Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод виявлення аномалій в автоматизованій системі локалізації транспортного засобу

(тема)

Виконав:
здобувач 2 року навчання,
групи СПм-23-3
Іван ХАРАХАЙЧУК
(власне ім'я, прізвище)

Спеціальність
123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма
Системне програмування
(повна назва освітньої програми)

Керівник: проф. Алєксандр ТОРБА
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Харахайчуку Івану Анатолійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод виявлення аномалій в автоматизованій системі локалізації транспортного засобу

затверджена наказом по університету від "21" квітня 2025 р. № 296 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 16 червня 2025 р.

3. Вхідні дані до роботи 1) транспортні засоби – довільні (підключені та автономні);
2) набір аномалій виявляється на основі проведеного аналізу;
3) використання реальних або симульованих даних для експериментального дослідження.

4. Перелік питань, що потрібно опрацювати у роботі
Аналіз задачі локалізації транспортних засобів
Основні технології локалізації транспортних засобів
Методи розпізнавання аномалій
Розробка методу
Експерименти та результати
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

Слайд-презентація – 14 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Аналіз задачі локалізації транспортних засобів	22.04.25-29.04.25	
	(ТЗ)		
2	Основні технології локалізації ТЗ	30.04.25-05.05.25	
3	Методи розпізнавання аномалій	06.05.25-09.05.25	
4	Розробка методу	10.05.25-21.05.25	
5	Проведення експериментів	22.05.25-02.06.25	
6	Оформлення матеріалів кваліфікаційної роботи	03.06.25-05.06.25	
7	Подання кваліфікаційної роботи керівникові та	06.06.25-09.06.25	
	її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	10.06.25-12.06.25	
	вання		

Дата видачі завдання " 21 " квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ проф. Алєксандр ТОРБА
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 65 с., 7 рис., 3 табл., 1 дод., 72 джерела.

ВИЯВЛЕННЯ АНОМАЛІЙ, ГАУСІВСЬКА ЗМІШАНА МОДЕЛЬ, КІБЕРБЕЗПЕКА, ФАЛЬСИФІКОВАНІ ТРАЄКТОРІЇ, CAV, LSTM.

Метою кваліфікаційної роботи є розробка методу виявлення аномалій в автоматизованій системі локалізації транспортного засобу.

Запропоновано модель GMLM для виявлення аномалій, яка дозволяє ідентифікувати аномальні траєкторії CAV у режимі реального часу. GMLM складається з двох основних компонентів: LSTM-автокодувальника та декодера, які формують низькорівневі представлення початкових зразків. Запропонований метод забезпечує підвищення точності виявлення на 3% та precision на 6,4% порівняно з сучасними методами, що підтверджує ефективність запропонованого алгоритму.

Важливим наступним кроком є валідація продуктивності моделі на різноманітних реальних даних автономних транспортних засобів. Розширення оцінювання на різноманітні реалістичні сценарії дозволить краще продемонструвати універсальність підходу. Подальші дослідження також передбачають удосконалення можливостей моделі щодо розрізнення різних типів аномалій, таких як короткочасні імпульси, шум, поступовий дрейф тощо.

ABSTRACT

Master’s thesis: 65 pages, 7 figures, 3 tables, 1 appendices, 72 sources.

ANOMALY DETECTION, CAV, CYBERSECURITY, FALSIFIED TRAJECTORIES, GAUSSIAN MIXTURE MODEL, LSTM.

The objective of this qualification work is to develop a method for anomaly detection in an automated vehicle localization system.

A GMLM-based anomaly detection model is proposed, which enables the identification of anomalous CAV (Connected and Autonomous Vehicle) trajectories in real time. The GMLM consists of two main components: an LSTM autoencoder and a decoder, which form low-level representations of the initial samples. The proposed method provides a 3% improvement in detection accuracy and a 6.4% increase in precision compared to state-of-the-art methods, confirming the effectiveness of the proposed algorithm.

An important next step is the validation of the model’s performance on diverse real-world data from autonomous vehicles. Extending the evaluation to various realistic scenarios will further demonstrate the versatility of the approach. Future research also involves enhancing the model's ability to distinguish between different types of anomalies, such as short-term impulses, noise, and gradual drift.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ADAS – система допомоги водію (англ., Advanced Driver-Assistance Systems)

AEDF – адаптивний розширений фільтр Калмана (англ., Adaptive Extended Kalman Filter)

ATM – активне керування дорожнім рухом (англ., Active Traffic Management)

AV – автономний транспортний засіб (англ., Autonomous Vehicle)

CACC – кооперативний адаптивний круїз-контроль (англ., Cooperative Adaptive Cruise Control)

CAN – мережа контролерів (англ., Controller Area Network)

CARMA – платформа кооперативних автоматизованих мобільних дослідницьких застосувань (англ., Cooperative Automated Research Mobility Applications)

CAVs – підключені й автономні транспортні засоби (англ., Connected and Autonomous Vehicles)

CNN – згорткова нейронна мережа (англ., Convolutional Neural Network)

DAGMM – глибокий автоенкодер із ґауссовою змішаною моделлю (англ., Deep Autoencoder Gaussian Mixture Model)

EKF – розширений фільтр Калмана (англ., Extended Kalman Filter)

FV – ведений автомобіль (англ., Following Vehicle)

GAN – генеративна змагальна мережа (англ., Generative Adversarial Network)

GMLM – автокодувальник на основі довготривалої короткочасної пам’яті з гаусівською сумішшю

GMM – модель змішування ґауссіанів (англ., Gaussian Mixture Model)

GNSS – глобальні навігаційні супутникові системи (англ., Global

Navigation Satellite Systems)

IMU – інерціальна вимірювальна одиниця (англ., Inertial Measurement Unit)

IoT – інтернет речей (англ., Internet of Things)

IRL – інверсне навчання з підкріпленням (англ., Inverse Reinforcement Learning)

LiDAR – лідар (англ., Light Detection and Ranging)

LSTM – довготривала короткочасна пам’ять (англ., Long Short-Term Memory)

LSTM-AE – автоенкодер на основі LSTM (англ., LSTM Autoencoder)

LV – ведучий автомобіль (англ., Lead Vehicle)

NLP – обробка природної мови (англ., Natural Language Processing)

OBD – система бортової діагностики (англ., On-Board Diagnostics)

RNN – рекурентна нейронна мережа (англ., Recurrent Neural Network)

SVM – метод опорних векторів (англ., Support Vector Machine)

V2I – комунікація «транспортний засіб – інфраструктура» (англ., Vehicle-to-Infrastructure, V2I)

V2N – комунікація «транспортний засіб – мережа» (англ., Vehicle-to-Network, V2N)

V2P – комунікація «транспортний засіб – пішохід» (англ., Vehicle-to-Pedestrian, V2P)

V2V – комунікація «транспортний засіб – транспортний засіб» (англ., Vehicle-to-Vehicle, V2V)

V2X – комунікація «транспортний засіб – усе» (англ., Vehicle-to-Everything, V2X)

ВСТУП

Технологія підключених і автономних транспортних засобів (Connected and Autonomous Vehicles, CAVs) має потенціал для трансформації транспортної системи. Незважаючи на численні переваги цих нових технологій, їх впровадження супроводжується суттєвими викликами, пов’язаними з безпекою, захистом та конфіденційністю. Аномалії у даних датчиків, викликані помилками або кібернападами, можуть призводити до серйозних аварій.

Для вирішення цієї проблеми у дослідженні запропоновано інноваційний алгоритм виявлення аномалій LSTM-автокодувальник з гаусівською сумішшю. Запропонована модель забезпечує виявлення аномальних траєкторій CAV у реальному часі з використанням комунікаційних можливостей сенсорів CAV.

LSTM-автокодувальник застосовується для генерації низькорівневих представлень та обчислення похибок реконструкції для кожної вхідної точки даних, у той час як гаусівська змішана модель (GMM) використовується завдяки своїм перевагам у оцінюванні густини розподілу. Запропонована модель була одночасно оптимізована як для LSTM-автокодувальника, так і для GMM. У дослідженні використано реальні дані CAV, отримані в рамках експерименту з формування транспортного «потяга» для системи Cooperative Automated Research Mobility Applications (CAR-MA).

Результати експерименту показують, що підхід GMLM підвищує точність виявлення аномалій на 3% та прецизійність на 6,4% порівняно з сучасними методами, що свідчить про суттєве покращення у цій сфері.

Дане дослідження має такі наукові результати:

1. Використано дані реального експерименту з рухом автоколони CAV для моделювання аномалій та виявлення фальсифікованої активності у складах транспортних засобів, що включають як провідні, так і ведені

автомобілі.

2. Розроблено алгоритм GMLM для виявлення аномальних траєкторій CAV у реальному часі. Ця модель враховує часову динаміку траєкторій CAV, що часто ігнорується у попередніх дослідженнях, і забезпечує підвищення точності виявлення у порівнянні з існуючими підходами.

3. GMLM використовує двоетапну стратегію декомпозиції і оцінки щільності, які оптимізуються одночасно. Це дозволяє уникати локальних субоптимальних рішень і додатково знижувати похибки реконструкції.

4. Досліджено різні типи кібернападів у системах CAV і проведено їхню валідацію із застосуванням запропонованої моделі. Експерименти підтвердили ефективність моделі для виявлення атак, що впливають на функціонування CAV.

Робота містить:

- огляд сучасних досліджень і літератури для формування чіткого уявлення про предмет;
- організацію експерименту та опис даних;
- емуляцію аномалій;
- формалізацію і вдосконалення моделі, її топологію;
- аналіз експериментів та підсумкові висновки.

1 АНАЛІЗ ПРОБЛЕМНОЇ ОБЛАСТІ

1.1 Задача локалізації транспортних засобів

Локалізація транспортних засобів – це фундаментальна задача для забезпечення безпеки, ефективності та автоматизації руху у сучасних транспортних системах. Від точності визначення місцезнаходження транспортного засобу залежить якість роботи навігаційних систем, коректність роботи допоміжних систем безпеки (ADAS), а також функціонування автономних транспортних засобів (CAV) і систем керування трафіком у Smart City [1-3].

Таблиця 1.1 – Основні фактори, що впливають на якість локалізації транспортних засобів

Фактор	Приклад впливу	Джерело
Міське середовище	Затінення супутникового сигналу будівлями, «каньйони»	[1], [5]
Погодні умови	Дощ, сніг, туман впливають на LiDAR, камери	[6]
Множинні траєкторії	Щільний трафік, близьке розташування інших ТЗ	[2]
Сенсорні збої	Дрейф IMU, шум у GPS	[3], [7]
Кіберзагрози	GPS spoofing, атаковані V2X-повідомлення	[8], [9]
Мережеві затримки	Запізнення/втрата V2X-даних	[4], [9]

З розвитком концепції Інтернету речей (IoT) та впровадженням V2X-комунікацій (Vehicle-to-Everything) локалізація стала ще більш критичною для координації транспортних потоків, попередження заторів, оптимізації маршрутів та запобігання аварійним ситуаціям [4]. Однак досягнення високої

точності та надійності залишається складним завданням через вплив численних факторів – як технічних, так і природних (таблиця 1.1).

Розвиток автономних систем висуває нові вимоги до локалізації – не лише в плані точності, а й у контексті робастності до збоїв, здатності працювати у складних умовах (тунелі, підземні паркінги, міські каньйони) та стійкості до кібератак [10, 11].

Сучасна наукова та галузева спільнота постійно працює над підвищенням надійності локалізації – зокрема, через впровадження технологій багатосенсорного аналізу, використання картографічних даних високої точності, застосування методів машинного навчання для обробки аномалій та оптимізації роботи в умовах поганої видимості або сигналу [12].

1.2 Основні технології локалізації транспортних засобів

Локалізація транспортних засобів є ключовим аспектом для реалізації сучасних систем автоматизованого та автономного водіння. Вона базується на використанні комплексу технологій, які дозволяють визначати місцезнаходження, швидкість і орієнтацію транспортного засобу у просторі. Нижче розглянуто основні підходи та технічні засоби локалізації.

1.2.1 Глобальні навігаційні супутникові системи

Глобальні навігаційні супутникові системи (GNSS), до складу яких входять GPS (США), ГЛОНАСС (РФ), BeiDou (КНР), Galileo (ЄС), забезпечують визначення координат об'єкта з високою точністю у глобальному масштабі. Принцип роботи ґрунтується на прийомі сигналів від кількох супутників і розрахунку положення шляхом тріангуляції [13]. GNSS є основним джерелом позиціонування для більшості транспортних засобів, забезпечуючи точність до кількох метрів у відкритих місцевостях. Інтеграція декількох систем дозволяє підвищити надійність та стійкість до локальних

відмов окремих супутникових систем.

1.2.2 Інерціальні вимірювальні одиниці (IMU)

Інерціальні вимірювальні одиниці (IMU) складаються з акселерометрів, гіроскопів і іноді магнітометрів, що дозволяє вимірювати прискорення, кутову швидкість та орієнтацію транспортного засобу. IMU відіграють важливу роль у локалізації, особливо в умовах відсутності супутникового сигналу, наприклад, у тунелях або міських каньйонах. Інтеграція IMU із супутниковими системами дозволяє згладжувати неточності та забезпечувати безперервність визначення положення [14].

1.2.3 LiDAR, радар, ультразвукові сенсори

LiDAR (Light Detection and Ranging) – це технологія, що використовує лазерне сканування для отримання тривимірної карти навколишнього середовища. Радар (Radio Detection and Ranging) застосовує радіохвилі для виявлення об'єктів і вимірювання відстані до них. Ультразвукові сенсори використовуються переважно для близьких відстаней, наприклад, під час паркування. Поєднання LiDAR, радарів та ультразвукових сенсорів дозволяє створити комплексну картину навколишнього світу, що істотно підвищує точність та надійність локалізації, особливо в складних або динамічних умовах [15, 16].

1.2.4 Камери та комп’ютерний зір

Використання камер високої роздільної здатності у поєднанні з алгоритмами комп’ютерного зору дає змогу ідентифікувати дорожні знаки, розмітку, пішоходів та інші об'єкти. Методи обробки зображень та машинного навчання використовуються для визначення положення

транспортного засобу відносно об'єктів довкілля, а також для розпізнавання та відслідковування траєкторій руху [17]. Комп’ютерний зір дозволяє підвищити точність локалізації, особливо в умовах міста, де GNSS може працювати нестабільно.

1.2.5 V2X-комунікації та мережеві підходи

Технології V2X (vehicle-to-everything) включають обмін інформацією між транспортними засобами (V2V), між транспортними засобами та інфраструктурою (V2I), а також із пішоходами (V2P) та мережею (V2N). Такі комунікації дають змогу передавати та отримувати дані щодо позиції, швидкості, дорожньої ситуації тощо, що додатково підвищує точність та безпеку локалізації [18]. Мережеві підходи сприяють більш гнучкій та адаптивній побудові систем локалізації, дозволяючи ефективно інтегрувати різноманітні джерела даних.

1.3 Проблеми та обмеження основних технологій локалізації транспортних засобів

Попри суттєвий прогрес у розвитку технологій локалізації, їх застосування супроводжується низкою технічних та експлуатаційних обмежень.

Вразливість до глушіння та спуфінгу сигналів GPS/GNSS. Супутникові системи позиціонування є чутливими до навмисного або випадкового глушіння (jamming) та спуфінгу (підміни сигналу). Це може призвести до втрати зв’язку із супутниками або до невірного визначення місця розташування транспортного засобу, що є серйозною загрозою для безпеки автономних систем [8]. Проблема посилюється в умовах міської забудови, де відбиваються сигнали або їх перекривають високі будівлі.

Накопичення помилок у IMU. Інерціальні вимірювальні одиниці

схильні до накопичення похибок, особливо при тривалому автономному функціонуванні без корекції від зовнішніх джерел. Навіть невеликі початкові відхилення акселерометрів та гіроскопів з часом призводять до значних помилок у визначенні положення, що потребує регулярного калібрування або корекції даних [19].

Вплив погодних умов та перешкод на LiDAR, камери, радари. Оптичні та радіолокаційні сенсори є чутливими до атмосферних явищ. Дощ, туман, сніг або бруд на сенсорах можуть значно знижувати точність та достовірність даних. Наприклад, LiDAR і камери мають обмежену ефективність при недостатньому освітленні чи сильній засвітці, а радари іноді неправильно ідентифікують об’єкти через складні відбивальні властивості [20, 21].

Неточності та затримки V2X-комунікацій. V2X-комунікації залежать від стабільності мережі, ширини пропускного каналу, затримок у передачі та обробці даних. В умовах перевантаженості мережі, втрат пакетів або атаки на мережу можливі збої, які негативно впливають на оперативність і точність локалізації. Відсутність єдиного стандарту для взаємодії різних виробників транспортних засобів та інфраструктури також ускладнює впровадження V2X-технологій [22].

1.4 Задачі виявлення аномалій в локалізації транспортних засобів

Технології підключених і автономних транспортних засобів (Connected and Autonomous Vehicles, CAVs) мають потенціал трансформувати транспортну систему. CAVs здатні безперервно обмінюватися інформацією, такою як швидкість руху, місцезнаходження, прискорення або уповільнення, з навколишніми транспортними засобами чи інфраструктурою завдяки використанню комунікацій Vehicle-to-Vehicle (V2V) та Vehicle-to-Infrastructure (V2I). Очікується, що ці технології сприятимуть зниженню заторів, підвищенню ефективності дорожнього руху та його безпеки. Попри численні переваги, безпека, захист інформації та конфіденційність

залишаються основними проблемами для реального впровадження таких систем [23].

CAVs значною мірою залежать від даних, що надходять із сенсорів. Аномальні показники сенсорів, викликані помилками чи кібернападами, можуть мати серйозні наслідки, включаючи аварії та затримки руху. У системах CAV можливі різні типи внутрішніх та зовнішніх кібернападів. Згідно з проведеними дослідженнями [24], у середовищі CAV виділяють три основних типи кібернападів:

- атаки на рівні застосунків у V2V-комунікації, наприклад, підробка повідомлень, атака на відключення та атака-відповідь;
- атаки на рівні мережі у V2I-комунікації, наприклад, підміна, атака відмови у наданні послуг і радіоглушіння;
- атаки, що здійснюються шляхом фізичного доступу до самих транспортних засобів.

Аналіз атак різних типів подано в декількох дослідженнях [24-26].

У застосуванні CAV кібербезпека є однією з найважливіших проблем. Загроза кібернападів на CAV становить серйозний ризик не лише для пасажирів цих транспортних засобів, але й для пішоходів, велосипедистів та інших учасників дорожнього руху, які з ними взаємодіють. Такі напади можуть призвести до численних проблем із безпекою – від втрати контролю над транспортним засобом до порушення конфіденційності даних, що підкреслює актуальність розробки надійних методів виявлення аномалій.

Для ефективної протидії цим викликам необхідно розробляти сучасні системи виявлення аномалій, здатні ідентифікувати та усувати загрози в режимі реального часу. Такі системи повинні постійно аналізувати поведінкові патерни транспортних засобів та виявляти відхилення, що можуть свідчити про кібернапад або збій системи.

Більшість існуючих досліджень зосереджені на підвищенні безпеки комунікаційних каналів або сенсорів у мережі CAV з метою запобігання атакам типу першого типу [27-29]. Однак атаки другого типу є значно більш

небезпечними для системи. Наприклад, зловмисник може отримати доступ до таких точок атаки та взяти під контроль CAV, маніпулюючи рекомендаціями щодо зміни смуги V2I так, що цільовий транспортний засіб почне прискорюватися, коли інший автомобіль приєднується до тієї ж смуги попереду нього. Подібні атаки можуть порушувати основні функції CAV, зокрема прискорення, швидкість руху, позиціонування, гальмування, зміну смуг та регулювання потоків на з'їздах і в'їздах. Це не лише ставить під загрозу самі CAV, а й спричиняє додаткові затори та аварії.

Інші дослідники [30] запропонували нелінійну схему керування для компенсації динамічної невизначеності автоколон. Методика може бути використана для повернення контролю над атакованими транспортними засобами та підтримання стабільності мережі. Проте цей підхід не дозволяє керувати великими відхиленнями та ґрунтується на певних припущеннях щодо невизначеностей.

Деякі дослідники використовують дані з CAV, керованих людиною, для розробки алгоритмів виявлення аномалій на основі машинного навчання, ігноруючи часові зв'язки між аномальними траєкторіями. Ігнорування таких кореляцій може призвести до моделей, неспроможних розпізнавати складні, часово-залежні ситуації, що знижує їхню ефективність щодо виявлення потенційних загроз.

Тому розробка ефективного алгоритму виявлення аномалій для CAV є вкрай важливою для своєчасного виявлення аномальної поведінки в реальному часі, що дозволить запобігти тяжким наслідкам кібернападів або сенсорних аномалій.

Дане дослідження усуває зазначені обмеження та фокусується на виявленні атак шляхом використання реальних даних CAV, отриманих в експерименті з рухом автоколони. У цій роботі запропоновано модель виявлення аномалій – автокодувальник на основі довготривалої короткочасної пам'яті з гаусівською сумішшю (GMLM) для ідентифікації аномальної поведінки в автоколоні CAV. LSTM-автокодувальник

застосовується для отримання низькорівневих представлень та обчислення похибки реконструкції для кожної точки вхідних даних. Для задач оцінки щільності використовується гаусівська змішана модель (GMM). Запропонована модель одночасно оптимізується як для LSTM-автокодувальника, так і для GMM.

Загалом існує два типи поведінки/траєкторій CAV:

- нормальне функціонування з використанням даних сенсорів транспортного засобу;
- фальсифіковані траєкторії, що виникають внаслідок кібернападів (у цьому дослідженні розглядаються різні типи таких атак).

Для дослідження застосовано реальні дані CAV, отримані в ході експерименту з руху автоколони для платформи Cooperative Automated Research Mobility Applications (CARMA). Деталі експерименту та даних наведені далі.

1.5 Огляд сучасних досліджень

Існує низка сучасних досліджень, у яких для виявлення аномалій застосовуються моделі глибокого навчання. Більшість із них спрямовані на виявлення фальсифікованих траєкторій автономних транспортних засобів (AV) в офлайн-режимі. Тобто після збору даних про рух AV (нормальні та фальсифіковані траєкторії) використовуються різні методи контрольованого та неконтрольованого навчання для класифікації траєкторій.

В роботі [25] запропоновано багаторівневий механізм уваги з моделлю CNN на основі довготривалої короткочасної пам’яті (LSTM). Запропонований підхід дозволив підвищити F-метрику до 3,24%.

В іншій роботі [26] запропоновано модель вбудовування траєкторій, використавши підходи зі сфери обробки природної мови (NLP). Модель генерувала векторні представлення траєкторій CAV для обчислення схожості між ними. Спочатку нейронна мережа навчалася для отримання векторних

представлень траєкторій, а потім за допомогою ієрархічного алгоритму кластеризації оцінювалася матриця відстаней між парами траєкторій та ідентифікувалися фальсифіковані траєкторії. Запропонований метод забезпечує високий рівень виявлення аномалій (>97%).

В роботі [31] автори розробили згорткову нейронну мережу (CNN) з фільтрацією Калмана для виявлення та ідентифікації аномальної поведінки CAV. Результати їхнього експерименту показали, що запропонована модель забезпечує високу точність, чутливість і F1-метрику.

Існує пропозиція алгоритму виявлення неправомірної поведінки (MDA) [32], використовуючи дані із змодельованого середовища в SUMO. Дослідники згенерували скомпрометовані дані за допомогою шести різних методів атаки й застосували методи машинного навчання для виявлення неправомірної поведінки.

Для виявлення аномалій можна застосовувати метод адаптивного розширеного фільтра Калмана (AEDF) [33]. Це дослідження було зосереджене на русі автоколони, а не окремих транспортних засобів. Для виявлення аномалій вони використовували дані про швидкість і розташування навколишнього транспорту цільового автомобіля.

В роботі [34] було промодельовано атаки на колони з кооперативним адаптивним круїз-контролем з метою аналізу впливу на дорожній рух і безпеку. Було встановлено, що зростання частоти та інтенсивності атак на цільові транспортні засоби негативно впливає на трафік і підвищує ризик зіткнень.

В іншій роботі [35] автори проаналізували ефективність різних алгоритмів керування світлофорами на основі зворотного тиску (delay-based, queue-based) в умовах кібернападів. Було виявлено, що delay-based алгоритми вразливі до атак із підміною часу прибуття транспортного засобу.

В роботі [36] автори досліджували вплив кібернападів на колону з десяти автомобілів із кооперативним адаптивним круїз-контролем. Вони спостерігали значні зміни в профілях прискорення та порушення стабільності

автоколони.

Інші дослідники [37] запропонували алгоритм виявлення неправомірної поведінки шляхом відстеження сигналів транспортного засобу та перевірки індустріального консенсусу для придорожніх пристроїв (RSU) у середовищі V2X (Vehicle-to-Everything).

Можна проаналізувати підміну координат із застосуванням правдоподібнісних перевірок за допомогою k-нейронної мережі та SVM для класифікації неправомірної поведінки на основі еталонного датасету неправомірної поведінки транспортних засобів, змодельованого у VEINS [38]. Автори вказаного дослідження відзначили покращення правдоподібнісних перевірок на 20% завдяки запропонованому алгоритму.

Ще одне дослідження [39] аналізувало колону із шести автомобілів з кооперативним адаптивним круїз-контролем (CACC) щодо атак із затримкою у часі, і було встановлено, що алгоритм CACC залишається стабільним за відсутності круїзу або ривків.

В деяких дослідженнях якісно оцінювався рівень кіберризиків. Наприклад [40], було проведено опитування серед співробітників Департаменту транспорту штату Орегон (DOT) з метою оцінки їхньої готовності до впровадження систем CAV. Результати показали, що майже 40% учасників опитування висловили занепокоєння щодо ризиків, пов’язаних із безпекою CAV. Інше дослідження [41] було сфокусовано на ймовірності відмов автономних транспортних засобів у змішаних транспортних потоках. Використовуючи метод аналізу дерев відмов для оцінки ймовірності відмови кожного автономного елементу, автори виявили 14% частку відмов серед компонентів автономних транспортних засобів. Тако слід зазначити комплексний огляд системи V2X [42], де проаналізовано заходи безпеки, стандарти та сучасні стратегії захисту. Автори також визначили наявні недоліки рішень із безпеки та окреслили нерозв’язані проблеми.

За підсумками дослідження виявлення й усунення кібернападів за

допомогою фреймворку CVGuard [43] було відзначено, що цей фреймворк зменшує кількість конфліктів у системі, порівнюючи ситуацію до та після його активації. В іншому дослідженні [44] з використанням мікросимуляції проаналізовано флот із десяти транспортних засобів CACC в умовах кібератак у сценарії з однією смугою. Радіоглушіння було визначено як одну з основних кіберзагроз, що спричиняє коливання швидкості та зіткнення.

Декілька дослідників використовували кількісні підходи для оцінки впливу кібернападів на CAV. Прикладом можна вважати застосування OMNET++ для аналізу десяти транспортних засобів із кооперативним адаптивним круїз-контролем (CACC) у сценарії з однією смугою, зосередившись на наслідках атак радіоглушіння та підміни повідомлень [45]. Під час атак підміни повідомлень зловмисники змінювали налаштування бажаного прискорення, що призводило до зростання нестабільності серед транспортного парку. Аналогічно, у разі радіоглушіння транспортні засоби переходили до режиму адаптивного круїз-контролю, збільшуючи часові інтервали між собою.

Також було досліджено [46] вразливості системи кібербезпеки у каналі зв’язку системи активного керування дорожнім рухом (ATM). За підсумками аналізу створено прототип системи моніторингу загроз, призначеної для відновлення функціонування ATM після кібератак. В роботі [47] автори досліджували вплив кібератак на окремий транспортний засіб та його поздовжню безпеку у складі CAV. Атака тривала короткий проміжок часу. Положення та швидкість ведучих транспортних засобів використовувалися як елементи атаки. Це дало зрозуміти, що навіть незначна кібератака суттєво впливає на профілі прискорення, більше ніж на профілі гальмування дев’яти транспортних засобів.

В роботі [48] запропоновано модель для систем керування автономними транспортними засобами, яка оцінює ризики поточних та очікуваних сценаріїв з метою формування стратегії керування. Такий підхід дозволяє підтримувати рівень ризику у межах мінімально прийнятного

безпечного значення. Зроблено висновок, що підвищення продуктивності та безпеки можливе завдяки комунікації й співпраці між транспортними засобами (V2V).

Ще один колектив дослідників [49] оцінив вплив кібератак на одну автоколону, що рухалася однією смугою, розглядаючи кібератаки як поширення шкідливої інформації. Було виявлено, що такі кібератаки істотно порушують потік транспорту.

У сучасних дослідженнях активно вивчається використання методів машинного навчання та глибоких нейронних мереж, таких як згорткові й рекурентні мережі, для ефективного виділення ознак із часових рядів. Більшість статистичних методів виявлення аномалій стикаються з труднощами при моделюванні волатильності та довгострокових тенденцій у даних часових рядів. Це пояснюється тим, що вони часто базуються на підходах, які краще працюють із простими наборами даних і не здатні врахувати коливання змінних з низькою кореляцією в системі [50-52]. Останніми роками набули великої популярності та використовуються у багатьох сучасних моделях глибокі нейронні мережі.

Запропоновано застосування архітектури Bi-Transformer [53] для одночасного виділення ознак із двох різних вимірів. У моделі реалізовано адаптивний механізм багатоголової уваги, що дає змогу виявляти взаємозв’язки між різними змінними часових рядів. Представлений підхід ґрунтується на сучасних технологіях, зокрема на Transformer-мережах і багатоголовій self-attention, які модифіковано та адаптовано для вирішення задачі виявлення аномалій у багатовимірних часових рядах.

В роботі [54] запропоновано фреймворк, що поєднує розширений фільтр Калмана (EKF) для фільтрації шумів у даних сенсорів та метод опорних векторів (SVM) для ідентифікації атак. Важливо зазначити, що модель EKF враховує різнорідні часові затримки та розширені стани для підвищення точності при стохастичних затримках та похибках моделі. Автори також провели теоретичний аналіз, що пов’язує рівень виявлення

атак із концепцією «псевдо-струнної стабільності», запропонованою для оцінки стабільності автоколони в умовах невизначеності моделі.

Група дослідників [55] запропонувала фреймворк для виявлення аномалій, спрямований на ідентифікацію атак на CAV шляхом моделювання типових шаблонів водіння. У цьому дослідженні використано інверсне навчання з підкріпленням (IRL) для побудови оптимальної політики на основі демонстраційних траєкторій, після чого аномалії виявляються через зіставлення спостережуваної поведінки з передбаченнями політики. Ключовими нововведеннями є застосування IRL з максимальною ентропією для навчання моделі поведінки за обмеженою кількістю траєкторій, а також розробка метрик для визначення відмінностей між прогнозованими та реальними траєкторіями з метою подальшої класифікації атак.

Сучасний стан досліджень у цій сфері має кілька обмежень. По-перше, через відсутність реальних даних CAV більшість робіт використовували дані шини Controller Area Network (CAN) із традиційних транспортних засобів, керованих людиною, для моделювання кібератак. У результаті спостерігається розрив у літературі щодо оцінки кіберризиків і виявлення аномальної поведінки у реальних умовах експлуатації CAV. Крім того, значна частина досліджень застосовує офлайн-моделі для виявлення аномалій, що підкреслює необхідність розвитку онлайн-методів у реальному часі. Існуючі дослідження також характеризуються високими обчислювальними витратами, що ускладнює їх практичне застосування в реальному часі.

По-друге, існуючі підходи часто не диференціюють різні типи атак, зокрема несправності сенсорів CAV. Наприклад, поступовий дрейф сенсора суттєво відрізняється від відмови зі зсувом [31, 33]. Запропонована модель має забезпечувати виявлення різних типів атак.

По-третє, поточні дослідження, що використовують як класичне машинне навчання, так і передові методи глибокого навчання, не враховують часові залежності у фальсифікованих траєкторіях CAV, що може суттєво

впливати на прогнозування аномалій. Дорожні потоки та траєкторії транспортних засобів постійно й динамічно змінюються з часом, тому часові параметри швидкості й положення мають бути враховані у моделі.

2 МЕТОДИ РОЗПІЗНАВАННЯ АНОМАЛІЙ

2.1 Розпізнавання аномалій із використанням LSTM

Архітектура LSTM була запропонована [56] як розв'язання проблеми зникнення градієнта, що притаманна традиційним рекурентним нейронним мережам (RNN) та ускладнює навчання довготривалих залежностей у часових рядах. Зокрема, явище зникнення градієнта полягає у поступовому припиненні оновлення частини вагових коефіцієнтів мережі протягом процесу навчання, що спричиняє втрату впливу попередніх подій на поточний стан. Відтак, модель фокусується переважно на останніх даних, ігноруючи важливу інформацію з минулого, що унеможливлює якісне моделювання довгострокових залежностей.

Механізм роботи LSTM передбачає особливу організацію потоку інформації через структуру внутрішніх вентилів нейрона. Ключову роль відіграє так званий вентиль забування, який забезпечує керування процесом оновлення та видалення інформації із стану комірки, що передається у часовому просторі. Це дозволяє моделювати як коротко-, так і довготривалі залежності у даних. Архітектурна схема LSTM представлена на рисунку 2.1.

На відміну від класичних RNN, у LSTM вихід нейрона /i(t) визначається не лише вхідними значеннями x(t) та попередніми виходами h(t - 1), а й внутрішнім станом комірки z(t), який регулюється системою вентилів. Зокрема, вектор /(t) формується на основі елемента забування, а вектор n(t) – елемента додавання; разом вони здійснюють поступову адаптацію стану комірки, контролюючи механізм пам’яті.

Зворотний зв’язок між цими елементами дозволяє реалізувати динамічне додавання та видалення інформації у стані комірки, завдяки чому забезпечується кероване збереження даних у пам’яті мережі. Це імітує обмеженість людської пам’яті, уникаючи накопичення надлишкової

інформації. Вихідний вентиль додатково формує оновлений стан комірки, що використовується для обчислення підсумкового виходу.

Таким чином, LSTM-мережа здатна підтримувати релевантну історичну інформацію та враховувати вплив важливих минулих подій у процесі формування вихідного сигналу. Водночас модель зменшує вплив поточних вхідних даних із низькою інформативністю, оскільки стан комірки містить зважене представлення попереднього досвіду. Усі вентилі LSTM формуються динамічно на основі поточних входів та попередніх виходів мережі.

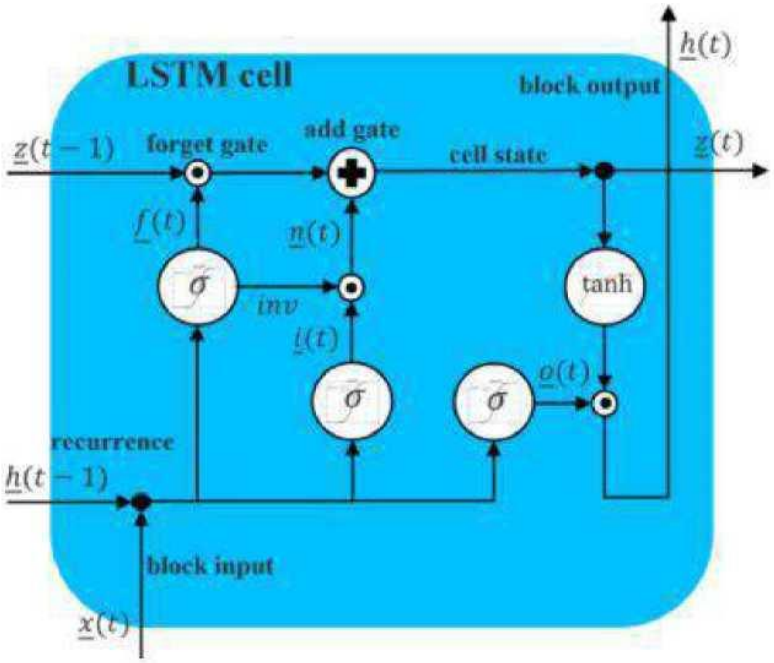

Рисунок 2.1 – Архітектура LSTM із реалізацією зворотного зв’язку між воротами забування та додавання [56].

Архітектуру LSTM можливо інтегрувати у різноманітні нейронні мережі, що відкриває широкі можливості для її застосування. У подальшому розглядаються архітектури, що ґрунтуються на LSTM і призначені для вирішення завдань з виявлення аномалій. Зокрема, увагу буде приділено підходам, заснованим на архітектурі кодувальник-декодувальник, гібридних, графових моделях та методах трансферного навчання.

2.2 Підходи на основі LSTM

LSTM-мережі ефективно використовуються для виявлення контекстуальних аномалій, оскільки здатні моделювати складні часові взаємозв’язки та фіксувати їх у стислому представленні стану. Це стосується як стаціонарних, так і нестаціонарних процесів, а також коротко- та довгострокових залежностей у даних. LSTM-мережі вважаються оптимальними для аналізу багатовимірних часових рядів та систем із часовою мінливістю [57]. У процесі виявлення аномалій реальні вихідні дані системи порівнюються з очікуваними, згенерованими моделлю, а відхилення використовуються як критерій для фіксації аномальних станів. Численні дослідження підтверджують високу ефективність підходів, заснованих на LSTM, у задачах виявлення аномалій.

У [58] представлено архітектуру LSTM для ідентифікації аномалій у часових рядах. На відміну від класичних або шумозахищених LSTM-автокодувальників, у цій архітектурі вхідні дані не зменшуються за розмірністю. Виявлення аномалій базується на аналізі дисперсії відхилень між прогнозованими та фактичними результатами. Глибока LSTM-мережа використовується для прогнозування нормальної поведінки шинового зв’язку в транспортних засобах, а значні відхилення визначаються динамічним порогом, що дозволяє виявляти аномалії, викликані кібератаками. У цьому підході LSTM-модель виконує прогнозування динаміки системи, а SVM застосовується для класифікації аномалій, що забезпечує адаптивність і здатність до самонавчання системи виявлення.

Завдяки таким архітектурам можливо реалізувати як напівконтрольоване, так і неконтрольоване виявлення тимчасових аномалій у багатовимірних даних. Оригінальність підходу полягає в тому, що оцінюється сукупність похибок прогнозування на один крок уперед, а не окремі похибки для кожного моменту часу. LSTM-мережі підвищують точність виявлення аномалій, забезпечуючи якісне прогнозне моделювання

як стаціонарних, так і нестаціонарних часових залежностей. Це дає змогу ефективно ідентифікувати структурні тимчасові аномалії, зокрема у реальному часі – завдяки використанню двох LSTM-мереж [59]. Одна з них моделює короткострокові характеристики та дозволяє виявляти окремі аномальні точки в часових рядах, тоді як інша відповідає за контроль виявлення на основі довгострокових порогових значень.

2.3 Підходи, засновані на кодувальниках-декодувальниках

У більшості сучасних практичних застосувань, зокрема у виробничих та комунікаційних системах, доступні дані, як правило, не мають маркування та лише частково супроводжуються інформаційними моделями, що визначають контекст. Відповідно, актуальними є методи навчання без учителя, які дозволяють реалізувати непряме маркування даних і, таким чином, виявляти аномалії. Одним із провідних напрямів таких методів є використання нейронних мереж із архітектурою кодувальник-декодувальник, які останніми роками зарекомендували себе як ефективний інструмент для задач виявлення аномалій без учителя.

Автокодувальні мережі (Autoencoder, AE) слугують типовим прикладом, коли кодувальник формує стислий простір ознак вхідних даних, а декодувальник відновлює їх на основі цього скороченого представлення [60]. В процесі навчання AE моделює нормальну динаміку системи, навчаючись стискати та реконструювати типові дані. У випадку подачі аномальних зразків, модель, що навчена на нормальних даних, продукує значно більшу помилку реконструкції, динаміка якої може бути основою механізму виявлення аномалій, зокрема в архітектурах надійних глибоких автокодувальників. Для підвищення стійкості до шуму до складу мережі інтегруються шари аналізу головних компонент та регуляризації, що дозволяє зменшити вплив неінформативних ознак.

Для детекції аномальної поведінки формується метрика реконструкції,

яка складається з двох складових: одна відповідає за відокремлення аномалій (наприклад, викидів) від звичайних спостережень, інша – за збереження внутрішніх зв’язків у даних. Подібна ідея покладена в основу скорочувальних LSTM-AE [58], що дозволяє виявляти аномалії у часових рядах із глибокими тимчасовими залежностями. Додатково застосовуються шумопоглинаючі LSTM-AE, здатні виокремлювати основні та незашумлені залежності у даних, що зазнають впливу перешкод.

Поєднання LSTM та автокодувальників дає змогу моделювати як коротко-, так і довгострокові часові залежності у стислому представленні, що формує надійну основу для виявлення складних аномалій у динаміці систем. Подальший розвиток цього підходу передбачає використання варіативних автокодувальників LSTM, у яких кодувальник і декодувальник використовують імовірнісні механізми проєкції.

У цьому випадку вхідні послідовності трансформуються у розподіли ознак меншої розмірності та реконструюються на підставі відповідних статистичних характеристик. Аномалії виявляються шляхом обчислення логарифмічної правдоподібності для реальних і реконструйованих результатів. Крім того, навчений кодувальник може використовуватись для ймовірнісного зменшення розмірності даних. Зокрема, LSTM-AE успішно застосовується для моделювання типової поведінки у дискретних виробничих процесах [61], а декодувальник слугує моделлю зворотного процесу для ідентифікації аномалій через порівняння реальних та реконструйованих змінних. Такий підхід дозволяє виявляти як стаціонарні, так і нестаціонарні аномалії, що впливають на роботу систем керування.

Окрім автокодувальників, для задач виявлення аномалій ефективно використовуються мережі типу sequence-to-sequence (Seq2Seq) із архітектурою кодувальник-декодувальник [62]. У таких моделях аномалії визначаються на основі значних відхилень у станах комірок між шаром кодера та декодера; ці відхилення додатково кластеризуються для остаточної оцінки. Різновиди Seq2Seq-мереж дозволяють моделювати й прогнозувати

різноманітні атрибути, підвищуючи чутливість до різних типів аномалій і демонструючи кращу ефективність порівняно з накопичувальними LSTM-моделями. Окремо підкреслюється підхід до підвищення здатності узагальнення та екстраполяції Seq2Seq-LSTM шляхом оптимізації виявлення аномалій.

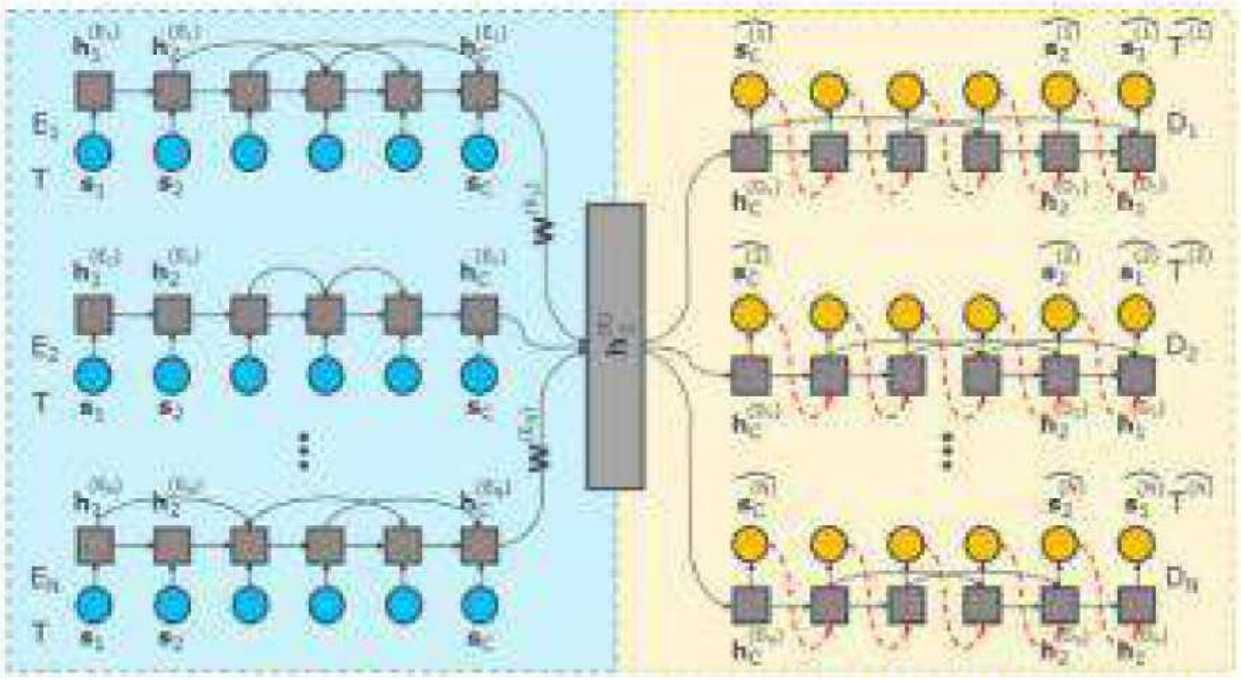

Рисунок 2.2 – Ансамбль LSTM автоенкодерів із пропускними з’єднаннями

На рисунку 2.2 представлена архітектура, що складається з розріджених кодувальників та декодувальників, пов’язаних через шар копіювання, щільність з’єднань у якому адаптується відповідно до інформаційної насиченості вхідних даних. Це дозволяє уникати перенавчання та підвищує здатність до узагальнення [63]. Функція втрат у такій архітектурі мінімізує загальну помилку реконструкції та містить додатковий штрафний член, який регулює потік інформації через копіювальний шар.

2.4 Гібридні підходи

Гібридні підходи до виявлення аномалій вирізняються інтеграцією двох різних нейронних мереж у межах однієї архітектури для підвищення ефективності аналізу. Зазвичай один із компонентів виконує прогнозування динаміки процесу, а інший – фіксує відхилення між прогнозованим та реальним результатом, виявляючи аномальну поведінку. Головною ідеєю гібридних підходів є використання сильних сторін кожної із мереж, одночасно компенсуючи їх окремі недоліки.

Локальні аномалії характеризуються короткотривалими відхиленнями, що спостерігаються лише протягом обмеженого періоду часу та можуть стосуватися одного або кількох зразків. Натомість глобальні аномалії відображають довготривалі зміщення або тренди, які свідчать про нестаціонарність у системі.

Серед перших реалізацій гібридних архітектур варто відзначити поєднання акумулятивного автокодувальника (AE) та LSTM, орієнтованих на роботу з немаркованими даними та невідомою динамікою [59]. Кодувальна частина такої мережі призначена для обробки кількох послідовностей на кожному кроці дискретного часу й може працювати з вихідними або зниженими ознаками. Це дає змогу максимізувати інформаційну насиченість у стислому представленні. Виявлення аномалій здійснює друга мережа у складі комплексної архітектури: LSTM навчається ідентифікувати аномальні відхилення у реконструйованому просторі ознак.

Інший приклад гібридного підходу – розширення LSTM-AE за допомогою алгоритму кластеризації. У цій схемі відновлена динаміка системи відображається у просторі станів, де аномальні процеси ідентифікуються через різкі або поступові зміни стану, а також появу нових структур станів [61]. З метою підвищення якості виявлення взаємодію предиктора та детектора оптимізують через використання генеративних змагальних мереж (GAN) на основі LSTM. У таких архітектурах генератор

моделює дані реальної системи, а дискримінатор навчається розрізняти згенеровані та справжні дані, і таким чином підвищується якість реконструкції та детекції [63].

Для виявлення багатовимірних аномалій до складу гібридних систем інтегрують згорткові нейронні мережі (CNN) разом із LSTM. CNN дозволяють ефективно виділяти ознаки з даних високої розмірності, що дає змогу аналізувати залежності у кількох вимірах (просторових, часових тощо). Таким чином, поєднання CNN і LSTM дає змогу виявляти складні контекстуальні аномалії, навіть якщо вони не проявляються одночасно в усіх вимірах. Класифікація здійснюється на основі крос-ентропії, що дозволяє оцінювати відповідність прогнозів реальним даним (рисунок 2.3) [58].

З метою подальшого підвищення точності виявлення аномалій використовується комбінація LSTM із методами експоненціально зваженого ковзного середнього (EWMA) та динамічного порогового значення. Цей підхід дозволяє аналізувати залишки прогнозу та оперативно виявляти аномальні структури у багатовимірних часових рядах, забезпечуючи комплексне виявлення контекстуальних аномалій у нових послідовностях та значне підвищення ефективності детекції.

3 РОЗРОБКА МЕТОДУ

3.1 Визначення даних

Федеральна адміністрація автомобільних доріг США (Federal Highway Administration, FHWA) у партнерстві з Volpe Center провела низку натурних випробувань для збору реальних даних. У роботі [64] дослідники використовували ці дані для демонстрації концепції руху автоколони із застосуванням CACC (кооперативного адаптивного круїз-контролю) та ACC (адаптивного круїз-контролю). Випробування проводилися на майданчику Aberdeen Center (штат Меріленд) на трасі завдовжки 4,5 милі, яка імітує геометрію типової автомагістралі США. Траса була обладнана геолокаційними точками (waypoints) для передачі сигналів, наприклад, цільових швидкостей, випробувальним транспортним засобам.

У випробуваннях брала участь автоколона з п’яти Cadillac SRX, включаючи ведучі (LV) та ведені (FV) автомобілі, які були оснащені контролерами CACC та тестувалися в різних конфігураціях. Після отримання сигналу від waypoint ведучі автомобілі використовували цю інформацію разом із даними GPS для налаштування CACC. Склад транспортних засобів рухався від першої до останньої контрольної точки, що вважалося завершенням одного випробувального заїзду. Схема випробувальної траси з позначенням ключових waypoint для тестування автоколони наведена на рисунку 3.1 [64].

Згідно з [65], дані про швидкість і прискорення піддавалися попередній обробці: профілі швидкості згладжувалися методом ковзного середнього, а прискорення обчислювалося на основі згладжених значень швидкості, що мінімізувало розбіжності між прискоренням, обчисленим із сирих і згладжених даних.

Рисунок 3.1 – Випробувальна траса для польових експериментів

Для розробки алгоритму виявлення аномалій були використані очищені дані про траєкторії CAV із CARMAs [11]. Кожна траєкторія CAV містить чотири ознаки, що реєструються кожні 0,5 с:

- швидкість CAV;
- прискорення CAV;
- середня швидкість не-CAV у тій самій автоколоні;
- кут повороту рульового колеса CAV.

Тривалість однієї траєкторії складає 10 секунд.

3.2 Емуляція кібератак

Оскільки публічно доступні аномальні дані сенсорів CAV відсутні, у цьому дослідженні аномалії сенсорів моделювалися на основі реальних траєкторних даних CAV. За даними літератури, такі сенсори є вразливими до кібератак і збоїв у роботі [66-68]. Розглянуто три типи атак, які можуть

спричиняти чотири типи сенсорних аномалій:

- атака шляхом ін’єкції хибних даних через шину CAN або систему бортової діагностики (OBD); може впливати на вимірювання швидкості та прискорення;

- зловмисник із дійсними обліковими даними може змінювати показники сенсорів за допомогою глушіння або підміни GPS; це призводить до появи аномалій;

- акустична ін’єкція може порушувати цілісність сенсора прискорення, викликаючи додаткові збої.

Дане дослідження зосереджене на виявленні нормальних та аномальних траєкторій CAV. Виходячи зі згаданих сценаріїв атак, аномальні траєкторії створювалися шляхом включення чотирьох типів аномалій у чотирьох сценаріях відповідно до проведених іншими авторами досліджень [32].

Сценарій 1: короткочасна аномалія.

Характеризується різкою зміною у даних траєкторії CAV. Для імітації використовувалася випадкова гаусівська змінна із середнім нуль і дисперсією 0,001. Вона масштабувалася за допомогою $N \in (0;0,01)$, де $N \in \{25, 100, 1000, 10000\}$, і додавалася до базового значення сенсора.

Сценарій 2: шум.

Довготривала зміна (протягом кількох послідовних вимірювань) у варіативності даних траєкторії. Аномалія моделювалася як незалежна і однаково розподілена послідовність випадкових гаусівських змінних із середнім нуль, довжиною l та дисперсією c.

Сценарій 3: зсув (bias).

Відхилення від справжніх показників сенсора. Моделювалося як тимчасове зміщення від нормальних значень, величина якого визначалася випадковою величиною з рівномірного розподілу. Аномальні показники формувалися шляхом додавання зміщення до істинних значень сенсора на різні інтервали $d \in \{25, 50, 100, 1000\}$.

Сценарій 4: поступовий дрейф.

Повільна і стійка зміна даних у часі. Аномалія моделювалася додаванням лінійно зростаючих значень до базових, наприклад, лінійно зростаюча швидкість 0-5 миль/год при $c \in \{3,5\}$, з використанням функції linspace(0,c). Аномалія моделювалася на різні інтервали часу.

Аномалії навмисно впроваджувалися в сенсори CAV. Передбачалося, що поява сенсорних аномалій, спричинених кібератаками чи збоєм, відбувається незалежно, що спрощувало моделювання. Відповідно, предиктивні моделі розроблялися без урахування можливості кореляції помилок сенсорів. Також передбачалося, що у будь-який момент часу виникає лише одна аномалія, що відображає незалежний характер атак або збоїв і притаманну надійність сенсорних систем. Аномалії генерувалися випадковим чином і застосовувалися до різних сенсорів стохастично. Симульовані аномалії додавалися до нормальних (базових) показників відповідних сенсорів як у ведучих, так і у ведених автомобілях. Характер і тривалість цих аномалій змінювалися: деякі тривали 5 хвилин, інші – до 20 хвилин. Також моделювався змішаний сценарій аномалій для оцінки чутливості механізмів виявлення.

3.3 Побудова моделі виявлення аномалій

3.3.1 Запропонована модель

Як показано на рисунку 3.2, запропонована модель складається з двох основних компонентів:

1) мережа стискання, яка призначена для створення низькорівневої апроксимації (позначеної як z) вхідних даних за допомогою LSTM-автокодувальника. У цьому процесі об'єднуються ознаки зі зменшеного простору z_c з ознаками, що представляють похибки реконструкції z_r;

2) модель GMM, метою якої є передбачення ймовірності або

енергетичного рівня зразка.

Сині точки в кожному шарі на рисунку 2.2 позначають окремі нейрони, які обробляють та передають інформацію в межах мережі.

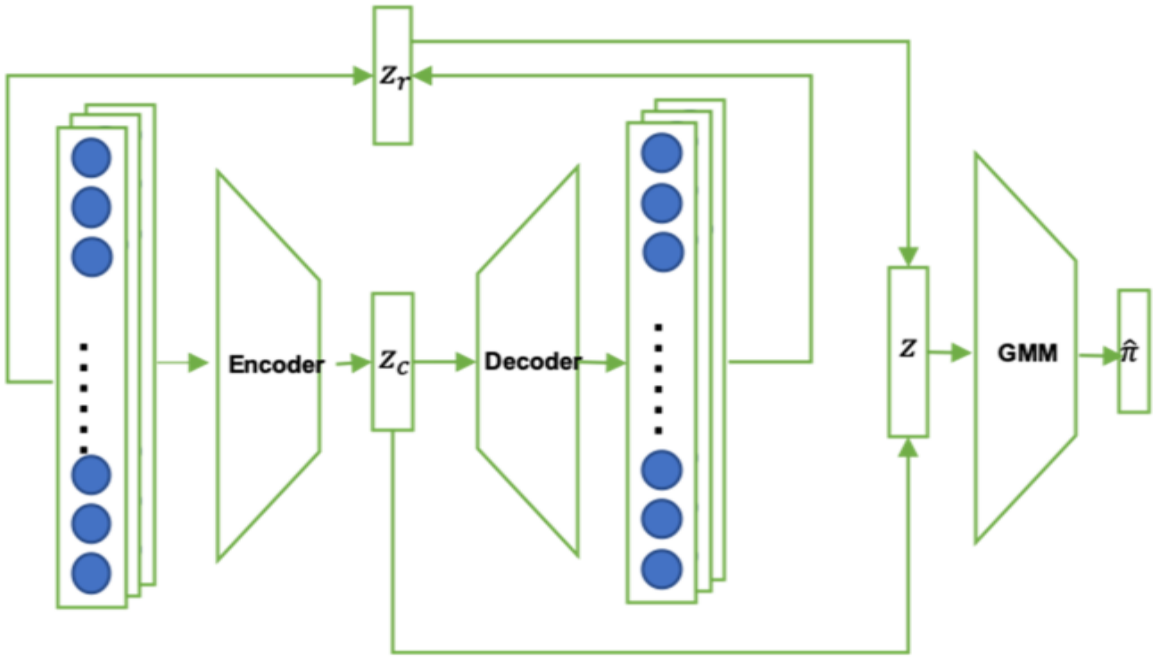

Рисунок 3.2 – Структурна схема моделі LSTM-автокодувальника з гаусівською сумішшю

Для вхідного зразка x LSTM-автокодувальник обчислює низьковимірне представлення z відповідно до рівнянь:

$$z_c = h(x;\theta_e), \tag{3.1}$$

$$x^0 = g(z_c;\theta_d), \tag{3.2}$$

$$z_r = f(x;x^0), \tag{3.3}$$

$$z = [z_c, z_r], \tag{3.4}$$

де z_c – це низькорівнева апроксимація, отримана LSTM-

автокодувальником; z_r – ознаки, отримані на основі похибки реконструкції; θ_e та θ_d – параметри LSTM-автокодувальника; x^0 – реконструйоване значення x; $h(\cdot)$ і $g(\cdot)$ – функції кодування та декодування відповідно. Крім того, $f(\cdot)$ – функція для обчислення ознак, пов'язаних із похибкою реконструкції.

Маючи низькорівневу апроксимацію вхідних даних, мережа оцінювання на основі GMM призначена для оцінки функції щільності розподілу. GMM зазвичай застосовується для моделювання розподілу класів шляхом навчання параметрів для кожного класу під час тренування. Для класифікації нових даних GMM обчислює ймовірність належності до кожного класу, що дозволяє вибрати клас із найвищою ймовірністю. Окрім цього, GMM може ідентифікувати зразки, які істотно відхиляються від вивченого нормального розподілу.

В GMM невідомими параметрами є:

- розподіл компонент суміші ϕ;
- середні значення сумішей μ;
- коваріація сумішей Σ.

Для визначення належності кожного зразка до компонентів суміші використовується багатошарова нейронна мережа (MLNN):

$$p = \mathrm{MLNN}\left[z, \theta_m\right], \tag{3.5}$$

$$\hat{\gamma} = \mathrm{soft\,max}(p), \tag{3.6}$$

де $\hat{\gamma}$ – вектор, що визначає прогнозовану «м’яку» належність до компонентів суміші, а p – вихід MLNN. Використовуючи N та прогнозовану належність, параметри GMM можна додатково оцінити наступним чином:

$$\hat{\phi}_k = \sum_{i=1}^{N} \frac{\hat{\gamma}_{ik}}{N}, \tag{3.7}$$

$$\hat{\mu}_k = \frac{\sum_{i=1}^{N} \hat{\gamma}_{ik} z_i}{\sum_{i=1}^{N} \hat{\gamma}_{ik}}, \tag{3.8}$$

$$\hat{\Sigma}_k = \frac{\sum_{i=1}^{N} \hat{\gamma}_{ik} \left(z_k - \hat{\mu}_j\right)\left(z_k - \hat{\mu}_j\right)^T}{\sum_{i=1}^{N} \hat{\gamma}_{ik}}, \tag{3.9}$$

де $\hat{\phi}_k$, $\hat{\mu}_k$ і $\hat{\Sigma}_k$ – ймовірність, середнє значення та коваріація для компонента k у GMM. Енергію зразка можна оцінити так:

$$\Sigma(z) = -\log\left(\sum_{k=1}^{K} \hat{\phi}_k \frac{\exp\left(-\frac{1}{2}(z - \hat{\mu}_k)T\right)\hat{\Sigma}_k^{-1}(z - \hat{\mu}_k)}{\sqrt{\left|2\hat{\pi}_k\right|}}\right). \tag{3.10}$$

У тестовій фазі рівень енергії використовується для визначення, чи містять дані фальсифіковані траєкторії. Зростання енергетичного рівня свідчить про більшу ймовірність наявності аномалій.

3.3.2 Цільова функція

Цільова функція моделі GMLM:

$$j(\theta_e, \theta_d, \theta_m) = \frac{1}{N}\sum_{i=1}^{N} L(x_i, x_i') + \frac{\lambda_1}{N}\sum_{i=1}^{N} E(z_i) + \lambda_2 P(\hat{\Sigma}), \tag{3.11}$$

де $L(x_i, x'_i)$ – це функція втрат, яка кількісно оцінює похибку реконструкції, згенеровану LSTM-автокодувальником, і може бути визначена за допомогою L2-норми; $E(z_i)$ позначає ймовірності спостереження вхідних зразків.

Мінімізація j спрямована на уникнення проблеми сингулярності

шляхом штрафування малих значень на головній діагоналі.

3.3.3 Відмінності від попередніх досліджень

Для початку було використано мережу на основі LSTM як базову модель. LSTM навчали розпізнавати нормальні патерни поведінки. На кожному кроці часу виконувалися передбачення, а помилки цих передбачень сигналізували про відхилення від норми. Далі застосовувався метод кластеризації для ідентифікації аномалій. Однак результати виявилися недостатньо задовільними, особливо з урахуванням різних типів кібератак. Тому для виявлення аномалій було запропоновано нову модель GMLM.

На основі дослідження Purohit [69] у цій роботі реалізовано такі удосконалення:

- врахування часових зв’язків у даних про траєкторії CAV за допомогою LSTM-автокодувальника;
- тестування моделі проти декількох типів кібератак.

Зокрема, було впроваджено LSTM-автокодувальник замість багатошарової нейронної мережі, яку використовували в оригінальній роботі [69].

4 ЕКСПЕРИМЕНТИ ТА РЕЗУЛЬТАТИ

4.1 Конфігурація та гіперпараметри GMLM

Для набору даних CARMA LSTM-автокодувальник передає тривимірний вхід до мережі оцінювання, що складається з одного зменшеного виміру та двох вимірів, отриманих із похибки реконструкції. Зокрема, GMLM використовує LSTM-шар із параметрами ((20, 4), 128, tanh) та вісім повнозв'язних шарів (FC) з різними розмірами:

- FC (128, 64, tanh);
- FC (64, 32, tanh);
- FC (32, 16, tanh);
- FC (16, 1, none);
- FC (1, 16, tanh);
- FC (16, 32, tanh);
- FC (32, 64, tanh);
- FC (64, 128, none).

Мережа оцінювання складається з FC (3, 10, tanh), шару Dropout (0.5) та FC (10, 4, softmax).

Також були протестовані різні комбінації LSTM та Deep Autoencoder Gaussian Mixture Model (DAGMM) для пропонованої моделі. У цьому дослідженні налаштовувалися такі гіперпараметри:

- кількість LSTM-шарів;
- кількість FC-шарів;
- рівень Dropout;
- швидкість навчання в оптимізаторі Adam.

Наведена конфігурація є найкращою з отриманих.

4.2 Продуктивність мережі та метрики

Для порівняння ефективності виявлення аномалій використовувалися такі метрики:

- точність (precision);
- F1-метрика;
- правильність (accuracy).

Для ідентифікації аномальних зразків було обрано порогове значення. Наприклад, у випадку роботи GMLM на наборі CARMA зразки з найвищими енергетичними перцентилями класифікуються як фальсифіковані траєкторії. Клас аномалії вважається позитивним, відповідно визначаються метрики precision, F1-score та accuracy.

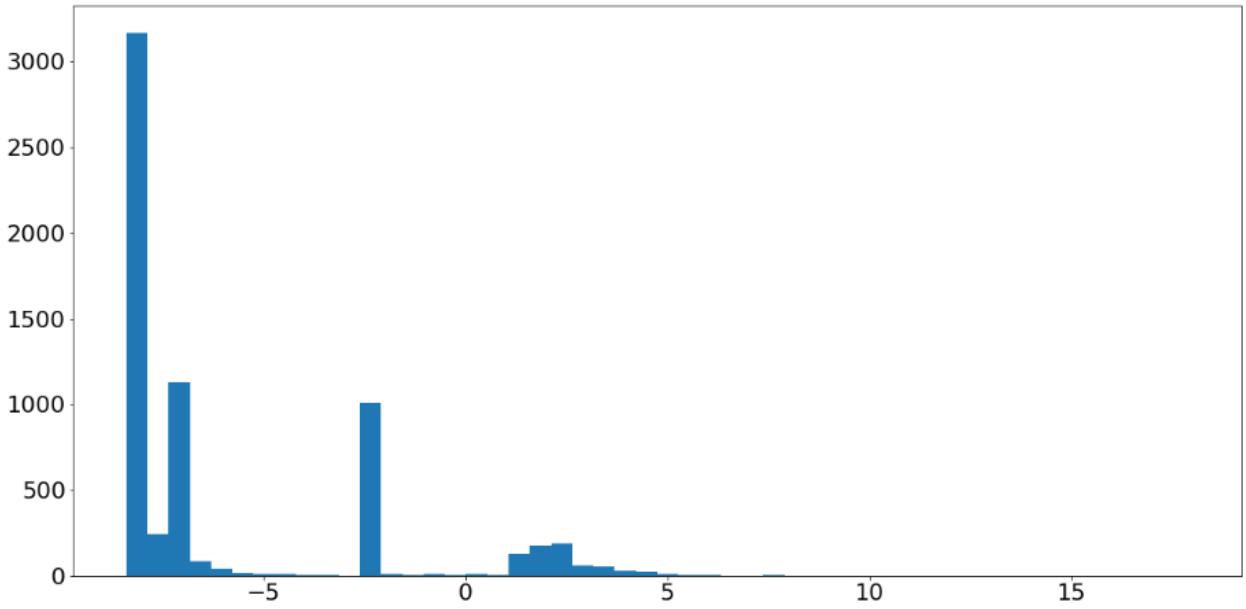

Рисунок 4.1 – Гістограма енергії GMLM

Було змодельовано змішані атаки трьох різних типів для створення більш реалістичного середовища, і час їх виникнення не задавався явно. На рисунку 4.1 представлено гістограму розподілу енергії, обчисленої GMLM-моделлю. Більші значення енергії вказують на вищу ймовірність наявності фальсифікованих траєкторій CAV. Як показано на рисунку 3.1, більшість

зразків мають від’ємну енергію, тоді як лише невелика частина має енергію понад 5 по горизонталі. Цей графік дає змогу отримати уявлення про ймовірність кібератак у наборі даних для операторів CAV.

На рисунку 3.2 показано розподіл енергії GMLM для всіх зразків. Це свідчить, що невелика частина зразків має високу енергію, наприклад, понад 10, що вказує на високу ймовірність фальсифікованих траєкторій чи аномальної поведінки CAV.

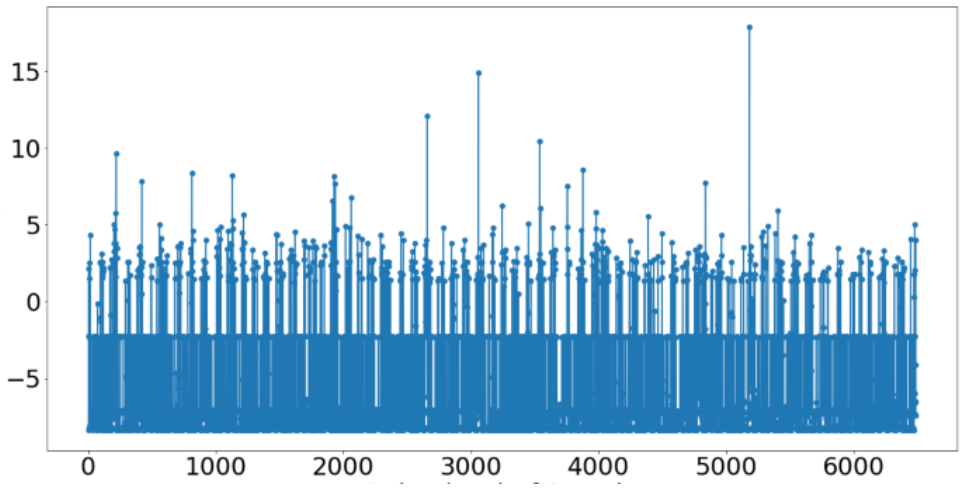

Рисунок 4.2 – Енергія GMLM для всіх зразків.

Рисунок 4.3 ілюструє нормальні траєкторії CAV (сині точки) та фальсифіковані траєкторії CAV (червоні хрестики) для кожної комбінації двох із чотирьох ознак (чотири рядки та чотири стовпці).

Результати порівняння запропонованої моделі із базовими підходами, зокрема NLP-моделлю та DAGMM із [70], наведені в таблиці 4.1. Спочатку 99% зразків класифікувалися як аномалії. Виявилося, що precision та accuracy моделі були подібні до випадкового вибору (близько 49,43% accuracy та 51,44% precision). Із зменшенням перцентиля зросли як precision, так і accuracy, які перевищили ці показники в базових методах.

Зниження перцентиля дає змогу даним мати більш гнучкі критерії, тому отримані результати є більш точними. Крім того, під час тестування запропонована модель демонструвала дуже швидке прогнозування – 0,08 с на

один зразок. Така швидкість дозволяє водію CAV оперативно реагувати на появу ймовірних кібератак у режимі реального часу.

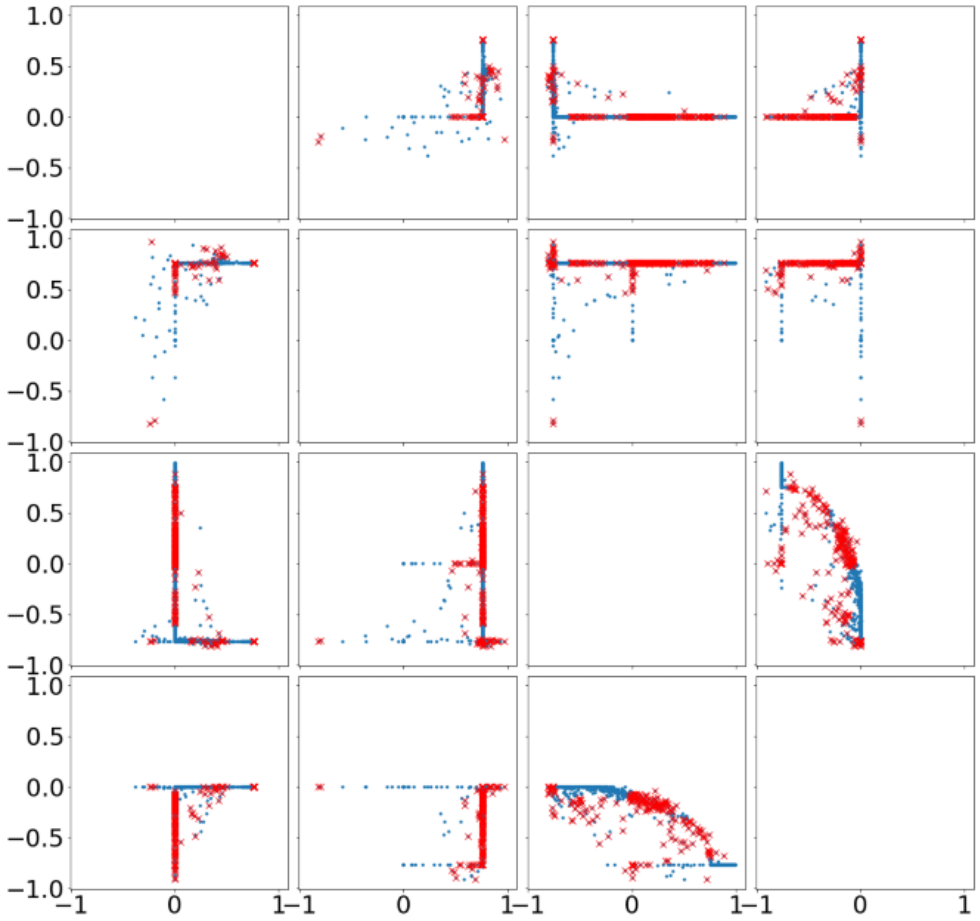

Рисунок 4.3 – Енергія GMLM для різних ознак

Таблиця 4.1 – Порівняння ефективності моделей

Модель-Перцентиль	Precision, %	Accuracy, %	F1-Score
NLP	60,32	63,88	1,27
DAGMM	64,23	71,96	0,092
LSTM	50,87	51,93	0,27
GMLM-99%	49,43	51,44	0,024
GMLM-97%	64,76	53,55	0,058
GMLM-70%	70,63	74,99	0,53

Крім того, результати валідаційного тестування моделі є обнадійливими, як показано в таблиці 4.2. GMLM-70% усе ще демонструє кращі показники у порівнянні з традиційними моделями LSTM чи NLP (точність 65%). Це свідчить про збалансованість між складністю моделі та її ефективністю.

Таблиця 4.2 – Результати валідаційного тестування

Модель–Перцентиль	Precision, %	Accuracy, %	F1-Score
GMLM-99%	50,63	68,47	0,034
GMLM-97%	50,5	55,1	0,068
GMLM-70%	63	65,51	0,54

Оскільки атаки генеруються випадково, неможливо виконати точне кількісне порівняння між різними типами атак. Однак було відмічено, що певні атаки детектуються точніше за інші: наприклад, короткочасна аномалія визначається більш точно, ніж поступовий дрейф, а шум є найскладнішою для виявлення аномалією. У цьому контексті ідентифікація відображає більшу ймовірність кібератаки, що оцінюється за рівнем енергії. Причиною такої поведінки може бути природа атак: перші два типи простіше розпізнати моделі під час навчання, у той час як для шуму, що містить більше випадкових компонентів, може знадобитися складніша структура моделі. Таким чином, постає питання про баланс між складністю моделі та її продуктивністю.

ВИСНОВКИ

У кваліфікаційній роботі було запропоновано модель GMLM для виявлення аномалій, яка дозволяє ідентифікувати аномальні траєкторії CAV у режимі реального часу.

GMLM складається з двох основних компонентів:

- LSTM-автокодувальника та декодера, які формують низькорівневі представлення початкових зразків, зберігаючи при цьому ключову інформацію;

- моделі GMM, здатної оцінювати енергію у зниженому вимірі простору.

Зокрема, LSTM-автокодувальник дозволяє вилучати довгострокові часові залежності у даних про траєкторії CAV. Запропонований метод виявлення аномалій продемонстрував обнадійливі результати у цьому дослідженні. Підхід GMLM забезпечує підвищення правильності виявлення на 3% та точності на 6,4% порівняно з сучасними методами, що підтверджує ефективність запропонованого алгоритму.

Перспективи подальших досліджень.

1. Валідація продуктивності моделі на різноманітних реальних даних автономних транспортних засобів. Для цього потрібно дослідити можливості збору таких даних у співпраці з промисловими партнерами або з використанням публічних репозиторіїв.

2. Розширення оцінювання на різноманітні реалістичні сценарії дозволить краще продемонструвати універсальність підходу.

3. Удосконалення можливостей моделі щодо розрізнення різних типів аномалій, таких як короткочасні імпульси, шум, поступовий дрейф тощо. Вміння визначати джерело аномалій є важливим для забезпечення здатності автономних транспортних засобів реагувати належним чином [71]. Модель може бути розширена шляхом впровадження класифікації за шаблонами

похибок реконструкції для розпізнавання різних типів фальсифікованих траєкторій.

4. Іншим перспективним напрямом досліджень є інтеграція моделей на основі Transformer. Механізми self-attention у Transformer дозволяють ефективно моделювати складні послідовні залежності у часових рядах. Інтеграція Transformer-енкодера у структуру запропонованої моделі може покращити якість навчання представлень із багатовимірних сенсорних потоків. Додаткове донавчання на реальних даних автономних транспортних засобів дозволить моделі Transformer фокусуватися на закономірностях, найбільш релевантних до траєкторій транспортних засобів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Zang, Y., Chen, S., Liu, S., He, Z., Liu, Y., He, X. Urban vehicle localization: Challenges and recent advances. IEEE Transactions on Intelligent Transportation Systems, 23(5), 3541–3557, 2022. DOI: 10.1109/TITS.2021.3085772.

2. Zeng, W., Li, K., Luo, X., Liu, Q., Fu, M., Zhou, Y. Accurate vehicle localization in dense urban scenarios. IEEE Access, 11, 47962–47977, 2023. DOI: 10.1109/ACCESS.2023.3288592.

3. Gu, Y., Wu, Z., Xue, J., Liu, J., Zhu, L. Survey of indoor positioning systems for autonomous vehicles. Sensors, 22(3), 951, 2022. DOI: 10.3390/s22030951.

4. Li, R., Zhou, F., Zheng, Y., Wang, Z., Liu, Y. V2X-based cooperative vehicle localization: State of the art and future directions. IEEE Internet of Things Journal, 10(4), 3328–3342, 2023. DOI: 10.1109/JIOT.2022.3208398.

5. Wang, Y., Chen, J., Xu, Y., Wang, Q., Zhang, X. Urban canyon effects on GNSS localization. Navigation, 68(2), 233–246, 2021. DOI: 10.1002/navi.415.

6. Kim, H., Lee, D., Choi, H., Park, S., Cho, J. Effects of weather on LiDAR sensors for autonomous vehicles. Sensors, 21(8), 2872, 2021. DOI: 10.3390/s21082872.

7. Qi, J., Liu, D., Zhang, Y., Xu, C., Chen, X. IMU drift compensation for vehicle localization. IEEE Sensors Journal, 22(12), 11562–11574, 2022. DOI: 10.1109/JSEN.2022.3161476.

8. Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., Kintner, P.M. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In Proceedings of the ION GNSS International Technical Meeting, St. Louis, MO, USA, 20–24 September 2021, pp. 2314–2325.

9. Ben Saad, M., Triki, A., Kaddour, M., Boudriga, N. Security threats and countermeasures in V2X: A survey. IEEE Access, 11, 22221–22238, 2023. DOI:

10.1109/ACCESS.2023.3262676.

10. El-Sheimy, N., Youssef, A.M. Inertial sensors for vehicle navigation: State-of-the-art and future trends. Sensors, 22(3), 1239, 2022. DOI: 10.3390/s22031239.

11. Eichelberger, A., Stork, W., Schmid, M., Reuter, J. Autonomous vehicle localization in GNSS-denied environments. Journal of Field Robotics, 40(3), 399–415, 2023. DOI: 10.1002/rob.22137.

12. Kuutti, S., Fallah, S., Bowden, R., Barber, P. A survey of deep learning applications to autonomous vehicle control. IEEE Transactions on Intelligent Transportation Systems, 23(4), 3232–3247, 2022. DOI: 10.1109/TITS.2021.3067634.

13. Milanes V., Shladover S.E. Automated Vehicles for Safety, Security, and Productivity. IEEE Transactions on Intelligent Transportation Systems. 2016. Vol. 17, No. 2. P. 290–300.

14. Grewal M.S., Andrews A.P. Applications of Kalman Filtering in Aerospace 1960 to the Present [Historical Perspectives]. IEEE Control Systems Magazine. 2015. Vol. 30, No. 3. P. 69–78.

15. Li Y., Ibanez-Guzman J. Lidar for Autonomous Driving: The Principles, Challenges, and Trends for Automotive Lidar and Perception Systems. IEEE Signal Processing Magazine. 2020. Vol. 37, No. 4. P. 50–61.

16. Levinson J., Thrun S. Robust vehicle localization in urban environments using probabilistic maps. Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), 2010. P. 4372–4378.

17. Wang Y., Ferman M.A., Zeng Y. Computer vision in intelligent vehicles: Advances and challenges. Engineering. 2022. Vol. 8, No. 6. P. 823–838.

18. Karagiannis G., Altintas O., Ekici E., Heijenk G., Jarupan B., Lin K., Weil T. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. IEEE Communications Surveys & Tutorials. 2011. Vol. 13, No. 4. P. 584–616.

19. Rezaei M., Sengupta R. Kalman Filter-Based Integration of DGPS and

Vehicle Sensors for Localization. IEEE Transactions on Control Systems Technology. 2007. Vol. 15, No. 6. P. 1080–1088.

20. Carballo A., Talbot J., Yamamoto K., Nakaoka M., Kato S., Takeda K., Katayama T. Camera and LiDAR Sensor Fusion for Accurate and Robust Vehicle Localization: A Deep Learning Approach. IEEE Transactions on Intelligent Transportation Systems. 2022. Vol. 23, No. 2. P. 1205–1218.

21. Liu W., Ma Y., Ma X., Zeng G., Chen Y. All-Weather Autonomous Vehicle Localization Using Radar and LiDAR. Sensors. 2021. Vol. 21, No. 1. 143.

22. Raza S., Wallgren L., Voigt T. Security and Performance Considerations in V2X Communications for Vehicle Safety Applications. Computers. 2017. Vol. 6, No. 4. 27.

23. AlSalem, T.S., Almaiah, M.A., Lutfi, A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. Electronics 2023, 12, 3958.

24. Khattak, Z.H., Smith, B.L., Fontaine, M.D. Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes. Accid. Anal. Prev. 2021, 150, 105861.

25. Javed, A.R., Usman, M., Rehman, S.U., Khan, M.U., Haghighi, M.S. Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. IEEE Trans. Intell. Transp. Syst. 2020, 22, 4291–4300.

26. Huang, S.E., Feng, Y., Liu, H.X. A data-driven method for falsified vehicle trajectory identification by anomaly detection. Transp. Res. Part C Emerg. Technol. 2021, 128, 103196.

27. Wen, X., Chen, J., Hu, Z., Lu, Z. A p-opportunistic channel access scheme for interference mitigation between v2v and v2i communications. IEEE Internet Things J. 2020, 7, 3706–3718.

28. Yang, T., Lv, C. A secure sensor fusion framework for connected and automated vehicles under sensor attacks. IEEE Internet Things J. 2021, 9, 22357–22365.

29. Zhong, H., Cao, W., Zhang, Q., Zhang, J., Cui, J. Toward trusted and

secure communication among multiple internal modules in CAV. IEEE Internet Things J. 2021, 8, 17734–17746.

30. Guo, H., Liu, J., Dai, Q., Chen, H., Wang, Y., Zhao, W. A distributed adaptive triple-step nonlinear control for a connected automated vehicle platoon with dynamic uncertainty. IEEE Internet Things J. 2020, 7, 3861–3871.

31. Van Wyk, F., Wang, Y., Khojandi, A., Masoud, N. Real-time sensor anomaly detection and identification in automated vehicles. IEEE Trans. Intell. Transp. Syst. 2019, 21, 1264–1276.

32. Kamel, J., Ansari, M.R., Petit, J., Kaiser, A., Jemaa, I.B., Urien, P. Simulation framework for misbehavior detection in vehicular networks. IEEE Trans. Veh. Technol. 2020, 69, 6631–6643.

33. Wang, Y., Masoud, N., Khojandi, A. Real-time sensor anomaly detection and recovery in connected automated vehicle sensors. IEEE Trans. Intell. Transp. Syst. 2020, 22, 1411–1421.

34. Dong, C., Wang, H., Ni, D., Liu, Y., Chen, Q. Impact evaluation of cyber-attacks on traffic flow of connected and automated vehicles. IEEE Access 2020, 8, 86824–86835.

35. Yen, C.C., Ghosal, D., Zhang, M., Chuah, C.N., Chen, H. Falsified data attack on backpressure-based traffic signal control algorithms. In Proceedings of the 2018 IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, 5–7 December 2018, pp. 1–8.

36. Singh, P.K., Tabjul, G.S., Imran, M., Nandi, S.K., Nandi, S. Impact of security attacks on cooperative driving use case: CACC platooning. In Proceedings of the TENCON 2018-2018 IEEE Region 10 Conference, Jeju, Republic of Korea, 28–31 October 2018, pp. 138–143.

37. Nguyen, V.L., Lin, P.C., Hwang, R.H. Physical signal-driven fusion for V2X misbehavior detection. In Proceedings of the 2019 IEEE Vehicular Networking Conference (VNC), Los Angeles, CA, USA, 4–6 December 2019, pp. 1–4.

38. So, S., Sharma, P., Petit, J. Integrating plausibility checks and machine

learning for misbehavior detection in VANET. In Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018, pp. 564–571.

39. Cui, L., Chen, Z., Wang, A., Hu, J., Park, B.B. Development of a robust cooperative adaptive cruise control with dynamic topology. IEEE Trans. Intell. Transp. Syst. 2021, 23, 4279–4290.

40. Bertini, R.L., Wang, H., Knudson, T., Carstens, K., Rios, E. Assessing state department of transportation readiness for connected vehicle-cooperative systems deployment: Oregon case study. Transp. Res. Rec. 2016, 2559, 24–34.

41. Bhavsar, P., Das, P., Paugh, M., Dey, K., Chowdhury, M. Risk analysis of autonomous vehicles in mixed traffic streams. Transp. Res. Rec. 2017, 2625, 51–61.

42. Hasan, M., Mohan, S., Shimizu, T., Lu, H. Securing vehicle-to-everything (V2X) communication platforms. IEEE Trans. Intell. Veh. 2020, 5, 693–713.

43. Islam, M., Chowdhury, M., Li, H., Hu, H. Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention. Transp. Res. Rec. 2018, 2672, 66–78.

44. Cui, L., Hu, J., Park, B.B., Bujanovic, P. Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: Assessing cooperative adaptive cruise control under cyber attack. Transp. Res. Part C Emerg. Technol. 2018, 97, 1–22.

45. Amoozadeh, M., Raghuramu, A., Chuah, C.N., Ghosal, D., Zhang, H.M., Rowe, J., Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Commun. Mag. 2015, 53, 126–132.

46. Khattak, Z.H., Park, H., Hong, S., Boateng, R.A., Smith, B.L. Investigating cybersecurity issues in active traffic management systems. Transp. Res. Rec. 2018, 2672, 79–90.

47. Li, Y., Tu, Y., Fan, Q., Dong, C., Wang, W. Influence of cyber-attacks on longitudinal safety of connected and automated vehicles. Accid. Anal. Prev.

2018, 121, 148–156.

48. Wardzinski, A. Dynamic risk assessment in autonomous vehicles motion planning. In Proceedings of the 2008 1st International Conference on Information Technology, Gdansk, Poland, 18–21 May 2008, pp. 1–4.

49. Wang, P., Yu, G., Wu, X., Wang, Y., He, X. Spreading patterns of malicious information on single-lane platooned traffic in a connected environment. Comput. Civ. Infrastruct. Eng. 2019, 34, 248–265.

50. Zhou, J., Zhang, B., Fan, L., Lu, Z. Aeromagnetic Anomaly Detection under Low SNR Conditions Using Multiscale Wavelet Energy Accumulation. In Proceedings of the 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020, pp. 1641–1644.

51. Son, E.J., Kim, W., Kim, Y.M., McIver, J., Oh, J.J., Oh, S.H. Time series anomaly detection for gravitational-wave detectors based on the Hilbert-Huang transform. J. Korean Phys. Soc. 2021, 78, 878–885.

52. Jin, Y., Qiu, C., Sun, L., Peng, X., Zhou, J. Anomaly detection in time series via robust PCA. In Proceedings of the 2017 2nd IEEE International Conference on Intelligent Transportation Engineering (ICITE), Singapore, 1–3 September 2017, pp. 352–355.

53. Ma, M., Han, L., Zhou, C. BTAD: A binary transformer deep neural network model for anomaly detection in multivariate time series data. Adv. Eng. Inform. 2023, 56, 101949.

54. Wang, Y., Zhang, R., Masoud, N., Liu, H.X. Anomaly detection and string stability analysis in connected automated vehicular platoons. Transp. Res. Part C Emerg. Technol. 2023, 151, 104114.

55. Yang, Z., Ying, J., Shen, J., Feng, Y., Chen, Q.A., Mao, Z.M., Liu, H.X. Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning From Demonstration. IEEE Trans. Intell. Transp. Syst. 2023, 24, 9462–9475.

56. Hochreiter, S., Schmidhuber, J. Long short-term memory. Neural Computation, 9(8), 1735–1780, 1997. DOI: 10.1162/neco.1997.9.8.1735.

57. Su, Y., Zhao, Y., Niu, C., Liu, R., Sun, W., Pei, D. Robust anomaly detection for multivariate time series through stochastic recurrent neural network. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD ’19), Anchorage, AK, USA, 4–8 August 2019, pp. 2828–2837. DOI: 10.1145/3292500.3330680.

58. Park, D., Hoshi, Y., Kemp, C.C. A multimodal anomaly detector for robot-assisted feeding using an LSTM-based variational autoencoder. IEEE Robotics and Automation Letters, 3(3), 1544–1551, 2018. DOI: 10.1109/LRA.2018.2801476.

59. Hundman, K., Constantinou, V., Laporte, C., Colwell, I., Soderstrom, T. Detecting spacecraft anomalies using LSTMs and nonparametric dynamic thresholding. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD ’18), London, UK, 19–23 August 2018, pp. 387–395. DOI: 10.1145/3219819.3219845.

60. Brownlee, J. A Gentle Introduction to LSTM Autoencoders. Machine Learning Mastery, 17 June 2020. Available online: https://machinelearningmastery.com/lstm-autoencoders/ (accessed on 18 June 2025).

61. Wei, Y., Jang-Jaccard, J., Xu, W., Sabrina, F., Camtepe, S., Boulic, M. LSTM-Autoencoder based anomaly detection for indoor air quality time series data. Sensors, 22(2), 502, 2022. DOI: 10.3390/s22020502.

62. Srivastava, N., Mansimov, E., Salakhutdinov, R. Unsupervised learning of video representations using LSTMs. In Proceedings of the 32nd International Conference on Machine Learning (ICML 2015), Lille, France, 6–11 July 2015, pp. 843–852. Available online: https://arxiv.org/abs/1502.04681 (accessed on 18 June 2025).

63. Aytekin, C., Ni, X., Cricri, F., Aksu, E. Clustering and unsupervised anomaly detection with L2 normalized deep auto-encoder representations. arXiv preprint, 2018. Available online: https://arxiv.org/abs/1802.03905 (accessed on 18 June 2025).

64. Tiernan, T., Richardson, N., Azeredo, P., Najm, W.G., Lochrane, T. Test and Evaluation of Vehicle Platooning Proof-of-Concept Based on Cooperative Adaptive Cruise Control (No. DOT-VNTSC-FHWA-17-13), John A. Volpe National Transportation Systems Center (US): Cambridge, MA, USA, 2017.

65. Hansun, S. A new approach of moving average method in time series analysis. In Proceedings of the 2013 Conference on New Media Studies (CoNMedia), Tangerang, Indonesia, 27–28 November 2013, pp. 1–4.

66. Trippel, T., Weisse, O., Xu, W., Honeyman, P., Fu, K. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 26–28 April 2017, pp. 3–18.

67. Currie, R. Developments in Car Hacking. 2015. Available online: https://sansorg.egnyte.com/dl/FTn9FydfUC.

68. Petit, J., Shladover, S.E. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 2014, 16, 546–556.

69. Purohit, H., Tanabe, R., Endo, T., Suefusa, K., Nikaido, Y., Kawaguchi, Y. Deep autoencoding GMM-based unsupervised anomaly detection in acoustic signals and its hyper-parameter optimization. arXiv 2020, arXiv:2009.12042.

70. Zong, B., Song, Q., Min, M.R., Cheng, W., Lumezanu, C., Cho, D., Chen, H. February. Deep autoencoding gaussian mixture model for unsupervised anomaly detection. In Proceedings of the International Conference on Learning Representations, Vancouver, BC, Canada, 30 April– 3 May 2018.

71. Yun, K., Yun, H., Lee, S., Oh, J., Kim, M., Lim, M., Lee, J., Kim, C., Seo, J., Choi, J. A Study on Machine Learning-Enhanced Roadside Unit-Based Detection of Abnormal Driving in Autonomous Vehicles. Electronics 2024, 13, 288.

72. Torba, A., Diachenko, M., Kharakhaichuk, I. Enhancing Trustworthiness of IoT-Enabled Automated Vehicle Localization Systems // Системи управління, навігації та зв’язку, 2025. Вип. 3 (81) – прийнято до друку.