УДК 004.8:004.7
DOI: 10.31673/2412-9070.2025.041241
А. Ю. БАНАР, аспірант;
ORCID: 0009-0006-7817-2058
Г. І. ВОРОБЕЦЬ, канд. фіз.-мат. наук, доцент,
ORCID: 0000-0001-8125-2047
Чернівецький національний університет імені Юрія Федьковича

АЛГОРИТМИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОПТИМІЗАЦІЇ ФУНКЦІОНУВАННЯ SDN: СУЧАСНІ ПІДХОДИ ТА ПЕРСПЕКТИВИ

У статті проаналізовано сучасні підходи до застосування алгоритмів штучного інтелекту (ШІ) для підвищення ефективності програмно-конфігурованих мереж (SDN). Розглянуто типові завдання SDN - забезпечення якості обслуговування та надання послуг (Quality of Service / Quality of Experience, QoS / QoE), безпека, балансування навантаження, виявлення збоїв, енергоефективність та способи їх вирішення за допомогою алгоритмів штучного інтелекту. Здійснено огляд публікацій, що демонструють практичну ефективність алгоритмів ШІ у цих завданнях. Проведено аналіз підходів, наведено досягнуті результати й обмеження. Зроблено висновки щодо перспектив подальшого розвитку інтеграції ШІ у SDN для створення адаптивних, масштабованих і безпечних мереж.

Ключові слова: SDN; штучний інтелект; машинне навчання; глибоке навчання; QoS; балансування навантаження; енергоефективність; ресурси мережі.

Вступ

Програмно-конфігуровані мережі - це сучасна концепція побудови мереж, що передбачає відокремлення площини управління від площини передавання даних, завдяки чому забезпечується централізоване управління мережними ресурсами. У традиційних мережах пристрої (комутатори, маршрутизатори) самостійно приймають рішення у питаннях маршрутизації або пересилання даних. На противагу цьому, в архітектурі SDN використовується централізований контролер, який через програмні інтерфейси здійснює управління всіма мережними вузлами [1]. Архітектуру SDN умовно поділяють на три функціональні рівні - рівень передавання даних, рівень управління та прикладний рівень, які взаємодіють між собою за допомогою стандартизованих інтерфейсів (південний, північний та схід-захід - у спілкуванні в межах одного рівня). Централізований контролер SDN володіє цілісною картиною про поточний стан мережі, що дозволяє здійснювати ефективний розподіл ресурсів, на відміну від традиційних мереж, де інформація про стан мережі є фрагментованою поміж окремих вузлів. Це спрощує механізми балансування навантаження, управління якістю обслуговування та впровадження нових політик керування трафіком. Крім того, SDN істотно полегшує масштабування мережі: додавання нових комутаторів не потребує індивідуального переналаштування кожного пристрою, оскільки налаштування здійснюється централізовано через південний інтерфейс (Southbound API).

Попри переваги, архітектура SDN залишається вразливою до нових викликів. Централізоване управління призводить до зростання складності обробки великих обсягів мережної інформації, що вимагає використання ефективних алгоритмів та піднімає питання масштабованості контролера. Існують також ризики безпеки, оскільки компрометація контролера може надати зловмисникам можливість захопити контроль над усією мережею [2]. Також, важливим викликом є неоднорідність мережної інфраструктури: у практичних умовах мережа часто складається з пристроїв, які підтримують різні версії протоколів (таких як OpenFlow), або взагалі не підтримують функціональність SDN.

Для подолання згаданих викликів і розкриття повного потенціалу SDN, останнім часом все ширше застосовуються методи штучного інтелекту. По суті, SDN надає гнучку централізо-

вану інфраструктуру, а ШІ – інструменти для розумного прийняття рішень [3]. Така комбінація дає змогу прогнозувати мережне навантаження, виявляти аномалії, оптимізувати маршрути і розподіляти ресурси автоматично.

Аналіз останніх досліджень і публікацій

За останні роки опубліковано значну кількість оглядових і наукових робіт, присвячених використанню ШІ в контексті SDN. З'явилися докладні оглядові статті, які систематизують попередні дослідження. Наприклад, у статті [4] виконано огляд проблем продуктивності SDN у датацентрах та шляхів їх вирішення, акцентуючи на масштабованості контролерів і затримках. Класифіковано підходи ML для покращення різних показників SDN. Автори виділили основні напрями оптимізації (продуктивність, ефективність, безпека тощо) та відповідні метрики оцінювання, а також окреслили наявні прогалини для майбутніх досліджень.

У роботі [5] представлено модульну архітектуру для виявлення та нейтралізації DDoS атак у SDN, де ключову роль відіграють алгоритми машинного навчання. Моделі ШІ забезпечили високу точність виявлення атак (до 95 %), що підтверджено у віртуалізованому середовищі з використанням контролера ONOS. Подальший розвиток системи передбачає інтеграцію методів глибокого навчання для підвищення ефективності та масштабованості рішень у великих мережах.

В огляді [6] виконано систематичний аналіз літератури та підтверджено стійке зростання наукової активності на стику SDN і ШІ. В роботі також визначено основні тематичні кластери досліджень, що включають безпеку SDN, керування трафіком, інтеграцію з технологіями Big Data.

Аналіз цитувань показує, що найбільш популярними темами досліджень є забезпечення якості обслуговування та безпека SDN - ці напрями мають найбільше публікацій. Так, у роботі [7] запропоновано підхід до автоматичного виявлення «важких» потоків (надзвичайно великий безперервний потік даних) для запобігання перевантаженню мережі та оптимізації QoS за допомогою алгоритмів глибокого навчання H2O та Autoencoder. Інший блок досліджень стосується маршрутизації та управління трафіком: з'явилися огляди методів оптимізації маршрутів у SDN на основі навчання з підкріпленням, нейронних мереж та інших алгоритмів [8, 9]. Також, актуальним напрямом є виявлення атак та аномалій: наприклад у [10] опубліковано детальний огляд методів виявлення вторгнень в SDN за допомогою ML / DL (Machine Learning / Deep Learning), де проаналізовано ефективність різних класифікаторів на тестових наборах даних. Показано, що глибоке навчання значно підвищує ефективність систем виявлення вторгнень, зменшуючи рівень хибних спрацьовувань і підвищуючи точність. Окремо виділяються роботи з балансування навантаження - зокрема, автори в [11] провели розгорнутий огляд алгоритмів балансування на основі ШІ в SDN. Класифіковано існуючі підходи за чотирма напрямами - натхненні природними процесами, методи машинного навчання, математичні моделі та прогностичні підходи.

Аналіз сучасних публікацій свідчить, що впровадження методів штучного інтелекту істотно розширює функціональні можливості SDN-мереж. У літературі відзначають успішне використання ML / DL-алгоритмів для підвищення пропускної здатності, зниження затримок та своєчасного виявлення атак. Водночас, дослідники акцентують увагу на низці викликів: потребі у великих об'ємах якісних даних для навчання моделей, проблемі пояснень рішень систем на основі «чорних ящиків» ШІ та сумісності алгоритмів із реальними мережними протоколами. Багато оглядових робіт наголошують, що для повноцінного впровадження SDN з використанням ШІ необхідно забезпечити надійність і безпеку самих моделей (зокрема, стійкість до атак на навчальні дані), а також гарантувати здатність алгоритмів працювати у режимі, наближеному до реального часу, у великих масштабованих мережах.

Постановка задачі

Дослідити сучасні підходи застосування алгоритмів штучного інтелекту для підвищення ефективності функціонування SDN. Вияснити як саме методи ШІ використовуються для розв'язання типових завдань SDN - таких як забезпечення якості обслуговування, захист мережі,

оптимізація маршрутизації, балансування навантаження, виявлення несправностей та енергоефективність, і яких результатів вдається досягти. Актуальність теми визначається зростаючою складністю мереж та обсягами трафіку: традиційні методи управління вже не забезпечують потрібної гнучкості та швидкості реакції. На противагу, алгоритми ШІ можуть допомогти мережам самонавчатися на основі даних і адаптуватися до динамічних умов у режимі реального часу.

Основна частина

Зважаючи на велику кількість напрямів застосування штучного інтелекту у програмно-визначених мережах, доцільним є структурування відповідних підходів відповідно до функціональних завдань SDN. На рис. 1 представлено загальну класифікацію напрямів інтеграції алгоритмів ШІ в SDN, далі детально розглянемо кожен із зазначених аспектів, проаналізувавши поточні виклики, алгоритми ШІ, які використовуються, а також результати експериментальних впроваджень та їх ефективність.

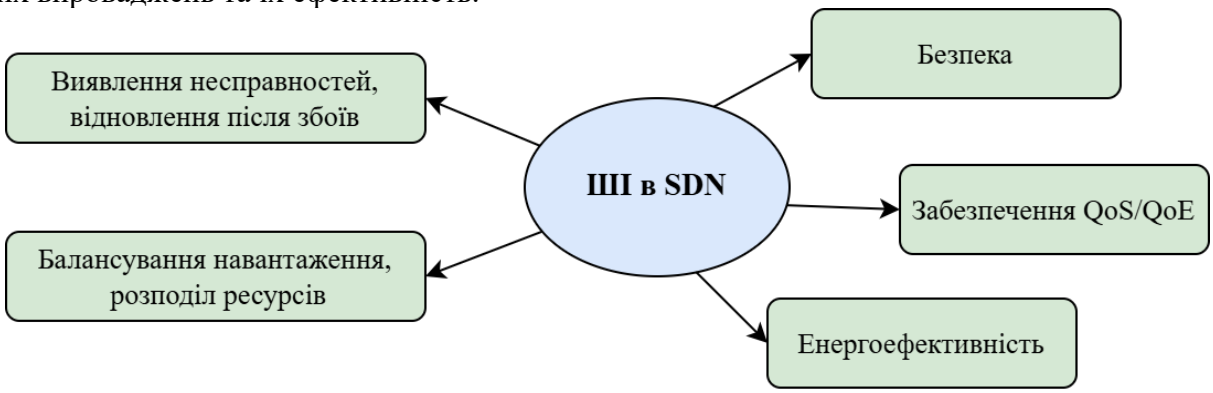

Рис. 1. Напрями інтеграції ШІ в SDN

Забезпечення QoS / QoE. Підтримання високого рівня якості обслуговування та якості користувацького досвіду є ключовим завданням для сучасних мереж, особливо з урахуванням зростаючих вимог потокових відеосервісів, соціальних мереж, фінансових систем, військової інфраструктури та інших критичних галузей. У середовищі SDN завдання забезпечення QoS та QoE охоплюють класифікацію трафіку для виявлення пріоритетних потоків, управління чергами і пропускною здатністю, а також динамічну маршрутизацію із врахуванням вимог до затримок. Проблема полягає в тому, що трафік мережі постійно змінюється і важко статично налаштувати мережу так, щоб за будь-яких умов гарантувати потрібний рівень QoS. Тому виникає потреба в інтелектуальних механізмах, які прогнозують стан мережі і автоматично регулюють параметри для підтримання QoS.

Для розв'язання завдань QoS / QoE в SDN широко застосовуються методи машинного навчання, зокрема нейронні мережі як їх різновид. Наприклад, для класифікації трафіку за типами сервісів (файлообмін, відео, веб тощо) використовують алгоритми на кшталт SVM, Random Forest або глибокі нейронні мережі (DNN). Класифікація дозволяє контролеру SDN призначати різні пріоритети та політики обслуговування потокам залежно від їх вимог до QoS. Інший підхід - прогнозування мережного трафіку за допомогою моделей глибокого навчання (рекурентних нейронних мереж, LSTM [12]), щоб завчасно виявляти можливі «важкі» потоки та запобігати перевантаженню з'єднань. Також дослідники застосовують навчання з підкріпленням для динамічного управління чергами і маршрутизацією: агент ШІ (розгорнутий на контролері) може навчитися розподіляти пропускну здатність між потоками або перемикати маршрути трафіку, щоб мінімізувати затримки та втрати пакетів. У статті [13] запропоновано метод глибокого навчання для поліпшення QoS у чутливих до затримки застосунків у SDN. Автори застосували нейронну мережу для розпізнавання типів потоків (deep flow discrimination), на основі чого контролер автоматично коригує пріоритети і маршрути для критичних потоків (наприклад, відеоконференцій) з метою зменшення затримки. Результати показали покращення показників затримки для критичного трафіку.

Безпека. Безпека в SDN - важливий напрям, адже розміщення інтелекту мережі в окремому контролері відкриває нові потенційні вразливості. Типові загрози включають атаки типу «відмова в обслуговуванні» (DoS / DDoS) на контролер або комутатори, вторгнення або несанкціонований доступ до площини керування, а також різноманітні атаки на протоколи SDN (наприклад, підробка повідомлень OpenFlow). Завдання полягає у своєчасному виявленні аномального трафіку або поведінки в мережі та у швидкому реагуванні (блокування або перенаправлення трафіку) до того, як атака завдасть шкоди. Системи виявлення вторгнень (Intrusion Detection System, IDS) можуть бути адаптовані до SDN, але SDN також має можливість встановлення правил фільтрації «на льоту» через контролер при виявленні атаки. У цьому питанні в SDN ефективно себе показують алгоритми класифікації: моделі, навчені розрізняти «нормальний» та «атакуючий» трафік за такими ознаками, як інтенсивність надсилання пакетів, кількість нових потоків, тощо. Використовуються як класичні ML-алгоритми (SVM, K-nearest neighbors, дерева рішень), так і глибокі нейронні мережі (наприклад, багатошарові персептрони, згорткові мережі) для виявлення складних патернів атак. У роботі [14] проведено порівняльний аналіз кількох методів ML / DL для виявлення DDoS-атак у SDN-мережі. Вони випробували SVM, KNN, дерева рішень, MLP та CNN на наборі даних CICDDoS2019 і показали, що найвищу точність прогнозування (95,5 %) - забезпечує SVM (метод опорних векторів). Це означає, що модель SVM змогла найкраще розрізняти нормальний і шкідливий трафік, перевершивши навіть CNN у цьому експерименті. Автори роблять висновок, що модель на основі SVM є ефективною для виявлення DDoS у SDN і має відносно невисоку складність реалізації. Дослідження [15] зосереджено на захисті контролера SDN від атак типу DoS. У роботі застосовано глибокі нейронні мережі - зокрема, архітектура GRU (Gated Recurrent Unit) та LSTM – для аналізу мережних потоків і виявлення ознак атак на контролер. Моделі навчено на наборі даних InSDN (спеціалізованому датасеті для SDN-вторгнень) і вони продемонстрували здатність розпізнавати атаки з високою точністю. Окрім DDoS, у літературі також зустрічаються реалізації ШІ для виявлення сканування портів, підробки маршрутної інформації та аналізу аномальних потоків.

Балансування навантаження та розподіл ресурсів. Під балансуванням навантаження у SDN розуміється як розподіл трафіку між різними маршрутами, так і розподіл контролю між декількома контролерами (у сценаріях із розподіленим SDN-контролером). Метою балансування є запобігання ситуаціям, коли одні канали перевантажені, а інші простоюють, або коли один контролер обслуговує надто багато комутаторів, що призводить до затримок, тоді як інший - має мінімальне навантаження. Один з напрямів застосування ШІ для даного завдання - передбачення навантаження за допомогою ML-моделей: наприклад, побудова прогнозів трафіку на кожному маршрутизаторі з використанням методів регресії або RNN. Маючи прогноз, контролер може завчасно перенести частину потоків на інші шляхи. Інший напрям - пошук оптимального розподілу пристроїв між контролерами. Тут використовуються алгоритми оптимізації, підсилені ШІ: зокрема, застосовано глибоке навчання з підкріпленням для вирішення завдання міграції комутаторів між контролерами.

У дослідженні [16] представлено стратегію балансування навантаження між декількома контролерами SDN на основі глибокого навчання з підкріпленням. Запропоновано алгоритм DRL-SMS (Deep Reinforcement Learning - Switch Migration Strategy), який визначає коли і які комутатори слід мігрувати до іншого контролера, щоб вирівняти завантаження площини контролю даних. Агент отримує винагороду за зменшення дисбалансу навантаження і в результаті навчання виробляє політику, що забезпечує швидке відновлення балансу при зміні навантаження з мінімальними накладними витратами. Експерименти показали, що DRL-SMS досягає швидшого часу відгуку на відмову контролера або сплески трафіку, ніж статичні алгоритми, а також має нижчу середню затримку обслуговування запитів контролера.

Виявлення несправностей та відновлення після збоїв. Надійність мережі - не менш важливий аспект, ніж розподіл ресурсів або безпека. У контексті SDN йдеться про виявлення збоїв на різних рівнях (фізичний збій підключення, відмова комутатора, аварія контролера) та автоматичне відновлення роботи мережі після таких інцидентів. Забезпечення відмовостій-

кості може бути реалізоване доволі гнучко - контролер має змогу перепрограмувати топологію при виникненні збою. Але складність полягає в тому, щоб швидко і точно виявити, що сталася несправність, і прийняти правильне рішення про відновлення. Так, при зникненні зв'язку з комутатором контролер має визначити, чи це збій комутатора, чи проблема у підключенні до нього, і відповідно перенаправити трафік альтернативним маршрутом, або задіяти резервний контролер. Людське втручання у ці процеси небажане, бо час іде на секунди.

Дослідники [17] розробили ігрову модель для автоматичного відновлення після збоїв контролера SDN. Вони розглядають сценарій, коли в мережі є кілька взаємопов'язаних контролерів, і один із них відмовляє. Запропонований алгоритм моделює вибір нового головного контролера для потерпілого домену як гру між контролерами: кожен контролер оцінюється з точки зору залишкової пропускної здатності, затримки до проблемного домену тощо, гра завершується вибором оптимального кандидата. Розроблений ними автономний алгоритм відновлення на основі теорії ігор забезпечує швидке перемикання контролю і низькі накладні витрати на міграцію порівняно з традиційними методами резервування контролерів. Інший підхід - аналітика логів контролера за допомогою ML: застосовується машинне навчання для аналізу журналів подій SDN-контролера з метою визначення першопричини збою (Root Cause Analysis). У роботі [18] запропоновано метод, де ML модель навчена розпізнавати у послідовності подій характерні патерни, що передують збою контролера. Це дозволяє не лише діагностувати причину після факту виникнення збою, а й потенційно попередити його, якщо модель побачить схожий патерн заздалегідь.

Енергоефективність. Споживання енергії комп'ютерними мережами (особливо великими датацентрами та операторами зв'язку) постійно зростає, що стимулює пошук «зелених» рішень. SDN надає більше контролю над мережними елементами, а тому дає змогу оптимізувати енергоспоживання за рахунок централізованого вимкнення або переходу у сплячий режим частини обладнання під час низького навантаження, чи перенаправляти трафік на менш завантажені маршрути. Це складна оптимізаційна проблема: наприклад, вимкнення деяких комутаторів заощадить енергію, але може збільшити довжину маршрутів для частини потоків. Потрібні механізми, які шукають компроміс між енергозаощадженням та якістю роботи мережі.

ШІ-рішення дають змогу досягнути цього компромісу шляхом інтелектуального керування енергорежимами обладнання. В одному з досліджень 2022 року [19] було запропоновано ML-алгоритм на базі логістичної регресії, який передбачає оптимальну конфігурацію мережі з точки зору енергоспоживання. Цей підхід дозволив швидко знаходити, які мережні з'єднання можна вимкнути чи уповільнити при низькому навантаженні: система змогла з більш ніж 95 % достовірністю визначати енергоефективні налаштування, перевершивши при цьому генетичні алгоритми за рівнем заощадження енергії. У статті [20] запропоновано енергоефективну оптимізовану маршрутизацію для великих промислових IoT-мереж (I-IoT) з використанням розподіленої архітектури SDN, підсиленої штучним інтелектом. Рішення передбачає динамічне формування кластерів і балансування навантаження за допомогою еволюційних алгоритмів, зокрема алгоритму рою часток (PSO) та штучного бджолиного рою (ABC), які реалізовані у хмарній інфраструктурі.

Наведемо аналіз розглянутих аспектів застосування алгоритмів ШІ в SDN. У таблиці зведено основні характеристики рішень для кожного аспекту.

Оцінка ефективності ШІ підходів у вирішенні ключових завдань SDN

Аспект SDN	Приклад ШІ-підходу	Досягнута ефективність	Обмеження підходу
Забезпечення QoS/QoE	Прогноз «важких» потоків DL-моделлю [12].	Точність «важких» потоків > 90 %. Зниження затримки для чутливих до QoS додатків.	Висока обчислювальна складність, потреба у якісних навчальних даних.

	Класифікація потоків нейронною мережею [13].		Потреба у якісних навчальних даних.
Безпека	SVM-класифікатор для виявлення DDoS [14]. LSTM для IDS [15].	Точність виявлення атак > 95 % (DDoS). Швидке спрацювання IDS (мілісекунди на класифікацію).	Необхідність оновлення моделей під нові атаки. Можливі хибні спрацювання (False Positive).
Балансування навантаження та розподіл ресурсів	DRL-алгоритм міграції комутаторів між контролерами [16].	Час відновлення балансу після збою контролера скорочено до мілісекунд.	Складність реалізації контролера.
Виявлення несправностей та відновлення після збоїв	Ігрова модель + ML для вибору резервного контролера [17]. ML аналізатор збоїв [18].	Час переключення при відмові контролера < 1 с (проти кількох сек без ШІ). Висока точність виявлення збоїв при низькій затримці обробки.	Тонке налаштування моделей під конкретну мережу. Залежність від топології тренування, обмежена кількість типів збоїв.
Енергоефективність	ML-алгоритм на базі логістичної регресії [19]. Алгоритм рою часток (PSO) та штучний бджолиний рій (ABC) [20].	95 % достовірність у визначенні енергоефективних налаштувань. Зменшення енергоспоживання на 60-80% в залежності від підходу.	Залежність від якісного навчального набору даних. Потреба у хмарних обчислювальних ресурсах.

Як видно з таблиці, спостерігається покращення метрик ефективності завдяки впровадженню алгоритмів ШІ: кращі показники QoS, вища точність і швидкість виявлення атак, зменшення затримок та більш рівномірне використання ресурсів, швидке реагування на збої, економія енергії. Однак жоден з підходів не позбавлений недоліків - переважно це стосується необхідності якісних навчальних даних, обчислювальних витрат на тренування моделей, а також обмеженої здатності моделей узагальнюватись на непередбачені ситуації. Відтак, розробники повинні ретельно збалансовувати використання ШІ з традиційними інженерними методами, застосовуючи гібридні рішення там, де це доцільно (наприклад, залишати резервні протоколи безпеки на випадок збою AI підходу).

Висновки

У роботі проведено всебічний аналіз сучасних підходів використання алгоритмів ШІ для оптимізації різних аспектів функціонування SDN. Алгоритми ШІ вже продемонстрували здатність суттєво покращувати продуктивність і керованість SDN. Застосування методів машинного і глибокого навчання дозволяє покращити якість обслуговування мережних додатків за

рахунок розумного керування трафіком, значно підвищити точність і швидкість виявлення атак, автоматизувати маршрутизацію і балансування навантаження краще, ніж це роблять статичні алгоритми. Крім того, за допомогою ШІ реалізовано концепції автономного відновлення мережі після збоїв. Отже, інтеграція ШІ в SDN є не просто популярним трендом, а об'єктивно надає переваги, підтверджені багатьма дослідженнями.

Попри досягнуті результати, існує ряд недоліків та обмежень поточних рішень. Моделі ШІ часто працюють як «чорні ящики» і їх рішення важко інтерпретувати, що є проблемою для мережних адміністраторів. Деякі алгоритми (особливо глибокі нейронні мережі) потребують значних обчислювальних ресурсів і часу на навчання - це може обмежувати їх застосування у реальному часі або вимагати попереднього тренування в емуляторах. Існує проблема узагальнення: модель, навчена на одній топології або наборі даних, може втрачати ефективність при зміні умов. Також, як показує практика, для критичних сценаріїв (наприклад, безпека) моделі ML поєднують з традиційними механізмами як резерв.

Список літератури

1. Z. A. Bhuiyan, S. Islam, M. M. Islam, A. B. M. A. Ullah, F. Naz and M. S. Rahman, On the (in)Security of the Control Plane of SDN Architecture: A Survey // IEEE Access, vol. 11, pp. 91550-91582, 2023, DOI: https://doi.org/10.1109/ACCESS.2023.3307467

2. R. DeLany, A. Smith, Y. Li and L. Du. SDN Dynamic Controller Configuration to Mitigate Compromised Controllers, 2023 // IEEE Transportation Electrification Conference & Expo (ITEC) / Detroit, MI, USA, 2023, pp. 1-5, DOI: https://doi.org/10.1109/ITEC55900.2023.10186974

3. Pathak, Y., Prashanth, P.V.N., Tiwari, A. (2023). AI Meets SDN: A Survey of Artificial Intelligent Techniques Applied to Software-Defined Networks. In: Kumar, M., Gill, S.S., Samriya, J.K., Uhlig, S. // 6G Enabled Fog Computing in IoT. Springer, DOI: https://doi.org/10.1007/978-3-031-30101-8_16

4. Faezi, S., Shirmarz, A. A Comprehensive Survey on Machine Learning using in Software Defined Networks (SDN) // Hum-Cent Intell Syst 3, 312–343 (2023), DOI: https://doi.org/10.1007/s44230-023-00025-3

5. Pérez, Jesus & Amezcua Valdovinos, Ismael & Choo, Kim-Kwang Raymond & Zhu, Dakai. (2020). A Flexible SDN-based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks using Machine Learning // IEEE Access. PP. 1-1, DOI: http://dx.doi.org/10.1109/ACCESS.2020.3019330

6. Ospina Cifuentes, B.J.; Suárez, Á.; García Pineda, V.; Alvarado Jaimes, R.; Montoya Benitez, A.O.; Grajales Bustamante, J.D. Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey // Technologies 2024, DOI: https://doi.org/10.3390/technologies12070099

7. Wassie, G., Ding, J. & Wondie, Y. Traffic prediction in SDN for explainable QoS using deep learning approach // Sci Rep 13, 20607 (2023), DOI: https://doi.org/10.1038/s41598-023-46471-8

8. Dake D., Gadze D., Klogo G., Nunoo-Mensah H. (2021). Traffic Engineering in Software-defined Networks using Reinforcement Learning: A Review // International Journal of Advanced Computer Science and Applications, DOI: http://dx.doi.org/10.14569/IJACSA.2021.0120541

9. Jiang, W.; Han, H.; Zhang, Y.; Wang, J.; He, M.; Gu, W.; Mu, J.; Cheng, X. Graph Neural Networks for Routing Optimization: Challenges and Opportunities // Sustainability 2024, DOI: https://doi.org/10.3390/su16219239

10. Ahmed, N.; Ngadi, A.b.; Sharif, J.M.; Hussain, S.; Uddin, M.; Rathore, M.S.; Iqbal, J.; Abdelhaq, M.; Alsaqour, R.; Ullah, S.S.; et al. Network Threat Detection Using Machine / Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Cha-llenges, and Future Research Direction // Sensors 2022, DOI: https://doi.org/10.3390/s22207896

11. Ahmed H. A., Ahmadreza M., Artificial intelligence based load balancing in SDN: A comprehensive survey // Internet of Things, Volume 22, 2023, DOI: https://doi.org/10.1016/j.iot.2023.100814

12. Kharbech, S., Benayed, N., Boubaker, A., & Seddik, H. (2023). Elephant Flows Detection Using Deep Neural Network, Convolutional Neural Network, Long Short-Term Memory, and Autoen-coder // Complexity, 2023, DOI: https://doi.org/10.1155/2023/1495642

13. Mohammadi R., Akleylek S., Ghaffari A., Shirmarz A. (2022). Automatic delay-sensitive applications quality of service improvement with deep flows discrimination in software defined networks. Cluster Comput vol. 26, pp. 437–459 (2023), DOI: http://dx.doi.org/10.1007/s10586-022-03729-6

14. Ali, T.E.; Chong, Y.-W.; Manickam, S. Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN // Appl. Sci. 2023, DOI: https://doi.org/10.3390/app13053033

15. Alshra'a, Abdullah & Farhat, Ahmad & Seitz, Jochen. (2021). Deep Learning Algorithms for Detecting Denial of Service Attacks in Software-Defined Networks // Procedia Computer Science. Vol. 191. Pp. 254-263, DOI: https://doi.org/10.1016/j.procs.2021.07.032

16. Xiang Min., Chen M., Wang D., Luo Z. (2022). Deep Reinforcement Learning-based load balancing strategy for multiple controllers in SDN // Advances in Electrical Engineering, Electronics and Energy, DOI: http://dx.doi.org/10.1016/j.prime.2022.100038

17. Xu, T.; Chen, C.; Hu, K.; Zhuang, Y. A Game Model and Fault Recovery Algorithm for SDN Multi-Domain // Sensors 2025, DOI: https://doi.org/10.3390/s25010164

18. V. Tong, S. Souihi, H. A. Tran and A. Mellouk. Machine Learning based Root Cause Analysis for SDN Network // 2021 IEEE Global Communications Conference (GLOBECOM) / Madrid, Spain, 2021, pp.. 1-6, DOI: http://dx.doi.org/10.1109/GLOBECOM46510.2021.9685185

19. Jiménez-Lázaro, M.; Herrera, J.L.; Berrocal, J.; Galán-Jiménez, J. Improving the Energy Efficiency of Software-Defined Networks through the Prediction of Network Configurations // Elec-tronics 2022, DOI: https://doi.org/10.3390/electronics11172739

20. P. K. Udayaprasad et al. Energy Efficient Optimized Routing Technique With Distributed SDN-AI to Large Scale I-IoT Networks // IEEE Access, vol. 12, pp. 2742-2759, 2024, DOI: https://doi.org/10.1109/ACCESS.2023.3346679

A. Banar, H. Vorobets

ARTIFICIAL INTELLIGENCE ALGORITHMS FOR OPTIMIZING SDN FUNCTIONING: MODERN APPROACHES AND PROSPECTS

This article presents a comprehensive review of modern approaches to the application of artificial intelligence (AI) algorithms for optimizing the functioning of Software-Defined Networks (SDN). SDN, as a modern approach that separates control and data planes, provides a flexible architecture for centralized network management. However, the increasing complexity of network traffic, rising security threats, and growing energy demands challenge traditional static control mechanisms. In this context, AI emerges as a key enabler of intelligent, adaptive, and scalable SDN solutions.

The paper explores the application of AI algorithms to address key SDN challenges: Quality of Service and Experience (QoS / QoE), security, load balancing and resource distribution, failure detection and recovery, and energy efficiency. For each aspect, the study systematizes current research, highlights algorithmic approaches (including supervised, unsupervised, deep, and reinforcement learning), and provides examples of real-world use cases. AI-based models such as SVM, LSTM, CNN, and DRL have demonstrated significant effectiveness in traffic classification, DDoS detection, intelligent routing, and proactive network reconfiguration.

Results across multiple publications show that AI integration improves SDN metrics: reducing packet loss and latency, increasing attack detection accuracy (up to 95 %), minimizing controller overloads, and saving energy by dynamically optimizing active components. The study highlights existing challenges, including intensive computational demands, the requirement for high-quality training data, and difficulties in explaining the behavior of opaque AI models. SDN offers the infrastructure for programmable control, while AI supplies the intelligence to make proactive, data-driven decisions. The analysis reveals the potential for further integration, particularly through hybrid approaches combining classical engineering with AI-driven optimization for robust, scalable, and auto-nomous networking.

Keywords: Software-Defined Networking; Artificial Intelligence; Machine Learning; QoS; Load Balancing; Network Security; Energy Efficiency; Intrusion Detection.