МАГІСТЕРСЬКА РОБОТА

МР. ІПм - 23.00.00.000 ПЗ

Група ІПм-23-3

Слижук Андрій

2024

Івано-Франківський національний технічний університет нафти і газу

Інститут інформаційних технологій

Кафедра інженерії програмного забезпечення

Слижук Андрій Іванович

(прізвище, ім'я, по батькові)

УДК 004.942

(індекс)

МАГІСТЕРСЬКА РОБОТА

Моделі та методи машинного навчання для контролю контекстів в комунікаційних системах

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Слижук А.І.

(підпис, ініціали та прізвище здобувача освітнього ступеня)

Науковий керівник Тимків Дмитро Федорович, д.т.н., професор

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту

Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Нормоконтроль

доц. Вовк Р.Б.

(посада) (підпис) (дата) (ініціали та прізвище)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Івано-Франківськ – 2024

Івано-Франківський національний технічний університет нафти і газу

Інститут інформаційних технологій

Кафедра інженерії програмного забезпечення

Освітній рівень магістр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**
доц. В.В. Бандура
“ 04 ” вересня 2024 р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Слижуку Андрію Івановичу

(прізвище, ім’я, по-батькові)

1. Тема магістерської роботи “ Моделі та методи машинного навчання для контролю контекстів в комунікаційних системах”

керівник проекту (роботи) Тимків Дмитро Федорович, д.т.н., професор

затверджені наказом закладу вищої освіти від “ 22 ” листопада 2024 р. № 781/7

2. Строк подання студентом проекту (роботи) 15 грудня 2024 р.

3. Вихідні дані до проекту (роботи) Теоретичні концепції та формальні моделі побудови та функціонування інформаційних технологій машинного навчання

4. Зміст розрахунково - пояснювальної записки(перелік питань, які потрібно розробити)

1. Аналіз предметної області застосування штучного інтелекту в комунікаційних системах
2. Дослідження алгоритмів та методів машинного навчання для обробки інформації
3. Імплементація методів машинного навчання для контролю контекстів
4. Виявлення аномалій у бездротових комунікаційних мережах засобами машинного навчання

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

1. Застосування ШІ в бездротових системах (рис. 1.1)
2. Особливості машинного та глибокого навчання (рис. 1.2)
3. Приклад системи контрольованого навчання (рис. 1.3)
4. Машинне навчання без вчителя (рис. 1.4)
5. Використання CNN для класифікації рукописних цифр (рис. 1.5)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата
Перевірка на плагіат	доц., к.т.н. Вовк Р.Б.	

7. Дата видачі завдання 04 вересня 2024 р.

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір і вивчення літератури по темі магістерської роботи	15.09.2024	виконано
2	Аналіз концепцій та алгоритмів предметної області	29.09.2024	виконано
3	Дослідження предметної області застосування штучного інтелекту в комунікаційних системах	15.10.2024	виконано
4	Дослідження алгоритмів та методів машинного навчання для обробки інформації	08.11.2024	виконано
5	Імплементація методів машинного навчання для контролю контекстів	20.11.2024	виконано
6	Виявлення аномалій у бездротових комунікаційних мережах засобами машинного навчання	01.12.2024	виконано
7	Затвердження пояснювальної записки роботи завідувачем кафедри	15.12.2024	виконано

Студент – магістр _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Магістерська робота: 81 с., 26 рис., 2 табл., 54 джерела.

Тема: Моделі та методи машинного навчання для контролю контекстів в комунікаційних системах

Об'єкт дослідження: процеси контролю контекстів і виявлення аномалій у комунікаційних системах на основі методів машинного та глибокого навчання.

Мета роботи: розробка ефективних моделей і методів машинного навчання для контролю контекстів та виявлення аномалій у комунікаційних системах, що забезпечують семантичний аналіз даних у відеоінформації та ресурсах бездротових мереж.

Предмет дослідження: методи та моделі машинного навчання для вилучення релевантних ознак та виявлення аномалій у спектральній інформації у бездротових мережах.

Результати дослідження

В роботі запропоновано дві моделі використання H-Score для вилучення малорозмірних релевантних ознак як у відеоданих IoBT, так і в спектральній інформації.

Висновок

Розроблені моделі можуть бути використані для підвищення безпеки та надійності комунікаційних систем у складних умовах, таких як IoBT та бездротові мережі з обмеженими ресурсами. Використання запропонованих методів дозволить створити ефективніші системи для виявлення загроз та адаптивного контролю контекстів у мережах.

МАШИННЕ НАВЧАННЯ, ГЛИБОКЕ НАВЧАННЯ, ВИЯВЛЕННЯ АНОМАЛІЙ, КОНТРОЛЬ КОНТЕКСТІВ, ВІДЕОІНФОРМАЦІЯ, СПЕКТРАЛЬНИЙ АНАЛІЗ, H-SCORE, ІНТЕРНЕТ ПОЛЯ БИТВИ (IoBT), БЕЗДРОТОВІ КОМУНІКАЦІЙНІ МЕРЕЖІ.

ABSTRACT

Master Thesis: 81 pp., 26 fig., 2 tab., 54 sources.

Thesis Subject: Machine learning models and methods for context control in communication systems

Research object: processes of context control and anomaly detection in communication systems based on machine and deep learning methods.

The purpose of the work: development of effective models and methods of machine learning for monitoring contexts and detecting anomalies in communication systems that provide semantic analysis of data in video information and wireless network resources.

Research subject: machine learning methods and models for extracting relevant features and detecting anomalies in spectral information in wireless networks.

Research results

In the paper, we propose two models to use H-Score to extract small-scale relevant features in both IoBT video data and spectral information.

Conclusion

The developed models can be used to improve the security and reliability of communication systems in complex environments, such as IoT and wireless networks with limited resources. The use of the proposed methods allows creating more effective systems for detecting threats and adaptive control of contexts in networks.

MACHINE LEARNING, DEEP LEARNING, ANOMALY DETECTION, CONTEXT MONITORING, VIDEO INFORMATION, SPECTRAL ANALYSIS, H-SCORE, INTERNET OF BATTLEFIELD (IoBT), WIRELESS COMMUNICATION NETWORKS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DL - Deep Learning (Глибоке навчання)

ML - Machine Learning (Машинне навчання)

AI - Artificial Intelligence (Штучний інтелект)

NN - Neural Network (Нейронна мережа)

CNN - Convolutional Neural Network (Згорткова нейронна мережа)

LSTM - Long Short-Term Memory (Довгострокова короткочасна пам'ять)

GRU - Gated Recurrent Unit (Рекурентний блок з воротами)

NLP - Natural Language Processing (Обробка природної мови)

CIE - Contextual Information Extraction (Вилучення контекстної інформації)

UE - Unsupervised Extraction (Ненаглядна екстракція)

FE - Feature Extraction (Вилучення ознак)

HDI - High-Dimensional Information (Високовимірна інформація)

LDI - Low-Dimensional Information (Низьковимірна інформація)

5G - Fifth-generation wireless technology (П'яте покоління бездротової технології)

IoBT - Internet of Battlefield

UE - User Equipment (Користувацьке обладнання)

BS - Base Station (Базова станція)

SNR - Signal-to-Noise Ratio (Співвідношення сигнал-шум)

BER - Bit Error Rate (Швидкість помилок бітів)

QoS - Quality of Service (Якість обслуговування)

HGR - Hirschfeld-Gebelein-Rényi correlation (Кореляція Хіршфельда-Гебелеїна-Реньї)

ВСТУП

Актуальність теми.

Розвиток сучасних технологій передачі даних та зростання обсягів інформації у комунікаційних системах висувають нові вимоги до надійності, безпеки та ефективності цих систем. Зокрема, у бездротових мережах, де обмежені ресурси спектру та інтенсивний потік даних ускладнюють контроль за якістю і безпекою зв’язку, є потреба у нових підходах до обробки та контролю контекстів, особливо в умовах різнорідної та великовимірної інформації. Питання стає особливо актуальним у рамках концепції "Інтернет поля битви" (IoBT), де семантична обробка інформації має вирішальне значення для забезпечення ефективного управління ситуаційною обізнаністю у військових та інших критично важливих середовищах.

Окрім того, у сучасних бездротових мережах постає проблема обмеженої доступності спектра через зростання кількості користувачів і пристроїв, які конкурують за ресурси спектра. Це призводить до збільшення ризику несанкціонованого втручання та зловживань спектральними ресурсами, що може значно знизити ефективність і безпеку комунікацій. Виявлення таких вторгнень та аномалій у спектрі стає критично важливим завданням, яке потребує надійних та ефективних рішень на основі машинного навчання, здатних виявляти потенційні загрози в режимі реального часу.

З огляду на обсяги і складність даних, що зростають, традиційні методи аналізу й контролю даних виявляються недостатніми для забезпечення гнучкої, точної та адаптивної обробки інформації. Методи машинного та глибокого навчання дозволяють підвищити продуктивність таких систем завдяки здатності швидко обробляти великі масиви даних та виділяти значущі ознаки навіть у непередбачуваних і динамічно змінюваних умовах. Крім того, машинне навчання дозволяє вирішувати завдання семантичного аналізу відеоінформації, що є необхідним для створення систем, які можуть

оперативно реагувати на зміни в контексті ситуацій, таких як розташування ворогів або інші важливі об’єкти в полі бою.

Актуальність дослідження також обумовлена необхідністю впровадження систем інтелектуального моніторингу та управління, здатних до адаптації під час виникнення нових загроз або змін у комунікаційних середовищах. У такому контексті розробка систем для контролю контекстів на основі машинного навчання сприятиме підвищенню якості та безпеки зв'язку, дозволить зменшити ризики несанкціонованого доступу до спектра, а також забезпечить підтримку семантичних комунікацій у високозавантажених середовищах з обмеженою пропускною здатністю, що робить дане дослідження особливо актуальним для сучасних умов.

Мета дослідження - розробка ефективних моделей і методів машинного навчання для контролю контекстів та виявлення аномалій у комунікаційних системах, що забезпечують семантичний аналіз даних у відеоінформації та ресурсах бездротових мереж.

Об’єкт дослідження - процеси контролю контекстів і виявлення аномалій у комунікаційних системах на основі методів машинного та глибокого навчання.

Предмет дослідження - методи та моделі машинного навчання для вилучення релевантних ознак та виявлення аномалій у спектральній інформації у бездротових мережах.

Відповідно до мети роботи було сформовано наступні **задачі:**

- Провести аналіз існуючих моделей та алгоритмів машинного навчання для контролю контекстів та виявлення аномалій.
- Розробити архітектуру системи обробки відеоінформації на основі глибокого навчання для мереж IoBT.
- Запропонувати модель для виявлення аномалій у спектрі бездротових комунікаційних мереж.

- Оцінити ефективність розроблених методів та моделей, зокрема точність вилучення релевантних ознак і продуктивність у виявленні аномалій.
- Провести експериментальні дослідження з використанням H-Score для вилучення значущих ознак у відеосимуляторі бою та спектральних даних Wi-Fi.

Методи дослідження.

У дослідженні використано методи глибокого та машинного навчання для вилучення ознак, метод м'якої кореляції Хіршфельда-Гебелеїна-Реньї (HGR), а також інформаційно-теоретичні підходи для аналізу аномалій у даних. Ефективність розроблених моделей оцінювалась за допомогою метрик точності та співвідношення сигнал/шум (SNR).

Наукова новизна отриманих результатів

Запропоновано архітектуру системи для вилучення критичних ознак із відеоінформації на основі глибокого навчання, що дозволяє підвищити точність відстеження об'єктів у реальному часі навіть за умов непередбачуваного фону.

Практичне значення магістерської роботи

Розроблено підхід для виявлення аномалій у спектрі сигналів бездротових мереж на основі глибокого навчання, що демонструє високу точність у різних діапазонах SNR.

Структура магістерської роботи. Робота складається зі вступу, трьох розділів та висновків. Загальний обсяг роботи становить 81 сторінку, і містить 26 рисунків, 2 таблиці, список використаних джерел із 54 найменувань.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1. Особливості використання методів машинного навчання в бездротових комунікаційних системах

У останні роки спостерігається стрімке зростання обсягу даних, що генеруються бездротовими системами. З розвитком технологій 5G стало критично важливим ефективно обробляти ці дані.

Зокрема, коли обсяг інформації є надмірним, виникає практична необхідність знаходити корисну інформацію для ефективного використання комунікаційних ресурсів та для кращого прийняття рішень.

Широко поширена інтеграція між бездротовими стандартами 5G (B5G) і новими кіберфізичними системами генеруватиме величезний обсяг трафіку даних у масштабі зетабайтів і створюватиме значне навантаження на сучасні бездротові мережі з обмеженою пропускною здатністю [36, 42]. Вкрай важливо ефективно обробляти дані, щоб можна було оптимізувати використання основних комунікаційних ресурсів і отримувати низьку затримку даних, що могла б сприяти кращому прийняттю рішень.

Більшість існуючих систем бездротового зв'язку розроблено для оптимізації метрики, орієнтованої на дані, наприклад, бітової швидкості та частоти бітових помилок, і ігнорує контекст інформації, наприклад, терміновість, цінність і пріоритет [29]. На рис. 1.1 [2] ми можемо побачити деякі застосування машинного навчання в бездротових системах. Таким чином, застарілі засоби бездротового зв’язку не в змозі визначити пріоритет критичного та термінового інформаційного вмісту над некритичною та нетерміновою інформацією. Навпаки, семантичні комунікації надають пріоритет сприйняттю та використанню точного значення переданих повідомлень над звичайними показниками точності на рівні бітів [4 , 25]. У семантичних комунікаціях передавач витягує важливу та релевантну

інформацію (також відому як семантичні характеристики) з повідомлень, які потрібно надіслати, кодує ці особливості в бітові послідовності, а приймач інтерпретує семантичні характеристики відповідно до передбачуваного значення [3]. Передаючи необхідну інформацію невеликою кількістю пакетів даних через бездротове середовище, семантичні комунікації можуть значно заощадити ресурси пропускної здатності, зменшити затримку та перевантаження трафіку, а також підвищити своєчасність отриманої інформації. Однак семантичні комунікації вимагають інтелектуальних і складніших трансиверів із глибоким навчанням (DL), які дають змогу витягувати семантичні характеристики з повідомлень і відновлювати значення з них.

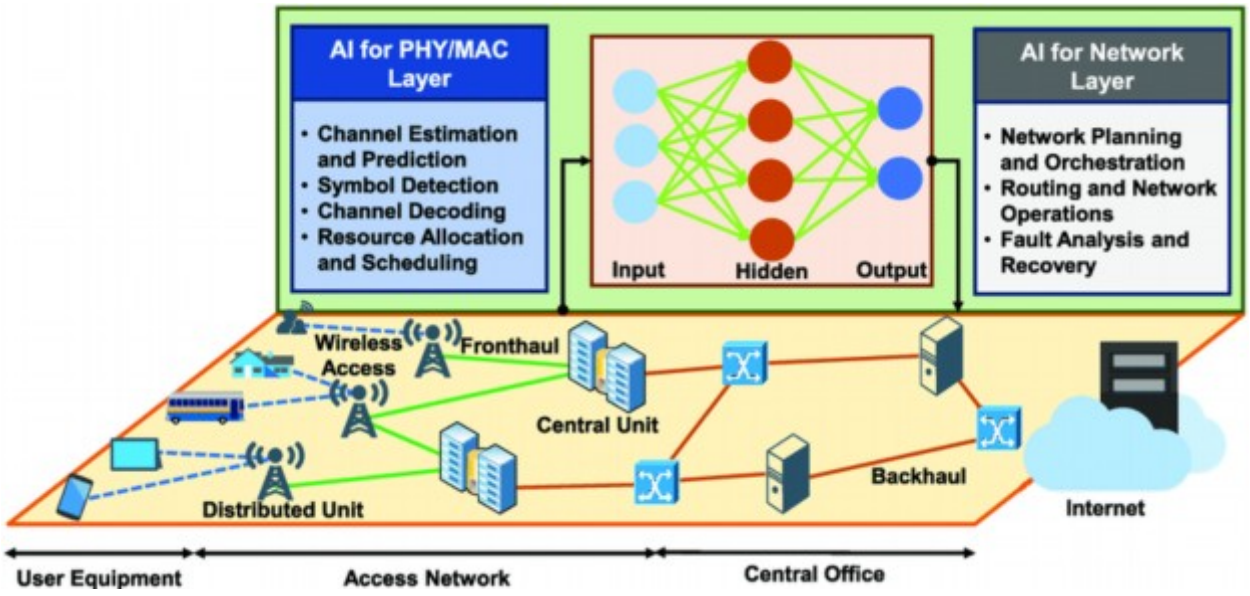

Рис. 1.1. Застосування ШІ в бездротових системах [2]

Критичним аспектом семантичних комунікацій є обробка контекстної інформації для генерації інформаційних функцій, які точно передають бажане значення одержувачу. Обробка контекстної інформації в практичному сценарії бездротового зв'язку демонструє такі проблеми. По-перше, інформація, отримана у формі аудіо, зображення та відео, справді є мультимодальною. За своєю суттю складно виділити важливі та критичні

характеристики для передбачуваного значення з мультимодальних даних, особливо за наявності обширної довідкової інформації. По-друге, згенеровані функції повинні бути стійкими до семантичного шуму, викликаного невідповідністю між базою знань у передавача та приймача, а також помилок, викликаних бездротовим каналом [29]. Нарешті, отримана інформація в дуже динамічному сценарії, що змінюється в часі, має сильну просторову та часову кореляцію. По суті, обробка контекстної інформації в динамічному середовищі не тільки вимагає ефективного придушення фонового шуму, але також вимагає використання просторово-часової кореляції.

Зі стрімким розвитком радіотехнологій постає ще один виклик. Зростання кількості пристроїв Інтернету речей і кінцевих користувачів, які використовують радіотехнології та їхній основний спектр, погіршив обмежену доступність спектру. Цей сплеск використання також призвів до різкої активності зловмисників у використанні спектру, наприклад, останнім часом значно зросли перешкоди в Глобальній навігаційній супутниковій системі (GNSS). Стало дуже важливо ідентифікувати цих учасників або аномалії в спектрі, щоб це не вплинуло на реальний досвід користувача на платформі.

У сценаріях реального світу дані генеруються в Інтернет-масштабі, більшість із яких є немаркованими. Нестача цих позначених даних ускладнює використання алгоритмів глибокого навчання для отримання важливої інформації. У програмах виявлення аномалій аномалія часто не позначена. Алгоритми виявлення аномалій знаходять шаблон нормального сигналу/неаномального сигналу, а потім позначають будь-яку іншу точку даних як аномалію, якщо шаблон відрізняється від нормального шаблону. Виявлення цієї нормальної моделі стає ще більш складним за наявності шуму. Фактичні сигнали можуть бути поховані під шумом і перешкодами в спектрі. Такі алгоритми, як автокодери, знаходять прихований латентний простір даних, але вони також кодують шум, що ускладнює обробку сигналу.

Отже, новий алгоритм для вилучення корисних функцій зі спектру також має вирішальне значення для виявлення сигналу та моніторингу спектру.

1.2. Задачі магістерського дослідження

Наша мета полягала в тому, щоб розробити структуру неконтрольованого навчання, яку можна використовувати для вилучення критичних даних із постійного потоку даних, особливо даних відеопотоку. Ми демонструємо наш підхід, використовуючи два сценарії: перший сценарій – це вилучення критичної інформації в динамічному середовищі на полі бою, а другий – виявлення радіочастотних аномалій у бездротових сигналах без використання будь-яких позначених прикладів у всьому конвеєрі.

Зокрема, важливість вилучення функцій у мережах з обмеженими ресурсами в контексті мереж IoBT (Internet of Battlefield) передбачає збір величезних обсягів мультимодальних даних із широко розгорнутих мережевих датчиків і обчислювальних пристроїв [7]. Через дуже динамічний характер полів битв важлива та критична інформація легко ховається під некритичною інформацією. Тим часом через обмеження пропускної здатності вкрай неефективно безпосередньо надсилати необроблені зображення чи відео до командного центру. Отже, мережеві ресурси повинні бути пріоритетними для надійної передачі критичної інформації до командного центру.

У цьому контексті ключовими питаннями дослідження є:

1) яка інформація є більш критичною?

2) наскільки ефективно можна отримати таку критичну інформацію, зменшуючи розмір інформації та кінцеве споживання пропускної здатності?

Щоб відповісти на ці запитання, у цій роботі ми розробляємо новий метод глибокого навчання (DL) для вилучення важливих функцій із набору багатовимірних, багатомодальних і корельованих спостережень мереж IoBT.

Витягнуті функції, незважаючи на низькі розміри, містять критичну та статистично значущу інформацію, тому їх можна використовувати для прийняття рішень у командному центрі, одночасно зменшуючи затримку та вимоги до пропускної здатності.

Так само в бездротовому спектрі важливо ідентифікувати зловмисників, щоб захистити спектр обмежених ресурсів. Часто буває так, що шаблон передбачуваного сигналу прихований під шумом. Ми можемо визначити аномалії краще, якщо зможемо якось певною мірою прибрати шум. У цій роботі досліджено систему виявлення бездротових аномалій на основі H-Score для виявлення таких аномалій у РЧ-спектрі за наявності шуму.

В обох сценаріях мета полягала в тому, щоб отримати низьковимірне представлення (важливу інформацію) з безперервного потоку даних, одночасно придушуючи шум, щоб система, що виходить за потоком, могла скористатися вилученою, чистішою версією фактичних даних (сигнал) і виконати задумане завдання.

1.3. Типи та особливості машинного навчання

Термін «машинне навчання» вперше ввів у 1959 році Артур Семюель. Він був лідером у галузі комп'ютерних ігор та штучного інтелекту, працюючи в IBM у той час, він визначив машинне навчання як «галузь дослідження, яка дає комп'ютерам можливість навчатися без явного програмування». Ми можемо загалом визначити машинне навчання як здатність машини імітувати складну людську поведінку. У 1998 році Том Мітчелл, відомий вчений-комп'ютерник, дав більш формальне визначення машинного навчання, він визначив його так: «Кажуть, що комп'ютерна програма навчається на досвіді E щодо деякого класу завдань T і показника продуктивності P, якщо її продуктивність у завданнях у T, як вимірюється P, покращується з досвідом E». Наприклад, якщо ми візьмемо алгоритм, який

грає в шахи з людиною, ми можемо визначити E як самі дані [ходи, які роблять алгоритм і гравець-людина], T як завдання гри в шахи, а P як коефіцієнт виграшу.

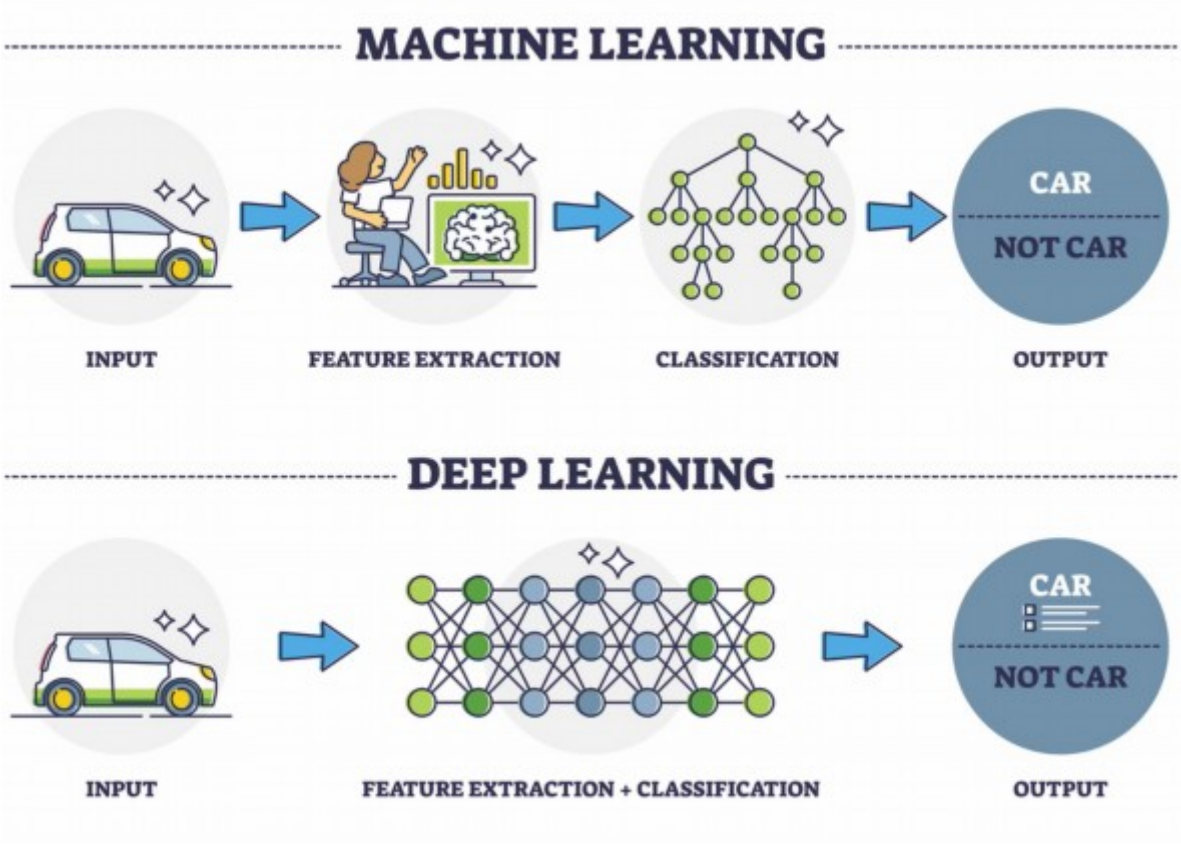

Рис. 1.2. Особливості машинного та глибокого навчання

Алгоритми машинного навчання складаються з побудови моделі з використанням деяких зразків даних, також відомих як навчальні дані, а потім виконання висновку на невидимих даних, зібраних із того самого середовища. Розглянемо приклад алгоритму ML, який може розрізняти зображення кота та собаки. Щоб навчити модель, ми спочатку передаємо алгоритму зображення котів і собак з наших навчальних даних. Коли алгоритм буде достатньо навчено, ми можемо попросити алгоритм (модель) ідентифікувати котів або собак на новому зображенні, якого раніше не бачили алгоритм.

Алгоритми машинного навчання можна класифікувати за чотирма основними категоріями залежно від типу проблеми, яку ми вирішуємо, це

навчання з наглядом, неконтрольоване навчання, навчання з підкріпленням і напівконтрольоване навчання. Що стосується теми нашої дисертації, ми зосередимося лише на алгоритмах навчання під контролем і без контролю.

1.3.1. Контрольоване навчання (з вчителем)

Контрольоване навчання – це тип алгоритму машинного навчання, який навчається на попередньо позначених даних. Давайте розглянемо приклад маленької дитини, як дитина дізнається, що таке яблуко, коли дитина бачить яблуко кілька разів, мозок дитини створює високорівневе розуміння яблука та зберігає його в пам’яті. Дитина може сплутати апельсини та яблука на початку процесу, але згодом дитина ідеально визначить яблуко серед купи інших фруктів. Ось як працює алгоритм навчання під наглядом. Спочатку ми навчаємо нашу модель за допомогою набору даних, що містить позначені дані (правильні та неправильні приклади), а потім використовуємо навчену модель, щоб робити прогнози на основі нових даних. Алгоритм робить це шляхом оптимізації для функції втрат, яка має високе значення у разі неправильного прогнозу та низьке значення для правильного прогнозу. Коли ми наводимо моделі сотні таких прикладів, вона зрештою навчиться передбачати правильне значення.

У навчанні під наглядом існує в основному два типи проблем.

1. Проблема регресії
2. Проблема класифікації

Розберемо приклад, щоб розібратися в них докладніше. Вважайте, що ми маємо такі дані, як показано в таблиці 1.1.

Кожна модель машинного навчання має певний вхід x(i) і вихід y(i) . У нашому випадку входом може бути житлова площа, а виходом — ціна. Пара (x(i), y(i) називається навчальним прикладом, а n таких точок даних разом називається набором даних. Весь вхідний простір можна позначити X , а наш вихідний простір можна представити R. Тепер, ми можемо формально визначити нашу постановку задачі для алгоритму вивчення функції f : X <—

> R так, щоб f (x) був хорошим предиктором у. Це можна візуально показано на рисунку 1.3.

Таблиця 1.1.

Приклад даних для контрольованого навчання

Living Area (feet^2)	Dwelling Type	Price (1000$s)
1400	Apartment	200
2400	House	450
1850	Apartment	275
1200	Apartment	175
2250	House	400
.	.	.
.	.	.

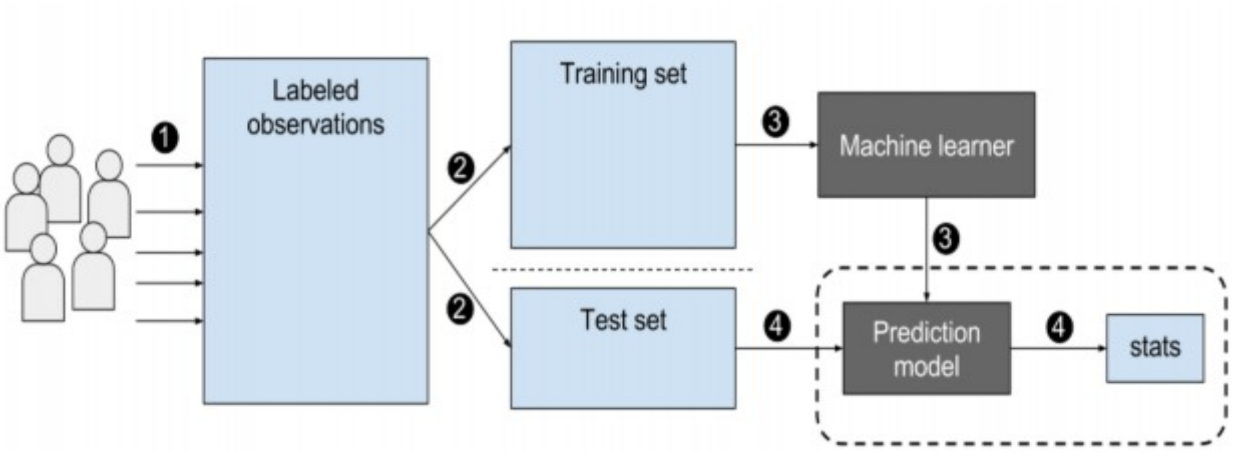

Рис. 1.3. Приклад системи контрольованого навчання

Якщо наша цільова змінна є безперервним значенням, таким як ціна, у нашому випадку це називається проблемою регресії, а коли цільове значення може приймати лише дискретні числові значення, як у категоріях, це називається проблемою класифікації. Наприклад, якщо ми намагаємося передбачити тип житла на основі житлової площі як вхідних даних для моделі, це стає проблемою класифікації.

1.3.2. Неконтрольоване навчання (без вчителя)

У більшості сценаріїв реального світу наявність позначеного набору даних є розкішшю. Часто дослідники вирішують проблеми, які не мають фіксованої відповіді. При неконтрольованому навчанні моделі навчаються без будь-яких конкретних інструкцій. Алгоритми навчаються з використанням немічених даних, а потім алгоритм намагається знайти певну структуру в даних, витягуючи ознаки з даних, як показано на рис. 1.4. Алгоритм намагався знайти приховану структуру в даних, які надаються моделі.

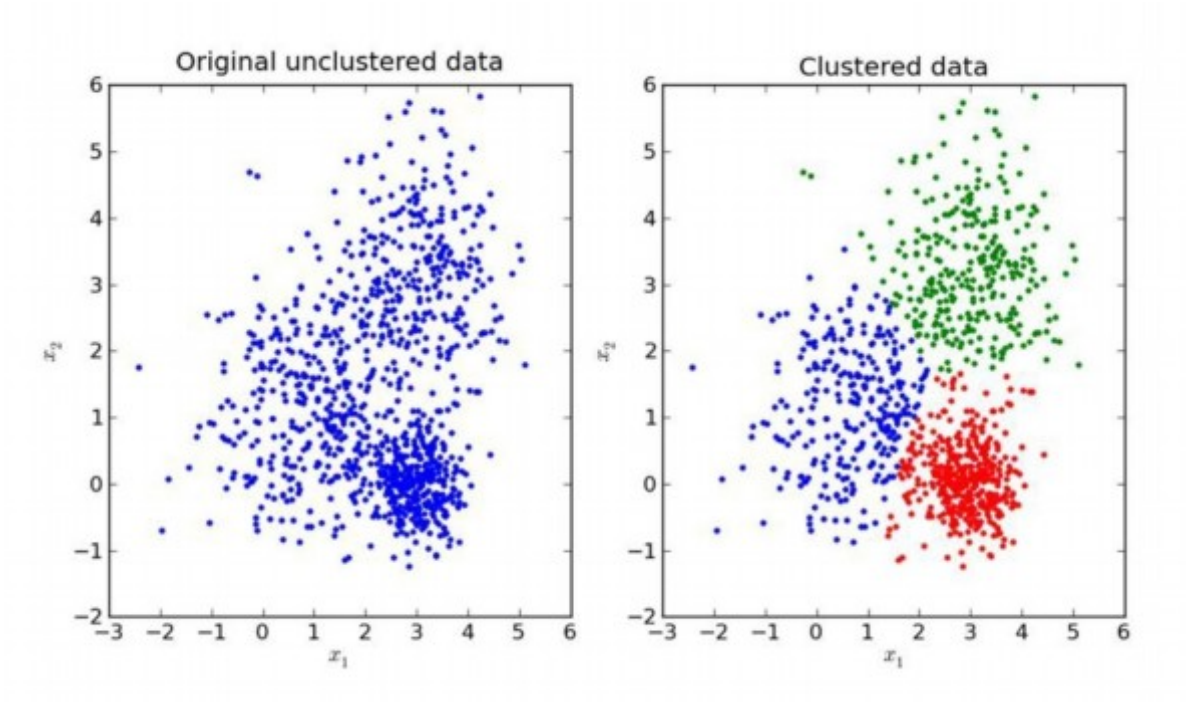

Рис. 1.4. Машинне навчання без вчителя

Його також можна розглядати як інструмент організації даних на дуже високому рівні та залежно від моделі, що організовує ці дані, можуть бути різні види задач:

1. Кластеризація: кластеризація – це техніка, за якої моделі намагаються згрупувати подібні дані в кластер без попередньої інформації про дані. Наприклад, якщо ми хочемо розділити типи автомобілів (седан, хетчбек, позашляховик, вантажівки тощо), ми можемо надати алгоритму

неконтрольованого навчання набір даних, що містить усі ці зображення автомобілів без жодних міток, алгоритм може складатися з кількох кластерів де кожен кластер представляє сегмент автомобілів. Існує багато алгоритмів кластеризації, KMeans і DBSSCAN тощо.

2. Виявлення аномалій: ще одним цікавим випадком використання алгоритмів неконтрольованого навчання є виявлення аномалій. Уявіть, що у вас є тисячі зразків даних транзакцій кредитної картки без міток, тепер ми хочемо з'ясувати, чи є якась транзакція шахрайською. Ми можемо використовувати алгоритми виявлення аномалій, як-от One Class SVM (OC-SVM) або Isolation Forest, щоб виявити ці шахрайські транзакції. На дуже високому рівні алгоритм виявлення аномалій намагається дізнатися межу прийняття рішення навколо правдивих даних, і будь-які точки даних за межами цієї межі називаються викидами або аномаліями.

3. Асоціація: пошук асоціацій у наборі даних у нашому наборі даних є однією з найважливіших проблем для веб-сайтів електронної комерції. Кожного разу, коли ми відвідуємо сторінку продукту електронної комерції, є розділ під назвою «речі, які також купили покупці», який визначається за допомогою аналізу правил асоціації. Ми можемо використовувати алгоритми аналізу правил асоціації, як-от алгоритми Apriori та FP-Growth, щоб виявляти асоціації одного продукту з іншим продуктом, навчаючи модель за допомогою набору даних, що містить прості транзакційні дані.

4. Автокодери за останні кілька років автокодери набули величезної популярності. Це архітектура нейронної мережі, яка має симетричну кількість нейронів у шарах, а внутрішній шар цієї архітектури можна розглядати як прихований простір, який використовується як представлення вхідних даних нижчого розміру. Однією з архітектур із повністю підключеними рівнями може бути [128, 64, 32, 16, 32, 64, 128]. Тут 128 є розміром вхідного шару та вихідного шару, а шар із 16 нейронами є внутрішнім шаром, який фіксує представлення нижчих розмірів.

Автокодувальники успішно використовувалися для видалення шумів із зображень і відеоданих для покращення якості зображення.

1.4. Аналіз та опис алгоритмів та методів штучного інтелекту

1.4.1. Згорткова нейронна мережа (CNN)

Згорткова нейронна мережа (CNN) — це нейронна мережа прямого зв'язку, яка аналізує зображення, обробляючи їх у сітчастій архітектурі. CNN вперше була розроблена Янном Лекуном у 1988 році. Перша CNN називалась LeNet і використовувався для розпізнавання символів, таких як поштові індекси та цифри.

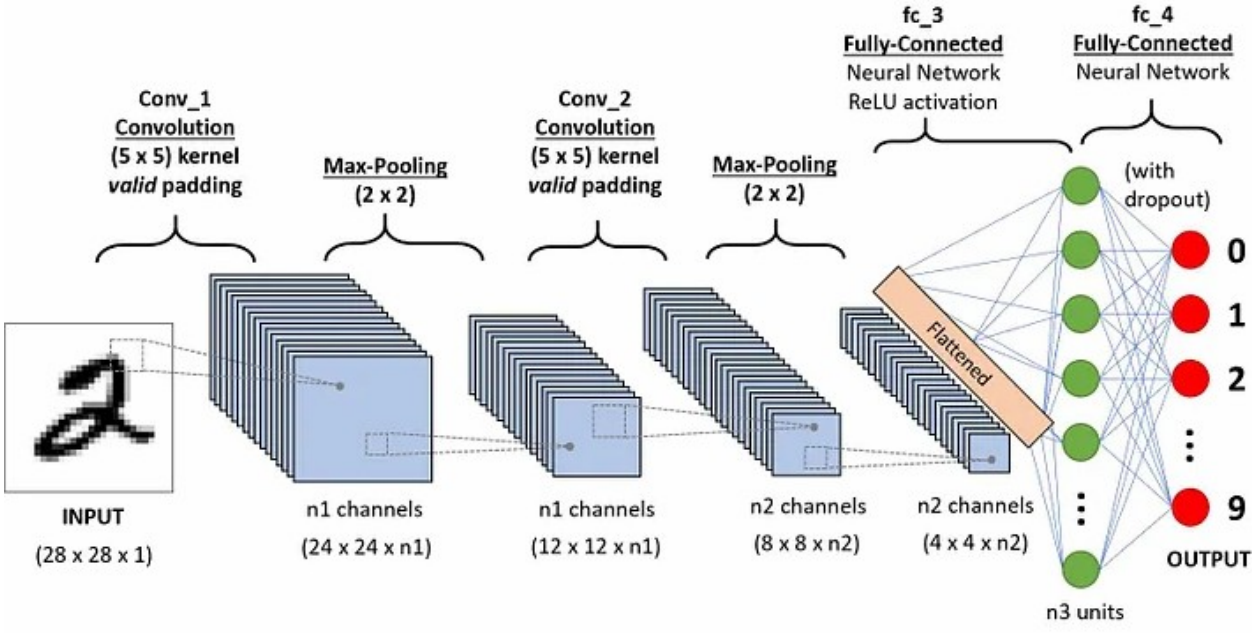

Рис. 1.5. Використання CNN для класифікації рукописних цифр

Основна відмінність між повністю зв'язаною нейронною мережею та CNN полягає в тому, що в CNN кілька нейронів можуть розділяти ваги. Ця архітектура спільної ваги змушує CNN змінювати варіанти. Інваріант зсуву можна краще зрозуміти на прикладі, припустімо, що ми навчаємо модель

CNN ідентифікувати кота на зображенні, оскільки цей кіт може з’явитися будь-де на зображенні.

1.4.2. Алгоритм One Class SVM

Алгоритм One Class SVM (OC-SVM) був запропонований для виявлення новизни. Виявлення новизни також можна визначити як виявлення рідкісних подій у наборі даних. Це тип алгоритму виявлення аномалій, коли звичайні алгоритми класифікації не вдаються через відсутність позначених даних. Більшість алгоритмів виявлення аномалій або новизни засновані на оцінці щільності ймовірності даних. Аномалією в даних є ті точки даних, які існують у регіоні, де щільність ймовірності дуже низька. OC-SVM відрізняється від інших алгоритмів у цьому відношенні, він працює за принципом максимального запасу, він не моделює розподіл ймовірностей, а знаходить функцію, яка дає позитивний результат для точок високої щільності та негативний для точок низької щільності регіони, як показано на рис. 1.6.

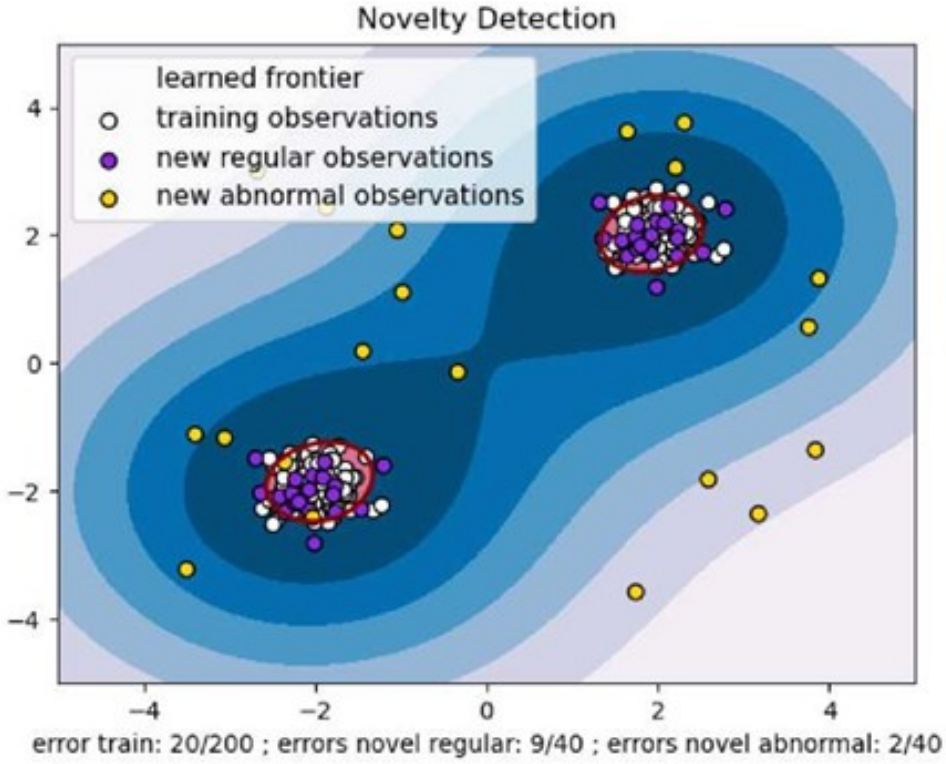

Рис. 1.6. Межі прийняття рішень OC-SVM

Алгоритм One-Class SVM (One-Class Support Vector Machine) — це варіант методу опорних векторів (SVM), який використовується для задач одно класової класифікації та виявлення аномалій. Його мета полягає в тому, щоб відокремити дані одного класу від інших (потенційних аномалій або нових зразків), створюючи межу, яка оточує основну масу даних.

Основні характеристики One-Class SVM:

- Задача: One-Class SVM використовується, коли всі наявні дані належать до одного класу, і мета полягає в тому, щоб виявити відхилення або аномалії, які не відповідають "нормальним" зразкам. Це корисно у випадках, коли ми маємо лише "нормальні" дані і хочемо знайти невідомі або небажані відхилення.

- Гіперплощина: Алгоритм будує гіперплощину в багатовимірному просторі ознак так, щоб максимізувати відстань між гіперплощиною і початком координат. Таким чином, більшість нормальних даних розташовується на одній стороні цієї гіперплощини, а потенційні аномалії — на іншій.

- Ядра (kernel functions): Як і звичайний SVM, One-Class SVM може використовувати різні ядра для роботи з нелінійними даними. Найпоширенішими є радіальна базисна функція (RBF), поліноміальне ядро і лінійне ядро. Використання ядер дозволяє One-Class SVM працювати з даними, які нелінійно розділені у вихідному просторі ознак.

- Гіперпараметри:

  - ν (nu): Гіперпараметр ν контролює частку аномальних точок, яку алгоритм допускає в наборі даних, та частку опорних векторів, що використовується. Він визначає баланс між кількістю аномалій і коректною класифікацією нормальних даних.

  - γ (gamma): Гіперпараметр γ контролює вплив окремих точок у виборці на побудову межі (залежить від типу ядра). Для RBF ядра γ визначає, наскільки близько одна точка даних впливає на інші точки.

Основні етапи роботи:

- Навчання. Модель One-Class SVM навчається на даних одного класу, тобто на нормальних зразках. Під час навчання алгоритм будує гіперплощину, яка відокремлює ці зразки від аномалій.

- Класифікація. Після навчання кожен новий зразок класифікується як "нормальний" (якщо він знаходиться в тому ж просторі, що й тренувальні дані) або як "аномалія" (якщо він значно відхиляється від тренувальних даних і потрапляє за межі гіперплощини).

Перевагою даного методу є те, що він може бути ефективно використаний у випадках, коли доступні лише нормальні дані, а аномалії не відомі або дуже рідкісні. Також можна використовувати різні ядра для роботи з лінійно і нелінійно розподіленими даними.

1.4.3. Алгоритм Isolation Forest

Ізоляційний ліс — це інший тип алгоритму виявлення аномалій, який належить до сімейства методів Ensemble. Ізоляційний ліс подібний до алгоритму випадкового лісу тим, що ми створюємо багато дерев рішень на основі підвибірки даних. Основна ідея використання ізольованого лісу для пошуку аномалій полягає в тому, що аномальні точки або викиди часто легше відокремити від звичайних точок даних, тобто вони вимагають менше розділень у дереві рішень.

Ізоляційний ліс також відрізняється від більшості традиційних алгоритмів виявлення аномалій, оскільки нам не потрібно профілювати набір даних, щоб з’ясувати, яким є нормальний розподіл даних, а потім приймати рішення щодо точки вибірки, якщо воно підтверджує існуючий розподіл. Ізоляційний ліс працює шляхом явної ізоляції викидних точок даних замість побудови моделі розподілу щільності. Часова складність алгоритму є лінійною та має дуже низький відбиток пам’яті, тому це робить його ідеальним кандидатом для виявлення аномалій у великих обсягах даних.

У ізольованому лісі ми випадково вибираємо елементи та точки даних із набору даних, щоб створити кілька дерев. Точки даних, які потребують

більшого розбиття або знаходяться глибше у прийнятті рішення дерева менш імовірно будуть викидами або аномаліями, тоді як точки даних, які потребують менше розбиття або знаходяться на вищих рівнях, швидше за все, будуть викидами або аномаліями, оскільки деревам легше відокремити їх від інших точок даних. Ми можемо візуалізувати це на рис. 1.7.

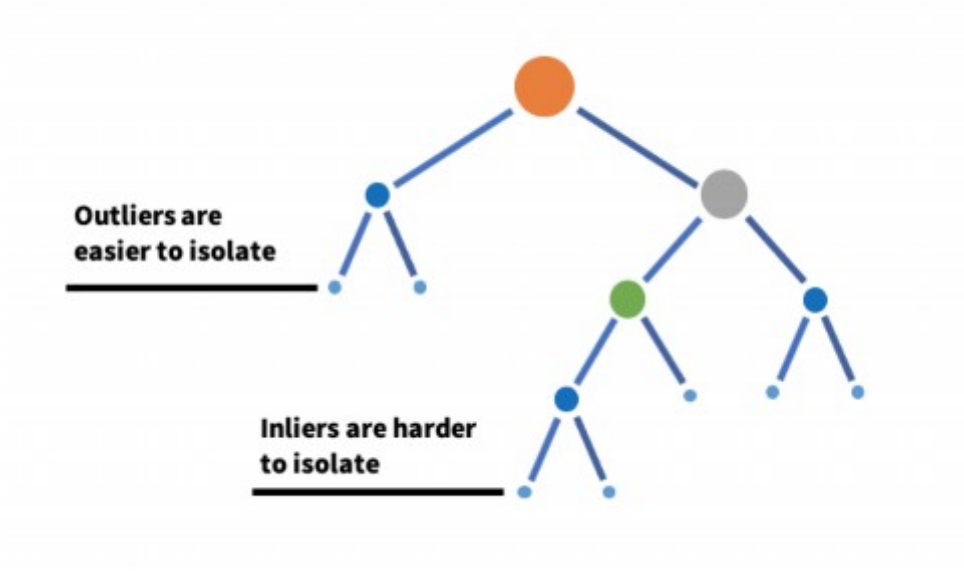

Рис. 1.7. Діаграма ізольованого лісу

Алгоритм можна пояснити більш детально в наступних кроках:

1. Створення множини дерев рішень:

Генерується декілька дерев рішень на основі випадкових підвибірок вихідного набору даних.

2. Вибір ознак та розбиття вузлів:

Для кожного дерева випадковим чином обирається підмножина ознак, які будуть використані для розбиття вузлів.

Для кожного вузла вибирається випадкова ознака та випадкове порогове значення для розбиття даних на дві гілки.

3. Розподіл даних по гілках:

Дані, що потрапляють у вузол, розподіляються по двох гілках залежно від того, чи значення обраної ознаки для даного зразка менше або більше за порогове значення.

4. Рекурсивне побудування дерева:

Кроки 2 та 3 рекурсивно застосовуються до кожної з отриманих гілок до тих пір, поки не буде досягнуто одного з умов зупинки:

Всі зразки у вузлі належать до одного класу.

Досягнуто максимальної глибини дерева, заданої користувачем.

Вищезазначені кроки створюють повністю навчену модель ізольованого лісу, яка має кілька дерев рішень. Щоб зробити висновки щодо нової точки вибірки, ми передаємо цю точку даних усім деревам рішень у навченій моделі. Оцінка аномалії призначається точці даних кожним деревом рішень на основі глибини дерева, до якого досягає наша точка вибірки. Нарешті, ми об’єднуємо всі бали, надані кожним окремим деревом, і отримуємо оцінку аномалії на основі середньої глибини всіх дерев рішень і глибини поточної точки даних. Якщо оцінка аномалії < 0, це можна вважати аномалією або викидом, інакше це є нерівністю.

Висновки до розділу

У першому розділі проведено аналіз предметної області застосування штучного інтелекту в комунікаційних системах, зокрема, досліджено особливості використання методів машинного навчання у бездротових комунікаційних системах. Зазначено, що технології штучного інтелекту мають великий потенціал для вирішення актуальних задач у таких системах, зокрема покращення якості передачі даних, зменшення затримок та підвищення ефективності використання частотного спектра.

У розділі детально розглянуто основні типи машинного навчання, зокрема контрольоване (з вчителем) та неконтрольоване (без вчителя), їхні особливості та застосування в комунікаційних системах. Контрольоване навчання дозволяє використовувати існуючі дані для побудови моделей, що здатні прогнозувати майбутню поведінку систем, тоді як неконтрольоване

навчання є ефективним для виявлення прихованих закономірностей у даних, що використовуються в задачах кластеризації та виявлення аномалій.

Окремо було проаналізовано такі популярні алгоритми штучного інтелекту, як згорткові нейронні мережі (CNN), алгоритм One-Class SVM та Isolation Forest. Згорткові нейронні мережі продемонстрували свою ефективність у задачах розпізнавання та класифікації сигналів, а також в обробці зображень. One-Class SVM та Isolation Forest використовуються для виявлення аномалій та можуть бути корисними для підвищення безпеки в комунікаційних системах.

Таким чином, проведений аналіз підкреслює важливість використання методів машинного навчання у вирішенні різних задач, пов'язаних із оптимізацією та покращенням функціонування комунікаційних систем, що підтверджує актуальність магістерського дослідження в даній галузі.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ АЛГОРИТМІВ ТА МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ОБРОБКИ ІНФОРМАЦІЇ

2.1. Огляд літератури в області дослідження методів семантичної комунікації

У цьому розділі ми розглянемо деякі роботи, пов’язані із застосуванням алгоритмів машинного та глибокого навчання для отримання найбільш корисної інформації в середовищі, що складається з мультимодальної інформації.

Існуюча література досліджує кілька стратегій зменшення затримки в бездротових мережах. Наприклад, кодований фреймворк кінцевої довжини блоку (FBL) був використаний для підтримки наднадійного зв’язку з низькою затримкою в мережах 5G [13, 18,]. У [3] були запропоновані структури множинного доступу без дозволу для подальшого зменшення затримки планування та накладних витрат у системах зв’язку з короткими пакетами. Крім зменшення наскрізної затримки, в нещодавній літературі також досліджувалися схеми планування ресурсів для підвищення свіжості отриманих пакетів шляхом мінімізації терміну зберігання інформації в бездротових мережах [8, 9]. Однак вищезазначені структури в основному зосереджувалися на оптимізації каналів зв’язку для зменшення затримки, повністю ігноруючи контексти інформації. Такі структури не відрізняють критичну та релевантну інформацію від некритичної та нерелевантної інформації, і тому вони неефективні для мереж, що мають багатовимірні мультимодальні спостереження.

Виділення семантичних ознак у передавача виконується за допомогою спільного кодера семантичного каналу, а значення отриманих семантичних ознак відновлюється за допомогою спільного декодера семантичного каналу. Отже, ефективна конструкція кодера та декодера є надзвичайно важливою для семантичного зв’язку. У [14] розроблено спільний семантичний і

канальний кодер і декодер на основі DL для семантичної текстової комунікації шляхом спільного збільшення семантичної подібності та взаємної інформації між вихідним і відновленим текстами. Така структура була розширена для передачі мовних сигналів, зображень [6] і відео [23]. Вищезазначені роботи широко використовують автокодер (AE) для вилучення та використання функцій. Ключовою проблемою AE є те, що він вимірює лише якість вилучених функцій з точки зору можливості реконструкції [22]. Для мультимодальних даних реконструкція вимагає великого набору функцій. Однак у багатьох застосуваннях реконструкція всього мультимодального спостереження не є необхідною. Наприклад, у мережах IoBT важливіше точно відновити позицію/стани ворога, а не повну реконструкцію всіх зображень/відео, зібраних датчиками. Отже, коли критична інформація має значно менший розмір, ніж спостережувані дані, семантичне кодування та декодування на основі AE є неефективними, оскільки вони потребують високої затримки як для передачі, так і для обробки інформації.

Крім AE, в існуючій літературі також досліджувалися інші методи DL для обробки семантичної інформації. У [21] автори застосували федеративне навчання для розробки моделей виділення семантичних ознак на розподілених вузлах, зберігаючи при цьому конфіденційність локальних даних і зменшуючи накладні витрати на зв’язок.

У [28] автори запропонували структуру з підкріпленням навчання, уповноважену для захоплення значення переданої інформації в невідомому шумному середовищі. У [11] автори запропонували цілеспрямовану семантичну комунікаційну структуру для виконання набору послідовних завдань у динамічному середовищі. Тим не менш, вищезазначені дослідження не використовували статистичну взаємозалежність між послідовними багатовимірними та багатомодельними спостереженнями для вилучення семантичних ознак.

Щоб подолати вищезазначені обмеження існуючих методів виділення семантичних ознак, у цій роботі ми застосовуємо H-показник для вилучення важливої та критичної інформації. Запропонований підхід:

1) має справу з мультимодальними спостереженнями в динамічному середовищі;

2) виділяє семантичні ознаки малої розмірності та високої взаємної інформаційності;

3) враховує статистичну взаємозалежність між спостереженнями.

Дійсно, такі характеристики роблять дану роботу унікальною порівняно з найсучаснішими підходами до вилучення ознак.

2.2. Алгоритми виявлення аномалії

Виявлення аномалій було життєво важливою сферою досліджень спільного використання спектру та моніторингу. Попередні традиційні алгоритми використовували виключно вимірювання потужності спектра [24, 27], останні роботи використовують частотно-часове представлення спектру.

З удосконаленням глибокого навчання алгоритми на основі машинного навчання (ML) замінили традиційні алгоритми для виявлення аномалій у спектрі. Останні алгоритми, які приймають спектрограму спостережуваного спектру як вхідні дані [5, 12], показали кращі результати, ніж традиційні алгоритми, такі як Anomaly Detection Framework for Dynamic Spectrum Access Network (ALDO) [27].

Алгоритм ALDO (Anomaly Detection Framework for Dynamic Spectrum Access Network) призначений для виявлення незвичайних або аномальних подій у мережах з динамічним доступом до спектру. Ці мережі постійно змінюються, що ускладнює визначення того, що є "нормальним" і що є "аномальним". ALDO використовує машинне навчання для виявлення відхилень від нормальної поведінки.

На рисунку 2.1 представлена спрощена блок-схема алгоритму ALDO. Кожен етап алгоритму відображається у вигляді окремого блоку, а стрілки показують напрямок потоку даних.

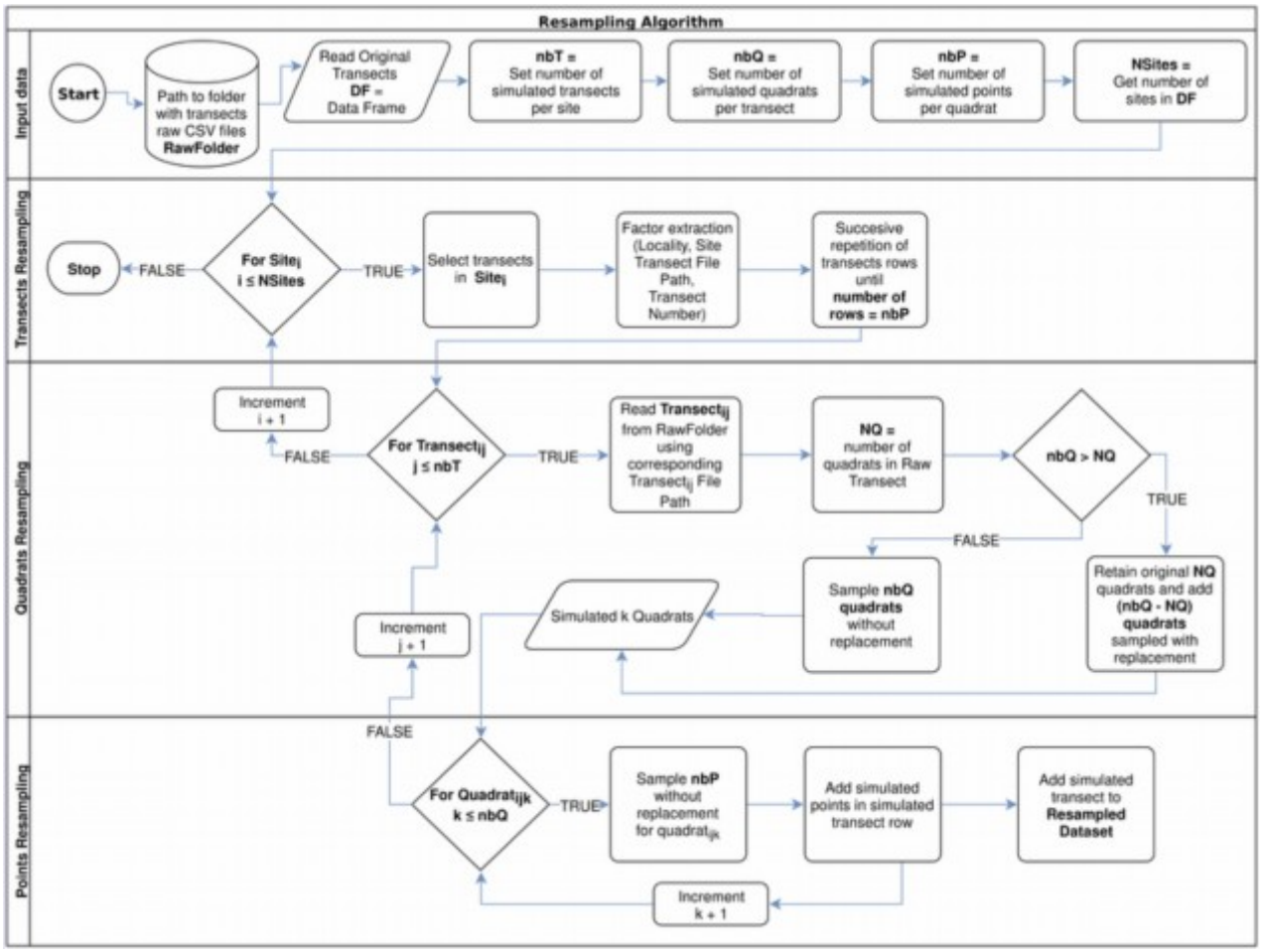

Рис. 2.1. Блок-схема алгоритму ALDO

Ключові елементи рисунка 2.1:

- Блок збору даних: Представлений у вигляді антени, що приймає сигнали з різних джерел.

- Блок перед обробки даних: Зображений як фільтр, який очищає дані від шуму та нормалізує їх.

- Блок навчання моделі: Представлений у вигляді нейронної мережі, яка навчається на історичних даних.

- Блок виявлення аномалій: Зображений як компаратор, який порівнює нові дані з моделлю.

- Блок реагування на аномалії: Представлений у вигляді дзвіночка або іншого сигналу, що вказує на виявлення аномалії.

Алгоритм ALDO є важливим інструментом для забезпечення безпеки та ефективності мереж з динамічним доступом до спектру. Завдяки використанню методів машинного навчання, ALDO дозволяє виявляти аномалії, які важко виявити за допомогою традиційних методів.

Існуючу роботу можна розділити на два класи залежно від того, як вони фіксують візерунок у спектрі. Традиційні алгоритми використовували розроблені вручну методи виділення шаблонів, тоді як сучасні алгоритми використовують методи навчання, керовані даними, для вилучення шаблонів зі спектру. Традиційні алгоритми перетворили проблему виявлення аномалії в задачу перевірки статистичної значущості, коли в [27] помітили, що потужність отриманого сигналу (RSS) майже лінійно зменшується з логарифмічною відстанню від джерела, і використали характеристики розповсюдження для ідентифікації незаконних передавачів. Усереднюючи дані за попередні сім днів, в [16] змогли визначити історичну закономірність. Щоб знайти ймовірні аномалії, вони оцінили відстань Махаланобіса між вимірювальним спектром та історичною тенденцією.

На відміну від звичайних алгоритмів, сучасні алгоритми використовують методи навчання, керовані даними, для виділення шаблонів. Моделі автокодерів успішно використовувалися в минулому для виявлення аномалій у спектрі. Для досягнення нормального виділення шаблону в [34] і [12] обидва використовували глибокі моделі автокодерів. Вхідними даними для обох цих підходів була спектрограма. Амплітуду на підчастотах справжньої спектрограми та відповідної реконструйованої спектрограми порівнювали, а середню квадратичну помилку (MSE), отриману в результаті, використовували як оцінку аномалії. З метою виявлення аномалій спектру в [16] прийнято концепцію класифікації. Як вхідні дані вони використали послідовність зайнятості спектру. Приховані моделі Маркова (HMM) використовувалися для моделювання як типових, так і аномальних моделей

спектру. Таким чином, для ідентифікації аномалій можна використовувати найвищу логарифм правдоподібності даних щодо кожного спектрального шаблону.

В дослідженні [30] використовували рекурентну мережу на основі довготривалої короткочасної пам'яті (LSTM) для навчання моделі часових рядів і отримання ознак. По-перше, він обчислив різницю між прогнозованим значенням і справжнім значенням на навчальному наборі. Потім він моделював вектор помилки за допомогою параметричного багатовимірного розподілу Гауса. Нарешті, він обчислив ймовірність імовірності в очікуваному розподілі помилок на тестовому наборі, щоб розрізнити аномалію. В [26] вивчали виявлення аномалії спектру в діапазоні LTE. Вони створили моделі глибокої нейронної мережі (DNN) для фіксації моделей використання спектру та обчисленої середньоквадратичної помилки (RMSE) між справжньою амплітудою на підчастотах і значеннями прогнозу моделі.

2.3. Аналіз метрики H-Score для отримання даних

У цьому розділі ми проведемо аналіз метрики під назвою H-Score. Він є основою цієї роботи, оскільки наступні розділи залежать від нього. H-Score — це основний алгоритм, який ми використовуємо для отримання важливої інформації з даних.

Здатність людського сприйняття отримувати інформацію за допомогою кількох органів чуття часто є більш точною, ніж використання лише одного органу чуття. Ця ідея викликала великий інтерес у сфері машинного навчання, де дослідники шукали способи отримання інформації за допомогою кількох модальностей. Одним із методів є використання вилучення ознак на основі кореляції, що передбачає пошук зв’язків між різними фрагментами даних.

Однак машинам набагато важче вивчити зв’язки між різними об’єктами, ніж людям. Це пояснюється тим, що статистичні властивості

даних із вхідних джерел, що постійно змінюються, можуть приховати кореляції між різними модальностями. Це може ускладнити вивчення ефективного представлення функцій. Існуючі методи вирішення цієї проблеми включають канонічний кореляційний аналіз, мінімізацію евклідової відстані та забезпечення часткового порядку.

Максимальна кореляція Гіршфельда-Гебелейна-Реньї (HGR) є спрощенням кореляції Пірсона, і було доведено, що вона є хорошим показником для вимірювання залежності між статистичними даними. Це робить його привабливою ідеєю для вилучення мультимодальних функцій з багатьох причин. Наприклад, максимізація максимальної кореляції HGR дозволяє виявити нелінійні зміни між двома факторами, які максимально корельовані. З точки зору теорії інформації, кореляція HGR містить інформацію про одну змінну та іншу, і навпаки.

Однак у максимальної кореляції HGR є два недоліки. По-перше, це вимагає, щоб кожна функція була некорельованою, що відомо як обмеження відбілювання. Зазвичай це досягається за допомогою методу відбілювання, який передбачає інверсію матриці або обчислення декомпозиції ¬. Ці операції є обчислювально складними та можуть спричинити проблеми чисельної стабільності під час роботи з великими розмірами об’єктів. По-друге, максимальна кореляція HGR явно не враховує дискримінаційну інформацію. Якщо вся дискримінаційна інформація знаходиться в одному підпросторі різних модальностей, це може призвести до кращої продуктивності в наступних контрольованих завданнях. Однак, якщо вхідні модальності слабо корельовані та є всі спільні знання, це може бути не так. Після відображення функції основна дискримінаційна інформація, ймовірно, буде втрачена, що призведе до втрати виходу.

Щоб вирішити ці проблеми, автори [48] пропонують новий метод під назвою Soft-HGR. Цей метод дозволяє вивчати асоційовані представлення через модальності без жорстких обмежень. Він використовує два внутрішні

продукти, один із відображеннями ознак, а інший із коваріаціями ознак, як ціль.

Останнім часом автокодери успішно використовувалися для вилучення представлення даних нижчого розміру, однак автокодерам не вдається витягти контекстну інформацію. Vision Transformers [10, 14] також використовувався для вилучення критичних характеристик із даних зображення, але основною проблемою з використанням алгоритмів вилучення на основі трансформаторів є те, що вони є контрольованими за своєю природою, тобто вони вимагають анотованих позначених зображень у процесі навчання, і алгоритму H-Score не потрібні зображення з мітками для навчання моделі, він знаходить критичні особливості в зображеннях, максимізуючи взаємну інформацію між двома наборами вхідних даних.

Оптимальне рішення проблеми максимальної кореляції HGR може бути безпосередньо отримано з розкладу сингулярного значення (SVD) канонічної матриці залежності (CDM) [21]. CDM для спільно розподілених випадкових величин X і Y є |Y| x |X| розмірна матриця B (y, x) запис CDM визначається як

$$\tilde{B}(y,x) = \frac{P_{X,Y}(x,y) - P_X(x)P_Y(y)}{\sqrt{P_X(x)}\sqrt{P_Y(y)}}$$

Оптимальні вектори ознак отримують як

$$f_i^*(x) = \frac{\Psi_i^X(x)}{\sqrt{P_X(x)}}, i = 1, 2, \cdots, K-1$$
$$g_i^*(y) = \frac{\Psi_i^Y(y)}{\sqrt{P_Y(y)}}, i = 1, 2, \cdots, K-1$$

Де $\Psi^X_i(x)$ і $\Psi^X_i(y)$ – і-та компонента векторів x та y відповідно. Позначимо останній вираз як прямий метод обчислення. Через наступні дві причини обчислити оптимальні характеристики за допомогою даного виразу досить

складно. По-перше, для надійного обчислення CDM необхідно зібрати велику кількість вибірок випадкових величин X і Y. Однак збір великої кількості зразків є дорогим і трудомістким, особливо коли і X, і Y представляють багатовимірні вектори. По-друге, велика обчислювальна складність $O(2mK^2 + K^3)$ потрібна для обчислення SVD CDM, де m є загальною кількістю зібраних зразків. В якості альтернативи методу прямого обчислення в [19] запропоновано багатоваріантний алгоритм умовного очікування (MACE). Порівняно з методом прямого обчислення, обчислювальна складність алгоритму MACE лінійно збільшується з кількістю функцій. Однак алгоритм MACE все ще вимагає великої кількості вибірок для обчислення умовного сподівання. Щоб подолати таку перешкоду, використовується метод DL для вивчення інформативних ознак із наведених зразків X і Y .

Далі ми формулюємо проблему максимальної кореляції Soft-HGR для створення інформативних ознак. Як видно з останнього виразу, сингулярні вектори матриці CDM лінійно залежать від оптимальних функцій ознак. Таким чином, замість обчислення SVD CDM, проблему вивчення ознак можна альтернативно сформулювати як задачу оптимізації виявлення низькорангової апроксимації CDM так, щоб було отримано найбільше K - 1 власних векторів. Для цього спочатку визначимо змінні

$$\mathbf{\Phi}_1 = \left[\sqrt{P_X(\mathcal{X}(1))}\boldsymbol{f}(\mathcal{X}(1)), \cdots, \sqrt{P_X(\mathcal{X}(|\mathcal{X}|))}\boldsymbol{f}(\mathcal{X}(|\mathcal{X}|))\right],$$

$$\mathbf{\Phi}_2 = \left[\sqrt{P_Y(\mathcal{Y}(1))}\boldsymbol{g}(\mathcal{Y}(1)), \cdots, \sqrt{P_Y(\mathcal{Y}(|\mathcal{Y}|))}\boldsymbol{g}(\mathcal{Y}(|\mathcal{Y}|))\right]$$

Тут X(n) і Y(n) відносяться до n-го елемента X і Y відповідно. Використовуючи оптимізовані функції функцій, Φ_1 і Φ_2 вирівнюємо

відповідно до лівого та правого сингулярних векторів CDM матриці B. На основі перетворень отримаємо наступне:

$$\max_{f,g} \mathbb{E}\left[f^T(X)g(X)\right] - \frac{1}{2}\mathrm{tr}\left(\mathrm{cov}\left(f(X)\right)\mathrm{cov}\left(g(X)\right)\right)$$
$$\text{s.t.} \quad \mathbb{E}[f(X)] = \mathbb{E}[g(Y)] = 0$$

Останнє рівняння є проблемою максимальної кореляції Soft-HGR, і її цільова функція позначається як H-показник. H-показник містить два внутрішніх добутку, а саме, внутрішній добуток між ознаками та внутрішній добуток між коваріацією ознак. Рис. 2.2 надає візуальне представлення алгоритму H-Score.

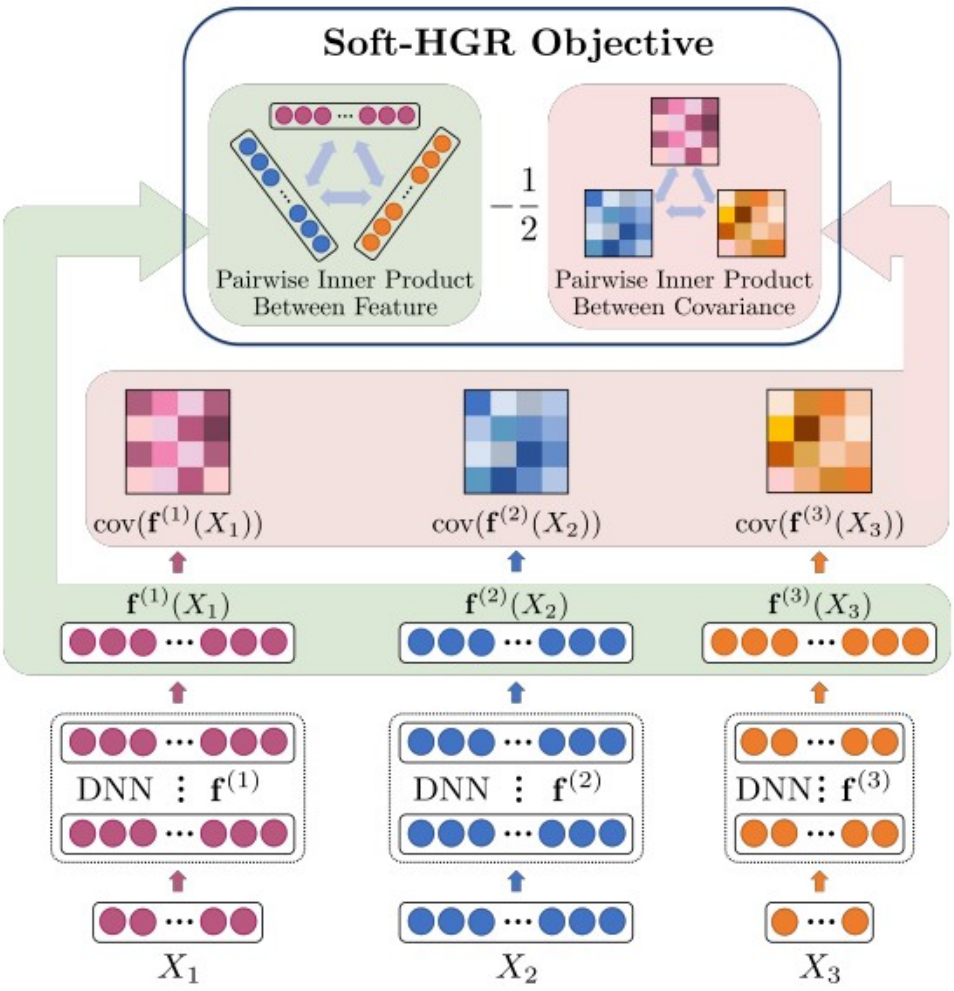

Рис. 2.2. Алгоритм H-Score

Зокрема, H-score зменшує обчислювальну складність проблеми максимальної кореляції HGR шляхом заміни обмеження відбілювання як м'якого регуляризатора. Ознаки, що містять статистично значущу інформацію про X та Y, отримують з оптимального розв'язку останнього виразу.

Даний вираз є нескінченномірною оптимізаційною задачею над функціональним простором, і, як наслідок, розв'язати цю задачу нетривіально. З цією метою ми застосовуємо глибоке неконтрольоване навчання розв'язування. Більш конкретно, ми представляємо глибоку нейронну мережу, параметризовану в θ, для обчислення функцій ознак f(•) і g(•). В результаті еквівалентно останньому виразу запишемо наступне:

$$\begin{aligned}\theta^* = \arg\max_{\boldsymbol{\theta}} & \mathbb{E}\left[\boldsymbol{f}_{\boldsymbol{\theta}}^T(X)\boldsymbol{g}_{\boldsymbol{\theta}}(X)\right] \\ & -\frac{1}{2}\mathrm{tr}\left(\mathrm{cov}\left(\boldsymbol{f}_{\boldsymbol{\theta}}(X)\right)\mathrm{cov}\left(\boldsymbol{g}_{\boldsymbol{\theta}}(X)\right)\right) \\ \text{s.t.} \quad & \mathbb{E}[\boldsymbol{f}_{\boldsymbol{\theta}}(X)] = \mathbb{E}[\boldsymbol{g}_{\boldsymbol{\theta}}(Y)] = 0\end{aligned}$$

де $f_\theta(\bullet)$ і $g_\theta(\bullet)$ функції ознак, отримані з параметризованої нейронної мережі. Отримане рівняння розв'язується шляхом розгляду H-показника як функції втрат нейронної мережі та застосування методів стохастичного градієнта (SGD) і зворотного поширення. Загальний алгоритм для виділення ознак за допомогою H-показника підсумовано як Алгоритм 1 (Algorithm 1).

Обчислювальна складність Алгоритму 1 домінує крок 7, тобто складність обчислення мети H-показника. Загальна обчислювальна складність Алгоритму 1 отримуємо як $O(mK^2)$. Отже, Алгоритм 1 вимагає набагато меншої обчислювальної складності для виділення важливих ознак порівняно з методом прямого обчислення.

Мотивація застосування підходу максимізації H-оцінки для виділення семантичних ознак пояснюється наступним чином. Звернемо увагу, що

семантичні ознаки є низьковимірним представленням високовимірних і багатомодальних спостережень зі значним взаємним нформаційним змістом.

Algorithm 1 Proposed Feature Extraction Algorithm

Input: Paired video frames in a m mini-batch: $(\boldsymbol{x}^{(1)}, \boldsymbol{y}^{(1)}), (\boldsymbol{x}^{(2)}, \boldsymbol{y}^{(2)}), \cdots, (\boldsymbol{x}^{(m)}, \boldsymbol{y}^{(m)})$.
Initialize: Neural Network Parameters $\boldsymbol{\theta}$.
repeat
Compute feature functions, $\mathrm{f}_{\boldsymbol{\theta}}(\boldsymbol{x}^{(i)})$ and $\mathrm{g}_{\boldsymbol{\theta}}(\boldsymbol{y}^{(i)})$, $\forall i = 1, 2, \cdots, m$.
Compute normalized feature functions:

$$\mathrm{f}_{\boldsymbol{\theta}}(\boldsymbol{x}^{(i)}) \leftarrow \mathrm{f}_{\boldsymbol{\theta}}(\boldsymbol{x}^{(i)}) - \frac{1}{m}\sum_{i=1}^{m} \mathrm{f}_{\boldsymbol{\theta}}(\boldsymbol{x}^{(i)}), \forall i = 1, 2, \cdots, m$$

$$\mathrm{g}_{\boldsymbol{\theta}}(\boldsymbol{y}^{(i)}) \leftarrow \mathrm{g}_{\boldsymbol{\theta}}(\boldsymbol{y}^{(i)}) - \frac{1}{m}\sum_{i=1}^{m} \mathrm{g}_{\boldsymbol{\theta}}(\boldsymbol{y}^{(i)}), \forall i = 1, 2, \cdots, m$$

Compute the sample covariance:

$$\mathrm{cov}(\mathrm{f}) \leftarrow \frac{1}{m}\sum_{i=1}^{m} \mathrm{f}_{\boldsymbol{\theta}}(\boldsymbol{x}^{(i)})\mathrm{f}_{\boldsymbol{\theta}}(\boldsymbol{x}^{(i)})^T$$

$$\mathrm{cov}(\mathrm{g}) \leftarrow \frac{1}{m}\sum_{i=1}^{m} \mathrm{g}_{\boldsymbol{\theta}}(\boldsymbol{y}^{(i)})\mathrm{g}_{\boldsymbol{\theta}}(\boldsymbol{y}^{(i)})^T$$

Compute the H-score:

$$\frac{1}{m}\sum_{i=1}^{m} \mathrm{f}_{\boldsymbol{\theta}}(\boldsymbol{x}^{(i)})\mathrm{g}_{\boldsymbol{\theta}}(\boldsymbol{y}^{(i)}) - \frac{1}{2}\mathrm{tr}\left(\mathrm{cov}(\mathrm{f})\mathrm{cov}(\mathrm{g})\right)$$

Update the neural network parameters, θ, by considering H-score as the loss function and applying the SGD and backpropagation techniques.
until Convergence or maximum number of iterations are reached
Output: Feature functions $\mathrm{f}_{\boldsymbol{\theta}^*}(\cdot)$ and $\mathrm{g}_{\boldsymbol{\theta}^*}(\cdot)$

Ми підкреслюємо, що підхід максимізації H-показника виділяє ознаки з високим вмістом взаємної інформації, і, таким чином, він вимагає невеликого набору ознак для представлення події. Крім того, максимізація H-показника використовує статистичну взаємозалежність між одночасними спостереженнями (тобто зображеннями, зібраними різними датчиками в мережі IoBT), щоб виділити характеристики. Варто зазначити, що цільова функція H-score у наближає втрату крос-ентропії AE [19]. Незважаючи на це, підхід H-score має певну перевагу перед AE у виділенні семантичних ознак.

Зокрема, AE вимагає великого набору функцій для реконструкції всього спостереження. Через обмеження пропускної здатності та затримки важко передати великий набір функцій від передавача до приймача, що робить AE неефективним для семантичного зв'язку. Однак підхід максимізації H-балу не може перевершити AE з точки зору реконструкції спостережень. Тим не менш, мета семантичних комунікацій є не для точної реконструкції оригінальних зображень/відео, які спостерігаються на кінці передачі. Швидше, суть семантичної комунікації полягає в тому, щоб надати корисні факти про подію, що відстежується/спостерігається на стороні передачі, використовуючи невеликий набір функцій. По суті, знаходячи невеликий набір функцій з важливою інформацією, підхід максимізації H-оцінки забезпечує справжні аспекти семантичних комунікацій у мережах зв'язку з обмеженими ресурсами.

Висновки до розділу

В даному розділі здійснено аналіз існуючих алгоритмів і методів машинного навчання для обробки інформації, що застосовуються в семантичних комунікаційних системах та системах виявлення аномалій. Були розглянуті сучасні підходи та наукові праці, присвячені методам передачі і обробки семантичної інформації. Це дозволило визначити ключові виклики та можливості для впровадження машинного навчання в таких системах, зокрема у контексті підвищення ефективності обміну інформацією. Було проаналізовано різні алгоритми, що використовуються для виявлення аномалій у комунікаційних мережах. Огляд показав, що методи машинного навчання, як-от алгоритми класифікації та кластеризації, значно підвищують точність виявлення аномальних патернів, забезпечуючи надійний контроль за станом мереж.

Проведено дослідження метрики H-Score, яка допомагає у визначенні значущості даних та виділенні важливої інформації. Це стало основою для

подальших етапів розробки, зокрема у вилученні ключових контекстів та маркуванні даних, що є необхідним для точного семантичного аналізу.

Таким чином, проведені дослідження в цьому розділі створили базу для подальшого застосування методів машинного навчання для обробки інформації, забезпечуючи високу продуктивність і точність контролю семантичних та аномальних аспектів у комунікаційних системах.

РОЗДІЛ 3. ІМПЛЕМЕНТАЦІЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ КОНТРОЛЮ КОНТЕКСТІВ В КОМУНІКАЦІЙНИХ СИСТЕМАХ

3.1. Розробка архітектури систему обробки відеоінформації на основі глибокого навчання

Загальна архітектура системи показана на рис. 3.1, яка реалізується за допомогою наступних двох кроків. На першому кроці критична інформація з вхідного відеокадру витягується за допомогою набору малорозмірних та інформативних функцій.

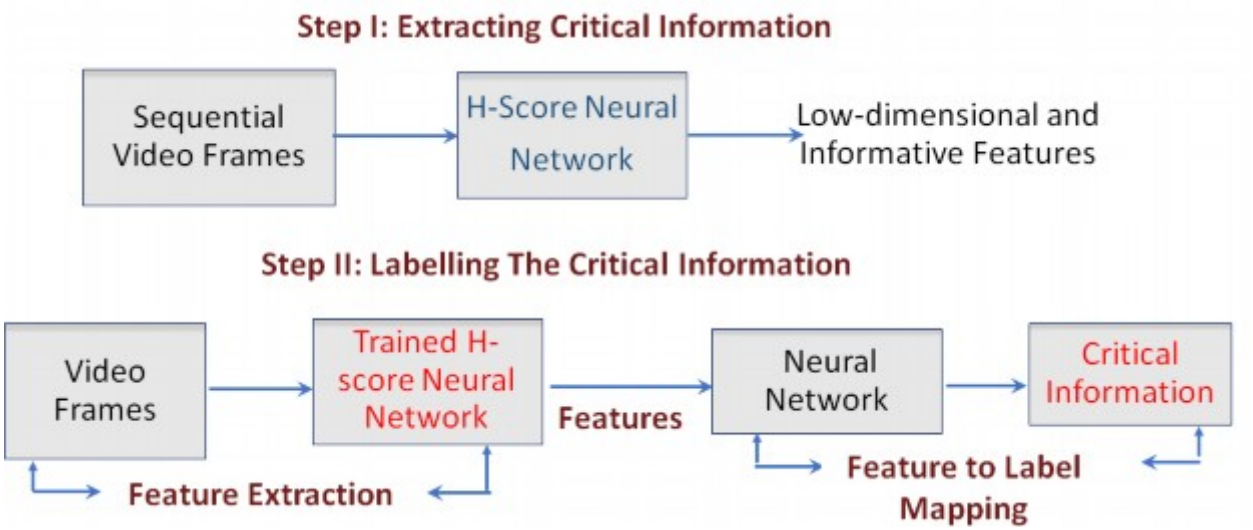

Рис. 3.1. Загальна архітектура системи обробки відеоінформації на основі глибокого навчання

Зауважимо, що перший крок – це неконтрольоване навчання, коли послідовність статистично залежних відеокадрів обробляється новою нейронною мережею H-score. Нейронна мережа H-score, зображена на рис. 3.3, реалізована шляхом використання CNN і унікальної функції втрат. На відміну від звичайного CNN, нейронна мережа H-score визначає залежність двох наступних зображень одне від одного, представлених вибраним

набором ознак. Оскільки нейронна мережа H-score навчається без вчителя, вона не впорядковує функції у спосіб, зрозумілий людині. Точніше, цільова інформація відеокадрів прихована у вигляді певної невідомої лінійної комбінації вилучених особливостей. Щоб вирішити цю проблему, на другому кроці використовується нейронна мережа, щоб дізнатися відповідні мітки функцій або інформації, витягнутої на першому кроці. Зауважимо, що другим кроком є процес навчання з вчителем. Щоб полегшити це, перед навчанням другого кроку створюється набір мічених відеокадрів, а їхні характеристики витягуються з навченої нейронної мережі H-score.

3.1.1. Етап 1. Вилучення важливої інформації за допомогою нейронної мережі H-score

Спочатку ми пояснюємо використання моделі CNN для вилучення критичних характеристик зібраних відеокадрів у мережах IoBT. IoBT (Internet of Battlefield Things) — це концепція, що відноситься до використання Інтернету речей (IoT) у військовій сфері. Вона включає мережу взаємопов'язаних пристроїв, систем і датчиків, які взаємодіють на полі бою для збору, обміну і аналізу даних в реальному часі. Це можуть бути дрони, роботи, військова техніка, сенсори, персональні гаджети військових, що допомагають автоматизувати процеси на полі бою, підвищити ефективність операцій і безпеку військових. Це новітня концепція, яка знаходиться на стадії активної розробки і тестування для використання у військових конфліктах майбутнього.

Варто зазначити, що вороги в практичних сценаріях бою постійно змінюють свої позиції. Багатошарова модель CNN може фіксувати узагальнене представлення, яке може виявляти рухомих ворогів, коли вони знаходяться на нових позиціях. Відповідно, пропонована система використовує модель CNN для отримання важливої інформації з відеокадрів.

Далі ми обговорюємо загальний підхід до отримання важливої інформації з нейронної мережі H-score на основі CNN. Ключова суть

пропонованого підходу полягає в одночасному навчанні двох CNN, знімаючи послідовні зображення відео кадр як вхідні дані та застосовуючи H-показник, як функцію втрат. Для кожного CNN, ми використовуємо два шари згортки з функцією активації ReLu та шар максимального пулу. Ми також використовуйте повністю пов’язаний шар із функцією активації сигмоїда для вибору ознак. Загальна мережа DL, яка використовується для вилучення ознак, показана на рис. 3.2 , де {Y n } представляє індекс послідовних відеокадрів. Мережа DL, зображена на рис. 3.2, приймає два послідовних кадри відео (Yn, Yn+1), Wn як вхідні дані. Вихідні значення з двох моделей використовуються для розрахунку H-показника.

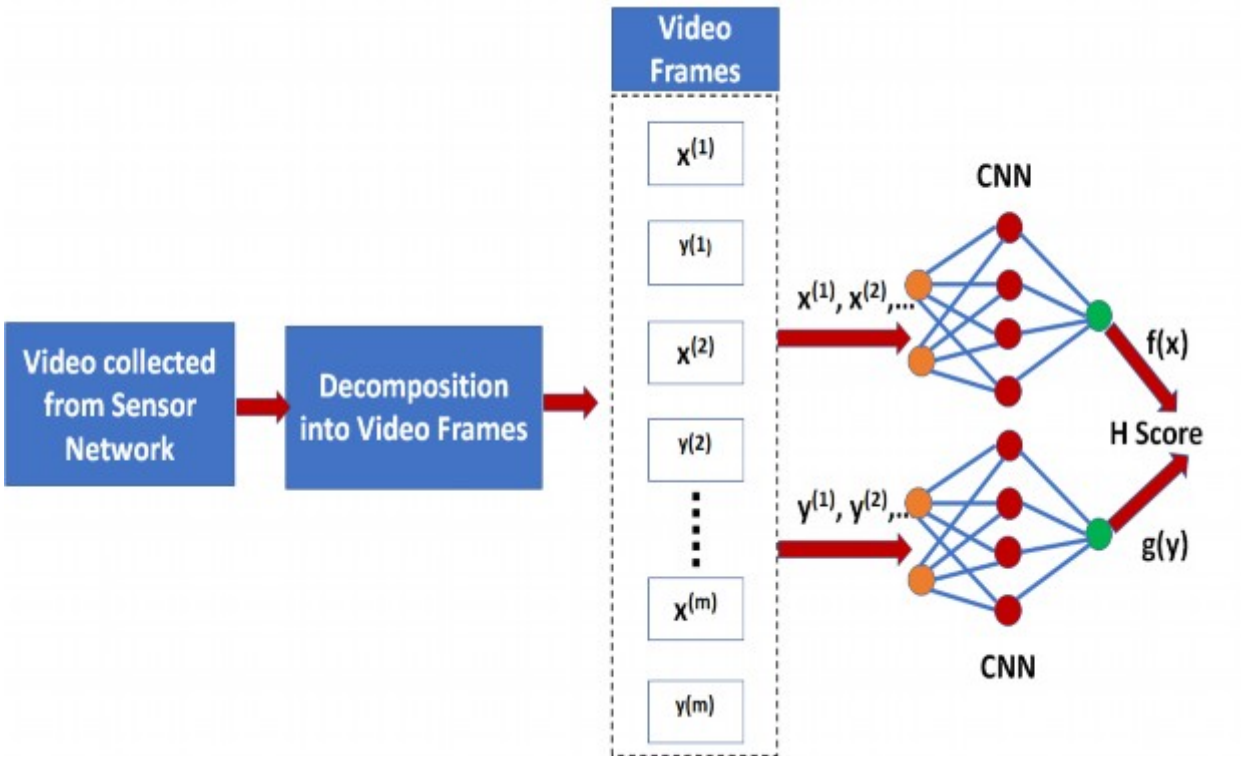

Рис. 3.2. Запропонована мережа для вилучення ознак

Щоб звести до мінімуму функцією втрат (тобто від'ємною від H-показника), використовується оптимізатор SGD. Нарешті, ваги обох мереж CNN оновлюються за допомогою технології зворотного поширення. Загальний алгоритм вилучення ознак за допомогою нейронної мережі H-score узагальнено в Алгоритмі 1 .

Хоча нейронна мережа AE і H-score охоплює маловимірні характеристики, існує суттєва різниця між навчанням цих двох нейронних мереж. На рисунку 3.3 показано, що приймає зображення X як вхідні дані для кодера, витягує маловимірні функції на шар вузького місця та реконструює зображення за допомогою декодера. Хоча функції, виділені за допомогою AE, дозволяють реконструювати все зображення, такі функції не обов'язково зосереджені на критичних факторах, які викликають зміни в наступних зображеннях або відеокадрах.

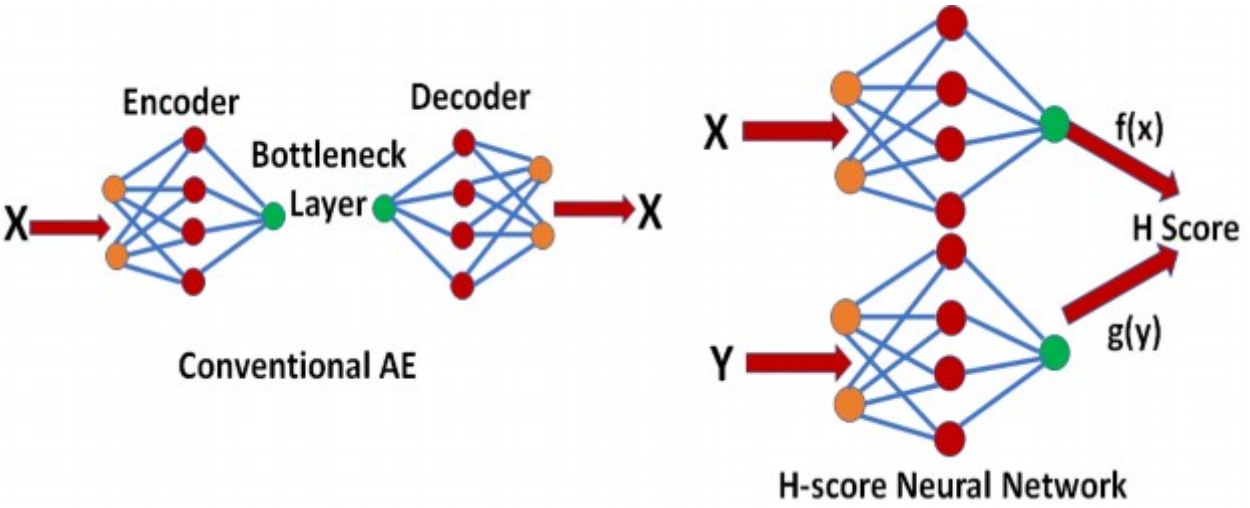

Рис. 3.3. Порівняння між традиційною нейронною мережею AE та мережею H-score

Навпаки, нейронна мережа H-score, показана на рис. 3.3, може одночасно обробляти два зображення X і Y, взяті з одного відеокадру в два послідовні моменти часу. Завдяки новій функції втрат, нейронна мережа H-score зменшує розмірність ознак, витягнутих із зображень, і максимізує взаємну інформацію серед отриманих ознак. Одночасно виконуючи обидві дії, внутрішнє навчання мережі H-score змушене розглядати критичні фактори, які викликають зміни в наступних зображеннях або відеокадрах. Відповідно, на відміну від AE, нейронній мережі H-score не потрібно вивчати цілі зображення для пошуку корисної інформації.

3.1.2 Етап II. Маркування важливої інформації

Спочатку ми опишемо особливості цього етапу. Для певного відеокадру вихід навченої нейронної мережі H-score представлений набором каналів CNN, як показано на рис. 3.4.

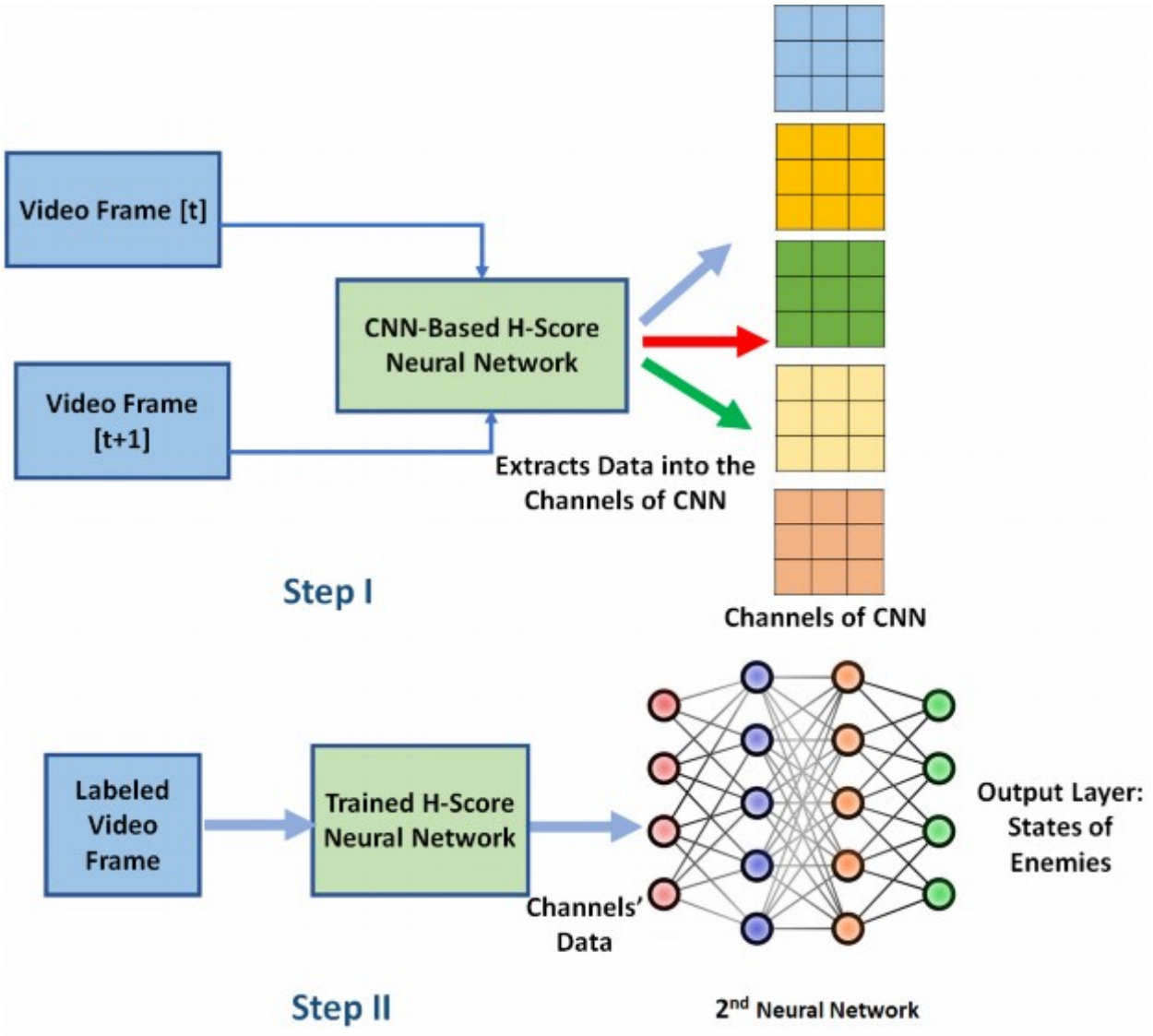

Рис. 3.4. Візуалізація етапів реалізації системи

Ці канали відповідають кількості фільтрів, які використовуються в CNN, і вони фіксують важливу інформацію вхідних зображень. На жаль, інформація зображень, яка нас цікавить, часто прихована у вигляді невідомої лінійної комбінації цих каналів. Таким чином, нетривіально відновити

призначену інформацію з вихідних даних каналів CNN навченої нейронної мережі H-score. Щоб вирішити вищезазначену проблему, ми навчаємо іншу нейронну мережу з невеликою кількістю міток, щоб навчена нейронна мережа могла вибирати важливу інформацію з виділених низьковимірних ознак. Як показано на рис. 3.4, така нейронна мережа навчається, враховуючи вихідні дані каналів CNN навченої нейронної мережі H-score та стани ворога як вхідні та вихідні дані відповідно. Зауважте, що другий крок виконується у просторі ознак, який має значно зменшену розмірність порівняно з оригінальними вхідними зображеннями. Як результат, для навчання відображення ознак на критичну інформацію потрібно лише кілька позначених зразків, і тому другий крок можна коригувати майже в реальному часі.

3.2. Імплементація пропонованої навченої нейронної мережі для моделювання відеоігр

У цьому розділі представлено підтвердження ефективності системи обробки відеоінформації на основі глибокого навчання у динамічно мінливому середовищі. З цією метою ми симулюємо гру Atari Space Invader, яку можна розглядати як спрощене зображення сценарію військового поля бою. Atari Space Invaders – це легендарна аркадна відеогра, випущена компанією Atari в 1978 році. Вона вважається однією з найвпливовіших ігор усіх часів, яка визначила жанр "шутер" і стала символом золотого віку аркадних ігор.

Якщо говорити точніше, ця відеогра повторює реальний сценарій на полі бою, містить потік даних, середовище, що постійно змінюється, і кілька рухомих космічних кораблів противника, які стріляють у гравця. Ми застосовуємо пропоновану мережу для точного відстеження цих ворогів, що рухаються, обробляючи безперервні відеокадри гри. Подібно до сценарію на полі бою, зібрані зображення з відеоігри містять довідкову інформацію, яка

робить отримання важливої інформації (наприклад, позиції та стан ворогів) нетривіальним. Детальний опис реалізації для отримання інформації такої відеогри наведено нижче.

3.2.1. Реалізація етапу I

Для отримання інформації з відеокадрів реалізовано нейронну мережу H-score на основі CNN. Конфігурація розглянутої моделі CNN представлена в таблиці 3.1.

Таблиця 3.1.

Конфігурація CNN для гри

Number of input samples, n	20000
Size of minibatch	50
Optimizer	Stochastic gradient descent
Learning rate	e^{-5}
Epochs	200
Input shape	$3 \times 800 \times 600$
Output shape	1x15 vector
Weight decay	e^{-4}
Size of the background objects	10x10 pixels
Kernel size	10x10
CNN output channels	16
Shape of the channel	18×18

Ми підкреслюємо, що архітектура та складність необхідної моделі CNN залежать від складності середовища (наприклад, кількості станів і кількості ворогів). Повідомлена конфігурація CNN вибирається після кількох експериментів методом проб і помилок. Зауважимо, що після належного навчання нейронна мережа H-score навчиться видаляти некритичні дані із зображення та зберігає лише необхідну інформацію. Щоб продемонструвати цей факт, ми побудували теплову карту інформації, отриманої кожним із 16 каналів навченого CNN на рис. 3.5. Такий рисунок показує, що коли ми подаємо зображення на вхід навченої нейронної мережі H-Score, більша частина фону зображення видаляється в останній шар і лише позиція ворога

виділяється на теплових картах. По суті, навчена нейронна мережа H-score вчиться ефективно фіксувати потрібну інформацію з відеокадрів.

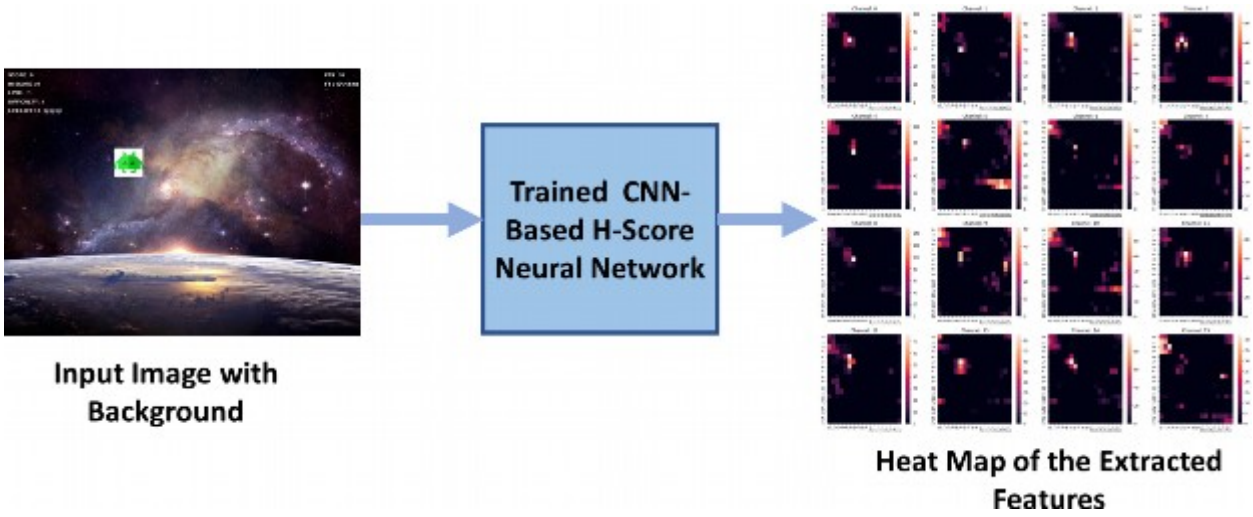

Рис. 3.5. Теплова карта, отримана від навченої CNN

3.2.2. Реалізація етапу II

Для асоціації отриманої інформації з відповідними мітками використовується нейронна мережа, вхідний рівень якої містить 16 нейронів, а вихідний — 3 нейрони (відповідають трьом можливим станам ворога, а саме: рух, стрілянина та бездіяльність). Розглянута мережа CNN на кроці I має загалом 16 каналів (або карт активації), і кожен канал є двовимірною матрицею 18 x 18. Зв'язування інформації цих каналів з відповідними мітками, наприклад, станами та позиціями ворогів, здійснюється в наступні три кроки.

1. Крок 1: спочатку ми паралельно переглядаємо канали мереж CNN і вибираємо одну комірку з кожного з цих каналів по рядку. Таким чином ми вибираємо загалом 16 клітинок, які формують вхідні дані нашої другої нейронної мережі.

2. Крок 2: Далі створюємо позначений набір даних для навчання другої нейронної мережі. Нагадаємо, вихідний рівень другої нейронної мережі забезпечує стани ворога. Оскільки стан кожної вибраної комірки на Етапі 1 відомий, загалом 324 (тобто 18 x 18) навчальних зразків отримують з одного

позначеного вхідного зображення. Навчання другої нейронної мережі здійснюється шляхом розгляду навчальних зразків, отриманих з кількох позначених зображень, як вхідних даних і застосування методу зворотного поширення.

3. Крок 3: на етапі тестування ми спочатку проходимо всі комірки каналів CNN і визначаємо стан(и) комірок, застосовуючи нейронну мережу, навчену на кроці 2 . Якщо будь-яка клітинка в каналах CNN містить стани руху або стрільби, ми витягуємо фактичне положення ворожого космічного корабля, захопленого цією клітинкою, шляхом відображення положення клітинки в оригінальному зображенні. Загальна процедура отримання фактичної позиції ворога на вихідному зображенні пояснюється на наступному прикладі. Припустімо, що фактичний розмір вихідного зображення становить 500 x 500 пікселів, вхідний сигнал навченої нейронної мережі H-score становить 100 x 100 пікселів (тобто вхідне зображення зменшено в 5 разів), а розмірність канали CNN, отримані з навченої нейронної мережі H-score становить 10 x 10. Припустимо, що в певному каналі CNN виявлено, що комірка, розташована в позиції (5, 5), містить рухомий або перезавантажуваний космічний корабель противника.

Відповідно до рис. 3.5, канал CNN, по суті, є версією вхідного зображення зі зниженою дискретизацією з пригніченим фоном. Таким чином, положення ворожого космічного корабля на вхідному зображенні, представленому нейронній мережі H-score, визначається шляхом масштабування положення клітинки 100/10 або в 10 разів, тобто позиція ворожого космічного корабля на вхідному зображенні для нейронної мережі H-score отримана в (50, 50) піксельних координатах. Подібним чином, застосовуючи 500/10 = 50-кратне масштабування, положення ворожого космічного корабля на вихідному зображенні отримується в (250, 250) піксельних координатах. Примітно, що на практиці в різних каналах CNN може бути виявлено, що ряд комірок містить ворожий космічний корабель, і,

відповідно, вищезгаданий підхід передбачає кілька положень ворожих космічних кораблів на вихідному зображенні.

Тим не менш, наші експериментальні результати показують, що всі ці прогнозовані позиції близькі до фактичної позиції ворожого космічного корабля на зображенні, і, отже, вищезгаданий підхід забезпечує високу впевненість у визначенні місцезнаходження ворожих космічних кораблів на зображенні. Тепер, на останньому кроці, якщо позиція ворога, виявлена після класифікації кожної клітинки карти активації, знаходиться на (5,5) у координатах x,y. Ми масштабуємо його в 10 разів (100/10 = 10), щоб отримати позицію у вхідному зображенні моделі H-Score CNN. Використовуючи цю техніку, ми можемо сказати, що ворог знаходиться в позиції (50,50) на вхідному зображенні розміром 100 x 100. Подібним чином ми можемо виконати ще одне масштабування від позиції карти активації до вихідного зображення.

Можна сказати, що якщо ворог знаходиться на позиції (5,5) на карті активації, то, збільшивши її в 50 разів (500/10 = 50), ми отримаємо координату (250,250) на вихідному зображенні розміром 500 x 500. Ми вважаємо, що карти активації є просторовим представленням початкового зображення нижчого розміру. Оскільки карти активації є нижчими, важко отримати точне розташування ворога на вихідному зображенні, тому ми можемо визначити лише регіон, а не точні (x,y) координати ворога на вихідному зображенні.

3.3. Оцінка продуктивності глибокого навчання мережі

В експериментах із симуляцією ми розглядаємо гру Atari space invader із наступними налаштуваннями за умовчанням. Гра містить N ворожих космічних кораблів, які змінюють стани через випадкові проміжки часу, де N змінюється від 2 до 20 ворожих космічних кораблів. Кожен ворожий космічний корабель міг перебувати в одному з двох станів - (I) рух і (II)

стрілянина, в будь-який момент часу. Зокрема, кожен ворожий космічний корабель рухається більшу частину часу по екрану та змінює свій стан на перезарядження/стрілянину протягом невеликого проміжку часу.

Наше завдання полягає в тому, щоб виділити низьковимірні семантичні ознаки відеокадрів і якомога точніше визначити стани та позиції всіх ворогів на екрані за такими семантичними ознаками. Ми програмуємо ворожі космічні кораблі двома різними кольорами, щоб розрізняти їхні стани. Якщо колір ворожого космічного корабля червоний, це означає, що ворог знаходиться в русі. Навпаки, зелений колір ворожого космічного корабля вказує на те, що противник перебуває в стані стрільби. Знімок відеоігри з різними станами космічного корабля противника показано на рис. 3.6.

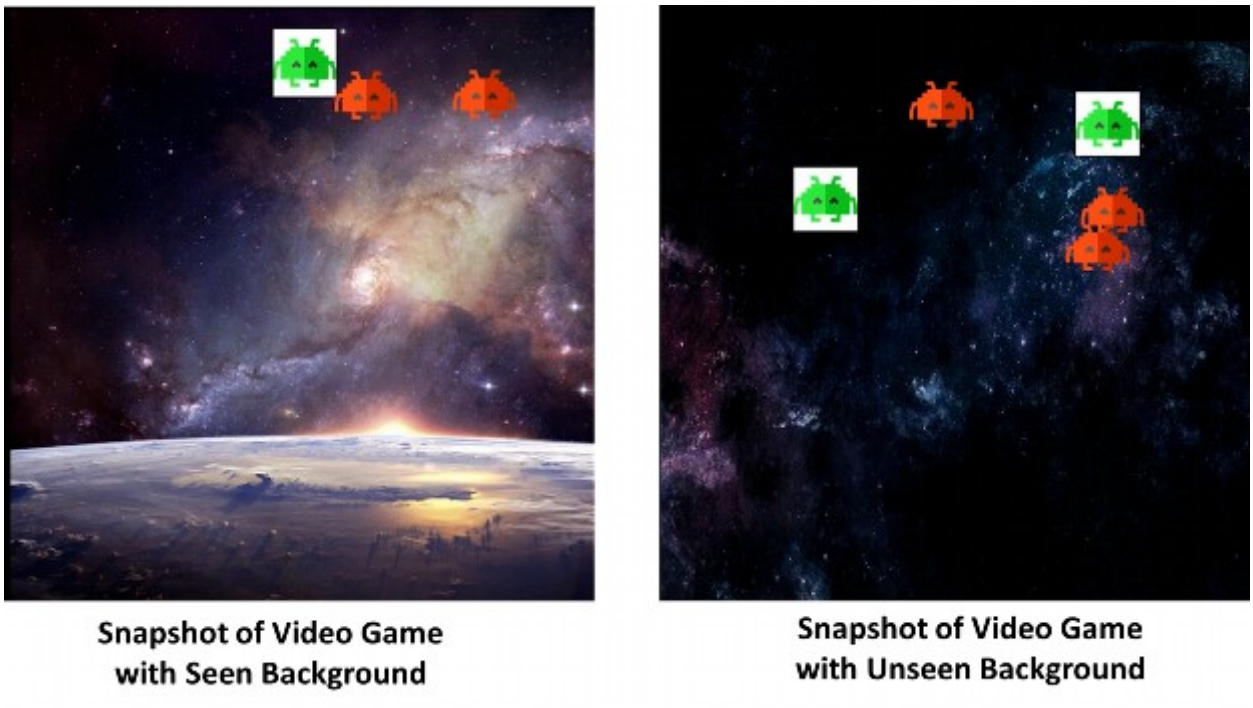

Рис. 3.6. Скріншоти відеогри

Під час навчання ми використовуємо один фон як фон для нашої гри. Для навчання нейронної мережі H-score на основі CNN (параметри якої описано в таблиці 3.2) ми беремо безперервні кадри з наших відеоігор без жодних міток. Навпаки, ми використовуємо 462 мічені зображення для навчання нейронної мережі, яка використовується на етапі II. Оскільки

навчена нейронна мережа H-Score зберігає лише важливі дані із зображення, другій нейронній мережі набагато легше вивчати представлення даних без використання великої кількості навчальних зразків. На етапі тестування алгоритму ми збільшуємо загальну кількість космічних кораблів противника до 20 і змінюємо фон противника, щоб перевірити масштабованість і здатність нашого алгоритму отримувати критичну інформацію в невидимому фоні. Для кожного розглянутого сценарію ми проводимо 50 незалежних експериментів, щоб усереднити незначні відхилення отриманих результатів шляхом одного запуску експерименту.

3.3.1. Визначення показника точності (Accuracy)

Ми визначаємо точність передбачення стану (або просто точність) як відношення загальної кількості правильних передбачень до загальної кількості передбачень станів супротивника. Зокрема, метрика точності розраховується як

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

де TP, TN, FP і FN означають загальну кількість істинних передбачень рухомих станів, істинних передбачень станів стрільби, хибних передбачень рухомих станів і хибних передбачень станів стрільби, відповідно. У наступних експериментальних результатах ми демонструємо точність роботи нашої моделі як для видимого, так і для невидимого фону.

На рис. 3.7 показано малюємо середню точність мережі, змінюючи кількість ворогів (тобто кількість об’єктів) у відеокадрах як для видимого, так і для невидимого фону. Для заданої кількості ворогів і фону метрика точності обчислюється для всіх 50 симуляцій, а потім повідомляється середнє значення цих значень точності. Рисунок 3.7 ілюструє, що пропонована мережа досягає високої точності для невеликої кількості ворогів як у видимому, так і в невидимому фоні. Однак точність знижується зі

збільшенням кількості ворогів. Це інтуїтивно очікувано, оскільки збільшення кількості ворогів ускладнює середовище. Тим не менш, з рис. 3.7, ми спостерігаємо, що пропонована мережа досягає понад 90% точності навіть з 20 ворогами в системі. Нагадаємо , що як для видимого, так і для невидимого фону модель тренується з використанням лише 2 ворожих космічних кораблів у кадрах відео. По суті, дану мережу можна масштабувати для великої кількості ворогів і стійкий до зміни фонових сценаріїв.

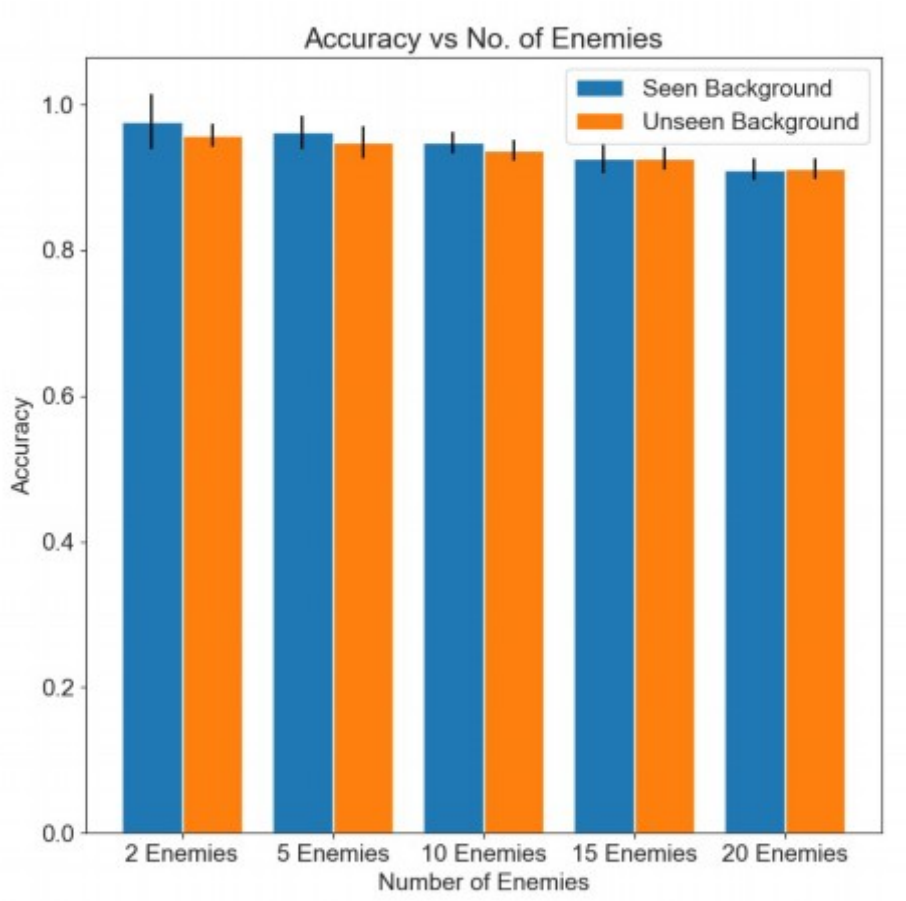

Рис. 3.7. Середні показники точності

У вищезазначених показниках середньої точності ми ілюструємо точність моделі для кінцевих зображень, застосованих до навченої моделі. Щоб підтвердити стабільність навченої мережжі, також важливо проаналізувати тимчасову поведінку точності моделі. У цьому контексті ми

будуємо графік залежності точності від кроку за часом на рис. 3.8 як для видимого, так і для невидимого фону.

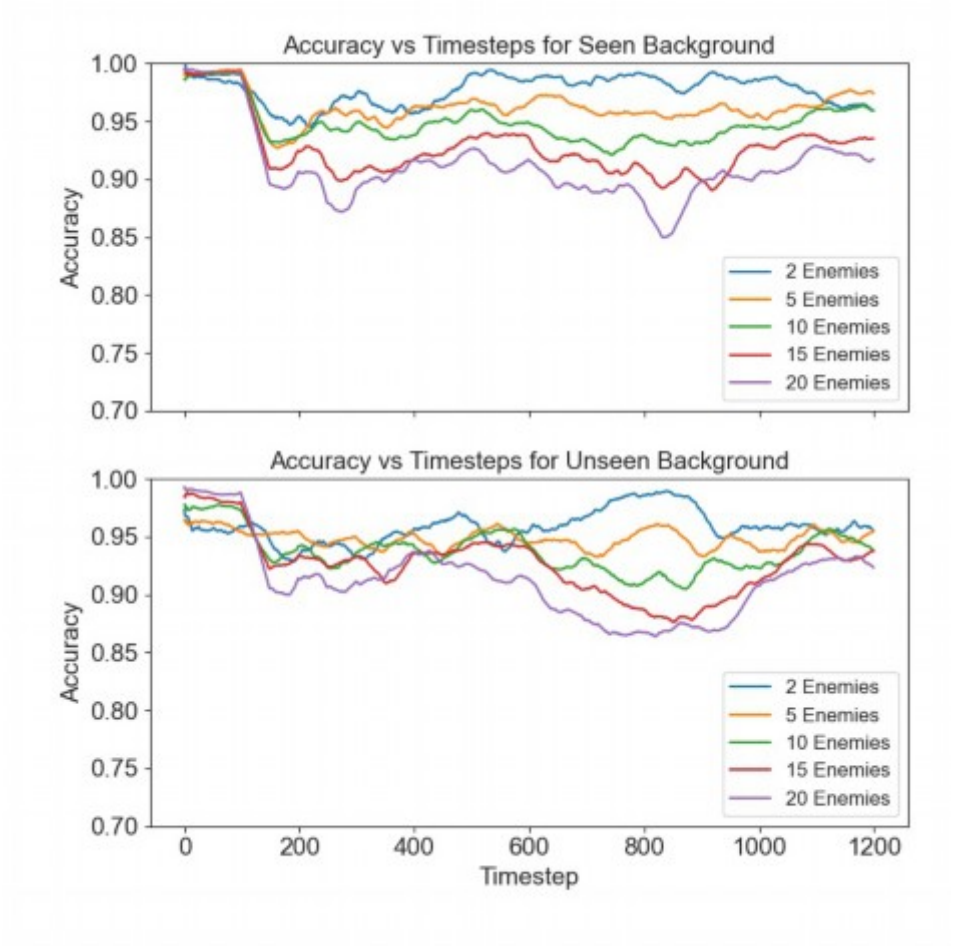

Рис. 3.8. Точність роботи навченої мережі залежно від часового кроку

Для невеликої кількості ворогів, у видимому та невидимому фоні, точність залишається стабільною між 95% і 100% протягом усіх часових кроків. Однак для великої кількості ворогів (тобто 20) точність моделі падає приблизно до 87% лише на частку часу. Загалом ми робимо висновок, що дана мережа досягає стабільно високої точності протягом усіх часових кроків, незалежно від кількості ворогів і фонових сценаріїв.

3.3.2. Визначення середньої похибки відстані (MDE)

MDE (Mean Distance Error) є важливим інструментом для оцінки точності моделей і алгоритмів в різних областях. Вона дозволяє порівнювати

різні методи, вибирати оптимальні параметри моделей та оцінювати якість отриманих результатів.

У цьому розділі оцінюється метрика помилки середньої відстані (MDE), щоб зафіксувати різницю між фактичним і прогнозованим положенням противника у відеокадрах. Позиція ворога у відеокадрах прогнозується шляхом визначення місцезнаходження активованої комірки в каналі CNN і зіставлення такої комірки з вихідним вхідним кадром зображення. Метрика MDE визначає середнє значення евклідових відстаней між фактичною та всіма прогнозованими позиціями противника.

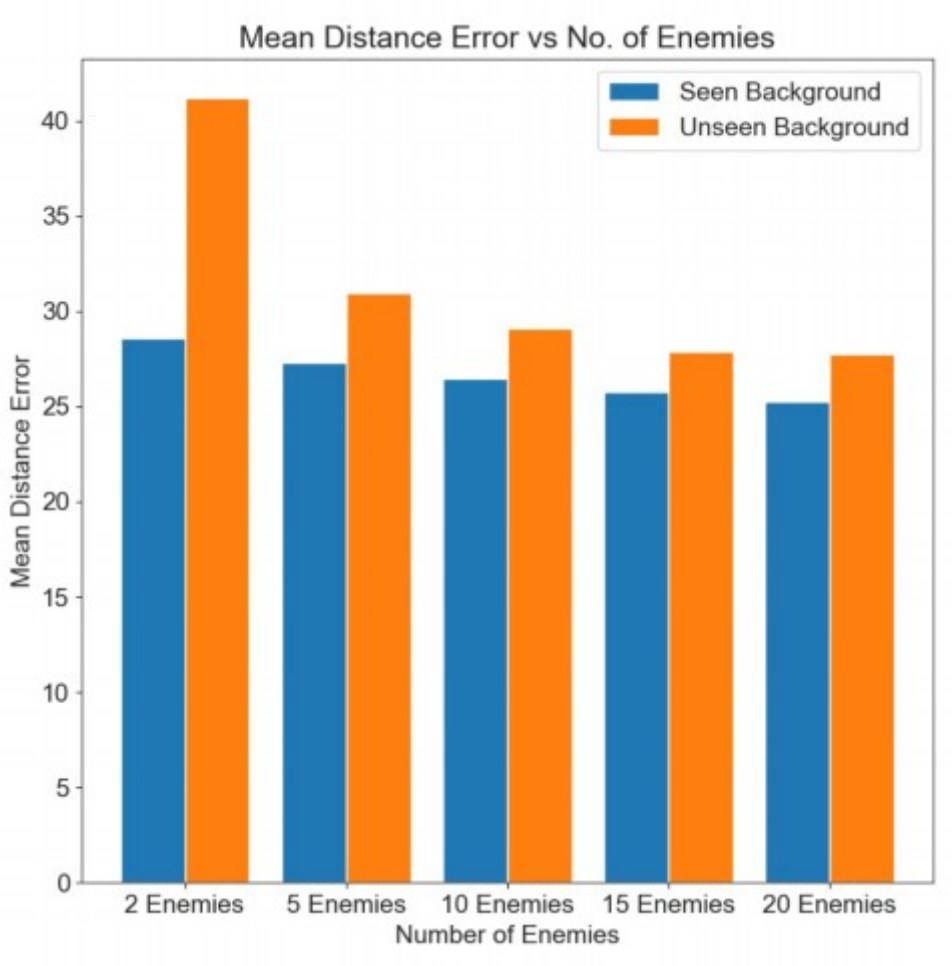

Рис. 3.9. Показник середньої похибки відстані (MDE)

На рис. 3.9, показано графік метрики MDE, що спостерігається у видимому та невидимому фонах, змінюючи кількість ворогів у відеокадрах. Як і очікувалося, показник MDE збільшується для невидимого фону. Крім

того, як для видимого, так і для невидимого фону показник MDE зменшується зі збільшенням кількості ворогів. Інтуїтивне пояснення такого спостереження надається наступним чином. Нагадаємо, що мережа передбачає набір можливих позицій кожного ворога на зображенні. Для простоти припустімо, що це передбачення відбувається цілком випадковим чином, тобто система вибирає випадкові точки у двовимірному просторі, щоб визначити місцезнаходження ворога. Коли є невелика кількість ворогів, більшість цих передбачуваних точок будуть далеко від фактичних позицій ворогів, що призведе до великого MDE. Навпаки, якщо на зображенні є велика кількість ворогів (тобто об'єктів), шанси на визначення місцезнаходження ворога (тобто об'єкта) шляхом випадкового прогнозування положення збільшуються. Це призводить до зниження MDE. Наголошуємо, що на практиці мережа не випадково передбачає позиції ворогів на зображенні. Натомість, завдяки нейронній мережі H-score, мережа спочатку захоплює частину (частини) зображень, що містять високу щільність ворогів, а потім прогнозує позиції ворогів на основі захоплених частин за допомогою відображення клітинок. По суті, здатність пропонованої мережі знаходити ворога у відеокадрах (кадрах) збільшується, коли в грі є велика кількість ворогів. Завдяки такому факту показник MDE знижується зі збільшенням кількості ворогів у розглянутій відеогрі.

На рисунку 3.10, показано еволюцію метрики MDE відносно кроку в часі вздовж довірчого інтервалу передбачень, зроблених пропонованою навченою мережею. Як і очікувалося, MDE зменшується, коли кількість ворогів збільшується з 10 до 20. Крім того, для різної кількості ворогів у відеокадрах ми спостерігаємо, що положення, передбачені системою, не мають великої дисперсії, і, як наслідок, метрика MDE залишається майже незмінною для всіх часових кроків. Зокрема, вищезгадана тенденція метрики MDE застосовна як до видимого, так і до невидимого фону, як показано на рис. 3.10. Отже, пропонована навчена мережа також дуже стабільна і надійна з точки зору точного передбачення позицій ворогів у відеокадрах.

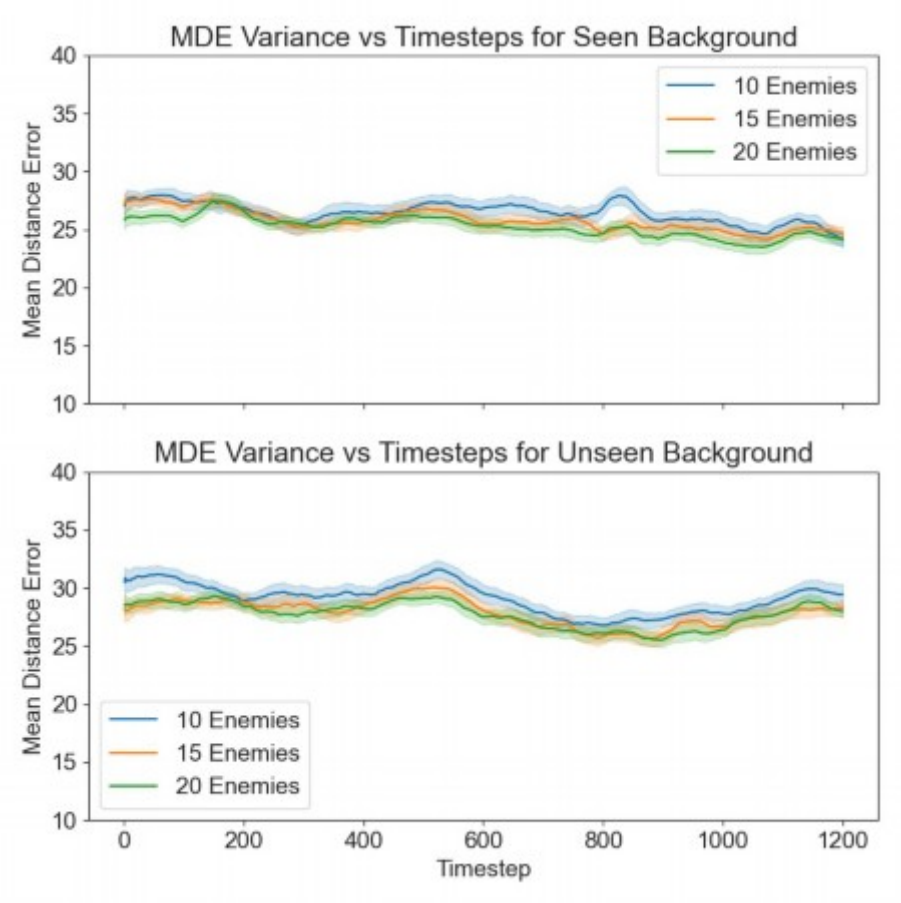

Рис. 3.10. Середня похибка відстані навченої мережі залежно від часового кроку

3.4. Виявлення аномалій у бездротових комунікаційних мережах засобами машинного навчання

Загальний випадок використання під час роботи з наборами даних реального світу полягає в тому, щоб з'ясувати, які точки даних у нашому наборі даних відрізняються від усіх інших точок даних. Ці точки даних також називають аномаліями або викидами. Аномалії можуть виникати через численні причини, наприклад, неправильні журнали, помилки в коді, збій системи, незвичайна поведінка користувача тощо. Якщо метою проблеми є визначення місцезнаходження всіх таких точок даних, проблема називається виявленням аномалії. Одним із таких прикладів є виявлення вторгнень у бездротові системи.

Нещодавно відбувся прогрес у радіотехнологіях, що призвело до різкого зростання попиту на ресурси спектру, що поставило під напругу і без того обмежену доступність спектру. Зі збільшенням такої технології спостерігається поступове зростання кількості зловмисників, які хочуть використовувати спектр і використовувати його без будь-якого дозволу, наприклад, втручання; до глобальної навігаційної супутникової системи (GNSS) значно зросла [43, 44]. Спільне використання спектру також може бути порушено під час планування стільникового зв'язку оператора, що вплине на клієнтів. Виявлення аномалій у спектрі стало важливим для виявлення таких вторгнень, щоб їх можна було швидко усунути.

Тепер питання полягає в тому, як ми можемо визначити аномалію? Відповідно до [12], це «щось інше, ненормальне, незвичайне або непросто класифіковане відхилення від загального правила». Аномалії можуть бути в будь-якій формі, наприклад, обсяг транзакції в 1 мільйон доларів на веб-сайті електронної комерції може бути аномалією, раптовий сплеск мережевих ресурсів комп'ютерного сервера через зловмисне вторгнення може бути аномалією.

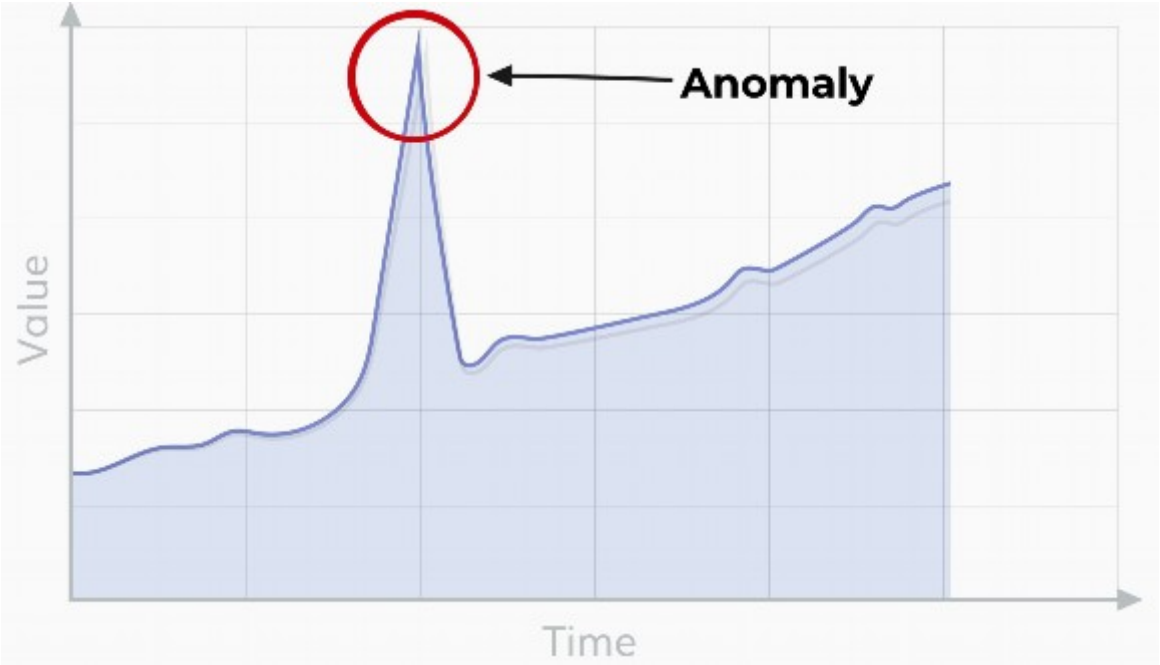

Рис. 3.11. Приклад аномалії в даних

Один із прикладів аномалії показаний на рис. 3.1 діаграма відображає вартість ресурсу в часі. Існує чітка тенденція до зростання вартості, але раптовий сплеск вартості протягом дуже короткого інтервалу є аномалією.

Для нашого дослідження ми вважали звичайний бездротовий сигнал (WiFi) базовими даними (базовим сигналом) і наклали його на сигнал Bluetooth протягом певного періоду часу, щоб створити перешкоди. Такі перешкоди також можна вважати аномалією, у загальному випадку цей сигнал Bluetooth може бути будь-яким іншим сигналом.

Основна мета нашого дослідження полягала в тому, щоб побачити, чи можемо ми виявити аномалії в існуючих бездротових сигналах без жодного позначеного набору даних. Одна з головних причин такого підходу замість навчання з даними з мітками полягає в тому, що дані з мітками важко отримати, а в мережі занадто багато різних типів аномалій (WiFi, Bluetooth, LTE тощо), які нам доведеться враховувати для. Таким чином, навчання моделі одного класу для виявлення будь-яких аномалій було хорошим шляхом вперед.

Це можна подумати з іншої точки зору, давайте розглянемо кімнату та спектр у цій кімнаті як сигнали базового спектру, і ми хочемо провести кілька експериментів у цьому стабільному середовищі. Тепер, якщо є будь-які перешкоди через будь-які зовнішні пристрої, ми хочемо їх уникати, щоб вони не впливали на наше оточення, тому ми можемо використовувати цей алгоритм виявлення аномалій, щоб визначити, чи є якісь аномалії в сигналах і чи вони є правильно, перш ніж продовжити наш звичайний експеримент у нашому середовищі.

3.4.1. Постановка проблеми

Нашою метою було виявити аномалії в даному спектрі. Ми використовували набір даних CRAWDAD [38] як наш основний набір даних для бездротових сигналів. CRAWDAD (California Repository for Alternative Wide-Area Data) – це велика колекція даних, зібраних з реальних мереж та

систем. Сигнал WiFi вважався основним сигналом або сигналом за замовчуванням, і сигнал Bluetooth перекривався сигналом WiFi протягом певного часу, щоб створити перешкоди. Мета полягала в тому, щоб визначити це втручання без будь-яких попередніх позначок. Ми назвали інтерференцією аномалію в спектрі. Набір даних містив сигнали з різними значеннями співвідношення сигнал/шум (SNR) -10 дБ, 0 дБ, 10 дБ і 20 дБ. Ми хотіли побачити, як працює наш алгоритм у кожній із цих точок даних SNR і як він порівнюється зі звичайними алгоритмами виявлення аномалій.

3.4.2. Попередня обробка набору даних

Нашим першим завданням було створити набір даних, що моделює потік необроблених сигналів. CRAWDAD має 225 тисяч зразків, і кожен сигнал мав 128 точок вибірки IQ. У цьому наборі даних є 15 класів сигналів, класи 11, 12 і 13 належать до Wi-Fi, а класи від 1 до 10 належать до сигналів Bluetooth.

Відношення сигнал/перешкода (SIR)

Для створення нашого набору даних нам довелося об’єднати звичайний сигнал Wi-Fi із сигналом Bluetooth, щоб створити аномалію. Коли ми об’єднуємо ці два сигнали з відповідними SNR, ми можемо обчислити значення SIR. Ми взяли сигнал Wi-Fi з різними значеннями SNR [-10, 0, 10, 20] і об’єднали його з сигналом Bluetooth із SNR 0 дБ. Після об’єднання значення SIR нового сигналу можна обчислити як:

$$SIR(dB) = SignalSNR(dB) - InterferenceSNR(dB)$$

У нашому випадку SignalSNR був сигналом Wi-Fi з різними SNR, а InterferenceSNR був сигналом Bluetooth, який ми зафіксували на рівні 0 дБ.

Попередня обробка необробленого набору даних

Мережа на основі H-Score потребує залежного від часу потоку даних, тому ми хотіли перетворити наші дані в хронологічну форму, імітуючи моніторинг реальних випадків використання. Спочатку ми об’єднали сотні сигналів [128 розмірів кожен] разом, щоб створити єдиний сигнал із 256 тис. балів IQ. Це було зроблено для імітації реального потоку даних, і ми створили кілька таких зразків 256 тис. балів IQ.

Рис. 3.12. Демонстрація ковзного вікна [17]

Потім ми використали техніку ковзного вікна, як показано на рис. 3.12 взявши вікно розміром 256 і крок із 10 точок даних, щоб створити кілька менших сигналів з одного сигналу. Ми використовували ту саму техніку, щоб створити загалом 51487 навчальних зразків і 36773 тестових зразків. Отже, таким чином ми могли б створити залежний від часу потік даних з кожного сигналу, який ми очікуємо в реальному сценарії. Коли ми отримали цю підмножину необроблених зразків IQ, нашим наступним кроком було перетворення цих даних у формат, сумісний із архітектурою нашої нейронної мережі.

Створення спектрограм

Наша нейронна мережа на основі H-Score потребує даних у формі наших зображень, тому ми вирішили використати спектрограму з наших

зразків IQ як вхідні дані для нашої моделі. Спектрограма — це візуальне представлення потужності сигналу та того, як він змінюється з часом. Потужність сигналу визначається його частотою та амплітудою. Спектрограма має два виміри, одна вісь представляє час, а інша частота. Амплітуда певної частоти або сила сигналу в будь-який момент часу представлена кольором цієї точки на зображенні. Наприклад, на рис. 3.13 показана спектрограма, де частота коливається від 0 до 125, а час – від 0 до 1800 одиниць, а силу сигналу можна побачити на кольоровій панелі, вона коливається від -10 до 30.

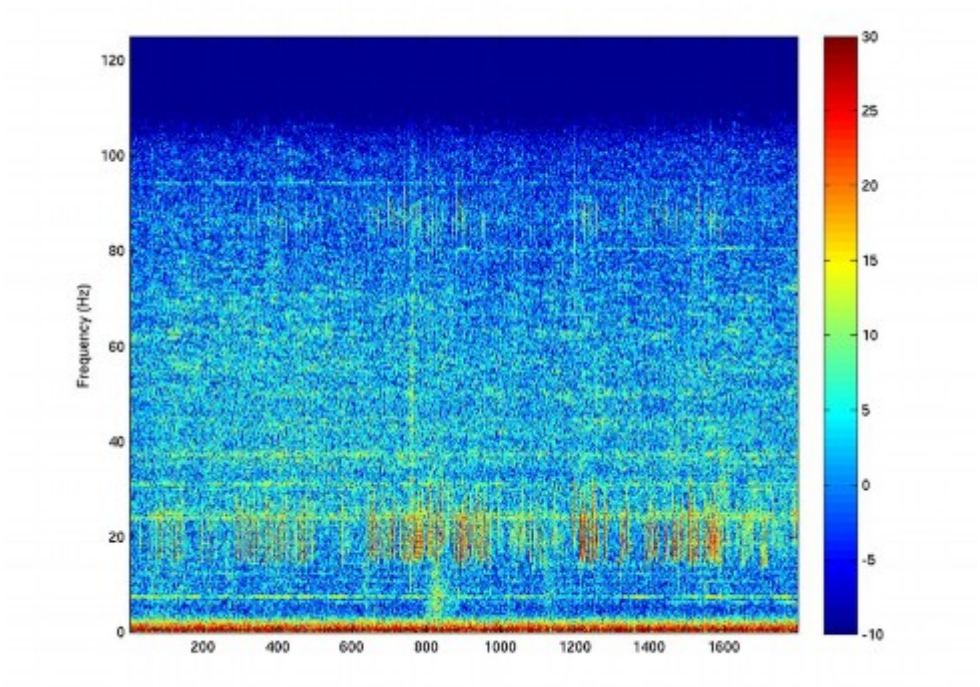

Рис. 3.13. Зразок спектрограми

Спектрограма була нашим вибором вхідних даних через дві причини: по-перше, це дуже швидко обчислити спектрограму, а по-друге, це широко вивчений алгоритм, який буде використовуватися як вхідні дані для моделей глибокого навчання, і це задовольнило наше обмеження щодо використання спектрограми зображення як відеопотік даних.

Спектрограму можна розрахувати за необробленими зразками IQ шляхом короткочасного перетворення Фур'є (STFT) сигналу. У цій роботі ми використовували функцію pspectrum з MATLAB для генерації спектрограм з використанням наступного набору параметрів:

1. Мінімальний поріг = - 80 дБ
2. Частота дискретизації = 10^7 Гц
3. Відсоток перекриття = 99%
4. Витік = 1
5. Роздільна здатність по частоті = $3 * 10^5$ Гц

Після того, як ми згенерували спектрограми, ми зберегли їх у форматі зображення з відповідними індексами, щоб спектрограма, створена для вікна часу t, мала індекс i , а спектрограма вікна t+1 мала індекс i+1. Порядок спектрограми було збережено, оскільки алгоритм H-Score вимагає, щоб вхідні дані залежали від часу. Після цих кроків ми створили 20 тисяч зразків спектрограми з індексом часу для кожного значення SIR.

3.4.3. Запропонований підхід виявлення аномалій

Подібно до системи обробки відеоінформації на основі глибокого навчання, було розбито постановку проблеми на дві частини та розв'язали їх окремо. На першому кроці ми використовували мережу CNN на основі H-Score, щоб витягти характеристики з набору даних, а на другому кроці ми використали звичайний алгоритм виявлення аномалій у цьому наборі даних, щоб виявити аномалії.

На першому кроці ми взяли дві послідовні спектрограми, проіндексовані за часом, як вхідні дані для моделі H-Score CNN. Конфігурація моделі CNN наведена в таблиці 3.2.

Повідомлена конфігурація CNN вибирається після кількох спроб і помилок, щоб отримати найкращий результат. Щоб перевірити правдивість нашої навченої моделі, ми також побудували теплові карти каналів CNN для спектрограм з перешкодами та без них, як показано на рис. 3.14 та 3.15.

Таблиця 3.2.

Конфігурація CNN для виявлення аномалії

Number of input samples, n	$3 \times 128 \times 128$
Size of minibatch	256
Optimizer	Stochastic gradient descent
Learning rate	e^{-5}
Epochs	200
Input shape	$3 \times 64 \times 64$
Kernel size	9×9
CNN output channels	8
Shape of the channel	16×16

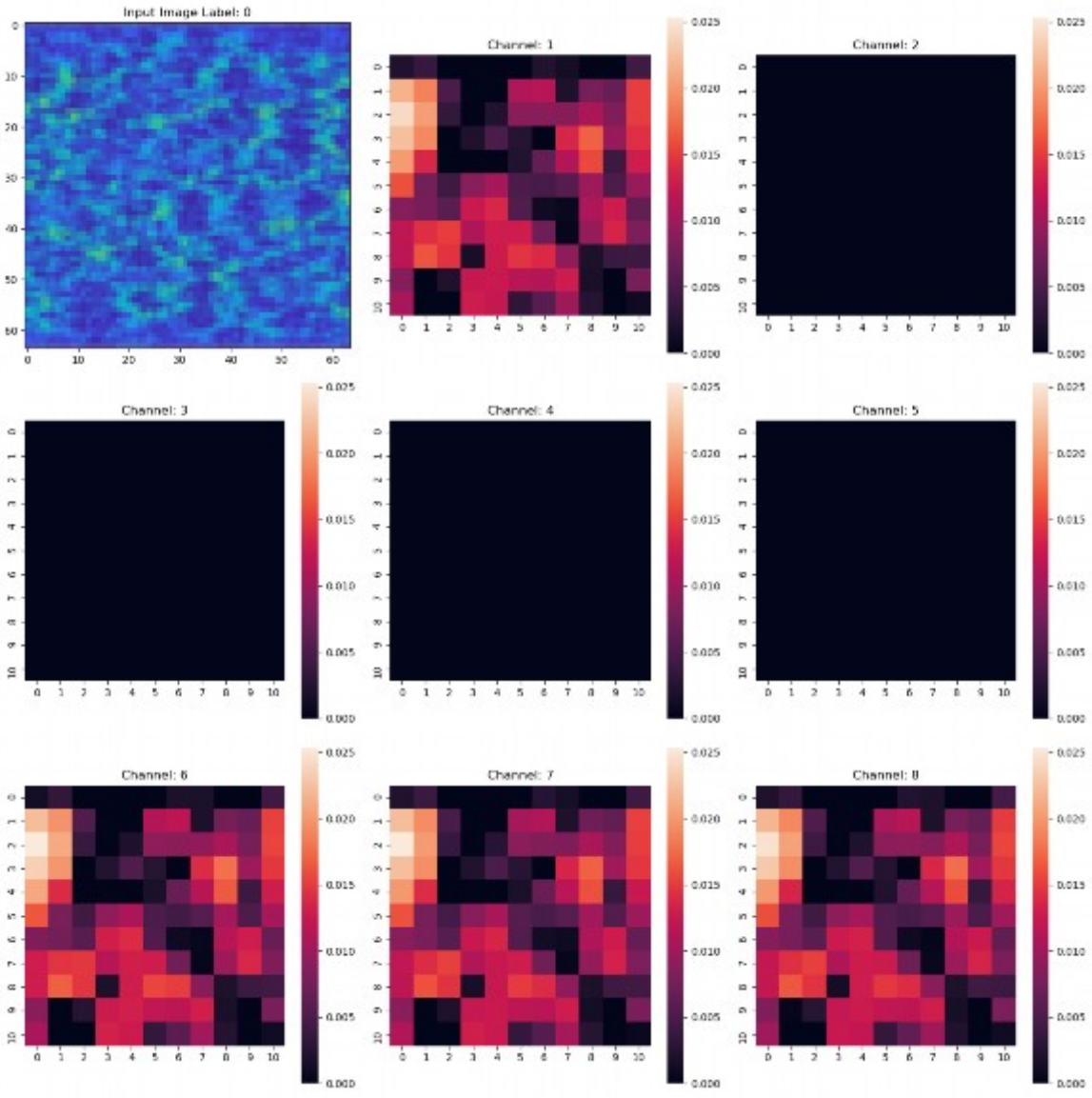

Рис. 3.14. Теплова карта каналів CNN без перешкод

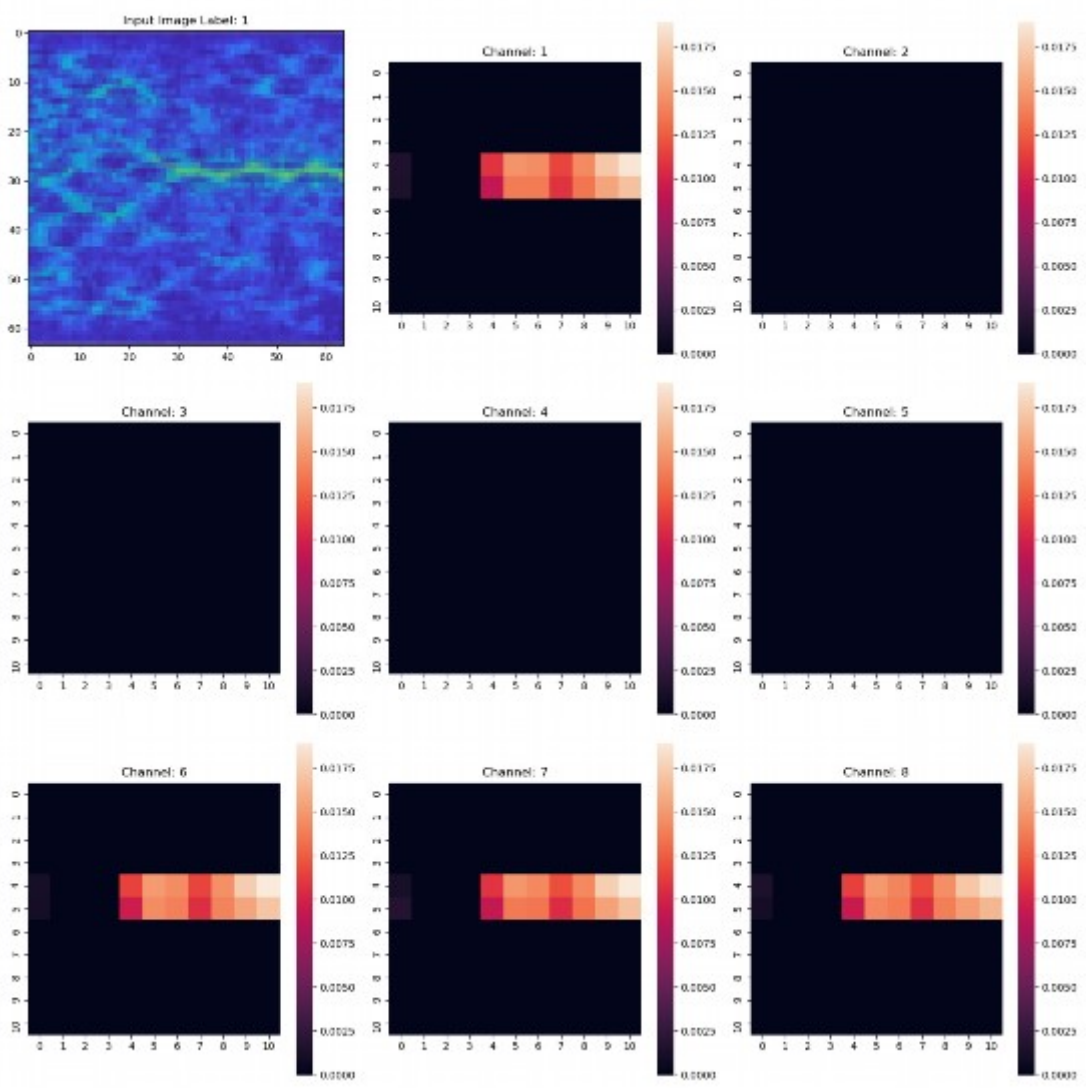

Рис. 3.15. Теплова карта каналів CNN з перешкодами

Перше зображення в сітці є вхідним зображенням для моделі H-Score, а решта зображень є тепловими картами карт активації CNN або каналів активації. Ми бачимо, що коли спектрограма без перешкод подається в мережу, вона визначає загальну структуру сигналу, але коли спектрограма сигналу з перешкодами подається в модель, вона пригнічує всі шуми та лише підкреслює частину перешкод. сигнал. З рисунків 3.14 і 3.15, очевидно, що принаймні деякі канали навченого H-показника захоплюють шаблон сигналу (з перешкодами та без них), навіть за наявності шуму.

На другому кроці ми використовуємо навчену модель з кроку 1. Спершу ми пропускаємо спектрограми без перешкод через модель CNN, а потім використовуємо зведені карти активації як функції для алгоритму

виявлення аномалії. Ми навчили кілька алгоритмів виявлення аномалій Isolation Forest, OneClass SVM і Deep SVDD, щоб створити найкращий алгоритм.

У традиційних керованих алгоритмах машинного навчання завжди існує цикл зворотного зв'язку, коли ми коригуємо нашу модель на основі попередніх позначених даних, але у випадку алгоритмів виявлення аномалій мітки відсутні, тому неможливо отримати цикл зворотного зв'язку . Одним із способів зробити це є використання техніки перевірки K-Fold, коли ми оптимізуємо моделі та оцінюємо нашу модель на основі набору тестів, але це призведе до переобладнання моделі та витоку даних, що призведе до низької узагальненої продуктивності.

3.5. Оцінка продуктивності машинного навчання для виявлення аномалій в комунікаційних мережах

Оптимізація гіперпараметрів є дуже критичним завданням для будь-якого порівняння моделей машинного навчання. Щоб знайти найкращі гіперпараметри для моделей машинного навчання, ми використали фреймворк Optuna [1], найсучасніший оптимізатор . Ми оцінили та порівняли моделі, використовуючи їхні найкращі параметри після їх точного налаштування за допомогою параметрів, знайдених Optuna.

Щоб порівняти та порівняти ефективність підходу H-Score, ми також навчили алгоритми виявлення аномалій без попередньої обробки моделі CNN H-Score. Ці моделі були заповнені необробленими зразками спектрограм порівняно з тими, де ми вперше передали ці спектрограми через мережу H-Score.

Оцінку результатів і порівняння обох підходів (з і без H-Score) проводили з двох різних точок зору: по-перше, ми розглянули загальні значення AUC і значення AUC для кожного алгоритму, а по-друге, ми подивився на криві ROC для кожного алгоритму.

Ми вибрали AUC як наш основний показник оцінки, оскільки такі показники, як точність і оцінка F1, не дають повної картини того, як працює модель машинного навчання. AUC означає площу під кривою ROC (Receiver Characteristic Operator). Це один із найкращих показників для оцінки моделей бінарної класифікації, оскільки він повідомляє нам, як працюють наші моделі для різних (частота справжніх позитивних результатів) і FPR (частота помилкових позитивних результатів) за різних порогів. Чим вище значення AUC, тим краще модель розрізняє позитивні зразки від негативних. Крива ROC будується разом із TPR (вісь x) проти FPR (вісь y). TPR також називається Recall або Sensitivity і визначається як:

$$TPR = Recall = Sensitivity = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{TN + FP}$$

Тут TP – це кількість істинних позитивних результатів, FN – це помилкові негативні результати, FP – це помилкові позитивні результати, а TN – це справжні негативні результати в наборі даних. Ми обчислюємо значення TPR і FPR для кожного порогу та будуємо криву ROC, а значення під цією кривою називається AUC.

Нашою основною метою було порівняння нашого алгоритму з існуючими алгоритмами. Алгоритм H-Score можна розглядати як техніку попередньої обробки, яка використовується для вилучення важливої інформації з даних, і якщо ми передамо моделі виявлення аномалій нижче за потоком ці попередньо оброблені функції з моделі H-Score, ми побачимо краща продуктивність порівняно з тим, коли ми просто подаємо алгоритми, попередньо не оброблені моделлю H-Score.

Ми бачимо з рис. 3.16 , що алгоритми працюють значно краще, якщо використовувати модель H-Score як попередницю для них. Підхід H-Score

стабільно показував кращі результати для всіх алгоритмів, One Class SVM (OC-SVM) показав найкращі результати серед інших алгоритмів, за яким йшли Deep SVDD та Isolation Forest.

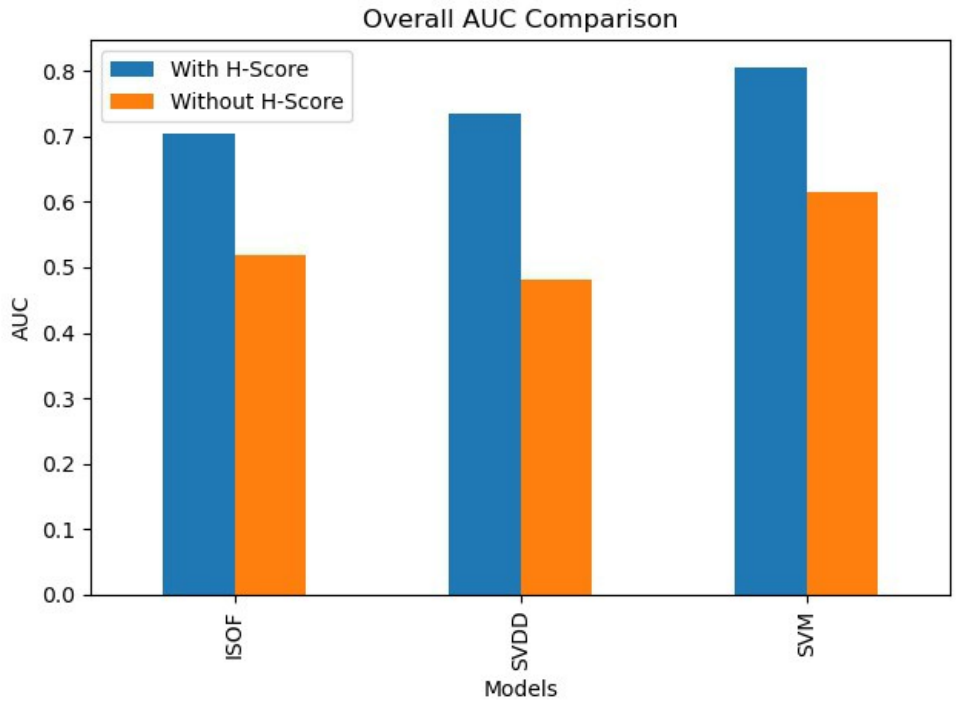

Рис. 3.16. Загальне порівняння AUC

Отримавши загальну картину продуктивності нашої моделі, ми хотіли подивитися, як працює алгоритм для кожного значення SIR. На рис. 3.17 ми наносимо AUC різних алгоритмів виявлення аномалії для таких SIR сигналів WiFi: -10 дБ, 0 дБ, 10 дБ і 20 дБ. У всіх випадках SNR сигналу Bluetooth становив 0 дБ.

Як і очікувалося, алгоритм на основі H-Score показав кращі результати, ніж звичайна версія для всіх алгоритмів виявлення аномалій. Ми спостерігаємо, що алгоритм виявлення аномалій не тільки покращився завдяки нашому підходу, але також відбулося підвищення продуктивності майже в 1,75 рази в кількох сценаріях, наприклад, SVDD та ізольований ліс у SIR 20 дБ і SIR 10 дБ.

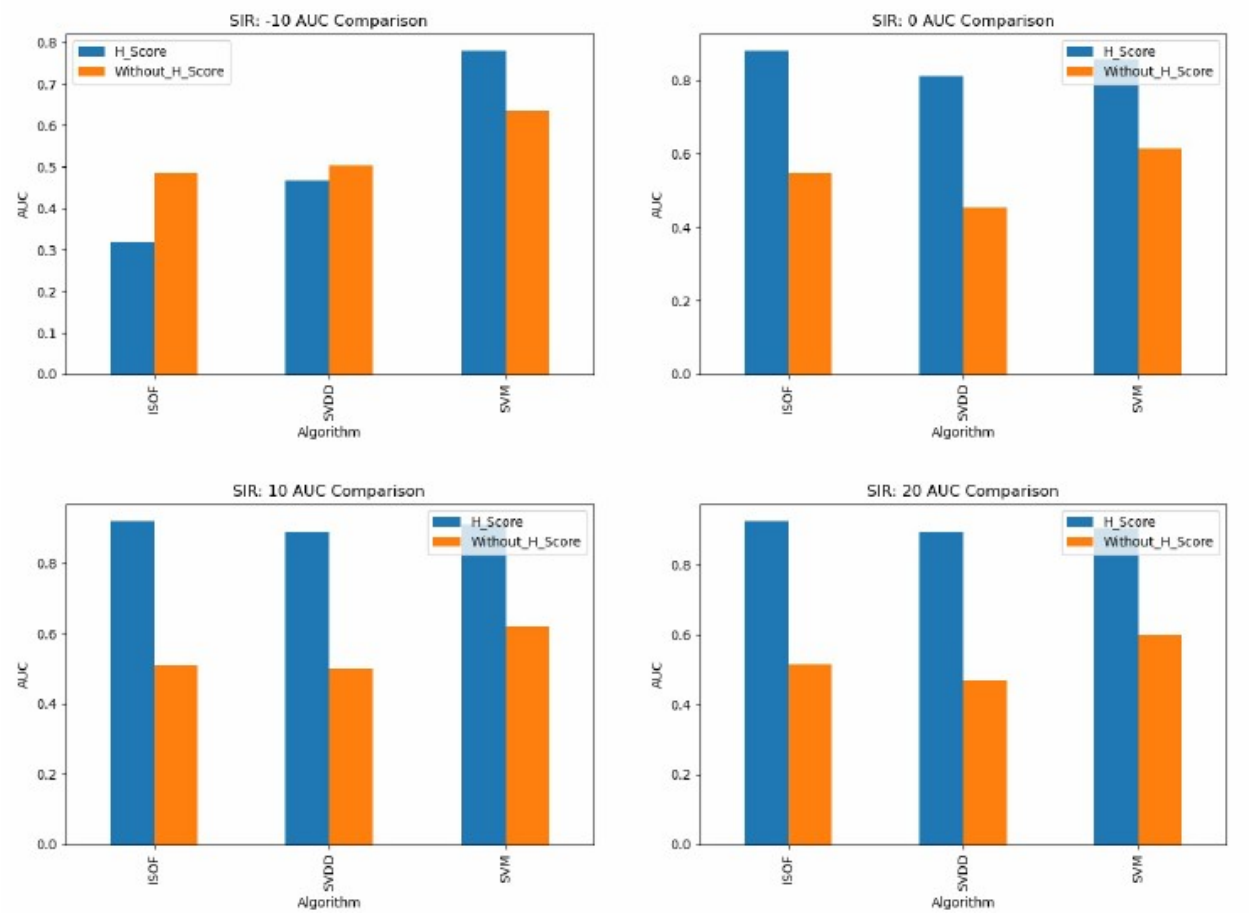

Рис. 3.17. Порівняння продуктивності SIR усіх алгоритмів

Ми помітили, що для SIR -10 дБ алгоритм Isolation Forest із вхідними даними H-Score мав AUC 30%, тоді як вхідні дані без H-Score мали AUC 48%. Однією з причин низької продуктивності в цьому діапазоні SIR є те, що загальна модель, навчена на всіх SIR, може не працювати добре з дуже низьким SIR, це тому, що розподіл даних SIR надзвичайно відрізняється від SIR 10 дБ або 20 дБ. дБ. Дивлячись на розподіл даних балів аномалії для SIR -10 дБ, поріг для розрахунку аномалії буде сильно відрізнятися від порогового значення для SIR 20 дБ. Щоб підтвердити це, ми навчили нашу модель лише на SIR 10 дБ і перевірили значення AUC, ми помітили, що алгоритм із H-Score працює дуже добре та отримав AUC понад 80% порівняно з моделями без H-Score, які отримали 52% показник AUC. Таким чином, під час тренування лише на SIR -10 дБ, алгоритм H-Score знову показав кращі результати, ніж традиційні алгоритми виявлення аномалій. SIR

сигналу не є попередньою інформацією, тому ми не можемо навчити моделі для різних SIR, щоб отримати найкращу продуктивність, тому нам завжди потрібно навчати модель з усіма SIR і максимізувати продуктивність. Це призводить до хорошої продуктивності в деяких значеннях SIR і поганої продуктивності в інших.

Висновки до розділу

Отже, в цьому розділі представлено процес імплементації методів машинного навчання для підвищення ефективності контролю контекстів у комунікаційних системах, зокрема у середовищах відеоінформації та бездротових мереж. Основна увага була приділена побудові архітектури, здатної виділяти ключові об'єкти та контексти у відео. Було реалізовано два основні етапи — вилучення важливої інформації за допомогою нейронної мережі H-score та маркування цієї інформації для підвищення точності розпізнавання контексту.

Було розроблено та протестовано етапи вилучення і маркування інформації, зокрема для симуляційних систем. Це допомогло досягти більш точного моделювання об'єктів і динаміки у відеоіграх, що є важливим для навчання агентів у віртуальному середовищі.

Для оцінки ефективності запропонованої моделі застосовувалися показники точності (Accuracy) та середньої похибки відстані (MDE). Це дало змогу встановити надійність та точність методів, використаних для контролю контекстів у відеоінформації.

У межах цього розділу було сформульовано проблему виявлення аномалій у мережах, проведено попередню обробку набору даних та розроблено ефективний підхід до виявлення аномалій. Було виконано оцінку запропонованого методу за допомогою метрик ефективності, що підтвердило його здатність точно ідентифікувати аномалії у комунікаційних мережах.

ВИСНОВКИ

У магістерській роботі проведено дослідження моделей та методів машинного навчання для контролю контекстів у комунікаційних системах, зокрема у задачах вилучення корисних ознак з великовимірних спостережень, пов'язаних з бездротовим зв'язком. У рамках дослідження розроблено контекстну систему обробки відеоінформації на основі глибокого навчання, здатну точно витягувати критичну і статистично значущу інформацію (наприклад, розташування ворогів на полях битви) із зображень та відео, пригнічуючи фонові елементи. Цей підхід сприяє підтримці семантичної комунікації в мережах "Інтернет поля битви" (IoBT).

Зі швидким розвитком радіотехнологій зростає попит на ресурси спектру, що створює додаткове навантаження на його обмежену доступність. У зв’язку зі збільшенням кількості потенційних зловмисників, які намагаються використовувати спектр несанкціоновано, критично важливим стає швидке виявлення таких вторгнень. У роботі розроблено систему глибокого навчання для виявлення аномалій, здатну ефективно виявляти вторгнення в спектр.

Пропоновані системи використовують метод м'якої кореляції Хіршфельда-Гебелеїна-Реньї (HGR) для виділення важливих ознак із багатомодальних, великовимірних і статистично корельованих спостережень. Для демонстрації можливостей системи було змодельовано відеогру про поле битви, в якій запропонована система використовувалася для відновлення станів і позицій ворожих космічних кораблів. Аналогічно, розроблена система аномалій забезпечила високу продуктивність у виявленні порушень у спектрі сигналів Wi-Fi. Результати експериментів свідчать, що розроблена система машинного навчання здатна точно відстежувати стани та позиції ворогів у реальному часі, навіть за умов невизначеності щодо фонової інформації. Система виявлення аномалій також показала високі результати, перевищуючи ефективність аналогічних підходів у широкому діапазоні

співвідношень сигнал/шум (SNR), досягаючи високого рівня правильних спрацьовувань при низькому рівні хибнопозитивних результатів.

У рамках дослідження розглянуто два різні підходи до застосування H-Score: було запропоновано фреймворк глибокого навчання для вилучення малорозмірної важливої інформації з імітованої мережі IoBT, а також фреймворк на основі теорії інформації для виявлення аномалій у бездротових мережах. Пропонована система обробки відеоінформації на основі глибокого навчання виділяє малорозмірні релевантні характеристики з безперервних відеокадрів, зібраних у мережах IoBT. Ці функції забезпечують точне та своєчасне інформування про події, пригнічуючи фонові дані, що сприяє семантичному відеозв’язку в мережах IoBT з обмеженою пропускною здатністю.

Для підтвердження концепції запропонований фреймворк було протестовано на відеосимуляторі бою, де система досягла середньої точності визначення станів ворожих космічних кораблів на рівні 90% у сценаріях з видимим та невидимим фоном, ефективно відстежуючи положення 20 ворожих об'єктів. Таким чином, реалізовані підходи підтвердили свою ефективність для контролю контекстів, що сприяє підвищенню якості та безпеки комунікаційних систем.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Takuya Akiba, Shotaro Sano, Toshihiko Yanase, Takeru Ohta, and Masanori Koyama. Optuna: A next-generation hyperparameter optimization framework, 2019. URL https://arxiv.org/abs/1907.10902.
2. Ian F. Akyildiz, Ahan Kak, and Shuai Nie. 6g and beyond: The future of wireless communications systems, 2020.
3. Amin Azari, Petar Popovski, Guowang Miao, and Cedomir Stefanovic. Grant-free radio access for short-packet communications over 5g networks. In GLOBECOM 2017 – 2017 IEEE Global Communications Conference, pages 1–7, 2017. doi: 10.1109/GLOCOM. 2017.8255054.
4. Jie Bao, Prithwish Basu, Mike Dean, Craig Partridge, Ananthram Swami, Will Leland, and James A. Hendler. Towards a theory of semantic communication. 2011 IEEE Network Science Workshop, pages 110–117, 2011.
5. Aniqua Baset, Christopher Becker, Kurt Derr, Samuel Ramirez, Sneha Kasera, and Aditya Bhaskara. Towards wireless environment cognizance through incremental learning. In 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pages 256–264, 2019. doi: 10.1109/MASS.2019.00038.
6. Eirina Bourtsoulatze, David Burth Kurka, and Deniz Gündüz. Deep joint sourcechannel coding for wireless image transmission. In ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 4774–4778, 2019. doi: 10.1109/ICASSP.2019.8683463.
7. Aniello Castiglione, Kim-Kwang Raymond Choo, Michele Nappi, and Stefano Ricciardi. Context aware ubiquitous biometrics in edge of military things. IEEE Cloud Computing, 4(6):16–20, 2017. doi: 10.1109/MCC.2018.1081072.

8. Xianfu Chen, Celimuge Wu, Tao Chen, Honggang Zhang, Zhi Liu, Yan Zhang, and Mehdi Bennis. Age of information aware radio resource management in vehicular networks: A proactive deep reinforcement learning perspective. IEEE Transactions on Wireless Communications, 19(4):2268–2281, 2020. doi: 10.1109/TWC.2019.2963667.
9. Biplav Choudhury, Vijay K. Shah, Avik Dayal, and Jeffrey H. Reed. Joint age of information and self risk assessment for safer 802.11p based v2v networks. In IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, pages 1–10, 2021. doi: 10.1109/INFOCOM42981.2021.
10. Thomas Delteil, Edouard Belval, Lei Chen, Luis Goncalves, and Vijay Mahadevan. Matrix – modality-aware transformer for information extraction, 2022. URL https://arxiv.org/abs/2205.08094.
11. Mohammad Karimzadeh Farshbafan, Walid Saad, and Merouane Debbah. Curriculum learning for goal-oriented semantic communications with a common language, 2022. URL https://arxiv.org/abs/2204.10429.
12. Qingsong Feng, Zheng Dou, Chunmei Li, and Guangzhen Si. Anomaly detection of spectrum in wireless communication via deep autoencoder. In James J. (Jong Hyuk) Park, Yi Pan, Gangman Yi, and Vincenzo Loia, editors, Advances in Computer Science and Ubiquitous Computing, pages 259–265, Singapore, 2017. Springer Singapore. ISBN 978-981-10-3023-9.
13. Yifan Gu, He Chen, Yonghui Li, and Branka Vucetic. Ultra-reliable short-packet communications: Half-duplex or full-duplex relaying? IEEE Wireless Communications Letters, 7(3):348–351, 2018. doi: 10.1109/LWC.2017.2777857.
14. Ali Hatamizadeh, Hongxu Yin, Jan Kautz, and Pavlo Molchanov. Global context vision transformers, 2022. URL https://arxiv.org/abs/2206.09959.
15. Adam Hayes. Anomaly, 2021. URL https://www.investopedia.com/terms/a/anomaly.asp.
16. Wei Honghao, Jia Yunfeng, and Wang Lei. Spectrum anomalies autonomous detection in cognitive radio using hidden markov models. In

2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pages 388–392, 2015. doi: 10.1109/IAEAC.2015.7428581.

17. H. S. Hota, Richa Handa, and Akhilesh Kumar Shrivas. Time series data prediction using sliding window based rbf neural network, 2017.
18. Yulin Hu, Anke Schmeink, and James Gross. Blocklength-limited performance of relaying under quasi-static rayleigh channels. IEEE Transactions on Wireless Communications, 15(7):4548–4558, 2016. doi: 10.1109/TWC.2016.2542245.
19. Shao-Lun Huang, Lin Zhang, and Lizhong Zheng. An information-theoretic approach to unsupervised feature selection for high-dimensional data. In 2017 IEEE Information Theory Workshop (ITW), pages 434–438, 2017. doi: 10.1109/ITW.2017.8277927.
20. Shao-Lun Huang, Anuran Makur, Gregory W. Wornell, and Lizhong Zheng. On universal features for high-dimensional learning and inference, 2019. URL https://arxiv.org/abs/1911.09105.
21. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
22. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
23. Dey, A. K., & Abowd, G. D. (2000). Towards a Better Understanding of Context and Context-Awareness. Proceedings of CHI.
24. Abowd, G. D., & Mynatt, E. D. (2000). Charting Past, Present, and Future Research in Ubiquitous Computing. ACM Transactions on Computer-Human Interaction, 7(1), 29–58.
25. Schilit, B. N., Adams, N., & Want, R. (1994). Context-Aware Computing Applications. In Proceedings of the Workshop on Mobile Computing Systems and Applications (WMCSA).
26. Gu, T., Pung, H. K., & Zhang, D. Q. (2005). A Middleware for Building Context-Aware Mobile Services. In Proceedings of IEEE Vehicular Technology Conference.

27. Chen, G., & Kotz, D. (2000). A Survey of Context-Aware Mobile Computing Research. Dartmouth Computer Science Technical Report TR2000-381.
28. Baltrunas, L., Ludwig, B., Peer, S., & Ricci, F. (2011). Context-Aware Places of Interest Recommendations for Mobile Users. In Proceedings of the 5th ACM Conference on Recommender Systems.
29. Bettini, C., Brdiczka, O., Henricksen, K., & Indulska, J. (2010). A Survey of Context Modelling and Reasoning Techniques. Pervasive and Mobile Computing, 6(2), 161-180.
30. Chahuara, P., Portet, F., & Vacher, M. (2016). Context-Aware Decision Making under Uncertainty for Voice-Based Control of Smart Home Environments. Expert Systems with Applications, 75, 63-79.
31. Ye, J., Dobson, S., & McKeever, S. (2012). Situation Identification Techniques in Pervasive Computing: A Review. Pervasive and Mobile Computing, 8(1), 36-66.
32. Van Kasteren, T., Englebienne, G., & Kröse, B. (2011). An Activity Monitoring System for Elderly Care Using Generative and Discriminative Models. Personal and Ubiquitous Computing, 14(6), 489-498.
33. Varshney, L. R., & Chang, K. (2017). Context-Aware Communication: Advances and Challenges. IEEE Communications Magazine, 55(10), 144-150.
34. Akl, A., & Valaee, S. (2011). Accelerometer-Based Gesture Recognition via Dynamic-Time Warping, Affinity Propagation, and Compressive Sensing. In Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).
35. Zheng, Y., & Zhou, X. (2011). Computing with Spatial Trajectories. Springer.
36. Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2013). Efficient Estimation of Word Representations in Vector Space. arXiv preprint arXiv:1301.3781.

37. Liu, L., & Zhang, M. (2018). Context-Aware Crowdsourcing for IoT-Based Mobile Social Networks. IEEE Access, 6, 16170-16182.
38. Ngu, A. H., Gutierrez, M., Metsis, V., & Fernandez, C. (2016). IoT Middleware for Context-Aware Smart Healthcare Applications. In Proceedings of IEEE International Conference on Mobile Cloud Computing.
39. Lan, K. C., Tsai, C. T., & Tseng, C. (2013). Context-Aware Hand Gesture Recognition Using a Kinect Sensor. Sensors, 13(10), 13737-13752.
40. Calatroni, A., Roggen, D., & Tröster, G. (2010). Context-Aware Activity Recognition: Enabling Techniques, Application Challenges, and Performance Evaluation. In Proceedings of ACM International Workshop on Situation Recognition and Medical Data Analysis.
41. Kumar, S., & Srivastava, J. (2013). Context-Based Learning and Adaptation in Social Media Environments. In Proceedings of IEEE International Conference on Data Mining (ICDM).
42. Abowd, G. D., & Dey, A. K. (2001). Towards a Better Understanding of Context and Context-Awareness. Lecture Notes in Computer Science, 1707, 304-307.
43. Ge, M., Ricci, F., & Massimo, D. (2015). Context-Aware Recommendations Based on User's Contextual Behavior. In Proceedings of the 23rd Conference on User Modeling, Adaptation and Personalization.
44. Rashidi, P., & Cook, D. J. (2010). Activity Knowledge Transfer in Smart Environments. Pervasive and Mobile Computing, 6(4), 393-407.
45. Ziebart, B. D., Maas, A. L., Dey, A. K., & Bagnell, J. A. (2008). Navigate Like a Cabbie: Probabilistic Reasoning from Observed Context-Aware Behavior. In Proceedings of the 10th International Conference on Ubiquitous Computing (UbiComp).
46. Bettini, C., & Riboni, D. (2015). Privacy Protection in Pervasive Systems: State of the Art and Technical Challenges. Pervasive and Mobile Computing, 17, 159-174.

47. Hoang, D. B., & Chen, L. (2010). Mobile Cloud for Assistive Healthcare (MoCAsH). Future Generation Computer Systems, 29(2), 131-139.
48. Qi, H., & Gani, A. (2012). Research on Mobile Cloud Computing: Review, Trend, and Perspectives. In Proceedings of IEEE International Conference on Digital Information Management.
49. Cheng, X., Li, P., & Liu, M. (2015). Mobile Cloud Computing and the Internet of Things: Challenges and Applications. Journal of Network and Computer Applications, 60, 12-25.
50. Seneviratne, S., & Seneviratne, A. (2014). Context-Aware Mobile Computing: A Survey on Context-Aware Computing, Mobile Networks, and Big Data Analytics. ACM Computing Surveys, 46(4), 1-36.
51. Zhan, Y., Zong, Z., & Yang, X. (2015). Energy-Efficient Cloud Workflow Scheduling Based on Decision Making under Uncertainty. IEEE Transactions on Cloud Computing, 3(1), 17-29.
52. Wang, S., & Chen, X. (2012). Cloud Computing for Mobile Users: Can Offloading Computation Save Energy? IEEE Communications Magazine, 49(4), 68-73.
53. Zhang, Y., & Wang, W. (2015). Context-Aware Mobile Cloud Computing: A Survey. Wireless Communications and Mobile Computing, 17(4), 1-11.
54. Rao, S. S., & Kartik, B. (2020). Machine Learning in Communication Networks: Future Directions and Challenges. Journal of Communications and Networks, 22(3), 159-167.