Методика ідентифікації трафіку в телекомунікаційних мережах 5G/IMT-2020 на основі штучного інтелекту

Олександр Корецький[1], Анастасія Кондакова[2]

[1]Державний університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, м. Київ, Україна, 03110
[2]Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037
[1]koretsky@gmail.com, https://orcid.org/0009-0001-4809-7556
[2]a_kondakova@ukr.net, https://orcid.org/0000-0003-1302-2244

Received 03.02.2025, accepted 29.03.2025
https://doi.org/10.32347/st.2025.3.1206

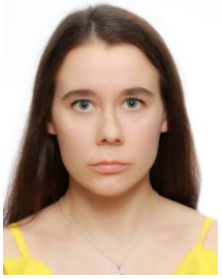
Анотація. В роботі проведено аналіз процесу ідентифікації вхідного трафіку в мережах 5G/IMT-2020, побудованій по технології Ultra-reliable and low latency communications, визначені його особливості та напрямки досліджень по підвищенню ефективності ідентифікації трафіку х урахуванням вимог до функціонування розглянутої мережі.

Для вирішення завдання ідентифікації трафіку мережі 5G/IMT-2020в роботі розроблена та подана відповідна методика. Вказана методика включає формування масивів метаданих вхідного потоку, модифікацію їх в набір навчальних даних, формування навчального програмно-апаратного комплексу та розбудову структури нейронної мережі, проведення процесу навчання нейронної мережі та втілення її в процес ідентифікації трафіку в телекомунікаційних мережах 5G/IMT-2020.

Оцінка результатів процесу навчання запропонованої нейронної мережі та перевірки її роботи на тестових наборах даних у навченому стані показала, що подана в роботі нейронна мережа здатна провести моніторинг та ідентифікувати згенерований від сервісів Інтернету Речей трафік з ймовірністю до 99,7%. В процесі ідентифікації трафіку від двох та більше сервісів дана ймовірність може знизитися, проте перебуває у допустимих межах 80-90%.

Ключові слова: ідентифікація вхідного трафіку інформаційно-комунікаційної мереж, мережа 5G/IMT-2020, штучний інтелект, нейронна мережа, управління навантаження інформаційно-комунікаційної мережі

Корецький Олександр
Аспірант кафедри штучного інтелекту



Анастасія Кондакова
Аспірант кафедри кібербезпеки та комп'ютерної інженерії

ПОСТАНОВКА ПРОБЛЕМИ

Необхідність забезпечення розвитку глобальних економічних відноси, інтенсивний розвитку науки та посилення сфери оборони вимагають постійного удосконалення та розвитку галузі інформаційних технологій в напрямку збільшення швидкості та якості передачі корисних даних. Одним з напрямків досліджень в вказаній сфері є розбудова та швидке впровадження перспективних концепцій мереж передачі даних, а саме стандарту 5G/IMT-2020 та, в його розвиток, наступних поколінь таких мереж.

Розбудова сучасних та перспективних концепцій мереж зв'язку, на даному етапі сконцентрована на реалізації трьох основних технологій, на основі яких безпосередньо будується мережа 5G/IMT-2020. А саме [1,2,3]:

1. Глобальні міжапаратні взаємодії – MMC (Massive Machine type Communications);
2. Високоефективний мобільний широкосмуговий зв'язок – eMBB (Enhanced Mobile Broadband);
3. Високонадійний зв'язок з мінімальними затримками – URLLC (Ultra-reliable and low latency communications).

На даний момент реалізація інформапційно-комунікаційних мереж на основі концепції високонадійного зв'язку з мінімальними затримками (URLLC) є одним з найскладніших завдань, що стоять перед науково-технічною спільнотою. Основна вимога до мереж класу мереж URLLC, це висока надійність передачі даних при мінімальних затримках [3].

Дані послуги реалізуються в таких напрямках як електронна медицина (e-health), автономний транспорт, небезпечні промислові виробництва формату 4.0 та інші.

Одним із найвідоміших типів сервісів мереж URLLC є Інтернет речей (IoT) та Тактильний Інтернет (Tactile Internet). В випадку реалізації мережі для забезпечення функціонування сервісу Tactile Internet слід зазначити, що на архітектуру побудови мережі та її ефективне функціонування найбільший вплив чинять саме ультрамалі затримки. Їх критичне значення впливає на децентралізацію мережі внаслідок обмежень на відстані, на яких можна надавати послуги Tactile Internet. Досягнення ультрамалих затримок в мережі Tactile Internet та IoT, в свою чергу, має призвести до децентралізації економіки та стирання цифрової нерівності між територіями як однієї держави так і в межах певного суспільно-економічного регіону [1,2].

Сучасний обсяг трафіку, його гетерогенність та різноманітність сервісу Tactile Internet та інших сервісів, у тому числі тих, що належать до URLLC, диктує нові вимоги до оперативності прийнятих рішень щодо забезпечення якості обслуговування (QoS) [2,3].

Аналіз можливостей існуючих інструментів управління трафіком 5G/IMT-2020 та забезпечення високого значення QoS показує, що вони неспроможні надати необхідний рівень ефективності безпосередньої та швидкої ідентифікацій трафіку URLLC, його оцінки та управління [4,5,6]. Основною проблемою, яка обумовлює такі висновки, є невідповідність можливостей по прогнозу очікуваного навантаження на мережу. В даному випадку, вже в більшості рішень концепції URLLC потрібно мати прогнози навантажень на ті чи інші сервіси, враховуючи географічні та динамічні (пересування абонента), в тому числі, при переміщені його в просторі на високих швидкостях [4,5,6].

Варто також зауважити, що в процесі розробки рішень у мережах 5G/IMT-2020, розробки їх стандартів та проведення відповідних досліджень було досягнуто висновку, які свідчать про те, що вимоги URLLC складно виконати з точки зору широкомасштабного впровадження даного типу послуг [4,6]. Вони можуть бути надані в обмеженому географічному просторі за виділеними мережевими каналами і за інших обмеженнях.

Неоднорідність трафіку, складність ініціалізації потоків та розрахунку зростання трафіку, а також питання оперативного виявлення та вчасного розрахунку змін профілю трафіку призводять до того, що існуючі «ручні» методи моніторинг в мережах покоління 5G/IMT-2020 втрачають свою актуальність.

Дані обставини формують нову наукову проблему, а саме забезпечення функціонування мережі покоління 5G/IMT-2020 на надвисоких швидкостях передачі даних з ультрамалими затримками.

Для забезпечення оперативного реагування систем управління мережею на зростання трафіку та зміни гетерогенності в мережах 5G/IMT-2020 (в тому числі періодичного трафіку), аналізу змін профілю трафіку потрібно розробити та втілити відповідну низку механізмів та процедур, пристосованих для ідентифікації, розрахунку навантаження, його прогнозу та управління трафіком в мережах даного покоління без впливу на їх продуктивність.

Одним з таких механізмів, призначених для вирішення часткового завдання своєчасної ідентифікації вхідного трафіку є

застосування методика ідентифікації трафіку в телекомунікаційних мережах 5G/IMT-2020. А її розробка формує нове актуальне наукове задання, вирішенню якого присвячена дана робота.

Основні вимоги до вирішення такого завдання, це вчасне та ефективне виявлення змін структури трафіку, розрахунок його навантаження та оперативне прийняття рішень по управлінню трафіком в нових умовах. При цьому, необхідно зазначити, що для того, щоб забезпечити постійний моніторинг та оперативне реагування мережі зв'язку на зміни трафіку відповідні пристрої та механізми комутації та маршрутизації трафіку і його аналізу в ході моніторингу та реагування повинні мати необхідний рівень абстрагування від «фізики» процесів передачі даних через мережу.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ

Питанням ідентифікації та моніторингу трафіку в інформаційно-комунікаційних мережах останніх поколінь присвячено рад наукових публікацій. Основні підходи та принципі рішення задання ідентифікації та моніторингу подано в наукових роботах [7-10]

На даний момент якість обслуговування в мережах зв'язку забезпечується за допомогою технологій DiffServ (Differential Services), а також інших TE (Traffic Engineering) рішень, наприклад MPLS-TE, що використовує в основі протокол резервування ресурсів RSVP-TE [7,8]. Однак ці рішення мають ряд недоліків для їх застосування в ряді сервісів у мережах п'ятого та наступних поколінь. Основними недоліками є відсутність динамічного управління залежно від мінливості профілю трафіку в мережі та відсутність можливості швидкого переконфігурування політик обслуговування підконтрольного домену мережі, а також обмежений набір класифікаторів трафіку, що в умовах, що з'являються та відрізняються за вимогами до якості обслуговування сервісів IoT та інших, що є дуже критичним недоліком.

Необхідний рівень абстрагування від фізичних процесів реалізують концепції SDN (software-defined networking, SDN; програмно-конфігурована мережа) і NFV (Network Functions Virtualization, NFV – концепція віртуалізації мережевої архітектури), що викладені в роботах [9,10]. Відмічене, що для оперативного реагування систем управління мережі, у разі застосування концепцій SDN та NFV контролера SDN і Оркестратора, потрібно проводити високоточну ідентифікацію трафіку без безпосереднього втручання у потік на рівні передачі даних та відповідно, без внесення змінень до його профілю, а також мінімізації затримок трафіку [9,10]. Механізми такої ідентифікації та процедури моніторингу без втручання в потік даних в поданих роботах не розглянуті а викладені процедури концепцій SDN і NFV загалом не дозволяють здійснити такий моніторинг при одночасному вирішення покладного на SDN забезпечення кібербезпеки мережі.

Таким чином, завдання по ідентифікації трафіку в мережах 5G/IMT-2020 потребує розробки окремої методики. Основні вимоги до такої методики, це вчасне та ефективне виявлення змін трафіку, його розрахунок та оперативне прийняття рішень по управлінню трафіком при забезпечені необхідного рівня абстрагування від «фізики» процесів передачі даних в телекомунікаційних мережах 5G/IMT-2020.

Метою дослідження є розробка методики ідентифікації трафіку в телекомунікаційних мережах 5G/IMT-2020, які функціонують в межах концепції передачі даних URLLC.

Для досягнення визначеної мети необхідно:

- визначити механізми ідентифікації та моніторингу трафіка без втручання процес передачі даних та сформувати принципи його функціонування;
- побудувати програмно - апаратний комплекс для оцінки застосовності запропонованого механізму ідентифікації та моніторингу трафіку;
- розробити алгоритм ідентифікації трафіку в телекомунікаційних мережах 5G/IMT-2020, яка повинна функціонувати в межах концепції передачі даних URLLC;
- оцінити можливості застосування поданого алгоритму та створеної на його основі

методики для моніторингу навантаження в телекомунікаційних мережах 5G/IMT-2020, які повинні функціонувати в межах концепції передачі даних URLLC

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Як було зазначено раніше, завдання ідентифікації та моніторингу трафіку включає необхідність розпізнавання великої кількості типів (враховуючи URLLC) сервісів, не вносячи додаткових затримок у трафік, та можливість розширення та налаштування алгоритму під певне географічне розташування мережі та сервісів [4,6]. Неоднорідність трафіку, складність його ініціалізації та розрахунку його зростання, а також складність оперативного розрахунку змінення профілю трафіку призводять до того, що існуючі «ручні» методи розрахунку втрачають свою актуальність.

Одними з перспективних рішень, які дадуть змогу значно розширити можливості мереж

п’ятого покоління по забезпеченню вимог URLLC розглядаються наступні рішення [5,7,8]:

1. Зміна технологій фізичного рівня та перехід на так звані "квантові комунікації", які реалізують інший фізичний принцип передачі інформації, заснований на принципі квантової заплутаності. Однак цей метод знаходиться на стадії ранніх досліджень.

2. Децентралізація мереж зв'язку та децентралізація систем обчислень, гнучке їх управління з імплементацією Штучного інтелекту (ШІ) як системи моніторингу та управління.

Виходячи з поточного рівня мережевих технологій 5G/IMT-2020, які повинні функціонувати в межах концепції передачі даних URLLC та часткових завдань моніторингу та управління, в рамках процесу впровадження Штучного інтелекту в системи управління вказаними мережами найбільш актуальними завданнями для нейромерж будуть наступні [6,9,10]:

– однозначна ідентифікація трафіку з подальшим прогнозуванням його характеристик;

– ефективний та динамічний розподіл обчислень на інфраструктурі розподілених обчислень;

– прогнозування та ідентифікація можливих перевантажень керуючих систем.

При цьому завдання ідентифікації трафіку включає необхідність розпізнавання великої кількості типів сервісів (враховуючи URLLC) при умові виключення додаткових затримок у трафік, та можливість розширення та налаштування алгоритму під певне географічне розташування мережі та сервісів [4,6].

Існуючі системи моніторингу трафіку зазвичай використовували технології, що засновані на періодичному захопленні трафіку та аналізі його заголовків. Такий метод має низку недоліків, а саме: внесення затримки в потік, реалізація аналітичного модуля у вигляді додаткового апаратно-програмного рішення рівня передачі даних (Data Plane), складність побудови такого пристрою [4,6,8].

Поява технологій ШІ, та розробка на їх основі спеціалізованих систем глибокої інспекції пакетів DPI (Deep Packet Inspection) дозволяє перейти до моніторингу трафіку на сервісному рівні інфраструктури програмно-конфігурованих мереж [12,13,14].

Таким чином, як результат проведеного аналізу можливостей по моніторингу трафіку в мережах 5G/IMT-2020, в даній роботі пропонується підхід до виконання вище вказаного завдання, заснований на використання нейронних мереж певної архітектури, завдання яких виявлення та ідентифікація визначеного типу трафіку в сумі загального вхідного трафіку визначеної мережі.

Система DPI, як видно з назви, виконує глибокий аналіз всіх пакетів вхідних даних, що проходять через неї. Термін «глибокий» має на увазі аналіз пакета на верхніх рівнях моделі OSI, а не лише за стандартними номерами портів. Крім вивчення пакетів за

деякими стандартними патернами, за якими можна однозначно визначити приналежність пакета певному додатку, скажімо, за форматом заголовків, номерами портів і т.п., система DPI здійснює і так званий поведінковий аналіз трафіку, який дозволяє розпізнати додатки, які не використовують для обміну даними заздалегідь [14,15].

Втілення технології DPI в вигляді окремо реалізованої програмно-апаратної системи, її залучення до ідентифікації та моніторингу трафіку на серверному рівні за інтерфейсом REST формує окрему систему ідентифікації трафіку з властивістю виключення затримок та мінімізації складності реалізації програмно-апартного комплексу. Така система може бути представлена і як апаратно-програмний комплекс, так і програмне рішення (у вигляді програми мережі).

Принципова архітектура запропонованого рішення по побудові системи ідентифікації трафіку представлена на Рис. 1.

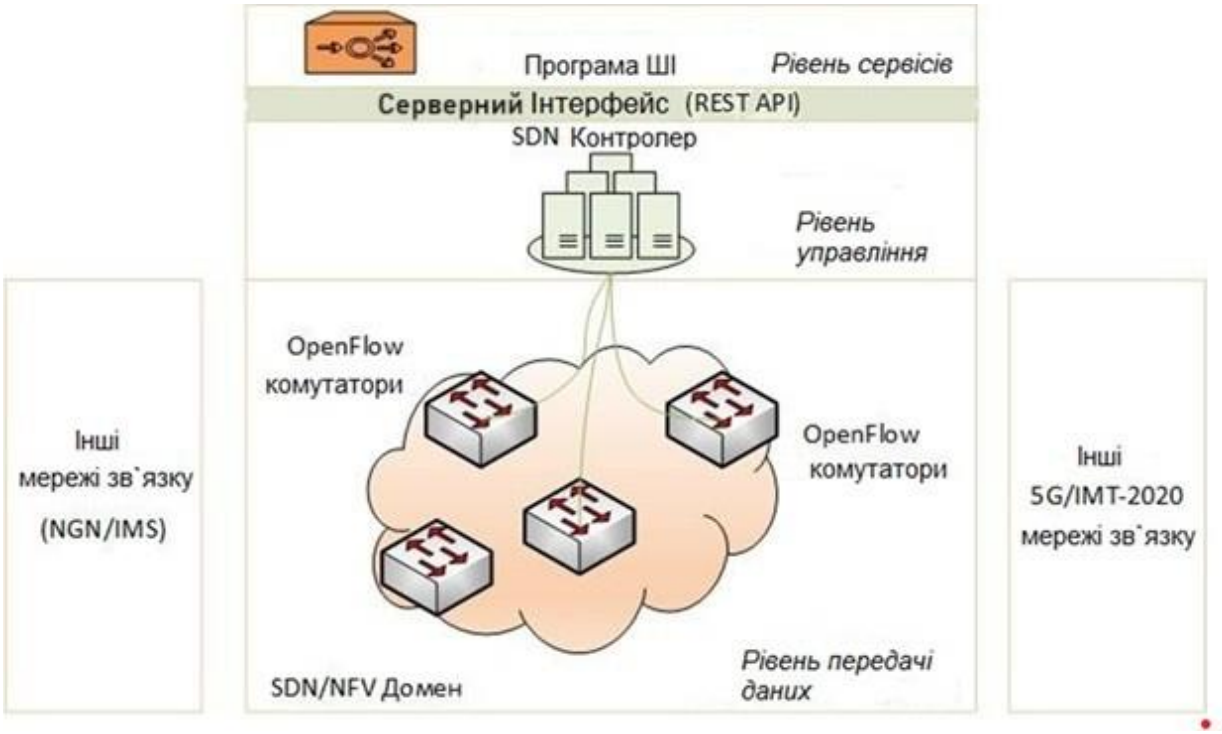


Рис. 1. Принципова архітектура системи ідентифікації трафіку на основі технології DPS

Для системи моніторингу трафіку поданого типу на основі технології DPS всі пристрої та потоки є «цифровим об'єктом», що має ряд параметрів та функцій (дій над параметрами), представленим набором методів [14,15.

Такий підхід дозволяє реалізувати систему моніторингу інфомаційно-комунікаційної мережі, яка працюватиме з даними про потоки (метадані) у режимі «на льоту». Дана система, через свої властивості, дозволяє не вносити додаткові затримки у трафік, а також будь-яким чином змінювати його активність (зміни законів розподілу, інтенсивність тощо). Основою функціонування даної системи є процес «спостереження» за активністю потоків і формування «загальної картини» передачі даних, що відбувається в підконтрольній мережі.

Вхідні дані для поданої системи формуються на основі тих даних, які система може отримати через серверний Інтерфейс контролера і Оркестратора мережі.

Оскільки у цій роботі розглядається аналітика активності потоків і виявлення потоків Інтернету Речей лише на рівні передачі даних, аналітична система має можливість запитати дані таблиць потоків

(Flow Tables) з усіх підконтрольних комутаторів SDN у контролера. Аналізуючи дані, що відображаються у двох глобальних частинах таблиці: Match Field і Actions, можна дійти висновку, що на їх основі можна скласти метамодель потоків. Скорочену структуру таблиці потоків комутатора відображено на Рис. 2.

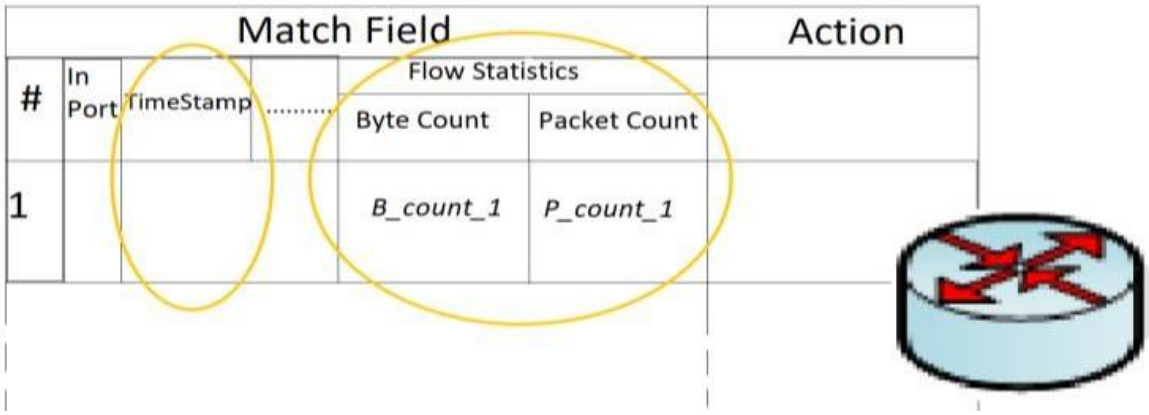


Рис. 2. Структура таблиці потоків комутатора S

На Рис. 2 жовтими колами виділено ті дані, які використовуються для формування метамоделі про досліджуваний потік у мережі.

Однією з важливих особливостей цих даних є те, що на основі лічильників Byte Count та Packet Count не можна визначити точну довжину пакета в потоці, оскільки за один момент часу лічильники можуть дорівнювати: Byte Count 1500, Packet Count

2. Відповідно, на основі цих даних не можна точно визначити довжину кожного з пакетів, зареєстрованих у потоці за проміжок часу: $\Delta T = 1$ с.

Варто також відзначити, що лічильники відображають сумарне значення параметрів [Byte Count, Packet Count]. Однак, крім даних лічильників у таблиці потоків існує ще один параметр – Time Stamp, який дозволяє оцінити в кожен момент часу миттєве значення [ByteCount_delta] та [PacketCount_delta]. Таким чином, за довільний період часу ΔT, маючи відліки значень [Byte Count], [Packet Count], [TimeStamp], можливо скласти набір даних з встановленої структурою даних, де кожен відлік відображає миттєве значення [ByteCount_delta] та [PacketCount_delta].

Відліки значень [Byte Count], [Packet Count], [TimeStamp] формуються шляхом щосекундних запитів на контролер мережі SDN через програмний інтерфейс RESTAPI. Структура формується на підставі запитів $DataSet_{RQ}$ з «сирими» даними. Вираз (1) та вираз (2), що є залежностями перетворення на необхідний формат $DataSet_{ML}$ з миттєвими значеннями (3) наведено нижче.

Приймемо:
TimeStamp_deltas –TS = 1 [sec.] = const,
PacketCount_delta – PC_{delta},
ByteCount_delta – BC_{delta}, а
Тоді:

$$DataSet_{RQ} = \begin{matrix} [TimeStamp] & [ByteCount] & [PacketCount] \\ TimeStamp_{11} & ByteCount_{12} & PacketCount_{13} \\ TimeStamp_{21} & ByteCount_{22} & PacketCount_{23} \\ \dots & \dots & \dots \\ TimeStamp_{N1} & ByteCount_{N2} & PacketCount_{N3} \end{matrix} \quad (1)$$

$$BC\_delta_{N2} = ByteCount_{N2} - ByteCount_{(N-1)} \quad \text{if } N \geq 1$$
$$PC\_delta_{N2} = PacketCount_{N2} - PacketCount_{(N-1)2} \quad \text{if } N \geq 1 \quad (2)$$

$$DataSet_{ML} = \begin{matrix} [TimeStamp] & [ByteCount] & [PacketCount] \\ TS_{delta11} & BC_{delta12} & PC_{delta13} \\ TS_{delta21} & BC_{delta22} & PC_{delta23} \\ \dots & \dots & \dots \\ TS_{deltaN1} & BC_{deltaN2} & PC_{deltaN3} \end{matrix} \quad (3)$$

При цьому розрахунок сумарних значень параметрів трафіку за встановлений проміжок часу пропонується здійснювати за виразами (4) та (5):

$$ByteCount = \sum_{\Delta T \rightarrow N=1}^{N=\Delta T/TS} BC_{deltaN2} \quad (4)$$

$$PacketCount = \sum_{\Delta T \rightarrow N=1}^{N=\Delta T/TS} PC_{deltaN2} \quad (5)$$

При цьому розрахунок сумарних значень параметрів трафіку за встановлений проміжок часу пропонується здійснювати за виразами (4) та (5):

ByteCount = ∑_(ΔT □(→⊥) N=1)^(N=ΔT⁄TS)▒〖BC〗 _deltaN2 (4)

PacketCount = ∑_(ΔT □(→⊥) N=1)^(N=ΔT⁄TS)▒〖PC〗 _deltaN2 (5)

Як було зазначено вище, для вирішення вищеописаного завдання було проведено комплексний аналіз математичних методів класифікації з урахуванням особливостей вхідних даних, аналізованих даних про потоки, а також особливостей початкової вимоги – роботи системи у режимі «на льоту».

В результаті проведеного аналізу обрано підхід використання нейронних мереж.

Визначена мета застосування нейронної мережі, а саме – ідентифікація та моніторинг трафіку мережі 5G/IMT-2020 при умові

роботи системи у режимі «на льоту» (мінімізація затримок вхідного потоку) та особливості ідентифікації та аналізу вхідних даних DataSetML - вир. (1)- (5) формують вимоги до нейронної мережі, що буде обрана для досягнення поставленої мети.

Відповідно до поставленої мети та особливостей вхідних даних DataSetML обрана відповідна архітектура нейронної мережі та подана система, алгоритм та методика її застосування.

На даний момент існує великий різновид нейронних мереж. Одним з типових завдань таких мереж є класифікація потоків даних (інформації) як об’єкту спостереження. Поширений спосіб класифікації – спосіб на основі описів об'єктів з використанням типових ознак, у якому кожен об'єкт характеризується набором числових чи нечислових ознак [16].

Аналіз типів даних, що включені в трафік мережі 5G/IMT-2020 показує, що їх відкриті ознаки не дають точності класифікації даних. Причина полягає в тому, що ці дані містять приховані ознаки, як то кількість та розміри пакетів даних, час їх затримки та інші.

Виходячи з цього, виникає необхідність в підборі стандартної нейронної мережі, призначеної до класифікації та аналізу даних трафіку, що мають приховані ознаки.

Аналіз ряду відомих нейронних мереж, призначених для моніторінгу потоків різних даних показав, що однією з таких нейронних мереж є нейронна мережа з функцією Deep Learning – функцією машинного навчання, що використовує багатошарові мережі для аналізу даних, автоматичного виоучення ознак та створення більш складних моделей для атрішення заданя індентифікації, моніторингу та аналізу. [16,17].

Вказана мережа є набором алгоритмів машинного навчання, які дозволяють моделювати високорівневі абстракції в масивах даних. В процесі такого моделювання вказана нейрона мережа Deep Learning здатна виділяти з даних приховані ознаки, при цьому нейронні мережі містять більше, ніж 2 прихованих шари. Тому, враховуючи особливості об'єкта моніторингу – трафік мережі 5G/IMT-2020) та його ознаки (числові статистичні ряди, що є метаданими) обрано вказану нейронну мережу з Deep Learning.

Розробка та навчання нейронної мережі Deep Learning проводилися на основі високорівневої мови програмування Python з її різноманітними бібліотеками та фреймворками.

Як штучну нейронну мережу для вирішення завдання моніторингу трафіку обрано рекурентну нейронну мережу з додатковими шарами LSTM (Long Short-Term Memory) [18]. Мережа LSTM є універсальною тому, що з достатньою кількістю нейронів вона має можливість виконувати будь-які обчислення, які може виконувати звичайний комп'ютер. Включений в мережу глибинний модуль LSTM, як частина штучної нейронної мережі (ШНМ), дозволяє виявляти закономірності впливу даних попередніх відліків на поточні з урахуванням великого розкиду значень між ними. Тобто, наприклад, періодичність, що може виявляється у трафіку Інтернету Речей, самоподібність характеру якого наводиться у багатьох працях [5,6,19].

Оскільки обрана архітектура нейронної мережі реалізує принцип «навчання із залученням вчителя», процес її застосування вимагає формування початкового навчального набору даних з маркованими позначками, та наступного збереження стану навченої мережі [19].

Для навчання нейронної мережі вхідний трафік DataSetML перетворюється в DataSetMLtrain шляхом додавання нового стовпчика даних, в кожномурядку якого стоїть ідентифікатор статистичної вибірки. Відповідно, для навчання розпізнавання більшого типу трафіку даний навчальний набір даних потрібно розширити, помітивши відповідну статистичну вибірку міткою трафіку, наприклад – IoT [17,18].

Архітектура мережі Deep Learning містить 2 повнопов'язані глибинні рівні LSTM і 2 пов'язані глибинні рівні RNN (Recurrent Neural Network), кожен з яких містить 7 прихованих нейронів.

Запропонований метод моніторингу трафіку мережі пропонується реалізуватиу вигляді

програмного модуля мовою програмування Python версії 2.7 для аналітичної системи, реалізованої на основі MVC патерну.

Дане програмне забезпечення, відповідного обраного підходу до ідентифікації, схематично поданого на Рис.3 втіленням відповідної функції, реалізованої через програмний застосунок, вкладений поверх серверного програмного інтерфейсу API контролера програмно-конфігурованої мережі та Оркестратора мережі лабораторії.

Для формування навчальних для Штучної Нейронної Мережі наборів даних визначено спеціальні умови [17,18]:

– будь-який інший трафік, що не відноситься до дослідження, що проводиться, повинен бути вимкнений і не проходити в SDN-сегмент;

– мережа повинна бути модифікована так, щоб була можливість однозначно ідентифікувати потік з трафіком, що генерується в таблиці потоків комутаторів.

Для апаратної реалізації програмно-апаратного комплексу нейронної мережі, що забезпечить дослідження методів та алгоритмів застосування Штучного інтелекту для мереж зв'язку 5G/IMT-2020 пропонується наступна архітектура лабораторного комплексу, що подана на Рис.1 [20,21,22].

Лабораторний комплекс пропонується побудувати в вигляді з'єднаних в кільце трьох програмно-керованих комутаторів SDN, що реалізують протокол OpenFlow версії 1.0. Вибраний SDN- контролер з відкритим вихідним кодом OpenDaylight програмно-конфігурованої мережі реалізує розподіл навантаження по мережі за замовчуванням. Оскільки цей стенд зібраний в першу чергу з метою проведення досліджень, у рівень управління вказаним компрлексом інтегрований звичайний комутатор Ethernet, який агрегує всі службові потоки і забезпечує доступність контролера SDN. Також в мережі даного комутатора реалізовано доступ до серверного рівня контролера SDN.

Для розширення кількості можливих підключень до кожного комутатора SDN був послідовно підключений простий Ethernet-комутатор, що виконує роль агрегації вхідного потоку в топології поданого комплексу.

За основу програмного забезпечення SDN-контролер пропонується застосувати модульну архітектуру Java Karaf, яка забезпечує необхідну розширюваність контролера шляхом встановлення необхідних додаткових модулів або власної розробки модулів з подальшою інтеграцією до програмної шини контролера.

В якості Оркестратора мережі пропонується застосування програмного рішення – OpenStack, яке інтегрується також із рішенням OpenDaylight через програмний модуль «OpenStack Neutron» [11,23].

Для реалізації трафік-генератора типового сервісу Інтернету Речей пропонується застосування серверу з операційною системою Linux Ubuntu версії LTS з встановленим і налаштованим сервісом IoTDM (Internet of Things Data Management), що розроблений окремим підрозділом OpenDaylight з складу консорціуму The Linux Foundation [20,23].

Функціонування комплексу передбачає умову, при якій всі програми розгортаються на одному фізичному сервері. У процесі розробки роль сервера виконує персональний ноутбук, у процесі тестування стаціонарний ПК.

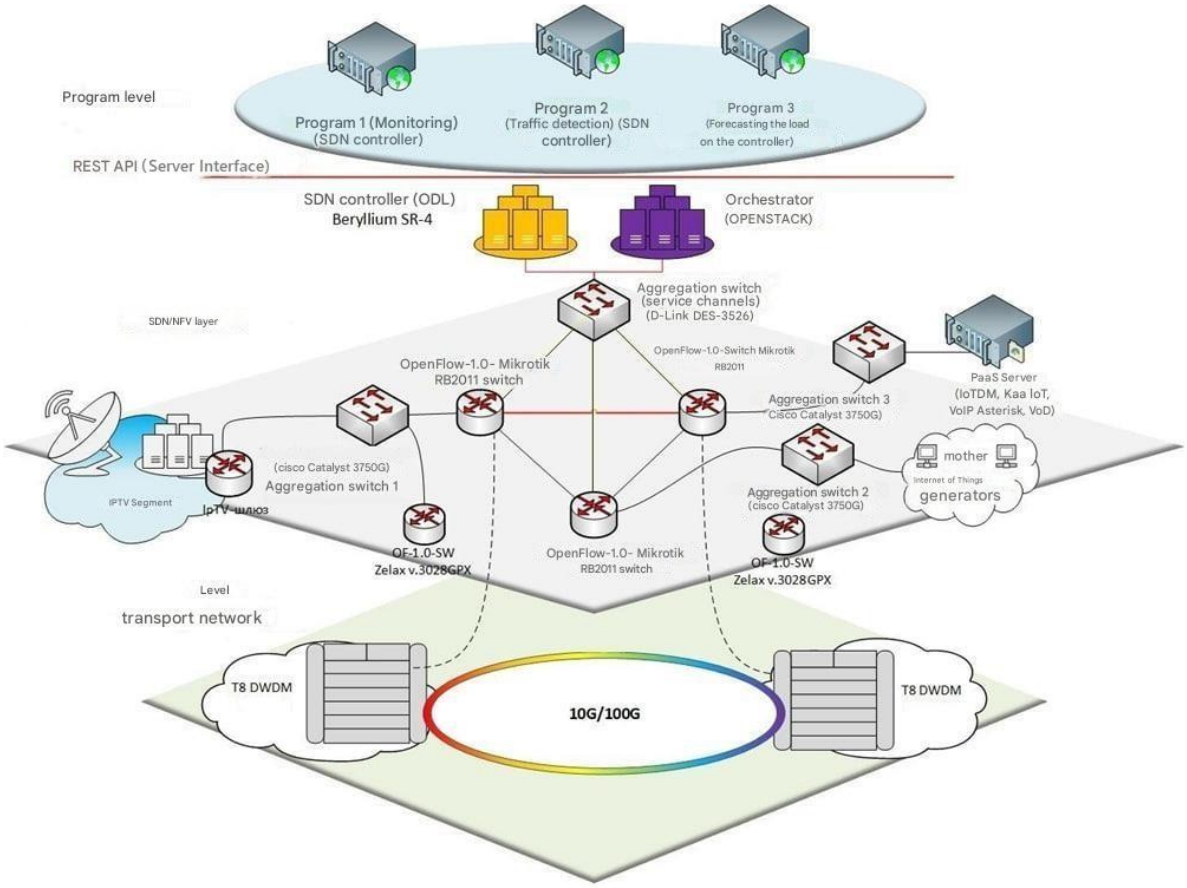


Рис. 3. Архітектура програмно-апаратного комплексу нейронної мережі

В результаті експериментального дослідження за допомогою запропонованого програмно-апаратного комплексу, схематично поданого на Рис.3 отримано масив даних DataSetMLtrain, який сформований з двох маркованих наборів даних (IoT, Video).

Далі DataSetMLtrain подається на вхід нейронної мережі, конфігурація якої відображена вище.

За отриманим масивом DataSetMLtrain побудована діаграма розкиду значень. Діаграма наведена на Рис. 4.

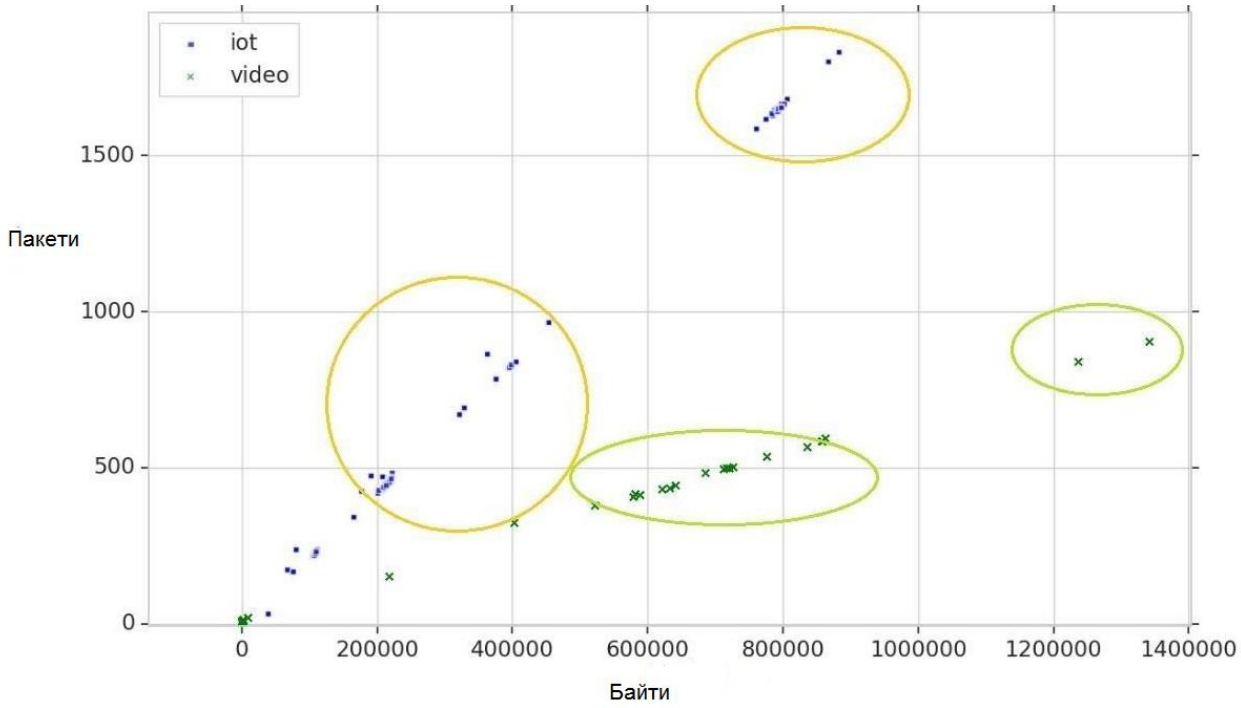


Рис. 4. Діаграма розкиду значень DataSetML$train$

Після того, як навчальний набір даних сформований, згідно з алгоритмом, викладеним вище в цій роботі, програмний модуль розробленого додатка, що реалізує Штучну Нейронну Мережу, переходить до процесу навчання нейронної мережі.

Протягом процесу навчання нейронної мережі розробленим додатком контролюються та фіксуються значення наступних параметрів [23,24]:

Train Accurancy (Точність навчання);

Test Accurancy (Точність проходження тесту ШНМ);

Train loss (Помилки під час навчання);

Test loss (Помилки під час проходження тесту ШНМ);

Графік, що відображає дані параметри у процесі проходження епох навчання, наведено на Рис.5.

Аналіз залежностей, поданих на Рис.5, Рис.6, де відображено процес навчання мережі, показав, що для поставленого завдання моніторингу трафіку розроблена штучна нейронна мережа успішно пройшла процес навчання. В результаті процесу навчання нейронної мережі та перевірки її роботи на тестових наборах даних у навченому стані розроблена нейронна мережа може ідентифікувати потік Інтернету Речей, що генерується, з ймовірністю 99,7%.

Варто відзначити, що отримана ймовірність розпізнавання потоків даних (трафік даних від мережі Інтернету Речей та трафік Відео) має досить високі значення і при збільшенні кількості типів трафіку, що розпізнаються, дана ймовірність може знизитися, проте перебуває у допустимих межах (80-90%) [21,22].

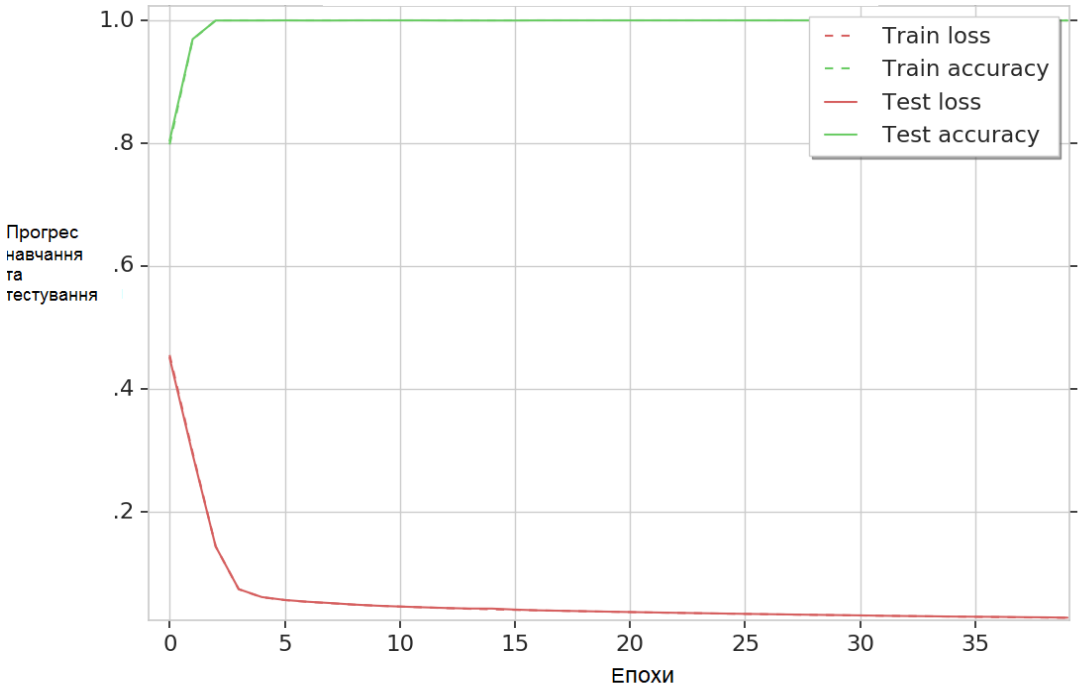


Рис. 5. Графік навчання та тестування штучної нейронної мережі

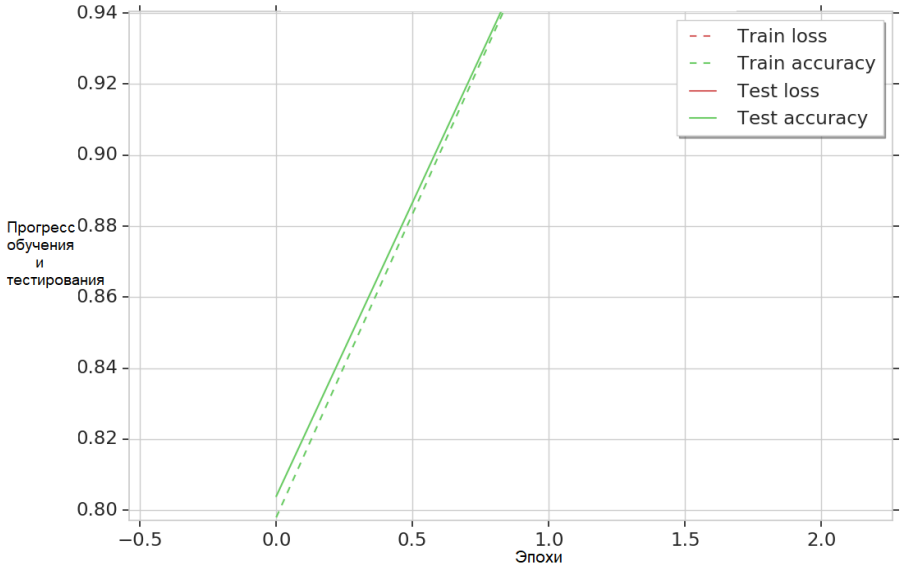


Рис. 6. Масштабований графік навчання та тестування штучної нейронної мережі

Таким чином, запропоновано метод моніторингу навантаження в телекомунікаційних мережах 5G/IMT-2020, який включає:

– процес формування метамоделі потоків вхідних даних в мережу 5G/IMT-2020: DataSetML = ([Byte Count], [Packet Count], [TimeStamp]);

– модифікація DataSetML в навчальний набір DataSetMLtrain шляхом включення в набір даних ідентифікаторів статистичної вибірки;

– формування програмно-апаратного комплексу навчання та оцінки ефективності застосування нейронної мережі для моніторингу навантаження в мережі 5G/IMT-2020;

– побудову структури нейронної мережі Deep Learning з додатковими шарами LSTM;

– реалізацію процесу навчання нейронної мережі та підготовка її до функціонування за призначенням;
– втілення запропонованого методу та програмно – апаратного комплексу в процес моніторингу навантаження трафіку в телекомунікаційних мережах 5G/IMT-2020.

ВИСНОВКИ

1. В роботі проведено аналіз процесу ідентифікації вхідного трафіку в мережах 5G/IMT-2020, побудованих по технології Ultra-reliable and low latency communications та визначені його особливості та напрямки досліджень по підвищенню ефективності його моніторингу.
2. Для вирішення завдання моніторингу та ідентифікації трафіку мережі 5G/IMT-2020в роботі розроблена та подана відповідна методика моніторингу. Вказана методика включає формування масивів метаданих вхідного потоку, модифікацію їх в набір навчальних даних, формування навчального програмно-апаратного комплексу та розбудову структури нейронної мережі, проведення процесу навчання нейронної мережі та втілення її в процес моніторингу навантаження в телекомунікаційних мережах 5G/IMT-2020.
3. Оцінка результатів процесу навчання запропонованої нейронної мережі та перевірки її роботи на тестових наборах даних у навченому стані показала, що подана в роботі нейронна мережа здатна провести моніторинг та ідентифікувати згенерований від сервісів Інтернету Речей трафі з ймовірністю до 99,7%.

В процесі моніторингу та ідентифікації трафіку від двох та більше сервісів дана ймовірність може знизитися, проте перебуває у допустимих межах 80-90%.

REFERENCES

1. В.**С. Шуста, А.І. Сусла, В.Ю. Біганич**, «Трансформація мережевих технологій: від 4G до 5G», Вчені записки ТНУ імені В.І. Вернадського, Серія: Технічні науки, 2024, 3, С.94-99
2. **Technical Report I**TU-T GSTP-TN5G: Transport network support of IMT-2020/5G. – SG15- TD338/PLEN, October 2018.
3. Draft Recommendation Characteristics of transport networks to support IMT-2020/5G (Gctn5g). – SG15-TD295/PLEN, October 2018
4. **S. Hendaoui, F. Hendaoui, N. Zangar**, «Dynamic proactive–reactive scheduling for URLLC in 5G: Leveraging XGBoost and network virtualization», Physical Communication, 68, art. no. 102553. 2025.
5. **X. Shen, W. Liao, Q.Yin**, «A Novel Wireless Resource Management for the 6G-Enabled High-Density Internet of Things», IEEE Wirel. Commun, 2022, 29, p.32–39.
6. **X. Li, L.D. Xu**, «A Review of Internet of Things—Resource Allocation», IEEE Internet Things J., 2021, 8, p.8657–8666.
7. the Internet of Things: A Survey», J. Netw. Comput. Appl. 2022, 206, 103464.
8. **A.A. Ateya, S. Bushelenkov, A. Muthanna, A. Paramonov,** «Multipath Routing Scheme for Optimum Data Transmission in Dense Internet of Things», Mathematics. 2023; 11(19):4168.
9. **Yongho Seok, Youngseok Lee, Yanghee Choi and Changhoon Kim,** "Dynamic constrained multipath routing for MPLS networks", Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495), Scottsdale, AZ, USA, 2001, pp. 348-353.
10. **W.A. Aljoby, X. Wang, D.M. Divakaran, T.Z.J. Fu,** «DiffPerf: Toward Performance Differentiation and Optimization WithSDN Implementation», IEEE Transactions on Network and Service Management, 2024, 21(1), pp. 1012 – 1031.
11. **L. Brown,** «Advanced Techniques in NFV and SDN for Scalable Networks», International Journal of Communications Technology, 2022, 12(4), з.78-92.
12. **L.-H. Chang, Tsung-Han Lee, Hung-Chi Chu, and Cheng-Wei Su,** "Application-Based Online Traffic Classification with Deep Learning Models on SDN Networks", Adv. technol. innov., Sep. 2020, 5(4), pp. 216–229.
13. **P.K.R. Maddikunta, Q.-V. Pham, D.C. Nguyen**, (eds), «Incentive Techniques for the Internet of Things: A Survey», J. Netw. Comput. Appl. 2022, 206, 103464.
14. **Foreman, Justin, Waters, Willie L., Kamhoua, Charles A., Hemida, Ahmed H. Anwar, Acosta** (2024) Detection of Hacker Intention Using Deep Packet Inspection? Journal of Cybersecurity and Privacy, 4 (4), pp. 794 – 804. DOI: 10.3390/jcp4040037

15. **Parra G. D. L. T., Rad P., Choo K. K. R., Beebe N.** Detecting internet of things attacks using distributed deep learning. Journal of Network and Computer Applications, 2020, vol. 163, pp. 102662. doi:10.1016/ j.jnca.2020.102662
16. **Al-Garadi M. A., Mohamed A., Al-Ali A., Du X., Guizani M. A** Survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 2020, vol. 22, no. 3, pp. 1646–1685. doi:10.1109/COMST.2020.2988293
17. **Pacheco, Fannia & Exposito, Ernesto & Gineste, Mathieu & Baudoin, Cédric & Aguilar**, **Jose.** (2018). Towards the Deployment of Machine Learning Solutions in Network Traffic Classification: A Systematic Survey. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2018.2883147.
18. **Hochreiter, Sepp & Schmidhuber, Jürgen**. (1997). Long Short-Term Memory. Neural Computation. 9. 1735-1780. 10.1162/neco.1997.9.8.1735.
19. **Кондакова, А., Корецький, О.** (2024). Моделі побудови мереж інтернету речей для управління інфраструктурою міста. Smart Technologies, 2(15), 124–132. DOI: https://doi.org/10.32347/st.2024.2.1901
20. **Oleksandr Koretskyi, Rodion Khvorostianyi, Yevhen Bondarenko** Hardware and software complex for the functioning of a neural network for identification and traffic management in 5G/IMT-2020 networks. The IV International Conference «Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT», м. Київ, Україна, 21-22 січня 2025 р., Київ, КНУБА. С.44-49. https://drive.google.com/file/d/145aOtud0A7zl 4N9RKXiFyt9iMLKYsMt_/view
21. **J.Yao, Y. Wang, Q. Li, Mao** (2022). An Efficient Routing Protocol for Quantum Key Distribution Networks. Entropy, No.24, 911.
22. Study on Scenarios and Requirements for Next Generation Access Technologies (3GPP TR 38.913 version 14.2.0 Release 14). https://www.etsi.org/deliver/etsi_tr/138900_138 999/138913/14.02.00_60/tr_138913v140200p.p df
23. **F. H. Nazir, Q. Ahmad, R. Badlishah, & Elias**, (2017). «Software-Defined Network Testbed Using ZodiacFX a Hardware Switch for OpenFlow», ICST Transactions on Scalable Information Systems», No.4. 153150.
24. **V. Artem, A.A. Ateya , A. Muthanna, A. Koucheryavy**, (2019). Novel AI-Based Scheme for Traffic Detection and Recognition in 5G Based Networks», In: Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds), «Internet of Things, Smart Spaces, and Next Generation Networks and Systems», Lecture Notes in Computer Science, No. l, 11660. Springer, Cham.

Traffic identification method in 5g/imt-2020 telecommunication networks based on artificial intelligence

Oleksandr Koretskyi, Anastasiia Kondakova

Abstract. The paper analyzes the process of identifying incoming traffic in 5G/IMT-2020 networks, built on the Ultra-reliable and low latency communications technology, identifies its features and research directions to improve the efficiency of traffic identification taking into account the requirements for the functioning of the considered network.

To solve the problem of identifying traffic in the 5G/IMT-2020 network, the paper develops and presents an appropriate methodology. The specified methodology includes the formation of metadata arrays of the incoming stream, their modification into a set of training data, the formation of a training software and hardware complex and the development of the neural network structure, the training process of the neural network and its implementation in the process of identifying traffic in 5G/IMT-2020 telecommunication networks.

Evaluation of the results of the training process of the proposed neural network and verification of its operation on test data sets in the trained state showed that the neural network presented in the work is able to monitor and identify traffic generated from Internet of Things services with a probability of up to 99.7%. In the process of monitoring and identifying traffic from two or more services, this probability may decrease, but is within the acceptable limits of 80-90%.

Keywords: identification of incoming traffic of information and communication networks, 5G/IMT-2020 network, artificial intelligence, neural network, information and communication network load management.