ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

КВАЛІФІКАЦІЙНА РОБОТА

МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ У МОБІЛЬНІЙ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ

ВИКОНАВ:
Студент гр СПм-23-4 Коротецький О. О.

КЕРІВНИК:
доц. Мартовицький В.О.

ХАРКІВ
2025р.

Актуальність дослідження

Розробка методу виявлення аномалій у мобільних мережах обумовлена:

експоненційним зростанням трафіку (5G/6G, IoT)

зростанням кіберзагроз (DDoS, спуфінг)

неефективністю традиційних методів

потребою в адаптивних AI-рішеннях для реального часу

Ключові проблеми:
- ✔ Загроза стабільності мережі
- ✔ Погіршення QoS/QoE
- ✔ Вразливість даних абонентів

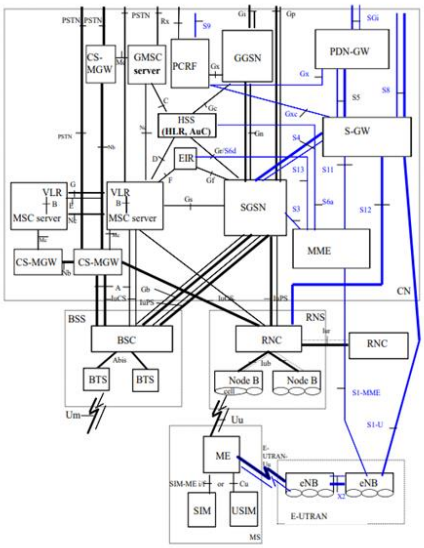
Мета та завдання

Мета дослідження:
Розробити та дослідити ефективний метод виявлення аномалій у мобільній мережі передачі даних, що дозволяє підвищити рівень безпеки та надійності функціонування мережі.

Завдання дослідження:
1.Проаналізувати сучасні загрози та типи аномалій у мобільних мережах передачі даних.
2.Оцінити існуючі методи виявлення аномалій та визначити їх обмеження.
3.Розробити новий або вдосконалити існуючий метод виявлення аномалій з урахуванням специфіки мобільного трафіку.
4.Реалізувати прототип методу та провести його моделювання на тестових даних.
5.Проаналізувати результати: точність, повноту виявлення та продуктивність розробленого підходу.

3

Базова конфігурація мережі доступу 3GPP PLMN



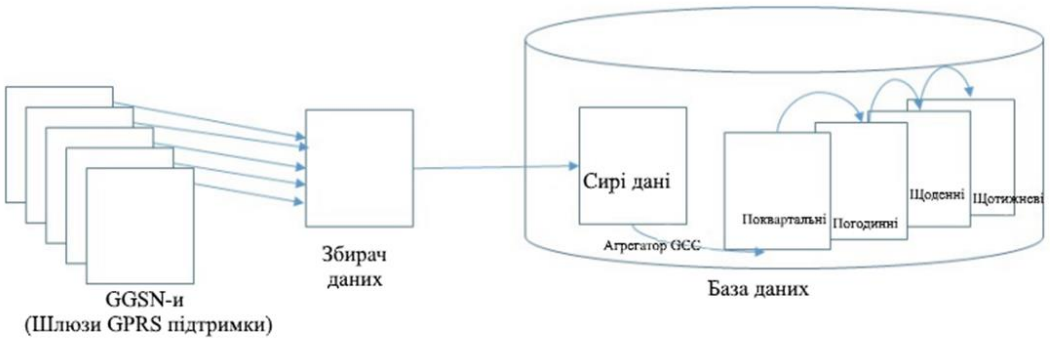
4

Функції SGW згідно

- локальна точка прив'язки мобільності для міжвузлового хендлінгу;
- точка прив'язки мобільності для мобільності між 3gpp;
- буферизація низхідних пакетів у режимі ecm-idle та ініціювання мережевих srp;
- законне перехоплення;
- маршрутизація та переадресація пакетів;
- маркування пакетів на транспортному рівні у висхідній та низхідній лініях;
- облік з деталізацією по користувачам і qci для міжоператорської тарифікації;
- звітування про події (зміна rat тощо) до pcrf;
- прив'язка носія висхідної та низхідної лінії до доступу 3gpp;
- перевірка прив'язки висхідної лінії зв'язку з відкиданням пакетів "неадекватного ul-трафіку";
- шлюз мобільного доступу (mag) функціонує, якщо використовується s5 або s8 на базі pmip;
- підтримка необхідних функцій для забезпечення роботи ланцюжка gtp/pmip.

5

Потік даних від генерації через GCC. Від агрегації до зберігання



6

Підрахунок даних "статистика" та "ключова змінна

Схема	Таблиці	Підсхеми	Ключові змінні	Статистика
APN	4	4	3	309
APNQCI	1	1	2	16
CARD	3	3	2	136
DCCA	2	2	4	26
DCCASCH	1	3	3	123
DIAUSCH	1	1	7	44
DISCH	1	1	1	53
DPCA	1	1	4	41

Опис даних зі схеми SGW

SGW_ID	VPN_ID	VPN_NAME	SERV_ID	SERV_NAME
CSGNMT01	6	SGW	8	SGW_SVC
GGCF01	4	SGW	9	SGW_SVC
GGCF02	5	SGW	9	SGW_SVC
GGCT01	14	SGW	9	SGW_SVC
GGCT03	7	SGW	9	SGW_SVC
GGCT04	3	SGW	9	SGW_SVC
GGDM01	4	SGW	9	SGW_SVC
GGDM02	3	SGW	9	SGW_SVC
GGDN01	5	SGW	9	SGW_SVC
GGDN02	9	SGW	9	SGW_SVC
GGDN03	3	SGW	9	SGW_SVC
GGJF01	4	SGW	9	SGW_SVC
GGMT01	20	SGW	11	SGW_SVC
GGMT03	7	SGW	9	SGW_SVC
GGMT04	7	SGW	9	SGW_SVC

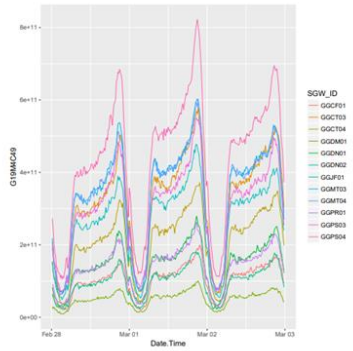


Рисунок 1 – Байти в нисхідному каналі на інтерфейсі S1U SGW

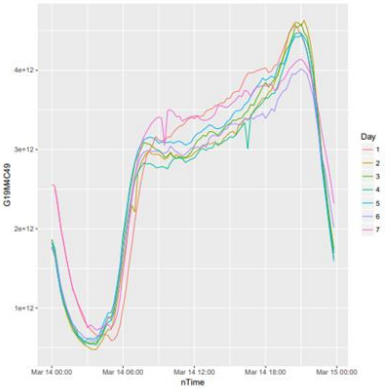


Рисунок 2 – Порівняння днів тижня

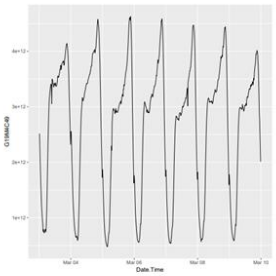
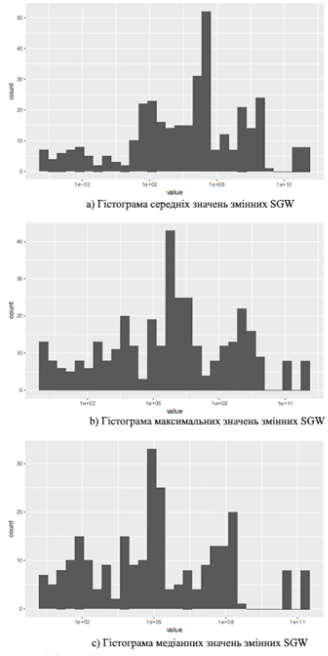


Рисунок 3 – Загальний обсяг байт S1U- за 7 днів

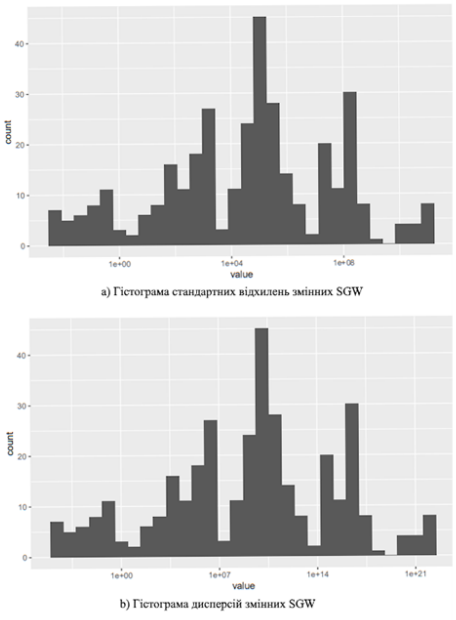


a) Гістограма середніх значень змінних SGW

b) Гістограма максимальних значень змінних SGW

c) Гістограма медіанних значень змінних SGW

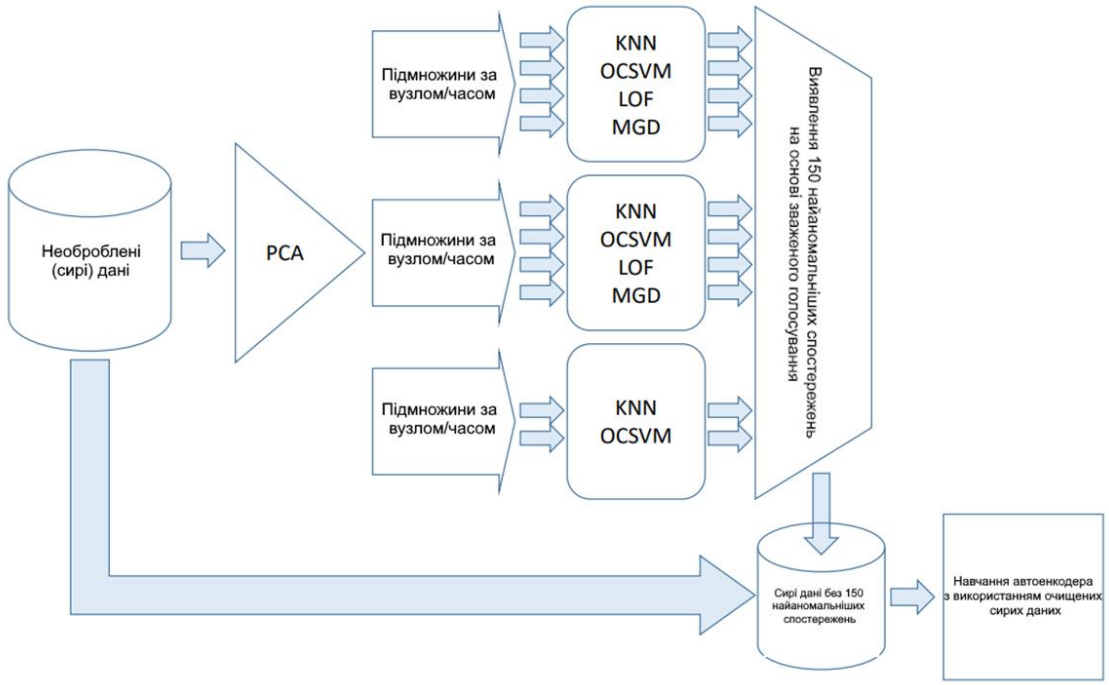
Рисунок 3 – Узагальнення даних SGW



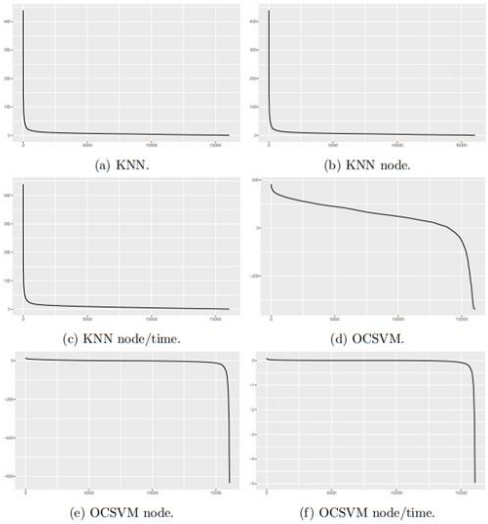
a) Гістограма стандартних відхилень змінних SGW

b) Гістограма дисперсій змінних SGW

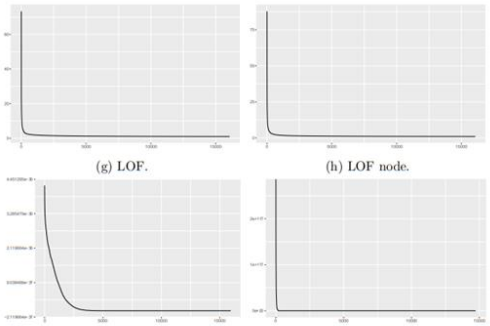
Рисунок 4 – Узагальнення даних по SGW



Впорядковані значення факторів аномальності за кожним підходом



(a) KNN. (b) KNN node. (c) KNN node/time. (d) OCSVM. (e) OCSVM node. (f) OCSVM node/time.



(g) LOF. (h) LOF node. (i) MGD. (j) MGD node.

Кількість спостережень із топ-150 кожного методу, які увійшли до остаточного списку аномалій

Метод	Відсоток у фінальній вибірці
KNN.Weight50	0,847
KNN.Node.Weight50	0,86
KNN.Node.Time.Weight8	0,8
OCSVM.ν=0.13, γ=0.002	0,818
OCSVM.Node.ν=0.5, γ=1e-04	0,8
OCSVM.Node.Time.ν=0.5, γ=1e-04	0,8
LOF.K100	0,687
LOF.Node.K100	0,647
MGD.Node	0,507
MGD	0,987

13

Навчання напівкерованого автоенкодера

Розподіл даних:
•Тренувальний набір: **80%**
•Валідаційний набір: **10%**
•Тестовий набір: **10%**
Результати навчання:
•**MSE після 1 епохи**: 0,001
•**MSE після 4,8 епохи**: 0,0008 (тренувальний та валідаційний набори)
Аналіз важливості змінних:
•**665 змінних** незначущі (в основному — лише нулі)
•**493 змінні** мали невеликий, але внесок:

- Найважливіша змінна: **Time.4:30** – 0,2393%
- Найменш важлива: **G19M4C8** – 0,1749%

•**Загальний висновок:** усі змінні певною мірою впливають на модель
Додатково:
•**Найменш важливі групи**: лічильники
•**Найважливіша група**: змінні, пов’язані з **часом доби**

14

Висновки

В кваліфікаційній роботі було представлено підхід для виявлення аномалій у високовимірних даних SGW у мобільному мережевому середовищі. Цей підхід доповнює існуючу модельну методику, яка виявляє деградації у заздалегідь визначених ключових показниках ефективності (KPI). Підхід виявлення аномалій заповнює «сліпу пляму», що залишилась у поточній методиці, охоплюючи всі лічильники. Було продемонстровано здатність цього підходу виявляти аномалії, що впливають на багатьох абонентів і лічильників,

Аномалії, виділені цим підходом, лише вказують на зміни від цієї базової лінії. Зміни можуть відображати як погіршення, так і покращення роботи мережі. Для визначення цього та з'ясування деталей змін потрібне подальше дослідження мобільної мережі. На жаль, чорний ящик кінцевого автоенкодера не надає користувачу допомоги у таких дослідженнях.

Апробація результатів: МАРТОВИЦЬКИЙ, В., СВИРИДОВ, А., АВДЄЄВ, О., ГУДЗИНСЬКИЙ, І., & КОРОТЕЦЬКИЙ, О. ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У API ЖУРНАЛАХ. Вісник Херсонського національного технічного університету, 2(1 (92)), С. 142-148.