

Розробка математичної моделі GPS спуфінгу в умовах роботи CRPA

Олександр Білик^{1*} та Олександр Мартинчук^{1†}

¹ Харківський національний університет радіоелектроніки, проспект Науки, 14, Харків, Україна

Анотація

В дослідженні проведено аналіз та створення математичних моделей для оцінки ефективності GPS спуфінгових атак та засобів захисту сигналів навігації з адаптивним використанням антенних решіток (CRPA). Розроблено програму в середовищі моделювання Matlab та проаналізовано на основі моделі впливу спуфінгових атак на правильність прийому сигналів супутникової навігації.

Ключові слова

GPS, CRPA, spoofing, навігація, моделювання сигналів

1. Вступ

CRPA (Controlled Reception Pattern Antenna) — це технологія антен, яка використовує масив антенних елементів для контролю діаграми спрямованості прийому сигналу. Вона дозволяє керувати напрямком прийому сигналу та приглушувати завади, покращуючи якість прийому супутникових сигналів в GPS або GNSS системах. До основні переваг CRPA слід віднести:

1. Придушення завад: CRPA може активно приглушувати сигнали від джерел перешкод, що дозволяє надійно приймати сигнал навіть у складних умовах.
2. Покращена точність позиціонування: завдяки здатності адаптувати приймальну діаграму, CRPA може підвищити точність визначення місцезнаходження.
3. Захист від спуфінгу: така антена може бути більш стійкою до спроб фальсифікації сигналу.

GPS спуфінг — це форма впливу на прийом корисного сигналу, під час якого транслюються підроблені сигнали, які імітують справжні супутникові сигнали, з метою змусити приймач прийняти неправильні дані про своє місцезнаходження або час і в подальшому дезорієнтувати об'єкт у просторі.

2. Основні підходи спуфінгу в GPS/GNSS

1. Імітація супутникових сигналів: Спуфер (той, хто проводить атаку) генерує сигнали, що виглядають як справжні GPS/GNSS сигнали, але містять неправильну інформацію про позицію або час. Приймач, приймаючи ці підроблені сигнали, визначає своє місцезнаходження чи час неправильно.

Information Systems and Technologies (IST-2024), November 26-28, 2024, Kharkiv, Ukraine

* Corresponding author.

† These authors contributed equally.

✉ oleksandr.bilyk@nure.ua (О.Білик); oleksandr.martynchuk@nure.ua (О.О.Мартинчук)

ORCID [0009-0007-4846-1585](https://orcid.org/0009-0007-4846-1585) (О. Білик); [0000-0001-9729-4401](https://orcid.org/0000-0001-9729-4401) (О.О.Мартинчук)



© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

2. Зміщення позиції: Однією з цілей спуфінгу є зміна координат, які отримує жертва. Наприклад, корабель або автомобіль можуть почати рух у неправильному напрямку через те, що їхній приймач GNSS показує помилкове місцезнаходження.
3. Зміна часу: Системи, які покладаються на точний час від супутників, можуть отримати неправильні дані про час, що може спричинити серйозні наслідки для банківських транзакцій, телекомунікацій або енергетичних систем, які синхронізуються через GNSS.

Створення процесу спуфінга:

- Підроблений сигнал: Зловмисник генерує сигнал, схожий на сигнал справжнього супутника. Цей сигнал зазвичай сильніший за оригінальний супутниковий сигнал, тому приймач помилково приймає його за правильний.
- Захоплення приймача: Після того, як приймач починає приймати підроблений сигнал, спуфер поступово зміщує дані про місцезнаходження чи час, змушуючи приймач показувати некоректну інформацію.
- Перешкоди в роботі: Це може вплинути на транспортні засоби (автомобілі, судна, дрони), які залежать від точного визначення місцезнаходження, і може призвести до серйозних аварій або порушень..

3. Розробка математичної моделі GPS спуфінгу в умовах роботи з CRPA

Розробка математичної моделі GPS спуфінгу в умовах роботи з CRPA (Controlled Reception Pattern Antenna) передбачає врахування таких аспектів:

1. Симуляція сигналу супутника: корисний сигнал із GPS/GNSS.
2. Симуляція спуфінгового сигналу: навмисно сформований завадами сигнал із характерними затримками, зміщенням частоти та поляризаційними параметрами.
3. CRPA-система: антени, які забезпечують просторово-поляризаційну обробку сигналу для придушення спуфінгу.

Спуфінгові сигнали, які намагаються імітувати корисний сигнал, мають схожу фазу та частоту. CRPA здатна розрізняти такі сигнали, оцінюючи фазові зсуви та амплітуду сигналів з різних елементів антенної решітки:

$$\Delta\varphi = \arg \arg (W^H y(t)) - \arg(y(t)) \quad (1)$$

Модель прийнятого сигналу:

$$r(t) = A_{GPS} \cos \cos(2\pi f_{GPS} t + \varphi_{GPS}) + A_{spoof} \cos \cos(2\pi f_{spoof} t + \varphi_{spoof} + \Delta\varphi) \quad (2)$$

Основними методами протидії спуфінгу є:

- Аналіз фазових та амплітудних зсувів у системі.
- Використання методів спектрального аналізу для ідентифікації спуфінгових сигналів.

На рисунку 1 представлені результати моделювання за допомогою програмного забезпечення Matlab. На графіках можна побачити нормалізовані значення АЧХ корисного сигналу, спуфінгового сигналу (постановника завади) та результуючий сигнал після обробки з виходу CRPA.

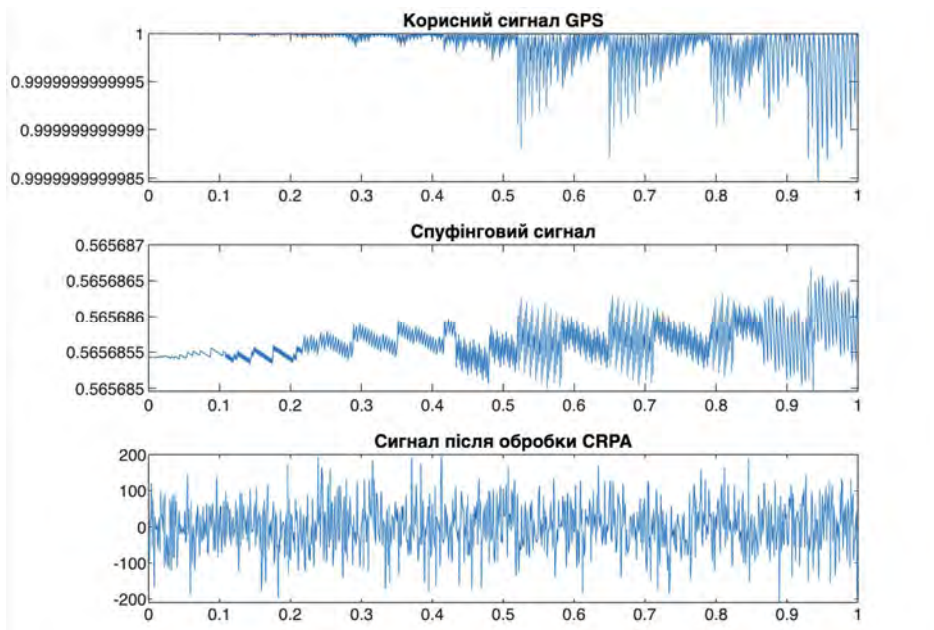


Рисунок 1. Моделювання процесу GPS спуфінгу.

1. Створення сигналів: GPS та спуфінговий сигнал мають різну частоту й фазу, що імітує реальні умови.
2. CRPA: вектор напрямної діаграми враховує просторові параметри.
3. Придушення завад: застосовано інверсію коваріаційної матриці для оптимального формування діаграми направленості.
4. Візуалізація: Аналіз ефективності CRPA в придущенні спуфінгу.

Дана модель може бути розширена додаванням поляризаційного аналізу та більш складними умовами поширення.

4. Висновки

Використання адаптивних антенних решіток та алгоритмів просторово-часової обробки навігаційних системах значно підвищує стійкість сигналів на виході антени. Для покращення аналізу можливого впливу на системи навігації дана модель може бути розширена додаванням поляризаційного аналізу та більш складними умовами поширення.

References

- [1] A. Altaweel, H. Mulkath and I. Kamel, "GPS Spoofing Attacks in FANETs: A Systematic Literature Review," in *IEEE Access*, vol. 11, pp. 55233-55280, 2023, doi: 10.1109/ACCESS.2023.3281731.
- [2] E. Horton and P. Ranganathan, "Development of a GPS spoofing apparatus to attack a DJI Matrice 100 quadcopter", *J. Global Positioning Syst.*, vol. 16, no. 1, pp. 1-11, Dec. 2018.
- [3] T. Humphreys, Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing, Austin, TX, USA, pp. 1-16, Jul. 2012.
- [4] I. Bisio, C. Garibotto, H. Haleem, F. Lavagetto and A. Sciarrone, "A systematic review of drone based road traffic monitoring system", *IEEE Access*, vol. 10, pp. 101537-101555, 2022.