкий характер помилок для пари Benign/UDPFlood, зберігши загальну якість на рівні RandomForest і BoostedTrees.

Висновки та перспективи подальших досліджень

У роботі було сформовано експериментальну підвибірку набору 5G-NIDD для багатокласового розпізнавання мережевого трафіку. Повний набір містив 1 215 890 записів, а використана підвибірка — 186 877 записів. У ній було зменшено домінування найбільших класів, але збережено неоднорідність задачі. Окремо було виділено критичну пару Benign/UDPFlood, для якої помилка Benign→UDPFlood означала хибну тривогу, а UDPFlood→Benign — можливий пропуск атаки.

Перед фінальним порівнянням було визначено робочу область параметрів Hybrid AWRED. Для цього проведено дробний факторний експеримент типу $2^{(8-4)}$, який дав змогу скоротити простір пошуку та зафіксувати конфігурацію методу перед основною перевіркою.

Фінальне порівняння було виконано для восьми підходів у п'яти незалежних прогонах із початковими станами генератора випадкових чисел 1081–1085. Hybrid AWRED v8 досяг Macro-F1 $0,92747 \pm 0,00048$, тобто залишився на рівні RandomForest і BoostedTrees. Основна відмінність методу проявилася не в різкому зростанні інтегрального показника, а в характері помилок критичної пари.

Hybrid AWRED v8 забезпечив найвищу повноту Benign $0,66373 \pm 0,00721$, найнижчу частку помилки P_{BU} $0,33490 \pm 0,00729$ та найвищий коридорний індекс $0,77618 \pm 0,00227$. Повнота UDPFlood становила $0,73703 \pm 0,00777$ і залишалася конкурентною. Найближчим конкурентом був MLP-Focal, однак він поступився за Macro-F1, повнотою Benign, P_{BU} та коридорним індексом. Отже, Hybrid AWRED доцільно розглядати як механізм коригування характеру рішень для пари Benign/UDPFlood, а не як ще один звичайний класифікатор.

Подальші дослідження доцільно спрямувати на перевірку Hybrid AWRED на інших наборах мережевого трафіку, інших критичних парах класів, а також в умовах зміщення області даних, нерівномірного навантаження та надходження трафіку в потоці.

Декларація про штучний інтелект

Автор не використовував штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів.

Список використаної літератури

- 1 Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Bani Hani, I., Alkhalaileh, M., & Hamad, F. (2023). A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions. *Electronics*, 12(22), 4604. <https://doi.org/10.3390/electronics12224604>
- 2 Noor, K., Imoize, A. L., Li, C.-T., & Weng, C.-Y. (2025). A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond. *Mathematics*, 13(7), 1088. <https://doi.org/10.3390/math13071088>
- 3 Imanbayev, A., Tynymbayev, S., Odarchenko, R., Gnatyuk, S., Berdibayev, R., Baikenov, A., & Kaniyeva, N. (2022). Research of machine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond. *Sensors*, 22(24), 9957. <https://doi.org/10.3390/s22249957>

- 4 Siriwardhana, Y., Samarakoon, S., Porambage, P., Liyanage, M., Chang, S.-Y., Kim, J., Kim, J., & Ylianttila, M. (2025). Descriptor: 5G Wireless Network Intrusion Detection Dataset (5G-NIDD). *IEEE Data Descriptions*, 2, Article 11098458. <https://doi.org/10.1109/IEEEDATA.2025.3592888>
- 5 Ghani, H., Salekzamankhani, S., & Virdee, B. S. (2024). Critical analysis of 5G networks' traffic intrusion using PCA, t-SNE, and UMAP visualization and classifying attacks. In *Data Analytics and Management: Proceedings of ICDAM 2023* (Lecture Notes in Networks and Systems, Vol. 785, pp. 421–437). Springer. https://doi.org/10.1007/978-981-99-6544-1_32
- 6 Lassoued, N., Filali, I., & Ejbali, R. (2026). Supervised machine learning-based intrusion detection for 5G networks: Evaluation on the 5G-NIDD dataset. *Computers*, 15(6), 362. <https://doi.org/10.3390/computers15060362>
- 7 Ilias, L., Doukas, G., Lamprou, V., Ntanos, C., & Askounis, D. (2025). Convolutional neural networks and mixture of experts for intrusion detection in 5G networks and beyond. *Frontiers in Artificial Intelligence*, 8, 1708953. <https://doi.org/10.3389/frai.2025.1708953>
- 8 Yuan, L., Sun, J., Zhuang, S., Liu, Y., Geng, L., Zou, J., Xin, P., Huang, W., & Ma, W. (2024). Manticore: An unsupervised intrusion detection system based on contrastive learning in 5G networks. In *ICASSP 2024 – 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 4705–4709). IEEE. <https://doi.org/10.1109/ICASSP48485.2024.10447814>
- 9 Mozo, A., Pastor, A., Karamchandani, A., de la Cal, L., Rivera, D., & Moreno, J. I. (2022). Integration of machine learning-based attack detectors into defensive exercises of a 5G cyber range. *Applied Sciences*, 12(20), 10349. <https://doi.org/10.3390/app122010349>
- 10 Lango, M., & Stefanowski, J. (2022). What makes multi-class imbalanced problems difficult? An experimental study. *Expert Systems with Applications*, 200, 116962. <https://doi.org/10.1016/j.eswa.2022.116962>
- 11 Довженко, Т. П. (2026). Hybrid AWRED: синергія адаптивної реконструкції та топологічної кластеризації для виявлення аномалій у мультимодальних даних. *Зв'язок*, 1, 80–88. <https://doi.org/10.31673/2412-9070.2026.017405>
- 12 Довженко, Т. П., & Зінченко, О. В. (2026). Стабільність моделей глибокого виявлення вторгнень в умовах масованих кібератак: стрес-тестування та архітектурні особливості Hybrid AWRED. *Телекомунікаційні та інформаційні технології*, 1, 199–207. <https://doi.org/10.31673/2412-4338.2026.019019>
- 13 Pannakkong, W., Thiwa-Anont, K., Singthong, K., Parthanadee, P., & Buddhakulsomsiri, J. (2022). Hyperparameter tuning of machine learning algorithms using response surface methodology: A case study of ANN, SVM, and DBN. *Mathematical Problems in Engineering*, 2022, Article 8513719. <https://doi.org/10.1155/2022/8513719>
- 14 Bischl, B., Binder, M., Lang, M., Pielok, T., Richter, J., Coors, S., Thomas, J., Ullmann, T., Becker, M., Boulesteix, A.-L., Deng, D., & Lindauer, M. (2023). Hyperparameter optimization: Foundations, algorithms, best practices, and open challenges. *WIREs Data Mining and Knowledge Discovery*, 13(2), e1484. <https://doi.org/10.1002/widm.1484>
- 15 Chicco, D., & Jurman, G. (2023). The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. *BioData Mining*, 16, Article 4. <https://doi.org/10.1186/s13040-023-00322-4>
- 16 Chen, W., Yang, K., Yu, Z., Shi, Y., & Chen, C. L. P. (2024). A survey on imbalanced learning: Latest research, applications and future directions. *Artificial Intelligence Review*, 57, Article 137. <https://doi.org/10.1007/s10462-024-10759-6>
- 17 Khan, A. A., Chaudhari, O., & Chandra, R. (2024). A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation. *Expert Systems with Applications*, 244, 122778. <https://doi.org/10.1016/j.eswa.2023.122778>
- 18 Mozo, A., Karamchandani, A., de la Cal, L., Gómez-Canaval, S., Pastor, A., & Gifre, L. (2023). A machine-learning-based cyberattack detector for a cloud-based SDN controller. *Applied Sciences*, 13(8), 4914. <https://doi.org/10.3390/app13084914>
- 19 Ilias, L., Doukas, G., Lamprou, V., Mouzakitis, S., Ntanos, C., & Askounis, D. (2026). A federated learning-based network intrusion detection system for 5G and IoT using mixture of experts. *Electronics*, 15(5), 1057. <https://doi.org/10.3390/electronics15051057>

Надійшла до редакції: 01.06.2026

Прийнята до друку: 15.09.2026

Опубліковано: 30.09.2026