Міністерство освіти і науки України
Харківського національного університету імені В.Н. Каразіна
Навчально-наукового інституту комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Безпека інформаційних і комунікаційних систем»

В.о. зав. кафедрою КІСМТ
Марина ЄСІНА
"Допущено до захисту"

" " _____2024р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Методи та засоби побудови web-ресурсу для захищеної A-GPS»

оцінка «_____ »

Голова ЕК

Лемешко О.В.

Керівник: к. т. н., доцент
Нарєжній Олексій Павлович

Рецензент: к. т. н., старш. викл.
Лисицький Костянтин Євгенійович

Виконавець: студент групи КБ-61
Андрєєв Ярослав Юрійович

Харків – 2024

РЕФЕРАТ

Пояснювальна записка до проєкту магістра містить 65 сторінок, 17 рисунків, 4 таблиці, 5 додатків, 72 посилання на джерела.

Мета дослідження полягає в розробці та впровадженні інноваційного web-ресурсу, який би сприяв покращенню безпеки, надійності та ефективності системи A-GPS, а також валідації та тестування розробленого web-ресурсу.

Об'єктом дослідження – проблема захисту GPS-даних, можливі шляхи її вирішення та наслідки у разі недотримання стандартів кібербезпеки та методологій розробки.

Предметом дослідження – застосування методів побудови A-GPS web-ресурсу та методологій розробки під час імплементації частини цієї системи– клієнтської частини.

Основними методами дослідження дослідження є аналіз сучасних рішень, аналіз існуючих загроз та методів протидії, порівняння методів захисту та вибір найбільш актуального з них в умовах воєнного стану, аналіз методологій розробки web-ресурсів, емпіричні методи, зокрема розробка клієнтської частини системи з подальшим тестуванням.

У роботі досліджено: особливості A-GPS технології, проблематику спуфінг-атак та можливих протидій, доцільність і особливості розробки web-ресурсу для захищеної A-GPS для державних і військових установ та підприємства, об’єктів критичної інфраструктури, що використовують GPS-дані для своєї роботи.

Результати роботи можуть бути використані у різних наукових виданнях, під час викладання у ЗВО відповідного профілю, а розроблений застосунок – для захищеної передачі GPS-даних.

Ключові слова: ВЕБРЕСУРС, СПУФІНГ-АТАКА, A-GPS, КРИПТОСТІЙКІСТЬ, ГЕОЛОКАЦІЯ.

ABSTRACT

The explanatory note to the master's project contains 65 pages, 17 drawings, 4 tables, 5 annexes, 72 references to sources.

The purpose of the study is to develop and implement an innovative web resource that would improve the safety, reliability and efficiency of the A-GPS system, as well as validation and testing of the developed web resource.

The object of the study is the problem of protecting GPS data, possible solutions and consequences in case of non-compliance with cybersecurity standards and development methodologies.

The subject of research is the use of methods for building an A-GPS web resource and development methodologies during the implementation of part of this system−the client part.

The main methods of research are the analysis of modern solutions, analysis of existing threats and methods of counteraction, comparison of methods of protection and selection of the most relevant of them under martial law, analysis of methodologies for the development of web-resources, empirical methods, in particular the development of the client part of the system with subsequent testing.

The research explore: peculiarities of A-GPS technology, problems of spoofing attacks and possible counteractions, expediency and peculiarities of development of a web-resource for protected A-GPS for state and military institutions and enterprise, objects of critical infrastructure that use GPS data for their work.

The results of the work can be used in various scientific publications, when teaching the appropriate profile in the HEI, and the developed application for the secure transmission of GPS data.

Key words: WEB RESOURCE, SPOOFING ATTACK, A-GPS, CRYPTOGRAPHIC RESILIENCE, GEOLOCATION.

ЗМІСТ

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ

A-GPS – Assisted Global Positioning System

AGC – automatic gain control

ADC – analog-to-digital converter

INS – inertial navigation system

GNSS – Global Navigation Satellite Systems

PSD – power spectral density

ВСТУП

Сучасний світ зазнає непередбачуваних змін, а однією з головних ділянок цих трансформацій є розширення та інтеграція глобальних навігаційних систем. Геопросторові дані та локальні сервіси стають необхідними складовими сучасного життя, від навігації великогабаритних транспортних засобів до миттєвого визначення місця розташування друзів на смартфоні. Однак споживачі цих послуг, а також сектори, де вони використовуються, стикаються з викликами, пов'язаними з точністю та безпекою.

Захищена A-GPS (Assisted Global Positioning System) – це один із підходів, який спрямований на покращення точності та безпеки глобальної навігації. Ця технологія поєднує в собі використання супутників, наземних станцій, інтернет-серверів та спеціалізованих алгоритмів, щоб забезпечити швидке та точне визначення місцезнаходження користувача. Однак реалізація цієї технології на практиці вимагає створення спеціалізованих web-ресурсів, які можуть обробляти та забезпечувати доступ до цих даних.

Ця магістерська робота присвячена дослідженню та розробці методів та засобів для побудови web-ресурсу для захищеної A-GPS. Метою роботи є розробка та імплементація web-ресурсу, який буде не лише забезпечувати доступ до A-GPS даних, але й гарантувати їх безпеку та надійність. Використовуючи сучасні технології та методи, ми спробуємо вирішити складні завдання, пов'язані із захищеною навігацією та обробкою геопросторових даних.

У вступі ми визначимо актуальність теми, сформулюємо завдання роботи, та обґрунтуємо структуру магістерської роботи. Далі в роботі будуть розглянуті питання теорії та практики, а також викладено результати досліджень та розробок, які сприятимуть подальшому розвитку та вдосконаленню систем захищеної A-GPS.

1 СПЕЦИФІКА A-GPS ТЕХНОЛОГІЇ ТА МЕТОДІВ ЗАХИСТУ ВІД СПУФІНГУ

1.1 Огляд A-GPS технології

A-GPS, або Assisted Global Positioning System, представляє собою покращену версію традиційної системи глобального позиціонування (GPS). Ця технологія була розроблена для вдосконалення точності та швидкості визначення місцезнаходження користувачів, особливо в умовах обмеженого доступу до супутникових сигналів, які можуть бути заблоковані географічними перешкодами або слабким сигналом. Основні особливості A-GPS технології включають полягають у наявності таких позицій:

Супутниковий сигнал та допоміжні дані. У стандартному GPS отримання супутникових сигналів і їх обробка можуть займати багато часу, особливо при холодному запуску (коли немає збережених даних). A-GPS використовує додаткові допоміжні дані, що включають інформацію про супутникові сигнали, щоб прискорити цей процес.

Спеціалізовані сервери. A-GPS вимагає звертання до спеціалізованих серверів для отримання допоміжних даних. Ці сервери містять інформацію про стан супутників, їхні орбіти та інші параметри, які допомагають визначити місцезнаходження користувача.

Короткий час ініціалізації. Однією з головних переваг A-GPS є можливість швидко визначити місцезнаходження навіть при слабкому сигналі або в умовах, коли супутникові сигнали блокуються. Це особливо важливо в сучасних мобільних пристроях, де швидкість та точність визначення місцезнаходження відіграє важливу роль.

Підтримка мультиплатформеності. A-GPS може бути використаний на різних типах пристроїв, включаючи смартфони, автомобільні системи навігації

та інші. Це дозволяє розширити можливості визначення місцезнаходження для різних застосувань.

Забезпечення безпеки та конфіденційності. Однією з важливих аспектів A-GPS технології є забезпечення конфіденційності та безпеки користувача, особливо при передачі особистої геолокаційної інформації через мережу.

A-GPS технологія є важливим кроком у розвитку систем глобального позиціонування, яка дозволяє отримувати більш точні та швидкі результати визначення місцезнаходження. Ця технологія має широкий спектр застосувань, від навігації великогабаритних транспортних засобів до розробки мобільних додатків, які використовують геопросторові дані. У наступних розділах магістерської роботи буде розглянуто більше деталей щодо методів та засобів побудови web-ресурсу для захищеної A-GPS та способів забезпечення безпеки та надійності цієї технології.

У магістерській роботі будуть розглянуті різні аспекти A-GPS технології, включаючи теоретичний аналіз методів позиціонування, використання допоміжних даних та спеціалізованих серверів. Крім того, ми дослідимо методи забезпечення конфіденційності та безпеки в межах цієї технології, оскільки це надзвичайно важливо для використання геолокаційних даних у різних сферах, включаючи медицину, транспорт, телекомунікації та інші.

У контексті практичної частини магістерської роботи ми зосередимося на розробці та імплементації власного вебресурсу для захищеної A-GPS. Ця частина роботи включатиме архітектурне проєктування, розробку серверної та клієнтської частин, а також забезпечення безпеки та конфіденційності даних, що обробляються ресурсом.

Завданням роботи буде створення інтерактивного та високоефективного вебдодатку, який забезпечить швидкий доступ до A-GPS даних, надійність та безпеку, а також зручність використання для кінцевих користувачів. Додатково,

робота буде включати в себе тестування та оцінку розробленого ресурсу на різних платформах та в різних умовах використання.

У висновках магістерської роботи ми підсумуємо отримані результати та висвітлимо їх значущість для практики та подальших досліджень у галузі A-GPS технології. Робота також міститиме рекомендації щодо можливого використання розробленого вебресурсу та напрямків подальшого розвитку в цьому напрямку.

1.2 Виділення основних проблем та викликів, пов'язаних з захищеною A-GPS

Хоча GPS широко використовується в різних як цивільних, так і військових системах, вона не є безпечною. Тобто цивільні (публічні) GPS-сигнали, які надсилаються супутниками, не проходять аутентифікацію та не шифруються. У результаті літаки та БПЛА стають вразливими до атак на підробку GPS-сигналів, коли зловмисник передає сигнали, схожі на супутникові, але з вищою потужністю та, можливо, з дещо іншими затримками в часі. GPS-приймач літака підключається до підробленого сигналу, оскільки він надходить із вищою потужністю, ніж справжні сигнали.

Шляхом вибіркової зміни часових зсувів підроблених супутникових сигналів зловмисники можуть імітувати довільні позиції. Ці види атак добре відомі [31], [51], [63] і були підтверджені в реальних умовах [26], [27]. Насправді вважається, що підробка GPS використовувалася для перехоплення безпілотника-стелса ЦРУ (RQ-170) в Ірані у 2011 році [52] або для збивання кораблів із курсу [48], [5]. Крім того, підробка GPS використовувалася як захист від БПЛА, контрольованих GPS, які літали поблизу Кремля в Росії [57].

З роками ціна на виконання атак підробки GPS значно знизилася. Комерційні портативні пристрої для підробки GPS доступні менш ніж за $1,000 [48], а загальнодоступні програмні інструменти [46] дозволяють генерувати довільні GPS-сигнали. Падіння цін і низькі вимоги до технічної підготовки

підвищують ризик для застосувань, які покладаються на GPS для ухвалення критично важливих рішень або виконання безпечних процесів. Одним з найпоширенішим видом вразливостей є спуфінг атаки.

GPS спуфінг-атаки використовують відсутність шифрування та аутентифікації в цивільних GPS-сигналах, імітуючи легітимні сигнали з метою зміни результатів локалізації або часу у жертви [25], [63], [62]. Технічно такі атаки базуються на підроблених GPS-сигналах, які маніпулюють часом надходження сигналів (ToA), але використовують те саме корисне навантаження, що й справжні сигнали.

У минулому були зафіксовані інциденти [48], [31], [51], [63], коли спуфери успішно порушували цілісність систем, які залежать від GPS, що підтверджує реальність загрози GPS спуфінг атак. У результаті сучасні дрони, літаки, вертольоти або будь-які транспортні засоби, що покладаються на GPS, є вразливими до спуфінг атак і не мають ефективних засобів протидії.

GPS Spoof атаки можуть використовувати пристрої, які знаходяться поруч з приймачем жертви або на відстані від нього. Якщо вони знаходяться на відстані, то можуть отримувати реальні сигнали від видимих супутників GPS через свою приймальну антену RX. Запропонований на (рис. 1.1) варіант спуферу у випадку успішної атаки, генерує фальшивий сигнал для кожного отримуваного реального сигналу і надсилає їх на антену БПЛА, з урахуванням що кожен надісланий сигнал вирівнюється за кодовою фазою з реальним аналогом.

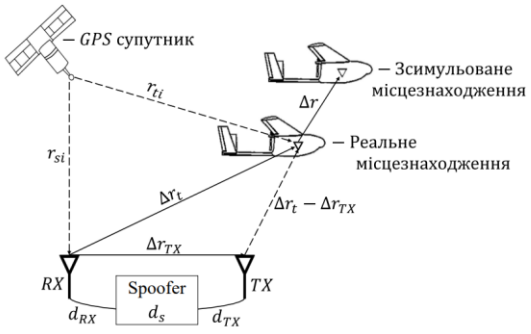


Рис. 1.1 – Зображення елементів що задіяні в процесі здійснення атаки з підробкою навігаційних GPS сигналів [43]

Після перехоплення опорних частот та фаз приймача на безпілотнику, спуфер регулює фази своїх сигналів так, щоб змусити передавач на БПЛА повідомляти змодельоване значення $\triangle r$ відносно реального місцезнаходження. До того ж часовий зсув цього приймача також корегується зміщенням фаз фальшивого коду. Варто відзначити, що атака такого типу може бути успішною тільки у випадку, якщо спуфер компенсує затримки при отриманні та передачі сигналу, створюючи передбачувану версію сигналів. У цивільних GPS сигналах така компенсація затримки є досить простою, оскільки отримувані дані не зашифровані, супутники рухаються по стандартним орбітам, а модульовані дані навігації відповідають стандартним шаблонам. Однак, військові сигнали зазвичай зашифровані, оскільки непередбачуваність їх дій є основою їх безпеки. На приклад для деякого і-го супутнику, така системна затримка, що має компенсуватись, визначається за формулою (1.1)

$$cd_i = r_{si} - r_{ti} + c(d_{RX} + d_{TX} + d_s) + ||\triangle r_t - \triangle r_{TX}|| \qquad (1.1)$$

де dRX та $dT\ X$ – це затримки на приймальномута передавальному кабелях; ds – затримка обробки сигналу спуфером; c – швидкість світла; Тут діапазони rsi

та rti розраховуються за допомогою таблиці Ефемерид, якщо спуферу відомо розташування приймальної антени та відносні координати цілі $\triangle rt$;

Затримки dRX та $dT\ X$ – обчислюються точно лише в випадку достовірних даних про довжину і тип кабелів; Затримка ж ds – є складнішою, адже джерелом її виникнення є недетермінована затримка буферизації під час увімкнення. Щоб зсимулювати свою версію сигналів і-го супутника, спуфер прогнозує для кожного з отриманих сигналів три величини з великою точністю:

- Значення модульованих навігаційних даних;
- Доплерівський зсув частот;
- Зміщення фази.

Такі точні прогнози можливі лише в випадку точної інформації про положення та швидкість супутника. Навігаційна система вважається захопленою, коли спуфер може контролювати 6-вимірну оцінку
позиції та швидкості (1.2):

$$\hat{x} = [\hat{r}^T, \hat{v}^T]^T PV \tag{1.2}$$

Тобто це означає, що під контролем розуміється ситуація, коли спуфер змушує значення $\hat{x}$ відповідати значенню $x\star$, що встановлене ним же, з точністю стандартної служби позиціювання GPS SPS, котра на цей час перевищує 3 м і 10 см/с швидкості, коли приймач має доступ до поправок із супутникової системи, наприклад – системи поширення поправок до даних WAAS.

1.2 Аналіз методів та засобів для захисту від спуфінг-атак

Демократизація технологій підробки GPS спонукала до розробки різних заходів протидії, які можна грубо поділити на три класи: (i) криптографічні методи, (ii) виявлення на рівні сигналу та (iii) визначення напрямку надходження сигналу. Криптографічні методи спрямовані на аутентифікацію сигналів від

супутників за допомогою додаткових сигналів, які неможливо передбачити користувачам, які не володіють секретним ключем. Однак ці методи не захищені від повторних атак і потребуватимуть дорогого оновлення GPS-інфраструктури. Виявлення підробки на рівні сигналу базується або на перевірках аномалій у фізичній формі сигналу , або на вимірюванні кута прибуття сигналу Хоча ці методи не потребують змін у структурі GPS-сигналів, вони накладають зміни на існуючі приймачі та збільшують складність і обчислювальні вимоги до цих пристроїв. Техніки захисту від Spoof атак полягають у виявленні атак та відновленні реальної позиції БПЛА. Уникнути відновлення навігації можливо у двох випадках: Перший - коли сигнали повністю знищені. Другий - коли спуфер використовується з високою потужністю, що глушить справжні сигнали настільки, що відновлення їх стає неможливим, особливо, якщо спуфер також захоплює радіочастотний інтерфейс жертви. Стратегії виявлення підробки базуються на двох методах: Пошук відмінностей між підробленими та справжніми сигналами і пошук взаємозв’язку між ними. Зазвичай кращі стратегії поєднують моніторинг потужності з певною формою моніторингу взаємодії, оскільки це забезпечує більш ефективний захист від GPS спуфінг-атак [15]. Також варто звернути увагу, що пунктирні криві на графіках є фактичними атаками підміни реального сигналу. Метод можна оптимізувати шляхом нанесення фактичних атак на графіки відповідних періодів часу в які здійснюється атака. Це дозволить виявити спотворення у лівій частині графіка на (рис. 1.2), залежно від зміщення фази коду.

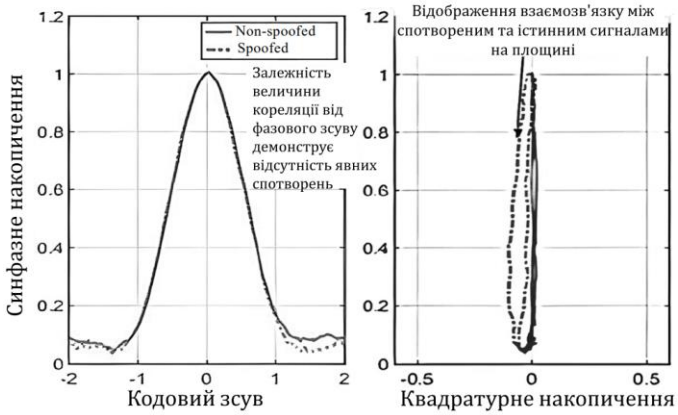


Рис. 1.2 — Два види комплексної кореляції без спотворення (суцільна лінія) та зі спотворенням (пунктирна лінія) [43].

1.2.1 Захист шляхом шифрування сигналів

Одним із методів захисту БПЛА від GPS спуфінг атак є шифрування сигналів, що передаються [43], для ускладнення їх підміни та копіювання. Найефективнішим методом є застосування симетричного ключа з повним кодом розповсюдження $Ci\,(t)$, коли супутник та приймач мають копії секретного ключа. Цей метод вимагає конфіденційного розповсюдження ключів серед пристроїв, що одержують сигнал, тому є досить громіздким у використанні.

Для виявлення підміни в приймачах без необхідності доступу до секретного ключа, можна застосувати сигнали, зашифровані симетричним ключем.Замість розповсюдження ключів одержувачам використовується публічний зв’язок відкритого коду зашифрованим кодом. Приймач використовує свою систему відстеження кодів для запису версії зашифрованого коду в базовому діапазоні. Це дозволяє виявляти підміну сигналу на приймачі потенційної жертви та інших захищених пристроях. Для цього дві версії зашифрованого коду взаємно корелюються для пошуку піка кореляції, який існує тільки в випадку, якщо сигнал потенційної жертви є реальним. Якщо пік кореляції високий, то сигнал є справжнім, в іншому випадку викликається сигнал

тривоги. Цей метод може працювати постфактум або майже в режимі реального часу, проте його ефективність залежить від пропускної здатності лінії зв’язку

1.2.2 Захист заснований на методах моніторингу дрейфу тактової частоти

Ці методи захисту виявляють незвичні зміни у позиції приймача або значенні годинника, що можуть бути викликані дією спуфера. Якщо спуфер прискорено змінює тактову частоту приймача, то приймач може виявити, що швидкість дрейфу тактової частоти, тобто її зміна, перевищує нормальні межі для його класу генератора. Залежно від класу генератора, спуфер повинен діяти все більш обережно. Наприклад, для кварцових, рубідієвих або водневих генераторів і т.д. Для виявлення підробки можна також використовувати інерційний вимірювальний пристрій (IMU) або інший датчик руху, щоб встановити аналогічні обмеження на швидкість дрейфу. Якщо будуть виявлені незвичайні дії, приймач жертви видаватиме сигнал тривоги Засоби захисту, засновані на моніторингу дрейфу, можуть бути ефективними проти атак з аналізом та відтворенням коду безпеки (SCER Spoofing Attacks), які обмежені затримкою підробки $\tau si(t) > \tau i\ (t)$ для всіх $i = 1, \ldots, N$. Фальсифікатор спуфера може спробувати уникнути виявлення моніторингом дрейфу, повільно створюючи помилкові значення положення. Проте, навіть такий підхід може зробити спуфер вразливим до виявлення іншими методами. Якщо підроблені сигнали будуть затримуватись відносно реальних сигналів на мінімальну величину, то спуфер не зможе одночасно підтримувати низький початковий зсув тактової частоти та позиції. Це може призвести до значних змін показників на приймачі жертви, що дозволяє йому виявити атаку.

1.2.3 Захист з використанням геометричного подання сигналів

Цей тип захисту полягає в відстеженні напрямку приходу сигналів на приймач і врахуванні фази опорної частоти биття цих сигналів (1.3), що моделюється як [43].

$$\frac{\lambda\phi_i}{2\pi} = \rho_0^i + (\widehat{\rho^l})^T \triangle d + c(\delta_r - \delta^i) + \frac{\lambda\beta^i}{2\pi} \quad (1.3)$$

λ – довжина хвилі опорного сигналу, $\rho\ i\ 0$ – номінальна відстань до і-го супутника, $\hat{}\rho\ l$ – одиничний вектор від супутника до приймача, $\triangle d$ – величина зсуву приймальної антени від місця приймача, δr і $\delta\ i$ – відповідно зсув тактової частоти приймача і супутника, а $\beta\ i$ – невідомий зсув фази опорної частоти і-го супутника. Щоб виміряти напрямок прибуття $\hat{}\rho\ l$, можна використовувати три або більше антен з різним зсувами $\triangle d$ або одну антену, яка відслідковує рух за відомим $\triangle d(t)$. Якісно сконструйований приймач може вимірювати фазу опорної частоти биття з точністю близько 1/40-ї частини циклу, що дозволяє вимірювати напрямок з точністю близько 3 градусів, використовуючи лише зміщення антени $\triangle d$ від місця приймача на 0,1 м. На жаль спуфери, що передають сигнал з декількох напрямків таким методом виявити важче, але якщо спрямоване різноманіття не відповідає реальному пакету векторів $\hat{}\rho\ l$ – це все ще реально.

1.2.4 Захист шляхом використання метрики тестування

Одним із методів виявлення підробки є метод моніторингу якості сигналу SQM [43], який дозволяє виявити атаку на етапі відстеження шляхом моніторингу якості кореляції. Для реалізації цього методу можна використовувати метрику тестування відношення (Ratio Test), яка працює на виході кореляторів та відстежує форму кореляційної функції. Дана метрика дозволяє ефективно захистити безпілотні літальні апарати від атаки GPS Spoofing. Така метрика (1.4) буде визначена як:

$$M_1[k] = \frac{I_e[k] + I_l[k]}{\xi I_p[k]} \quad (1.4)$$

$Ie\ [k]$, $Il\ [k]$ та $Ip\ [k]$ це початкова, кінцева та швидка кореляції відповідно, а ξ – це постійний коефіцієнт, що представляє кутовий нахил кореляційної

функції. Вже після того як метрика була розрахована необхідно визначити чи здійснюється атака. Один із можливих методів є використання детектора Неймана-Пірсона, який реалізує перевірку двох гіпотез і вибір між ними. Першою є гіпотеза лише про перший сигнал - $H0$, а другою гіпотеза про заміну справжнього сигналу - $H1$ (1.5). Сформулювати її можна як:

$$\mu_1[k] = \begin{cases} \mu_{1,0} \rightarrow H_0 \\ \mu_{1,1} \rightarrow H_1 \end{cases} \quad (1.5)$$

Загалом ми можемо стверджувати, що атака здійснюється і є достатньо успішною, якщо спотворення кореляційної функції досягає чітко визначених значень на початковому етапі атаки, що б розблокувати реальні сигнали. $\mu 1,1$ також може бути визначено на основі моделі сигналу прийнятого для підміни.

2 ПОСТАНОВКА ЗАВДАННЯ, ЦІЛІ РОБОТИ, МЕТОДОЛОГІЯ

2.1 Формулювання конкретної мети магістерської роботи

Мета магістерської роботи "Методи та засоби побудови web-ресурсу для захищеної A-GPS" полягає в розробці та впровадженні інноваційного web-ресурсу, який би сприяв покращенню безпеки, надійності та ефективності системи A-GPS.

Конкретною метою роботи є розробити та налагодити web-ресурс для захищеної A-GPS технології, який би забезпечував надійну обробку та зберігання геолокаційних даних, забезпечував конфіденційність та захист даних користувачів, а також сприяв оптимізації використання ресурсів та покращенню якості геолокаційних послуг.

Ця мета вимагає дослідження сучасних методів та інструментів забезпечення безпеки та надійності A-GPS технології, розробки відповідних алгоритмів та програмного забезпечення, а також валідації та тестування розробленого web-ресурсу. Робота магістра має на меті внести вагомий внесок в розвиток захищеної A-GPS технології та забезпечити користувачів надійними та безпечними геолокаційними рішеннями.

2.2. Визначення основних завдань та цілей

Основні завдання та цілі магістерської роботи "Методи та засоби побудови web-ресурсу для захищеної A-GPS" визначаються для досягнення загальної мети роботи. Основні завдання:

1) Аналіз сучасних методів та засобів захищеної A-GPS технології: Провести огляд і аналіз існуючих методів та засобів, включаючи архітектуру, алгоритми та технічні рішення, що застосовуються в системах A-GPS.

2) Розробка та реалізація web-ресурсу: Розробити web-ресурс, який би забезпечував можливість взаємодії з A-GPS технологією, обробку та збереження геолокаційних даних, а також забезпечував конфіденційність і безпеку даних користувачів.

3) Оптимізація використання ресурсів та ефективність системи: Розробити методи та рішення для оптимізації використання ресурсів, включаючи мережеву пропускну здатність та обчислювальні ресурси, з метою підвищення ефективності системи A-GPS.

4) Валідація та тестування розробленого web-ресурсу: Провести валідацію та тестування розробленого web-ресурсу для підтвердження його працездатності, безпеки та надійності.

Основні цілі:

1) Забезпечити безпеку та конфіденційність даних: Розробити web-ресурс, який би забезпечував високий рівень безпеки та конфіденційності геолокаційних даних користувачів.

2) Покращити надійність та якість геолокаційних послуг: Забезпечити надійну та високоякісну роботу системи A-GPS через оптимізацію процесів та методів обробки даних.

3) Забезпечити оптимізацію використання ресурсів: Зменшити споживання мережевої пропускної здатності та енергії на мобільних пристроях для поліпшення ефективності та зручності використання A-GPS.

4) Забезпечити користувачам доступ до безпечних та надійних геолокаційних послуг: Забезпечити користувачам можливість використовувати A-GPS технологію з високим рівнем довіри до безпеки та конфіденційності своїх даних.

5) Створити інноваційний web-ресурс для захищеної A-GPS технології: Розробити інноваційний та конкурентоспроможний web-ресурс, який би відповідав сучасним вимогам і використовував передові технології та методи.

Ці завдання та цілі допоможуть досягти мети магістерської роботи та сприяти розвитку безпечної та ефективної A-GPS технології.

2.3 Опис використовуваних методів дослідження

У магістерській роботі будуть використовуватися такі методи дослідження, які, на нашу думку, якнайкраще забезпечують досягнення поставлених завдань і цілей. А саме:

1) Літературний аналіз. Метод літературного аналізу передбачає огляд наукової літератури, статей, публікацій та документації, що стосуються A-GPS технології, методів захисту та технічних рішень. Цей метод допоможе отримати фундаментальні знання про сучасний стан галузі та розробити теоретичну основу для роботи.

2) Аналіз методів та інструментів розробки web-ресурсу. Дослідження різних методів та інструментів, що використовуються для створення web-ресурсів, включаючи мови програмування, фреймворки, бази даних, інструменти розробки, допоможе вибрати найбільш відповідні технології для реалізації web-ресурсу.

3) Емпіричні дослідження та експерименти. Для валідації розробленого web-ресурсу та оцінки його ефективності та безпеки будуть проводитися експерименти та тестування. Це включає в себе тестування на справжніх пристроях та симуляторах, а також аналіз результатів та порівняння їх з очікуваними показниками.

4) Аналіз даних та статистика. Для обробки результатів експериментів та валідації web-ресурсу будуть використовуватися методи аналізу даних та статистики. Це допоможе визначити статистичну достовірність та важливі взаємозв'язки.

5) Дослідження та аналіз сучасних підходів до захисту даних. Для розробки методів та засобів забезпечення безпеки використовуватимуться аналіз сучасних підходів до захисту геолокаційних даних та конфіденційності користувачів.

6) Експертні опитування і консультації. Для отримання експертних думок та рекомендацій будуть проведені експертні опитування та консультації з фахівцями в галузі A-GPS технології, кібербезпеки та розробки web-ресурсів.

7) Практична реалізація web-ресурсу. Сама розробка та реалізація web-ресурсу буде єдиною з методів дослідження, оскільки це дозволить використовувати практичні навички та знання для створення інноваційного ресурсу.

3 ВИКОРИСТАНІ ЗАСОБИ ЗАХИСТУ ПРИ СТВОРЕННІ WEB-РЕСУРСУ

3.1 Виявлення GPS-спуфінгу

Виявлення GPS-спуфінгу є першим кроком у стратегії протидії GPS спуфінг атакам. Моя ідея для виявлення GPS-спуфінг атак базується на транслюваних повідомленнях системи спостереження, наприклад ADS-B/Flarm, які можуть містити підроблену інформацію про позицію. Я пропоную процес перевірки, що складається з двох взаємодоповнюючих перевірок. Перша перевірка - узгодження часу передачі. Оскільки повідомлення ADS-B/Flarm транслюються у змінний час, необхідно узгодити час цих звітів, щоб зробити їх порівнюваними. Це досягається шляхом використання результатів обчислення багатолатерації (MLAT). Для узгодження звітів про позицію з глобальним еталонним часом виконуються два послідовні кроки. Перший крок визначає час передачі tTX (3.1), у який було передано позицію, отриману з GPS:

$$t_{\mathrm{TX}} = t_s - \frac{dist(s,a)}{c}, \tag{3.1}$$

де t(s) — це час, у який сенсор sss позначив повідомлення часовою міткою, dist(s, a) представляє евклідову відстань між розглянутим сенсором та літаком, а c— це швидкість світла. Другим кроком є інтерполяція для наближення позиції об’єкта aREF до глобального еталонного часу tREF (3.2). Необхідно врахувати такі три випадки:

$$a_{\mathrm{REF}} = \begin{cases} \frac{a_{\mathrm{TX}} \cdot (t_{\mathrm{TX}+1} - t_{\mathrm{REF}}) + a_{\mathrm{TX}+1} \cdot (t_{\mathrm{REF}} - t_{\mathrm{TX}})}{t_{\mathrm{TX}+1} - t_{\mathrm{TX}}} & t_{\mathrm{TX}} < t_{\mathrm{REF}} \\ a_{\mathrm{TX}} & t_{\mathrm{TX}} = t_{\mathrm{REF}} \\ \frac{a_{\mathrm{TX}} \cdot (t_{\mathrm{REF}} - t_{\mathrm{TX}-1}) + a_{\mathrm{TX}-1} \cdot (t_{\mathrm{TX}} - t_{\mathrm{REF}})}{t_{\mathrm{TX}} - t_{\mathrm{TX}-1}} & t_{\mathrm{TX}} > t_{\mathrm{REF}} \end{cases} \tag{3.2}$$

aTX = ˆa, що позначає позицію летючого пристрою в момент передачі, TX−1, TX, та TX+1, які відповідають попередній, поточній та наступній події передачі відповідно. Після цієї інтерполяції всі передані позиції узгоджуються за часом і можуть порівнюватися на основі однієї часової бази. У подальшій частині роботи я припускаю, що позиції узгоджені за часом. Друга перевірка - перехресна перевірка з MLAT. Я пропоную виконати перехресну перевірку між переданими позиціями та оціненими реальними позиціями, отриманими за допомогою підходу MLAT (3.3). Ми перевіряємо для кожного отриманого звіту про позицію, чи

$$dist(a_i, \hat{a}_i) \overset{?}{<} \mathcal{T}_1 \tag{3.3}$$

виконується, де ai — реальна позиція літака i, визначена за допомогою MLAT, aˆi — позиція, передана літаком i через ADS-B/Flarm, dist() — функція Евклідової відстані, а T1 — заздалегідь визначений поріг, який враховує похибки вимірювання у ai та aˆi. Вибір правильного порогу T1 залежить від точності вторинного методу локалізації (у цьому випадку MLAT). Менші T1 призводять до вищого рівня хибних спрацьовувань, тоді як більші T1 створюють більше можливостей для непомічених маніпуляцій.

3.2 Використані рішення для захисту від спуфінг-атак

Було зазначено, що багато стратегій виявлення підміни можуть мати свої слабкі місця, які можуть бути використані нападником. Однак, якщо використовувати кілька стратегій одночасно, які взаємодоповнюють одна одну, це може стати потужним інструментом для виявлення підробки. Наприклад, для уникнення очевидного спотворення кореляційної функції під час підміни, спуфер може використати $Asi \gg Ai$, як показано на (рис. 1.2).

Проте, якщо система захисту від підробки використовує таку кореляцію на кількох етапах моніторингу отриманої потужності, то вона може виявити початок атаки незалежно від того, скільки енергії використовує спуфер. Крім того, якщо відстежувати швидкість дрейфу тактових значень та положення, то спуфер буде вимушений виконувати повільне відключення, що дозволить жертві приймачу більше часу на виявлення спотворення кореляційної функції. Ще однією ефективною комбінацією стратегій може стати використання так званих ”непередбачуваних” бітів даних (NMA), моніторинг спотворення цих бітів та зсув тактових імпульсів. Ці методи можуть змусити спуфер починати свою атаку повільно, щоб уникнути виявлення через значні зміни в положенні. Це обмеження допоможе запобігти накопиченню небезпечних похибок в положенні приймача під час очікування підробки на основі NMA. Якщо ж спуфер вирішить використовувати атаку SCER [43], щоб аналізувати та відтворити непередбачувані біти NMA, жертва зможе виявити початкові похибку цих бітів завдяки моніторингу зсуву тактових імпульсів, який обмежить початкову здатність спуфера використовувати затримку, що дозволяє надійно оцінити біт до початку його трансляції.

Перший засіб — симетричне шифрування без розповсюдження ключів. Сигнали GNSS із симетричним шифруванням можна використовувати для виявлення спуфінгу в цивільних приймачах без доступу до секретного ключа [35]. Замість розповсюдження ключів серед цивільних приймачів, використовується відома залежність між відкритим цивільним кодом розгортання та зашифрованим військовим кодом, наприклад:

1) У GPS ці коди модуляційно накладаються на одну і ту саму несучу хвилю.

2) Приймач записує зашумлену базову версію зашифрованого коду, використовуючи цивільну систему відстеження коду.

3) Потім ці сигнали порівнюються з записами іншого приймача, який точно не піддавався атакам спуфінгу.

Під час крос-кореляції двох версій зашифрованого коду перевіряється наявність кореляційного піку. Якщо пік високий, сигнали вважаються справжніми, інакше подається сигнал тривоги про спуфінг. Ця система може працювати в режимі офлайн або майже в реальному часі, якщо між приймачами є високошвидкісний канал зв’язку.

Другий засіб — затримане симетричне шифрування (SSSC). Цей метод забезпечує захист цивільних приймачів за рахунок комбінації коротких сегментів шифрованого розгортання із довгими передбачуваними сегментами Ci(t) [35] . Цей підхід забезпечує високий рівень автентифікації сигналу, але має суттєву затримку виявлення, яка може тривати від секунд до хвилин.

Третій засіб — асиметричний підхід із закритими/відкритими ключам. Асиметричний підхід забезпечує ще один спосіб використання шифрування для виявлення атак спуфінгу на відкриті GNSS-системи.

1) У цьому підході частина переданого потоку даних Di(t) містить цифровий підпис, згенерований закритим ключем контрольного сегмента.

2) Цей підпис використовується для підписання решти даних у Di(t).

3) Приймач знає, де шукати ці біти в демодульованому потоці даних, і після збору необхідного обсягу даних перевіряє підпис за допомогою відомого відкритого ключа.

Цей метод, відомий як Навігаційна автентифікація повідомлень (NMA) [35], також передбачає затримку через необхідність збору достатньо довгого цифрового підпису. Затримка залежить від довжини підпису та обмежень кількості доступних бітів у потоці даних Di(t).

Методи затриманого симетричного шифрування (SSSC) і асиметричного підходу (NMA) забезпечують високу автентифікацію GNSS-сигналів, але обидва мають затримки, які обмежують їх застосування в реальному часі. Незважаючи на ці недоліки, ці підходи, нам мій погляд, є вдалими елементами захисту від сучасних атак спуфінгу

4 РОЗРОБКА ТА ІМПЛЕМЕНТАЦІЯ КЛІЄНТСЬКОЇ ЧАСТИНИ WEB-РЕСУРСУ

4.1 Архітектура web-ресурсу для захищеної A-GPS

Розглянута архітектура наведена у додатку А. Архітектура web-ресурсу для захищеної A-GPS технології повинна бути добре продуманою і враховувати вимоги до безпеки, масштабованості та продуктивності. Ось загальний огляд архітектури A-GPS системи:

Серверна частина:

1) A-GPS Web-сервер представлена програмно апаратним комплексом, який включає сервер з криптомодулем, програмним генератором випадкових чисел, та REST API, який використовується для передачі даних до клієнтської частини. Кожен переданий пакет підписаний хеш-сумою за допомогою алгоритма SHA-1. Також у моїй системі сервер отримує дані від супутника за допомогою L1/CA зв’язку.

Клієнтська частина:

1) Десктоп-інтерфейс: клієнтська частина може бути реалізована у вигляді додатку для персонального комп’ютера.

2) Мобільні додатки: додатки для Android та iOS можуть надавати додатковий функціонал та зручний доступ до геолокаційних послуг.

Безпека:

1) Шифрування даних: усі дані, які передаються між клієнтом та сервером, мають бути шифрованими за допомогою протоколу HTTPS.

2) Автентифікація та авторизація: для керування доступом до функціоналу ресурсу використовується система автентифікації та авторизації. Користувачі повинні проходити автентифікацію перед доступом до особистих даних. Далі формується сесія в межах якої відбувається передача трафіку.

3) Засоби моніторингу: використання засобів моніторингу для відстеження продуктивності ресурсу, а також виявлення можливих проблем.

4) Аналітика даних: відстеження та аналіз користувацької активності, який може бути використаний для покращення функціоналу та взаємодії з користувачами.

Архітектура повинна бути розроблена так, щоб бути масштабованою та забезпечувати високу доступність. Також важливо враховувати вимоги до безпеки, включаючи захист даних, аутентифікацію та авторизацію користувачів, а також валідацію вхідних даних для запобігання можливим атакам.

Хмарні послуги: використання хмарних сервісів, таких як Amazon Web Services (AWS), Microsoft Azure або Google Cloud, може спростити керування і масштабуванням інфраструктури, забезпечуючи високу доступність та резервне копіювання даних. Також при їх використанні буде забезпечена фізична безпека, бо сервери розташовані на стороні вендора в захищених дата-центрах.

Мікросервісна архітектура: розробка за допомогою мікросервісної архітектури дозволяє розділити різні компоненти системи на окремі сервіси, що спрощує розгортання та масштабування, а також полегшує обслуговування і розвиток.

Архітектурні діаграми: створення діаграм архітектури допомагає візуалізувати різні компоненти та їх взаємозв'язок в системі, що полегшує розуміння та спілкування з командою розробки, наведена у додатку А.

Аутентифікація та авторизація: забезпечена міцну аутентифікацію користувачів на веб-ресурсі та системі A-GPS, щоб уникнути несанкціонованого доступу. Використовуйте сильні паролі та двофакторну аутентифікацію.

Захист від спуфінгу: розроблені та впроваджені заходи для захисту системи A-GPS від атак спуфінгу.

4.2 Розробка клієнтської частини

Під час дослідження було створено клієнтську частину, а саме desktop застосунок для OS Windows фрагмент коду наведено в додатку Д, інтерфейс наведено у додатку Б. Застосунок отримує дані від A-GPS сервера, виводить їх у вигляді таблиці, будує графік та записує у файл, вивід файлу наведений у додатку В. Розробка клієнтської частини складалася з наступних етапів:

1) Вибір технологій: визначення технологій для розробки клієнтської частини, включаючи вибір мови програмування для веб-додатку та платформ для мобільних додатків, було обрано операційну систему Windows та .NET Framework 4.8.1 як платформу розробки.

2) Створення інтерфейсу користувача: при створення інтерфейсу користувача було використану технологію для побудування віконного застосунку Windows Forms.

3) Взаємодія з сервером: розробка коду, який дозволяє клієнтам взаємодіяти з серверною частиною через REST API за допомогою HTTP Get запитів.

4) Безпека і автентифікація: був розроблений функціонал, що перевіряє хеш суму отриманих даних, щоб переконатися в їх цілісності.

5) Тестування та налагодження: здійснені тести для впевненості, що клієнтська частина працює коректно і забезпечує зручну взаємодію для користувачів.

Розробка серверної та клієнтської частини повинна виконуватися паралельно, з регулярними ітераціями, тестуванням та вдосконаленням функціоналу на обох сторонах. Діалог між розробниками обох частин і вирішення можливих конфліктів допомагають забезпечити сумісність та ефективну роботу системи.

5 ДОСЛІДЖЕННЯ СТРАТЕГІЙ ГЛУШІННЯ GNSS У РЕАЛЬНОМУ ЧАСІ

5.1 Глушіння, виявлення перешкод

Грубе глушіння — це акт спрямування потужної електромагнітної хвилі на приймач-жертву з наміром порушити його роботу [23]. За наявності перешкод продуктивність приймача може значно погіршитися, і в крайньому випадку пристрій-жертва не зможе працювати. У глобальних навігаційних супутникових системах (GNSS) перешкоди мають чітке значення, де жертва та зловмисник зазвичай є одним і тим же суб’єктом. Перешкоди GNSS часто використовуються задля конфіденційності [49; с. 35], щоб уникнути відстеження третіми сторонами. Проблема глушіння GNSS полягає в тому, що потужність, яку передає глушник GNSS, тобто пристрій, який використовується для генерування заважаючого електромагнітного сигналу, зазвичай необмежений. У такий спосіб зачіпається не лише призначений жертвою приймач, але також можуть бути порушені кілька інших пристроїв поблизу джерела перешкод [18].

Перешкоди є незаконними в більшості країн, і розробка методів виявлення, здатних ефективно виявляти наявність джерела перешкод, є надзвичайно важливою. Наявність перешкод можна виявити за допомогою зразків, наданих інтерфейсом SDR [60; 34], або аналізуючи вимірювання з комерційного приймача GNSS [70].

У першому випадку показники виявлення можуть бути обчислені з використанням різних принципів. Наприклад, статистичний розподіл вибірок суттєво змінюється за наявності глушіння [20, с. 2]. Таким чином, можна отримати статистику прийняття рішень на основі гістограми вхідних вибірок. Наявність аномальних спектральних компонентів у зразках також може бути використана для виявлення наявності перешкод. Нарешті, виявлення може бути

виконано проєктуванням вхідних зразків у трансформований домен, де наявність перешкод є більш очевидною. До таких доменів належать частотний, частотно-часовий [13; 6] та вейвлет-домен [40, с. 7]. Якщо зразки з інтерфейсу недоступні, можна використовувати різні спостережувані. Наприклад, значення (C/N_0) від стандартного GNSS-приймача можуть бути використані для формування статистичних даних про наявність перешкод [70, с. 6], [9, с. 4]. На додаток до значень (C/N_0), можна використовувати кілька інших спостережуваних, включаючи вимірювання GNSS [10, с. 899] і вихідні дані корелятора [42, с. 123]. Деякі приймачі GNSS також мають апаратні індикатори, які надають інформацію про стан приймача. Загальним індикатором є значення автоматичного регулювання підсилення (ARP), яке описує підсилення, яке забезпечує радіочастотний інтерфейс для аналого-цифрового перетворення сигналів на антені приймача. Аномальні значення ARP можуть вказувати на наявність перешкод [3, с. 2043].

Незважаючи на велику кількість розроблених методів виявлення, тестова діяльність, пов’язана з виявленням перешкод, як правило, обмежена тим фактом, що перешкоди є незаконними: пристрої перешкод GNSS не можуть використовуватися законно без дозволу компетентних органів. З цієї причини тестування зазвичай обмежується контрольованим середовищем, таким як великі безехові камери [7, с. 13], [9, с.4].

Перешкоди GPS та їх вплив на морську навігацію були досліджені в [21], де авторизований тест на перешкоди проводився на східному узбережжі Великобританії. Автори зазначають, що У цьому випадку для трансляції сигналу перешкод використовувалася спрямована антена. Однак у документі зосереджено увагу на впливі перешкод на морську навігацію, а виявлення перешкод не розглядається.

Експерименти також проводилися на випробувальному полігоні Vidsel у Швеції [2]. Було розглянуто два випадки: статичний і динамічний. У першому

випадку перешкоди були статичними, а передана потужність поступово збільшувалась. У другому випадку глушник переміщували навколо двох будівель. Аналіз розглядав комерційні детектори, метод на основі C/N_0 і два підходи на основі ARP. Однак надається мало інформації про розглянуті методи. Крім того, в експериментах не враховувався вплив транспортних засобів, які зазвичай використовуються для перевезення та живлення засобів перешкод [7, с. 14].

Тут описані експериментальні результати, отримані під час тестової кампанії глушіння, проведеної у віддаленій місцевості поблизу міста Броди Львівської області. І в основному були зосереджені на застосуванні на дорогах, тобто на сценаріях, коли глушники перевозяться транспортним засобом. Основною метою випробувань була перевірка здатності детекторів перешкод виявляти наявність перешкод з урахуванням зіткнення транспортного засобу, що проїжджав по дорозі з різною швидкістю. Цей аналіз корисний у випадках, коли органи влади намагаються виявити та оштрафувати водіїв, які використовують незаконні перешкоди. У цьому випадку детектори перешкод розміщуються на узбіччях у конфігурації, подібній до тієї, що зараз використовується на радарах. Було проведено серію експериментів, під час яких пристрій перешкод залишався статичним у певному місці, а блок виявлення розміщувався на транспортному засобі, який проїжджав поруч із джерелом перешкод на різних швидкостях. Транспортний засіб, який перевозив вимірювальний блок, був оснащений інтегрованою системою GNSS інерціальної навігаційної системи (INS), яка могла визначити місцезнаходження автомобіля навіть у безпосередній близькості від джерела перешкод. Таким чином можна було проаналізувати вплив заклинювання як функцію положення автомобіля. Ця установка є зворотною для випадку, коли пристрій перешкод встановлено на транспортному засобі, а блок виявлення залишається нерухомим на узбіччі дороги. Хоча цей другий сценарій

є більш реалістичним, наявність перешкод на транспортному засобі перешкодила б обчисленню PVT користувача.

Однак вплив транспортного засобу на поширення сигналу перешкод враховується, оскільки приймальна антена була розміщена всередині автомобіля. Також у цьому випадку сигнал перешкод повинен був поширюватися через кузов автомобіля.

Експерименти повторювали для трьох різних типів перешкод. Для аналізу було розглянуто кілька методів виявлення перешкод.

Більш конкретно, було реалізовано кілька підходів до виявлення перешкод без використання сигналу, які використовувалися для виявлення наявності перешкод.

Розглянуті підходи не залежать від сигналу в тому сенсі, що для конструкції детекторів не робиться сильного припущення щодо структури сигналу перешкод. Цей вибір конструкції було зроблено з огляду на велику різноманітність доступних сигналів перешкод: строга модель сигналу може мати скомпрометовані можливості виявлення у випадку невідповідності моделі, тобто коли сигнал перешкод не відповідає моделі, прийнятій для конструкції детектора.

Проведені експерименти та аналіз доповнюють результати, які вже є в літературі: тести розглядають реалістичне дорожнє середовище з урахуванням впливу транспортних засобів.

Крім того, надається широкий аналіз методів виявлення. Цей аналіз і порівняння різних підходів з використанням реальних даних раніше не проводилися, і тому це є одним із головних нашої роботи.

5.2 Система збору даних

Вимірювальна платформа була розроблена для збору різних типів вимірювань і демонстрації ефективності розглянутих підходів до виявлення перешкод. Вимірювальний блок складається з двох компонентів: приймача GNSS

та інтерфейсу SDR. Параметри використаного інтерфейсу наведенов таблиці 5.1.

У цьому випадку були використані такі пристрої:

Таблиця 5.1 — Параметри, прийняті для інтерфейсу RTL2832U, який використовується як засіб захоплення даних GNSS [17, с. 95])

Частота дискретизації	Центральна частота	Біти	Тип дискретизації
2,048 МГц	1575,42 МГц	8	Комплексний IQ

- u-blox LEA-6T, одночастотний приймач GPS, який використовується для збору вимірювань GNSS,
- інтерфейс Realtek RTL2832U, який використовується для збору синфазних/квадратурних (I/Q) зразків.

Пристрої згадані підключаються до однієї GPS-антени через розгалужувач радіочастотного сигналу.

Приймач u-blox є стандартним пристроєм, який забезпечує декілька типів вимірювань [17, с. 95].

На додаток до класичних спостережень GNSS тобто псевдодальностей, доплерівських зсувів, фаз несучої та значень C/N_0, приймач u-blox також надає пов’язані з апаратним забезпеченням параметри, такі як підрахунок ARP. Вимірювання u-blox зберігаються на ноутбуці за допомогою u-center, що є власним програмним забезпеченням u-blox із частотою дискретизації 1 Гц.

Серед спостережень GNSS лише значення C/N_0 використовуються в нашій роботі з метою виявлення перешкод. Також параметри, пов’язані з апаратним забезпеченням, зберігаються та використовуються для виявлення перешкод.

Realtek RTL2832U — це недорогий ТВ-тюнер, який було модифіковано та налаштовано для роботи відповідно до налаштувань, наведених у Таблиці 1.

Пристрій Realtek RTL2832U використовувався для збору зразків IQ і забезпечення моніторингу в реальному часі гістограми та спектральної щільності потужності (PSD) даних. Зразки IQ використовуються для обчислення метрик для виявлення перешкод.

5.3 Характеристика глушників

Для тестової компанії було використано три глушники з різними характеристиками, аналогічні до запропонованих у [17, с. 95]. Два з цих пристроїв є одночастотними перешкодами, тоді як третій може працювати на різних частотах. Усі глушники транслюють широкосмугові перешкоди у формі частотно-модульованих (FM) сигналів ЛЧМ. Характеристики прийнятих пристроїв підсумовано в таблиці 5.2. Вигляд трьох пристроїв перешкод наведено на рисунку 5.1:

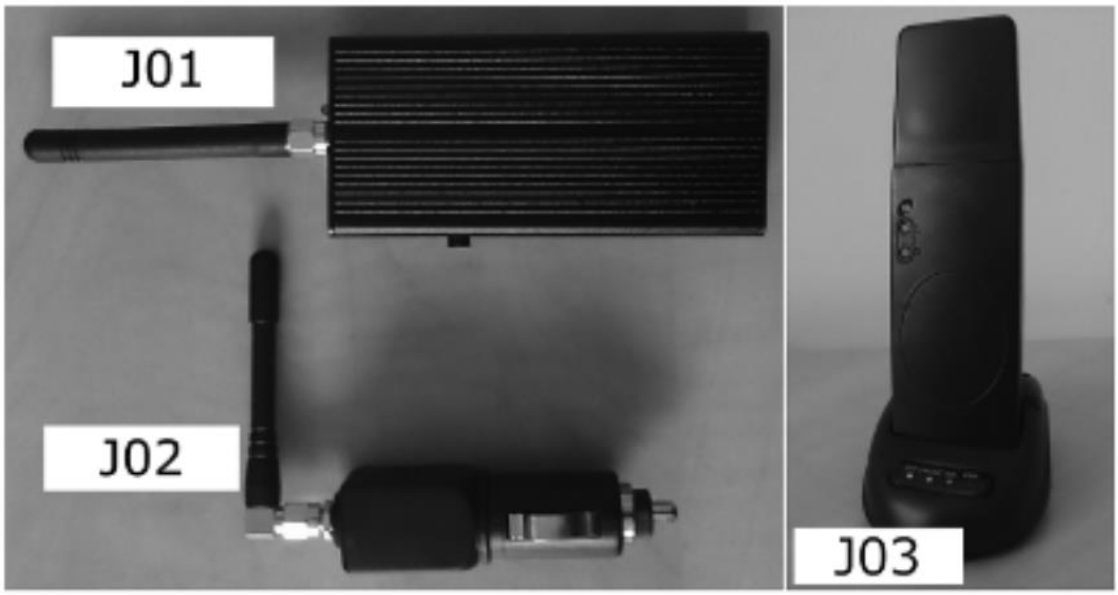


Рис. 5.1 — Вид трьох глушників, які використовуються для тестування різних підходів виявлення [17, с. 95]

JO1 — це пристрій перешкод для батареї, що транслює в діапазоні GPS L1 (він належить до групи 2 класифікації, наданої);

JO2 — глушник, що транслює у діапазоні GPS L1 (належить до групи 1 класифікації, наданої [17, с. 95]).

JO3 – це глушник із вбудованою антеною (група 3 класифікації, наданої [17, с. 95]). Пристрій має форму бездротового телефону і не може бути підключений до зовнішніх антен або кабелів. Він також транслює сигнали в кількох діапазонах частот, включаючи частоту GPS L1 [17, с. 95]). Повні дані глушників наведені в таблиці 5.2.

Таблиця 5.2 — Характеристики сигналів, випромінюваних трьома перешкодами, використаними для тестування [17, с. 95])

Глушник	Центральна частота	fmax	fmin	Діапазон розгортання	Період розгортання	Потужність
J01	1575,42 МГц	10,4 МГц	– 9,88 МГц	20,3 МГц	6,3 с	16
J02	1575,42 МГц	5,1 МГц	– 11,6 МГц	16,7 МГц	8,86 с	9
J03	1575,42 МГц	7,1 МГц	– 29,3 МГц	36,4 МГц	9,1 с	2

5.4 Агностичне виявлення перекладання сигналу

Система збору даних, дозволяє отримувати кілька типів вимірювань, які можна використовувати для виявлення глушіння. Діаграма, що містить класифікацію розглянутих показників, представлена на рисунку 5.2. Список показників, зображених на рисунку 5.2, не є вичерпним, і можна розробити та використовувати додаткові статистичні дані щодо рішень.

Можна знайти дві основні гілки: перша пов’язана з метриками, які можна обчислити за допомогою спостережуваних, наданих приймачем GNSS, тоді як друга стосується статистики виявлення, отриманої із зразків IQ, отриманих із інтерфейсу SDR. Ці дві гілки також відповідають приймачу GNSS і інтерфейсу SDR.

Метрики на основі приймача Коли розглядаються вимірювання з приймача GNSS, оцінюються два типи метрик:

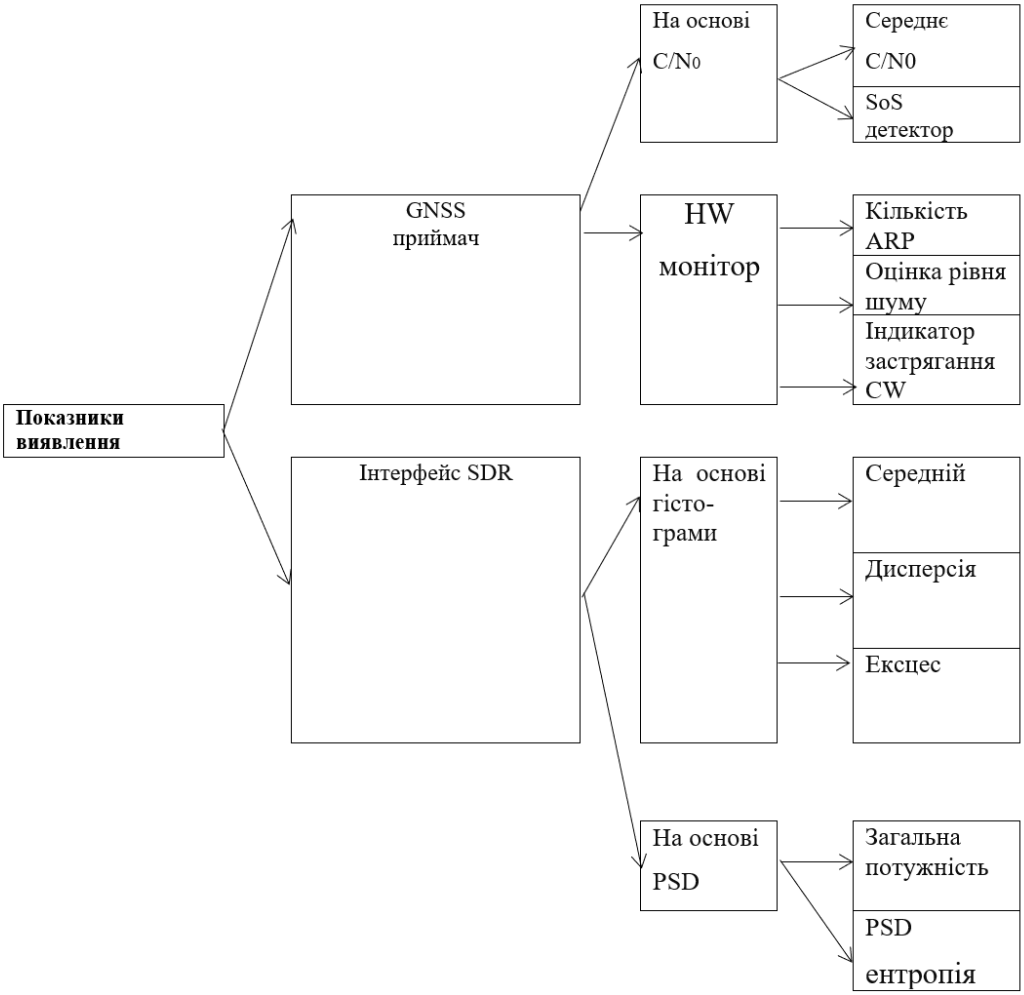


Рис. 5.2 — Різні підходи до виявлення перешкод, розглянуті в цій роботі

Перший тип ґрунтується на C/N_0 різних супутників, тоді як другий тип базується на наявних апаратних індикаторах у деяких комерційних приймачах GNSS, таких як приймач u-blox LEA-6T. Більшість приймачів GNSS надають сигнал C/N_0, і, отже, виявлення перешкод на основі C/N_0 може бути реалізовано на більшості пристроїв [9, с. 3]. У присутності перешкод C/N_0 отриманих сигналів може значно зменшитися, і цей факт може бути використаний для виявлення

сигналу. Метрика (5.1), заснована на припущенні, що всі отримані сигнали під впливом перешкод впливають однаковим чином, використовується для розробки детектора SOS, який характеризується наступною статистикою рішення:

$$\Lambda = \sum_{k=0}^{N-1} \left[\sum_{i=0}^{I-1} \left(\frac{C_i}{N_0}[n-k] - h_{LP}[n] * \frac{C_i}{N_0}[n-k] \right) \right]^2 \tag{5.1}$$

де N — це кількість періодів часу, врахованих у процесі виявлення, а I - кількість доступних супутників. $h_{LP}[n]$ це відповідь на імпульс низькочастотного фільтра з одиничним посиленням при прямому струмі, і символ * позначає згортку. [n] $\frac{C_i}{N_0}$ — це C/N_0 з і-го супутника в момент n, виражений у логарифмічній шкалі. Рішення приймається шляхом порівняння Λ з порогом прийняття рішення.

У цій статті розглядається експоненційний фільтр з коефіцієнтом забуття α = 0,75 [9, с. 3]. Крім того, для процесу прийняття рішення враховуються N = 5.

Цей детектор здатний виявляти наявність корельованих змін у значеннях C/N_0 від різних супутників, і він є своєрідним диференційним детектором: якщо потужність перешкод залишається постійною, і всі оцінки C/N_0 майже постійні, детектор SoS не здатний виявити наявність перешкоди. Можна показати, що статистика рішення (5.1) може бути записана як функція середнього C/N_0, яке задано:

$$\frac{C_{av}}{N_0}[n] = \frac{1}{I} \sum_{i=0}^{I-1} \frac{C_i}{N_0}[n] \tag{5.2}$$

де середнє обчислюється відносно супутникових сигналів. Виміри виконуються у логарифмічній шкалі, і може бути використаний критерій для вибору значень C/N_0, що будуть використані для обчислення (5.2). Далі показано, що середнє значення C/N_0 має зв'язок з отриманою потужністю перешкод, тому воно є ефективною метрикою для виявлення перешкоди.

Крім C/N0, деякі приймачі GNSS надають апаратні індикатори, які використовуються для моніторингу стану переднього кінця приймача. Найбільш поширеним апаратним індикатором для виявлення втручань є керований автоматичний підсилювач (AGC) [3, с. 2043]. Зокрема, сучасні приймачі мають багатобітну архітектуру, і сигнали на їх вході повинні бути належним чином масштабовані для зменшення втрат квантування. AGC забезпечує підсилення, яке використовується для масштабування сигналів на вході приймача. КАП-підсилення зазвичай залежить від вхідної потужності, тому воно приймає низькі значення у присутності перешкод.

Приймач u-blox LEA-6T також надає два додаткових апаратних індикатори: оцінювач шумового фону та індикатор постійного сигналу перешкод [67]. Перший повинен відображати кількість шуму, оцінену на виході приймача.

Другий індикатор повинен виявляти наявність перешкоди у вузькому діапазоні і, таким чином, не повинен бути ефективним для виявлення розглянутих тут сигналів перешкод. В інструкції користувача u-blox [67] надається обмежена інформація про ці два індикатори, які емпірично аналізуються у розділах 5 та 6.

5.5 Метрики, пов'язані з SDR

З вибірки IQ, наданої переднім кінцем SDR, можна обчислити різні метрики. У цій роботі розглядаються дві родини метрик. Перша базується на гістограмі вибірок, тоді як друга - на PSD отриманого сигналу.

Гістограма - це оцінка функції щільності ймовірності (pdf) вибірок, наданих переднім кінцем SDR, і відсутності перешкод, вона повинна відповідати розподілу Гаусса з нульовим середнім. Гістограма (5.3) обчислюється:

$$H(x) = \frac{1}{N_{tot}} \sum_{n=0}^{N_{tot}-1} \mathbb{1}\left(y[n] = x\right) \tag{5.3}$$

де *y[n]* позначає послідовність вибірок, наданих переднім кінцем SDR. У цьому випадку не робиться розрізнення між вибірками у фазі та квадратурі, і обчислюється спільна гістограма. *x* - значення розряду гістограми, і N_{tot} - загальна кількість вибірок, використаних для обчислення гістограми. *1(.)* - це індикаторна функція, яка дорівнює 1, коли умова в дужках істинна. В іншому випадку функція видає нуль. Варто зазначити, що передній кінець RTL2832U надає вибірки, квантовані на 8 біт, і *y[n]* набуває цілих значень у множині [-128, 127]. *H(x)* надає оцінку (5.4) pdf вхідних вибірок:

$$H(x) \approx P(y[n] = x) \approx f(x)\Delta x \tag{5.4}$$

де *P(·)* позначає ймовірність, *f(x)* - pdf вхідних вибірок, а Δx - відстань між двома сусідніми розрядами гістограми. У (4) ефекти квантування даних не враховані. Таким чином, *H(x)* можна використовувати для оцінки *f(x)* і виявлення перешкод.

Принцип, що лежить в основі виявлення перешкод на основі гістограми, показано на рисунку 5.3, де показано дві pdf, оцінені з двох гістограм, обчислених у відсутності і в присутності перешкод.

При номінальних умовах вхідні вибірки відповідають розподілу Гаусса з нульовим середнім, тоді як відхилення відбуваються в присутності перешкод. На рисунку 5.3 також присутні ефекти насичення в pdf, оціненому у присутності перешкоди: у цьому випадку сигнал настільки потужний, що найвищі та найнижчі рівні функції квантування переднього кінця SDR використовуються протягом значної частини часу. Передній кінець фактично обрізає вхідний сигнал. Насичення може мати значний вплив на метрики виявлення.

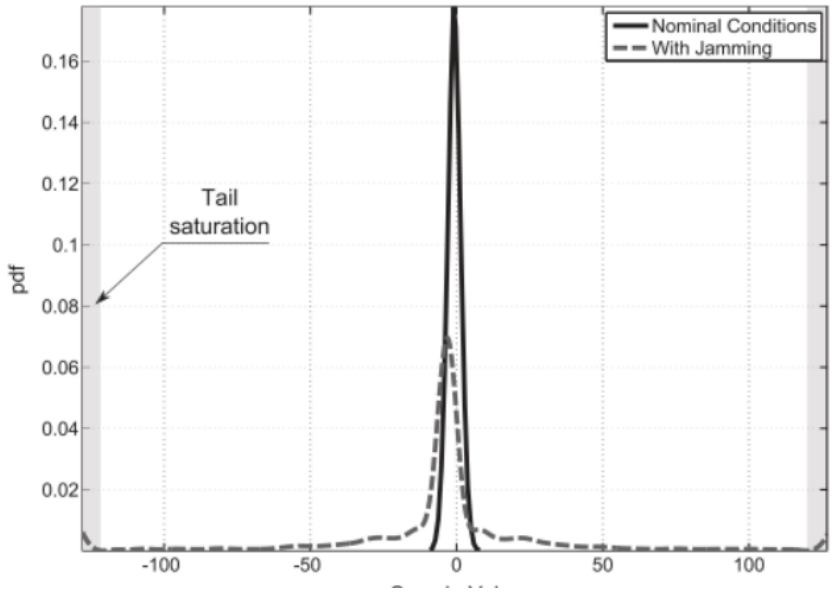


Рис. 5.3 — Порівняння pdf, оціненого за двома гістограмами, обчисленими у відсутності та у присутності перешкод [17, с. 97]

Виявлення перешкод може бути здійснене за допомогою обчислення метрик, які здатні показати відхилення гістограми від розподілу Гаусса.

У цій роботі розглянуті метрики включають середнє значення вибірки, яке використовується для перевірки значних відхилень середнього значення від нуля, дисперсію вибірки і надлишкову куртозу. Дисперсія вибірки є індикатором розподілу вхідних вибірок. З рисунка 5.3 чітко випливає, що сигнал перешкоди вводить значний розподіл в вибірку. Надлишкова куртоза є виміром "гостроти" pdf. Куртоза залежить від четвертого моменту pdf. Скошеність, яка є виміром асиметрії pdf, тут не розглядалася, оскільки навіть у присутності перешкод значних асиметрій не спостерігалося. Цей факт чітко випливає з лівої частини рисунка 5.4, на якому показана часова еволюція гістограми на вибірках, зібраних за допомогою переднього кінця RTL2832U під час тесту з автомобілем, що рухається зі швидкістю 50 км/год.

Хоча можна спостерігати чіткі спотворення в гістограмі, коли автомобіль проїжджає близько до перешкоди, значних асиметрій не спостерігається. Середнє

значення, дисперсія та надлишкова куртоза можуть бути оцінені за допомогою вибіркових оцінювачів або числовим інтегруванням вибіркової pdf, оціненої з гістограми. Тут був використаний другий підхід, де гістограми оцінювалися за допомогою 10 мс послідовних даних. Цей підхід дозволив проаналізувати всю гістограму, що надає більш повну картину, ніж середнє значення, дисперсія та надлишкова куртоза, які є узагальненими статистиками. Другий клас метрик виявлення може бути отриманий, розглядаючи PSD вибірок, наданих переднім кінцем. У цьому випадку був використаний метод Вельча [69, с. 71], і PSD вхідних вибірок було оцінено за допомогою блоків по 10 мс даних.

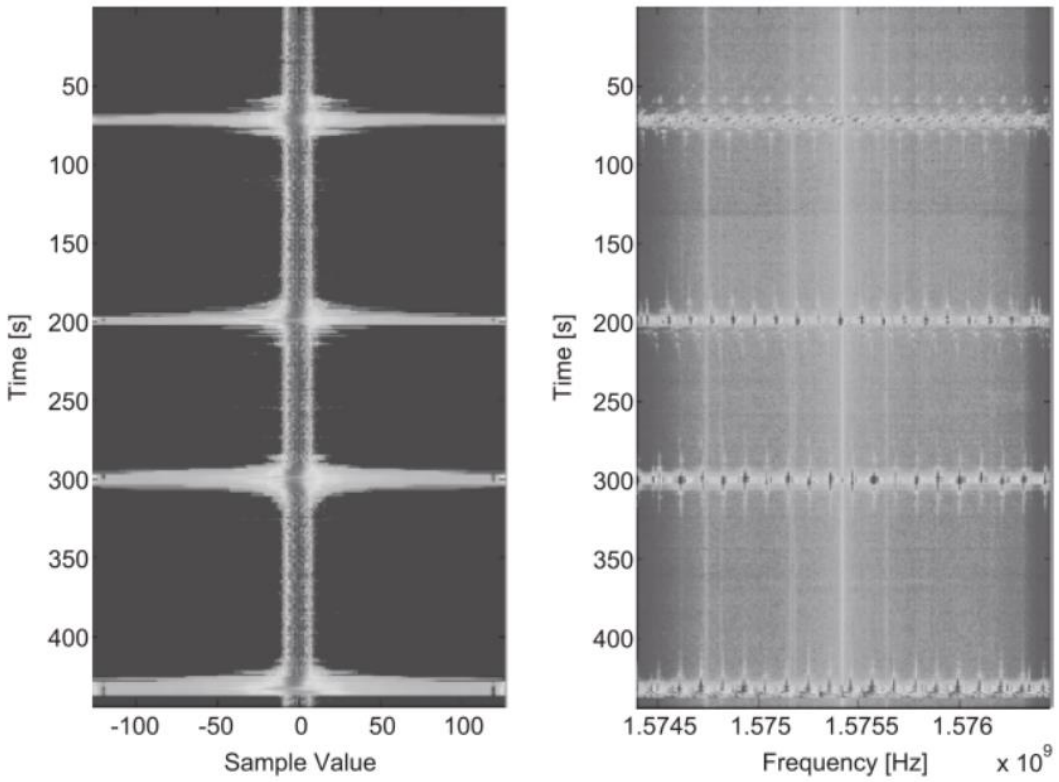


Рис. 5.4 — Часова еволюція гістограми та PSD вибірок, зібраних за допомогою переднього кінця RTL2832U. Статичний перешкоджувач (J02) з автомобілем, що рухається зі швидкістю 50 км/год [17, с. 97]

Часова еволюція PSD вибірок, зібраних за допомогою переднього кінця RTL2832U, показана у правій частині рисунка 5.3. Коли автомобіль проїжджає

близько до перешкоди, можна спостерігати чіткі спотворення в PSD. У відсутності перешкод, PSD вхідних вибірок майже плаский, і його форма в основному визначається фільтром переднього кінця. Єдиний помітний елемент - спектральна лінія, що відповідає самостійному перешкодженню. У присутності перешкод значна потужність розподіляється по частотному інтервалу, захопленому переднім кінцем. Більше того, з'являються сильні спектральні лінії. Це пов'язано з тим, що сигнали перешкоди проявляють періодичну поведінку.

Щодо випадку гістограми, виявлення перешкод може бути здійснене за допомогою метрик, які виокремлюють спотворення в оціненому PSD. У цій роботі розглядалися дві метрики: загальна потужність і спектральна ентропія [66, с. 183]. Загальна потужність (5.5) - це інтеграл PSD по розглянутому частотному інтервалу:

$$P_{Rx} = \sum_{i=f_{min}}^{f_{max}} P(i)\Delta f \tag{5.5}$$

де *P(i)* позначає оцінений за допомогою методу Вельча PSD, а *fmin* та *fmax* - мінімальна та максимальна частоти, які враховуються. PSD оцінюється на дискретній частотній сітці, і Δf позначає крок частоти між двома сусідніми частотами в сітці. Варто зазначити, що потужність P_{Rx} може бути оцінена безпосередньо з вибірок як:

$$P_{Rx} = \frac{1}{N_{tot}} \sum_{n=0}^{N_{tot}-1} |y[n]|^2. \tag{5.6}$$

Отже, вона безпосередньо пов'язана з вибірковою дисперсією, розглянутою вище. Проте в подальшому обидва показники були обчислені з використанням різних нормалізацій і відрізняються тим, що у випадку дисперсії зразу від вибірок віднімається середнє значення. Варто зазначити, що передній кінець RTL2832U не калібрується, і тому до вибірок застосовується довільне масштабування. Таким чином, оцінений PSD впливає на систематичне відхилення, яке не

дозволяє оцінити абсолютну отриману потужність. Оскільки можуть бути оцінені лише відносні зміни потужності, введення масштабного множника у обробку не впливає на результати виявлення.

Нарешті, останнім розглянутим показником є спектральна ентропія, визначена наступним чином [29]:

$$E_t = -\sum_{i=f_{min}}^{f_{max}} \tilde{P}(i)\log(\tilde{P}(i)) \tag{5.7}$$

$$\tilde{P}(i) = \frac{1}{P_{Rx}} P(i) \tag{5.8}$$

Нормалізований PSD є позитивною функцією з одиничною площею, яку можна узагальнити до pdf. Таким чином, спектральна ентропія є виміром спектральної неозначеності: у відсутності перешкод PSD максимально плаский, і спектральна ентропія приймає своє максимальне значення. Сигнали перешкод вводять регулярні особливості в PSD у вигляді спектральних ліній, що значно знижує ентропію. Таким чином, спектральна ентропія є потенційною метрикою для виявлення перешкод.

5.6 Обладнання, використане для тестів

Для демонстрації ефективності запропонованого підходу було проведено кілька тестів, включаючи кінематичні випробування з різними перешкодами та на різних швидкостях.

Середовище випробувань показано на рисунку 5.5. Середовище було обрано з метою мінімізації впливу перешкод на інших користувачів GPS; тому ним стала віддалена місцевість поблизу міста Броди Львівської області. Тести були проведені у липні 2023 року.

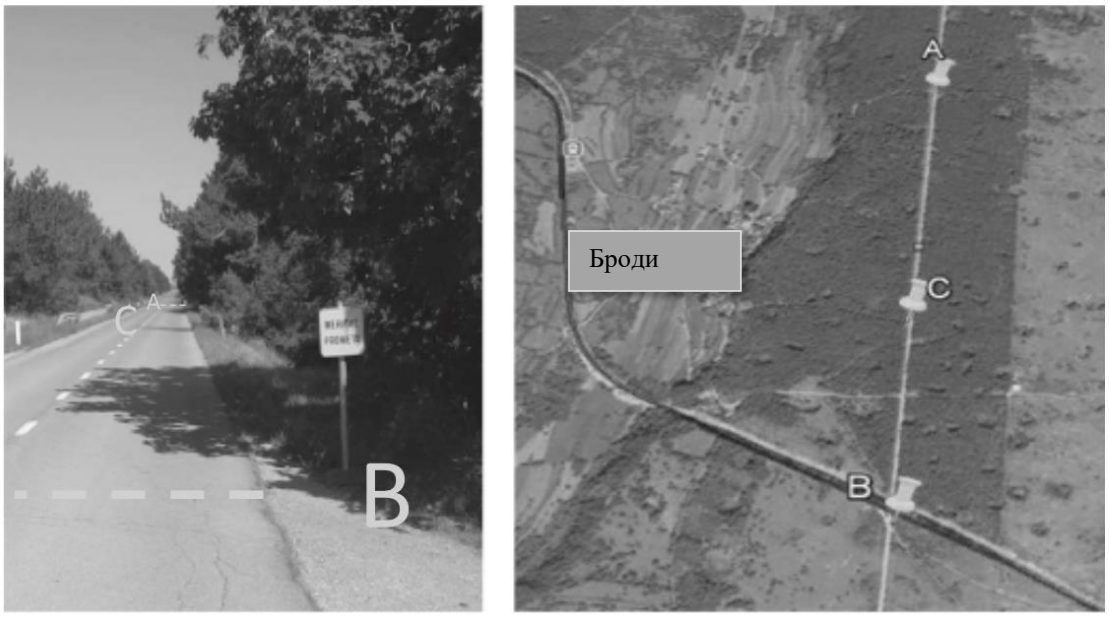


Рис. 5.5 — Середовище випробувань

Перешкоди залишалися статичними на позиції, вказаній як C на рисунку 5.5, тоді як автомобіль був обладнаний платформою. Автомобіль із блоком виявлення рухався, підтримуючи постійну швидкість, туди і назад між двома точками (A та B), показаними на рисунку 5.5. Тести проводилися зі швидкістю 50 км/год та 90 км/год. Сценарій повторювався для кожного перешкоджувача та для різних швидкостей. Крім того, автомобіль з вимірювальним блоком був обладнаний інтегрованим блоком GNSS/INS, який міг визначати місцезнаходження автомобіля навіть у безпосередній близькості від перешкоди. Таким чином, була можливість аналізувати вплив перешкод на основі позиції автомобіля та, отже, на основі відстані між перешкодою та блоком виявлення. Інтегрований блок GNSS/INS був мініатюрною системою визначення постави та напрямку X-sense MTi-G. Оцінки позиції від пристрою X-sense були інструментальними для дослідження потенційних зв'язків між метриками виявлення перешкод та відстанню від перешкоди. Максимальна відстань між перешкодою та блоком виявлення становила приблизно 700 м, коли автомобіль

перебував в одній з точок A/B, тоді як мінімальна відстань становила приблизно 5 м, коли автомобіль проїжджав перед станцією, обладнаною перешкодою.

5.7 Аналіз отриманих даних

Представляємо отримані експериментальні результати. Спочатку аналізується один експеримент для кожного типу метрики. Зокрема, метрики надаються у вигляді функції часу та для різних проходів автомобіля. Таким чином, досліджується послідовність результатів. Звітуються лише результати, пов'язані з перешкоджувачем JO2. Подібні висновки були отримані для двох інших перешкоджувачів. Потім порівнюються ефекти трьох перешкоджувачів, і наводяться результати для одного проходу.

Метрики, отримані зі значень C/N_0 різних супутників, відстежуваних приймачем u-blox LEA-6T під час сценарію з рухом автомобіля зі швидкістю 50 км/год, відображаються як функція часу на рисунку 5.6. Зокрема, значення C/N_0 чотирьох сигналів, відстежуваних, подаються в верхньому блоку фігури. Для зрозумілості розглядаються лише чотири сигнали. Ефект перешкоди чітко видно: помітне зниження значень C/N_0 можна помітити, коли приймач знаходиться близько до перешкоди. Втрата фіксації відбувається, коли автомобіль з приймачем проїжджає перед перешкодою. Ці ефекти узгоджені між різними проходами. Більше того, можна помітити кореляцію між значеннями C/N_0 в присутності перешкодження.

Середнє значення C/N_0 відображається як функція часу в другому блоку зверху на рисунку 5.6; середнє значення C/N_0 обчислюється лише за значеннями C/N_0 вищими за 30 дБ-Гц. Ця метрика дозволяє чітко ідентифікувати події перешкодження. Втрата C/N_0 найбільша, коли автомобіль знаходиться на мінімальній відстані від перешкоди. Цей факт чітко виявляється при розгляді нижньої частини рисунка 5.6, яка показує оцінену відстань між перешкодою та приймачем-жертвою.

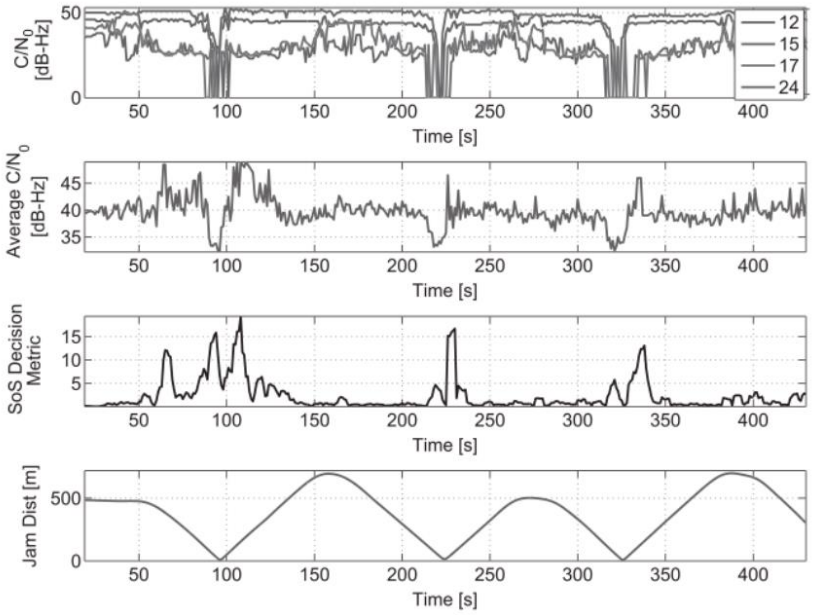


Рис. 5.6 — Показники, отримані з CIN(різних супутників, відстежених приймачем u-blox LEA-6T під час сценарію зі статичним перешкодами (J02) і автомобілем, що рухається зі швидкістю 50 км/год.

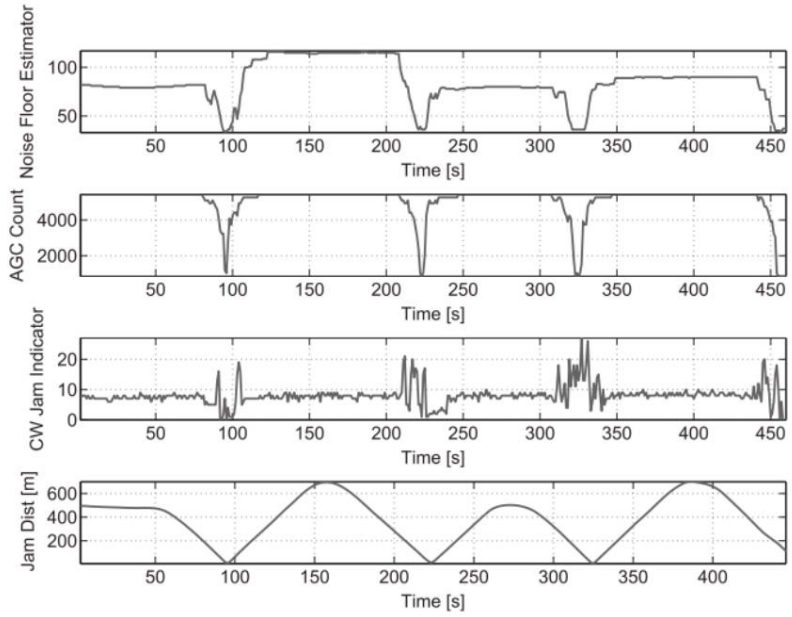


Рис. 5.7 — Апаратні індикатори приймача u-blox 6 як функція часу

Вимірювання проводилися за допомогою статичного джерела перешкод (J02) і автомобіля, який рухався зі швидкістю 50 км/год. Відносна відстань між джерелом перешкод і детектором вказана в нижній частині рисунка.

Статистика прийняття рішення детектора SoS зображена як функція часу в третій частині рисунка 5.7. Метрика правильно визначає наявність перешкод, але не надає чіткої інформації про потужність перешкод. Це узгоджується з результатами, представленими в [8], які показали, що детектор SoS в основному ефективний у визначенні початку та кінця події перешкод. Також спостерігається висока узгодженість між пасажами.

На рисунку 5.7 метрики, отримані з індикаторів апаратного моніторингу, зображені як функція часу. Також у цьому випадку відстань від другої та третьої частин фігури відповідно. З верхнього поля можна відзначити, що рівень шуму зменшується за наявності перешкод, переходячи приблизно від 80, у першому проході, до менше ніж 40. Одиниці вимірювання для цієї метрики не вказані в [67]. Коли приймач віддаляється від джерела перешкод, рівень шуму зростає, досягаючи вищого значення близько 110. Така поведінка не очікувалася, оскільки попереднє значення мінімального шуму мало бути відновлено. Однак доступні лише деякі деталі щодо індикатора, який обчислюється за допомогою власного алгоритму [67]. Крім того, можна відзначити низьку узгодженість оцінок за відсутності перешкод: цей факт, ймовірно, пов’язаний з ефектом пам’яті в приймачі, який не може повністю відновитися після події перешкод. Зокрема, різні рівні шуму реєструвалися після кожного випадку перешкод. Значення підрахунку AGC аналізуються у другому полі зверху на рисунку 5.7; отримані результати показують, що за наявності перешкод кількість AGC раптово падає, переходячи від значень, близьких до 6000, приблизно до 0. Така поведінка є узгодженою для різних проходів; крім того, можна відзначити чітку залежність від відстані. Нарешті, значення індикатора перешкод CW розглядаються в третій частині рисунка 5.7. Параметр може приймати значення від 0 до 255 [23]. У

досліджуваному випадку індикатор CW перешкод приймає відносно низькі значення від 0 до 20, що свідчить про його нездатність виявляти широкосмугові перешкоди. Це очікувано, оскільки такий індикатор був розроблений для перешкод CW. Глушник наведено в нижній частині рисунка як довідник. Значення оцінки мінімального рівня шуму нанесено на графік у верхньому полі, тоді як значення лічильника та індикатора перешкод CW нанесено на графік.

Незважаючи на цей факт, можна оцінити невелике збільшення мінливості оцінок за наявності перешкод. Тест, проаналізований на рисунка 5.6 і 5.7, проводився з постійною швидкістю приблизно 50 км/год і з глушником J02. Те саме випробування було повторено з двома іншими перешкодами; результати, отримані для цього сценарію, порівнюються на рисунку 5.8. Щоб мати більш чітке представлення результатів, розглядається один уривок. За цих умов ефекти перешкод помітні приблизно протягом 10 с, що відповідає приблизно +70 м.

Цей факт виділено сірими рамками на рисунку 5.8. Зокрема, J01 є найпотужнішим джерелом перешкод і має сильніший вплив на середнє C/N_0, як показано у верхній рамці на рисунку 5.8 падає швидше, ніж у двох інших випадках. Для детектора SoS крива J01 маскує інші два випадки. Незважаючи на цей ефект, детектор SoS чітко виявляє наявність перешкод у всіх випадках. Крім того, цей аналіз показує, що кількість ARP є одним із найбільш показових показників, оскільки для всіх трьох джерел перешкод значення кількості ARP значно зменшується в міру наближення до місця перешкод. У цьому випадку найбільш очевидний ефект пов'язаний з JO2, який не є найпотужнішим глушилом; однак кількість AGC пов’язана з отриманою потужністю, яка пов’язана не лише з переданою потужністю, але й із формою хвилі перешкод. Значення мінімального рівня шуму нанесено на графік у нижній рамці рисунка 5.8: важко визначити чіткий ефект для JO1 та J03. Проте зниження рівня шуму є очевидним для J02. Подібні випробування також проводилися на швидкості близько 90 км/год.

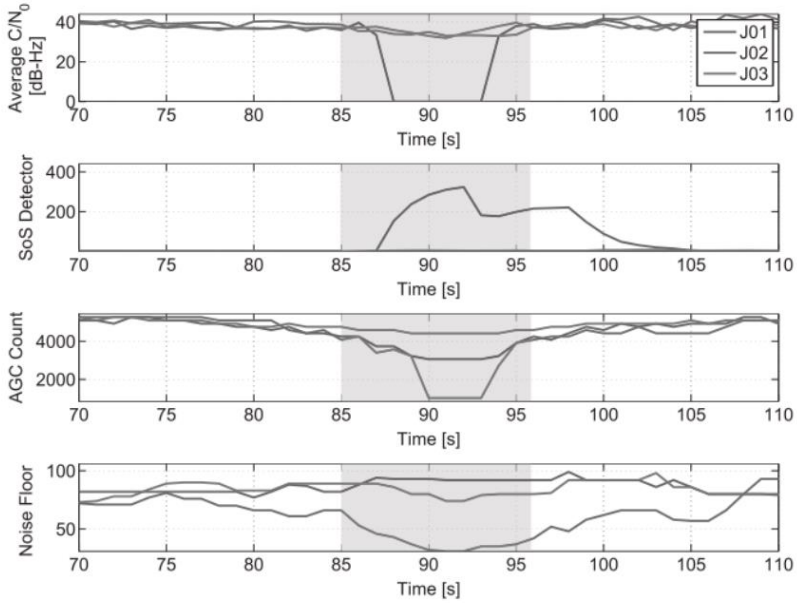


Рис. 5.8 — Показники виявлення, оцінені за допомогою вимірювань із приймача u-blox LEA-6T для експерименту з автомобілем, що рухається зі швидкістю 50 км/год [17, с. 101]

Результати, отримані для трьох джерел перешкод, були накладені. Результати щодо одноразового проїзду автомобіля перед станцією перешкод представлені на рисунку 5.9. У цьому випадку ефект перешкод видно протягом меншого інтервалу часу, близько 6 с. Цей факт пояснюється більшою швидкістю транспортного засобу. Крім того, отримані результати узгоджуються з обговореним вище. Крім того, у цьому випадку ефекти JO1 більш очевидні при розгляді середнього C/N_0 та показника SoS, тоді як для підрахунку AGC найбільший вплив має JO2. Рівень шуму демонструє іншу поведінку, ніж у попередньому випадку.

Метрики, пов’язані з SDR. Метрики, отримані із зразків RTL2832U під час сценарію зі статичним перешкодою (J02) і автомобілем, що рухається зі швидкістю 50 км/год, аналізуються спочатку. Показники виявлення на основі гістограми зображені як функція часу на рисунку 5.8. Зокрема, середнє значення зображено як функція часу у верхньому полі рисунка 5.9. Ця метрика надає

обмежену інформацію про виявлення перешкод; однак можна оцінити невелике збільшення мінливості за наявності перешкод.

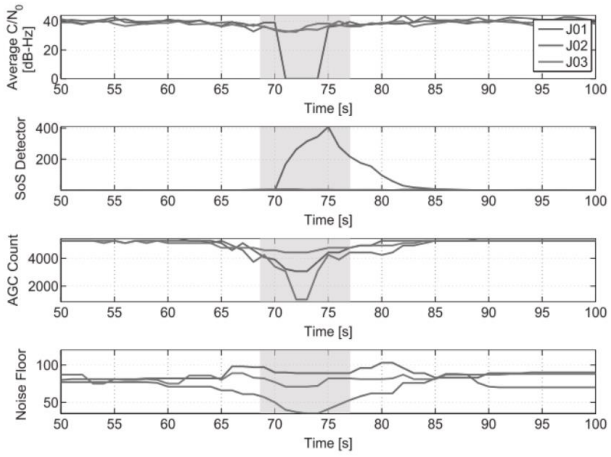


Рис. 5.9 — Показники виявлення, оцінені за допомогою вимірювань із приймача u-blox LEA-6T для експерименту з автомобілем, що рухається зі швидкістю 90 км/год [17, с. 100]

Результати, отримані для трьох джерел перешкод, були накладені, як це зазначено на рисунку 5.10.

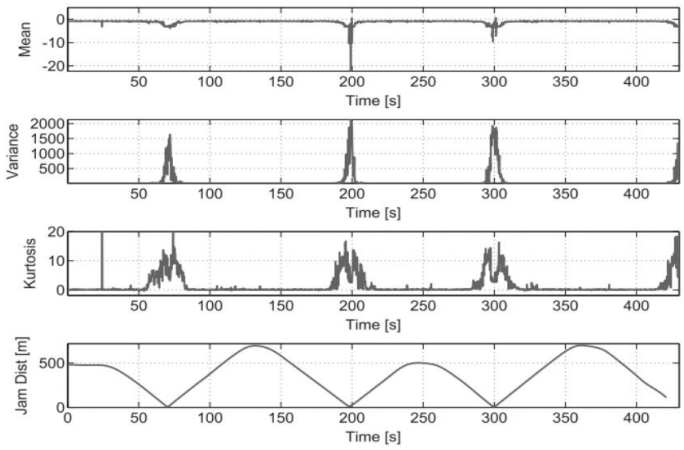


Рис. 5.10 — Показники виявлення на основі гістограми, оцінені за допомогою зразків інтерфейсу RTL2832U [17, с. 102]

Кілька проходів перед статичною перешкодою (J02) з автомобілем, що рухається зі швидкістю 50 км/год, можна чітко визначити. Відносна відстань між перешкодою та детектором наведена в нижній частині рисунка 5.11.

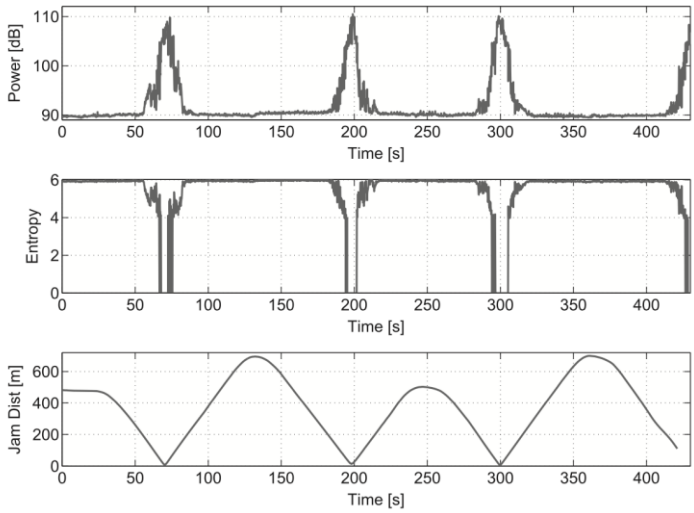


Рис. 5.11 Метрики виявлення на основі PSD, оцінені за допомогою зразків інтерфейсу RTL2832U [17, с. 103]

Чітко видно кілька проходів перед статичним глушником (J02) з автомобілем, що рухається зі швидкістю 50 км/год. Відносна відстань між джерелом перешкод і детектором вказана в нижній частині рисунка.

У другому полі зверху на рисунку 5.11 вибіркова дисперсія нанесена на графік як функція часу. На рисунку чітко проступає ефект джемера; значне збільшення дисперсії можна помітити, коли передній кінець знаходиться близько до джерела перешкод. Ці ефекти є послідовними серед різних уривків.

Нарешті, надлишковий ексцес розглядається в третій частині рисунка 5.11. Хоча наявність перешкод чітко визначено, важко встановити зв’язок із відстанню до перешкод, яка представлена в нижній частині рисунка. Розглянута метрика має невелике збільшення близькості перешкод. Крім того, ефекти насичення можна чітко визначити, коли пристрій перешкод знаходиться на мінімальній відстані від переднього кінця SDR. Метрики на основі PSD зображені як функція часу на

рисунку 5.11. Отримана потужність враховується у верхній частині рисунка: метрика дозволяє чітко ідентифікувати події перешкод, оскільки підвищена потужність вимірюється в проксі - імітивність глушника. Можна визначити чітку тенденцію між отриманою потужністю та відстанню перешкод. Отримана потужність збільшується при наближенні автомобіля до глушника і зменшується при віддаленні автомобіля від глушника. Спектральна ентропія зображена як функція часу в центральній частині рисунка 5.11. Крім того, у цьому випадку можна визначити наявність перешкод, і ефекти насичення очевидні, коли автомобіль досягає мінімальної відстані від перешкод. Вплив на отриману потужність і на спектральну ентропію є узгодженим між різними проходами.

Щоб оцінити відмінності між трьома джерелами перешкод, результати, отримані для показників на основі гістограми, представлені на рисунку 5.12, де розглядається один прохід. У лівому стовпчику рисунка розглянуто випадок, коли автомобіль рухається зі швидкістю 50 км/год. Випадок 90 км/год аналізується в правій колонці. Середні значення для трьох випадків перешкод майже збігаються, і лише трохи вищу мінливість можна відзначити для випадку J03. Вплив трьох перешкод чітко визначено дисперсією вибірки: J01 є найпотужнішим пристроєм і забезпечує найбільше збільшення дисперсії. Крива J03 нижче, ніж інші. Нарешті, надлишковий ексцес також показує наявність перешкод, хоча ефекти насичення чітко присутні в усіх трьох випадках.

Вплив трьох перешкод на метрику на основі PSD оцінюється в лівій частині рисунка 5.12. У верхній частині рисунка значення отриманої потужності нанесено на графік як функція часу. Крім того, у цьому випадку результати J01 показують найпотужніший пристрій, тоді як J02, здається, є найслабшим джерелом перешкод. Зауважте, що на отриману потужність значно впливають такі ефекти прийому, як передній фільтр. Таким чином, потужність, що передається глушилом, може бути значно послаблена передньою частиною приймача залежно від структури сигналу глушіння. У нижній частині рисунка

5.12 враховано спектральну ентропію; у всіх випадках можна чітко ідентифікувати подію перешкод. Хоча ефекти насичення очевидні для трьох розглянутих випадків, такі ефекти більш виражені для J02.

Проводиться аналіз за аналогічним методом, враховуючи тести, проведені при постійній швидкості приблизно 90 км/год.

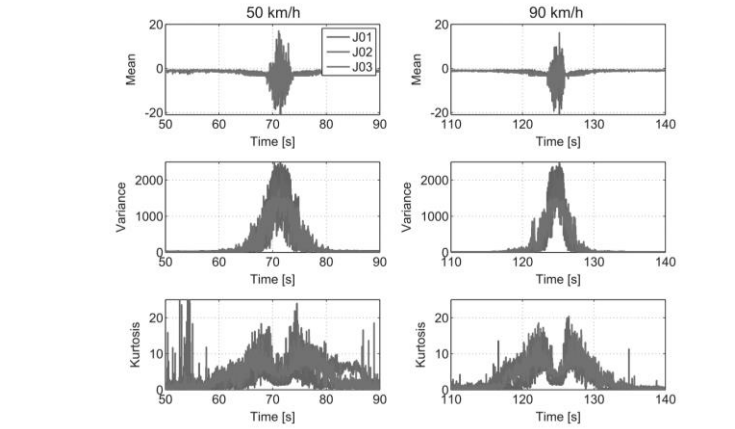


Рис. 5.12 —Метрики виявлення на основі гістограм, оцінені за допомогою вибірок з фронтенду RTL2832U для випадків зі швидкістю 50 км/год і 90 км/год

Результати, отримані для трьох перешкодопоглиначів, були накладені один на одного продемонстровано на рисунку 5.13.

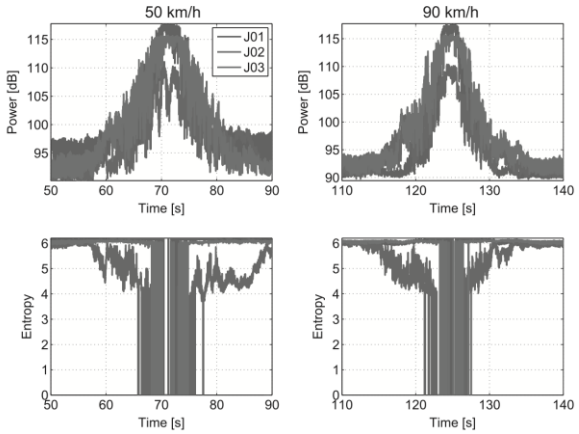


Рис. 5.13 — Метрики виявлення на основі спектральної густини потужності, оцінені за допомогою вибірок з фронтенду RTL2832U для випадків зі швидкістю 50 км/год і 90 км/год

Результати, отримані для трьох перешкодопоглиначів, були накладені один на одного.

Отримані результати показані у правих стовпчиках на рисунках 5.12 і 5.13. Результати узгоджені з результатами тестів, проведених при нижчій швидкості: середнє значення не надає інформації про відстань до перешкодопоглинача, і можна відзначити лише збільшену варіабельність; з графіків дисперсії та потужності чітко видно події, пов'язані з перешкодопоглиначем, а також спостерігається тенденція між метриками та відстанню до перешкодопоглинача. Нарешті, на графіках спектральної ентропії та зайвого куртозу видно ефекти насичення, спричинені присутністю перешкодопоглинача.

5.8 Аналіз на основі відстані

Зібрані дані були додатково проаналізовані з метою виділення можливих залежностей від відстані до перешкодопоглинача. Можливі функціональні відносини між метриками та відстанями до перешкодопоглинача є основою для розробки підходів до локалізації. Позицію користувача було отримано за допомогою рішення, наданого системою GNSS/INS, встановленою в автомобілі. Система змогла надати позицію користувача навіть у безпосередній близькості до перешкодопоглинача.

Відстані були отримані з рішень про позицію та пов'язані з різними оціненими метриками, як це зазначено на рисунку 5.14.

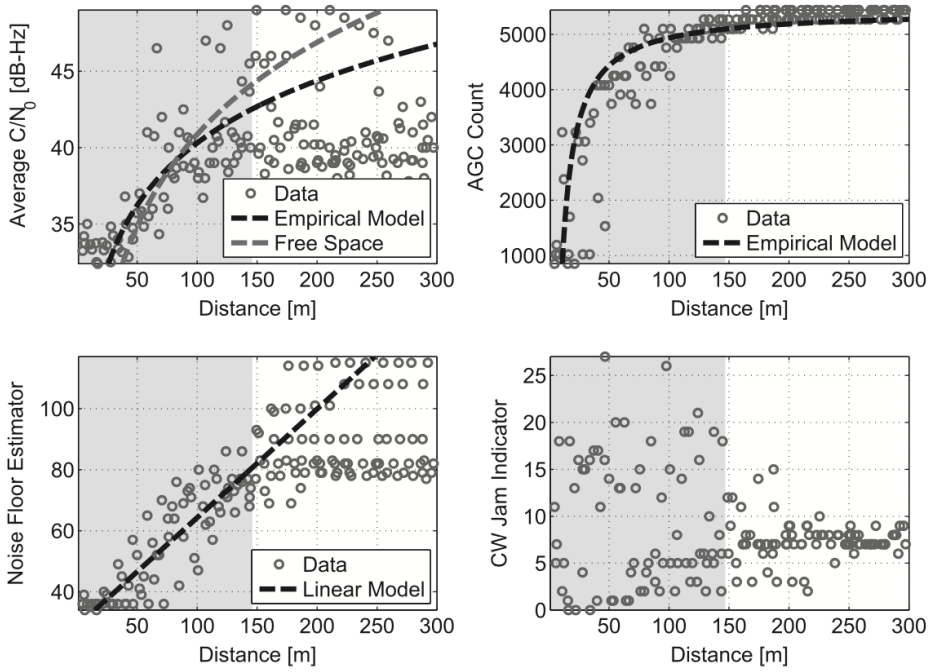


Рис. 5.14 — Метрики на основі приймача, побудовані як функція відстані. В сценарії зі статичним перешкодопоглиначем (J02) використовувався приймач u-blox LEA-6T, а автомобіль рухався зі швидкістю 50 км/год [17, с. 105].

5.9 Метрики на основі приймача

Метрики на основі приймача аналізуються як функція відстані на рисунку 5.14. Зокрема, розглядаються середнє значення C/N_0, лічильник AGC, оцінювач шумового фону та індикатор CW-перешкод. SoS не розглядається, оскільки не виявлено чіткої залежності від відстані. Для кожної метрики були зроблені спроби визначити функціональні відносини між метрикою та відстанню до перешкодопоглинача.

Випадок середнього C/N_0 розглядається у верхній лівій частині рисунка 5.14. За допомогою концепції ефективного C/N_0, запропонованої в [30], можна встановити емпіричну модель. Зокрема, C/N_0, виміряне приймачем GNSS у присутності перешкод, можна виразити як

$$\left.\frac{C}{N_0}\right|_{eff} = \frac{C}{N_0 + k_\alpha J} = \frac{C}{N_0}\frac{1}{1 + k_\alpha \frac{J}{N_0}} \tag{5.9}$$

де $\left.\frac{C}{N_0}\right|_{eff}$ є ефективним C/N_0, J - потужність перешкодопоглинача, а k_α - коефіцієнт спектрального розділення (КСР), який враховує ефект фільтрування приймача на сигнал перешкоди. Усі величини в (5.9) виражені в лінійних одиницях. Рівняння (5.9) можна виразити в логарифмічних одиницях як

$$\left.\frac{C}{N_0}\right|_{eff,dB-Hz} = \left.\frac{C}{N_0}\right|_{dB-Hz} - 10\log_{10}\left(1 + k_\alpha \frac{J}{N_0}\right) \tag{5.10}$$

де залежність від виділена спектральна щільність потужності перешкод до шуму 0.

Коли потужність перешкод є достатньо високою можна ввести таке наближення:

$$\left.\frac{C}{N_0}\right|_{eff,dB-Hz} \approx \left.\frac{C}{N_0}\right|_{dB-Hz} - 10\log_{10}\left(k_\alpha \frac{J}{N_0}\right) \tag{5.11}$$

Це можна подальше виразити як:

$$\left.\frac{C}{N_0}\right|_{eff,dB-Hz} \approx \left.\frac{C}{N_0}\right|_{dB-Hz} - 10\log_{10}\left(\frac{k_\alpha}{N_0}\right) - J\,|_{dBW}. \tag{5.12}$$

Припускаючи модель втрат сигналу [32] для J|dBW, потужність перешкоди можна виразити як функцію відстані до перешкоди, d:

$$J\,|_{dBW} = J_0 - 10\alpha\log_{10}\left(\frac{d}{d_0}\right) \tag{5.13}$$

де α - це показник втрат сигналу, а J_0 - це потужність перешкоди, виміряна на посиланні дистанції, d_0. Підставивши (5.13) в (5.12) і групуючи сталий член, в кінцевому підсумку отримуємо наступну модель:

$$\left.\frac{C}{N_0}\right|_{eff,dB-Hz} = \beta + 10\alpha\log_{10}(d) \tag{5.14}$$

$$\beta = \left.\frac{C}{N_0}\right|_{dB-Hz} - 10\log_{10}\left(\frac{k_\alpha}{N_0}\right) - J_0 - 10\alpha\log_{10}(d_0)\,. \qquad (5.15)$$

Середнє значення C/N_0 було отримане як середнє значення ефективних C/N_0 з різних супутникових сигналів, виражених в dB-Hz. Таким чином, воно також відповідає моделі (5.14), де у цьому випадку постійний член в (5.14) замінено середнім значенням для різних супутників. Середні значення наведені в таблиці 5.3.

Таблиця 5.3 – Параметри, оцінені для обговорених моделей на рисунку 5.14

Випадок	Параметр моделі	Значення
Середнє C/N_0, Емпірична модель	β	13.2
Середнє C/N_0, Емпірична модель	α	1.36˘
Середнє C/N_0, Модель вільного простору	β	0.86
Середнє C/N_0, Модель вільного простору	α	2
Лічильник AGC, Емпірична модель	$Gmax$	5440
Лічильник AGC, Емпірична модель	γ	50319

У верхньому лівому кутку рисунка 5.14 емпіричні дані порівнюються з моделлю (5.14), де розглядаються два випадки. У першому, позначеному як «Емпірична модель», β та α оцінюються на основі даних. У другому випадкуα фіксується на 2, і лише β оцінюється з даних. Цей випадок відповідає сценарію розповсюдження у вільному просторі. Значення, отримані для випадку, розглянутого на рисунку 5.14, наведено в таблиці 5.3. Здається, обидві моделі фіксують поведінку середнього C/N_0 за наявності перешкод, тобто в заштрихованих областях на рисунку 5.13.

Вважається, що кількість AGC у верхньому правому полі на рисунку 5.14. Існує декілька типів контурів зворотного зв’язку AGC [39, с. 135].

Таким чином, можна отримати кілька відгуків на напругу на вході AGC. Слід зазначити, що вхідна напруга AGC пропорційна кореню квадратному з вхідної потужності, і, отже, є функцією відстані перешкод.

У цій роботі розглянуто кілька моделей AGC. Проте модель, де коефіцієнт підсилення AGC прямо пропорційний вхідній напрузі і, отже, обернено пропорційний відстані перешкод, виявилася найефективнішою.

У цьому випадку підрахунок AGC, GAGC, можна змоделювати як GAGC = $G_{max} - \frac{\gamma}{d}$ (5.16),

де G_{max} є максимальним посиленням AGC і є коефіцієнтом пропорційності. Значення, отримані шляхом підгонки емпіричних даних, наведено в таблиці 3. Отримано хорошу підгонку між даними та моделлю. Оцінки мінімального рівня шуму аналізуються в нижньому лівому полі на рисунку 5.14.

Поведінка оцінювача є неінтуїтивною, оскільки значення мінімального шуму зменшуються зі збільшенням потужності перешкод. Однак виробник приймача не надає жодних деталей щодо способу отримання цього параметра та його інтерпретації.

Таким чином, неможливо вивести моделі з фізичним змістом. Проте лінійна тенденція була виявлена в нижньому лівому полі на рисунку 5.14. Нарешті, не можна визначити простий зв’язок для індикатора перешкод CW, який не підходить для виявлення широкосмугових сигналів перешкод.

5.10 Метрики, пов’язані з SDR

Подібно до випадку C/N_0, очікується, що потужність, яку отримує передній кінець, буде функцією відстані між джерелом перешкод і вимірювальною станцією. Зокрема, можна прийняти модель втрат на шляху логарифмічної відстані [45, с. 825]. У цьому випадку прийнята потужність P_{Rx} може бути виражена як:

$$P_{Rx}(d) = K_0 \cdot d^{-\alpha} \tag{5.16}$$

де K_0 є константою, що враховує передану потужність і масштабування, введене ланцюгом прийому, а α є показником втрати шляху. Ця модель відповідає (5.13), коли приймається лінійний масштаб.

У вільному просторі $\alpha = 2$. Розрахункова потужність із використанням зразків інтерфейсу RTL2832U надається як функція відстані. Вимірювання порівнюються з моделлю (5.16), де розглядаються два випадки.

У першому випадку, позначеному як «емпірична модель», і K_0, і α оцінюються на основі даних. У другому випадку α встановлюється рівним 2, і лише K_0 визначається емпірично. Результати, отримані для сценарію, розглянутого на рисунку 5.15, підсумовані в таблиці 5.4. Залежність між отриманою потужністю та відстанню чітко простежується на рисунку 5.13. Крім того, залежність між цими двома змінними добре враховується моделлю втрат на шляху. Для розглянутого сценарію можна зробити припущення вільного простору, $\alpha = 2$. Цей факт можна використати для розробки підходів до локалізації. Подібні міркування застосовуються до оціненої дисперсії, яка зображена в логарифмічному масштабі в нижній лівій частині рисунка 5.15.

Крім того, у цьому випадку модель (5.16) здатна зафіксувати поведінку оціненої дисперсії як функцію відстані. Параметри, оцінені для двох розглянутих випадків (повністю емпіричних і заснованих на моделі вільного простору), наведені в таблиці 5.5. Оцінені значення відрізняються від отриманих для потужності, враховуючи різні нормалізації, прийняті для обчислення цих двох метрики. Важливо відзначити, що насичення аналого-цифрового перетворювача (АЦП), здається, має обмежений вплив на ці два показники. Спектральна ентропія аналізується у верхньому правому полі на рисунку 5.15. У цьому випадку модель (5.16) більше не застосовна, і потрібні додаткові міркування. Спектральна ентропія є максимальною, коли PSD плоска, тобто коли присутній лише шум. При великих значеннях d можна вважати, що глушіння відсутнє і

досягається максимальна ентропія. У розглянутому випадку максимальна ентропія E_{max} дорівнює 6.

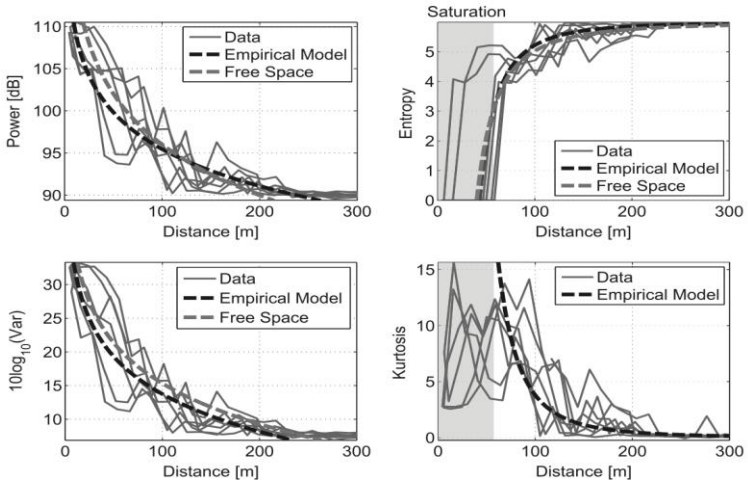


Рис. 5.15 – Метрики, пов’язані з SDR, нанесені на графік як функція відстані [17, с. 107]

RTL2832U використовувався в сценарії зі статичним глушником (J02) і автомобілем, що рухається зі швидкістю 50 км/год. Оцінені параметри моделей наведені в таблиці 5.4.

Таблиця 5.4 — Параметри, оцінені для моделей, розглянутих на рисунку 5.15

Тип	K_0	α
Потужність, емпірична модель	$10^{12.45}$	1.45
Потужність, модель вільного простору	$10^{13.6}$	2
Дисперсія, емпірична модель	$10^{5.05}$	1.83
Дисперсія, модель вільного простору	$10^{5.50}$	2
Ентропія, емпірична модель	$10^{4.8}$	2.3
Ентропія, модель вільного простору	10^{4}	2
Надмірний ексцес, емпірична модель	$10^{6.6}$	3

Ентропія мінімальна, коли PSD складається з чітких спектральних ліній. Можна припустити, що PSD сигналу, пошкодженого глушінням, є сумішшю глушильних спектральних ліній і плоских компонентів. Внесок цих двох компонентів залежить від потужності перешкод. Таким чином, можна припустити наступну емпіричну модель спектральної ентропії:

$$E_t(d) = E_{max} - K_0 d^{-\alpha} \tag{5.17}$$

У (5.17) $d^{-\alpha}$ моделює вплив потужності перешкод: коли d є достатньо великим, потужність перешкод дорівнює нулю, а ентропія приймає своє максимальне значення. d відіграє роль, подібну до ролі експоненти втрати на шляху в (5.16). K_0 є конверсійною константою, яка перетворює ефект потужності перешкод на ентропію. Хоча було використано однакове позначення, дві константи в (5.16) і (5.17) мають різні значення. Незважаючи на те, що модель (5.17) базується на евристичних міркуваннях, вона, здається, належним чином відображає поведінку спектральної ентропії, як показано у верхньому правому полі на рисунку 5.15.

Параметри, оцінені для двох розглянутих випадків, наведені в таблиці 5.4. У цьому випадку ефекти насичення АЦП чітко очевидні. Нарешті, надлишковий ексцес розглядається в нижній лівій частині рисунка 5.13. У цьому випадку неможливо вивести просту модель інтерполяції для вимірювання. Таким чином, розглядається повністю евристична імітація моделі (5.16). Зокрема, надлишковий ексцес моделюється як

$$E_K(d) = K_0 \cdot d^{-\alpha} \tag{5.18}$$

де в цьому випадку K_0 та α не мають фізичного значення. Хоча на надмірний ексцес сильно впливають ефекти насичення, модель (5.18), здається, відображає загальну поведінку цього показника.

Висновки до розділу

Було експериментально досліджено кілька типів метрик для виявлення подій перешкод. Для аналізу були проведені унікальні типи експериментів за участю автомобіля в дорожніх умовах. Випробування були повторені для трьох різних типів перешкод. Було розглянуто два основних типи показників: перший базується на вимірюваннях, наданих приймачем GNSS, тоді як другий використовує зразки, надані недорогим інтерфейсом SDR.

Проаналізовані метрики можна розділити на дві групи: перша забезпечує лише можливості виявлення, тоді як метрики, що належать до другої, також містять інформацію про відстань. В останньому випадку показники відображають отриману потужність перешкод, яка безпосередньо залежить від відстані між перешкодами та блоком виявлення.

Цей другий клас метрик підходить для розробки підходів до локалізації перешкод, які будуть досліджені в майбутньому. Для трьох розглянутих джерел перешкод більшість ефектів обмежені радіусом менше 150 м залежно від метрики, прийнятої для виявлення. Серед показників, заснованих на вимірюваннях стандартного приймача GNSS, середнє значення C/N_0 і кількість AGC є найефективнішою статистикою виявлення, оскільки вони безпосередньо залежать від відстані між джерелом перешкод і приймачем-жертвою.

Емпіричні моделі, що пов’язують метрику з відстанню джерела перешкод, були досліджені, показуючи гарну відповідність емпіричним даним. Середнє значення C/N_0 можна обчислити для більшості приймачів GNSS, і ніяких спеціальних повідомлень не потрібно. Навпаки, підрахунок AGC доступний лише в деяких спеціалізованих приймачах. Однак ця метрика не страждає від проблеми неоднозначності потужності, яка впливає на середнє C/N_0. Дійсно, падіння середнього C/N_0 також може бути наслідком ефектів розповсюдження, таких як ослаблення сигналу. Доступність зразків із інтерфейсу SDR забезпечує найбільшу гнучкість у розробці алгоритму виявлення.

Найбільш перспективні показники, базуються на потужності та дисперсії сигналу. Проведений аналіз також досліджував ефекти насичення, які особливо впливають на такі показники, як спектральна ентропія та надлишковий ексцес. Проведені експерименти та аналіз доповнюють результати, вже наявні в літературі, і дають уявлення про потенціал недорогих платформ для виявлення перешкод.

ВИСНОВКИ

1. Проблема захисту GPS-даних дуже актуальна у наш час, бо багато сервісів та систем критичної інфраструктури, зокрема військових, їх використовує. Тема є комплексною з технічною точки зору та вимагає детального проєктування, тестування та значний інвестицій. Щоб розробити вебресурс, стійкий до різних атак, зокрема популярних спуфінг-атак, окрім фізичної безпеки, треба подбати про надійне шифрування та захищену передачу даних між вузлами системи. Також слід пам’ятати, що найліпшим гарантом кібер-стабільності є простота системи, з кількістю вузлів системи зростає обсяг потенційних вразливостей та недоліків. Також варто подбати про логування трафіку та систему моніторингу, яка дозволить сповістити відповідальних осіб у разі аномалій або неочікуваних атак.

2. У цій магістерській роботі було розглянуто методи та засоби побудови захищеного A-GPS web-ресурсу. Досліджено огляд A-GPS технології та виділені основні проблеми та виклики, пов'язані з її захистом та ефективністю. На основі отриманих даних та аналізу існуючих рішень було сформульовано мету та завдання дослідження.

Для вирішення цих завдань були використані методи дослідження, включаючи тестування на різних платформах та пристроях, аналіз витрат енергії, тестування на точність та швидкість визначення місця, а також оцінку заходів забезпечення безпеки.

На основі проведеного порівняння з існуючими рішеннями було виявлено переваги та недоліки застосованої A-GPS технології. Вона продемонструвала високу точність та ефективність на різних платформах та пристроях, а також має високий рівень безпеки для геолокаційних даних користувачів. Результати дослідження свідчать про успішність та перспективність застосованої захищеної

A-GPS технології для створення web-ресурсу. Вона може бути використана для широкого спектру застосувань, де важливі аспекти точності, ефективності та безпеки геолокаційних даних. Подальші дослідження та вдосконалення можуть допомогти розширити цей підхід та забезпечити його успішне використання у різних сферах. Важливо відзначити, що розробка та впровадження захищеної A-GPS технології вимагає інтеграції технічних, безпекових та користувацьких аспектів. Але вона відкриває можливості для покращення точності та безпеки геолокаційних послуг та може знайти застосування у різних галузях, включаючи навігацію, мобільний маркетинг та безпеку користувачів.

Зокрема, досліджено важливість використання сучасних технологій та заходів безпеки для захисту системи A-GPS від спуфінгу та інших атак. Запропоновані заходи забезпечення безпеки включають аутентифікацію та авторизацію, шифрування даних, моніторинг безпеки, захист від атак на веб-ресурс та систему A-GPS, а також реагування на інциденти.

3. Важливим аспектом дослідження є вибір технологій для розробки web-ресурсу та реалізації функціональності для підтримки A-GPS. Використання сучасних технологій та стандартів дозволяє покращити точність та надійність системи A-GPS.

Крім того, досліджено взаємодію зі супутниковими системами та засобами збору даних A-GPS, а також вивчено можливості впровадження заходів захисту від спуфінгу та інших атак для підвищення надійності та точності місцезнаходження.

4. Отже, загальний висновок полягає в тому, що безпека та надійність системи A-GPS є критично важливими аспектами її розробки та експлуатації. Правильно розроблений web-ресурс, який використовує сучасні технології та заходи безпеки, може значно покращити функціональність та захист системи A-GPS. Така система може стати важливим інструментом для вирішення завдань

місцезнаходження в різних галузях, від навігації до рекреації, від екстреної допомоги до бізнес-аналітики.

У майбутньому дослідження в галузі безпеки A-GPS та розробки web-ресурсів для підтримки цієї технології буде продовжено з метою подальшого вдосконалення системи та забезпечення її безпеки та надійності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петровський А. Алгоритм виявлення впливу спуфінгу під час виконавчої прокладки програмними засобами електронної картографічної навігаційно-інформаційної системи. *Проблеми інформаційних технологій.* 2019. № 25. – [Електронний ресурс]. – Режим доступу: https://core.ac.uk/download/pdf/327130513.pdf (Дата звернення: 20.10.2023).

2. Axell E., Eklöf F. M., Alexandersson M., Johansson P. Jamming Detection in GNSS Receivers: Performance Evaluation of Field Trials, NAVIGATION, Vol. 61, No. 1, Spring 2015, pp. 73–82. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/274264639_Jamming_Detection_in_GNSS_Receivers_Performance_Evaluation_of_Field_Trials (date of the application: 31.08.2023).

3. Bastide F., Akos D., Macabiau C., Roturier B., Automatic Gain Control (AGC) as an Interference Assessment Tool, Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS), Portland, OR, September 2003, pp. 2042–2053. – [Electronic resource]. – Режим доступу: https://enac.hal.science/hal-01021721/document (date of the application: 20.10.2023).

4. Betz J. W. Effect of Partial-Band Interference on Receiver Estimation of C/N_0 : Theory, Proceedings of the National Technical Meeting of The Institute of Navigation, Long Beach, CA, January 2001, pp. 817–828. – [Electronic resource]. – Режим доступу: https://apps.dtic.mil/sti/tr/pdf/ADA457817.pdf (date of the application: 20.10.2023).

5. Bhatti J. A. Humphreys T. E. Hostile Control of Ships via False GPS Signals: Demonstration and Detection. The University of Texas at Austin, Tech. Rep., 2014. – [Electronic resource]. – Режим доступу:

https://radionavlab.ae.utexas.edu/images/stories/files/papers/yacht.pdf (date of the application: 03.10.2024).

6. Borio D., Camoriano L., Savasta S., Lo Presti L. Time-Frequency Excision for GNSS Applications,IEEE Systems Journal, Vol. 2, No. 1, March 2008, pp. 27–37.– [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/3481665_Time-Frequency_Excision_for_GNSS_Applications (Дата звернення: 17.10.2023).

7. Borio D., Fortuny J., O'Driscoll C. Spectral and Spatial Characterization of GNSS Jammers, Proceed- ings of the 7th GNSS Vulnerabilities and Solutions Conference, Baska, Croatia, April 2013, pp. 1–17. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/274951346_Spectral_and_Spatial_Characterization_of_GNSS_Jammers (Дата звернення: 20.10.2023).

8. Borio D., O'Driscoll C., Fortuny J., GNSS Jammers: Effects and Countermeasures, Proceedings of the 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, NL, December 2012, pp. 1–7. – [Electronic resource]. – Режим доступу: https://publications.jrc.ec.europa.eu/repository/handle/JRC80023 (Дата звернення: 20.10.2023).

9. Borio D., Gioia C. Real-Time Jamming Detection Using the Sum-of-Squares Paradigm, Proceed- ings of International Conference on Localization and GNSS (ICL-GNSS), Gothenburg, Sweden, June 2015, pp. 1–6. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/279186292_Real-time_Jamming_Detection_using_the_Sum-of-Squares_Paradigm (date of the application: 31.08.2023).

10. Bhuiyan M. Z. H., Kuusniemi H., Söderholm S., Airos E. The Impact of Interference on GNSS Receiver Observables – A Running Digital Sum Based Simple Jammer Detector, Radioengineering, Vol. 23, No. 3, September 2014, pp. 898–906. –

[Electronic resource]. – Режим доступу: https://www.semanticscholar.org/paper/The-Impact-of-Interference-on-GNSS-Receiver-%E2%80%93-A-Sum-Bhuiyan-Kuusniemi/41292273475e8966ea6d5df74c5e5e88449a635f (Дата звернення: 20.10.2023).

11. Choi K. W. et al., Toward realization of long-range wireless-powered sensor networks, IEEE Wireless Commun., vol. 26, no. 4, pp. 184–192, Aug. 2019. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/334382827_Toward_Realization_of_Long-Range_Wireless-Powered_Sensor_Networks (date of the application: 10.10.2023).

12. Chowdhury A., Karmakar G., Kamruzzaman J., Das R., Attacks on Self-Driving Cars and Their Countermeasures: A Survey, in IEEE Access, vol. 8, pp. 207308-207342, A. 2020. – [Electronic resource]. – Режим доступу: https://researchers.mq.edu.au/en/publications/attacks-on-self-driving-cars-and-their-countermeasures-a-survey (date of the application: 31.08.2023).

13. Cohen, L. Time Frequency Analysis: Theory and Applications, 1st ed., Prentice Hall: Upper Saddle River, NJ, USA, December 1994. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/257427459_Time-frequency_analysis_by_L_Cohen_Prentice_Hall_Signal_Processing_Series_Prentice_Hall_Englewood_Cliffs_New_Jersey_1995_-_Book_review (date of the application: 29.09.2023).

14. Cui Zhao, Zhenjiang Li, Han Ding, Wei Xi, Ge Wang, and Jizhong Zhao. Anti-Spoofing Voice Commands: A Generic Wireless Assisted Design. 2021. – [Electronic resource]. – Режим доступу: https://www.cs.cityu.edu.hk/~zhenjili/2021-UbiComp-WISE.pdf (date of the application: 31.08.2023).

15. Dang Y. , Benzaid C., Yang B., Taleb. T. Deep Learning for GPS Spoofing Detection in Cellular Enabled Unmanned Aerial Vehicle Systems. Jan. 2022. — [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/357552484_Deep_Learning_for_GPS_Spoo

fing_Detection_in_Cellular_Enabled_Unmanned_Aerial_Vehicle_Systems (date of the application: 03.10.2024).

16. Dargie W., Poellabauer C. Fundamentals of Wireless Sensor Networks: Theory and Practice (Wireless Communications and Mobile Computing). 2010. – [Electronic resource]. – Режим доступу: https://www.everand.com/book/145914759/Fundamentals-of-Wireless-Sensor-Networks-Theory-and-Practice (date of the application: 10.10.2023).

17. Dimc Fr. Bazec M. Borio D., Gioia C., Baldini G., Basso M. An Experimental Evaluation of Low-Cost GNSS Jamming Sensors. Journal of The Institute of NavigationVol. 64, No. 1, Spring 2017. pp. 93-109 – [Electronic resource]. – Режим доступу: https://www.ion.org/publications/abstract.cfm?articleID=102706 (date of the application: 10.10.2023).

18. Economist T., GPS Jamming: No Jamming Tomor- row, Technology Quarterly, March. 2011. – [Electronic resource]. – Режим доступу: esearchgate.net/publication/319352641_An_Experimental_Evaluation_of_Low-Cost_GNSS_Jamming_Sensors (date of the application: 10.10.2023).

19. European GNSS Agency (GSA). E-GNSS User Technologies Report. 2022. – [Electronic resource]. – Режим доступу: https://www.gsa.europa.eu/egnss-user-technologies-report-2022 (date of the application: 10.09.2023).

20. Gamba M. T., Motella B., Pini M., Statistical Test Applied to Detect Distortions of GNSS Signals, Proceedings of the International Conference on Local- ization and GNSS (ICL-GNSS), Turin, Italy, June 2013, pp. 1–6. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/261488819_Statistical_test_applied_to_detect_distortions_of_GNSS_signals (date of the application: 14.09.2023).

21. Georg T. Becker, Sherman C. Lo, David S. De Lorenzo, Per K., Christof PaarSecure Location Verification A Security Analysis of GPS Signal Authentication 1. 2010. – [Electronic resource]. – Режим доступу:

https://web.stanford.edu/group/scpnt/gpslab/pubs/papers/Becker_DBsec_2010_CameraReady.pdf (date of the application: 10.09.2023).

22. Global Positioning System Standard Positioning Service Performance Standard, 4th ed., U.S. Department of Defense, Sep. 2008. – [Electronic resource]. – Режим доступу: https://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf (date of the application: 31.08.2024).

23. Graham A., Communications, Radar and Electronic Warfare, John Wiley & Sons: Chichester, West Sussex, UK, January 2011. – [Electronic resource]. – Режим доступу: https://www.wiley.com/en-us/Communications%2C+Radar+and+Electronic+Warfare-p-9780470977170 (date of the application: 12.09.2023).

24. Grant A., Williams P., Ward N., Basker S., GPS Jamming and the Impact on Maritime Naviga- tion,Journal of Navigation, Vol. 62, April 2009, pp. 173–187.– [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/228897052_GPS_Jamming_and_the_Impact_on_Maritime_Navigation (date of the application: 12.09.2023).

25. Humphreys T. E., Ledvina B. M., Psiaki M. L. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer // 21st International Technical Meeting of the Satellite Division of The Institute of Navigation. ser. ION GNSS ’08, Savannah, GA, USA, Sep. 2008, pp. 2314–2325. – [Electronic resource]. – Режим доступу: https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf (date of the application: 30.09.2024).

26. Humphreys T. E. Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing. The University of Texas at Austin, Tech. Rep., Jul. 2012. – [Electronic resource]. – Режим доступу: https://rnl.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf (date of the application: 02.10.2024).

27. Humphreys T. E. Statement on the Security Threat Posed by Unmanned Aerial Systems and Posssible Countermeasures. The University of Texas at Austin, Tech. Rep., Mar. 2015. – [Electronic resource]. – Режим доступу: https://radionavlab.ae.utexas.edu/images/stories/files/papers/statement-humphreys-20150318.pdf (date of the application: 02.10.2024).

28. ICS-CERT. ICS-CERT Monthly Monitor. Industrial Control Systems Cyber Emergency Response Team. 2021. – [Electronic resource]. – Режим доступу: https://us-cert.cisa.gov/ics/monitors (date of the application: 10.09.2023).

29. Jaynes M., Dantu R., Varriale R., Evans N. Automating ecu identification for vehicle security," in Machine Learning and Applications (ICMLA), 2016 15th IEEE International Conference on. IEEE, 2016, pp. 632–635. – [Electronic resource]. – Режим доступу: https://nsl.cse.unt.edu/sites/default/files/biblio/documents/Automating_ECU_Identification_Vehicle_Security.pdf (date of the application: 10.11.2023).

30. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology (NIST) Special Publication 800-144. 2011. – [Electronic resource]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf (date of the application: 10.09.2023).

31. John A. Vulnerability assessment of the transportation infrastructure relying on the global positioning system. Final Report. 2001. – [Electronic resource]. – Режим доступу: https://rosap.ntl.bts.gov/view/dot/8435 (date of the application: 30.09.2024).

32. Kerry A. McKay, David A. Cooper Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. 2019. – [Electronic resource]. – Режим доступу: https://www.nist.gov/publications/guidelines-selection-configuration-and-use-transport-layer-security-tls-0 (date of the application: 31.08.2023).

33. Li T., Zhang H., Z. Gao, X. Niu, N. El-sheimy. Tight fusion of a monocular camera, MEMS-IMU, and single-frequency multi-GNSS RTK for precise navigation in GNSS-Challenged environments, Remote Sens., vol. 11, 2019. – [Electronic resource]. – Режим доступу: https://www.mdpi.com/2072-4292/11/6/610 (date of the application: 31.08.2023).

34. Lindstrom J., Akos D. M., IsozмO., Junered M., GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules, Proceed- ings of the 20th International Technical Meeting ofhe Satellite Division of The Institute of Navigation (ION GNSS), Fort Worth, TX, September 2007, pp. 1165–1172. – [Electronic resource]. – Режим доступу: https://www.diva-portal.org/smash/get/diva2:1011883/FULLTEXT01.pdf (date of the application: 10.11.2023).

35. Mark L. Psiaki, Todd E. Humphreys. GNSS Spoofing and Detection // Proceedings of the IEEE. 2016. Vol. 104. pp. 1258 - 1270. — [Electronic resource]. – Режим доступу: https://ieeexplore.ieee.org/document/7445815 (date of the application: 03.10.2024).

36. Michael Cobb M., Loshin P. What is SSL? A Comprehensive Guide to Secure Sockets Layer. SearchSecurity. 2021. – [Electronic resource]. – Режим доступу: https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL (date of the application: 10.09.2023).

37. Mitch R. H., Dougherty R. C., Psiaki M. L., and others Signal Characteristics of Civil GPS Jam- mers, Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION/GNSS), Portland, OR, September 2011, pp. 1907–1919. – [Electronic resource]. – Режим доступу: https://repositories.lib.utexas.edu/items/293e1da1-b2fc-4184-ae12-6e81452bca05 (date of the application: 30.08.2023).

38. Montemerlo M., Becker J., Bhat S., Dahlkamp H., Dolgov D., Ettinger S., Thrun S. Winning the DARPA Urban Challenge. Journal of Field Robotics. 2008. № 25(9),

pp. 569-597. – [Electronic resource]. – Режим доступу: https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=7239B2166AE65C95FE0876B7D0414B63?doi=10.1.1.375.6154&rep=rep1&type=pdf (date of the application: 31.08.2023).

39. Morgan D., On Discrete-Time AGC Amplifiers, IEEE Transactions on Circuits and Systems, Vol. 22, No. 2, February 1975, pp. 135–146. – [Electronic resource]. – Режим доступу: https://ieeexplore.ieee.org/document/1084014 (date of the application: 31.08.2023).

40. Musumeci, L., and Dovis, F., "Use of the Wavelet Transform for Interference Detection and Mitigation in Global Navigation Satellite Systems," International Journal of Navigation and Observation, Vol. 2014, 2014, pp. 1–14.

41. National Institute of Standards and Technology (NIST). Guide to the General Data Protection Regulation (GDPR). NIST Special Publication 800-183. 2020. – [Electronic resource]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf (date of the application: 10.09.2023).

42. Ndili A., Enge P., GPS Receiver Autonomous Interference Detection, IEEE Position Location and Navigation Symposium, Rancho Mirage, California, US, April 1998, pp. 123–130. – [Electronic resource]. – Режим доступу: https://web.stanford.edu/group/scpnt/gpslab/pubs/papers/Ndili_IEEELNS_1999_interfere_detect.pdf (date of the application: 15.09.2023).

43. Нетаврована, А. В. Методи виявлення GPS Spoof атак на безпілотні літальні апарати // XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 11-12 травня 2023 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2023. – С. 144-147. – [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/handle/123456789/62406 (Дата звернення: 20.10.2023).

44. OWASP Mobile Security Testing Guide. Open Web Application Security Project. 2022. – [Electronic resource]. – Режим доступу: https://owasp.org/www-project-mobile-security-testing-guide/ (date of the application: 10.11.2023).

45. Okumura Y., Ohmori E., Kawano T., Fukuda K., Field Strength and its Variability in VHF and UHF Land-Mobile Radio Service. of the Electrical Communication Laboratory, Vol. 16, No. 9–10, 1968, pp. 825–873.– [Electronic resource]. Режим доступу: https://www.scirp.org/reference/referencespapers?referenceid=3485198 (date of the application: 10.11.2023).

46. OSQZSS. Software-Defined GPS Signal Simulator. 2017. – [Electronic resource]. – Режим доступу: https://github.com/osqzss/gps-sdr-sim (date of the application: 03.10.2024).

47. Pham M., Xiong K. A survey on security attacks and defense techniques for connected and autonomous vehicles. Computers & Security. 2017. 109. pp. 102269. – [Electronic resource]. – Режим доступу: https://arxiv.org/abs/2007.08041 (date of the application: 31.08.2023).

48. Psiaki M. L., Humphreys T. E. Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies // IEEE Spectrum. 2016. Vol. 53. №. 8. pp. 26–53. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/305744597_Attackers_can_spoof_navigation_signals_without_our_knowledge_Here's_how_to_fight_back_GPS_lies (date of the application: 01.10.2024).

49. Pullen S., Gao G. X., GNSS Jamming in the Name of Privacy, Inside GNSS, March/April 2012, pp. 34–43. – [Electronic resource]. – Режим доступу: https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.74 (date of the application: 30.08.2023).

50. Qingming Chen, Peng Liu, Guoqiang Li, Zhenpo Wang GPS Attack Detection and Mitigation for Safe Autonomous Driving using Image and Map based Lateral

Direction Localization. – [Electronic resource]. – Режим доступу: https://arxiv.org/pdf/2310.05407.pdf (date of the application: 31.08.2023).

51. Ranganathan D.-Y. Yu, A., Locher T., Capkun S., Basin D. Short Paper: Detection of GPS Spoofing Attacks in Power Grids // ACM Conference on Security and Privacy in Wireless and Mobile Networks, ser. WiSec '14. Oxford, United Kingdom: ACM, Jul. 2014, pp. 99–104. – [Electronic resource]. – Режим доступу: https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/publications/pub2014/wisec039s-yu.pdf (date of the application: 02.10.2024).

52. Russon M.-A.Wondering how to hack a military drone? It's all on Google // International Business Times. May 2015. – [Electronic resource]. – Режим доступу: http://www.ibtimes.co.uk/wondering-how-hackmilitary-drone-its-all-google-1500326 (date of the application: 03.10.2024).

53. Ryan D. Restivo, Laurel C. Dodson, Jian Wang, Wenkai Tan. GPS Spoofing on UAV: A Survey. 2023. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/373498813_GPS_Spoofing_on_UAV_A_Survey (date of the application: 31.08.2023).

54. Rouse M. Two-Factor Authentication (2FA). SearchSecurity. 2021. – [Electronic resource]. – Режим доступу: https://searchsecurity.techtarget.com/definition/two-factor-authentication-2FA (date of the application: 03.08.2023).

55. Sabatini R., Terry Moore, Subramanian Ramasamy. Global Navigation Satellite Systems Performance Analysis and Augmentation Strategies in Aviation. 2017. – [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/321022891_Global_Navigation_Satellite_Systems_Performance_Analysis_and_Augmentation_Strategies_in_Aviation (date of the application: 10.10.2023).

56. Schmidt Desmond, Kenneth Radke, Seyit A Camtepe, Ernest Foo. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. 2016. – [Electronic

resource]. – Режим доступу: https://www.researchgate.net/publication/301798786_A_Survey_and_Analysis_of_the_GNSS_Spoofing_Threat_and_Countermeasures (date of the application: 31.08.2023).

57. Sebastian C. Getting lost near the Kremlin? Russia could be 'GPS spoofing' // CNN Business. Dec. 2016. – [Electronic resource]. – Режим доступу: http://money.cnn.com/2016/12/02/technology/kremlin-gps-signals (date of the application: 03.10.2024).

58. Song H. M., Kim H. R., Kim H. K. Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in Information Networking (ICOIN), 2016 International Conference on. IEEE, 2016, pp. 63–68. – [Electronic resource]. – Режим доступу: https://www.semanticscholar.org/paper/Intrusion-detection-system-based-on-the-analysis-of-Song-Kim/6c7e55e3b53029296097ee07ba75b6b6a98b14e5 (date of the application: 10.11.2023).

59. Shetty P., Hegadi R. S. Location Based Services Using A-GPS for Mobiles. International Journal of Advanced Research in Computer and Communication Engineering, 2(8). 2013 – [Electronic resource]. – Режим доступу: https://ijarcce.com/upload/2013/august/IJARCCE2D%20v%2021.pdf (date of the application: 03.08.2023).

60. Sheridan K., Ying, Y., Whitworth, T., Pre-and Post-Correlation GNSS Interference Detection Within Software Defined Radio, Proceedings of the 25th International Technical Meeting of The Satellite Division of The Institute of Navigation (ION GNSS), Nashville, TN, September 2012, pp. 3542–3548.– [Electronic resource]. – Режим доступу: https://aric-aachen.de/wordpress/wp-content/uploads/2021/06/ION2012_Paper-1.pdf (date of the application: 04.08.2023).

61. Sushant Pawar, Gaikwad K . Designing and Implementation of Real-Time GPS Receiver System for Navigation and Location Based Services. 2014.– [Electronic resource]. – Режим доступу: https://www.researchgate.net/publication/264041745_Designing_and_Implementation_of_Real-Time_GPS_Receiver_System_for_Navigation_and_Location_Based_Services (date of the application: 03.08.2023).

62. Swaszek P. F., Hartnett R. J. Spoof Detection Using Multiple COTS Receivers in Safety Critical Applications // International Technical Meeting of The Satellite Division of the Institute of Navigation, ser. ION GNSS+ ’13, Nashville, TN, USA, Sep. 2013, pp. 2921–2930. – [Electronic resource]. – Режим доступу: https://digitalcommons.uri.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1003&context=ele_facpubs (date of the application: 03.10.2024).

63. Tippenhauer N. O., Popper C., Rasmussen K. B., Capkun S. On the Requirements for Successful GPS Spoofing Attacks // ACM Conference on Computer and Communications Security, ser. CCS ’11. Chicago, IL, USA: ACM, Oct. 2011, pp. 75–86. – [Electronic resource]. – Режим доступу: https://nyuscholars.nyu.edu/en/publications/on-the-requirements-for-successful-gps-spoofing-attacks (date of the application: 02.10.2024).

64. Tyree Z., Bridges R. A., Combs F. L., Moore M. R. Exploiting the Shape of CAN Data for In-Vehicle Intrusion Detection. 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL. USA, 2018. pp. 1-5. – [Electronic resource]. – Режим доступу: https://www.osti.gov/servlets/pРежим доступу/1513428 (date of the application: 31.08.2023).

65. United States Computer Emergency Readiness Team (US-CERT). Security of Mobile Devices. 2021. – [Electronic resource]. –Режим доступу: https://us-cert.cisa.gov/ncas/tips/ST04-020 (date of the application: 03.08.2023).

66. Ulrych T. J., Bishop T. N., Maximum Entropy Spectral Analysis and Autoregressive Decomposition, Reviews of Geophysics and Space Physics, Vol. 13,

No. 1, February 1975, pp.183–200. – [Electronic resource]. – Режим доступу: https://agupubs.onlinelibrary.wiley.com/doi/abs/10.1029/RG013i001p00183. (date of the application: 31.08.2023).

67. Ublox AG, Thalwil, Switzerland, u-blox 6 Receiver Description Including Protocol Specification, April 2013. – [Electronic resource]. – Режим доступу: http://repository.umy.ac.id/bitstream/handle/123456789/11321/k.%20Lampiran.pdf?sequence=11&isAllowed=y (date of the application: 31.08.2023).

68. Yubin Zhao, Xiaofan Li , Senior Member, Huaming Wu, Cheng-Zhong Xu. Energy Beamforming for Cooperative Localization in Wireless-Powered Communication Network. IEEE INTERNET OF THINGS JOURNAL, VOL. 8, NO. 17, SEPTEMBER 1, 2021. – [Electronic resource]. – Режим доступу: http://huamingwu.cn/PDF/JIOT_Zhao.pdf (date of the application: 10.10.2023).

69. Welch P. D. The Use of Fast Fourier Transform for the Estimation of Power Spectra: A Method Based on Time Averaging Over Short, Modified Periodograms, IEEE Transactions on Audio Electroacoust, Vol. 15, No. 2, June 1967, pp. 70–73. – [Electronic resource]. – Режим доступу: https://ieeexplore.ieee.org/document/1161901 (date of the application: 10.10.2023).

70. Vallés E., Yu C., Elasmar R., Interfer- ence Detection Algorithms for Gnss-Enabled Android Devices, Proceedings of the 28th International Techni- cal Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), Tampa, Florida, September 2015, pp. 1–8. – [Electronic resource]. – Режим доступу: https://www.proceedings.com/content/028/028935webtoc.pdf (date of the application: 10.10.2023).

71. Zia Muhammad, Zahid Anwar, Abdul Rehman Javed. Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses. 2023. – [Electronic resource]. – Режим доступу: https://www.mdpi.com/2227-7080/11/3/76 (date of the application: 31.08.2023).

72. Zhuravlov D., Polshakova O. Detection of face spoofing attacks on biometric identification systems. *Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління».* 2023 № 1(42). – [Електронний ресурс]. – Режим доступу: file:///Users/admin/Downloads/279095-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-643346-1-10-20230512.pdf (Дата звернення: 20.10.2023)

Додаток А

Архітектура A-GPS системи

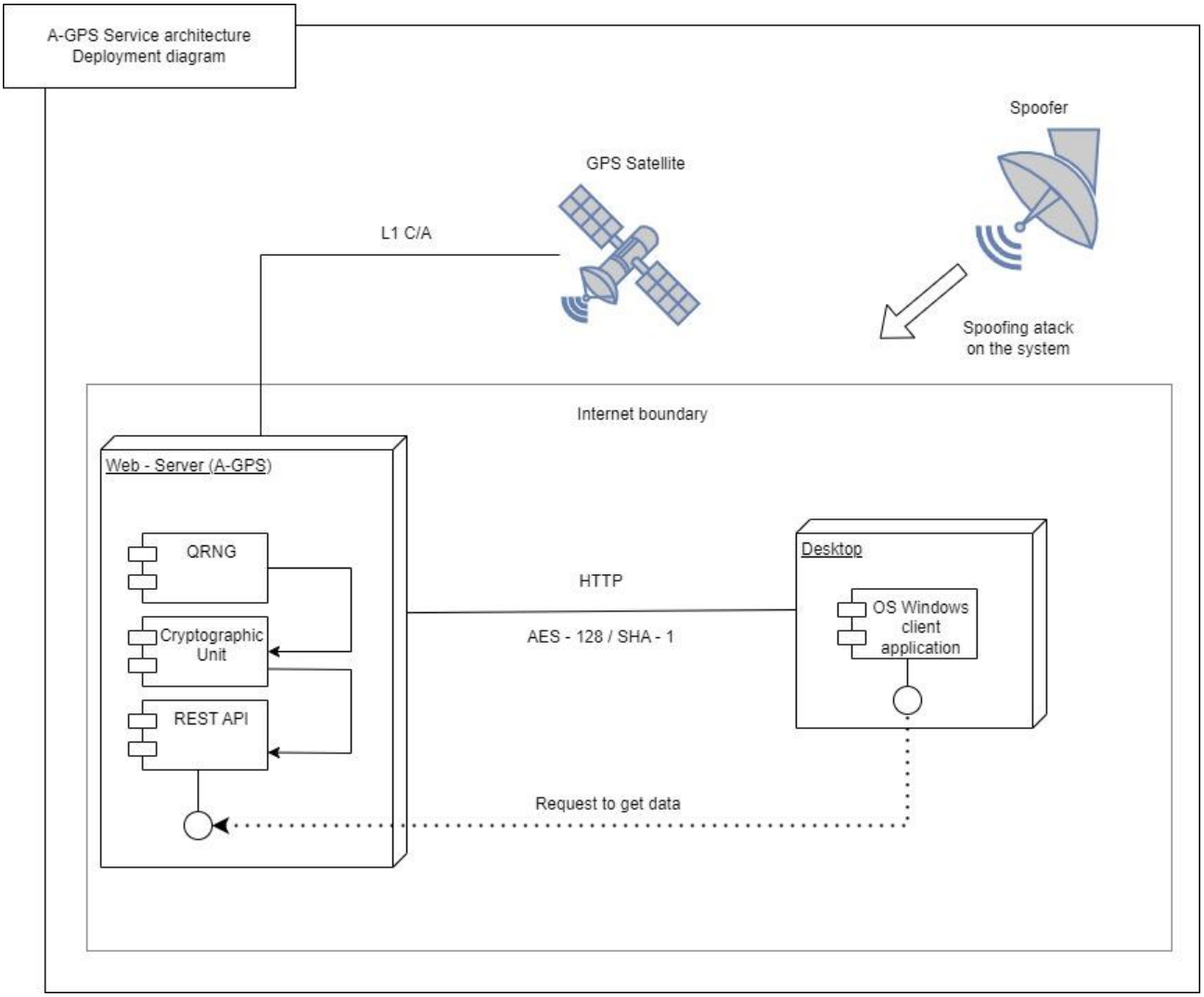


Рис. 1 — Діаграма розгортання A-GPS системи

Додаток Б

Інтерфейс користувача розробленого застосунку

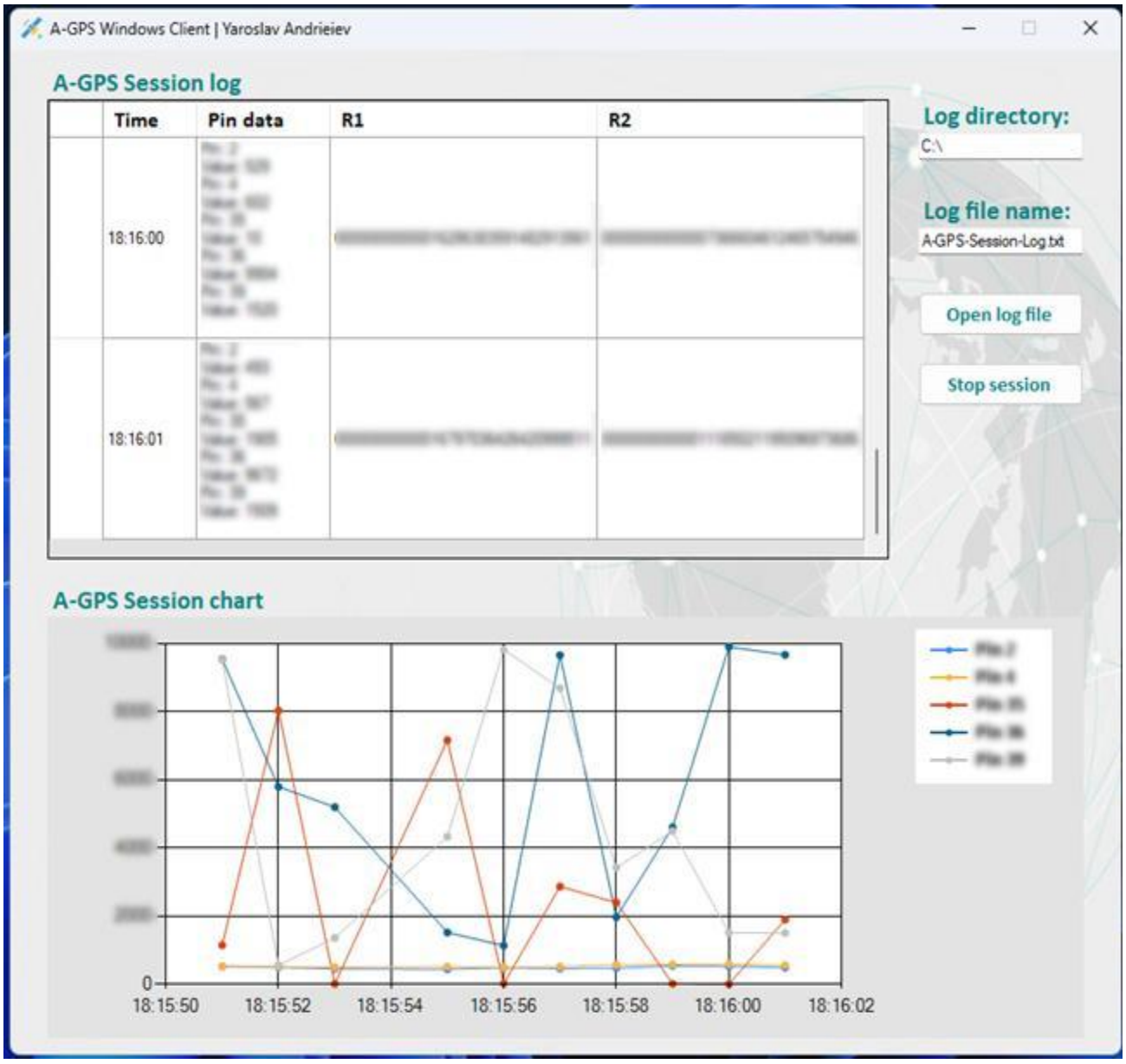


Рис. 2 — Інтерфейс користувача клієнського застосунку для операційної системи Windows

Додаток В

Вивід отриманих даних у текстовий файл

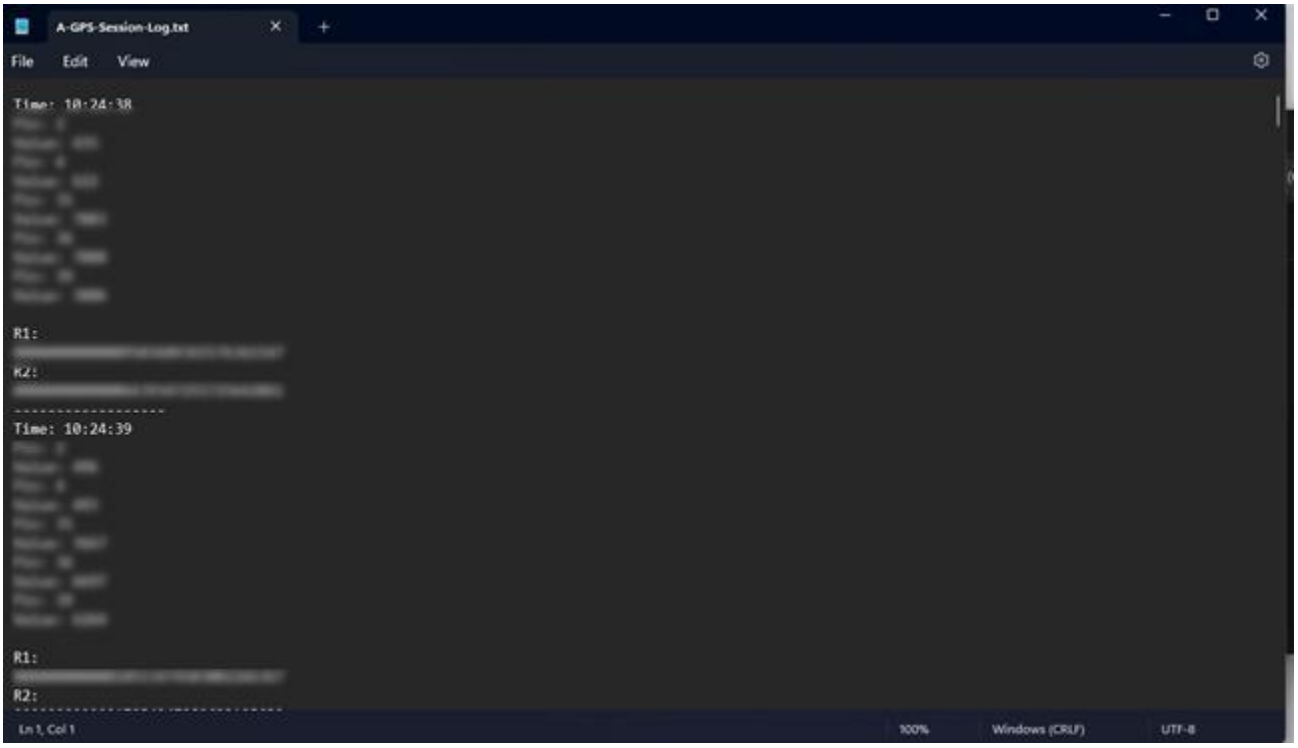


Рис. 3 — Результат виведення отриманих даних від серверу A-GPS

Додаток Г

Публікація у науковій конференції «II INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE Modern Approaches to Problem Solving in Science and Technology»

Modern Approaches to Problem Solving in Science and Technology

METHODS AND MEANS FOR BUILDING A SECURE A-GPS WEB RESOURCE

Yaroslav Andrieiev
Master's student at the Department
of Information Systems
and Technologies Security,
yaroslav.andrieiev@student.karazin.ua
Oleksiy Nariezhnii
Candidate of Technical Sciences,
Associate Professor at the Department
of Information Systems
and Technologies Security,
o.nariezhnii@karazin.ua
V. N. Karazin Kharkiv National University, Ukraine

Problem Statement. Contemporary world is undergoing unforeseen changes, and one of the main directions of these transformations is the expansion and integration of global navigation systems. Geospatial data and local services have become indispensable components of modern life, from navigating large-scale transportation to instantly pinpointing the location of friends on a smartphone. However, consumers of these services, as well as the sectors where they are utilized, face challenges related to accuracy and security.

Protected A-GPS (Assisted Global Positioning System) is one of the approaches aimed at improving the accuracy and security of global navigation. This technology combines the use of satellites, ground segment stations, internet servers, and specialized algorithms to provide fast and precise user location determination [1].

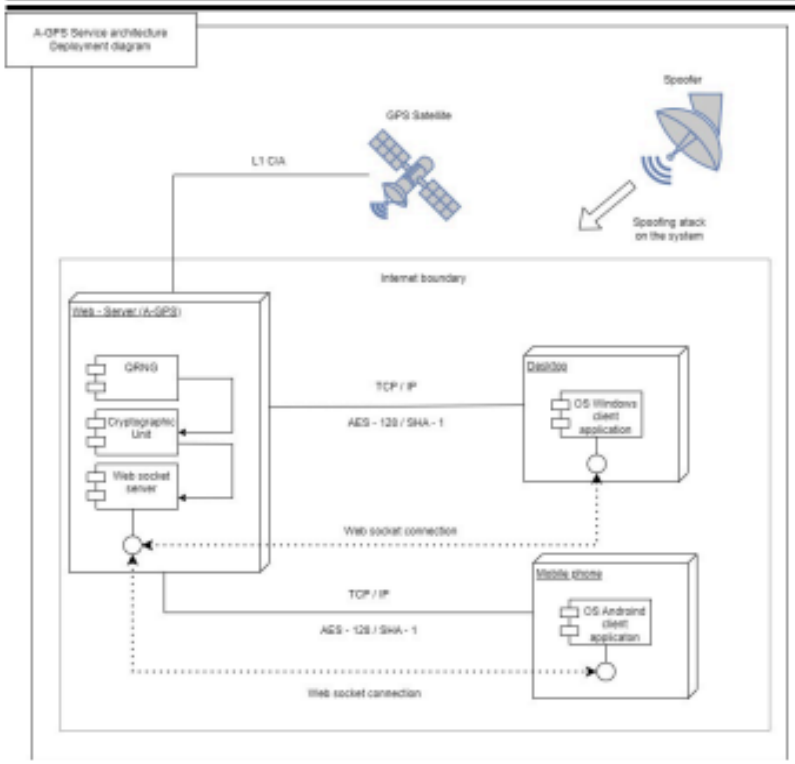
However, the practical implementation of this technology requires the creation of specialized web resources capable of processing and providing access to this data. Currently, there is a significant threat in Ukraine of various attacks on state and industrial institutions with the aim of reducing accuracy or disrupting services that rely on GPS information. One of the most common cases is the execution of spoofing attacks. Therefore, it is necessary to investigate the development of a secure A-GPS communication to ensure the stable operation of critical infrastructure.

Aims. The objective of our work is to develop and implement an innovative web resource that contributes to the improvement of security, reliability, and efficiency of the A-GPS system. This goal requires researching modern methods and tools for ensuring the security and reliability of A-GPS technology, developing appropriate algorithms and software, as well as validating and testing the developed web resource.

Results and discussion. Protection against spoofing in the A-GPS system requires the implementation of a comprehensive set of measures and technologies to ensure the reliability and integrity of location data.

153

Рис. 4 — Публікація у конференції перша сторінка



Picture 1 - Deployment Diagram of the Proposed Architecture

On the picture 1, the proposed application architecture is depicted, where the central component is the server-side «Web-server». This is a web application that receives coordinates from GPS satellites using L1 C/A. To transmit this data to clients, it must be encrypted using AES-128. For this purpose, on the server side, there is a quantum random number generator and a crypto module. Additionally, each data packet is signed using SHA-1. During data transmission, asymmetric encryption is employed, and upon receiving the data, the client-side verifies data integrity using SHA-1 hash sums.

Not recommended to use MD5 as it is not cryptographically secure. The client-side is represented by a personal computer «Desktop» as well as a mobile application «Mobile phone». Communication takes place via websockets to ensure real-time communication.

Conclusions. The issue of protecting GPS data is highly relevant today, as many services and critical infrastructure systems, including military ones, heavily rely on it. The topic is complex from a technical perspective and requires detailed design, testing,

Рис. 5 — Публікація у конференції друга сторінка

Додаток Д

Фрагмент коду клієнської частини, який відповідає за оновлення таблиці та графіків

```
private async Task UpdateTableInfinite(CancellationToken token)
      {
         while (!token.IsCancellationRequested)
         {
            GetSessionData();
  string[] cellTexts = { _sessionData.CurrentTime, JoinPinDataToDisplay(_sessionData.Pins),
_sessionData.R1, _sessionData.R2 };
            await Task.Run(() =>
            {
               this.Invoke((MethodInvoker)delegate
               {
                  dataGridView1.Rows.Add(cellTexts);
                  if (dataGridView1.RowCount > 1)
                  {
                    dataGridView1.FirstDisplayedScrollingRowIndex = dataGridView1.RowCount - 1;
                  }
                  var dateTime = DateTime.Parse(_sessionData.CurrentTime);
                  foreach (var pin in _pinNumbers)
                  {
                     var pinName = $"Pin {pin}";
                     chart1.Series[pinName].Points.AddXY(
                        dateTime.ToOADate(),
       _sessionData.Pins.FirstOrDefault(x => x.PinNumber.ToString().Equals(pin)).PinValue);
                  }
               });
            }, token);
            await WriteLogToFile().ConfigureAwait(false);
            await Task.Delay(700, token);
         }
      }
```