УДК 004.8

Сергєєв В.М., аспірант
П'ятаченко В.Ю., PhD., асистент
Сумський державний університет

СИМУЛЯЦІЯ АТАК ПІДМІНИ КООРДИНАТ У НАВІГАЦІЙНИХ ДАНИХ ДЛЯ ТЕСТУВАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Супутникові навігаційні системи широко використовуються в безпілотних і транспортних платформах для визначення координат та навігації. Однією з основних загроз для таких систем є атаки підміни координат (GNSS spoofing), які дозволяють змінювати навігаційні дані без фізичного впливу на об’єкт. У зв’язку з цим активно розробляються методи виявлення подібних атак, зокрема на основі аналізу навігаційних параметрів і алгоритмів машинного навчання.

Ефективність таких підходів значною мірою залежить від наявності даних із реальними сценаріями атак. Проте їх отримання є складним, оскільки проведення експериментів із підробленням навігаційного сигналу потребує спеціалізованого обладнання та може бути обмежене умовами експлуатації. Тому доцільним є використання тестових середовищ, які дозволяють відтворювати сценарії атак шляхом математичної трансформації навігаційних даних.

У сучасних дослідженнях виявлення GNSS-спуфінгу широко застосовується аналіз навігаційних даних та часових рядів параметрів руху. У роботі [1] запропоновано використання глибоких нейронних мереж для аналізу навігаційних параметрів (координати, швидкість, курс), що дозволяє виявляти аномалії траєкторії без аналізу сирих GNSS-сигналів. У дослідженні [2] показано ефективність поєднання кількох груп ознак навігаційного стану, включаючи похідні координат та параметри руху, для підвищення точності виявлення атак. У роботі [3] розглянуто фізичну модель GNSS-спуфінгу, відповідно до якої атака реалізується шляхом зміни псевдовідстаней до супутників, що призводить до поступового відведення навігаційного рішення приймача.

Для формування наборів даних із контрольованими сценаріями атак розроблено веборієнтований інструмент із API, що дозволяє працювати з реальними позиційними даними повітряних суден. Як вхідні дані використовуються координати польоту, отримані з джерел авіаційного моніторингу. В режимі симуляції формується атакована траєкторія шляхом модифікації навігаційних параметрів (рис.1). Отримані дані зберігаються у вигляді часових рядів реальних та атакованих координат і можуть використовуватися для тестування алгоритмів виявлення атак підміни координат.

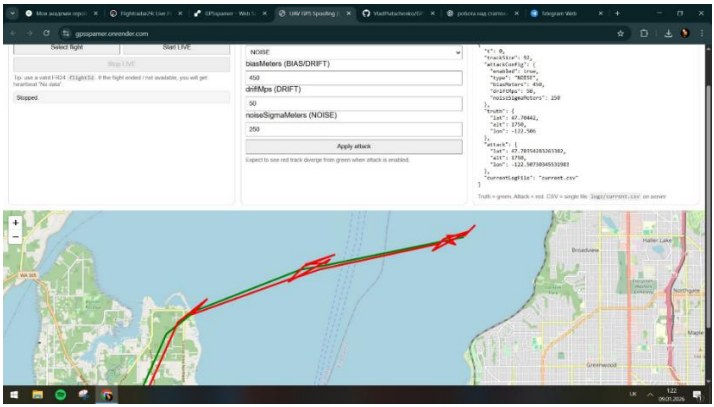

Рисунок 1 – Емуляція атаки підміни координат на основі реальної траєкторії руху об’єкта

Формування атакованих координат здійснюється шляхом додавання до реальної позиції комбінованої помилки, що складається із систематичного зміщення, поступового дрейфу та випадкового шуму. У загальному вигляді атакована позиція визначається як

$$P_a(t) = P(t) + \Delta bias + \Delta drift(t) + \Delta noise,$$

де $\Delta bias$ задає постійне зміщення координат, $\Delta drift(t)$ моделює поступове відведення позиції від реальної траєкторії, а $\Delta noise$ представляє випадкову компоненту помилки. Компонента дрейфу відповідає типовому сценарію drag-off spoofing, у якому підроблений навігаційний сигнал поступово відводить розраховане положення приймача від реальної траєкторії без різких стрибків координат.

Реалізований підхід дозволяє формувати контрольовані сценарії атак та використовувати їх для тестування методів виявлення GNSS-спуфінгу. Подальші дослідження можуть бути спрямовані на розширення моделей атак і використання отриманих даних для навчання та оцінювання алгоритмів машинного навчання.

Список використаних джерел

1. Meng, L., Yang, L., Yang, W., & Zhang, L. (2022). A Survey of GNSS Spoofing and Anti-Spoofing Technology. Remote Sensing, 14(19), 4826. https://doi.org/10.3390/rs14194826

2. He, Y., Zhuang, X., & Xu, B. (2025). Sparse Decomposition-Based Anti-Spoofing Framework for GNSS Receiver: Spoofing Detection, Classification, and Position Recovery. Remote Sensing, 17(15), 2703. https://doi.org/10.3390/rs17152703

3. Wang, W., Wang, J.(2022). GNSS induced spoofing simulation based on path planning. IET Radar Sonar Navig. 16(1), 103–112. https://doi.org/10.1049/rsn2.12167