ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ В АВТОМАТИЗОВАНІЙ СИСТЕМІ ЛОКАЛІЗАЦІЇ ТРАНСПОРТНОГО ЗАСОБУ

КВАЛІФІКАЦІЙНА РОБОТА
ДРУГИЙ (МАГІСТЕРСЬКИЙ) РІВЕНЬ

Автор:
Харахайчук І.А.,
студ. гр. СПм-23-3

Керівник:
Торба А.А.,
проф. каф. ЕОМ

МЕТА І ЗАДАЧІ РОБОТИ

Мета кваліфікаційної роботи:

- розробка методу виявлення аномалій в автоматизованій системі локалізації транспортного засобу.

Задачі:

- огляд проблеми локалізації транспортних засобів (основні технології локалізації транспортних засобів; проблеми та обмеження основних технологій локалізації транспортних засобів)
- аналіз методів виявлення аномалій в локалізації транспортних засобів, огляд сучасних досліджень;
- аналіз методів розпізнавання аномалій;
- розробка нового методу, побудова моделі виявлення аномалій;
- експериментальні дослідження.

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]

3

ТЕХНОЛОГІЇ ЛОКАЛІЗАЦІЇ ТРАНСПОРТНИХ ЗАСОБІВ ТА ПРОБЛЕМИ ЗАСТОСУВАННЯ

- Технології:
  - Глобальні навігаційні супутникові системи
  - Інерціальні вимірювальні одиниці (**IMU**)
  - **LiDAR**, радар, ультразвукові сенсори
  - Камери та комп'ютерний зір
  - **V2X**-комунікації та мережеві підходи
- Проблеми:
  - Вразливість до глушіння та спуфінгу сигналів **GPS/GNSS**
  - Накопичення помилок у **IMU**
  - Вплив погодних умов та перешкод на **LiDAR**, камери, радари
  - Неточності та затримки **V2X**-комунікацій

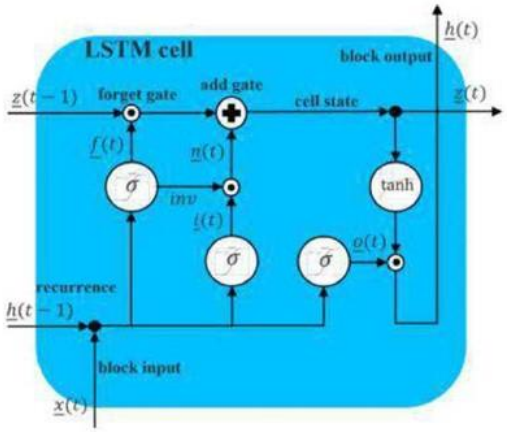
4

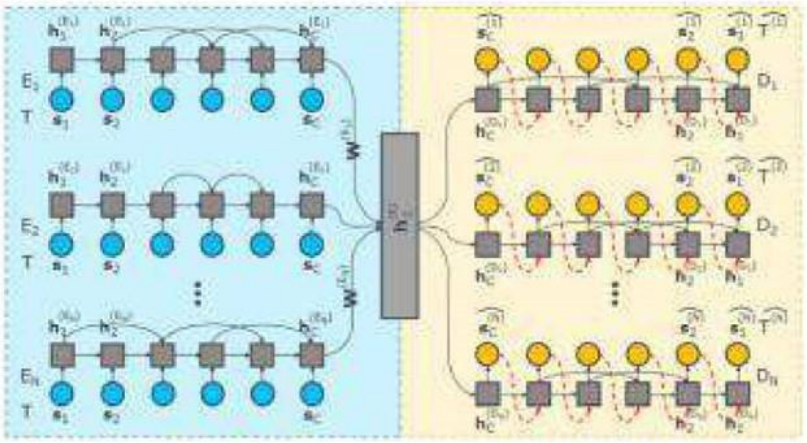
ОСНОВНІ ТИПИ КІБЕРНАПАДІВ У СЕРЕДОВИЩІ CAV

- 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.

5

АРХІТЕКТУРА LSTM





6

ВИПРОБУВАЛЬНА ТРАСА ДЛЯ ПОЛЬОВИХ ЕКСПЕРИМЕНТІВ

Джерело даних: **CARMAs**.

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**.

7

ЕМУЛЯЦІЯ КІБЕРАТАК

Типи атак:

- 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** → призводить до появи аномалій;
- акустична ін'єкція → може порушувати цілісність сенсора прискорення, викликаючи додаткові збої.

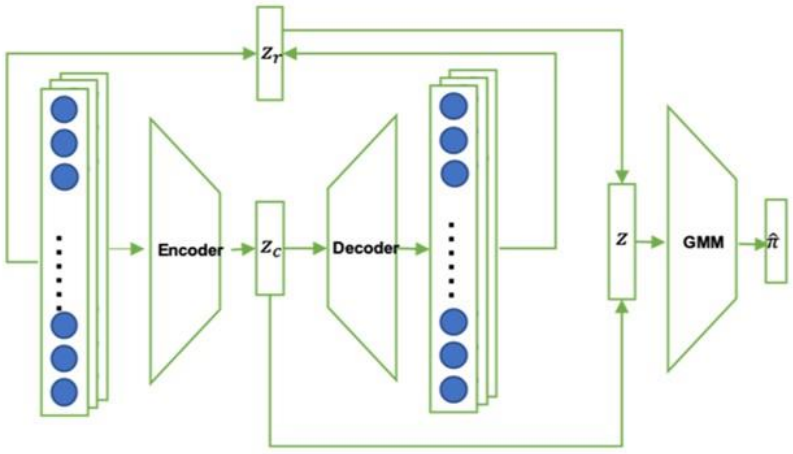
8

ЕМУЛЯЦІЯ КІБЕРАТАК

- **Сценарій 1**: короткочасна аномалія. Різка зміна у даних траєкторії CAV. Для імітації використовувалася випадкова гаусівська змінна із середнім нуль і дисперсією 0,001.
- **Сценарій 2**: шум. Довготривала зміна у варіативності даних траєкторії. 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.
- **Сценарій 4**: поступовий дрейф. Повільна і стійка зміна даних у часі. Аномалія моделювалася додаванням лінійно зростаючих значень до базових. Аномалія моделювалася на різні інтервали часу.

9

ПОБУДОВА МОДЕЛІ

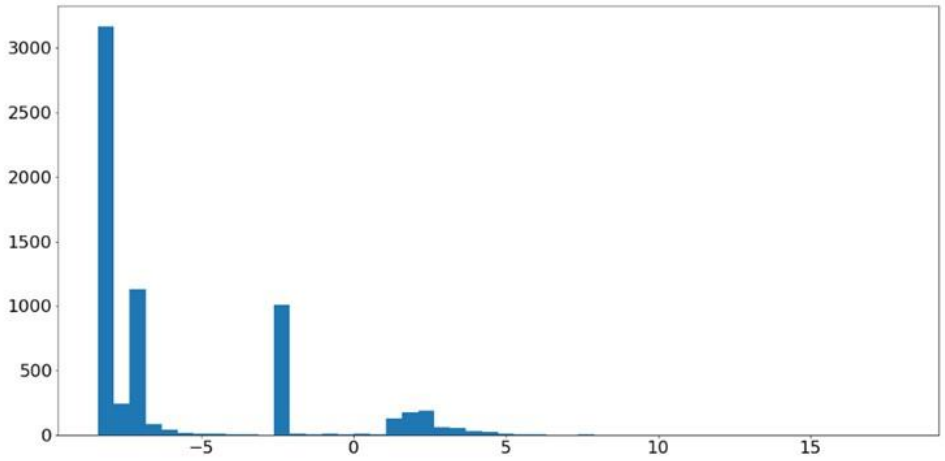


- Цільова функція:

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

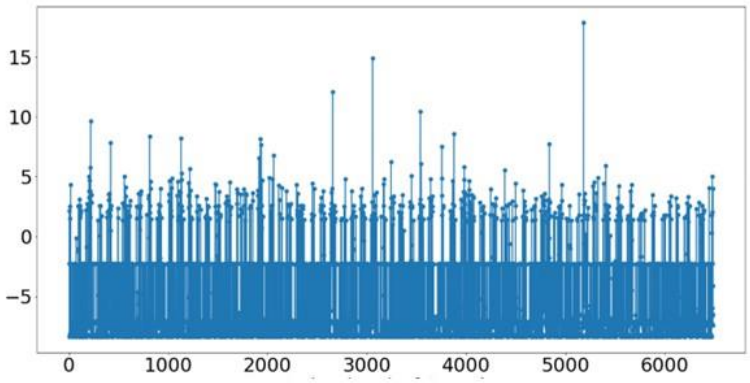
10

ГІСТОГРАМА ЕНЕРГІЇ GMLM



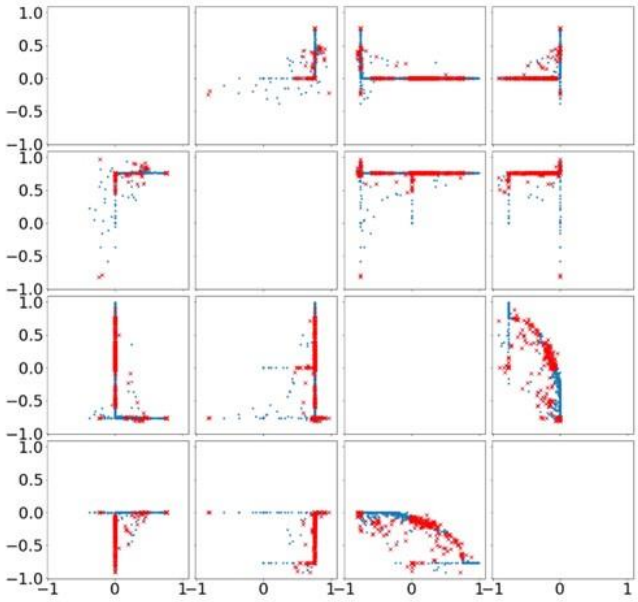
11

ЕНЕРГІЯ GMLM ДЛЯ ВСІХ ЗРАЗКІВ



12

ЕНЕРГІЯ GMLM ДЛЯ РІЗНИХ ОЗНАК



13

ПОРІВНЯННЯ ЕФЕКТИВНОСТІ МОДЕЛЕЙ. ВАЛІДАЦІЯ

2

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

1

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

14

ВИСНОВКИ

- 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.

15

ВИСНОВКИ

- Перспективи подальших досліджень.
- 1. Валідація продуктивності моделі на різноманітних реальних даних автономних транспортних засобів.
- 2. Розширення оцінювання на різноманітні реалістичні сценарії.
- 3. Удосконалення можливостей моделі щодо розрізнення різних типів аномалій, таких як короткочасні імпульси, шум, поступовий дрейф тощо.
- 4. Інтеграція моделей на основі **Transformer**, що дозволить ефективно моделювати складні послідовні залежності у часових рядах.
- Підготовлена публікація: **Torba A., Diachenko M., Kharakhaichuk I. «Enhancing Trustworthiness of IoT-Enabled Automated Vehicle Localization Systems».**

16